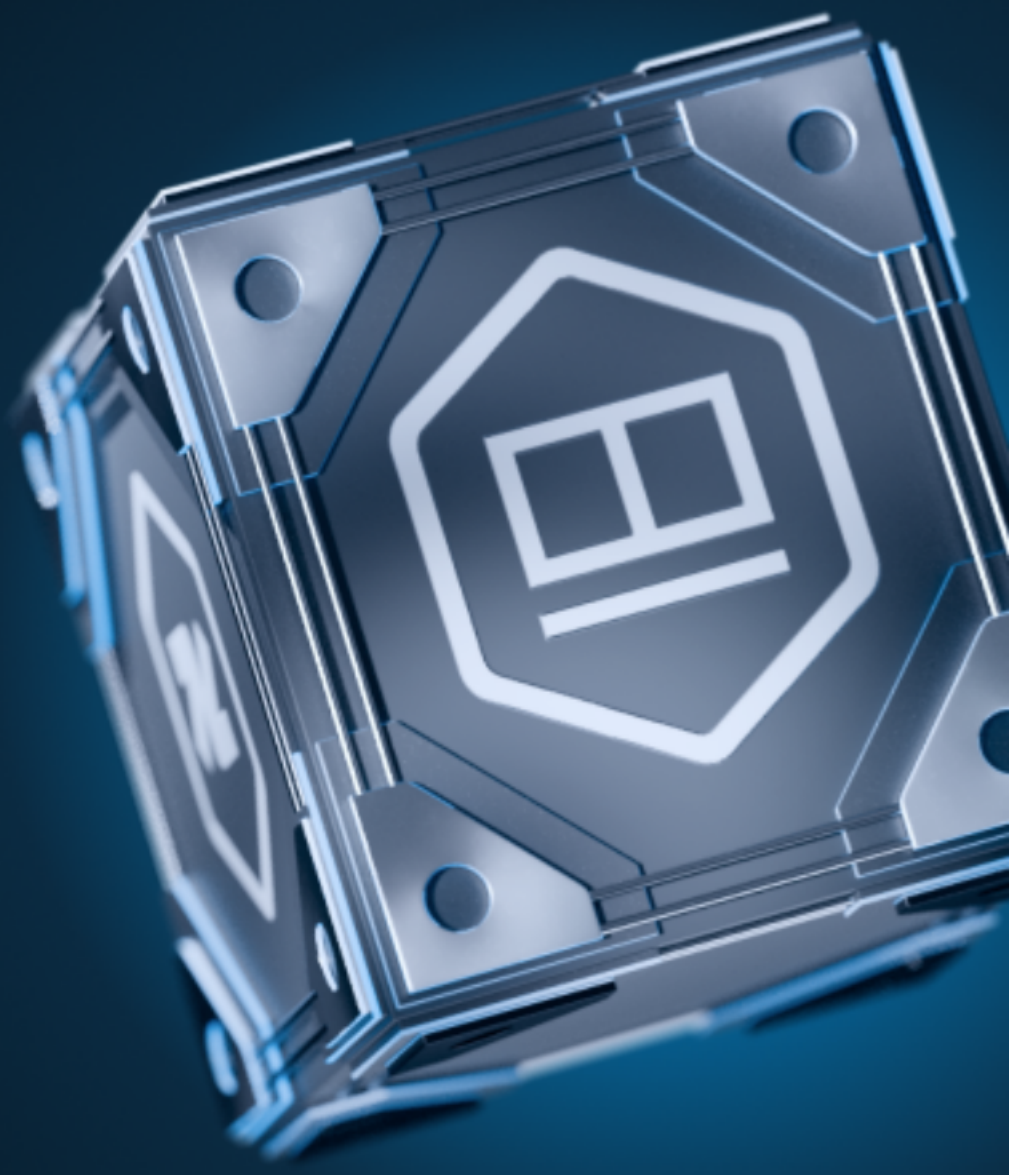
TERMIDESK VDI



Версия v7.0.2, 2026-10-09

Оглавление

СЛЕТ.10001-01 90 01. РУКОВОДСТВО АДМИНИСТРАТОРА. УСТАНОВКА ПРОГРАММНОГО КОМПЛЕКСА . . . 13
ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ . . . 13
ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММНОМ КОМПЛЕКСЕ . . . 13
Общие сведения о Termidesk VDI . . . 13
Требования к настройкам инфраструктуры . . . 24
Контекстуализация в ПК СВ Брест . . . 28
Получение пакетов установки . . . 28
Подготовка среды функционирования . . . 32
УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ TERMIDESK . . . 40
ОС Astra Linux Special Edition . . . 40
Проверка работоспособности после установки . . . 82
ЛИЦЕНЗИРОВАНИЕ . . . 83
НЕШТАТНЫЕ СИТУАЦИИ . . . 94
ТЕРМИНЫ . . . 97
СОКРАЩЕНИЯ . . . 100
СЛЕТ.10001-01 90 02. РУКОВОДСТВО АДМИНИСТРАТОРА. НАСТРОЙКА ПРОГРАММНОГО КОМПЛЕКСА . . . 103
ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ . . . 103
КОМПОНЕНТЫ И ИХ ВЗАИМОДЕЙСТВИЕ . . . 103
Схема взаимодействия компонентов и приложений . . . 103
Схема сетевого взаимодействия компонентов Termidesk VDI . . . 104
Последовательность сетевых запросов компонентов Termidesk VDI . . . 106
Перечень сетевых портов компонентов Termidesk VDI . . . 107
Перечень разрешающих правил межсетевого экрана для работы компонентов Termidesk VDI . . . 111
Перечень сертификатов и ключей для компонентов Termidesk VDI . . . 120
НАЧАЛО РАБОТЫ . . . 121
Последовательность ввода в действие Termidesk VDI . . . 121
Подготовка базового шаблона ВМ . . . 123
НАСТРОЙКА ГОСТЕВОЙ ОС РМ . . . 129
Обязательные настройки гостевой ОС РМ . . . 129
Опциональные настройки функционала для гостевой ОС РМ . . . 137
Технология бездисковой (сетевой) загрузки . . . 164
ДОМЕНЫ АУТЕНТИФИКАЦИИ . . . 188
Добавление доменов аутентификации . . . 188
Действия над группами в домене аутентификации . . . 251
Действия над пользователями в домене аутентификации . . . 257
Просмотр данных о пользователе домена аутентификации . . . 260
Действия над атрибутами в домене аутентификации . . . 261
ПОСТАВЩИКИ РЕСУРСОВ . . . 262
Добавление поставщиков ресурсов . . . 262
Режим техобслуживания поставщика ресурсов . . . 299
ШАБЛОНЫ РМ В ПОСТАВЩИКАХ РЕСУРСОВ . . . 299
ПАРАМЕТРЫ ГОСТЕВЫХ ОС . . . 326
Добавление параметров гостевых ОС . . . 326
Изменение изображения гостевых ОС . . . 334
Действие при выходе пользователя из ОС . . . 335

СЕТИ . . . 335
ПРОФИЛИ ШЛЮЗОВ . . . 337
ПРОТОКОЛЫ ДОСТАВКИ . . . 340
ПОЛИТИКИ . . . 358
БИБЛИОТЕКА СКРИПТОВ . . . 402
ТЕГИ . . . 404
ФОНД РМ . . . 407
Добавление фонда РМ . . . 407
Управление параметрами фонда РМ . . . 436
Объединение фондов в группы РМ . . . 441
Режим техобслуживания фонда РМ . . . 442
Публикация фонда РМ . . . 444
Настройка автоматического подключения к фонду РМ . . . 446
Управление расписанием задач . . . 447
СПИСКИ И СТАТУСЫ РМ . . . 451
Список РМ из всех фондов . . . 451
Статусы РМ . . . 461
УПРАВЛЕНИЕ СЕССИЯМИ И РМ . . . 463
Управление сессиями подключенных к фондам пользователей . . . 463
Управление терминальными сессиями . . . 467
Управление состоянием терминальных серверов . . . 470
Управление состоянием ВМ в назначенном фонде РМ . . . 470
Управление состоянием автономных машин в назначенном фонде . . . 476
Назначение владельца РМ . . . 479
Фильтрация списка сессий . . . 480
РАЗГРАНИЧЕНИЕ ФУНКЦИЙ АДМИНИСТРАТОРОВ И ПОЛЬЗОВАТЕЛЕЙ . . . 483
Разграничение функций . . . 483
Назначение служебных функций администраторам . . . 484
СИСТЕМНЫЕ НАСТРОЙКИ . . . 492
Конфигурационные файлы сервера Termidesk VDI . . . 492
Общие системные параметры Termidesk VDI . . . 529
Параметры безопасности Termidesk VDI . . . 538
Управление параметрами компонента «Клиент» . . . 539
Настройка отправки метрик для «Сессионного агента» . . . 546
Брендирование Termidesk VDI . . . 548
Управление экспериментальными параметрами Termidesk VDI . . . 551
Хранение чувствительной информации с выбранным способом хранения «hvac» . . . 557
Изменение способа хранения паролей на OpenBao . . . 563
Перенаправление на HTTPS . . . 564
Замена SSL-сертификата веб-сервера . . . 566
Установка корневого сертификата центра сертификации . . . 567
Работа веб-интерфейса Termidesk VDI с протоколом TLS . . . 568
Настройка mTLS . . . 569
Настройки после распределенной установки фермы Termidesk VDI . . . 573
Генерация отчета по моделям данных и структурам БД Termidesk VDI . . . 577
РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ . . . 578
УПРАВЛЕНИЕ ИНФРАСТРУКТУРОЙ TERMIDESK . . . 584
МОНИТОРИНГ И УВЕДОМЛЕНИЯ . . . 603
Настройка отправки уведомлений о системных событиях . . . 603

Шаблон для мониторинга Zabbix . . . 607
Получение метрик узлов компонентов . . . 607
Отслеживание жизненного цикла сессий и ресурсов пользователей . . . 615
Рекомендации по настройке отслеживания состояния компонентов Termidesk VDI . 616
СИСТЕМА АУДИТА . . . 620
Системные параметры аудита . . . 620
Описание шаблонов событий аудита . . . 621
Формат CEF . . . 642
ЖУРНАЛИРОВАНИЕ . . . 643
Системные параметры журналирования . . . 643
Настройка уровня журналирования сервера Termidesk VDI . . . 644
Журналы сервера Termidesk VDI . . . 644
Просмотр журналов в «Портале администратора» . . . 645
Просмотр централизованных журналов фермы Termidesk VDI . . . 648
Отчеты . . . 652
ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ TERMIDESK . . . 655
Утилита `termidesk-vdi-manage` . . . 655
Утилита `termidesk-config` . . . 664
Утилита `scramble` . . . 669
НЕШТАТНЫЕ СИТУАЦИИ . . . 671
ТЕРМИНЫ . . . 676
СОКРАЩЕНИЯ . . . 678
СЛЕТ.10001-01 90 03. РУКОВОДСТВО АДМИНИСТРАТОРА. ГРАФИЧЕСКИЙ ИНТЕРФЕЙС УПРАВЛЕНИЯ ПРОГРАММНЫМ КОМПЛЕКСОМ . . . 684
ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ . . . 684
ДОСТУП К ВЕБ-ИНТЕРФЕЙСУ . . . 684
ТИПЫ ВЕБ-ИНТЕРФЕЙСА TERMIDESK И ИЗМЕНЕНИЕ ФОНА . . . 685
РАБОТА С ОСНОВНЫМИ ФУНКЦИЯМИ ВЕБ-ИНТЕРФЕЙСА . . . 685
ТЕРМИНЫ . . . 693
СОКРАЩЕНИЯ . . . 694
СЛЕТ.10001-01 90 04. РУКОВОДСТВО АДМИНИСТРАТОРА. НАСТРОЙКА КОМПОНЕНТА «АГЕНТ» . . . 696
ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ . . . 696
АГЕНТ. ОБЩИЕ СВЕДЕНИЯ . . . 696
АГЕНТ. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ . . . 698
АГЕНТ. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ . . . 704
ОС Astra Linux Special Edition . . . 704
ОС Альт Рабочая станция . . . 713
Другие ОС Linux . . . 718
ОС Microsoft Windows . . . 721
АГЕНТ. НАСТРОЙКИ . . . 728
Переменные окружения и аргументы командной строки . . . 728
Агент ВРМ . . . 737
Конфигурационные файлы Агента ВРМ . . . 737
Настройка для ОС Astra Linux Special Edition . . . 747
Настройка для ОС Microsoft Windows . . . 758
Хранение информации о сессии пользователя . . . 768
Агент виртуальных смарт-карт . . . 770
Настройка Агента виртуальных смарт-карт . . . 770

Видеоагент . . . 771
Настройка видеоагента . . . 771
Агент узла виртуализации . . . 771
Использование альтернативного механизма сброса сессий . . . 772
Сессионный Агент . . . 774
Конфигурационные файлы сессионного Агента . . . 774
Первичная настройка . . . 784
Настройка сессионного Агента на использование протокола HTTPS . . . 784
Активация роли терминального сервера в ОС Microsoft Windows Server . . . 785
АГЕНТ. ЖУРНАЛИРОВАНИЕ . . . 785
АГЕНТ. НЕШТАТНЫЕ СИТУАЦИИ И СПОСОБЫ ИХ УСТРАНЕНИЯ . . . 789
ТЕРМИНЫ . . . 790
СОКРАЩЕНИЯ . . . 792
СЛЕТ.10001-01 90 06. РУКОВОДСТВО АДМИНИСТРАТОРА. НАСТРОЙКА КОМПОНЕНТА «ОРКЕСТРАТОР» . . . 794
ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ . . . 794
ОРКЕСТРАТОР. ОБЩИЕ СВЕДЕНИЯ . . . 794
ОРКЕСТРАТОР. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ . . . 795
ОРКЕСТРАТОР. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ . . . 798
Настройки среды функционирования . . . 798
ОС Astra Linux Special Edition . . . 799
Проверка работоспособности Оркестратора . . . 801
ОРКЕСТРАТОР. НАСТРОЙКИ . . . 803
Настройка сервера apache2 для Оркестратора . . . 803
Настройка Оркестратора . . . 803
Проверка заданных настроек Оркестратора . . . 804
Конфигурационные файлы Оркестратора . . . 804
Запуск служб Оркестратора . . . 806
ОРКЕСТРАТОР. ЖУРНАЛИРОВАНИЕ . . . 806
ТЕРМИНЫ . . . 806
СОКРАЩЕНИЯ . . . 807
СЛЕТ.10001-01 90 07. РУКОВОДСТВО АДМИНИСТРАТОРА. НАСТРОЙКА КОМПОНЕНТА «СЕРВЕР ТЕРМИНАЛОВ ASTRA LINUX» . . . 808
ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ . . . 808
STAL. ОБЩИЕ СВЕДЕНИЯ . . . 808
STAL. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ . . . 809
STAL. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ . . . 813
ОС Astra Linux Special Edition . . . 813
ОС Альт Рабочая станция . . . 817
STAL. НАСТРОЙКИ . . . 818
Конфигурационные файлы STAL . . . 818
Настройка динамического разрешения экрана и поддержки высокого разрешения 837
Задание списка разрешенных программ в STAL . . . 838
Задание списка запрещенных программ в STAL . . . 839
Ограничение ресурсов сессий пользователя . . . 839
Оптимизация работы FreeRDP3 . . . 839
Аутентификация OIDC в STAL . . . 840
Kerberos-аутентификация в STAL . . . 840
Аутентификация по смарт-картам в STAL . . . 843

STAL. ПЕРЕНАПРАВЛЕНИЕ РЕСУРСОВ . . . 844
Общие сведения по перенаправлению ресурсов в STAL . . . 844
Перенаправление принтеров в STAL . . . 844
Перенаправление дисков в STAL . . . 846
Перенаправление смарт-карт в STAL . . . 846
Перенаправление веб-камер в STAL . . . 846
STAL. ЖУРНАЛИРОВАНИЕ . . . 847
Журналирование в STAL . . . 847
Сбор журналов STAL для передачи в техническую поддержку . . . 847
STAL. НЕШТАТНЫЕ СИТУАЦИИ И СПОСОБЫ ИХ УСТРАНЕНИЯ . . . 848
ТЕРМИНЫ . . . 852
СОКРАЩЕНИЯ . . . 852
СЛЕТ.10001-01 90 08. РУКОВОДСТВО АДМИНИСТРАТОРА. УСТАНОВКА И НАСТРОЙКА «АГРЕГАТОРА» . . . 855
ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ . . . 855
АГРЕГАТОР. ОБЩИЕ СВЕДЕНИЯ . . . 855
АГРЕГАТОР. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ . . . 858
АГРЕГАТОР. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ . . . 861
Подготовка среды функционирования для «Агрегатора» . . . 861
ОС Astra Linux Special Edition . . . 862
Проверка работоспособности после установки «Агрегатора» . . . 886
АГРЕГАТОР. НАСТРОЙКА АГРЕГАЦИИ РЕСУРСОВ . . . 886
АГРЕГАТОР. ДОМЕНЫ АУТЕНТИФИКАЦИИ . . . 887
Добавление доменов аутентификации в «Агрегаторе» . . . 887
Действия над группами в домене аутентификации в «Агрегаторе» . . . 917
Действия над пользователями в домене аутентификации в «Агрегаторе» . . . 919
Просмотр данных о пользователе домена аутентификации в «Агрегаторе» . . . 921
Действия над атрибутами в домене аутентификации в «Агрегаторе» . . . 922
АГРЕГАТОР. ФЕРМЫ ПОСТАВЩИКОВ РЕСУРСОВ . . . 923
АГРЕГАТОР. УЗЛЫ ФЕРМ ПОСТАВЩИКОВ РЕСУРСОВ . . . 928
АГРЕГАТОР. САЙТЫ . . . 931
АГРЕГАТОР. ШАБЛОНЫ ТЕХОБСЛУЖИВАНИЯ . . . 942
АГРЕГАТОР. ШЛЮЗЫ . . . 943
АГРЕГАТОР. ТЕГИ . . . 945
АГРЕГАТОР. КОНСОЛЬ УПРАВЛЕНИЯ ФЕРМАМИ . . . 947
АГРЕГАТОР. НАЗНАЧЕНИЕ СЛУЖЕБНЫХ ФУНКЦИЙ АДМИНИСТРАТОРАМ . . . 951
АГРЕГАТОР. НАСТРОЙКИ . . . 954
Конфигурационные файлы «Агрегатора» . . . 954
Общие системные настройки «Агрегатора» . . . 992
Системные настройки безопасности «Агрегатора» . . . 995
АГРЕГАТОР. СИСТЕМА АУДИТА . . . 996
Системные настройки аудита «Агрегатора» . . . 996
Описание шаблонов событий аудита «Агрегатора» . . . 998
Формат `CEF` в «Агрегаторе» . . . 1009
АГРЕГАТОР. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ . . . 1010
Утилита `termidesk-vdi-manage` в «Агрегаторе» . . . 1010
Утилита `termidesk-config` в «Агрегаторе» . . . 1013
Утилита `scramble` в «Агрегаторе» . . . 1019
АГРЕГАТОР. ГРАФИЧЕСКИЙ ИНТЕРФЕЙС . . . 1021

Доступ к веб-интерфейсу «Агрегатора» . . . 1021
Типы веб-интерфейса «Агрегатора» . . . 1022
Работа с основными функциями веб-интерфейса «Агрегатора» . . . 1022
АГРЕГАТОР. ЖУРНАЛИРОВАНИЕ . . . 1025
Системные настройки журналирования «Агрегатора» . . . 1025
Настройка уровня журналирования «Агрегатора» . . . 1026
Журналы «Агрегатора» . . . 1026
Просмотр журналов в «Агрегаторе» . . . 1027
ТЕРМИНЫ . . . 1030
СОКРАЩЕНИЯ . . . 1030
СЛЕТ.10001-01 90 09. РУКОВОДСТВО АДМИНИСТРАТОРА. НАСТРОЙКА КОМПОНЕНТА TERA . . . 1033
ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ . . . 1033
TERA. ОБЩИЕ СВЕДЕНИЯ . . . 1033
TERA. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ . . . 1035
TERA. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ . . . 1041
ОС Astra Linux Special Edition . . . 1041
ОС Microsoft Windows . . . 1054
TERA. НАСТРОЙКИ В ОС LINUX . . . 1058
Конфигурационные файлы TERA в ОС Linux . . . 1058
Исполняемые файлы TERA в ОС Linux . . . 1107
Параметры запуска служб TERA . . . 1112
Переменные окружения . . . 1120
Блокирование локального доступа при подключении к физической машине . . . 1123
Разблокирование физической машины с помощью интерфейсов ввода . . . 1124
Режимы запуска ПО x11tera . . . 1124
Аутентификация подключений к TERA в ОС Linux . . . 1126
SASL-аутентификация в TERA . . . 1127
Kerberos-аутентификация в TERA . . . 1130
Разделение каналов и их приоритизация в TERA . . . 1131
Переключение протоколов TCP и UDP в TERA . . . 1132
Защита TCP-подключения с использованием SSL/TLS . . . 1134
TERA. НАСТРОЙКИ В ОС MICROSOFT WINDOWS . . . 1135
Конфигурационные файлы TERA в ОС Microsoft Windows . . . 1135
Просмотр списка сессий TERA в ОС Microsoft Windows . . . 1143
Аутентификация подключений к TERA в ОС Microsoft Windows . . . 1144
Сценарии подключений к TERA в ОС Windows . . . 1146
TERA. ОБЩИЕ НАСТРОЙКИ ДЛЯ ВСЕХ ОС . . . 1146
Масштабирование элементов клиентского приложения . . . 1146
TERA. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ . . . 1147
Интерфейс командной строки ПО x11tera . . . 1147
Интерфейс командной строки утилиты `x11tera_unlock` . . . 1149
Интерфейс командной строки ПО tera-vdagent . . . 1151
Интерфейс командной строки ПО tera-vdagentd . . . 1153
Интерфейс командной строки ПО tera-router . . . 1155
Интерфейс командной строки ПО tera-gateway . . . 1159
Интерфейс командной строки ПО tera-webdav . . . 1160
TERA. ЖУРНАЛИРОВАНИЕ . . . 1161
TERA. НЕШТАТНЫЕ СИТУАЦИИ И СПОСОБЫ ИХ УСТРАНЕНИЯ . . . 1164

ТЕРМИНЫ . . . 1173
СОКРАЩЕНИЯ . . . 1173
СЛЕТ.10001-01 90 10. РУКОВОДСТВО АДМИНИСТРАТОРА. НАСТРОЙКА КОМПОНЕНТА «РЕТРАНСЛЯТОР» . . . 1175
ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ . . . 1175
РЕТРАНСЛЯТОР. ОБЩИЕ СВЕДЕНИЯ . . . 1175
РЕТРАНСЛЯТОР. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ . . . 1176
РЕТРАНСЛЯТОР. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ . . . 1179
Подготовка среды функционирования для «Ретранслятора» . . . 1179
ОС Astra Linux Special Edition . . . 1182
РЕТРАНСЛЯТОР. НАСТРОЙКИ . . . 1184
Конфигурационные файлы «Ретранслятора» . . . 1184
РЕТРАНСЛЯТОР. ЖУРНАЛИРОВАНИЕ . . . 1192
РЕТРАНСЛЯТОР. НЕШТАТНЫЕ СИТУАЦИИ И СПОСОБЫ ИХ УСТРАНЕНИЯ . . . 1192
ТЕРМИНЫ . . . 1192
СОКРАЩЕНИЯ . . . 1193
СЛЕТ.10001-01 90 11. РУКОВОДСТВО АДМИНИСТРАТОРА. УСТАНОВКА И НАСТРОЙКА TERMIDESK PROFILES . . . 1194
ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ . . . 1194
TERMIDESK PROFILES. ОБЩИЕ СВЕДЕНИЯ . . . 1194
TERMIDESK PROFILES. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ . . . 1195
TERMIDESK PROFILES. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ . . . 1198
Подготовка среды функционирования . . . 1198
ОС Astra Linux Special Edition . . . 1204
Проверка работоспособности после установки . . . 1211
TERMIDESK PROFILES. НАЧАЛО РАБОТЫ . . . 1213
TERMIDESK PROFILES. ХРАНИЛИЩА . . . 1213
Общие сведения о хранилищах . . . 1213
Добавление хранилища . . . 1215
TERMIDESK PROFILES. ДОМЕНЫ АУТЕНТИФИКАЦИИ . . . 1216
Общие сведения о доменах аутентификации . . . 1216
Добавление доменов аутентификации . . . 1216
TERMIDESK PROFILES. ШАБЛОНЫ . . . 1218
Общие сведения о шаблонах . . . 1218
Настройка шаблона . . . 1220
Создание шаблона . . . 1221
TERMIDESK PROFILES. КОНФИГУРАЦИИ ДОСТАВКИ . . . 1221
Общие сведения о конфигурациях доставки . . . 1221
Добавление конфигурации доставки . . . 1222
TERMIDESK PROFILES. ОБРАЗЫ ПЕРЕМЕЩАЕМЫХ ПРОФИЛЕЙ . . . 1222
Общие сведения об образах Перемещаемых пПофилей . . . 1222
Просмотр списка базовых образов . . . 1222
Просмотр списка активных образов . . . 1223
TERMIDESK PROFILES. АГЕНТЫ . . . 1224
Общие сведения об агентах . . . 1224
Добавление группы агентов . . . 1224
Просмотр сведений об агенте . . . 1225
Просмотр списка агентов . . . 1226
TERMIDESK PROFILES. РАЗГРАНИЧЕНИЕ РОЛЕЙ АДМИНИСТРАТОРОВ И

ПОЛЬЗОВАТЕЛЕЙ . . . 1226
Разграничение ролей . . . 1226
Управление ролями . . . 1227
TERMIDESK PROFILES. СИСТЕМНЫЕ НАСТРОЙКИ . . . 1228
Общие системные параметры Termidesk Profiles . . . 1228
Параметры безопасности Termidesk Profiles . . . 1229
Параметры конфигурирования агентской части . . . 1230
Файл `/etc/default/trp-server` . . . 1231
Файл `/etc/default/trp-agent` . . . 1232
Переменные окружения . . . 1232
TERMIDESK PROFILES. СИСТЕМА АУДИТА . . . 1233
Системные параметры аудита . . . 1233
Просмотр событий аудита серверной части Termidesk Profiles . . . 1234
TERMIDESK PROFILES. ЖУРНАЛИРОВАНИЕ . . . 1236
Системные параметры журналирования . . . 1236
Журналы . . . 1238
Просмотр журналов серверной части Termidesk Profiles . . . 1238
TERMIDESK PROFILES. ВЕБ-ИНТЕРФЕЙС СЕРВЕРНОЙ ЧАСТИ . . . 1240
Доступ к веб-интерфейсу серверной части . . . 1240
Обзор доступных функций веб-интерфейса . . . 1240
TERMIDESK PROFILES. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ . . . 1243
Интерфейс командной строки серверной части Termidesk Profiles . . . 1243
TERMIDESK PROFILES. НЕШТАТНЫЕ СИТУАЦИИ И СПОСОБЫ ИХ УСТРАНЕНИЯ . . . 1249
ТЕРМИНЫ . . . 1249
СОКРАЩЕНИЯ . . . 1250
СЛЕТ.10001-01 92 01. РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ. НАСТРОЙКА И ЭКСПЛУАТАЦИЯ КОМПОНЕНТА «КЛИЕНТ» . . . 1251
ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ . . . 1251
КЛИЕНТ. ОБЩИЕ СВЕДЕНИЯ . . . 1251
КЛИЕНТ. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ . . . 1254
КЛИЕНТ. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ . . . 1260
ОС Astra Linux Special Edition . . . 1260
Другие ОС Linux . . . 1263
ОС macOS . . . 1265
ОС Microsoft Windows . . . 1268
КЛИЕНТ. ПОДКЛЮЧЕНИЕ К СЕРВЕРУ TERMIDESK . . . 1277
КЛИЕНТ. ПОДКЛЮЧЕНИЕ К РЕСУРСАМ . . . 1284
Подключение к РМ . . . 1284
Настройки подключения к РМ . . . 1292
КЛИЕНТ. АУТЕНТИФИКАЦИЯ В РАЗЛИЧНЫХ СЦЕНАРИЯХ . . . 1298
КЛИЕНТ. ДОСТУП К ДЕМОНСТРАЦИОННОМУ СТЕНДУ . . . 1308
КЛИЕНТ. ЦЕНТР ПОДКЛЮЧЕНИЙ . . . 1310
КЛИЕНТ. НАСТРОЙКИ . . . 1312
Конфигурационные файлы Клиента и ПО Termidesk Viewer . . . 1312
Установка корневых сертификатов в ОС macOS . . . 1317
КЛИЕНТ. ГРАФИЧЕСКИЙ ИНТЕРФЕЙС . . . 1317
КЛИЕНТ. ИнтерИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ . . . 1321
КЛИЕНТ. ВОЗМОЖНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ПО TERMIDESK VIEWER . . . 1330
КЛИЕНТ. ПЕРЕНАПРАВЛЕНИЕ РЕСУРСОВ . . . 1343

Перенаправление USB-устройств . . . 1343
Перенаправление USB-гарнитуры . . . 1345
Перенаправление принтеров . . . 1347
Перенаправление смарт-карт . . . 1351
Перенаправление каталогов . . . 1353
Перенаправление домашнего каталога пользователя . . . 1354
Перенаправление веб-камер . . . 1354
КЛИЕНТ. ЗАВЕРШЕНИЕ РАБОТЫ . . . 1356
КЛИЕНТ. ЖУРНАЛИРОВАНИЕ . . . 1361
КЛИЕНТ. НЕШТАТНЫЕ СИТУАЦИИ И СПОСОБЫ ИХ УСТРАНЕНИЯ . . . 1362
ТЕРМИНЫ . . . 1372
СОКРАЩЕНИЯ . . . 1373
СЛЕТ.10001-01 91 01. ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ. REST API . . . 1376
ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ . . . 1376
REST API. НАЗНАЧЕНИЕ . . . 1376
«УНИВЕРСАЛЬНЫЙ ДИСПЕТЧЕР» . . . 1377
Начало работы с REST API компонента «Универсальный диспетчер» Termidesk VDI . 1377
Команды компонента «Универсальный диспетчер» . . . 1381
«АГРЕГАТОР» . . . 1407
Начало работы с REST API портала «Агрегатор» . . . 1407
Команды портала «Агрегатор» . . . 1411
«ШЛЮЗ» . . . 1425
Начало работы с REST API компонента «Шлюз» . . . 1425
Команды компонента «Шлюз» . . . 1426
«АГЕНТ ВИРТУАЛЬНОГО РАБОЧЕГО МЕСТА» . . . 1429
Начало работы с REST API компонента «Агент виртуального рабочего места» . . . 1429
Команды компонента «Агент виртуального рабочего места» . . . 1430
«СЕССИОННЫЙ АГЕНТ» . . . 1433
Начало работы с REST API компонента «Сессионный агент» . . . 1433
Команды компонента «Сессионный агент» . . . 1434
«ОРКЕСТРАТОР» . . . 1436
Начало работы с REST API компонента «Оркестратор» . . . 1436
Команды компонента «Оркестратор» . . . 1437
«УДАЛЕННЫЙ ПОМОЩНИК» . . . 1440
Начало работы с REST API компонента «Удаленный помощник» . . . 1440
Команды компонента «Удаленный помощник» . . . 1441
ТЕРМИНЫ . . . 1441
СОКРАЩЕНИЯ . . . 1443
СЛЕТ.10001-01 91 02. ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ. КОМПОНЕНТ «УДАЛЕННЫЙ ПОМОЩНИК» . . . 1445
ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ . . . 1445
УДАЛЕННЫЙ ПОМОЩНИК. ОБЩИЕ СВЕДЕНИЯ . . . 1445
УДАЛЕННЫЙ ПОМОЩНИК. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ . . . 1446
УДАЛЕННЫЙ ПОМОЩНИК. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ . . . 1449
ОС Astra Linux Special Edition . . . 1449
Другие ОС Linux . . . 1454
ОС Microsoft Windows . . . 1456
УДАЛЕННЫЙ ПОМОЩНИК. НАСТРОЙКИ . . . 1459
Конфигурационные файлы «Удаленного помощника» . . . 1459

Переменные окружения «Удаленного помощника» . . . 1468
Количество одновременных подключений к серверу «Удаленного помощника» . . . 1471
Управление поведением курсора . . . 1471
Замена SSL-сертификата веб-сервера для «Удаленного помощника» . . . 1471
Взаимодействие с серверной частью «Удаленного помощника» по REST API . . . 1472
Отправка событий на сервер syslog для «Удаленного помощника» . . . 1474
УДАЛЕННЫЙ ПОМОЩНИК. ПОДКЛЮЧЕНИЕ И ОТКЛЮЧЕНИЕ . . . 1474
Подключение к удаленному рабочему столу . . . 1474
Завершение демонстрации рабочего стола . . . 1477
Возможности при подключении . . . 1478
УДАЛЕННЫЙ ПОМОЩНИК. ГРАФИЧЕСКИЙ ИНТЕРФЕЙС . . . 1479
УДАЛЕННЫЙ ПОМОЩНИК. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ . . . 1481
УДАЛЕННЫЙ ПОМОЩНИК. ЖУРНАЛИРОВАНИЕ . . . 1483
УДАЛЕННЫЙ ПОМОЩНИК. НЕШТАТНЫЕ СИТУАЦИИ И СПОСОБЫ ИХ УСТРАНЕНИЯ . . . 1483
ТЕРМИНЫ . . . 1484
СОКРАЩЕНИЯ . . . 1484
СЛЕТ.10001-01 91 03. ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ. КОМПОНЕНТ «ВИРТУАЛЬНЫЙ МОДУЛЬ TERMIDESK» (ВМТ) . . . 1486
ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ . . . 1486
ВМТ. ОБЩИЕ СВЕДЕНИЯ . . . 1486
ВМТ. ПОЛУЧЕНИЕ ОБРАЗОВ . . . 1487
ВМТ. УСТАНОВКА И ОБНОВЛЕНИЕ . . . 1487
Установка ВМТ . . . 1487
Обновление ВМТ . . . 1510
ВМТ. ДЕЙСТВИЯ В ГЛАВНОМ МЕНЮ . . . 1525
Изменение настроек сети . . . 1525
Диагностика сети . . . 1526
Изменение имени узла ВМТ . . . 1526
Смена пароля администратора ВМТ . . . 1527
Синхронизация параметров между ВМТ . . . 1528
ВМТ. НАСТРОЙКИ . . . 1530
Резервное копирование и восстановление БД для ВМТ . . . 1530
Удаленное подключение к ВМТ . . . 1532
ВМТ. ВЕБ-ИНТЕРФЕЙС . . . 1532
Обзор доступных функций веб-интерфейса ВМТ . . . 1532
Управление состоянием служб ВМТ . . . 1533
Формирование и выгрузка журнала ВМТ . . . 1534
Просмотр и замена сертификата через веб-интерфейс ВМТ . . . 1535
Управление датой и временем на ВМТ . . . 1538
ВМТ. ЗАВЕРШЕНИЕ РАБОТЫ . . . 1540
ТЕРМИНЫ . . . 1541
СОКРАЩЕНИЯ . . . 1542
СЛЕТ.10001-01 91 04. ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ. КОМПОНЕНТ TERMIDESK LIVE 1544
ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ . . . 1544
TERMIDESK LIVE. ОБЩИЕ СВЕДЕНИЯ . . . 1544
TERMIDESK LIVE. ПОЛУЧЕНИЕ ОБРАЗОВ . . . 1545
TERMIDESK LIVE. ПОДГОТОВКА К РАБОТЕ . . . 1545
Подготовка к загрузке с USB-носителя . . . 1545
Подготовка к PXE-загрузке по сети . . . 1549

TERMIDESK LIVE. НАСТРОЙКИ . . . 1553
Добавление приложений в Termidesk Live . . . 1553
TERMIDESK LIVE. РАБОТА С ОБРАЗОМ . . . 1559
Загрузка в ОС Termidesk Live . . . 1559
Начало работы в ОС Termidesk Live . . . 1561
TERMIDESK LIVE. ЗАВЕРШЕНИЕ РАБОТЫ . . . 1561
TERMIDESK LIVE. НЕШТАТНЫЕ СИТУАЦИИ И СПОСОБЫ ИХ УСТРАНЕНИЯ . . . 1561
ТЕРМИНЫ . . . 1570
СОКРАЩЕНИЯ . . . 1571

СЛЕТ.10001-01 90 01. РУКОВОДСТВО АДМИНИСТРАТОРА. УСТАНОВКА ПРОГРАММНОГО КОМПЛЕКСА

ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ

Назначение документа

Настоящий документ является первой частью руководства администратора на программный комплекс «Диспетчер подключений виртуальных рабочих мест Термидеск» (далее - Termidesk VDI, Termidesk VDI). Документ предназначен для администраторов системы и сети.

В первой части руководства приведено назначение и установка Termidesk VDI. Для того, чтобы получить информацию о настройке Termidesk VDI, необходимо обратиться ко второй части руководства администратора - СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

Типографские соглашения

Приняты следующие типографские соглашения:

- `моноширинный шрифт` – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk VDI, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММНОМ КОМПЛЕКСЕ

Общие сведения о Termidesk VDI

Назначение и основные характеристики Termidesk

Назначение

Termidesk VDI предназначен для доставки рабочих мест (РМ), таких, как: виртуальных рабочих мест (ВРМ), приложений, а также для организации терминального доступа пользователей к ресурсам посредством различных протоколов удаленного доступа.

Область применения

Termidesk VDI:

- может применяться для создания или модернизации инфокоммуникационной инфраструктуры масштаба организации, а также поставщиками услуг, реализующих облачную услугу РМ;
- ориентирован на образовательные и иные организации, в которых предусмотрено использование одного РМ множеством пользователей, с возможностью очистки РМ по

завершению сеанса работы;

- удобен для использования в организациях с обширной сетью филиалов;
- позволяет реализовать политики повышенных требований к безопасности данных, препятствующих несанкционированному распространению информации.

Помимо этого, Termidesk VDI обеспечивает работу с виртуализированными графическими процессорами (vGPU) и адаптацию к низкоскоростным каналам связи.

Основные характеристики

Termidesk VDI состоит из ряда компонентов, которые могут быть либо отделяемыми (подразумевает выбор роли при установке из общего пакета), либо самостоятельными (компонент устанавливается из отдельного пакета, но используется в составе общего комплекса). Такое разделение обеспечивает гибкое масштабирование системы для различных сценариев применения.

В состав Termidesk VDI входят следующие компоненты:

- «Универсальный диспетчер» - компонент, отвечающий за идентификацию пользователей, назначение и контроля доставки им РМ (ВРМ, приложений, терминального доступа);
- «Менеджер рабочих мест» - компонент, отвечающий за взаимодействие с поставщиком ресурсов и управления жизненным циклом ВРМ, включая создание, настройку, запуск, отключение и удаление;
- «Агент» - компонент, отвечающий за контролируемую доставку РМ, взаимодействие с «Универсальным диспетчером» и «Менеджером рабочих мест»;
- «Клиент» - компонент, отвечающий за доставку РМ на пользовательскую рабочую станцию с возможностью перенаправления периферии, каталогов, и оптимизацию их использования в протоколе доставки;
- «Оркестратор» - компонент, отвечающий за автоматизацию развертывания Termidesk VDI в облачных структурах;
- «Сервер терминалов Astra Linux» (англ. Terminal Server Astra Linux, STAL) - компонент, отвечающий за организацию терминального доступа в ОС Astra Linux Special Edition;
- «Удаленный помощник» - компонент, предоставляющий администратору или специалисту технической поддержки экран пользователя через сеанс удаленного подключения и обеспечивающий передачу голосовой информации для взаимодействия с пользователем;
- «Виртуальный модуль Termidesk» - компонент, представляющий собой образ виртуальной машины (ВМ) (или диска ВМ) с предварительно установленной и настроенной операционной системой (ОС) и набором программного обеспечения (ПО), необходимого для эксплуатации Termidesk VDI. Компонент позволяет быстро развернуть и использовать серверные компоненты - «Универсальный диспетчер», «Шлюз», «Менеджер рабочих мест»;
- Termidesk Live - компонент, представляющий собой загрузочный образ ОС с предустановленным компонентом «Клиент»;
- TERA (англ. Termidesk Remote Access protocol) - протокол удаленного доступа собственной разработки;
- «Ретранслятор» - компонент, отвечающий за сбор и фильтрацию записей журналов, поступающих от компонентов Termidesk VDI, и их перенаправления в централизованное хранилище журналов;
- «Брокер сообщений TermideskMQ» - компонент, отвечающий за взаимодействие между различными компонентами или приложениями, обеспечивая надежную асинхронную передачу данных для компонентов Termidesk VDI;
- Termidesk Profiles - компонент, отвечающий за использование домашнего каталога

пользователя в сеансе удаленного доступа к виртуальному или физическому рабочему столу, а также на управляемом ПК организации. Решение позволяет размещать домашний каталог пользователя, поддерживаемого ОС Linux, на диске в `qcow2`-формате, расположенном в сетевом хранилище.

Компоненты «Универсальный диспетчер», «Менеджер рабочих мест», «Брокер сообщений TermideskMQ» являются отделяемыми, устанавливаемыми из единого пакета. Они могут разворачиваться как в комплексном варианте (на одном узле), так и в распределенной конфигурации (на разных узлах).

Остальные компоненты являются самостоятельными, но работающими в составе программного комплекса.

Компоненты могут быть объединены в фермы.

Ферма - логическое объединение узлов, взаимодействующих с одной базой данных (БД).

Для объединения ресурсов с ферм Termidesk VDI используется специальная роль, доступная при установке Termidesk VDI - «Агрегатор», являющаяся единой точкой входа для получения ресурсов пользователями.

Установка «Агрегатора» должна быть отделена от установки фермы Termidesk VDI и должна использовать отдельную БД.

К компоненту «Агент» относятся следующие подкомпоненты, каждый из которых устанавливается отдельно:

- «Агент виртуального рабочего места», устанавливается в гостевую ОС ВМ или в ОС автономной ВМ;
- «Агент узла виртуализации», устанавливается на узел виртуализации;
- «Сессионный агент», устанавливается на узел терминального сервера;
- «Видеоагент», устанавливается в гостевую ОС ВМ;
- «Агент виртуальных смарт-карт», устанавливается в гостевую ОС ВМ.

Termidesk VDI обеспечивает доставку РМ на пользовательскую рабочую станцию посредством следующих протоколов удаленного доступа:

- SPICE (оптимизированный);
- TERA;
- RDP;
- Loudplay.

Termidesk VDI реализует режим прямого и туннельного соединения. Прямое соединение позволяет подключиться к протоколу, запущенному внутри гостевой ОС или на гипервизоре. Туннельное соединение применяется при подключении к РМ из недоверенных сетей. Комбинация протоколов и способы подключения предопределены в Termidesk VDI.

Termidesk VDI поддерживает работу с платформами виртуализации:

- программный комплекс «Средства виртуализации «Брест» (далее - ПК СВ Брест);
- VMmanager;
- zVirt;

- oVirt;
- «РЕД Виртуализация»;
- Openstack (версия Xena);
- VMware vSphere.

Termidesk VDI поддерживает работу с терминальными серверами (терминальными сессиями и приложениями):

- Microsoft Windows Server с ролью «Remote Desktop Session Host» из состава «Remote Desktop Services» (далее - MS RDS, MS RDSH);
- Terminal Server Astra Linux, реализуется компонентом «Сервер терминалов Astra Linux» (STAL).

Требования к аппаратному и программному обеспечению

Требования к аппаратному обеспечению

Минимальные аппаратные требования к узлу приведены в таблице Минимальные аппаратные требования.

Комплексная установка рекомендуется для использования в тестовой среде при количестве не более 50 одновременных подключений. Рекомендуемые аппаратные требования для данного варианта установки не приводятся.

Таблица 1. Минимальные аппаратные требования

CPU, шт	RAM, ГБ	HDD, ГБ	Сеть, Мбит/с
Узел «Универсального диспетчера» в комплексном варианте установки			
4	4	80	100
Узел «Универсального диспетчера» с ролью «Портал универсальный»			
4	4	80	100
Узел «Универсального диспетчера» с ролью «Портал администратора»			
4	4	60	100
Узел «Универсального диспетчера» с ролью «Портал пользователя»			
4	4	80	100
Узел «Универсального диспетчера» с ролью «Менеджер рабочих мест»			
4	4	60	100
Узел СУБД PostgreSQL			
4	4	60	100
Узел брокера сообщений RabbitMQ			
2	4	60	100
Узел «Шлюза» (Termidesk Connect с лицензией Termidesk Connect Basic)			
2	12	50	100
Узел балансировщика нагрузки (Termidesk Connect с лицензией Termidesk Connect)			
2	12	50	100

Рекомендуемые аппаратные требования к узлу приведены в таблице Рекомендуемые аппаратные требования.

В производственной среде следует использовать конфигурацию, соответствующую рекомендуемым аппаратным требованиям, исходя из расчета:

- один узел «Универсального диспетчера» на каждые 1000 одновременных подключений;
- один узел «Шлюза» или балансировщика нагрузки Termidesk Connect на каждые 2000 одновременных подключений. Подробные сведения об аппаратных требованиях Termidesk Connect доступны по ссылке: Требования к аппаратному и программному обеспечению

Для узлов СУБД PostgreSQL и брокера сообщений RabbitMQ приведены рекомендуемые аппаратные требования для указанного количества одновременных подключений. При выборе аппаратной конфигурации данных узлов также необходимо учитывать требования, приведенные в документации соответствующих компонентов.

Таблица 2. Рекомендуемые аппаратные требования

CPU, шт	RAM, ГБ	HDD, ГБ	Сеть, Мбит/с
Узел «Универсального диспетчера» с ролью «Портал универсальный»			
8	8	80	100
Узел «Универсального диспетчера» с ролью «Портал администратора»			
4	4	60	100
Узел «Универсального диспетчера» с ролью «Портал пользователя»			
8	8	80	100
Узел «Универсального диспетчера» с ролью «Менеджер рабочих мест»			
4	4	60	100
Узел СУБД PostgreSQL			
8	8	100	100
Узел брокера сообщений RabbitMQ			
4	4	60	100
Узел «Шлюза» (Termidesk Connect с лицензией Termidesk Connect Basic)			
2	12	50	20 000
Узел балансировщика нагрузки (Termidesk Connect с лицензией Termidesk Connect)			
2	12	50	20 000

Требования к программному обеспечению

В среде функционирования должны быть предварительно установлены:

- ОС Astra Linux Special Edition версии 1.8 (1.8.1, 1.8.2, 1.8.3, 1.8.4, 1.8.5, 1.8.6);
- СУБД PostgreSQL версии 15 из состава репозитория ОС Astra Linux Special Edition версии 1.8. Из внешних по отношению к ОС Astra Linux Special Edition версии 1.8 СУБД поддерживается СУБД PostgreSQL версии 14 и выше;
- брокер сообщений RabbitMQ из состава репозитория ОС Astra Linux Special Edition.

ОС Astra Linux Special Edition версии 1.8 должна быть установлена из `iso`-образа, доступного в личном кабинете на портале Astra Linux: https://lk.astra.ru/. Работа Termidesk VDI на преднастроенных образах ОС не гарантируется.

Требования к уровню подготовки персонала

Уровень подготовки персонала для штатной эксплуатации Termidesk VDI приведен в таблице.

Уровень персонала	Описание	Обязанности	Навыки
Уровень 1. Специалист(ы) службы поддержки	Оказывает первую линию технической поддержки по поступившим запросам: принимает, фиксирует запрос через доступные каналы связи. Выполняет первоначальный анализ и определение проблемы, классифицирует поступившие заявки, обслуживает типовые и повторяющиеся запросы по заранее подготовленным инструкциям	Определение проблемы, первоначальный анализ и базовое решение проблемы. Начальное устранение неполадок для определения характера проблемы. Создание заявки, сбор информации о пользователе и фиксация всех выполненных действий по устранению неполадок. Решение основных и повторяющихся проблем, связанных с Termidesk VDI, используя существующие статьи базы знаний и справочного центра. Предварительное соотнесение проблемы к определенной области: • ОС; • платформа виртуализации; • сетевая связность или наличие необходимых сервисов; • корректность конфигурации Termidesk VDI; • особенности настройки программного обеспечения в РМ. При недостаточности навыков или знаний для определения или разрешения проблемы – эскалирование проблемы на Уровень 2. Если проблема влияет на производственную среду или потенциально может привести к сбою на уровне системы, то эскалирование проблемы на Уровень 3. При необходимости создание запросов на дополнительные инструкции по решению проблем. Сбор обратной связи от конечного пользователя после закрытия заявки в службу поддержки для подтверждения решения проблемы	Необходимые навыки: • пользовательский опыт работы с настольными ОС Windows и ОС Linux; • знание персонального компьютера и офисных программ; • базовое понимание организации локальной сети и работы сетевого оборудования; • умение работать с ПО для приема, обработки и регистрации заявок и обращений пользователей; • понимание принципов работы с запросами пользователей (систематизация, определение уровня важности и приоритета запроса); • доброжелательное общение и способность ясно излагать свои мысли

Уровень персонала	Описание	Обязанности	Навыки
Уровень 2. Инженер(ы)	В первую очередь поддерживает ежедневные операции инфраструктуры Termidesk VDI, включающие проактивный мониторинг и управление. Выполняет устранение неполадок промежуточного уровня и использует доступные инструменты мониторинга или устранения неполадок. Помогает в решении проблем, эскалированных поддержкой Уровня 1.	Выполнение промежуточного анализа, определение и решение проблем, эскалированных с Уровня 1. Систематизация и связывание отдельных проблем для выявления возможной первопричины их появления. Оперативное реагирование на уведомления и сбои системы. Создание еженедельного отчета о количестве проблем, скорости их закрытия и контроль решения открытых проблем. Создание статей внутренней базы знаний и сценарий решения проблем, а также поддержание рабочих процессов устранения неполадок для Уровня 1. Выполнение основных процедур обслуживания и эксплуатации Termidesk VDI. При недостаточности навыков или знаний для определения или решения проблемы - эскалирование проблемы на Уровень 3 или обращение в службу технической поддержки производителя. Изучение и анализ встроенных журналов событий Termidesk VDI, ОС Windows и ОС Linux для выполнения базовых задач по устранению неполадок на основе общедоступной информации	Необходимые навыки: • успешное прохождение обучения по курсу «Установка и администрирование Termidesk»; • навыки администрирования ОС Windows и ОС Astra Linux, включая опыт работы в командной строке; • навыки администрирования систем серверной виртуализации; • понимание принципов работы сетей передачи и хранения данных

Уровень персонала	Описание	Обязанности	Навыки
Уровень 3. Администратор(ы)	Является центральной точкой внедрения, администрирования и обслуживания инфраструктуры VDI. Специализируется на развертывании и запуске новых вариантов использования Termidesk VDI и управлению жизненным циклом новых фондов РМ. Эскалирует проблему в техническую поддержку производителя стороннего ПО и уведомляет о проблеме Уровень 4	Выполнение расширенного анализа, моделирования и решения проблем. Выполнение технического обслуживания и модернизации среды функционирования Termidesk VDI. Устранение серьезных неполадок и сбоев в обслуживании. Управление Termidesk VDI и средой функционирования. Контроль и управление административными задачами, выполняемыми Уровнем 2. Управление сетевой инфраструктурой и инфраструктурой хранения данных, связанных с функционированием Termidesk VDI. Просмотр периодических отчетов о состоянии сервера, использовании ресурсов, пользовательском опыте и общей производительности среды. Ознакомление со статьями базы знаний производителей ПО и недавно выпущенными обновлениями, включая обновления безопасности ОС. Выполнение расширенного обслуживания серверов и инфраструктуры Termidesk VDI. При необходимости передача запроса в службу технической поддержки производителя и уведомление о проблеме Уровня 4	Необходимые навыки: • успешное прохождение обучения по курсу «Установка и администрирование Termidesk»; • практический опыт администрирования серверных ОС на базе ОС Windows и ОС Linux; • опыт администрирования систем серверной виртуализации; • опыт в проектировании, обслуживании и поиске неисправностей в сетях передачи и хранения данных; • опыт настройки и поиска неисправностей для сетевых сервисов и служб: DNS, DHCP, MS AD, LDAP, SSL, FIREWALL, LOAD BALANCING; • знание кластеризации систем управления базами данных (СУБД); • знание автоматизации использования командной строки при помощи скриптовых языков

Уровень персонала	Описание	Обязанности	Навыки
Уровень 4. Архитектор(ы)	Оказывает минимальное воздействие на административные задачи, но концентрируется на планировании и валидации системно значимых изменений сервисов доставки BPM и приложений, включая погружение в связанные изменения в работе корпоративной сети передачи и хранения данных и сопутствующих сервисов, оказывающих непосредственное влияние на работу Termidesk VDI	Техническое руководство предстоящими изменениями в программных компонентах, дизайне, сетевых сервисах организации. Устранение серьезных проблем и сбоев в обслуживании. Проведение нагрузочного тестирования для подтверждения соответствия технических характеристик потребностям бизнеса. Обновление проектной документации	Подтвержденные навыки разработки архитектуры, включая практический опыт в: • управлении жизненным циклом информационных систем масштаба организации; • понимании принципов управления жизненными циклами архитектурных ландшафтов и проектирования облачных приложений; • проектировании высоконагруженных систем, в том числе платформ виртуализации. Знание принципов построения облачных платформ

Рекомендации по численности персонала приведены в таблице (см. таблицу Рекомендации по численности персонала) для различных окружений, включая количественные характеристики ферм и образов ОС.

Под фермой понимается отдельный набор сервисов Termidesk VDI, реализуемый для задач масштабируемости, отказо- и катастрофоустойчивости, включая следующие компоненты:

- компонент Termidesk VDI «Универсальный диспетчер»;
- компонент Termidesk VDI «Шлюз»;
- компонент Termidesk VDI «Менеджер рабочих мест»;
- серверы БД;
- балансировщики БД;
- балансировщики подключений.

Под образом понимается пользовательское окружение, состав которого может кардинально отличаться:

- тип ОС;
- версия ОС;
- используемое ядро ОС;
- установленные драйверы;
- установленные обновления и исправления, в том числе исправления безопасности в ОС;
- набор используемых приложений;
- версионность установленных приложений.

Небольшое окружение: 1 ферма, менее 500 пользователей, до 2 образов.

Среднее окружение: до 2 ферм, от 1000 до 5000 пользователей, до 5 образов.

Большое окружение: от 2 ферм, от 5000 пользователей, от 5 образов.

Корпоративное окружение: от 2 ферм, от 10000 пользователей, от 10 образов.

Таблица 3. Рекомендации по численности персонала

Уровень персонала	Небольшое окружение	Среднее окружение	Большое окружение	Корпоративное окружение
Уровень 1. Служба поддержки	2	4	8	от 16
Уровень 2. Инженеры	1	2	4	от 12
Уровень 3. Администраторы	1	2	3	от 5
Уровень 4. Архитекторы	1	1	2	от 2

Требования к настройкам инфраструктуры

Требования к синхронизации времени

В сетевой инфраструктуре должен быть настроен NTP-сервер, обеспечивающий синхронизацию времени для компонентов Termidesk VDI.

Требования к DNS и DHCP

В сетевой инфраструктуре должны быть развернуты и исправно функционировать службы доменных имен (DNS) и автоматического назначения сетевых параметров (DHCP) в необходимых сегментах сети.

Службы DNS и DHCP могут быть реализованы как отдельно, так и средствами платформы виртуализации (например, контекстуализацией ПК СВ Брест).

Служба DNS должна обеспечивать надежное и корректное двустороннее разрешение имен: полного доменного имени (FQDN) узла в соответствующий IP-адрес (запись A/AAAA) и IP-адреса в соответствующий FQDN (запись PTR).

Требования к серверам каталогов

Серверы каталогов должны удовлетворять следующим требованиям:

- сервер каталогов должен размещаться в том же сегменте локальной сети, где будут развернуты РМ. Если выполнение требования невозможно и сервер каталогов находится в другом сегменте, то необходимо обеспечить маршрутизацию между этими сегментами;
- при использовании в качестве сервера каталогов MS AD необходимо создать сервисную учетную запись для взаимодействия Termidesk VDI с контроллером домена (КД). Допускается использование учетной записи администратора домена;
- при использовании MS AD рекомендуется создавать отдельные организационные подразделения (OU) для пользователей РМ и для учетных записей типа «Компьютер» для самих РМ. Права на OU для компьютеров должны быть либо у созданной сервисной учетной записи, либо у отдельной созданной учетной записи, допускается также использовать учетную запись администратора домена;
- при использовании серверов каталогов FreeIPA и ALDPro в качестве сервисной учетной записи для взаимодействия Termidesk VDI с КД по умолчанию используется учетная запись администратора домена, либо отдельная учетная запись с аналогичными полномочиями;
- в имени домена и поддоменов рекомендуется использовать латиницу, использование кириллицы не рекомендуется. При развертывании узла STAL выполнение требования обязательно;
- имена серверов каталогов должны корректно разрешаться: полное доменное имя (FQDN) узла в соответствующий IP-адрес (запись A/AAAA) и IP-адрес в соответствующий FQDN (запись PTR);
- при использовании единого входа на базе протокола Kerberos центр распространения ключей (KDC) сервера каталогов должен выдавать билет `krbtgt` с установленным флагом возможности пересылки (`forwardable`). Если этот флаг отсутствует, аутентификация пользователя завершится ошибкой.

Требования к терминальным серверам

При использовании терминального сервера Microsoft необходимо наличие внутри домена MS AD серверов с соответствующими ролями (MS RDSH - роль терминального сервера, MS RDS - роль сервера публикации приложений).

Требования к платформе виртуализации

Узлы платформы виртуализации должны удовлетворять следующим требованиям:

- должна быть поддержка виртуального чипсета (ich9-intel-hda);
- пул в настройках DHCP или параметрах контекстуализации должен поддерживать достаточное количество IP-адресов;
- виртуальный коммутатор платформы должен поддерживать достаточное количество MAC-адресов;
- в платформе виртуализации на базе QEMU/KVM должны быть реализованы необходимые для работы Termidesk VDI именованные каналы:
  - для перенаправления каталогов - `org.spice-space.webdav.0` (`/dev/virtio-ports/org.spice-space.webdav.0`);
  - для взаимодействия с `libvirt` (необходим компоненту «Агент узла виртуализации») - `ru.termidesk.tvm.0` (`/dev/virtio-ports/ru.termidesk.tvm.0`);
  - для перенаправления видеокамеры - `ru.termidesk.RealtimeStreaming.0` (`/dev/virtio-ports/ru.termidesk.RealtimeStreaming.0`);
  - для перенаправления смарт-карт - `ru.termidesk.PCSC.0` (`/dev/virtio-ports/ru.termidesk.PCSC.0`);
  - для перенаправления принтера - `ru.termidesk.Printer.0` (`/dev/virtio-ports/ru.termidesk.Printer.0`).

Для ПК СВ Брест включение именованных каналов определяется конфигурационным файлом `/etc/one/vmm_exec/vmm_exec_kvm.conf`, находящимся на фронтальных машинах ПК СВ Брест.

Для включения каналов на узле системы виртуализации ПК СВ Брест необходимо:

- установить компонент «Агент узла виртуализации»:

```
sudo apt install termidesk-vmsd
```

- убедиться, что состояние службы компонента «Агент узла виртуализации» находится в состоянии `active (running)`:

```
systemctl status termidesk-vmsd
```

Затем на фронтальной машине ПК СВ Брест выполнить активацию именованных каналов:

- открыть на редактирование файл `/etc/one/vmm_exec/vmm_exec_kvm.conf`;
- присвоить параметрам `WEBDAV_USE_DEFAULT`, `VIDEOCAM_OPTIMIZATION_USE_DEFAULT`, `PRINTER_OPTIMIZATION_USE_DEFAULT`, `USBTOKEN_OPTIMIZATION_USE_DEFAULT`, `SPICE_DETECT_USE_DEFAULT` значение «yes». Пример фрагмента файла с нужными значениями:

```
#rbt: webdav use
WEBDAV_USE_DEFAULT="yes"
WEBDAV_OPTIONS="
    <channel type='spiceport'>
        <source channel='org.spice-space.webdav.0'/>
```

```
        <target type='virtio' name='org.spice-space.webdav.0'/>
    </channel>"

#rbt: camera optimization
VIDEOCAM_OPTIMIZATION_USE_DEFAULT="yes"
VIDEOCAM_OPTIMIZATION_OPTIONS="
    <channel type='spiceport'>
        <source channel='TDSK_STREAM'/>
        <target type='virtio' name='ru.termidesk.RealtimeStreaming.0'/>
    </channel>"

#rbt: printer optimization
PRINTER_OPTIMIZATION_USE_DEFAULT="yes"
PRINTER_OPTIMIZATION_OPTIONS="
    <channel type='spiceport'>
        <source channel='TDSK_PRINTER'/>
        <target type='virtio' name='ru.termidesk.Printer.0'/>
    </channel>"

#rbt: USB token optimization
USBTOKEN_OPTIMIZATION_USE_DEFAULT="yes"
USBTOKEN_OPTIMIZATION_OPTIONS="
    <channel type='spiceport'>
        <source channel='TDSK_PCSC'/>
        <target type='virtio' name='ru.termidesk.PCSC.0'/>
    </channel>"

#rbt: SPICE detect
SPICE_DETECT_USE_DEFAULT="yes"
SPICE_DETECT_OPTIONS="
    <channel type='unix'>
        <source mode='connect' path='/var/run/tvmd.sock' >
            <reconnect enabled='yes' timeout='1'/>
        </source>
        <target type='virtio' name='ru.termidesk.tvm.0'/>
    </channel>"
```

Присвоение параметру `SPICE_DETECT_USE_DEFAULT` значения `yes` должно выполняться только после установки на узлы системы виртуализации компонента «Агент узла виртуализации» и успешного запуска его службы.

- сохранить изменения в файле `/etc/one/vmm_exec/vmm_exec_kvm.conf`;
- перезапустить службу `opennebula`:

```
sudo systemctl restart opennebula
```

Контекстуализация в ПК СВ Брест

В ПК СВ Брест применяется метод контекстуализации для отправки информации на ВМ во время загрузки. Основная задача метода - передача настроек сети и учетных данных для настройки ВМ. Дополнительная задача - передача индивидуальных сценариев для загрузки ВМ.

Использование метода контекстуализации ПК СВ Брест не является обязательным, однако значительно упрощает и автоматизирует процесс подготовки узлов с компонентами Termidesk VDI.

Для включения контекстуализации в гостевой ОС Astra Linux нужно в базовый образ установить пакет `one-context`:

```
sudo apt install one-context
```

Если после выполнения команды появляются сообщения об ошибке «Невозможно найти пакет one-context», «Пакеты имеют неудовлетворенные зависимости» необходимо убедиться, что в файле `/etc/apt/sources.list` заданы и не закомментированы источники получения пакетов (репозитории), затем обновить списки пакетов:

```
sudo apt update
```

После этого нужно вновь выполнить команду установки пакета `one-context`.

Для включения контекстуализации в гостевой ОС Microsoft Windows нужно включить службу, обрабатывающую скрипты контекстуализации. Для этого следует установить пакет `one-context-6.2.0` или более новый.

Параметры непосредственно контекста задаются в шаблоне ВМ, для этого в панели управления ПК СВ Брест надо открыть шаблон ВМ и перейти во вкладку «Контекст».

Получение пакетов установки

Получение пакетов установки в ОС Astra Linux Special Edition

Дистрибутив представлен бинарным файлом пакета ПО в `deb`-формате. Установка в ОС Astra Linux Special Edition производится из локального репозитория, распространяемого в формате `iso`-образа.

Получить `iso`-образ можно двумя способами:

- заполнив запрос через сайт Termidesk VDI: https://termidesk.ru/support/#request-support;
- через личный кабинет:https://lk.astra.ru/.

Для подключения локального репозитория Termidesk VDI на узле, где предполагается установка, нужно:

- скопировать в домашний каталог пользователя образ диска `termidesk-<версия>.iso`;
- подключить образ диска к файловой системе в каталог `/mnt`:

```
sudo mount -o loop termidesk-<версия>.iso /mnt
```

где:

`-o loop` - параметры для привязки петлевого устройства (`/dev/loop`) к файлу `termidesk-<версия>.iso`, устройство затем монтируется в указанный каталог `/mnt`;

- скопировать содержимое каталога `repos` подключенного образа диска в каталог `/var` локальной файловой системы:

```
sudo cp -Rp /mnt/repos /var
```

где:

`-Rp` - ключ для рекурсивного копирования подкаталогов и файлов с сохранением исходных свойств;

- отключить подключенный ранее образ диска от узла:

```
sudo umount /mnt
```

- установить пакет `lsb-release`:

```
sudo apt install -y lsb-release
```

- добавить локальный репозиторий Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list` через командный интерпретатор `sh`:
  - выяснить установленную версию ОС:

    ```
    sudo cat /etc/astra_version
    ```

  - определить актуальное имя каталога с пакетами в `/var/repos`;
  - указать в файле конфигурации APT корректное (фактическое) имя каталога:

    ```
    sudo sh -c 'echo "deb file:/var/repos/astra 1.8_x86-64 non-free" >
    /etc/apt/sources.list.d/termidesk_local.list'
    ```

    где:

    `-c` - ключ для чтения команд из вводимой строки (стандартный ввод);

    `echo` - команда вывода текста, совместно с символом «>» используется для перенаправления строки в файл;

    `deb file:/var/repos/astra 1.8_x86-64 non-free` - добавляемый репозиторий с вложенной командой получения версии ОС;

> Приведенный пример команды актуален для установки основных компонентов Termidesk, пакеты которых расположены в каталоге `1.8_x86-64`.

- для корректной установки компонентов TERA потребуется корректно подключить дополнительные репозитории и настроить их приоритет:
  - для версий ОС Astra Linux Special Edition меньше или равных 1.7.6, а также для версий 1.8.X:
    - подключить два репозитория:

```
sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
non-free" > /etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
/dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

    - добавить повышенный приоритет для репозитория с требуемой версией ОС (значение `$(cat /etc/astra_version)` может подходить не для всех репозиториев, т.к. версия может указываться без точек - в этом случае нужно вручную указать корректную версию):

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000
EOF"
```

  - для версий ОС Astra Linux Special Edition 1.7.7 и 1.7.8:
    - подключить три репозитория:

```
sudo sh -c 'echo "deb file:/var/repos/astra 1.7.6 non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
/dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

    - настроить два приоритета:

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=1.7.6
Pin-Priority: 950

Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000
```

```
EOF"
```

- выполнить поиск ключа репозитория Termidesk VDI `GPG-KEY-PUBLIC` и добавить его:

```
sudo cat /var/repos/astra/GPG-KEY-PUBLIC | sudo gpg --dearmour -o
/etc/apt/trusted.gpg.d/termidesk.gpg
```

- убедиться, что ключ `release@uveon.ru` был успешно добавлен:

```
apt-key list
```

В случае, если ключ не отображен в выводе команды, необходимо убедиться, что ключ `GPG-KEY-PUBLIC` существует:

```
cat /var/repos/astra/GPG-KEY-PUBLIC
```

Если ключ все же существует, следует проверить правильность выполнения шагов по добавлению репозитория Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list`.

При успешном выполнении всех шагов команда выведет содержимое ключа в формате Base64.

В зависимости от используемой версии ОС команды добавления ключа репозитория Termidesk VDI могут отличаться. Если для ОС Astra Linux Special Edition 1.8 ключ репозитория был добавлен командой, применимой к другой версии ОС, то для исправления нужно:

- узнать идентификатор добавленного ключа репозитория:

```
apt-key list
```

- удалить ключ:

```
apt-key --keyring /etc/apt/trusted.gpg del 4E1632CC
```

где `4E1632CC` - последние 8 символов идентификатора ключа;

- вновь добавить ключ репозитория.

- обновить данные пакетного менеджера:

```
sudo apt update
```

- проверить настройку приоритетов репозиториев:

```
apt-cache policy
```

Команду `sudo apt update` необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.

Подготовка среды функционирования

Установка и настройка брокера сообщений RabbitMQ

Установка брокера сообщений RabbitMQ

Если узел с уже установленным RabbitMQ будет переименован, то брокер сообщений перестанет принимать подключения. Для исправления ситуации необходимо удалить RabbitMQ, затем выполнить его переустановку.

В Termidesk VDI версии 6.1 в экспериментальном режиме поддерживается установка «Брокера сообщений TermideskMQ»:

- выбор «Брокера сообщений TermideskMQ» производится при установке пакета `termidesk-vdi`;
- одновременное использование RabbitMQ и «Брокера сообщений TermideskMQ» в рамках одной фермы не поддерживается. Рекомендуется удалить RabbitMQ или отключить службу `rabbitmq-server`, если будет использоваться «Брокер сообщений TermideskMQ».

Для установки RabbitMQ следует перейти в интерфейс командной строки через программу «Терминал Fly» и выполнить:

```
sudo apt install -y rabbitmq-server
```

Где:

`-y` - ключ для пропуска подтверждения установки.

Настройка брокера сообщений RabbitMQ

Для настройки RabbitMQ следует:

- перейти в интерфейс командной строки через программу «Терминал Fly» и убедиться в наличии каталога `/etc/rabbitmq`:

```
ls /etc/ | grep rabbitmq
```

- если каталог отсутствует, необходимо создать его:

```
sudo mkdir -p /etc/rabbitmq
```

где:

`-p` - ключ для автоматического создания директорий, указанных внутри пути;

- перейти в каталог `/etc/rabbitmq`:

```
cd /etc/rabbitmq
```

- создать пустой файл `rabbitmq.conf` (основной файл конфигурации RabbitMQ):

```
sudo touch rabbitmq.conf
```

- поменять владельца (`rabbitmq`) и идентификатор группы (`rabbitmq`) для созданного файла:

```
sudo chown rabbitmq:rabbitmq rabbitmq.conf
```

- отредактировать файл `rabbitmq.conf`, приведя его к виду:

```
tcp_listen_options.keepalive = true
```

Если необходимо, чтобы RabbitMQ работал через TLS-соединение, то файл `rabbitmq.conf` нужно привести к виду:

```
tcp_listen_options.keepalive = true
listeners.tcp.default = 5672

# TLS Порт
listeners.ssl.default = 5671
# Пути к сертификатам
ssl_options.cacertfile = /var/ssl/root-ca.crt
ssl_options.certfile   = /var/ssl/cert.crt
ssl_options.keyfile    = /var/ssl/private/private-key.key

# Пароль для ключа
ssl_options.verify     = verify_peer

ssl_options.fail_if_no_peer_cert = false

ssl_options.versions.default = tlsv1.2
```

Предполагается, что файлы корневого сертификата (`/var/ssl/root-ca.crt`), сертификата узла (`/var/ssl/cert.crt`) и закрытого ключа (`/var/ssl/private/private-key.key`) к нему уже существуют и доступны по указанному пути.

- выполнить настройку RabbitMQ с помощью `rabbitmqctl`:

- включить плагины управления и метрик:

```
sudo rabbitmq-plugins enable rabbitmq_management
sudo rabbitmq-plugins enable rabbitmq_prometheus
```

- предоставить права администратору:

```
sudo rabbitmqctl add_user admin StrongAdminPassword
sudo rabbitmqctl set_user_tags admin administrator
sudo rabbitmqctl set_permissions -p / admin ".*" ".*" ".*"
```

- удалить гостевого пользователя:

```
sudo rabbitmqctl delete_user guest
```

- создать виртуальный хост `termidesk` и пользователя RabbitMQ:

```
sudo rabbitmqctl add_vhost termidesk
sudo rabbitmqctl add_user termidesk ksedimret
```

- предоставить права пользователю `termidesk` на работу с виртуальным хостом `termidesk`:

```
sudo rabbitmqctl set_permissions -p termidesk termidesk ".*" ".*" ".*"
```

- предоставить права администратору на работу с виртуальным хостом `termidesk`:

```
sudo rabbitmqctl set_permissions -p termidesk admin ".*" ".*" ".*"
```

- предоставить права пользователю `termidesk` на работу с очередями виртуального хоста `termidesk`:

```
sudo rabbitmqctl set_topic_permissions -p termidesk termidesk ".*" ".*" ".*"
```

Имя пользователя и пароль должны задаваться в соответствии с внутренними стандартами организации по применению парольной защиты. Для задания пароля разрешено использовать только латинские буквы A-Z, a-z, цифры 0-9 и символы !$%^&_-=+~`.,()*{}[]\|.

- перезапустить службу `rabbitmq-server`:

```
sudo systemctl restart rabbitmq-server
```

- выполнить настройку поддержки TCP в ОС:
  - отредактировать файл `/etc/sysctl.conf`:

    ```
    net.ipv4.tcp_keepalive_time = 30
    net.ipv4.tcp_keepalive_intvl = 10
    net.ipv4.tcp_keepalive_probes = 3
    net.ipv4.tcp_retries2 = 5
    ```

  - применить изменения `sysctl`:

    ```
    sudo sysctl --system
    ```

Установка и настройка СУБД PostgreSQL

Установка СУБД PostgreSQL

Для установки СУБД PostgreSQL необходимо:

- отредактировать файл `/etc/apt/sources.list`, оставив в качестве источников получения пакетов сетевые репозитории. Пример файла `/etc/apt/sources.list` для ОС Astra Linux Special Edition 1.8:

> Приведен только пример файла! Он должен быть скорректирован, исходя из используемой и поддерживаемой версии ОС. Подробную информацию о сетевых репозиториях ОС Astra Linux Special Edition можно получить в справочном центре Astra Linux для ОС Astra Linux Special Edition 1.8: https://wiki.astralinux.ru/pages/viewpage.action?pageId=302043111.
>
> Если в файле `/etc/apt/sources.list` присутствует репозиторий `astra-ce`, то необходимо закомментировать его, чтобы избежать установки несовместимых версий пакетов.

```
deb https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-main/
1.8_x86-64 main contrib non-free
deb https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-extended/
1.8_x86-64 main contrib non-free
```

- перейти в интерфейс командной строки и обновить списков пакетов:

```
sudo apt update
```

- установить СУБД PostgreSQL. Команда установки выбирается в зависимости от того, требуется ли использование СУБД Tantor Basic Edition:
  - с СУБД Tantor Basic Edition:

```
sudo apt install -y postgresql
```

Начиная с версии ОС Astra Linux Special Edition 1.8.0 при подключенных основном и расширенном репозиториях данная команда устанавливает СУБД Tantor Basic Edition, лицензия на которую приобретается отдельно.

- без СУБД Tantor Basic Edition:

```
sudo apt install -y tantor-free-server-16
```

где:

`-y` - ключ для пропуска подтверждения установки.

Настройка СУБД PostgreSQL

Перед установкой Termidesk VDI нужно выполнить настройку базы данных (БД).

При работе с СУБД следует учитывать ее ограничения: суммарное количество подключений к СУБД должно быть не более 75% от максимально разрешенного количества подключений. Для СУБД PostgreSQL по умолчанию максимальное количество подключений - 100.

Для оценки количества подключений к СУБД можно воспользоваться формулой: (количество порталов «Универсального диспетчера» x количество ядер процессоров x 3) + (количество узлов с запущенными службами `termidesk-celery-beat` и `termidesk-celery-worker` x количество ядер на этих узлах).

Для настройки БД следует перейти в интерфейс командной строки и выполнить:

- переключиться на пользователя `postgres`:

```
sudo su postgres
```

- запустить терминальный клиент СУБД PostgreSQL:

```
psql
```

Если после выполнения команды отображается ошибка «could not change directory to "/home/": Отказано в доступе» и не появляется приглашение командной строки `postgres=`, необходимо вместо `su postgres` использовать конструкцию `su - postgres`. Если приглашение `postgres=` появилось, то сообщение об ошибке можно проингорировать.

Если приглашение `postgres=#` не появляется, то вероятнее всего ОС Astra Linux Special Edition используется в более защищенном режиме, например, «Смоленск». В таком случае нужно для пользователя `postgres` (по умолчанию) назначить классификационную метку:

```
sudo pdpl-user -i 63 postgres
```

- используя интерактивный интерфейс терминального клиента СУБД PostgreSQL, создать БД `termidesk` (символ ; в конце строки при работе с интерактивным интерфейсом обязателен):

```
postgres=# CREATE DATABASE termidesk LC_COLLATE 'ru_RU.utf8' LC_CTYPE 'ru_RU.utf8'
TEMPLATE template0;
```

где:

`LC_COLLATE` - порядок сортировки для использования в БД, влияет на порядок сортировки, применяемый к строкам. Значение `ru_RU.utf8` указывает на использование русской локализации;

`LC_CTYPE` - классификация символов для использования в БД, влияет на категоризацию символов;

`TEMPLATE` - имя шаблона, из которого создается БД. Шаблон `template0` используется для системной БД самой СУБД PostgreSQL.

- создать пользователя `termideskdb` с паролем `ksedimret` для дальнейшего подключения к БД:

```
postgres=# CREATE USER termideskdb WITH PASSWORD 'ksedimret';
```

В приведенной команде имя пользователя и пароль используются в качестве примера. Имя пользователя и пароль должны задаваться в соответствии с внутренними стандартами организации по применению парольной защиты. Для задания пароля разрешено использовать только латинские буквы A-Z, a-z, цифры 0-9 и символы $!@%^&#_-=+~`;:.,?()*{}[]\|/.

- назначить права по использованию БД `termidesk` созданному пользователю `termideskdb`:

```
postgres=# GRANT ALL PRIVILEGES ON DATABASE termidesk TO termideskdb;
```

- в случае, если используется СУБД PostgreSQL из состава ОС Astra Linux Special Edition 1.8, то сделать пользователя `termideskdb` владельцем БД `termidesk`, тем самым предоставив ему все возможные права:

```
postgres=# ALTER DATABASE termidesk OWNER TO termideskdb;
```

- выйти из интерактивного интерфейса терминального клиента СУБД PostgreSQL:

```
postgres=# \q
```

- выйти из сеанса пользователя `postgres`:

```
exit
```

- отредактировать файл `/etc/parsec/mswitch.conf`, установив параметр `zero_if_notfound` в значение `yes`, точно соблюдая отступы и пробелы:

```
# Return zero data instead of ENOENT/ENODATA in the absence of record
zero_if_notfound: yes
```

- создать системного пользователя `termideskdb` (имя должно совпадать с именем пользователя в БД):

```
sudo useradd -M termideskdb -s /usr/sbin/nologin -d /home/termideskdb
```

- для пользователя БД назначить классификационную метку (в примере используется `termideskdb`, в более ранних версиях использовалось имя пользователя `termidesk`):

```
sudo pdpl-user -i 0 termideskdb
```

- предоставить пользователю `termideskdb` права на чтение файла, содержащего классификационную метку:

```
sudo setfacl -m u:postgres:r /etc/parsec/macdb/$(id -u termideskdb)
```

В случае последующего обновления СУБД PostgreSQL может понадобиться пересоздать БД. В этом случае следует предусмотреть экспорт БД перед обновлением СУБД PostgreSQL.

Настройка СУБД Tantor

Помимо поддержки PostgreSQL Termidesk VDI может работать с другими СУБД, такими как Tantor, основанным на PostgreSQL. Установка СУБД должна быть выполнена согласно документации на нее.

После установки нужно последовательно выполнить шаги для настройки БД:

- переключиться на пользователя `postgres`:

```
sudo su postgres
```

- выполнить инициализацию БД:

```
/opt/tantor/db/<версия_Tantor>/bin/initdb -D
/var/lib/postgresql/<каталог_Tantor>/data/
```

- запустить терминальный клиент СУБД:

```
./psql
```

- используя интерактивный интерфейс терминального клиента СУБД, создать БД `termidesk` (символ «;» в конце строки при работе с интерактивным интерфейсом обязателен):

```
postgres=# CREATE DATABASE termidesk LC_COLLATE 'ru_RU.utf8' LC_CTYPE 'ru_RU.utf8'
TEMPLATE template0;
```

- создать пользователя `termidesk` с паролем `ksedimret` для дальнейшего подключения к БД:

```
postgres=# CREATE USER termidesk WITH PASSWORD 'ksedimret';
```

В приведенной команде имя пользователя и пароль используются в качестве примера. Имя пользователя и пароль должны задаваться в соответствии с внутренними стандартами организации по применению парольной защиты. Для задания пароля разрешено использовать только латинские буквы A-Z, a-z, цифры 0-9 и символы $!@%^&#_-=+~`;:.,?()*{}[]\|/.

- назначить все права по использованию БД `termidesk` созданному пользователю `termidesk`:

```
postgres=# GRANT ALL PRIVILEGES ON DATABASE termidesk TO termidesk;
```

- назначить права на создание объектов для схемы `public`:

```
postgres=# GRANT CREATE ON SCHEMA public TO termidesk;
```

- выйти из интерактивного интерфейса терминального клиента СУБД:

```
postgres=# \q
```

- выйти из сеанса пользователя `postgres`:

```
exit
```

- отредактировать файл `/etc/parsec/mswitch.conf`, установив параметр `zero_if_notfound` в значение `yes`, точно соблюдая отступы и пробелы:

```
# Return zero data instead of ENOENT/ENODATA in the absence of record
zero_if_notfound: yes
```

При работе с СУБД следует учитывать ее ограничения: суммарное количество подключений к СУБД должно быть не более 75% от максимально разрешенного количества подключений.

Для оценки количества подключений к СУБД можно воспользоваться формулой: (количество порталов «Универсального диспетчера» x количество ядер процессоров x 3) + (количество узлов с запущенными службами `termidesk-celery-beat` и `termidesk-celery-worker` x количество ядер на этих узлах).

УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ TERMIDESK

ОС Astra Linux Special Edition

Неавтоматизированная комплексная установка Termidesk VDI

Для установки фермы Termidesk VDI с использованием псевдографического интерфейса нужно:

- подготовить среду функционирования (см. подраздел **Подготовка среды функционирования**);
- подключить репозиторий Termidesk VDI;
- установить Termidesk VDI:

```
sudo apt install termidesk-vdi
```

При установке пакета `termidesk-vdi` возможно активировать режим отладки через переменную окружения `TDSK_DEBUG=1`.

Одним из параметров службы `termidesk-vdi` (`/lib/systemd/system/termidesk-vdi.service`) является `EnvironmentFile`, задающий дополнительные аргументы функционирования, перечисленные в файле `/etc/default/termidesk-vdi.local` (см. подраздел **Файл `/etc/default/termidesk-vdi.local`**).

Рекомендуется также установить пакеты `postgresql` и `expect` для возможности тестирования подключения к БД во время установки:

```
sudo apt -y install postgresql expect
```

В зависимостях пакета установки `termidesk-vdi` есть:

- служба ведения журналов `syslog-ng`. Работа с другими службами ведения журналов не гарантируется;
- пакет `libpython3.11` для ОС Astra Linux Special Edition 1.8, предоставляющий возможность установить Termidesk VDI в ОС с минимальной конфигурацией (без графического интерфейса ОС).

Перед обновлением ОС или службы `syslog-ng` рекомендуется создать резервную копию файла `syslog-ng.conf`. В случае обновления ОС или службы `syslog-ng` без предварительного создания резервной копии файла, может потребоваться переустановка Termidesk VDI для восстановления его корректной работы.

> Начиная с Termidesk VDI версии 6.1 компонент «Шлюз» (пакет `termidesk-gateway`) более не входит в поставку. Для использования «Шлюза» следует установить программу для электронной вычислительной машины «Балансировщик нагрузки Термидеск Коннект» (Termidesk Connect).

В процессе установки нужно:

> Для переключения между экранными кнопками **[Ок]** и **[Отмена]** в псевдографическом интерфейсе используется клавиша **<Tab>**.

- ввести домен по умолчанию для работы Kerberos-аутентификации. Ввод домена можно пропустить, оставив поле ввода пустым и нажав экранную кнопку **[Ok]** (см. рисунок Запрос настроек по умолчанию для Kerberos-аутентификации);

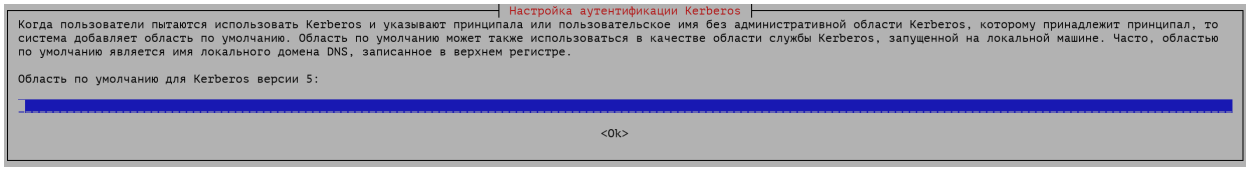


Рисунок 1. Запрос настроек по умолчанию для Kerberos-аутентификации

- ознакомиться с лицензионным соглашением и нажать экранную кнопку **[Далее]** (см. рисунок Лицензионное соглашение);

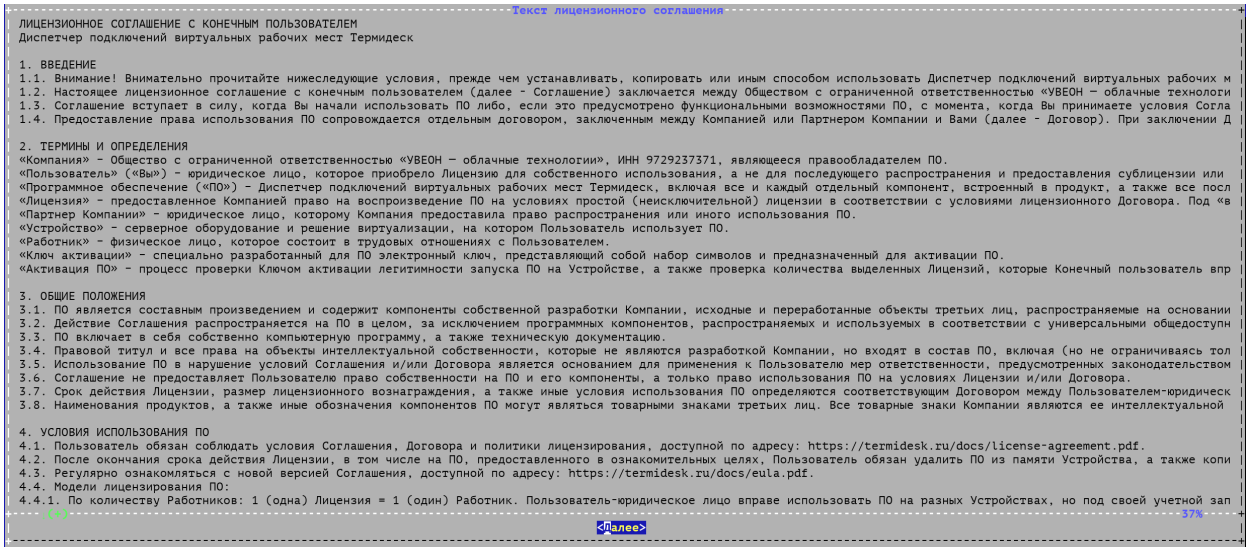


Рисунок 2. Лицензионное соглашение

- нажать экранную кнопку **[Да]** для принятия условий лицензионного соглашения и продолжения установки или экранную кнопку **[Нет]** в случае отказа, при этом установка прервется (см. рисунок Принятие условий лицензионного соглашения);

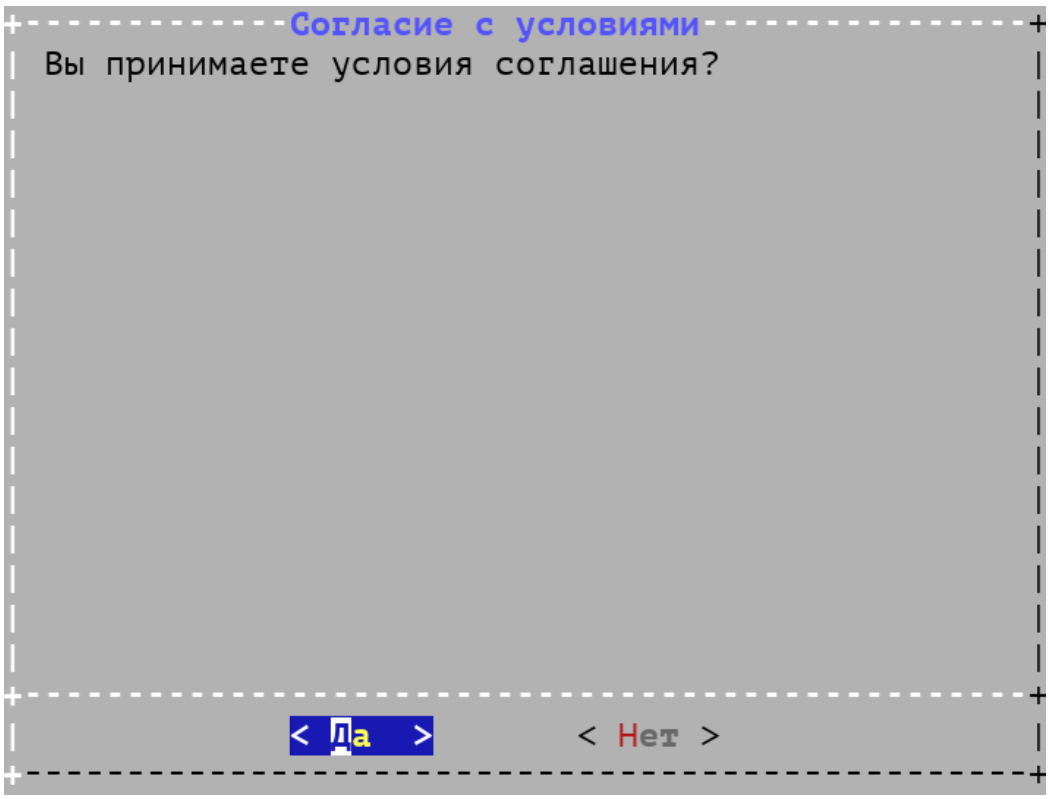


Рисунок 3. Принятие условий лицензионного соглашения

- далее настроить расположение каталогов для файлов Termidesk VDI (см. рисунок Настройка расположения каталогов):
  - «Расположения конфигурации»: каталог, в котором будет расположен файл `termidesk.conf`;
  - «Хранения журналов»: каталог, в котором будут расположены файлы журналов;
  - «Шаблонов syslog/logrotate»: каталог, в котором будут распололжены шаблоны для настройки регистрации событий и журналирования;

Каталог, в котором будут расположены файлы Termidesk VDI, должен обладать свойствами:

- права на каталог: `rwxr-x---` (`750`);
- владелец каталога: `root:termidesk`.

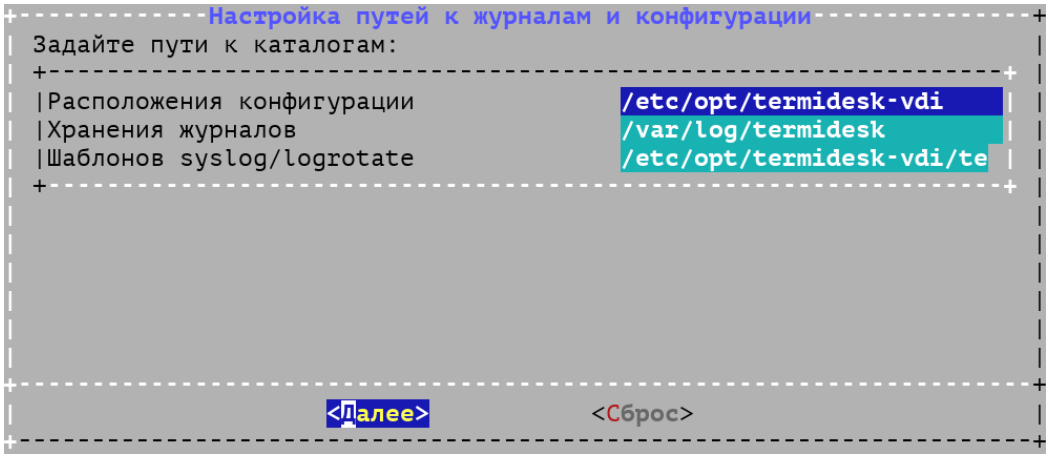


Рисунок 4. Настройка расположения каталогов

- далее выбрать режим работы (см. рисунок Выбор режима работы ПО):
  - «Диспетчер»: установка фермы «Универсального диспетчера»;
  - «Агрегатор»: установка фермы «Агрегатора»;

Установка «Агрегатора» должна производиться на отдельном узле, отличном от «Диспетчера».

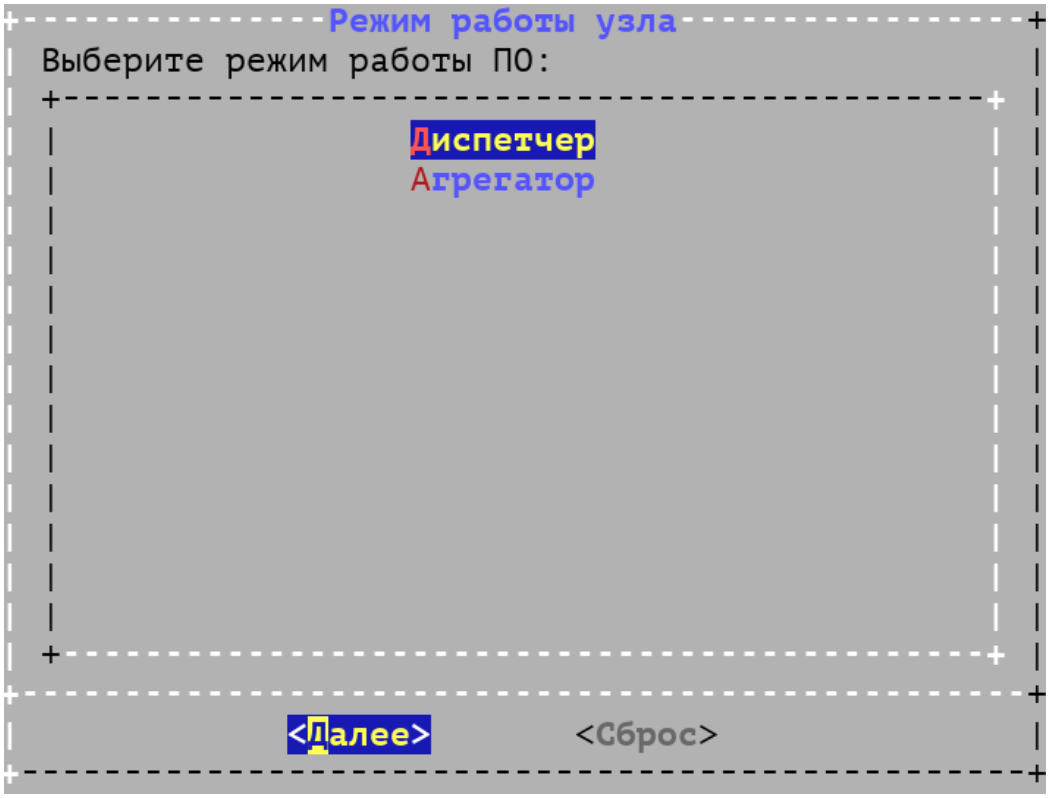


Рисунок 5. Выбор режима работы ПО

- затем выбрать устанавливаемую роль узла:

При комплексной установке необходимо выбрать роли:

- «Портал администратора»;
- «Портал пользователя»;
- «Менеджер рабочих мест».

Если не выбрать ни одной роли, то ни одна служба Termidesk VDI запущена не будет.

- «Портал администратора (ADMIN)»: установится «Портал администратора», предоставляющий интерфейс для управления Termidesk VDI и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API. После установки будет запущена служба `termidesk-vdi`;
- «Портал пользователя (USER)»: установится «Портал пользователя», предоставляющий пользовательский интерфейс Termidesk VDI и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API. Интерфейс управления Termidesk VDI будет недоступен. После установки будет запущена служба `termidesk-vdi`;
- при выборе и роли «Портал администратора», и роли «Портал пользователя» активируется «Портал универсальный» будут доступны функции обоих вариантов, при этом активируется доступ ко всем модулям документации по командам REST

API, предоставляемым интерфейсом Swagger;

- «Менеджер рабочих мест (CELERYMAN)»: установится компонент «Менеджер рабочих мест», после установки будут запущены службы `termidesk-celery-beat`, `termidesk-celery-worker`;
- «Брокер сообщений (TERMQ)»: установится компонент «Брокер сообщений TermideskMQ» (экспериментальный). После установки будет запущена служба `termidesk-tmq`;

- если для установки выбрана роль «Брокер сообщений (TERMQ)», то необходимо задать настройки брокера сообщений TermideskMQ:
  - «Адрес для подключений»: IP-адрес прослушивания входящих подключений для «Брокера сообщений TermideskMQ»;
  - «Базовый порт для подключений»: базовый номер порта «Брокера сообщений TermideskMQ» для незащищенного подключения (стандартный порт: 5555). Для «Брокера сообщений TermideskMQ» будет зарезервирован указанный порт, а также последующий: например 5555, 5556;

При использовании кластера «Брокера сообщений TermideskMQ»:

- должен использоваться режим mTLS;
- в зависимости от базового порта будут определены внутренние TCP-порты для запуска «Брокера сообщений TermideskMQ» на localhost;
- порты mTLS, использующиеся для IP-адреса, указанного в `TMQ_BASE_ADDRESS`:
  - базовый порт (например, 5555);
  - базовый порт +1 (например, 5556);
- внутренние TCP-порты для запуска на localhost:
  - базовый порт + 3 (например, 5558), используется для приема сообщений;
  - базовый порт + 3 + 1 (например, 5559), используется для приема подключения и отправки сообщений.

- далее задать уникальное имя узла для его идентификации (см. рисунок Настройка уникального имени узла). Это требуется для однозначной идентификации узлов, в частности, узлов «Агрегатора» во время балансировки подключений к ним;

Следует задавать уникальное имя узла понятным и отражающим его роль, например «AdminPortal-01», «UserPortal-01».

По умолчанию для заполнения параметра используется заданный в системе `hostname` и буквенно-числовой идентификатор.

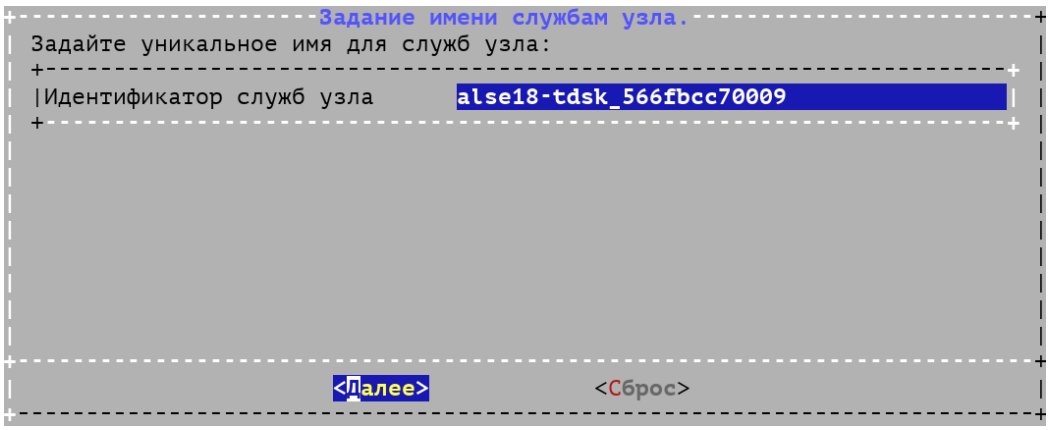


Рисунок 6. Настройка уникального имени узла

- далее выбрать способ хранения паролей подключения к СУБД и брокеру сообщений (см. рисунок Выбор способа хранения паролей);

Для всех узлов фермы Termidesk VDI должен выбираться единый способ хранения и единое хранилище (в случае выбора способа «hvac»).

  - «config» (по умолчанию) - пароли будут храниться в преобразованном виде в файле `/etc/opt/termidesk-vdi/termidesk.conf`;
  - «hvac» (рекомендуемый способ для безопасного хранения) - для хранения паролей будет использоваться хранилище паролей OpenBao или Hashicorp Vault (хранилище должно быть заранее создано и настроено). Подробная информация по этому способу хранения паролей приведена в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»;
  - «openbao» (экспериментальный) - для хранения паролей будет использоваться хранилище паролей OpenBao (хранилище должно быть заранее создано и настроено). При этом пароли располагаются внутри хранилища, имена контейнеров хранения генерируются автоматически;

```
+------------Способ хранения паролей---------------+
| Выберите способ хранения секретов (логинов,      |
| паролей, сертификатов, и т.д.):                  |
| +----------------------------------------------+ |
| |config    Конфигурационный файл               | |
| |hvac      Хранилище OpenBao/Hashicorp Vault   | |
| |openbao   Экспериментальное хранилище OpenBao | |
| |                                              | |
| |                                              | |
| |                                              | |
| |                                              | |
| |                                              | |
| |                                              | |
| |                                              | |
| |                                              | |
| |                                              | |
| +----------------------------------------------+ |
+--------------------------------------------------+
|              <Далее>        <Сброс>              |
+--------------------------------------------------+
```

Рисунок 7. Выбор способа хранения паролей

- при выборе хранения паролей «openbao» или «hvac» нужно задать параметры подключения к хранилищу и параметры, настроенные непосредственно на хранилище (см. рисунок Настройка подключения к OpenBao):
  - «URL хранилища» - IP-адрес или FQDN узла и порт с установленным хранилищем OpenBao. Формат: `http://<IP-адрес>:8200` или `http://<FQDN>:8200`;

    Хранилище паролей OpenBao должно быть реализовано в отказоустойчивом варианте, иначе Termidesk VDI не будет работать в период простоя узлов OpenBao.

  - «Версия API OpenBao» - установленная версия API на OpenBao (1 или 2);
  - «Путь к токену доступа к хранилищу» - путь к файлу с токеном доступа к OpenBao;
  - «Роль доступа Termidesk VDI (AppRole)» - роль, настроенная на OpenBao, имеющая доступ к логинам и паролям;
  - «ИД роли доступа (RoleID)» - идентификатор роли доступа;
  - «Путь к логину/паролю СУБД» - путь, настроенный на OpenBao для хранения логина и пароля СУБД;
  - «Путь к логинам/паролям RabbitMQ» - путь, настроенный на OpenBao для хранения логинов и паролей брокера сообщений;
  - «Путь к другим секретам Termidesk» - путь, настроенный на OpenBao для хранения других логинов и паролей Termidesk VDI;
  - «Время кеширования паролей, с» - время (в секундах) хранения пароля, полученного от OpenBao, во внутренней памяти;
  - «Период проверки токена доступа, с» - интервал (в секундах) проверки актуальности токена;
  - «Обновлять токен до его устар., с» - оставшееся время (в секундах) актуальности токена, по достижении которого он будет обновлен;
  - «Время жизни токена, с» - время актуальности (в минутах) одноразового токена;

- «Пространство имён» - пространство имени, заданного на OpenBao;

```
+-------------------------Настройка OpenBao.-----------------------------+
| Введите настройки для подключения к OpenBao:                            |
| +-----------------------------------------------------------------------+ |
| |URL хранилища                        http://127.0.0.1:8200           | |
| |Версия API OpenBao                   1                               | |
| |Путь к токену доступа к хранилищу    /etc/opt/termidesk-vdi/openbao.to | |
| |Роль доступа Termidesk (AppRole)     termidesk-role                  | |
| |ИД роли доступа (RoleID)             |                               | |
| |Путь к логину/паролю СУБД            hvac-kv://secret#/postgresql/   | |
| |Путь к логинам/паролям RabbitMQ      hvac-kv://secret#/rabbitmq/     | |
| |Путь к другим секретам Termidesk     hvac-kv://secret#/termidesk     | |
| |Время кешировнаия паролей, с         5                               | |
| |Период проверки токена доступа, с    10                              | |
| |Обновлять токен до его устар., с     30                              | |
| |Время жизни токена, с                600                             | |
| |Пространство имён                    |                               | |
| +-----------------------------------------------------------------------+ |
+-------------------------------------------------------------------------+
|        <   Далее   >      <Сертификаты>      <   Сброс   >              |
+-------------------------------------------------------------------------+
```

Рисунок 8. Настройка подключения к OpenBao

- подключение может выполняться по протоколу HTTPS, если OpenBao настроен соответствующим образом. Для подключения по HTTPS нужно нажать экранную кнопку **[Сертификаты]** и определить пути (см. рисунок Конфигурация сертификатов и ключей) к сертификатам и ключам (параметры «Сертификат OpenBao начального mTLS», «Секр. ключ OpenBao начального mTLS», «Серт. промеж. ЦС OpenBao нач. mTLS»);

Доступный список сертификатов приведен в подразделе **Утилита** `termidesk-config` документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

Справочная информация по работе с диалогом добавления сертификата доступна по экранной кнопке **[Справка]** при выборе нужного пункта из списка.

Если заданы сертификаты и ключ для подключения по mTLS, то будет выведено соответствующее предупреждение на этапе задания параметров подключения к СУБД или брокеру сообщений (при ответе «Нет» произойдет возврат к редактированию параметров подключения к узлу):

- имена узлов для подключения к СУБД или брокеру сообщений (в последующих пунктах установщика) обязательно должны быть заданы в формате FQDN. Использовать IP-адрес узла или `localhost` не рекомендуется;
- сертификат должен быть действителен и соответствовать FQDN узла.

При невыполнении условий работа mTLS не гарантируется.

```
Настройка путей к сертификатам и ключам
Выберите ключ для настройки:
Сертификат Health Check: Не задан
Секр. ключ Health Check: Не задан
Сертификат PostgreSQL mTLS: Не задан
Секр. ключ PostgreSQL mTLS: Не задан
Серт. промеж. ЦС PostgreSQL mTLS: Не задан
Сертификат OpenBao начального mTLS: Не задан
Секр. ключ OpenBao начального mTLS: Не задан
Серт. промеж. ЦС OpenBao нач. mTLS: Не задан
Путь к серт. для втор. mTLS с OpenBao: Не задан
Осн. серт. для расшифровки JWT-токена: Не задан
Рез. серт. для расшифровки JWT-токена: Не задан
Секр. ключ для подписи JWT-токена: Не задан
Сертификат ЦС сервера RA: Не задан
Сертификат RabbitMQ mTLS: Не задан
Секр. ключ RabbitMQ mTLS: Не задан
Серт. ЦС RabbitMQ mTLS: Не задан
Сертификат службы TermideskMQ: Не задан
(+)                                                    68%
<Выбрать>                < Далее >
```

Рисунок 9. Конфигурация сертификатов и ключей

- после настройки способа хранения паролей нужно задать ключ DJANGO. Значение создается автоматически, но при необходимости можно сформировать новое значение, нажав экранную кнопку **[Обновить]**. Поддерживается задание пути в хранилище чувствительной информации, если ключ DJANGO расположен в нем. Для продолжения установки нажать экранную кнопку **[Далее]**;

```
Задание ключа DJANGO.
Задайте настройки хранения данных в СУБД (ключ):
Задание ключа DJANGOHJHfxWUT9xVdQDSyateuuKBkpAYGc4J8cn2upfb3FIw=
< Далее >        <Обновить>        < Сброс >
```

Рисунок 10. Настройка хранения данных - задание ключа DJANGO

- далее выбрать протокол, который будет использоваться при подключении к серверу СУБД (см. рисунок Выбор протокола для подключения к СУБД):
  - при выборе значения «Открытый, без защиты» защищенное соединение при подключении к серверу СУБД использоваться не будет;
  - при выборе защищенного подключения нужно нажать экранную кнопку **[Сертификаты]** и определить пути к сертификатам и ключам (параметры «Сертификат PostgreSQL mTLS», «Секр. ключ PostgreSQL mTLS», «Серт. промеж. ЦС PostgreSQL mTLS»);

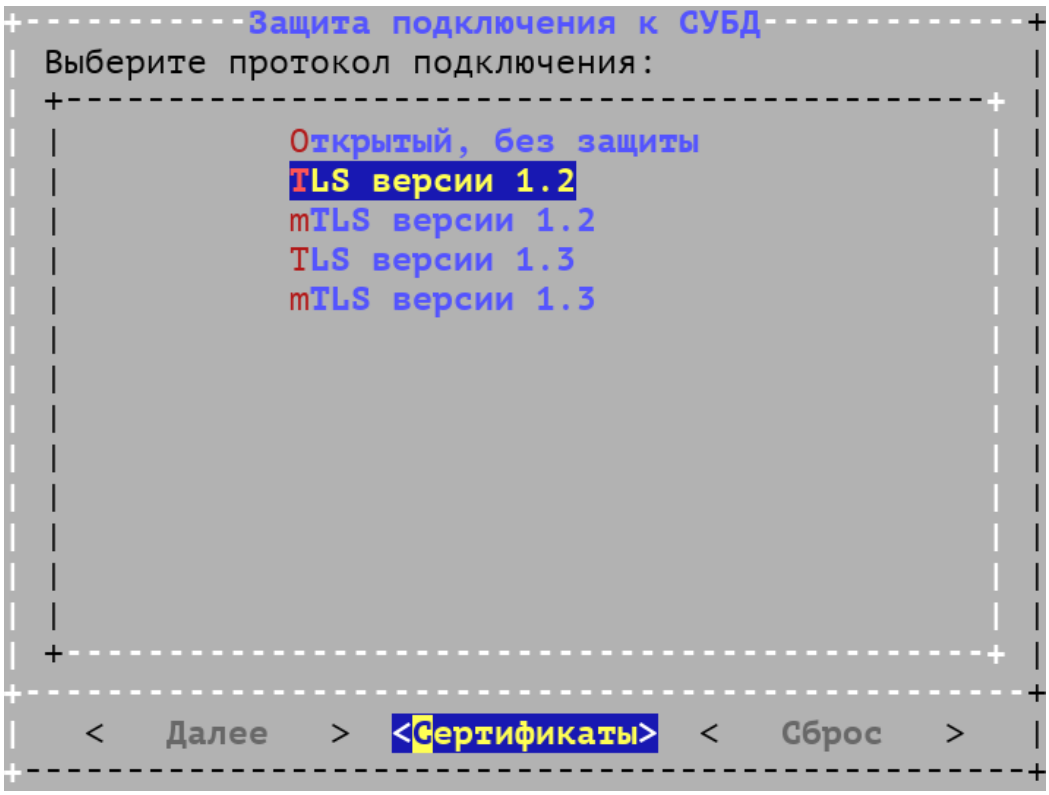


Рисунок 11. Выбор протокола для подключения к СУБД

- для продолжения установки нажать экранную кнопку **[Далее]**;
- выбрать тип установки СУБД (см. рисунок Выбор типа установки СУБД):
  - «Отдельно стоящий сервер»: подключение производится к отдельному серверу СУБД;
  - «Кластер СУБД»: подключение производится к кластеру СУБД;

При выборе типа установки СУБД «Кластер СУБД» можно задать до трех узлов СУБД, к которым будет подключаться Termidesk VDI. При этом предполагается, что порт, имя БД, имя пользователя и его пароль идентичны для всех узлов.

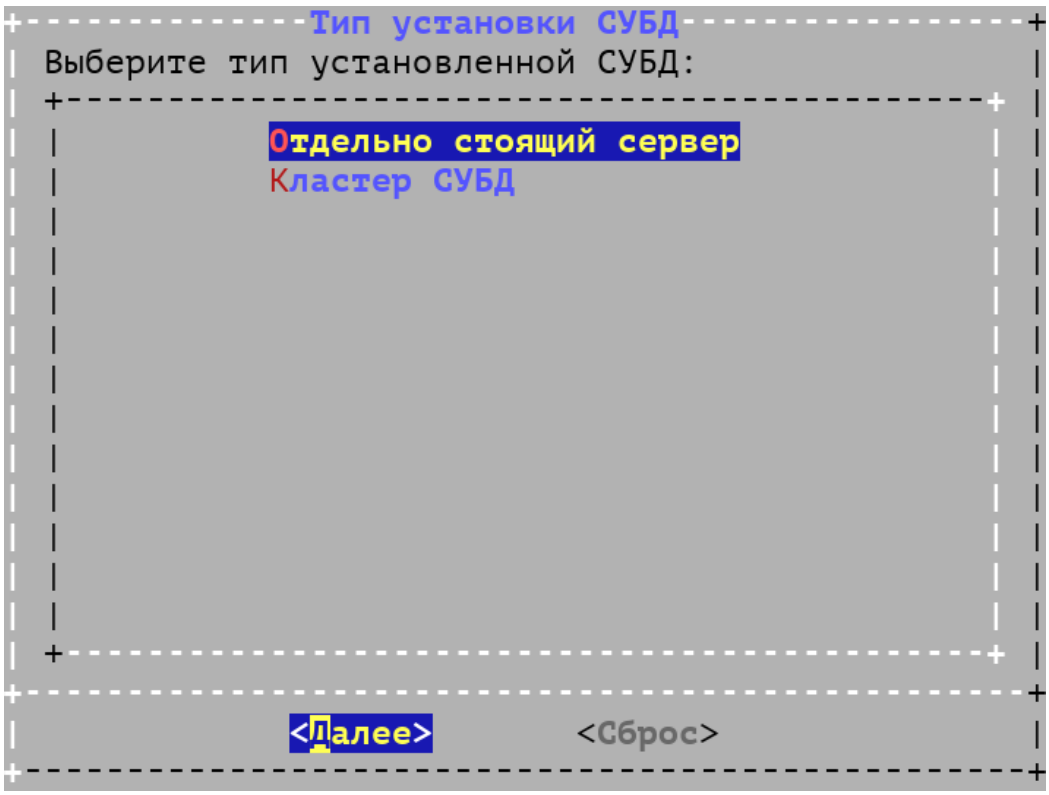


Рисунок 12. Выбор типа установки СУБД

- заполнить параметры подключения к СУБД (см. рисунок Ввод параметров подключения к СУБД):
  - «Адрес»: IP-адрес или FQDN узла с установленной СУБД (в случае локальной установки `127.0.0.1`);
  - «Адрес (узел 2)»: IP-адрес или FQDN дополнительного узла СУБД (необязательный параметр, при необходимости может быть задан только для кластера СУБД);
  - «Адрес (узел 3)»: IP-адрес или FQDN дополнительного узла СУБД (необязательный параметр, при необходимости может быть задан только для кластера СУБД);
  - «Порт»: номер порта, используемого для соединения с сервером СУБД (стандартный порт `5432`);
  - «Имя базы данных»: наименование БД (`termidesk`, параметр задавался при создании БД);
  - «Имя пользователя»: имя пользователя БД для подключения к ней (`termideskdb`, параметр задавался при создании БД);
  - «Пароль»: пароль для подключения к БД (`ksedimret`, параметр задавался при создании БД);
  - «Время жизни подключения, с»: максимально допустимое время (в секундах) существования одного подключения к БД;
  - «Кол-во задач на подключение»: количество фоновых задач, которое может быть выполнено в рамках одного подключения к БД;
  - «Таймаут подключения к СУБД, с»: время ожидания (в секундах) подключения к БД;

Если для хранения паролей был выбран режим «hvac», то имя пользователя и пароль не задаются в этом окне, т.к. значения для них берутся из хранилища.

```
+-------------------Настройка подключения к СУБД.-------------------------+
| Введите настройки для подключения к СУБД                                |
| +-----------------------------------------------------------------------+ |
| |Адрес                          localhost                               | |
| |Адрес (узел 2)                                                         | |
| |Адрес (узел 3)                                                         | |
| |Порт                           5432                                    | |
| |Имя базы данных                termidesk                               | |
| |Имя пользователя               termideskdb                             | |
| |Пароль                         *********                               | |
| |Время жизни подключения, с     600                                     | |
| |Кол-во задач на подключение    1000                                    | |
| |Таймаут подключения к СУБД, с  10                                      | |
| +-----------------------------------------------------------------------+ |
+-------------------------------------------------------------------------+
|                 <Далее>          <Тест >          <Сброс>               |
+-------------------------------------------------------------------------+
```

Рисунок 13. Ввод параметров подключения к СУБД

- нажать экранную кнопку **[Тест]** для проверки подключения, ознакомиться с результатом тестирования подключения и для продолжения установки нажать экранную кнопку **[Далее]**;

> Тест подключения к СУБД доступен и в режиме mTlS, если:
>
> - ранее была выбрана защита подключения к СУБД по mTLS;
> - были заданы сертификат, ключ и корневой сертификат УЦ для подключения к СУБД по mTLS.

- выбрать протокол, который будет использоваться при подключении к брокеру сообщений (см. рисунок Выбор протокола для подключения к брокеру сообщений):
  - при выборе значения «Открытый, без защиты» защищенное соединение при подключении использоваться не будет;
  - при выборе защищенного подключения нужно нажать экранную кнопку **[Сертификаты]** и определить пути к сертификатам и ключам (параметры «Сертификат RabbitMQ mTLS», «Секр. ключ RabbitMQ mTLS», «Серт. ЦС RabbitMQ mTLS»);

> В Termidesk VDI версии 6.1 установка «Брокера сообщений TermideskMQ» поддерживается в экспериментальном режиме (установка происходит на этапе выбора ролей узла далее).
>
> Одновременное использование RabbitMQ и «Брокера сообщений TermideskMQ» в рамках одной фермы не поддерживается. Рекомендуется удалить RabbitMQ или отключить службу `rabbitmq-server`, если будет использоваться «Брокер сообщений TermideskMQ».

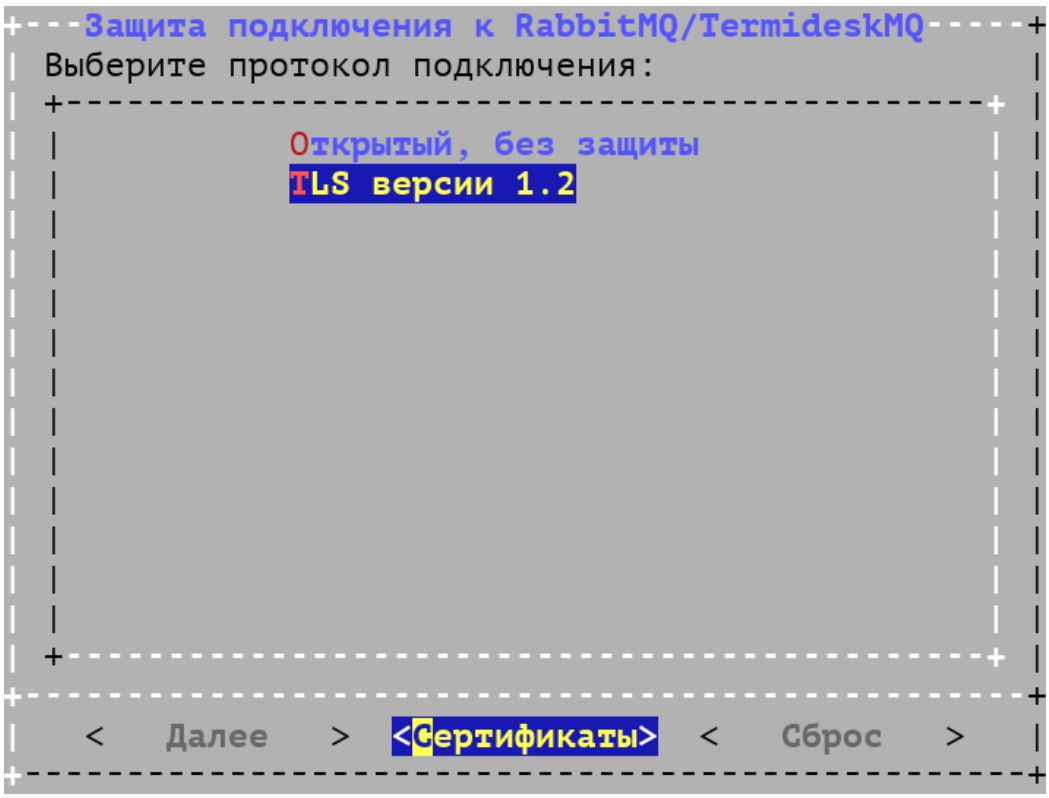


Рисунок 14. Выбор протокола для подключения к брокеру сообщений

- настроить подключение к брокеру сообщений. Для этого выбрать в следующем окне пункт «Empty» и нажать экранную кнопку **[Выбрать]** (см. рисунок Экранная форма начала настройки подключения к брокеру сообщений). Необходимо задать хотя бы одно подключение. Если не будет задано ни одно подключение, то при нажатии на кнопку **[Далее]** произойдет возврат в диалог настройки подключений;

Рисунок 15. Экранная форма начала настройки подключения к брокеру сообщений

- выполнить настройку подключения к брокеру сообщений, заполнив параметры (см. рисунок Настройка подключения к брокеру сообщений):

Если для хранения паролей был выбран режим «hvac», то имя пользователя и пароль не задаются в этом окне, т.к. значения для них берутся из хранилища.

- «Протокол (amqp/tmqp)»: протокол подключения к брокеру сообщений. Следует назначить: «amqp» для RabbitMQ, «tmqp» для «Брокера сообщений TermideskMQ»;
- «Адрес»: IP-адрес или FQDN узла с установленным брокером сообщений (в случае локальной установки 127.0.0.1);
- «Порт»: номер порта, используемого для соединения с брокером сообщения (стандартный порт: 5672 для RabbitMQ, 5555 для «Брокера сообщений TermideskMQ»);
- «Виртуальный хост»: виртуальный узел, к которому будет производиться подключение (termidesk);
- «Имя пользователя»: имя пользователя для подключения (termidesk);
- «Пароль»: пароль для подключения (ksedimret);

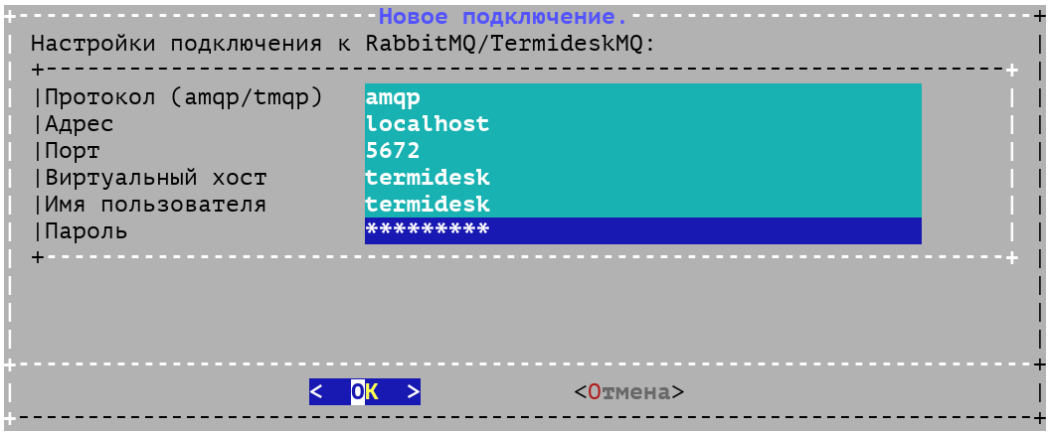


Рисунок 16. Настройка подключения к брокеру сообщений

- нажать экранную кнопку **[OK]** для продолжения установки;
- в следующем окне отобразится информация о настроенном подключении (см. рисунок Отображение параметров подключения к брокеру сообщений). При необходимости можно добавить до трех экземпляров брокера сообщений для подключения, выбрав пустые строки «Empty» и повторив ввод параметров подключения. Для продолжения установки следует нажать экранную кнопку **[Далее]**;

Если для хранения паролей был выбран режим «hvac», то имя пользователя будет скрыто.

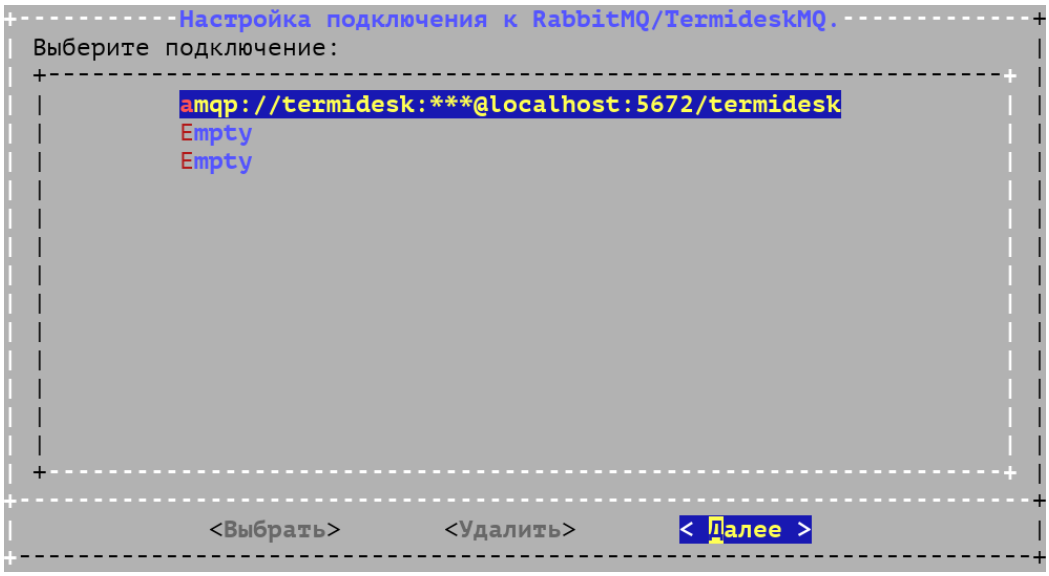


Рисунок 17. Отображение параметров подключения к брокеру сообщений

- задать токен доступа к службе проверки состояния узла. Значение создается автоматически, но при необходимости можно сформировать новое значение, нажав экранную кнопку **[Обновить]**. Поддерживается задание пути в хранилище чувствительной информации, если токен расположен в нем. Для продолжения установки нажать экранную кнопку **[Далее]**;
- задать токен доступа к службе получения метрик узла. Значение создается автоматически, но при необходимости можно сформировать новое значение, нажав экранную кнопку **[Обновить]**. Поддерживается задание пути в хранилище чувствительной информации, если токен расположен в нем. Для продолжения установки нажать экранную кнопку **[Далее]**;
- выбрать язык графического интерфейса, который будет использоваться в Termidesk VDI по умолчанию (см. рисунок Выбор языка графического интерфейса Termidesk VDI). Для продолжения установки нажать экранную кнопку **[Далее]**.

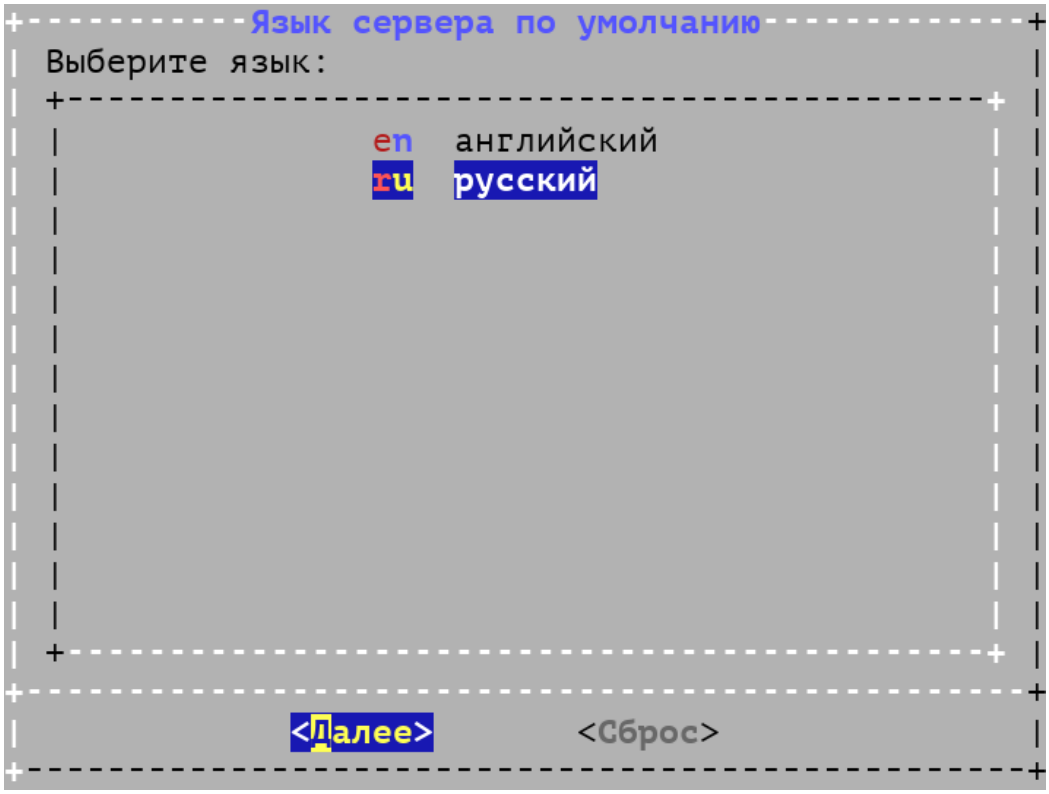


Рисунок 18. Выбор языка графического интерфейса Termidesk VDI

После установки Termidesk VDI необходимо:

- скорректировать файл конфигурации веб-сервера `/etc/apache2/apache2.conf`. Для этого нужно найти и раскомментировать строку с параметром `AstraMode`, далее присвоить данному параметру значение `off`, точно соблюдая отступы и пробелы в файле:

```
# Astra security mode
#
AstraMode off
```

- затем перезапустить веб-сервер:

```
sudo systemctl restart apache2
```

- если при установке было задано использование хранилище паролей, то необходимо выполнить запуск служб Termidesk VDI вручную:

```
sudo systemctl start termidesk-vdi.service termidesk-celery-beat.service termidesk-celery-worker.service
```

- если в инфраструктуре Termidesk VDI будет использоваться портал «Агрегатор» , нужно обязательно задать на узле компонента «Универсальный диспетчер» («Портал пользователя» или «Портал универсальный») сертификат для расшифровки JWT-токена. Сертификат может быть задан через файл `/etc/opt/termidesk-vdi/termidesk.conf` (параметры `AGGREGATOR_JWT_SSL_CERT` и `AGGREGATOR_JWT_SSL_CERT_SECOND`) или через утилиту `termidesk-config`.

После установки параметры могут быть изменены:

- через файл `termidesk.conf`;
- через утилиту `termidesk-config`.

В процессе установки будет выполнена настройка для работы в режиме мандатного контроля целостности и мандатного разграничения доступа:

- установлена метка `0` для пользователя `termidesk` и права на чтение файла с меткой пользователю `postgres`, если такой есть в ОС и метка ещё не устанавливалась. Если метка ранее была установлена, то она не изменится и не сбросится, права на файл с меткой не будут установлены;
- установлена метка `0` для пользователя, подключающегося к СУБД, и права на чтение файла с меткой пользователю `postgres`, если такой есть в ОС и метка ещё не устанавливалась. Если метка ранее была установлена, то она не изменится и не сбросится, права на файл с меткой не будут установлены.

Автоматизированная комплексная установка через конфигурационный файл

Перед установкой Termidesk VDI следует убедиться, что в БД отсутствуют записи (необходимо использовать чистую БД).

Описание приведено для фермы Termidesk VDI. Для установки портала «Агрегатор» следует использовать другую конфигурацию, приведенную в подразделе **Автоматизированная установка «Агрегатора»** документа СЛЕТ.10001-01 90 08 «Руководство администратора. Установка и настройка «Агрегатора»

Для автоматизированной установки нужно:

- создать файл `/etc/default/termidesk-vdi.local`:

```
sudo touch /etc/default/termidesk-vdi.local
```

- указать в созданном файле каталоги расположения конфигурационного файла и шаблонов настройки регистрации событий и журналирования:

```
ETC='/etc/opt/termidesk-vdi'
```

```
TEMPLATES_DIR='/etc/opt/termidesk-vdi/templates'
```

- создать каталог `/etc/opt/termidesk-vdi`:

```
sudo mkdir /etc/opt/termidesk-vdi
```

- создать файл `/etc/opt/termidesk-vdi/termidesk.conf`:

```
sudo touch /etc/opt/termidesk-vdi/termidesk.conf
```

- отредактировать созданный файл по примеру ниже;
- выполнить:

Переменная `NON_INTERACTIVE_INSTALLATION` используется для «тихой» установки без отображения дополнительных диалоговых окон. Переменная может быть передана другим способом, но после завершения установки должна быть отключена.

При использовании этой переменной со значением `yes` убедитесь, что в конфигурационном файле `termidesk.conf` присутствуют **все** параметры, которые имеются в файле конфигурации дистрибутива (`termidesk.conf.dist`). В противном случае установка пакета завершится ошибкой. Подробности о недостающих параметрах можно найти в файле `/var/log/syslog`.

```
sudo NON_INTERACTIVE_INSTALLATION='yes' apt install -y termidesk-vdi
```

Описание параметров файла приведено в подразделе **Конфигурационный файл `termidesk.conf`** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Настройка программного комплекса».

Пример файла `/etc/opt/termidesk-vdi/termidesk.conf`:

- используются значения по умолчанию для имени пользователи и пароля;
- пароли и имена хранятся в конфигурационном файле (хранилище не используется);
- используется незащищенное подключение к БД и RabbitMQ.

```
TERMIDESK_FARM_MODE='BROKER'
NODE_ROLES='ADMIN,USER,CELERYMAN'
NODE_NAME=astra18-tdsk-vdi-ea_0050568fef1a
SECRETS_STORAGE_METHOD='config'
DB_CLUSTER_MODE='single'
DBHOST='localhost'
DBPORT='5432'
DBSSL='Disable'
DBNAME='termidesk'
DBUSER='termideskdb'
```

```
DBPASS='ksedimret'
DB_CONN_MAX_AGE=600
CELERY_DB_REUSE_MAX=1000
DB_CONN_TIMEOUT=10
RABBITMQ_URL1='amqp://termidesk:ksedimret@localhost:5672/termidesk'
RABBITMQ_URL2=
RABBITMQ_URL3=
RABBITMQ_SSL='Disable'
DJANGO_SECRET_KEY='t6ajnMB3KMyfMEffz8SYlZMzCsGP0dENc2wFXYPAfgc='
LOG_LEVEL='INFO'
LOG_ADDRESS='/dev/log'
LOG_FACILITY='local3'
LOG_DIR='/var/log/termidesk'
LOG_OWNER='termidesk'
LOG_GROUP='adm'
LOG_PERM='0440'
LOG_DEEP='14'
FLUENTD_CACHE=15
FLUENTD_TABLE='logs'
FLUENTD_LOGGER_TIMEOUT=5
HEALTH_CHECK_ACCESS_KEY='7e3a48572334c022ce774668047b4b00d44a7129e7857ae0a068f00832
aee498'
METRICS_ACCESS_KEY='0f77b6a57b491e0aa4cd7a78d3d068386a5a0b6832c25b6b0c2bdcfbc079e91
a'
EULA_ACCEPTED='YES'
```

После установки указанные в открытом виде пароли можно привести к преобразованным значениям (см. подраздел **Конфигурационный файл** `termidesk.conf` документа СЛЕТ.10001-01 90 01 «Руководство администратора. Настройка программного комплекса»).

> Если в инфраструктуре Termidesk VDI будет использоваться портал «Агрегатор» («Агрегатор администратора» и/или «Агрегатор пользователя»), нужно обязательно задать на узле компонента «Универсальный диспетчер» фермы Termidesk VDI («Портал пользователя» или «Портал универсальный») сертификат для расшифровки JWT-токена. Сертификат может быть задан через файл `termidesk.conf` (параметры `AGGREGATOR_JWT_SSL_CERT` и `AGGREGATOR_JWT_SSL_CERT_SECOND`) или через утилиту `termidesk-config` (см. подраздел см. подраздел **Утилита** `termidesk-config` документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»).

После установки параметры могут быть изменены:

- через файл `termidesk.conf`;
- через утилиту `termidesk-config`.

Минимальная распределенная установка

Основные принципы минимальной распределенной установки

Минимальная распределенная установка компонентов выполняется на отдельные серверы или ВМ.

Описание применимо к ферме Termidesk VDI.

Реализация отказоустойчивости инфраструктурных сервисов выполняется организацией в соответствии с требованиями к инфраструктуре.

При использовании внешней по отношению к Termidesk VDI СУБД, следует установить брокер сообщений RabbitMQ на узел «Менеджера рабочих мест» или на отдельный узел.

Начиная с Termidesk VDI версии 6.1 компонент «Шлюз» (пакет `termidesk-gateway`) не входит в основную поставку. Для замены «Шлюза» следует использовать программу для электронной вычислительной машины «Балансировщик нагрузки Термидеск Коннект» (Termidesk Connect).

Инструкции по установке и настройке доступны по ссылкам: Инструкция по настройке Шлюза для Termidesk VDI (первый способ), Инструкция по настройке Шлюза для Termidesk VDI (второй способ, единая точка входа Termidesk VDI).

В минимальном варианте распределенной установки устанавливаются компоненты:

- «Универсальный диспетчер» (служба `termidesk-vdi`);
- «Менеджер рабочих мест» (службы `termidesk-celery-beat`, `termidesk-celery-worker`).

Перечень условий для распределенной установки:

- брокер сообщений RabbitMQ устанавливается на одном узле с СУБД (в общем случае этот компонент может устанавливаться на отдельный узел, но в рамках настоящей процедуры данный вариант не рассматривается);
- на всех узлах, предназначенных для установки компонентов, настроены статические IP-адреса;
- на всех узлах настроена синхронизация времени от единого источника.

Реализация отказоустойчивости инфраструктурных сервисов выполняется организацией в соответствии с требованиями к инфраструктуре.

При использовании внешней по отношению к Termidesk VDI СУБД, следует установить брокер сообщений RabbitMQ на узел «Менеджера рабочих мест» или на отдельный узел.

Упрощенная общая схема при минимальной распределенной установке Termidesk VDI приведена на рисунке (см. рисунок Схема минимальной распределенной установки).

Схема минимальной распределенной установки с Termidesk Connect приведена на рисунке (см. рисунок Схема минимальной распределенной установки при наличии лицензии Termidesk Connect).

Особенности:

- для реализации функционала «Шлюза» используется лицензия Termidesk Connect Basic;
- для реализации функционала балансировщика используется лицензия Termidesk Connect. При отсутствии лицензии допускается использование сторонних балансировщиков нагрузки.

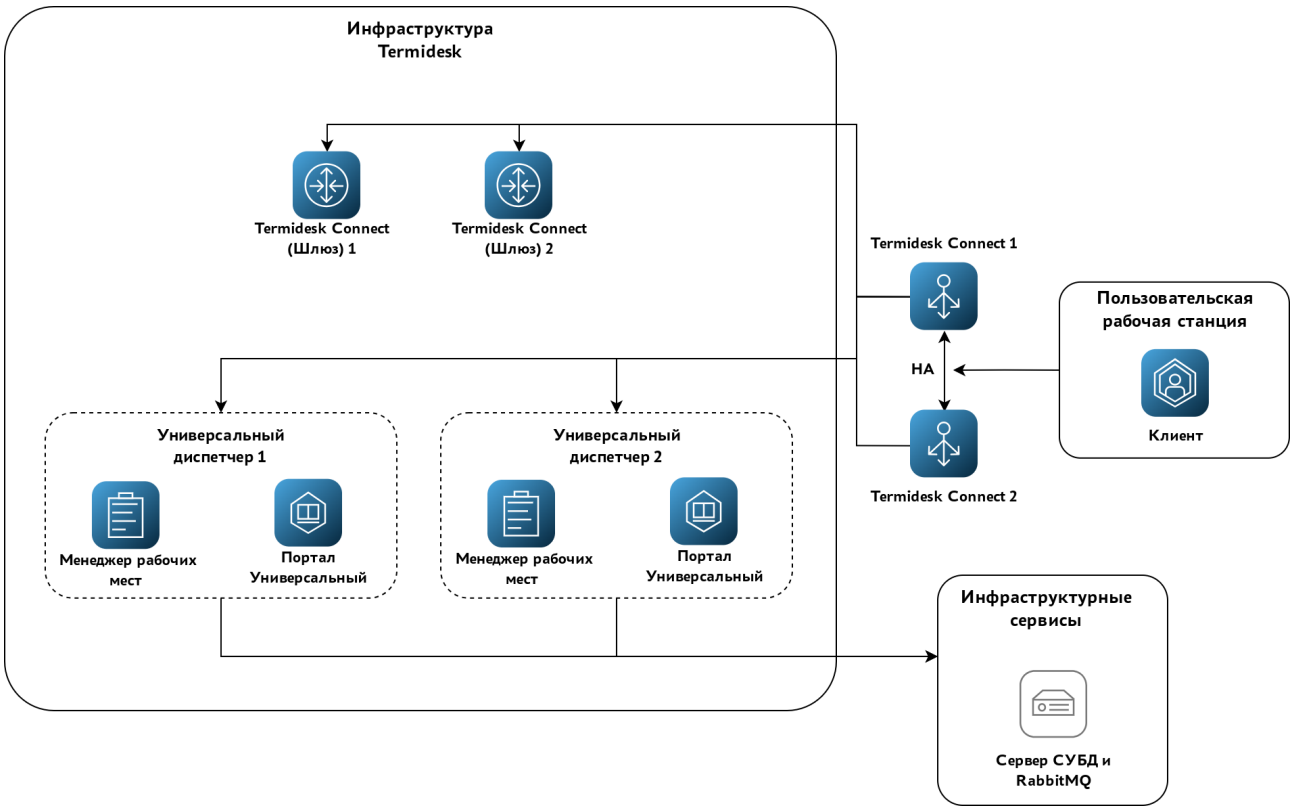


Рисунок 19. Схема минимальной распределенной установки

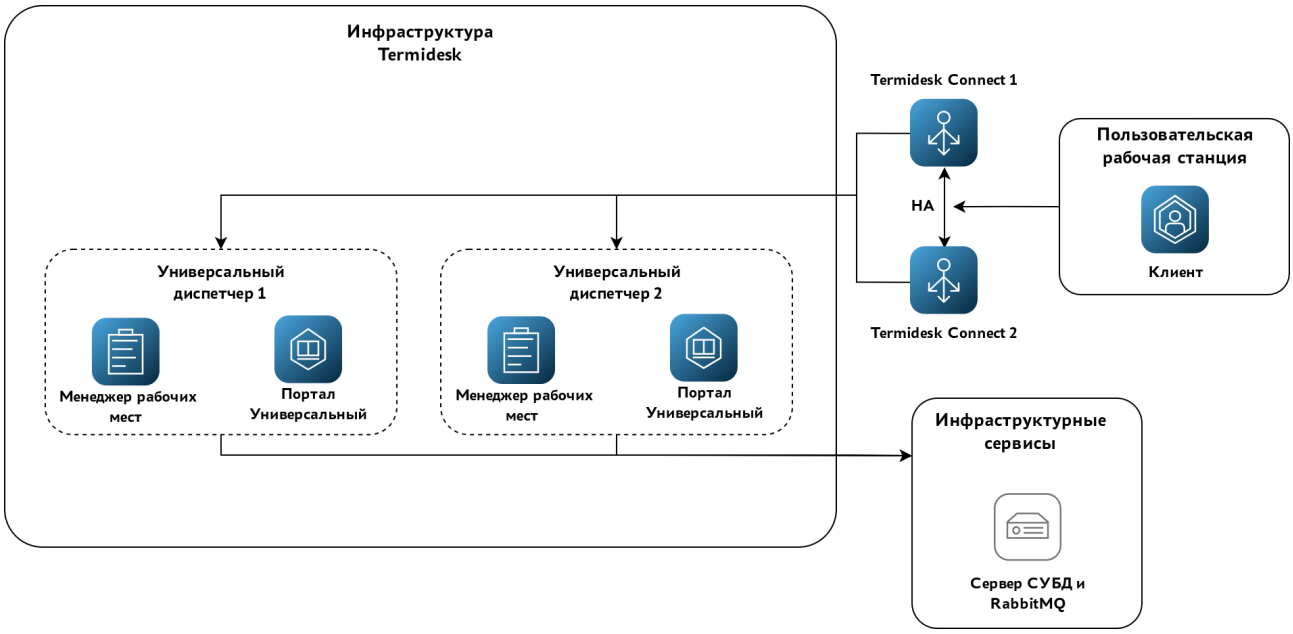


Рисунок 20. Схема минимальной распределенной установки при наличии лицензии Termidesk Connect

Перечень обозначенных на схемах компонентов приведен в таблице (см. таблицу Перечень компонентов схемы минимальной распределенной установки).

Таблица 4. Перечень компонентов схемы минимальной распределенной установки

Компонент	FQDN	^Подпись на схеме
«Универсальный диспетчер» №1 с ролями «Портал универсальный» и «Менеджер рабочих мест»	`disp1.termidesk.local`	«Универсальный диспетчер 1»
«Универсальный диспетчер» №2 с ролями «Портал универсальный» и «Менеджер рабочих мест»	`disp2.termidesk.local`	«Универсальный диспетчер 2»

Компонент	FQDN	^Подпись на схеме
Termidesk Connect (лицензия «Шлюз») №1	`tdc-gw1.termidesk.local`	«Termidesk Connect (Шлюз) 1»
Termidesk Connect (лицензия «Шлюз») №2	`tdc-gw2.termidesk.local`	«Termidesk Connect (Шлюз) 2»
Termidesk Connect №1	`tdc-lb1.termidesk.local`	«Termidesk Connect 1»
Termidesk Connect №2	`tdc-lb2.termidesk.local`	«Termidesk Connect 2»
База данных с брокером сообщений RabbitMQ	`db.termidesk.local`	«Сервер СУБД и RabbitMQ»

Распределенная установка проводится в следующей последовательности:

- на одном узле устанавливаются СУБД и RabbitMQ. При установке следует учесть, что в БД должны отсутствовать записи (необходимо использовать чистую БД);
- устанавливается первый (эталонный) узел с «Универсальным диспетчером». При установке необходимо выбрать роли «Портал универсальный» (роль активируется при одновременном выборе ролей «Портал администратора» и «Портал пользователя» в диалоговом окне псевдографического интерфейса инсталлятора) и «Менеджер рабочих мест».
- устанавливаются остальные «Универсальные диспетчеры» с копированием файлов с эталонного узла;
- устанавливаются и настраиваются «Шлюзы».

Заключительным этапом устанавливаются и настраиваются «Балансировщики нагрузки».

Настройки первого узла с «Универсальным диспетчером» Termidesk VDI будут использоваться как эталонные для другого узла «Универсального диспетчера».

Нужно скопировать каталог `/etc/opt/termidesk-vdi` вместе с его содержимым на узел другого «Универсального диспетчера». Этот каталог содержит ключи для синхронизации параметров между узлами, а также параметры конфигурации узла (файл `/etc/opt/termidesk-vdi/termidesk.conf`).

Установка, настройка СУБД PostgreSQL и RabbitMQ

Процесс установки брокера сообщений RabbitMQ и СУБД PostgreSQL не отличается от процесса, описанного в разделе **Подготовка среды функционирования**.

Установка и настройка СУБД PostgreSQL осуществляется согласно выбранной версии.

Для завершения настройки нужно:

- отредактировать файл `/etc/rabbitmq/rabbitmq-env.conf`, приведя его к виду:

```
# Defaults to rabbit. This can be useful if you want to run more than one node
# per machine - RABBITMQ_NODENAME should be unique per erlang-node-and-machine
# combination. See the clustering on a single machine guide for details:
# http://www.rabbitmq.com/clustering.html#single-machine
```

```
#NODENAME=rabbit

# By default RabbitMQ will bind to all interfaces, on IPv4 and IPv6 if
# available. Set this if you only want to bind to one network interface or#
# address family.
NODE_IP_ADDRESS=0.0.0.0
# Defaults to 5672.
NODE_PORT=5672
```

- сохранить файл и перезапустить службу `rabbitmq-server`:

```
sudo systemctl restart rabbitmq-server
```

Установка первого узла с «Универсальным диспетчером»

Процесс установки первого узла с «Универсальным диспетчером» аналогичен комплексной установке Termidesk VDI. В процессе установки следует выбрать роли: «Портал администратора (ADMIN)», «Портал пользователя (USER)» и «Менеджер рабочих мест (CELERYMAN)».

После установки передать каталог `/etc/opt/termidesk-vdi` на остальные узлы «Универсальных диспетчеров»:

```
sudo scp -r /etc/opt/termidesk-vdi localuser@ipaddr_or_fqdn_host:/home/user/
```

Где:

`-r` - ключ для рекурсивной (со вложенными каталогами) передачи;

`localuser` - имя пользователя целевого узла;

`ipaddr_or_fqdn_host` - IP-адрес или FQDN целевого узла;

`/home/user` - путь, куда будет скопирован каталог.

Перед началом установки остальных узлов «Универсальных диспетчеров» необходимо переместить скопированный ранее каталог `termidesk-vdi` в каталог `/etc/opt/`:

```
sudo mv /home/user/termidesk-vdi /etc/opt/
```

Установить второй узел с «Универсальным диспетчером» по аналогии с первым, не меняя параметры в диалогах подключения к СУБД и заполнения информации о подключении к RabbitMQ.

Установка «Шлюзов»

Начиная с Termidesk VDI версии 6.1 функционал «Шлюза» реализуется через продукт Termidesk Connect. Подробные сведения приведены в документации Termidesk Connect (доступ по ссылке: https://termidesk.ru/docs/).

Установка «Балансировщиков нагрузки»

Подробные сведения по установке «Балансировщика нагрузки» приведены в документации Termidesk Connect (доступ по ссылке: https://termidesk.ru/docs/).

При отсутствии полной лицензии на Termidesk Connect допускается использование сторонних балансировщиков нагрузки.

Действия после минимальной распределенной установки

Настройка «Балансировщика нагрузки» приведена в документации Termidesk Connect (доступ по ссылке: https://termidesk.ru/docs/).

Если в инфраструктуре Termidesk VDI будет использоваться портал «Агрегатор» («Агрегатор администратора» и/или «Агрегатор пользователя»), нужно обязательно задать на узле компонента «Универсальный диспетчер» («Портал пользователя» или «Портал универсальный») сертификат для расшифровки JWT-токена. Сертификат может быть задан через файл `/etc/opt/termidesk-vdi/termidesk.conf` (параметры `AGGREGATOR_JWT_SSL_CERT` и `AGGREGATOR_JWT_SSL_CERT_SECOND`) или через утилиту `termidesk-config`.

После установки параметры могут быть изменены:

- через файл `termidesk.conf`;
- через утилиту `termidesk-config`.

Стандартная распределенная установка

Основные принципы стандартной распределенной установки

В Termidesk VDI предусмотрена распределенная установка компонентов на отдельные серверы или ВМ.

Описание применимо к ферме Termidesk VDI.

Реализация отказоустойчивости инфраструктурных сервисов выполняется организацией в соответствии с требованиями к инфраструктуре.

При использовании внешней по отношению к Termidesk VDI СУБД, следует установить брокер сообщений RabbitMQ на узел «Менеджера рабочих мест» или на отдельный узел.

Начиная с Termidesk VDI версии 6.1, компонент «Шлюз» (пакет `termidesk-gateway`) не входит в основную поставку. Для замены «Шлюза» следует использовать программу для электронной вычислительной машины «Балансировщик нагрузки Термидеск Коннект» (Termidesk Connect).

Инструкции по установке и настройке доступны по ссылкам: Инструкция по настройке Шлюза для Termidesk VDI (первый способ), Инструкция по настройке Шлюза для Termidesk VDI (второй способ, единая точка входа Termidesk VDI).

В распределенном варианте устанавливаются компоненты:

- «Универсальный диспетчер» (служба `termidesk-vdi`);
- «Менеджер рабочих мест» (службы `termidesk-celery-beat`, `termidesk-celery-worker`).

Перечень условий для распределенной установки:

- брокер сообщений RabbitMQ устанавливается на одном узле с СУБД (в общем случае этот компонент может устанавливаться на отдельный узел, но в рамках настоящей процедуры данный вариант не рассматривается);
- на всех узлах, предназначенных для установки компонентов, настроены статические IP-адреса;
- на всех узлах настроена синхронизация времени от единого источника.

Упрощенная общая схема при стандартной распределенной установке Termidesk VDI приведена на рисунке (см. рисунок Схема стандартной распределенной установки).

Схема стандартной распределенной установки с Termidesk Connect приведена на рисунке (см. рисунок Схема стандартной распределенной установки при наличии лицензии Termidesk Connect).

Особенности:

- для реализации функционала «Шлюза» используется лицензия Termidesk Connect Basic;
- для реализации функционала балансировщика используется лицензия Termidesk Connect. При отсутствии лицензии допускается использование сторонних балансировщиков нагрузки.

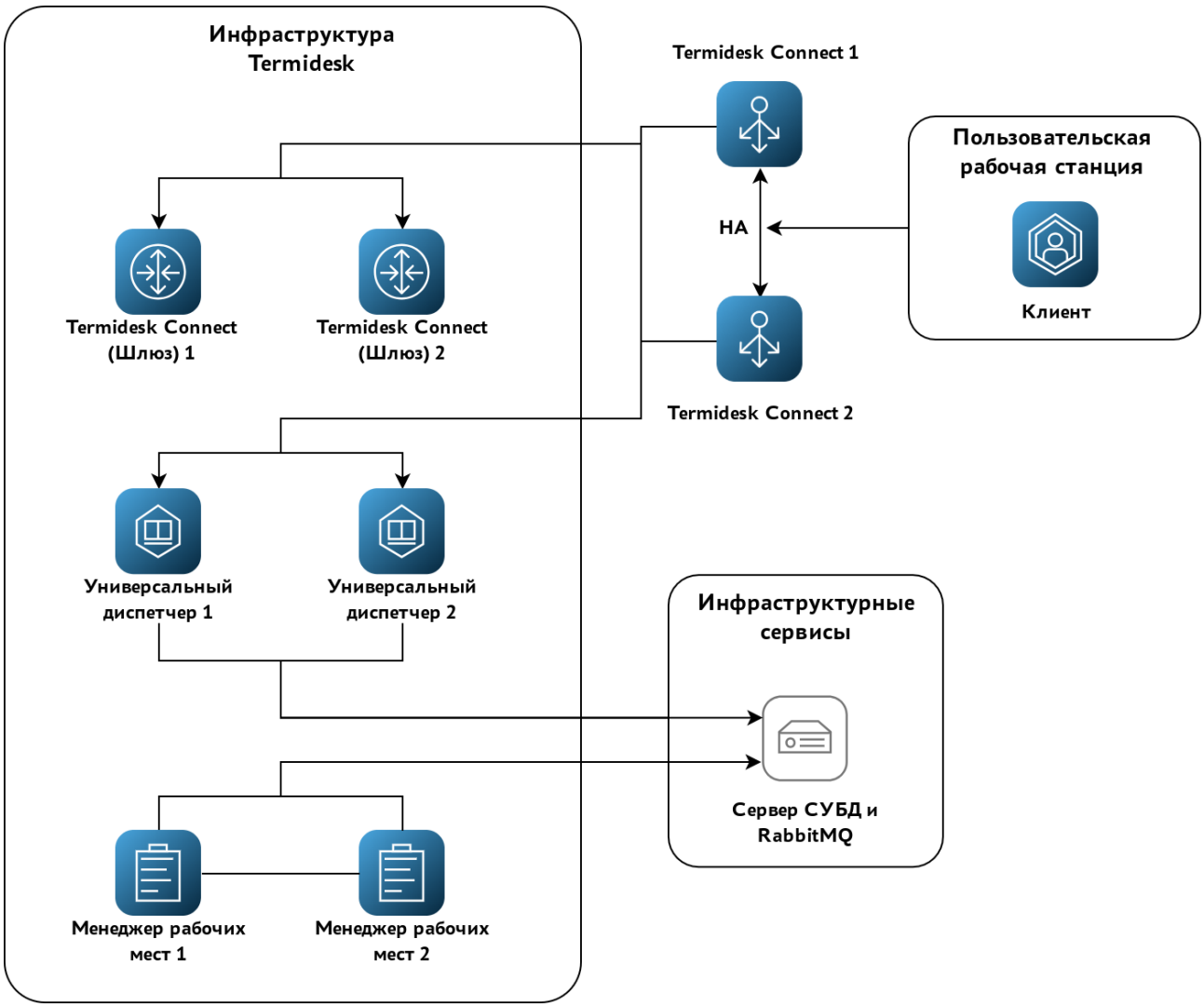


Рисунок 21. Схема стандартной распределенной установки

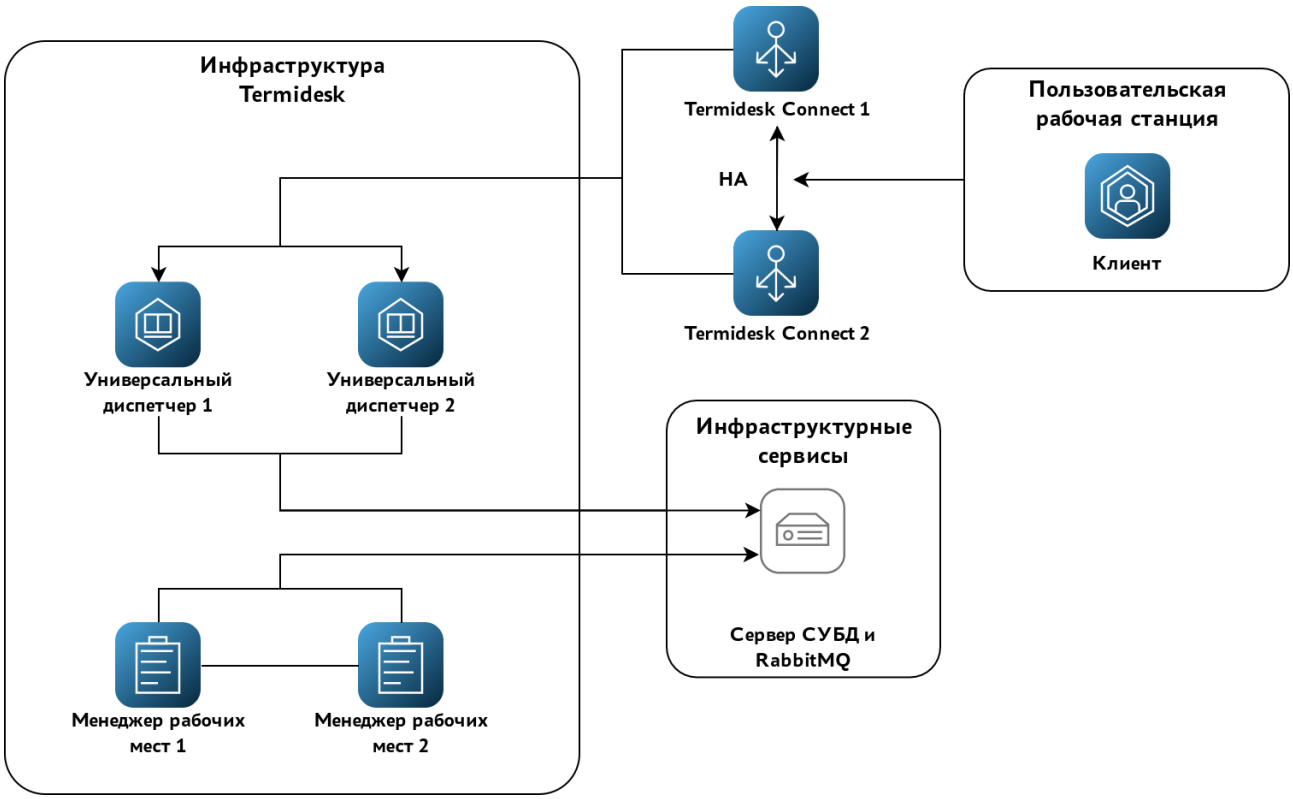


Рисунок 22. Схема стандартной распределенной установки при наличии лицензии Termidesk Connect

Перечень обозначенных на схемах компонентов приведен в таблице (см. таблицу Перечень компонентов).

Таблица 5. Перечень компонентов

Компонент	FQDN	Подпись на схеме
«Универсальный диспетчер» №1 с ролью «Портал универсальный»	`disp1.termidesk.local`	«Универсальный диспетчер 1»
«Универсальный диспетчер» №2 с ролью «Портал универсальный»	`disp2.termidesk.local`	«Универсальный диспетчер 2»
Termidesk Connect (лицензия «Termidesk Connect Basic») №1	`tdc-gw1.termidesk.local`	«Termidesk Connect (Шлюз) 1»
Termidesk Connect (лицензия «Termidesk Connect Basic») №2	`tdc-gw2.termidesk.local`	«Termidesk Connect (Шлюз) 2»
«Менеджер рабочих мест» №1	`tsk1.termidesk.local`	«Менеджер рабочих мест 1»
«Менеджер рабочих мест» №2	`tsk2.termidesk.local`	«Менеджер рабочих мест 2»
Termidesk Connect №1	`tdc-lb1.termidesk.local`	«Termidesk Connect 1»
Termidesk Connect №2	`tdc-lb2.termidesk.local`	«Termidesk Connect 2»
База данных с брокером сообщений RabbitMQ	`db.termidesk.local`	«Сервер СУБД и RabbitMQ»

Стандартная распределенная установка проводится в следующей последовательности:

- на одном узле устанавливаются СУБД и RabbitMQ. При установке следует учесть, что в БД должны отсутствовать записи (необходимо использовать чистую БД);

- устанавливается первый (эталонный) узел с «Универсальным диспетчером». При установке необходимо выбрать роли «Портал универсальный» (роль активируется при одновременном выборе ролей «Портал администратора» и «Портал пользователя» в диалоговом окне псевдографического интерфейса инсталлятора);
- устанавливаются остальные «Универсальные диспетчеры» с копированием файлов с эталонного узла;
- устанавливаются и настраиваются «Шлюзы»;
- устанавливаются «Менеджеры рабочих мест» с копированием файлов с эталонного узла.

Заключительным этапом устанавливаются и настраиваются «Балансировщики нагрузки».

Установка, настройка СУБД PostgreSQL и RabbitMQ

Процесс установки брокера сообщений RabbitMQ и СУБД PostgreSQL не отличается от процесса, описанного в разделе **Подготовка среды функционирования**.

Установка и настройка СУБД PostgreSQL осуществляется согласно выбранной версии.

Для завершения настройки нужно:

- отредактировать файл `/etc/rabbitmq/rabbitmq-env.conf`, приведя его к виду:

```
# Defaults to rabbit. This can be useful if you want to run more than one node
# per machine - RABBITMQ_NODENAME should be unique per erlang-node-and-machine
# combination. See the clustering on a single machine guide for details:
# http://www.rabbitmq.com/clustering.html#single-machine
#NODENAME=rabbit

# By default RabbitMQ will bind to all interfaces, on IPv4 and IPv6 if
# available. Set this if you only want to bind to one network interface or#
# address family.
NODE_IP_ADDRESS=0.0.0.0
# Defaults to 5672.
NODE_PORT=5672
```

- сохранить файл и перезапустить службу `rabbitmq-server`:

```
sudo systemctl restart rabbitmq-server
```

Установка первого узла с «Универсальным диспетчером»

Процесс установки первого узла с «Универсальным диспетчером» аналогичен комплексной установке Termidesk VDI, за исключением выбора только ролей «Портал администратора» и «Портал пользователя».

После установки передать каталог `/etc/opt/termidesk-vdi` на остальные узлы «Универсальных диспетчеров» и «Менеджеров рабочих мест»:

```
sudo scp -r /etc/opt/termidesk-vdi localuser@ipaddr_or_fqdn_host:/home/user/
```

Где:

`-r` - ключ для рекурсивной (со вложенными каталогами) передачи;

`localuser` - имя пользователя целевого узла;

`ipaddr_or_fqdn_host` - IP-адрес или FQDN целевого узла;

`/home/user` - путь, куда будет скопирован каталог.

Перед началом установки остальных узлов «Универсальных диспетчеров» необходимо переместить скопированный ранее каталог `termidesk-vdi` в каталог `/etc/opt/`:

```
sudo mv /home/user/termidesk-vdi /etc/opt/
```

При копировании конфигурации с эталонного узла на другие узлы параметр `NODE_NAME` в файле `/etc/opt/termidesk-vdi/termidesk.conf` также копируется. Этот параметр должен быть уникальным для каждого узла в ферме. На каждом узле необходимо изменить значение `NODE_NAME` на уникальное, либо удалить его, чтобы при следующем запуске инсталлятор сгенерировал новое значение автоматически. Изменить параметр можно вручную в файле или с помощью утилиты `termidesk-config`.

Установить второй узел с «Универсальным диспетчером» по аналогии с первым, не меняя параметры в диалогах подключения к СУБД и заполнения информации о подключении к RabbitMQ.

Установка «Шлюзов»

Начиная с Termidesk VDI версии 6.1, функционал «Шлюза» реализуется через продукт Termidesk Connect. Подробные сведения приведены в документации Termidesk Connect (доступ по ссылке: https://termidesk.ru/docs/).

Установка «Менеджеров рабочих мест»

Установка «Менеджеров рабочих мест» производится на два узла, работающих в режиме отказоустойчивой конфигурации, при которой оба узла активно обрабатывают трафик (конфигурация «Active - Active»), а отказ одного из них не нарушает работоспособность фермы Termidesk VDI.

Установка компонента на первый узел проводится в следующей последовательности:

- перемещается скопированный ранее каталог `termidesk-vdi` в каталог `/etc/opt/`:

```
sudo mv /home/user/termidesk-vdi /etc/opt/
```

При копировании конфигурации с эталонного узла на другие узлы параметр `NODE_NAME` в файле `/etc/opt/termidesk-vdi/termidesk.conf` также копируется. Этот параметр должен быть уникальным для каждого узла в ферме. На каждом узле необходимо изменить значение `NODE_NAME` на уникальное, либо удалить его, чтобы при следующем запуске инсталлятор сгенерировал новое значение автоматически. Изменить параметр можно вручную в файле или с помощью утилиты `termidesk-config`.

- создается файл `/etc/default/termidesk-vdi.local`:

```
sudo touch /etc/default/termidesk-vdi.local
```

- в созданном файле указываются каталоги расположения конфигурационного файла и шаблонов настройки регистрации событий и журналирования:

```
ETC='/etc/opt/termidesk-vdi'

TEMPLATES_DIR='/etc/opt/termidesk-vdi/templates'
```

- редактируется файл `/etc/opt/termidesk-vdi/termidesk.conf`, параметру `NODE_ROLES` присваивается значение `CELERYMAN`;
- устанавливается пакет `termidesk-vdi`:

```
sudo apt -y install termidesk-vdi
```

Где:

`-y` - ключ для пропуска подтверждения установки.

В результате установки пакета `termidesk-vdi` на узле будут запущены службы `termidesk-celery-beat`, `termidesk-celery-worker`.

Установка второго узла с «Менеджером рабочих мест» выполняется по аналогии с первым.

Установка «Балансировщиков нагрузки»

Подробные сведения по установке «Балансировщика нагрузки» приведены в документации Termidesk Connect (доступ по ссылке: https://termidesk.ru/docs/).

При отсутствии полной лицензии на Termidesk Connect допускается использование сторонних балансировщиков нагрузки.

Действия после стандартной распределенной установки

Настройка «Балансировщика нагрузки» приведена в документации Termidesk Connect (доступ по ссылке: https://termidesk.ru/docs/).

Если в инфраструктуре Termidesk VDI будет использоваться портал «Агрегатор» («Агрегатор администратора» и/или «Агрегатор пользователя»), нужно обязательно задать на узле компонента «Универсальный диспетчер» («Портал пользователя» или «Портал универсальный») сертификат для расшифровки JWT-токена. Сертификат может быть задан через файл `/etc/opt/termidesk-vdi/termidesk.conf` (параметры `AGGREGATOR_JWT_SSL_CERT` и `AGGREGATOR_JWT_SSL_CERT_SECOND`) или через утилиту `termidesk-config`.

После установки параметры могут быть изменены:

- через файл `termidesk.conf`;
- через утилиту `termidesk-config`.

Установка в режиме ЗПС

Замкнутая программная среда (ЗПС) является средством повышения безопасности ОС путем контроля целостности (неизменности) файлов.

Механизм контроля реализован в виде невыгружаемого модуля ядра ОС Astra Linux Special Edition (модуль `digsig_verif`), выполняющего проверку электронной цифровой подписи файлов (ЭЦП).

Перед установкой компонентов Termidesk VDI необходимо установить пакет `termidesk-digsig-keys`, для этого:

- подключить репозиторий Termidesk VDI или получить отдельный пакет `termidesk-digsig-keys` из репозитория;
- выполнить установку с использованием репозитория:

```
sudo apt -y install termidesk-digsig-keys
```

- либо выполнить установку из `deb`-пакета:

```
sudo apt install -y /home/user/termidesk-digsig-keys-XXXXXX_amd64.deb
```

где:

`-y` - ключ для пропуска подтверждения установки;

`/home/user/termidesk-digsig-keys-XXXXXX_amd64.deb` - расположение пакета `termidesk-digsig-keys-XXXXXX_amd64.deb`.

- перезагрузить ОС:

```
sudo reboot
```

- выполнить установку компонента Termidesk VDI.

Для ЗПС может быть активирован режим проверки встроенной ЭЦП в расширенных атрибутах (`DIGSIG_XATTR_MODE`). В этом случае потребуется подписать файлы, которые будут проходить проверку, имеющимися в организации ключами. Информация о процессе подписи и активации механизма проверки встроенной ЭЦП в расширенных атрибутах приведена в справочном центре Astra Linux: https://wiki.astralinux.ru/pages/viewpage.action?pageId=41190634.

Постановка Termidesk VDI на контроль целостности

После установки и настройки Termidesk VDI необходимо поставить его на контроль целостности. В подразделе приведена процедура для компонентов «Универсальный диспетчер» и «Менеджер рабочих мест».

Для контроля целостности используются встроенные в ОС Astra Linux Special Edition программные средства на основе `Another File Integrity Checker`, представленного пакетом `afick`.

Настройка регламентного контроля целостности выполняется в конфигурационном файле

/etc/afick.conf.

Настройку следует производить только после окончательного внедрения Termidesk VDI, поскольку с файлов конфигурации и исполняемых файлов будут сняты эталонные контрольные суммы.

Для постановки на контроль целостности компонента «Универсальный диспетчер» необходимо добавить в конфигурационный файл /etc/afick.conf строки:

```
/etc/default/termidesk-vdi PARSEC
/etc/logrotate.d/termidesk.conf PARSEC
/etc/opt/termidesk-vdi PARSEC
/etc/systemd/system/multi-user.target.wants/termidesk-vdi.service PARSEC
/opt/termidesk PARSEC
/usr/lib/systemd/system/termidesk-celery-beat.service PARSEC
/usr/lib/systemd/system/termidesk-celery-worker.service PARSEC
/usr/lib/systemd/system/termidesk-vdi.service PARSEC
/usr/lib/udev/rules.d/99-termidesk-vdi.rules PARSEC
/usr/share/doc/termidesk-vdi PARSEC
/var/opt/termidesk-vdi PARSEC

#Репозиторий Termidesk
/var/repos/ PARSEC
```

Для постановки на контроль целостности компонента «Менеджер рабочих мест» необходимо добавить в конфигурационный файл /etc/afick.conf следующие строки:

```
/etc/default/termidesk-vdi PARSEC
/etc/logrotate.d/termidesk.conf PARSEC
/etc/opt/termidesk-vdi PARSEC
/etc/systemd/system/multi-user.target.wants/termidesk-celery-beat.service PARSEC
/etc/systemd/system/multi-user.target.wants/termidesk-celery-worker.service PARSEC
/opt/termidesk PARSEC
/usr/lib/systemd/system/termidesk-celery-beat.service PARSEC
/usr/lib/systemd/system/termidesk-celery-worker.service PARSEC
/usr/lib/systemd/system/termidesk-vdi.service PARSEC
/usr/lib/udev/rules.d/99-termidesk-vdi.rules PARSEC
/usr/share/doc/termidesk-vdi PARSEC
/var/opt/termidesk-vdi PARSEC

#Репозиторий Termidesk
/var/repos/ PARSEC
```

Для снятия эталонных значений контрольных сумм используется команда:

```
afick -i
```

Для проверки соответствия контрольных сумм эталонным значениям автоматически создаются задания в системном планировщике заданий `cron`.

Для ручной проверки соответствия контрольных сумм используется команда:

```
afick -k
```

В случае отсутствия по какой-либо причине исполняемых фалов `*.pyc`, они будут повторно сгенерированы при перезапуске сервера Python. В этом случае нужно повторно проинициализировать средство регламентного контроля целостности `afick`.

Комплексное обновление Termidesk

Начиная с Termidesk VDI версии 6.1 компонент «Шлюз» (пакет `termidesk-gateway`) не входит в основную поставку. Для замены «Шлюза» следует использовать программу для электронной вычислительной машины «Балансировщик нагрузки Термидеск Коннект» (Termidesk Connect).

Инструкции по установке и настройке доступны по ссылкам: Инструкция по настройке Шлюза для Termidesk VDI (первый способ), Инструкция по настройке Шлюза для Termidesk VDI (второй способ, единая точка входа Termidesk VDI).

Особенности:

- для реализации функционала «Шлюза» используется лицензия Termidesk Connect Basic;
- для реализации функционала балансировщика используется лицензия Termidesk Connect. При отсутствии лицензии допускается использование сторонних балансировщиков нагрузки.

Описание применимо к ферме Termidesk VDI.

Комплексное обновление подразумевает, что компоненты «Универсальный диспетчер», «Менеджер рабочих мест» были установлены на одном узле, и ранее при установке были выбраны роли:

- «Портал администратора»;
- «Портал пользователя» (опционально);
- «Менеджер рабочих мест».

Обновление Termidesk VDI должно осуществляться с соблюдением условий:

- обновление выполняется последовательно, с установкой промежуточных версий релизов. Например, если сейчас установлена версия 6.0, то порядок обновления до 6.1 будет следующим: 6.0 - 6.0.2 - 6.1 - 6.1.1 - 7.0;
- обновление выполняется операцией установки поверх предыдущей версии. В противном случае, если ранее Termidesk VDI был удален без удаления БД, при повторной установке может возникнуть ряд ошибок;
- после начала процедуры обновления запрещается производить операции удаления объектов на «Порталах» с предыдущими версиями

Termidesk VDI.

Если после удаления Termidesk VDI (удаление БД при этом не производилось) возникла необходимость повторной установки программного комплекса, то после инсталляции может понадобиться снова ввести данные для доступа (пароль, токен доступа) в поставщике ресурсов.

Если в файлы запуска Termidesk VDI вручную были внесены какие-либо изменения, то эти изменения при обновлении не сохраняются.

Перед любым обновлением Termidesk VDI рекомендуется выполнить резервное копирование БД:

- остановить службы Termidesk VDI:

```
sudo systemctl stop termidesk-vdi termidesk-celery-beat termidesk-celery-worker
```

- выполнить резервное копирование БД:

```
pg_dump -d <наименование БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь> -W >
<имя_файла_для_сохранения_БД.sql>
```

Где:

`-d <наименование БД>` - имя БД. При стандартных настройках используется имя `termidesk`;

`-h <IP-адрес_хоста>` - IP-адрес узла, где расположена БД. Если БД устанавливалась локально, нужно указать `localhost`;

`-p <порт>` - порт для подключения к БД. При стандартных настройках используется `5432`;

`-U <пользователь>` - имя пользователя для подключения. При стандартных настройках используется имя `termidesk`;

`-W` - запрос пароля для подключения к БД. При стандартных настройках при появлении запроса нужно указать `ksedimret`;

`<имя_файла_для_сохранения_БД.sql>` - имя и формат файла (`sql`) для сохранения БД.

Для комплексного обновления Termidesk VDI нужно:

- убедиться, что службы Termidesk VDI были ранее остановлены;
- удалить кеш файла ответов `debconf` командами:

```
sudo rm -f /var/cache/debconf/config.dat
sudo rm -f /var/cache/debconf/config.dat-old
```

где:

`-f` - ключ игнорирования несуществующих файлов;

- подключить репозиторий Termidesk VDI;
- если ОС Astra Linux Special Edition используется в более защищенном режиме, например, «Смоленск», то:
  - для пользователя `termideskdb` (по умолчанию, создается на этапе настройки СУБД) назначить классификационную метку:

    ```
    sudo pdpl-user -i 0 termideskdb
    ```

  - предоставить пользователю `termideskdb` права на чтение файла, содержащего классификационную метку:

    ```
    sudo setfacl -m u:postgres:r /etc/parsec/macdb/$(id -u termideskdb)
    ```

  - создать системного пользователя `termideskdb` (имя должно совпадать с именем пользователя в БД):

    ```
    sudo useradd -M termideskdb -s /usr/sbin/nologin -d /home/termideskdb
    ```

- выполнить обновление:

```
sudo apt install -y termidesk-vdi
```

где:

`-y` - ключ для пропуска подтверждения установки;

- в диалогах ввода параметров подключения к СУБД и RabbitMQ нажать экранную кнопку **[OK]**;
- в диалоге выбора ролей Termidesk VDI нажать экранную кнопку **[OK]**;

Диалоги настройки параметров отображаются в том случае, если ранее они не были заданы.

Если нужно выполнить обновление без подключения репозитория (при наличии `deb` -пакета) следует выполнить:

```
sudo apt install -y <путь к deb-пакету>
```

В случае, если при обновлении появляется сообщение о неразрешенных зависимостях, следует выполнить:

```
sudo apt install -f
```

Где:

`-f` - ключ, указывающий, что нужно исправить зависимости пакетов.

После завершения обновления нужно:

- проверить состояние служб Termidesk VDI:

```
sudo systemctl -a | grep termidesk
```

где:

`-a` - ключ для вывода списка служб;

`grep` - утилита для поиска текста в выводе предыдущей команды;

- проверить доступность веб-интерфейса Termidesk VDI.

В процессе обновления будет выполнена настройка для работы в режиме мандатного контроля целостности и мандатного разграничения доступа:

- установлена метка `0` для пользователя `termidesk` и права на чтение файла с меткой пользователю `postgres`, если такой есть в ОС и метка ещё не устанавливалась. Если метка ранее была установлена, то она не изменится и не сбросится, права на файл с меткой не будут установлены;
- установлена метка `0` для пользователя, подключающегося к СУБД, и права на чтение файла с меткой пользователю `postgres`, если такой есть в ОС и метка ещё не устанавливалась. Если метка ранее была установлена, то она не изменится и не сбросится, права на файл с меткой не будут установлены.

Обновление для распределенной конфигурации установки

Общая концепция обновления

Описание применимо к ферме Termidesk VDI, установленной в распределенной конфигурации. Общая последовательность действий приведена на рисунке (см. рисунок Последовательность обновления распределенной конфигурации фермы Termidesk VDI).

Если в инфраструктуре Termidesk VDI используется портал «Агрегатор», то процесс обновления нужно начинать с него.

Во время обновления распределенной или отказоустойчивой конфигурации установки:

- изменение политик нужно проводить после обновления всех узлов Termidesk VDI;
- изменение системных параметров нужно проводить после обновления всех узлов Termidesk VDI.

Обновление Termidesk VDI должно осуществляться с соблюдением условий:

- обновление выполняется последовательно, с установкой промежуточных версий релизов. Например, если сейчас установлена версия 6.0, то порядок обновления до 7.0 будет следующим: 6.0 - 6.0.2 - 6.1 - 6.1.1 - 7.0;
- обновление выполняется операцией установки поверх предыдущей версии. В противном случае, если ранее Termidesk VDI был удален без удаления БД, при повторной установке может возникнуть ряд ошибок;
- после начала процедуры обновления запрещается производить

операции удаления объектов на «Порталах» с предыдущими версиями Termidesk VDI.

Во время обновления возможна временная неработоспособность функции автоматического входа пользователя в гостевую ОС ВМ, пока не будет обновлен последний узел с «Универсальным диспетчером».

Начиная с Termidesk VDI версии 6.1 компонент «Шлюз» (пакет `termidesk-gateway`) не входит в основную поставку. Для замены «Шлюза» следует использовать программу для электронной вычислительной машины «Балансировщик нагрузки Термидеск Коннект» (Termidesk Connect).

Инструкции по установке и настройке доступны по ссылкам: Инструкция по настройке Шлюза для Termidesk VDI (первый способ), Инструкция по настройке Шлюза для Termidesk VDI (второй способ, единая точка входа Termidesk VDI).

Особенности:

- для реализации функционала «Шлюза» используется лицензия Termidesk Connect Basic;
- для реализации функционала балансировщика используется лицензия Termidesk Connect. При отсутствии лицензии допускается использование сторонних балансировщиков нагрузки.

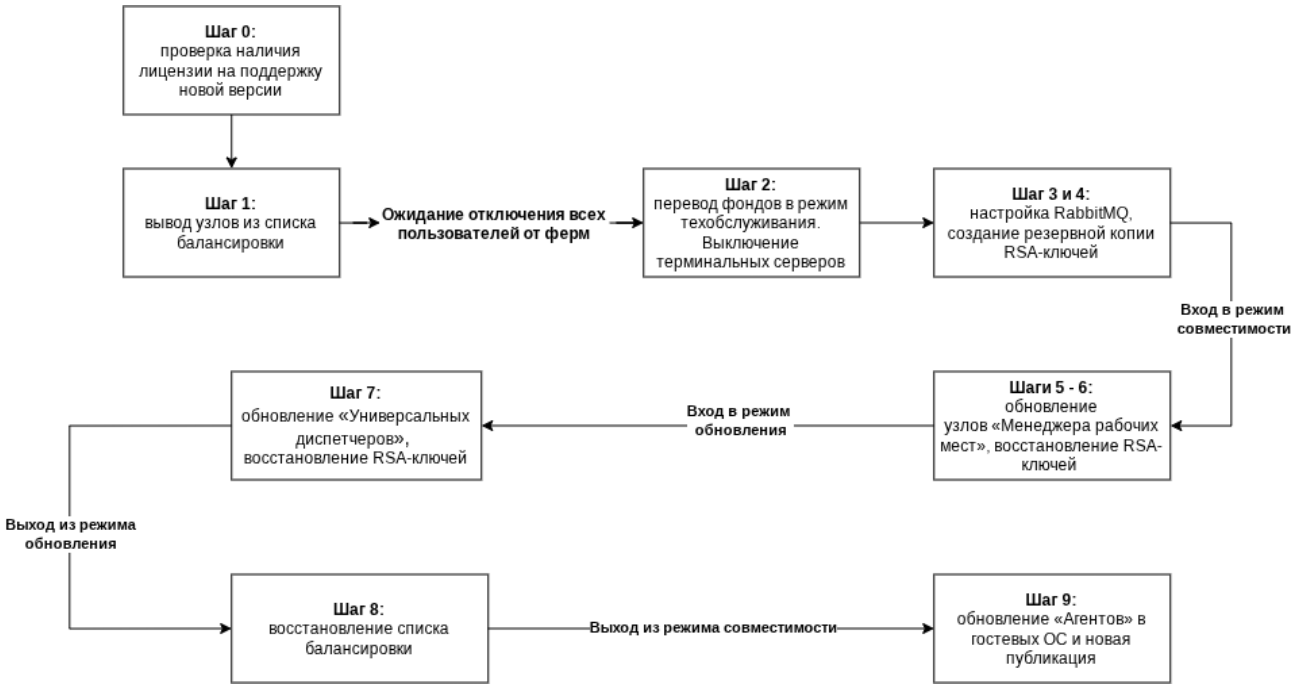


Рисунок 23. Последовательность обновления распределенной конфигурации фермы Termidesk VDI

На схеме:

- режим совместимости - режим, характеризующийся отличием в версиях между любыми компонентами фермы Termidesk VDI;
- режим обновления - режим, характеризующийся наличием не обновленных «Универсальных диспетчеров» при уже обновленных записях БД. Становится ограничен в действиях «Портал администратора». Ферма Termidesk VDI при этом должна работать с теми записями БД, которые есть на момент входа в этот режим.

Если планируется добавить новый узел с «Универсальным диспетчером»,

то любой новый узел будет иметь свой IP-адрес (или FQDN). В этом случае все компоненты «Агента» должны получить новый адрес для регистрации в Termidesk VDI.

Если в файлы конфигурации и запуска Termidesk VDI (`/lib/systemd/system/termidesk-*`) вручную были внесены какие-либо изменения, то необходимо выполнить резервное копирование данных файлов, поскольку эти изменения при обновлении сбрасываются до значений по умолчанию.

Обновление выполняется с приостановкой обслуживания пользователей!

Последовательность обновления фермы Termidesk VDI, установленной в распределенной отказоустойчивой конфигурации:

- Шаг 0. Проверить наличие лицензии на поддержку новой версии Termidesk VDI;
- Шаг 1. На всех балансировщиках нагрузки, отвечающих за распределение подключений к «Шлюзам» и «Универсальным диспетчерам», из списка балансировки исключаются все узлы, кроме одного (или нескольких) резервных, чтобы сохранить работоспособность балансировщика. Это позволит избежать ошибки при перезапуске nginx из-за пустого `upstream`;
- Шаг 2. Все пользователи должны отключиться от фондов РМ. Нужно дождаться завершения работы пользователей. Затем:
  - через веб-интерфейс «Портал администратора» перевести все фонды РМ в режим техобслуживания;
  - выключить все терминальные серверы, которые были подключены в Termidesk VDI как поставщики ресурсов;
- Шаг 3. На сервер с СУБД, либо на отдельно выделенный сервер, устанавливается и настраивается компонент RabbitMQ в случае, если ранее RabbitMQ не был установлен;
- Шаг 4. Создается резервная копия RSA-ключей, расположенных в каталоге `/etc/opt/termidesk-vdi/wsproxy/`;
- Шаг 5. Обновляется первый узел «Менеджера рабочих мест». Запуск служб выполняется автоматически. На обновленном «Менеджере рабочих мест» восстанавливаются RSA-ключи из резервной копии, созданной на **Шаге 4**. В этом процессе автоматически будут обновлены записи в БД;
- Шаг 6. Обновляются оставшиеся «Менеджеры рабочих мест». На обновленном «Менеджере рабочих мест» восстанавливаются RSA-ключи из резервной копии, созданной на **Шаге 4**;
- Шаг 7. Последовательно (по одному за раз) обновляются все «Универсальные диспетчеры» («Портал администратора», «Портал пользователя», «Портал универсальный»). Запуск служб выполняется автоматически. На обновленных «Универсальных диспетчерах» восстанавливаются RSA-ключи из резервных копий, созданных на **Шаге 4**. Узлы перезагружается;
- Шаг 8. По завершении обновления **ВСЕХ** узлов список балансировки восстанавливается до исходного (все ранее исключенные узлы возвращаются в списки `upstream`). Проверяется доступность графического интерфейса Termidesk VDI сначала обращением на IP-адрес каждого из «Универсальных диспетчеров», затем обращением на IP-адрес балансировщика нагрузки;
- Шаг 9. После выполнения обновления узлов:
  - обновить компоненты в гостевых ОС РМ (в базовом ВРМ - «золотом образе» или в ОС терминального сервера) в соответствии с документацией на них:
    - «Агент виртуального рабочего места»;
    - «Агент виртуальных смарт-карт»;

- «Видеоагент»;
- «Сессионный агент»;
- STAL (если используется);
- TERA (если используется);

- выполнить новую публикацию в фондах РМ, если публикация применима к ним (для фондов с терминальными серверами публикация не выполняется).

Описание каждого шага приведено ниже.

Шаг 1. Редактирование конфигурации балансировщика нагрузки

Пример для балансировщика nginx:

- на балансировщике нагрузки открыть и отредактировать файл `/etc/nginx/sites-available/sampledomain.ru.conf`;
- в конфигурационном файле найти директивы `daas-upstream-ws` и `daas-upstream-nodes` с перечислением списка «Шлюзов» и «Универсальных диспетчеров»;
- закомментировать все узлы, кроме одного (или нескольких) резервных, чтобы сохранить работоспособность балансировщика. Например, можно оставить один узел в каждом списке `upstream` активным.

Здесь и далее примеры IP-адресов приведены в соответствии с RFC 5737. Указанные IP-адреса должны быть заменены на актуальные, используемые согласно схеме адресации, принятой в инфраструктуре организации.

Пример для списка балансировки до исключения:

```
upstream daas-upstream-ws {
 least_conn;
     server 192.0.2.30;
     server 192.0.2.31;
     server 192.0.2.32;
 }

upstream daas-upstream-nodes {
 least_conn;
     server 192.0.2.33;
     server 192.0.2.34;
     server 192.0.2.35;
 }
```

Для исключения всех узлов, кроме одного, файл приводится к виду (оставлен активным узел 192.0.2.30 в `daas-upstream-ws` и 192.0.2.33 в `daas-upstream-nodes`):

```
upstream daas-upstream-ws {
 least_conn;
     server 192.0.2.30;
     # server 192.0.2.31;
     # server 192.0.2.32;
 }
```

```
upstream daas-upstream-nodes {
 least_conn;
     server 192.0.2.33;
     # server 192.0.2.34;
     # server 192.0.2.35;
 }
```

После изменения файла перезапустить `nginx`:

```
sudo systemctl restart nginx
```

Убедиться, что перезапуск прошел успешно и ошибок нет. При необходимости проверить логи nginx.

Шаг 2. Перевод фондов РМ в режим техобслуживания

Для продолжения обновления нужно дождаться отключения пользователей от фондов РМ.

Затем:

- через веб-интерфейс «Портал администратора» перевести **все** фонды РМ в режим техобслуживания. Для этого перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Техобслуживание]** с выбором из выпадающего списка значения «Включить». Подтвердить включение режима;
- выключить каждый узел терминального сервера, который подключен к Termidesk VDI как поставщик ресурсов.

Шаг 3. Установка и настройка RabbitMQ

При отсутствии ранее установленного RabbitMQ выполняется его установка в соответствии с подразделом **Подготовка среды функционирования**.

Предполагается, что СУБД установлена на узле RabbitMQ. При использовании ОС Astra Linux Special Edition в более защищенном режиме, например, «Смоленск», потребуется выполнить дополнительную настройку:

- для пользователя БД назначить классификационную метку (в примере используется `termideskdb`, в более ранних версиях использовалось имя пользователя `termidesk`):

```
sudo pdpl-user -i 0 termideskdb
```

- предоставить пользователю `postgres` права на чтение файла, содержащего классификационную метку пользователя `termideskdb`, подключающегося к БД:

```
sudo setfacl -m u:postgres:r /etc/parsec/macdb/$(id -u termideskdb)
```

- создать системного пользователя `termideskdb` (имя должно совпадать с именем пользователя в БД):

```
sudo useradd -M termideskdb -s /usr/sbin/nologin -d /home/termideskdb
```

Шаг 4. Резервное копирование RSA-ключей

Выполнить резервное копирование RSA-ключей с одного из узлов «Универсального диспетчера». Резервные копии ключей можно скопировать, например, на другой сетевой узел командой:

```
sudo scp -r /etc/opt/termidesk-vdi/wsproxy
localuser@ipaddr_or_fqdn_host:/home/localuser/
```

Где:

`-r` - ключ для рекурсивной (со вложенными каталогами) передачи;

`localuser` - имя пользователя целевого узла;

`ipaddr_or_fqdn_host` - IP-адрес или FQDN целевого узла;

`/home/user` - путь, куда будет скопирован каталог.

Шаг 5. Обновление первого «Менеджера рабочих мест»

Перед запуском процедуры обновления нужно:

- отредактировать файл `/etc/opt/termidesk-vdi/termidesk.conf` и задать значение для параметра `METRICS_ACCESS_KEY`, если оно не задано. Рекомендуется использовать одинаковое значение параметра `METRICS_ACCESS_KEY` для всех «Менеджеров рабочих мест»;
- остановить службы Termidesk VDI:

```
sudo systemctl stop termidesk-celery-beat termidesk-celery-worker
```

- удалить кеш файла ответов `debconf` командами:

```
sudo rm -f /var/cache/debconf/config.dat
sudo rm -f /var/cache/debconf/config.dat-old
```

Для обновления «Менеджера рабочих мест»:

- обновить список пакетов и выполнить запуск файла установщика:

```
sudo apt update
sudo apt install termidesk-vdi
```

- в диалоговом окне псевдографического интерфейса инсталлятора выбрать режим работы ПО «Диспетчер».

После обновления выполнить копирование сохраненных ранее RSA-ключей на узел с

обновленным «Менеджером рабочих мест».

Шаг 6. Обновление оставшихся «Менеджеров рабочих мест»

Выполняется аналогично **Шагу 5**.

Шаг 7. Обновление «Универсальных диспетчеров»

Перед запуском процедуры обновления нужно:

- отредактировать файл `/etc/opt/termidesk-vdi/termidesk.conf` и задать значение для параметра `METRICS_ACCESS_KEY`, если оно не задано. Рекомендуется задать одинаковое значение параметра `METRICS_ACCESS_KEY` для всех узлов «Универсального диспетчера»;

  Корректировка файла `/etc/apache2/apache2.conf` при обновлении не производится.

- остановить службу Termidesk VDI:

```
sudo systemctl stop termidesk-vdi
```

- удалить кеш файла ответов `debconf` командами:

```
sudo rm -f /var/cache/debconf/config.dat
sudo rm -f /var/cache/debconf/config.dat-old
```

где:

`-f` - ключ игнорирования несуществующих файлов.

Для обновления «Универсального диспетчера»:

- обновить список пакетов и выполнить запуск файла установщика:

```
sudo apt update
sudo apt install termidesk-vdi
```

- в диалоговом окне псевдографического интерфейса инсталлятора выбирается режим работы «Диспетчер», роль «Портал администратора» и/или «Портал пользователя» в зависимости от ранее установленной роли.

Далее выполнить копирование сохраненных ранее RSA-ключей на узлы с обновленными «Универсальными диспетчерами».

Затем перезагрузить узлы:

```
sudo reboot
```

После загрузки узла проверить состояние служб:

```
sudo systemctl -a | grep termidesk
```

Где:

`-a` - ключ для вывода списка служб;

`grep` - утилита для поиска текста в выводе предыдущей команды.

Проверить доступность веб-порталов Termidesk VDI через веб-браузер.

Шаг 8. Восстановление конфигурации балансировщика нагрузки

По завершении обновления **ВСЕХ** узлов фермы Termidesk VDI список балансировки на **ВСЕХ** балансировщиках восстанавливается до исходного (все ранее исключенные узлы возвращаются в списки `upstream`).

Пример для балансировщика nginx:

- ранее закомментированные строки нужно раскомментировать;
- затем выполнить перезагрузку службы `nginx` на каждом балансировщике:

```
sudo systemctl restart nginx
```

Выполнить проверку доступности веб-портала Termidesk VDI через веб-браузер сначала обращением на IP-адрес каждого из «Универсальных диспетчеров» (или «Шлюзов»), затем обращением на IP-адрес балансировщика нагрузки.

Шаг 9. Обновление компонентов в ОС РМ и новая публикация

После выполнения обновления **ВСЕХ** узлов:

- обновляются компоненты в ОС РМ (в базовом ВРМ или в ОС терминального сервера) в соответствии с документацией на них:
  - «Агент виртуального рабочего места»;
  - «Агент виртуальных смарт-карт»;
  - «Видеоагент»;
  - «Сессионный агент»;
  - STAL (если используется);
  - TERA (если используется);
- выполняется новая публикация в фондах РМ, если публикация применима к ним.

Для фондов терминальных серверов публикация не выполняется: достаточно того, чтобы узел терминального сервера был включен.

Удаление Termidesk

Для удаления нужно:

- выполнить:

```
sudo apt purge termidesk-vdi
```

- удалить файлы, задающие переменные окружения:

```
sudo rm /etc/default/termidesk-vdi.local
sudo rm /etc/default/termidesk-vdi
```

Для удаления БД и роли пользователя следует выполнить следующие действия, строго соблюдая их последовательность:

- переключиться на пользователя `postgres` (через пользователя `root`):

```
sudo su postgres
```

- запустить терминальный клиент СУБД:

```
psql
```

- используя интерактивный интерфейс терминального клиента СУБД, удалить БД:

```
postgres=# DROP DATABASE termidesk;
```

- удалить роль пользователя БД:

```
postgres=# DROP ROLE termidesk;
```

- выйти из интерактивного интерфейса терминального клиента СУБД:

```
postgres=# \q
```

- выйти из сеанса пользователя `postgres`:

```
exit
```

- удалить оставшийся каталог с файлами, содержащими переменные для подключения к БД, сертификат и ключ:

Если для хранения конфигурационных файлов, журналов и шаблонов использовались каталоги, отличные от стандартных, нужно удалить их.

```
sudo rm -R /etc/opt/termidesk-vdi
```

где:

-R - ключ для рекурсивного действия. Будут удалены все вложенные подкаталоги.

Проверка работоспособности после установки

Termidesk VDI является работоспособным, если в результате перехода в веб-браузере по адресу https://localhost/ или https://127.0.0.1/ отобразилась страница входа в Termidesk VDI (см. рисунок Начальная веб-страница Termidesk VDI). Если страница сразу не отобразилась, следует подождать 10-15 секунд и обновить ее.

Указанные адреса используются в случае локальной установки. Если Termidesk VDI установлен на сервере, отличном от узла, на котором происходит проверка, необходимо вместо localhost или 127.0.0.1 использовать IP-адрес сервера Termidesk VDI.

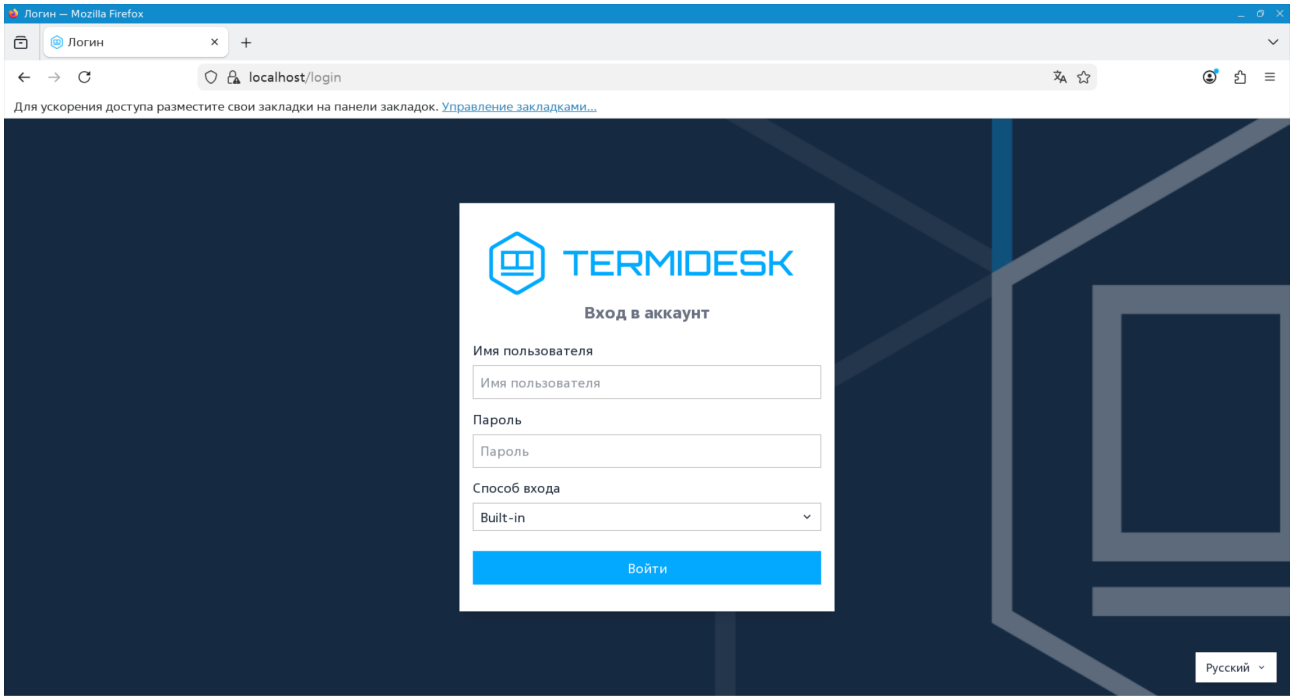


Рисунок 24. Начальная веб-страница Termidesk VDI

По умолчанию после установки вход в интерфейс управления Termidesk доступен только авторизованному пользователю ОС, являющемуся членом группы с идентификатором (GID) 1001.

В некоторых версиях ОС Astra Linux Special Edition указанной группе по умолчанию может быть назначен GID 1000 вместо 1001.

Группу можно поменять после установки через утилиту termidesk-config или командой:

```
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_config set --key
security.adminPamGroup --value ${ADMIN_GID}
```

Для входа в интерфейс управления в полях «Логин» и «Пароль» необходимо:

- указать идентификатор пользователя ОС и его пароль соответственно;

- затем нажать экранную кнопку **[Войти]**.

Проверка добавления ключа от репозитория производителя в ОС выполняется командой:

```
apt-key list
```

Проверка состояния компонентов выполняется командой:

```
systemctl status termidesk-vdi.service
```

Строка `Active` отображает состояние сервиса, где статус `active (running)` свидетельствует об успешном запуске Termidesk VDI.

ЛИЦЕНЗИРОВАНИЕ

Получение лицензионного ключа

Получение списка UUID узлов

Для получения лицензионного ключа нужно предварительно сформировать список системных UUID узлов Termidesk VDI, на которые будет сформирована лицензия.

Информация о системном UUID располагается на вкладке «Лицензия» графического интерфейса управления. Пример показан на рисунке (см. рисунок Расположение информации о системном UUID).

Для получения лицензионного ключа при распределенном варианте установки Termidesk VDI, необходимо предоставить в запросе системные UUID всех узлов с установленным компонентом «Универсальный диспетчер» и всех узлов с компонентом «Менеджер рабочих мест».

Для получения системных UUID узлов, установленных как в комплексном, так и в распределенном варианте, следует:

- открыть «Портал администратора» Termidesk VDI;
- перейти на вкладку «Лицензия» и нажать экранную кнопку **[Сохранить в файл сведения для лицензии]**;
- выбрать каталог и сохранить файл. По умолчанию он сохранится в формате `.tdsk`, который можно открыть простым текстовым редактором. Файл будет содержать список идентификаторов узлов инфраструктуры, совпадающий с тем, что перечислен в поле «UUID ноды» на странице «Инфраструктура - Диспетчеры подключений».

Информацию о системных UUID можно также получить из файла `/sys/devices/virtual/dmi/id/product_uuid`, выполнив на каждом узле с «Универсальным диспетчером»:

```
sudo cat /sys/devices/virtual/dmi/id/product_uuid
```

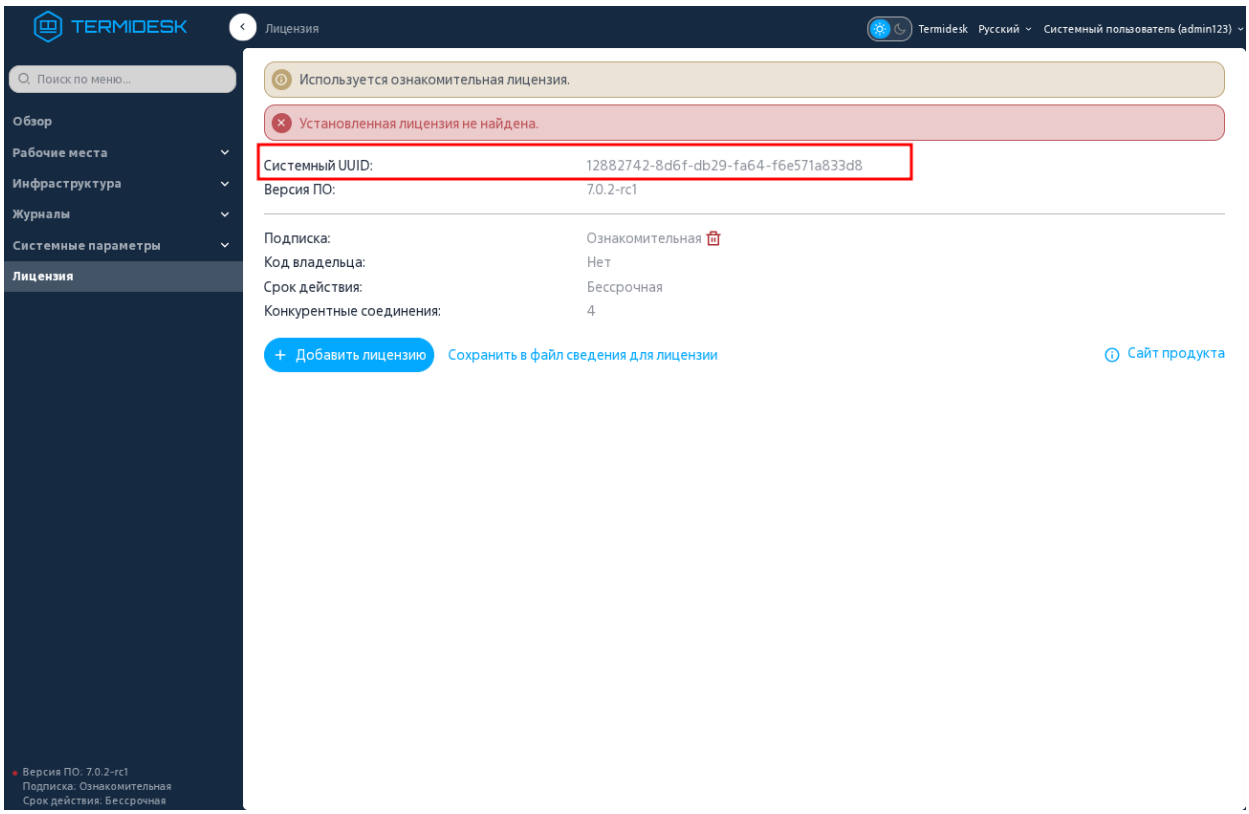


Рисунок 25. Расположение информации о системном UUID

Получение лицензионного ключа через личный кабинет

Получить лицензию Termidesk VDI можно через личный кабинет: https://lk.astra.ru/.

Для получения лицензии в личном кабинете:

- создать подписку, для этого перейти в раздел «Лицензии и сертификаты – Активация лицензий» и нажать экранную кнопку **[Создать подписку]** (см. рисунок Создание подписки);

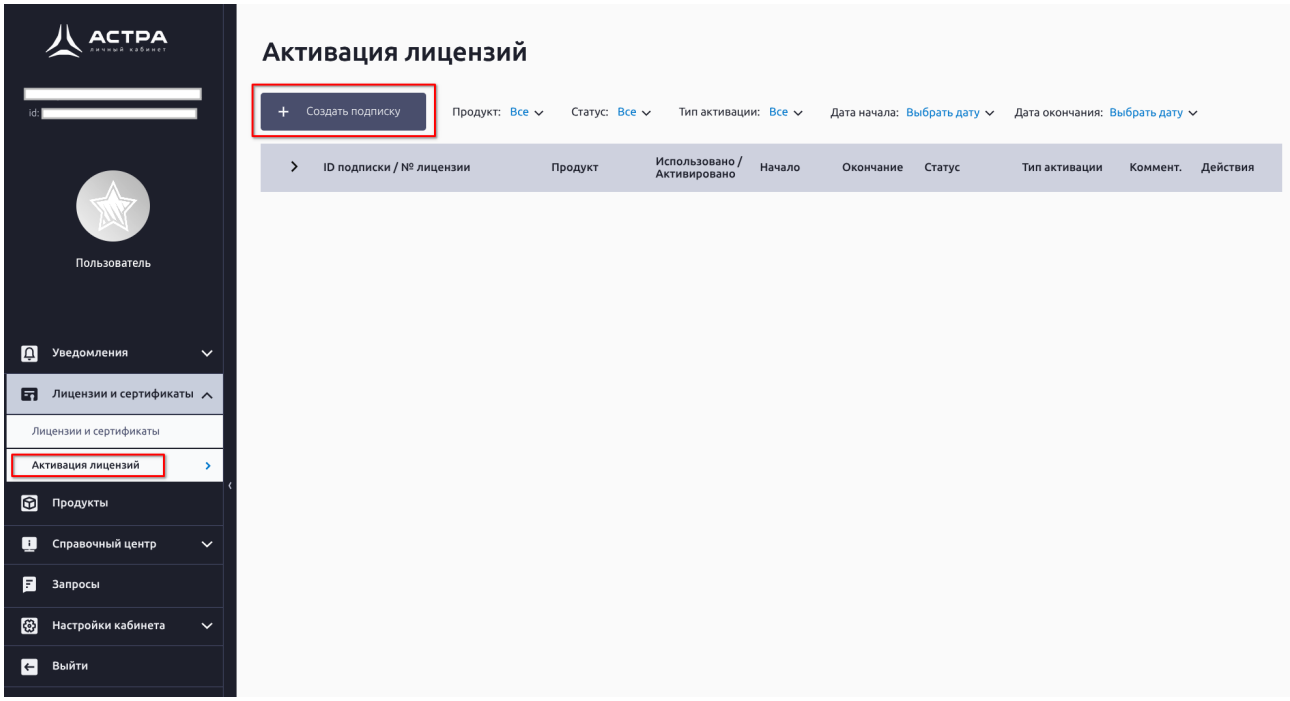


Рисунок 26. Создание подписки

- в открывшемся окне «Конструктор подписок» для выбранного продукта и номера лицензии в поле «Использовать» указать количество лицензий для активации, заполнить поле «Описание» (опционально), далее нажать экранную кнопку **[Собрать и активировать]** (см. рисунок Конструктор подписок);

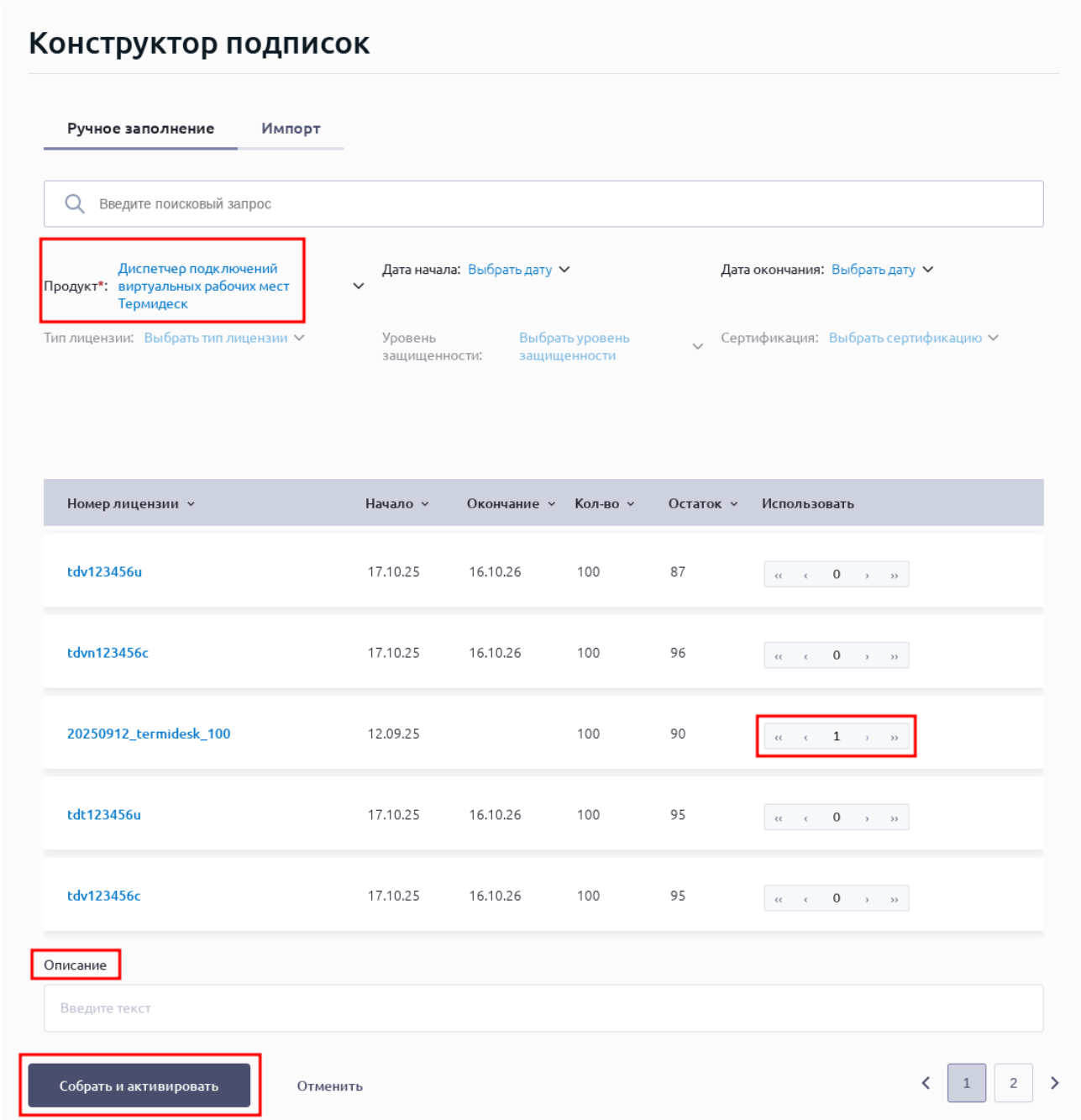


Рисунок 27. Конструктор подписок

- скачать манифест, для этого в области созданной подписки нажать экранную кнопку **[Скачать манифест]** (см. рисунок Скачивание манифеста);

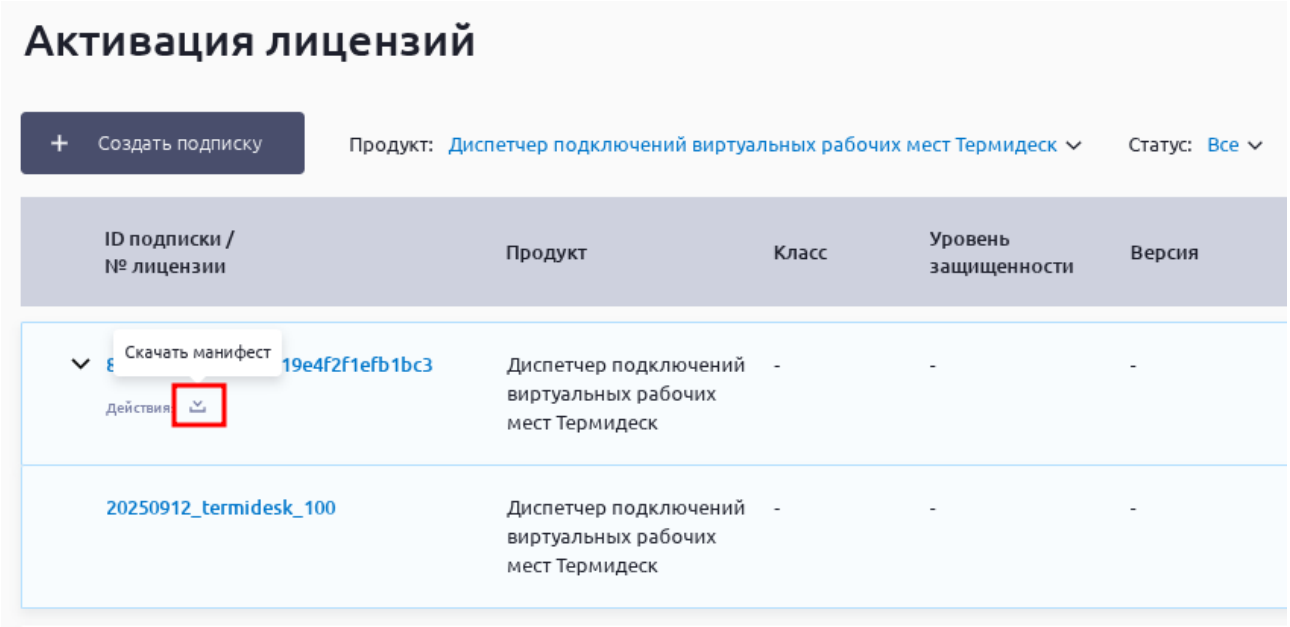


Рисунок 28. Скачивание манифеста

- в открывшемся окне «Скачать манифест» в поле ввода указать HWID устройства и нажать экранную кнопку **[Скачать]** (см. рисунок Формирование манифеста);

HWID устройства - это системный UUID, полученный ранее (см. подраздел **Получение списка UUID узлов**).

Если UUID несколько, то следует перечислить их через запятую.

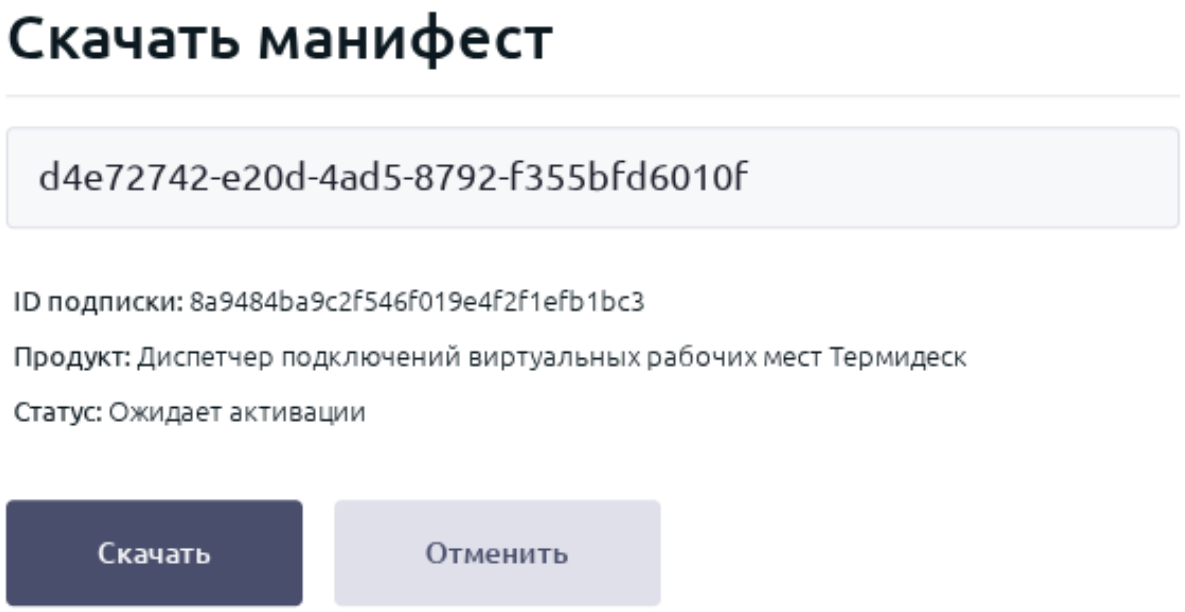


Рисунок 29. Формирование манифеста

Получение лицензионного ключа через сайт termidesk.ru

Этот вариант может использоваться, если возможность получения лицензионного ключа через личный кабинет отсутствует.

Для получения лицензионного ключа через сайт https://termidesk.ru/ нужно перейти по ссылке https://termidesk.ru/demonstration/ и выбрать пункт «Ключ активации». Далее:

- заполнить корректными данными следующие экранные поля:
  - «Имя»;
  - «Фамилия»;
  - «Телефон»;
  - «Место работы»;
  - «ИНН работодателя»;
  - «Корпоративная почта»;
  - «Укажите количество лицензий»;
  - «Системный UUID»;
- отметить согласие на обработку персональных данных;
- отправить данные, нажав экранную кнопку **[Отправить]**.

Ввод лицензии

Для добавления лицензионного ключа в Termidesk VDI в графическом интерфейсе управления следует перейти во вкладку «Лицензия» и нажать экранную кнопку **[+ Добавить лицензию]**. Затем:

- в открывшемся окне «Загрузка лицензии» нажать экранную кнопку **[Выберите файл]**;
- указать путь к файлу с лицензионным ключом и нажать экранную кнопку **[Загрузить]** (см. рисунок Окно добавления файла с лицензией);
- подтвердить перезапись лицензии в открывшемся окне «Подтверждение перезаписи лицензии», нажав экранную кнопку **[Загрузить]** (см. рисунок Окно подтверждения перезаписи лицензии).

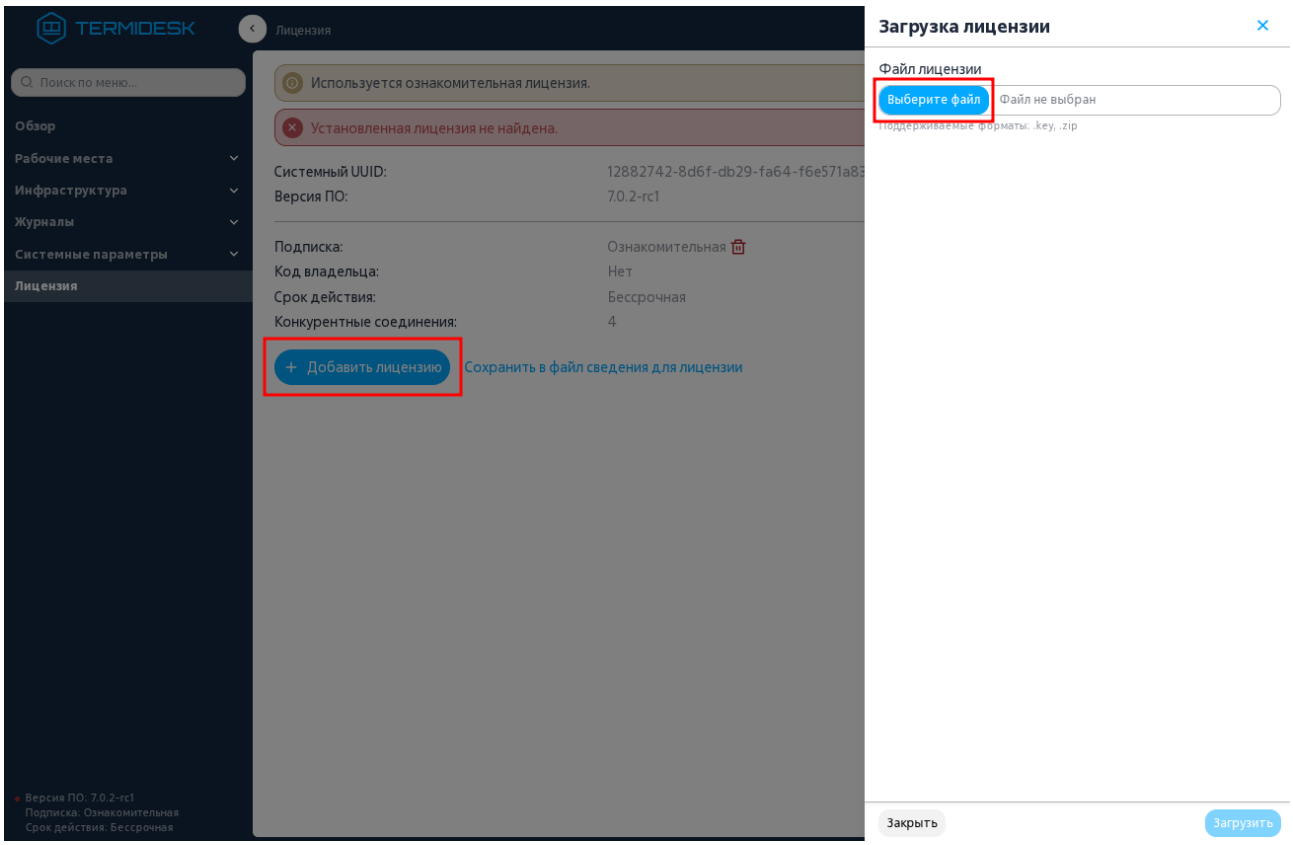


Рисунок 30. Окно добавления файла с лицензией

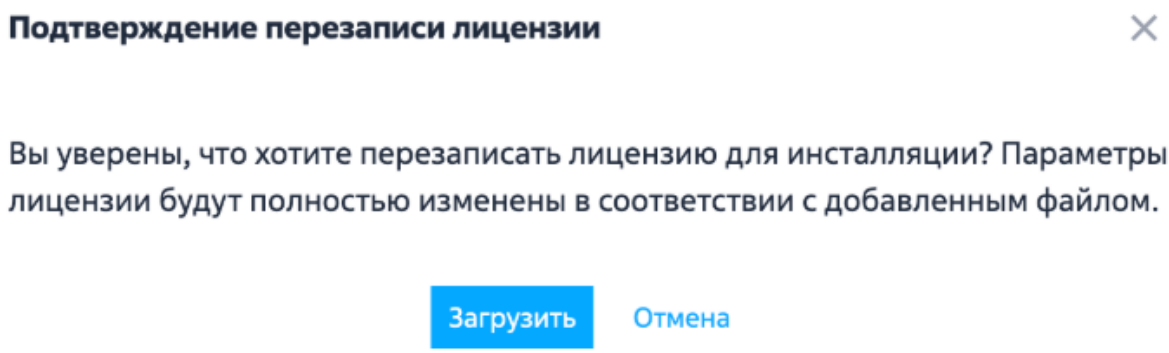


Рисунок 31. Окно подтверждения перезаписи лицензии

Редакции и типы лицензий Termidesk VDI

Компонент «Шлюз» (пакет `termidesk-gateway`) не входит в основную поставку. Для замены «Шлюза» следует использовать программу для электронной вычислительной машины «Балансировщик нагрузки Термидеск Коннект» (Termidesk Connect) с лицензией Termidesk Connect Basic (доступна для всех редакций Termidesk VDI). Документация Termidesk Connect доступна на сайте: https://termidesk.ru/docs/.

Для Termidesk VDI предусмотрены следующие обновленные редакции (см. таблицу Обновленные редакции Termidesk VDI):

- «Базовый»;
- «Стандартный»;

- «Расширенный».

Устаревшие редакции «Terminal» и «VDI» поддерживаются, если они были приобретены ранее. Возможности этих редакций представлены в таблице (см. таблицу Редакции «Terminal» и «VDI»).

В рамках доступных редакций существует поддержка двух типов лицензий:

- по пользователям - лицензия привязывается к пользователю системы и учитывает не только активных пользователей, но и всех, добавленных в Termidesk VDI. Любой один добавленный пользователь занимает одну лицензию, вне зависимости от числа активных сессий, при этом один встроенный пользователь (из домена аутентификации «Встроенный») отдельному лицензированию не подлежит и не учитывается при подсчете. При использовании метадомена аутентификации лицензия привязывается к учетной записи метапользователя. Учетные записи, привязанные к метапользователю из других доменов, отдельному лицензированию не подлежат;
- по конкурентным соединениям - лицензия привязывается к количеству пользователей, имеющих одновременные подключения. Количество сессий одного пользователя при этом не ограничено. Один встроенный пользователь (из домена аутентификации «Встроенный») отдельному лицензированию не подлежит и не учитывается при подсчете.

По срочности доступны лицензии следующих типов:

- срочные - лицензии с ограниченным временем действия. По истечении времени действия будет применена ознакомительная лицензия со всеми ее ограничениями;
- бессрочные - лицензии с неограниченным временем действия. Такие лицензии доступны в личном кабинете.

Количество пользователей для лицензии на странице «Обзор» в веб-интерфейсе «Портала администратора» может расходиться с суммарным количеством учетных записей в доменах аутентификации.

Дистрибутив Termidesk VDI распространяется с предустановленным лицензионным ключом, имеющим ограничение на 4 (четыре) конкурентных соединения для ознакомительных целей. Дистрибутив предназначен для проведения испытания, ознакомления или демонстрации его функциональных возможностей.

Дистрибутив для ознакомительных целей может предоставляться без заключения соответствующего договора на срок 90 (девяносто) календарных дней. Подробнее с условиями лицензионного соглашение с конечным пользователем можно ознакомиться на сайте: https://termidesk.ru/docs/eula.pdf.

Схема лицензирования по пользователям на примере:

- один пользователь с одним активным подключением - одно место из пула лицензии;
- один пользователь с двумя активными подключениями - одно место из пула лицензии;
- два пользователя с одним активным подключением у каждого - два места из пула лицензии;
- два пользователя с двумя активными подключениями у каждого - два места из пула лицензии;
- два пользователя с тремя активными подключениями у каждого - два места из пула лицензии;
- три пользователя без активных подключений - три места из пула лицензии;

- четыре пользователя, два из которых имеют три активных подключения у каждого - четыре места из пула лицензии.

Схема лицензирования по конкурентным соединениям на примере:

- один пользователь с одним активным подключением - одно место из пула лицензии;
- один пользователь с двумя активными подключениями - одно место из пула лицензии;
- два пользователя с одним активным подключением у каждого - два места из пула лицензии;
- два пользователя с двумя активными подключениями у каждого - два места из пула лицензии;
- два пользователя с тремя активными подключениями у каждого - два места из пула лицензии;
- три пользователя без активных подключений - нет занятых мест в пуле лицензии;
- четыре пользователя, два из которых имеют три активных подключения у каждого - два места из пула лицензии.

При использовании портала «Агрегатор» лицензии считаются в момент создания сессии на том узле «Универсального диспетчера», на котором она создалась, и расходуют лицензии того узла «Универсального диспетчера», к которому произошло подключение.

Таблица 6. Обновленные редакции Termidesk VDI

Возможности	Редакция «Базовый»	Редакция «Стандартный»	Редакция «Расширенный»
Компоненты			
Termidesk Client. Нативный клиент для подключений	Да	Да	Да
Termidesk Connect. Шлюз подключений (в лицензии Termidesk Connect Basic)	Да	Да	Да
Termidesk Live. Загрузка специализированного образа ОС и приложений по сети[1]	Нет	Да	Да
Termidesk Roaming Profiles. Перемещаемые пользовательские профили для ОС Linux	Нет	Да	Да
Termidesk Assistant. Интерактивная удаленная поддержка пользователей со стороны поддержки и администраторов	Нет	Да	Да
Ретранслятор. Мониторинг компонентов системы в формате Open Metrics	Нет	Да	Да
Агрегатор. Объединение ресурсов нескольких ферм в едином интерфейсе	Нет	Нет	Да

Возможности	Редакция «Базовый»	Редакция «Стандартный»	Редакция «Расширенный»
Программное обеспечение нагрузочного тестирования инфраструктуры Termidesk VDI	Нет	Нет	Да
Функционал			
Поддержка поставщиков услуг	MS RDS STAL (сервер терминалов Astra Linux)	MS RDS STAL (сервер терминалов Astra Linux) VMware VMmanager ПК СВ Брест zVirt	MS RDS STAL (сервер терминалов Astra Linux) VMware VMmanager ПК СВ Брест zVirt РЕД Виртуализация OpenStack
Поддержка клиентских ОС	Astra Linux и другие поддерживаемые ОС на базе Linux, Windows, MacOS		
Терминальный доступ к ВРМ (Windows, Linux)	Да	Да	Да
Терминальный доступ к приложениям (Windows, Linux)	Да	Да	Да
VDI доступ к ВРМ (Windows, Linux)	Нет	Да	Да
Подключение к фондам автономных машин (ФизПК, ВМ)	Да[2]	Да	Да
Метапоставщик – автоматическое создание фондов терминальных серверов (Windows Server, Astra Linux Server)	Нет	Да	Да
Балансировка подключений к терминальным серверам на основе их загрузки (CPU, RAM, HDD)	Нет	Да	Да
Планировщик – управление расписанием задач ВМ / фондов ВРМ	Нет	Да	Да
Подключение через HTML5-клиент	Нет	Да	Да
Поддержка протокола удаленного доступа TERA[3]	Нет	Да	Да

Возможности	Редакция «Базовый»	Редакция «Стандартный»	Редакция «Расширенный»
Поддержка технологии vGPU и протокола Loudplay	Нет	Нет	Да
Брендирование	Нет	Нет	Да
Безопасность			
Поддержка LDAP-совместимых доменов аутентификации	OpenLDAP ALD Pro FreeIPA MS AD		OpenLDAP ALD Pro FreeIPA MS AD АльтДомен Ред АДМ
Поддержка способов 2FA/MFA аутентификации	Токены и смарт-карты (Aladdin\RuToken)	Токены и смарт-карты (Aladdin\RuToken) RADIUS SAML OpenID Connect (OIDC)	
Поддержка единого входа через проброс учетных данных по защищенному каналу (Credential Passthrough)	Да	Да	Да
Поддержка сквозной аутентификации через билеты Kerberos	Нет	Да	Да
Поддержка mTLS	Нет	Нет	Да
Поддержка усиленной аутентификации ПО ИнфоКрипт Winnet или Vitamin	Нет	Нет	Да

Примечания:

[1] Компонент Termidesk Live переведён в режим ограниченной поддержки: обновления не выпускаются. Совместимость гарантируется с Termidesk VDI версии не выше 5.0.

[2] Использование автономных машин ограничено политикой лицензирования (для редакции «Базовый» допустимо добавлять не более 1 (одного) поставщика ресурсов «Автономная машина»): https://termidesk.ru/docs/license-agreement.pdf.

[3] Не реализовано в терминальных средах. После реализации будет доступен во всех редакциях.

Таблица 7. Редакции «Terminal» и «VDI»

Возможности	Редакция «Terminal»	Редакция «VDI»
Компоненты		
STAL. Сервер терминалов Astra Linux	Да	Да

Возможности	Редакция «Terminal»	Редакция «VDI»
Клиент	Да	Да
Сессионный агент	Да	Да
Менеджер рабочих мест	Да	Да
Агент виртуального рабочего места	Нет	Да
Termidesk Live	Нет	Да
Удаленный помощник	Нет	Да
Агрегатор	Нет	Да
Оркестратор	Нет	Да
Функционал		
Графическая панель управления с настраиваемыми правами доступа	Да	Да
Терминальные сессии ОС Microsoft Windows и Linux	Да	Да
Терминальный доступ к экрану приложений (для ОС Microsoft Windows и Linux)	Да	Да
Поддержка поставщиков ресурсов для терминальных серверов	Да	Да
Протокол удаленного доступа RDP	Да	Да
Отправка сообщений пользователям в сессию	Да	Да
Мониторинг	Да	Да
VDI-доступ для ОС Microsoft Windows и Linux	Да	Да
Собственный протокол удаленного доступа TERA	Нет	Да
Резервное копирование ВРМ с использованием платформы виртуализации	Нет	Да
Полные и связанные клоны	Нет	Да
Поддержка технологии vGPU	Нет	Да
Временные и постоянные ВРМ	Нет	Да
Планировщик (управление расписанием задач)	Нет	Да
Автоматическое формирование фондов ВРМ из шаблонов терминальных серверов под ОС Astra Linux Server и ОС Microsoft Windows Server (Метапоставщик) на платформе виртуализации	Нет	Да
Базовая балансировка нагрузки между терминальными серверами на основе сессий	Нет	Да
Интеллектуальная балансировка нагрузки между терминальными серверами на основе потребляемых вычислительных ресурсов	Нет	Да
Поддержка подключения к фондам автономных машин	Нет	Да
HTML5-клиент	Нет	Да
Нефункциональные характеристики		
Возможность установки сессионного агента на виртуальные машины	Нет	Да
Отказоустойчивость (избыточность) терминальных серверов	Нет	Да

Проверка сведений о лицензии

Для просмотра информации об используемой лицензии следует перейти в графический интерфейс управления во вкладку «Лицензия» и просмотреть сведения в следующих экранных полях:

В зависимости от типа лицензии состав полей может отличаться. Список ограничений не будет приведен, если используется редакция Termidesk VDI «Расширенный».

- «Подписка» - идентификатор лицензии;
- «Код владельца» - идентификатор владельца лицензии;Bpo
- «Владелец» - наименование организации, для которой сформирована лицензия;
- «Срок действия» - дата окончания действия лицензии;
- «Конкурентные соединения» - тип и размер пула лицензии;
- «Поставщики ресурсов» - список поставщиков ресурсов, доступных для установленного вида лицензии;
- «Транспорты» - список протоколов доставки, доступных для установленного вида лицензии;
- «Домены аутентификации» - список доменов аутентификации, доступных для установленного вида лицензии;
- «Параметры гостевых ОС» - список гостевых ОС, доступных для установленного вида лицензии.

За 30 дней до истечения срока лицензии будет показано предупреждение. Если новая лицензия не будет загружена, то будет использоваться ознакомительная версия.

Для удаления лицензии нужно воспользоваться графическим элементом . При удалении лицензии будет использоваться ознакомительная версия.

События, связанные лицензией и изменением лицензируемого количества подключений, записываются в таблицу БД `termidesk_cep_event`. Особенности:

- по умолчанию записи хранятся 30 дней, устаревшие записи (кроме событий о смене лицензии - такие события считаются постоянными и не подлежат удалению) очищаются периодической задачей раз в 24 часа;
- отчет о лицензиях можно просмотреть через API-запрос `/api/webui/license/history`;
- на основе событий об изменениях лицензируемого количества подключений рассчитывается статистика использования лицензий, просмотр которой доступен через API-запросы `/api/webui/server/license/stats/licensed_connections/{interval}`, `api/webui/server/license/stats/licensed_users/{interval}` (см. подраздел документа). Эта статистика также регистрируется в системном журнале («Журналы - Системные журналы»). Доступны разные значения интервала статистики:
  - по часам (`hourly`) за последние 7 дней с учетом часового пояса сервера;
  - по дням (`daily`) за последние 365 дней с учетом часового пояса сервера;
  - по месяцам (`monthly`) за весь период работы сервера.

НЕШТАТНЫЕ СИТУАЦИИ

Возможные неисправности при установке Termidesk VDI и способы их устранения приведены в таблице (см. таблицу Перечень возможных нештатных ситуаций).

Таблица 8. Перечень возможных нештатных ситуаций

Индикация	Описание	Возможное решение

Веб-интерфейс не отображается после установки	После установки веб-интерфейс не отображается, в журналах веб-сервера Apache присутствуют ошибки при доступе по адресу веб-интерфейса	Для исправления ситуации нужно:
		• проанализировать ошибки журнала Syslog;
		• проверить существование файла `termidesk.conf`;
		• проверить права доступа на файл `termidesk.conf`:
		`sudo -u termidesk test -r /etc/opt/termidesk-vdi/termidesk.conf && echo "Success" || echo "Error"`
		• если после выполнения команды вернулся ответ `Error`, то поменять права на каталог `/etc/opt/termidesk-vdi`, например:
		`sudo chmod 755 /etc/opt`
		`sudo chmod 755 /etc/opt/termidesk-vdi`

Предупреждение о некорректных параметрах локализации	При установке отображается диалог с сообщением: «The current session uses an invalid locale: LC_CTYPE="UTF-8"». Проблема возникает, если в системе некорректно заданы параметры локализации, например `LC_CTYPE=UTF-8`	Для исправления ситуации нужно:
		• прервать установку, нажав кнопку **[Abort]**;
		• проверить текущие параметры локализации с помощью команды `locale`;
		• если параметры заданы некорректно (например, `LC_CTYPE=UTF-8`), посмотреть список доступных значений в системе:
		`locale -a`
		• установить одно из доступных значений, например `C.UTF-8`:
		`export LC_CTYPE=C.UTF-8`
		• после исправления параметров локализации запустить установку заново

Индикация	Описание	Возможное решение

СУБД PostgreSQL не запускается после обновления ОС Astra Linux Special Edition	После обновления ОС Astra Linux Special Edition СУБД PostgreSQL может не запускаться, из-за чего не работают службы Termidesk (`termidesk-vdi`, `termidesk-celery-beat`, `termidesk-celery-worker`).
	
	В журнале службы СУБД PostgreSQL появляется сообщение: «Неверное значение для параметра "ac_audit_mode": "internal"».
	
	Параметр `ac_audit_mode` со значением `internal` больше не поддерживается в новых версиях ОС Astra Linux Special Edition
		Ситуация возникает при обновлении ОС Astra Linux Special Edition с установленной СУБД PostgreSQL из состава ОС. Ситуация не связана с работой Termidesk, однако может повлиять на процесс обновления фермы Termidesk VDI.
		
		Для восстановления работоспособности СУБД PostgreSQL необходимо:
		
		• в файле `/etc/postgresql/15/main/postgresql.conf` изменить значение параметра:
		
		`ac_audit_mode = default`
		
		• перезапустить СУБД PostgreSQL:
		
		`sudo systemctl restart postgresql`
		
		После успешного запуска СУБД PostgreSQL службы Termidesk запускаются штатно

Индикация	Описание	Возможное решение

После обновления брокера сообщений RabbitMQ не создаются очереди сообщений	После обновления брокера сообщений RabbitMQ очереди сообщений не создаются. В журнале брокера сообщений отображается ошибка: «operation queue.declare caused a connection exception internal_error: "Feature transient_nonexcl_queues is deprecated. By default, this feature is not permitted anymore."»	Ситуация возникает при использовании устаревших функций брокера сообщений RabbitMQ.
		
		Для восстановления работоспособности брокера сообщений RabbitMQ нужно:
		
		• отредактировать файл `/etc/rabbitmq/rabbitmq.conf`;
		• добавить строку с указанием устаревшей функции для использования обратной совместимости:
		
		`deprecated_features.permit.transient_nonexcl_queues = true`
		
		• перезапустить службу `rabbitmq-server`:
		
		`sudo systemctl restart rabbitmq-server`

Проблемы в работе задач «Менеджера рабочих мест»	В работе Termidesk VDI наблюдаются проблемы, при этом в журнале службы `termidesk-celery-worker` присутствует ошибка: «TimeoutError: The read operation timed out»	По умолчанию параметр `CELERY_TASK_TIME_LIMIT` имеет значение `0`, при котором время выполнения задач не ограничивается. Если задан ненулевой таймаут и его недостаточно для выполнения задач, значение следует увеличить. Чтобы полностью снять ограничение, нужно задать значение `0`. Например:
		
		`CELERY_TASK_TIME_LIMIT = 600`
		
		После изменения параметра нужно перезапустить службу `termidesk-celery-worker`:
		
		`sudo systemctl restart termidesk-celery-worker`

ТЕРМИНЫ

Компонент «Агент»

Самостоятельный компонент, отвечающий за контролируемую доставку РМ, взаимодействие с «Универсальным диспетчером» и «Менеджером рабочих мест».

Собирательное название для следующих компонентов Termidesk VDI:

- «Агент виртуального рабочего места»;
- «Агент узла виртуализации»;
- «Сессионный агент»;
- «Видеоагент»;
- «Агент виртуальных смарт-карт».

Компонент «Агент виртуальных смарт-карт»

Компонент Termidesk VDI. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление подключенных к пользовательской рабочей станции смарт-карт в ВРМ

Компонент «Агент виртуального рабочего места»

Компонент Termidesk VDI. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет взаимодействие с «Универсальным диспетчером», конфигурирует ВРМ, фиксирует действия пользователя, реализует передачу управляющих сообщений

Компонент «Агент узла виртуализации»

Компонент Termidesk VDI. Устанавливается на узел виртуализации, взаимодействует с гипервизором через модуль `libvirt`

Базовое виртуальное рабочее место

Также: золотой образ, базовый образ. Подразумевает собой образ диска ВМ с предустановленным прикладным ПО и установленным «Агентом виртуального рабочего места». Этот образ далее будет использоваться для создания ВРМ для пользователей

Балансировщик нагрузки

Самостоятельный компонент, отвечающий за распределение нагрузки на множество «Универсальных диспетчеров» и «Шлюзов»

Компонент «Видеоагент»

Компонент Termidesk VDI. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление видеокамеры с пользовательской рабочей станции в ВРМ

Виртуальное рабочее место

Развернутая на ВМ ОС с установленным «Агентом виртуального рабочего места» и необходимым прикладным ПО. Подключение к ВРМ происходит через протоколы удаленного доступа

Рабочее место

Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа. Под РМ подразумеваются как ВРМ, так и терминальный доступ или доступ к опубликованным на терминальном сервере приложениям

Гостевая ОС

ОС, функционирующая на ВМ

Домен аутентификации

Способ проверки субъектов и их полномочий

Компонент «Менеджер рабочих мест»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за взаимодействие с поставщиком ресурсов и управления жизненным циклом РМ, включая создание, настройку, запуск, отключение и удаление. Является обработчиком фоновых задач. Устанавливается из пакета `termidesk-vdi`. Наименование

служб после установки: `termidesk-celery-beat.service` и `termidesk-celery-worker.service`

Компонент «Оркестратор»

Компонент Termidesk VDI. Самостоятельный компонент, отвечающий за согласованную работу всех компонентов программного комплекса при децентрализованном развертывании, для нужд отказоустойчивости и комплексирования с облачными службами

Поставщик ресурсов

ОС, платформа виртуализации или терминальный сервер (MS RDS/STAL), предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов РМ

Протокол доставки

Поддерживаемый в Termidesk VDI протокол удаленного доступа к РМ

Связанный клон

Способ организации ВРМ на основе единого образа с возможностью экономии дискового пространства за счет технологии «копирование при записи» и ускорения операций возврата к базовому состоянию, установки дополнительного ПО и обновлений

Компонент «Сессионный агент»

Компонент Termidesk VDI. Устанавливается на терминальный сервер (MS RDS/STAL), активирует возможность множественного доступа пользователей к удаленным рабочим столам и приложениям

Компонент «Универсальный диспетчер»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им РМ и контроля доставки РМ. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-vdi.service `

Фонд рабочих мест

Совокупность подготовленных РМ для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей

Шаблон рабочего места

Параметры конфигурации РМ для использования в фонде РМ

Компонент «Шлюз»

Самостоятельный компонент, отвечающий за туннелирование протоколов доставки, использующих транспортный протокол TCP

Компонент «Сервер терминалов Astra Linux»

Компонент Termidesk VDI. Также: STAL. Обеспечивает подключение пользовательских рабочих станций к РМ с ОС Astra Linux Special Edition через сеанс удаленного терминала

Портал администратора

Предоставляет веб-интерфейс для управления Termidesk VDI и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API

Портал пользователя

Предоставляет пользовательский веб-интерфейс Termidesk VDI (без доступа к функциям управления) и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API

Портал универсальный

Предоставляет функции обоих вариантов - и «Портала администратора», и «Портала пользователя». При этом активируется доступ ко всем модулям документации по командам REST API, предоставляемым интерфейсом Swagger

Ключ

Применяется в контексте файла, не опции в команде. Последовательность псевдослучайных чисел, сгенерированная особым образом

Сертификат

Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу

Комплексная установка

Установка основных компонентов Termidesk VDI на одном узле

Распределенная установка

Установка основных компонентов Termidesk VDI на разных узлах

СОКРАЩЕНИЯ

БД	База данных
ВМ	Виртуальная машина
ВРМ	Виртуальное рабочее место
ЗПС	Замкнутая программная среда
КД	Контроллер домена
ОС	Операционная система
ПК СВ Брест	Программный комплекс «Средства виртуализации «Брест»
ПО	Программное обеспечение
РМ	Рабочее место
СУБД	Система управления базами данных
ЦС	Центр сертификации
ЭЦП	Электронная цифровая подпись
API	Application Programming Interface (программный интерфейс приложения)
DHCP	Dynamic Host Configuration Protocol (протокол назначения сетевого адреса)
DNS	Domain Name System (система доменных имен)
FQDN	Fully Qualified Domain Name (полностью определенное имя домена)
GID	Group Identification Data (идентификатор группы)
HTML	Hypertext Markup Language (язык гипертекстовой разметки)

HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
ID	Identification Data (идентификатор)
IP	Internet Protocol (межсетевой протокол)
JWT	JSON Web Token (открытый стандарт для создания токенов доступа)
KVM	Kernel Virtual Machine (виртуальная машина на основе ядра, технология аппаратной виртуализации)
LDAP	Lightweight Directory Access Protocol (легковесный протокол доступа к службам каталогов)
MAC	Media Access Control (уникальный идентификатор сетевого устройства)
MS AD	Microsoft Acive Directory (служба каталогов Microsoft)
MS RDS	Remote Desktop Services (службы удаленного рабочего стола Microsoft)
MS RDSH	Remote Desktop Session Host (хост сеансов удаленных рабочих столов)
mTLS	Multiplexed Transport Layer Security (протокол, основанный на TLS с усиленной безопасностью)
NTP	Network Time Proetwork Time Protocol (протокол сетевого времени)
OU	Organizational Unit (организационная единица)
QEMU	Quick Emulator (средства эмуляции аппаратного обеспечения)
RA	Remote Assistant (компонент «Удаленный помощник»)
RADIUS	Remote Authentication Dial-In User Service (протокол, предоставляющий функции аутентификации, авторизации и учета)
RDP	Remote Desktop Protocol (протокол удаленного рабочего стола)
REDIS	REmote DIctionary Service (резидентная СУБД)
REST	Representational State Transfer (программная архитектура, определяющая условия работы API)
RFC	Request for Comments (рабочее предложение Интернет)
RSA	Rivest, Shamir and Adleman (криптографический алгоритм с открытым ключом)
SPICE	Simple Protocol for Independent Computing Environments (простой протокол для независимой вычислительной среды)
SSL	Secure Sockets Layer (криптографический протокол)
STAL	Terminal Server Astra Linux (компонент «Сервер терминалов Astra Linux»)
TCP	Transmission Control Protocol (протокол управления передачей)
TERA	Termidesk Remote Access protocol (протокол удаленного доступа разработкиООО «УВЕОН»)

TLS	Transport Layer Security (протокол защиты транспортного уровня)
URL	Uniform Resource Locator (унифицированный указатель ресурса)
UUID	Unique User Identifier (уникальный идентификатор пользователя)
VDI	Virtual Desktop Infarsticture (инфраструктура виртуальных рабочих столов)
vGPU	Virtual Graphics Processing Unit (виртуальный графический процессор)
VRRP	Virtual Redundancy Routing Protocol (сетевой протокол виртуального резервирования маршрутизаторов, предназначенный для увеличения доступности)

СЛЕТ.10001-01 90 02. РУКОВОДСТВО АДМИНИСТРАТОРА. НАСТРОЙКА ПРОГРАММНОГО КОМПЛЕКСА

ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ

Назначение документа

Настоящий документ является второй частью руководства администратора на программный комплекс «Диспетчер подключений виртуальных рабочих мест Termidesk» (далее - Termidesk VDI, Termidesk VDI). Документ предназначен для администраторов системы и сети.

Во второй части руководства приведена настройка Termidesk VDI, рассмотрены взаимодействие компонентов, разграничение функций по администрированию. Для того чтобы получить информацию об установке программного комплекса, необходимо обратиться к первой части руководства администратора - СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса».

Типографские соглашения

Приняты следующие типографские соглашения:

- `моноширинный шрифт` – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk VDI, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

КОМПОНЕНТЫ И ИХ ВЗАИМОДЕЙСТВИЕ

Схема взаимодействия компонентов и приложений

Схема взаимодействия компонентов Termidesk VDI и приложений представлена на рисунке (см. рисунок Схема взаимодействия компонентов и приложений).

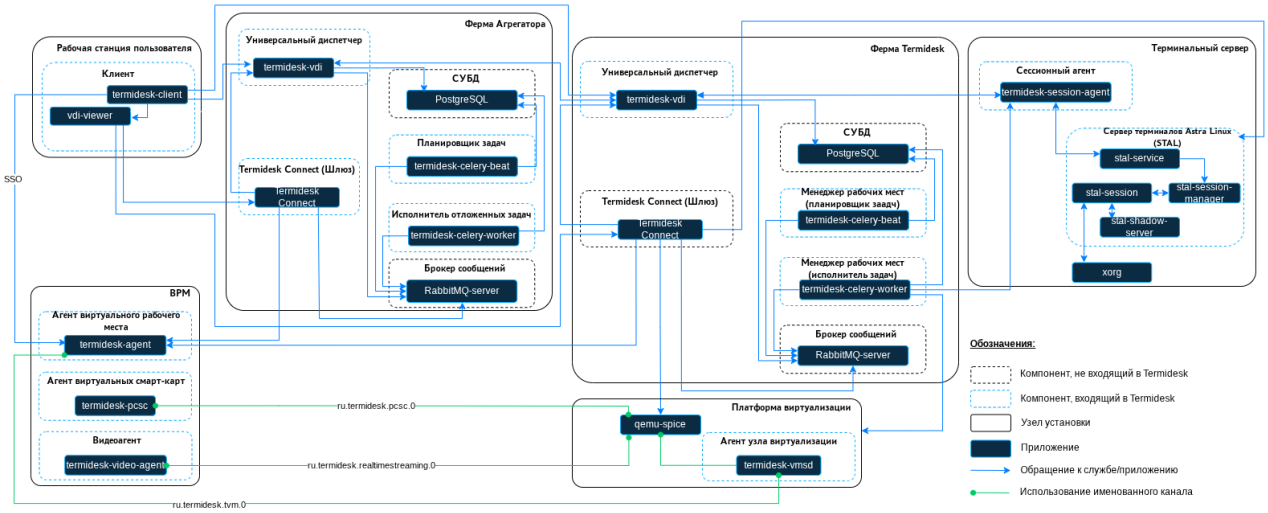


Рисунок 32. Схема взаимодействия компонентов и приложений

Схема сетевого взаимодействия компонентов Termidesk VDI

Схема взаимодействия между сетевыми портами и компонентами Termidesk VDI в классической схеме установки представлена на рисунке (см. рисунок Схема сетевого взаимодействия компонентов Termidesk VDI).

Сервер REDIS, с которым взаимодействует компонент «Удаленный помощник» (серверная часть), в текущей версии обращается на `localhost`.

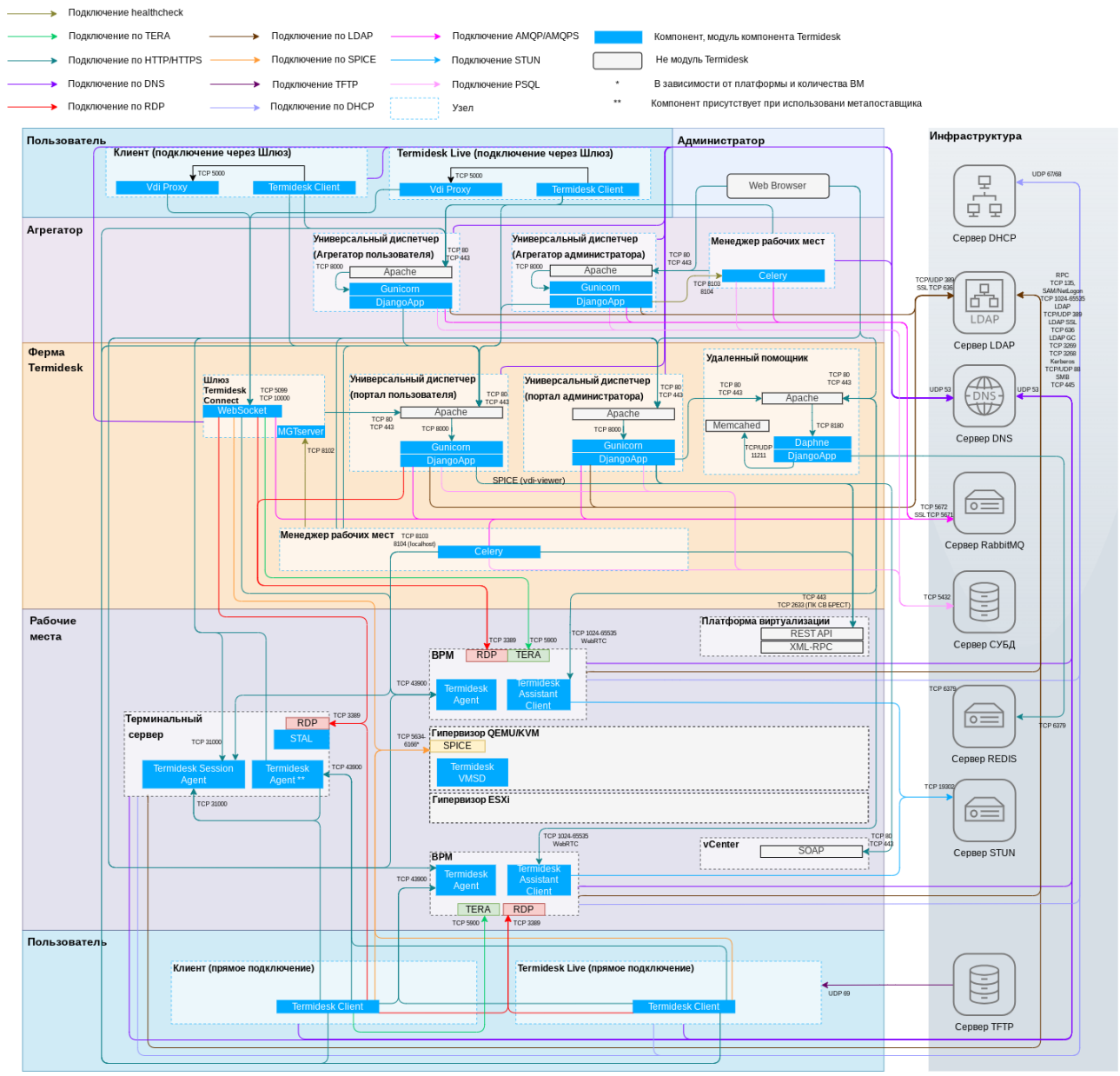


Рисунок 33. Схема сетевого взаимодействия компонентов Termidesk VDI

Общий перечень компонентов Termidesk VDI и их узлов установки представлен в таблице (см. таблицу Перечень узлов и компонентов).

Таблица 9. Перечень узлов и компонентов

Компонент	Узел установки	Наименование пакета установки
«Универсальный диспетчер»	Отдельный узел для установки	`termidesk-vdi`
«Менеджер рабочих мест»	Отдельный узел для установки или установка совместно с «Универсальным диспетчером» в составе фермы Termidesk VDI	`termidesk-vdi`
Termidesk Connect «Шлюз»	Отдельный узел для установки	Termidesk Connect
«Агент виртуального рабочего места»	ВМ или отдельный узел (автономная машина), который предоставляет рабочее место (РМ) для пользователя. Установка на этапе подготовки гостевой ОС РМ	`termidesk-agent`

Компонент	Узел установки	Наименование пакета установки
«Агент узла виртуализации»	Узел виртуализации (гипервизор) программного комплекса «Средства виртуализации «Брест» (ПК СВ Брест)	`termidesk-vmsd`
«Сессионный агент»	Установка на узле терминального сервера: • ОС Microsoft Windows Server с ролью «Remote Desktop Services»; • ОС Astra Linux Special Edition с установленным компонентом «Сервер терминалов Astra Linux»	`termidesk-session-agent`
«Видеоагент»	ВМ или отдельный узел (автономная машина), установка на этапе подготовки гостевой ОС РМ	`termidesk-video-agent`
«Агент виртуальных смарт-карт»	ВМ или отдельный узел (автономная машина), установка на этапе подготовки гостевой ОС РМ	`termidesk-pcsc-vscard`
«Клиент»	Рабочее место пользователя (пользовательская рабочая станция)	`termidesk-client`
«Оркестратор»	Отдельный узел для установки, применяется в облачной конфигурации	`termidesk-orchestrator`
«Сервер терминалов Astra Linux»	Отдельный узел для установки, возможна установка на том же узле, где установлен «Универсальный диспетчер»	`stal`
«Удаленный помощник» (серверная часть)	Отдельный узел для установки	`termidesk-assistant-server`
«Удаленный помощник» (клиентская часть)	Рабочее место пользователя (пользовательская рабочая станция) или ВМ (установка на этапе подготовки образа для ВРМ)	`termidesk-assistant-client`
Termidesk Live	Отдельный узел, тонкий клиент	`thinstation` (образ)
«Виртуальный модуль Termidesk»	Отдельная ВМ. Компонент позволяет быстро развернуть и использовать «Универсальный диспетчер», «Менеджер рабочих мест», «Шлюз»	`termidesk-virtual-appliance` (образ)

Последовательность сетевых запросов компонентов Termidesk VDI

Последовательность сетевых запросов с указанием перечня портов для компонентов Termidesk VDI и элементов инфраструктуры представлена на рисунке (см. рисунок Последовательность сетевых запросов).

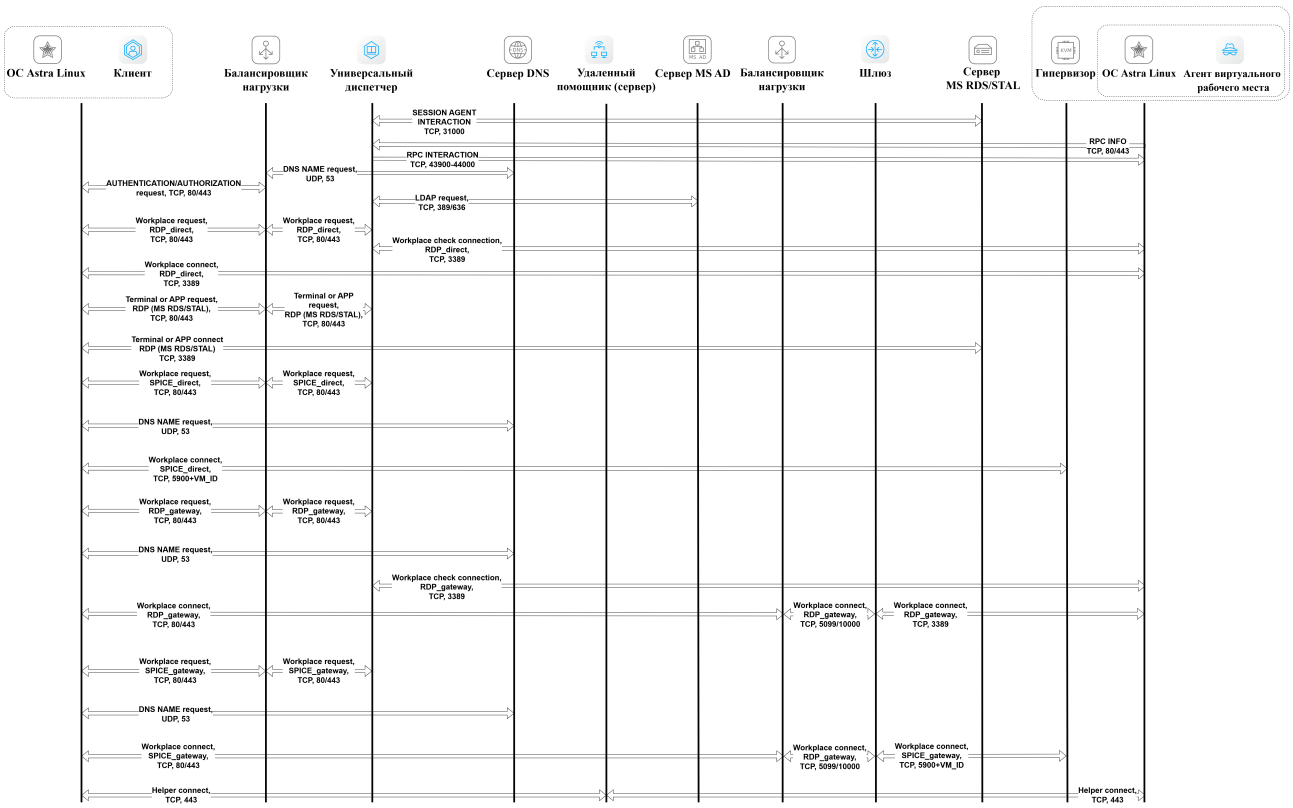


Рисунок 34. Последовательность сетевых запросов

Последовательность сетевых запросов с указанием перечня портов при аутентификации и авторизации пользователя через компонент «Клиент» представлена на на рисунке (см. рисунок Последовательность сетевых запросов при аутентификации и авторизации).

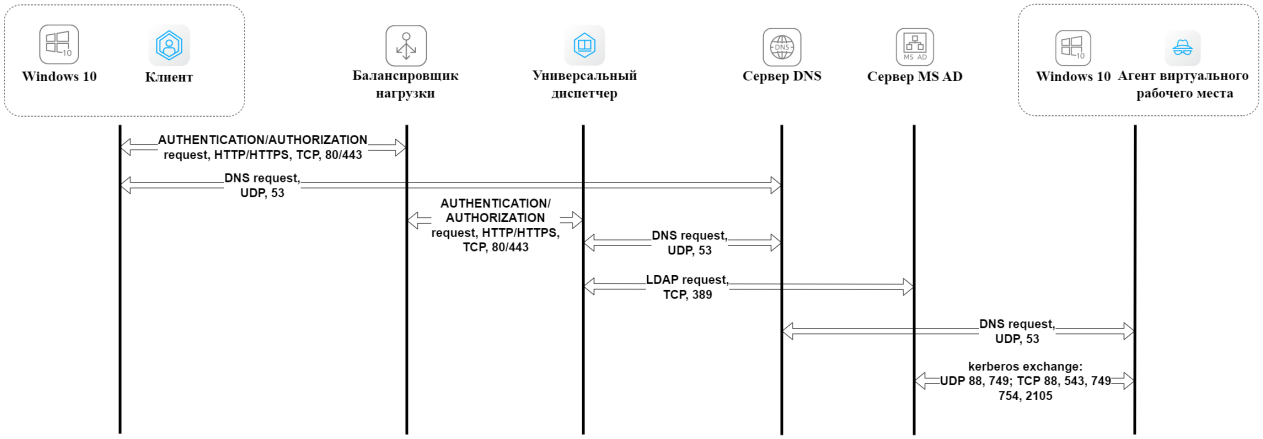


Рисунок 35. Последовательность сетевых запросов при аутентификации и авторизации

Перечень сетевых портов компонентов Termidesk VDI

Перечень сетевых портов, используемых компонентами Termidesk VDI, приведен в таблице (см. таблицу Перечень сетевых портов, используемых компонентами Termidesk VDI). Перечень содержит весь список портов: как входящих, так и исходящих.

Таблица 10. Перечень сетевых портов, используемых компонентами Termidesk VDI

Служба	Протокол	Порт
«Универсальный диспетчер»		
HTTP	TCP	80
LDAP	TCP/UDP	389

Служба	Протокол	Порт
HTTPS	TCP	443
LDAP SSL	TCP	636
AMQP (RabbitMQ)	TCP	5672
AMQPS (RabbitMQ)	TCP	5671
POSTGRESQL	TCP	5432
VDI (`termidesk-vdi`)	TCP	8000
SESSION AGENT (`TermideskSessionAgent`)	TCP	31000
AGENT (`termidesk-agent`)	TCP	43900
RPC INTERACTION	TCP	43900-44000
DNS	UDP	53
«Менеджер рабочих мест»[1]		
POSTGRESQL	TCP	5432
AMQP (RabbitMQ)	TCP	5672
AMQPS (RabbitMQ)	TCP	5671
HEALTHCHECK	TCP	8100
«Агент виртуального рабочего места»		
HTTP	TCP	80
HTTPS	TCP	443, 43900
Kerberos	TCP/UDP	88
RPC	TCP	135
LDAP	TCP/UDP	389
SMB	TCP	445
LDAP SSL	TCP	636
LDAP GC	TCP	3269
RDP	TCP	3389
SAM/NetLogon	TCP	1024-65535
AGENT (`termidesk-agent`)	TCP	39188
DNS	UDP	53
DHCP	UDP	67/68
«Агент узла виртуализации»		
VMSD (`termidesk-vmsd`)	TCP	17082
«Сессионный агент»		
SESSION AGENT HTTP/HTTPS (`TermideskSessionAgent`)	TCP	31000
«Клиент»		
HTTP	TCP	80
HTTPS	TCP	443
RDP	TCP	3389
CLIENT (`termidesk-client`)	TCP	49152-65535[2]
ПО Termidesk Viewer (устанавливается с компонентом «Клиент»)		
HTTP	TCP	80
HTTPS	TCP	443

Служба	Протокол	Порт
SPICE	TCP	5634-6166*
RDP	TCP	3389
«Виртуальный модуль Termidesk»		
ETCD	TCP/UDP	2379, 2380
«Оркестратор»		
HTTP	TCP	80
HTTPS	TCP	443
«Сервер терминалов Astra Linux» (STAL)		
RDP	TCP	3389
«Удаленный помощник»		
HTTP	TCP	80
HTTPS	TCP	443
STUN	TCP	19302
WebRTC	TCP/UDP	1024-65535
Memcached	TCP	6379
REDIS	TCP/UDP	11211

Примечания:

[1] Фактический верхний предел диапазона портов определяется платформой виртуализации и зависит от количества виртуальных машин (ВМ) на ее узле.

[2] Сетевой порт, открываемый узлом-источником для установления соединения, назначается динамически из диапазона 49152–65535, который определен настройками стека TCP/IP в ОС. В стеке TCP/IP ОС эти значения могут быть изменены.

При необходимости ограничить использование всех сетевых портов в ОС только теми, которые нужны компонентам, следует обратиться ко встроенным средствам ОС (например, «Брандмауэр» для ОС Microsoft Windows или `ufw` для ОС Linux).

Для управления сетевыми портами в ОС Microsoft Windows нужно:

- проверить список открытых портов и управляющих ими служб через интерфейс командной строки:

```
C:\Windows\system32> netstat -ab
```

- для разрешения или запрета сетевого порта перейти «Пуск» - «Параметры» - «Обновление и безопасность» - «Безопасность Windows» - «Брандмауэр и защита сети» - «Дополнительные параметры». Затем перейти во вкладку «Правила для входящих подключений», нажать экранную кнопку **[Создать правило]** и выбрать тип правила «Порт» (см. рисунок Создание правила для типа «Порт»). Далее выбрать нужный протокол (TCP или UDP), определить нужный порт (или несколько портов) в параметре «Определенные локальные порты» и на шаге «Действие» задать правило разрешения или запрета подключения.

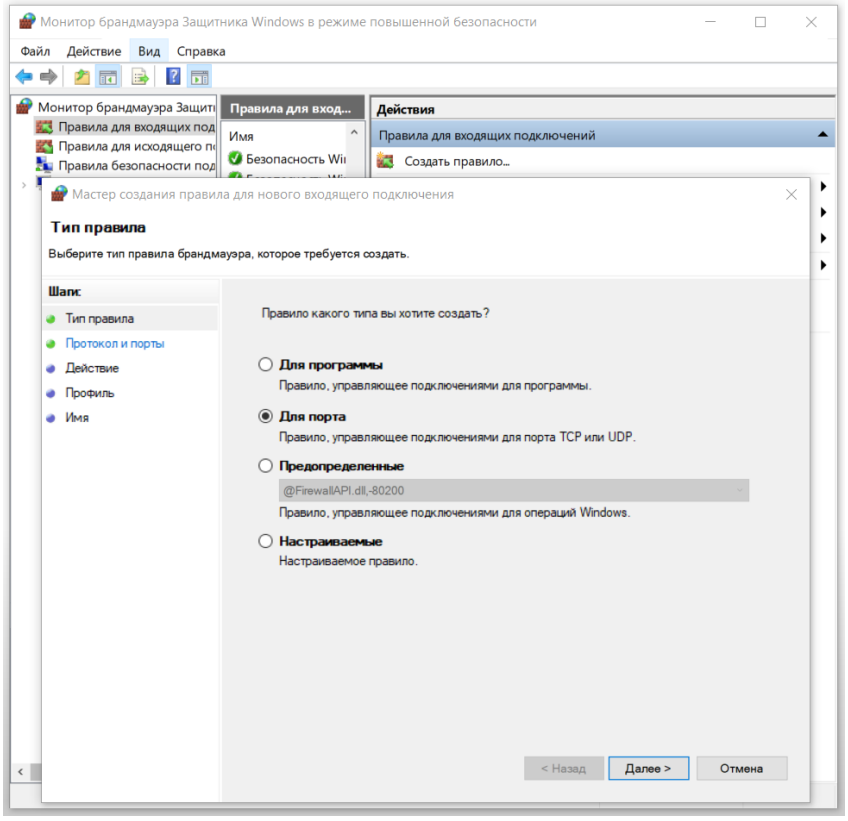


Рисунок 36. Создание правила для типа «Порт»

Для управления сетевыми портами в ОС Linux нужно:

- проверить список открытых портов через интерфейс командной строки:

```
sudo ss -tulpn
```

- убедиться, что брандмауэр активен (должен отобразиться статус `Status: active`):

```
sudo ufw status verbose
```

- если брандмауэр неактивен, включить его:

```
sudo ufw enable
```

- для разрешения определенного сетевого порта выполнить:

```
sudo ufw allow <номер порта>
```

- для разрешения определенного диапазона сетевых портов выполнить:

```
sudo ufw allow <начальный номер порта:конечный номер порта/протокол>
```

Пример команды для разрешения портов 6000-6007 для протокола TCP:

```
sudo ufw allow 6000:6007/tcp
```

- для запрета сетевых портов подходит синтаксис, приведенный выше, но вместо команды `allow` используется `deny`.

Перечень разрешающих правил межсетевого экрана для работы компонентов Termidesk VDI

На межсетевом экране, использующемся в организации, нужно задать следующие разрешающие правила для работы компонентов Termidesk VDI (см. таблицу Перечень правил межсетевого экрана).

В таблице приняты обозначения:

- «Узел-приемник» - узел, являющийся принимающей стороной сетевого соединения;
- «Протокол» - протокол транспортного уровня или уровня приложения, используемый в рамках соединения;
- «Порт приемника» - сетевой порт, прослушиваемый принимающей стороной.

Сетевой порт, открываемый узлом-источником для установления соединения, назначается динамически из диапазона 49152–65535, который определен настройками стека TCP/IP в ОС. В стеке TCP/IP ОС эти значения могут быть изменены.

Таблица 11. Перечень правил межсетевого экрана

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
«Универсальный диспетчер»	localhost	TCP	8000	Работа веб-сервера «Универсального диспетчера» для обслуживания входящих подключений. Порт открывается на localhost
	Контроллеры доменов аутентификации	TCP/UDP	389	LDAP
	Контроллеры доменов аутентификации	TCP	3268	LDAP
	Контроллеры доменов аутентификации	TCP	636, 3269	LDAPS
	Сервер DNS	UDP	53	DNS
	Платформа виртуализации	TCP	80, 443	Для обслуживания запросов к платформе виртуализации
	ПК СВ Брест	TCP/UDP	2633	Для взаимодействия с ПК СВ Брест
	«Сессионный агент»	TCP	31000	Для обслуживания подключений к терминальным серверам, на которых установлен «Сессионный агент»
	СУБД	TCP	5432	Для обслуживания запросов к СУБД
	Сервер RabbitMQ	TCP	5672, 5671 (TLS)	Для обслуживания запросов к RabbitMQ
	«Агент виртуального рабочего места»	TCP	43900	Для обслуживания подключения к «Агенту виртуального рабочего места»
	ВМ	TCP	3389	Для обслуживания подключений RDP к ВМ
Рабочее место администратора	«Универсальный диспетчер»	TCP	443	Защищенное подключение к порталу Termidesk
	«Удаленный помощник» (серверная часть)	TCP	80, 443	Защищенное подключение к серверной части «Удаленного помощника»

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
«Менеджер рабочих мест»				

	виртуального рабочего места»			подключения к «Агенту виртуального рабочего места», для функционала сброса сессии пользователя
Узел-источник	**Узел-приемник**	**Протокол**	**Порт приемника**	**Описание**
	Терминальный сервер	TCP	31000	Для получения состояния сессий, управления ими и периодического опроса состояния регистрации терминальных серверов, на которых установлен «Сессионный агент»
	Сервер электронной почты	TCP	25 (SMTP), 587 (SMTP Authentication), 465 (SMTPS)	Для отправки уведомлений «Универсального диспетчера» на сервер электронной почты

TERMIDESK VDI

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
«Шлюз»				

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
				подключении пользователя через «Шлюз»
	«Универсальный диспетчер»	TCP	80, 443	Защищенное подключение к порталу termidesk
	Терминальный сервер	TCP	31000	Для обслуживания подключений к терминальным серверам, на которых установлен «Сессионный агент»
	Сервер RabbitMQ	TCP	5672, 5671 (TLS)	Для обслуживания запросов к RabbitMQ
«Клиент»	Сервер DNS	UDP	53	DNS
	«Универсальный диспетчер»	TCP	80, 443	Для обслуживания подключений к «Универсальному диспетчеру»
	Платформа виртуализации	TCP	5634-6166	Для обслуживания подключений SPICE к ВМ при подключении к ВРМ. Фактический верхний предел диапазона портов определяется платформой виртуализации и зависит от количества ВМ на ее узле
	ВМ или терминальный сервер	TCP	3389	Для обслуживания подключений RDP к ВМ или терминальному серверу
	ВМ или терминальный сервер	TCP	43900	Для корректной работы технологии единого входа (SSO) при прямом подключении к ВРМ (не через «Шлюз»)
	ВМ или терминальный сервер	TCP	31000	Для обслуживания подключений к терминальным серверам, на которых установлен «Сессионный агент»

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
Клиент Loudplay (устанавливается на узел с «Клиентом» Termidesk VDI)	Сервер Loudplay	UDP	6970, 6971	Для обмена видеопотоком между клиентом Loudplay и Сервером Loudplay
	Сервер Loudplay	UDP	6972, 6973	Для обмена аудиопотоком между клиентом Loudplay и Сервером Loudplay
	Сервер Loudplay	UDP	6974, 6975	Для обмена между клиентом Loudplay и Сервером Loudplay при использовании двух виртуальных мониторов и двух vGPU
	Сервер Loudplay	TCP	8554	Для обслуживания подключений к RTSP-серверу
	Сервер Loudplay	UDP	8555	Для обмена сообщениями, связанными с клавиатурой и мышью, между клиентом Loudplay и Сервером Loudplay
	Сервер Loudplay	TCP	8556	Для обмена RPC-сообщениями между клиентом Loudplay и Сервером Loudplay
	Сервер Loudplay	TCP	8557	Для обмена между клиентом Loudplay и Сервером Loudplay

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
«Агент виртуального рабочего места»	localhost	TCP	39188	Для обслуживания входящих подключений к «Агенту виртуальных рабочих мест». Порт открывается на localhost
	localhost	TCP	43900	Порт HTTP-сервера «Агента виртуального рабочего места»
	«Универсальный диспетчер»	TCP	80, 443	Для подключения к «Универсальному диспетчеру» и передачи информации о готовности ВМ
	Контроллеры доменов аутентификации	TCP	389	LDAP
	Контроллеры доменов аутентификации	TCP	3268	LDAP
	Контроллеры доменов аутентификации	TCP	636, 3269	LDAPS
	Контроллеры доменов аутентификации	TCP	135	RPC
	Контроллеры доменов аутентификации	TCP	1024-65535	SAM/NetLogon
	Контроллеры доменов аутентификации	TCP/UDP	88	Kerberos
	Контроллеры доменов аутентификации	TCP	445	SMB
	Сервер DHCP	TCP	67, 68	DHCP
	Сервер DNS	UDP	53	DNS
Сервер Loudplay (устанавливается на узел с «Агентом виртуального рабочего места» Termidesk VDI)	Сервер лицензирования Loudplay	TCP	5555	Для обслуживания API-запросов о лицензиях и их статусе
	Сервер лицензирования Loudplay	TCP	5556	Для обслуживания запросов к модулю лицензирования
«Агент узла виртуализации»	localhost	TCP	17082	Для обслуживания входящих подключений к «Агенту узла виртуализации». Порт открывается на localhost

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
«Сессионный агент»	«Универсальный диспетчер»	TCP	80, 443	Для обслуживания подключений к «Универсальному диспетчеру»
«Сервер терминалов Astra Linux»	Сервер DNS	UDP	53	DNS
	Контроллеры доменов аутентификации	TCP/UDP	389	LDAP
	Контроллеры доменов аутентификации	TCP	3268	LDAP
	Контроллеры доменов аутентификации	TCP	636, 3269	LDAPS
	Сервер DHCP	TCP	67, 68	DHCP
«Оркестратор»	«Универсальный диспетчер»	TCP	80, 443	Для обслуживания подключений к «Универсальному диспетчеру»
	Служба облачной идентификации (cloud identity service)	TCP	Не определен	Для подключения к службе облачной идентификации с целью валидации токена. Порт определяется архитектурой конкретной облачной платформы
Агент облака (cloud agent)	«Оркестратор»	TCP	80, 443	Для обслуживания подключений между агентом облака (не является компонентом Termidesk VDI) и «Оркестратором»
«Виртуальный модуль Termidesk»	«Виртуальный модуль Termidesk»	TCP/UDP	2379, 2380	Подключение ETCD для хранения и синхронизации конфигураций между узлами «Виртуального модуля Termidesk»
«Удаленный помощник» (клиентская часть)	«Удаленный помощник» (серверная часть)	TCP/UDP	80, 443	Для обслуживания подключений к серверной части «Удаленного помощника»
	Сервер STUN	TCP	19302	Для обслуживания подключений к серверу STUN (stun://stun.l.google.com:19302)

Узел-источник	Узел-приемник	Протокол	Порт приемника	Описание
«Удаленный помощник» (серверная часть)	«Удаленный помощник» (клиентская часть)	TCP	1024-65535	Для обслуживания подключений к клиентской части «Удаленного помощника» WebRTC
	localhost	TCP	6379	Для обслуживания подключений к серверу REDIS. В текущей версии порт открывается на `localhost`
	localhost	TCP/UPD	11211	Для обслуживания подключений к серверу Memcached. Порт открывается на localhost

Перечень сертификатов и ключей для компонентов Termidesk VDI

Перечень сертификатов и ключей для компонентов Termidesk VDI

Компоненты Termidesk VDI и компоненты среды функционирования (например, брокер сообщений RabbitMQ или СУБД) могут использовать защищенное соединение для взаимодействия между собой.

Перечень сертификатов и ключей, используемых различными компонентами, приведен на схеме (см. рисунок Распределение сертификатов и ключей по компонентам).

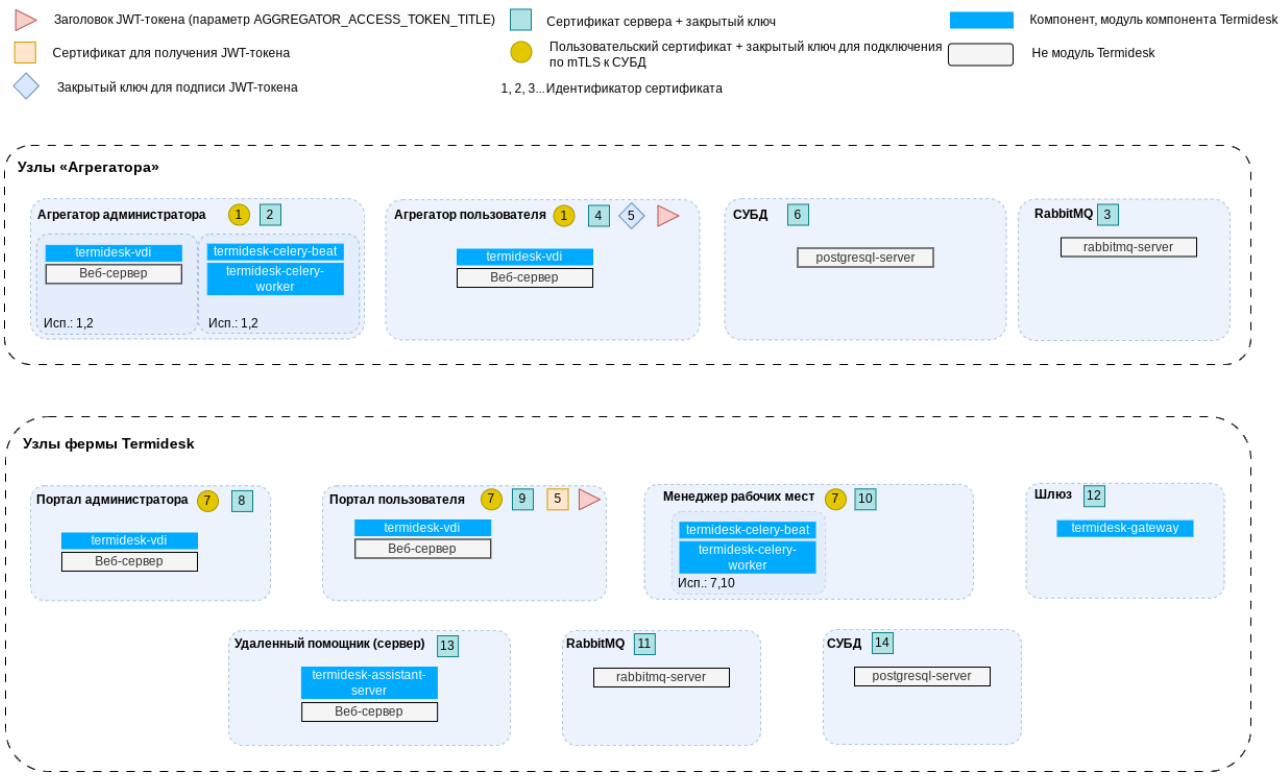


Рисунок 37. Распределение сертификатов и ключей по компонентам

НАЧАЛО РАБОТЫ

Последовательность ввода в действие Termidesk VDI

Последовательность настройки при использовании классического VDI

Общая последовательность шагов для ввода Termidesk VDI в действие состоит в следующем:

- подготовка сетевой инфраструктуры в соответствии с требованиями Termidesk VDI;
- подготовка узла виртуализации в соответствии с требованиями Termidesk VDI;
- установка Termidesk VDI в зависимости от выбранной конфигурации: комплексная или распределенная. Ввод в домен (при необходимости, согласно схеме сетевой инфраструктуры организации);
- установка компонента «Агент узла виртуализации» на узел виртуализации, если используется поставщик ресурсов ПК СВ Брест;
- подготовка базового шаблона ВМ на узле виртуализации;
- подготовка гостевой ОС базового ВРМ;

Базовое ВРМ - прототип будущих ВРМ.

- переход в графический интерфейс Termidesk VDI;
- добавление необходимого домена аутентификации (при необходимости, если в инфраструктуре используются серверы каталогов);
- добавление необходимого поставщика ресурсов;
- создание шаблона РМ в Termidesk VDI в добавленном поставщике ресурсов;
- добавление настроек гостевых ОС для созданного шаблона РМ;
- добавление протоколов доставки, которые будут использоваться для подключения к РМ;
- добавление сетей, которые будут использоваться для настройки доступа пользователей;
- создание и настройка фонда РМ в Termidesk VDI;
- назначение групп пользователей в созданном ранее фонде;
- назначение протоколов доставки в созданном ранее фонде;
- назначение сетей в созданном ранее фонде;
- выполнение публикации настроенного фонда РМ в Termidesk VDI.

Последовательность настройки при использовании терминального сервера

Общая последовательность шагов при необходимости использования терминальных серверов состоит в следующем:

- при использовании терминального сервера на базе ОС Astra Linux Special Edition - установка компонента STAL. Рекомендуется использовать отдельный узел (физический или виртуальный) и не совмещать установку с сервером Termidesk VDI;
- установка компонента «Сессионный агент» на терминальный сервер;
- переход в графический интерфейс Termidesk VDI и добавление поставщика ресурсов «Сервер терминалов» в Termidesk VDI;
- добавление необходимого домена аутентификации (при необходимости, если в

инфраструктуре используются серверы каталогов);

- создание шаблона РМ для поставщика ресурсов «Сервер терминалов» в Termidesk VDI;
- добавление протоколов доставки, которые будут использоваться для подключения к РМ;
- добавление сетей, которые будут использоваться для настройки доступа пользователей;
- создание и настройка фонда РМ в Termidesk VDI;
- назначение групп пользователей в созданном ранее фонде;
- назначение протоколов доставки в созданном ранее фонде;
- назначение сетей в созданном ранее фонде.

Поддерживается расширенный сценарий добавления терминальных серверов: помимо использования поставщика ресурсов «Сервер терминалов» добавить поставщик «Автономные машины», который будет объединять несколько узлов и выполнять роль служебного (не виден пользователю, но предоставляет ему ресурсы). Таким образом может быть несколько «Серверов терминалов», и одна «Автономная машина», в шаблоне которой будут заданы терминальные серверы, что предоставляет дополнительные возможности:

- поддержка нескольких сессий пользователя в рамках одного сервера. Каждой сессии пользователя назначается свой идентификатор, который передается в заголовке `X-TDSK-SID`;
- поддержка отправки сообщений в сессию пользователя терминального сервера. Сессия пользователя определяется по ее идентификатору, переданному в заголовке `X-TDSK-SID`;
- поддержка сбора метрик узла терминального сервера.

Последовательность настройки при использовании автономных машин

Общая последовательность шагов при необходимости использования автономных машин состоит в следующем:

- установка компонента «Агент виртуального рабочего места» в ОС автономной машины. Если автономная машина будет терминальным сервером, то требуется также установить компонент «Сессионный агент»;
- переход в графический интерфейс Termidesk VDI и добавление поставщика ресурсов «Автономные машины»;
- добавление необходимого домена аутентификации (при необходимости, если в инфраструктуре используются серверы каталогов);
- создание шаблона РМ для поставщика ресурсов «Автономные машины» в Termidesk VDI;
- добавление настроек гостевых ОС для созданного шаблона РМ;
- добавление протоколов доставки, которые будут использоваться для подключения к РМ;
- добавление сетей, которые будут использоваться для настройки доступа пользователей. Не требуется, если автономная машина будет использоваться совместно с поставщиком ресурсов «Сервер терминалов» в сценарии поддержки дополнительных возможностей при работе с терминальными серверами;
- создание и настройка фонда РМ в Termidesk VDI;
- назначение групп пользователей в созданном ранее фонде. Не требуется, если автономная машина будет использоваться совместно с поставщиком ресурсов «Сервер терминалов» в сценарии поддержки дополнительных возможностей при работе с

терминальными серверами;

- назначение протоколов доставки в созданном ранее фонде. Не требуется, если автономная машина будет использоваться совместно с поставщиком ресурсов «Сервер терминалов» в сценарии поддержки дополнительных возможностей при работе с терминальными серверами;
- назначение сетей в созданном ранее фонде. Не требуется, если автономная машина будет использоваться совместно с поставщиком ресурсов «Сервер терминалов» в сценарии поддержки дополнительных возможностей при работе с терминальными серверами;
- выполнение публикации настроенного фонда РМ в Termidesk VDI.

Подготовка базового шаблона ВМ

Подготовка базового шаблона ВМ на примере ПК СВ Брест

При создании базового шаблона ВМ в ПК СВ Брест необходимо учесть следующее:

- для стабильной работы ВМ рекомендуется назначать ресурсы в соответствии с минимальными системными требованиями, установленными производителем ОС;
- при создании образа диска в панели управления ПК СВ Брест следует перейти «Хранилище - Образ - Постоянный», затем в поле «Постоянный» выбрать значение «Да». Во время установки и настройки ОС тип образа должен быть подключен как постоянный. После установки и завершения настройки ОС в поле «Постоянный» выбрать значение «Нет» (см. рисунок Окно выбора типа подключаемого образа в ПК СВ Брест);

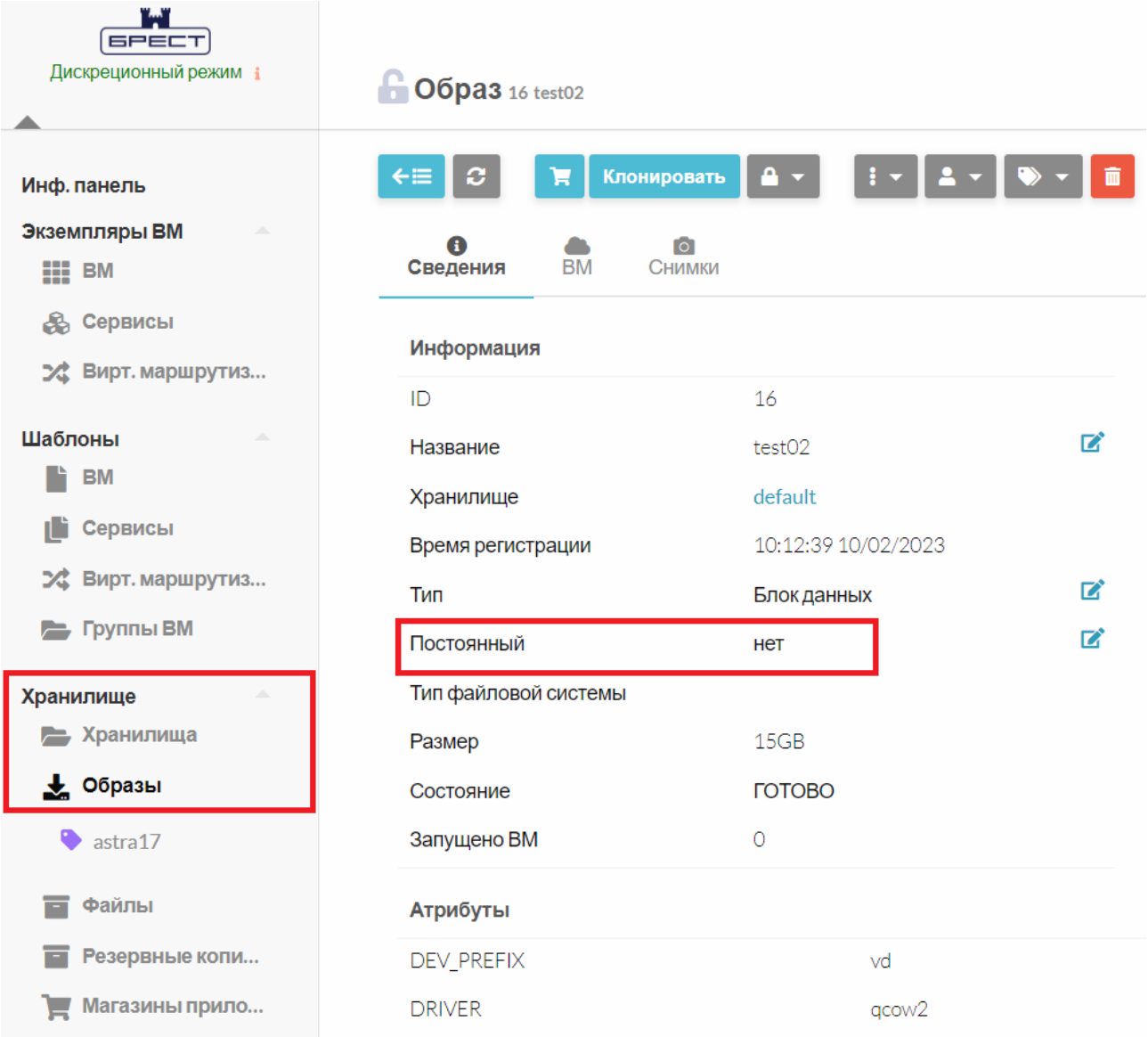


Рисунок 38. Окно выбора типа подключаемого образа в ПК СВ Брест

Если ВМ в качестве гостевой ОС будет использовать ОС Microsoft Windows, то при установке на диск на шине Virtio до включения ВМ необходимо подключить `iso`-образ диска с драйверами `Virtio-win`.

- при создании образа диска в панели управления ПК СВ Брест следует перейти «Хранилище - Образ - Расширенные настройки», затем в поле «Шина» выбрать значение «Virtio», а в поле «Формат» выбрать значение «qcow2» (см. рисунок Окно назначения параметров образа диска в ПК СВ Брест);

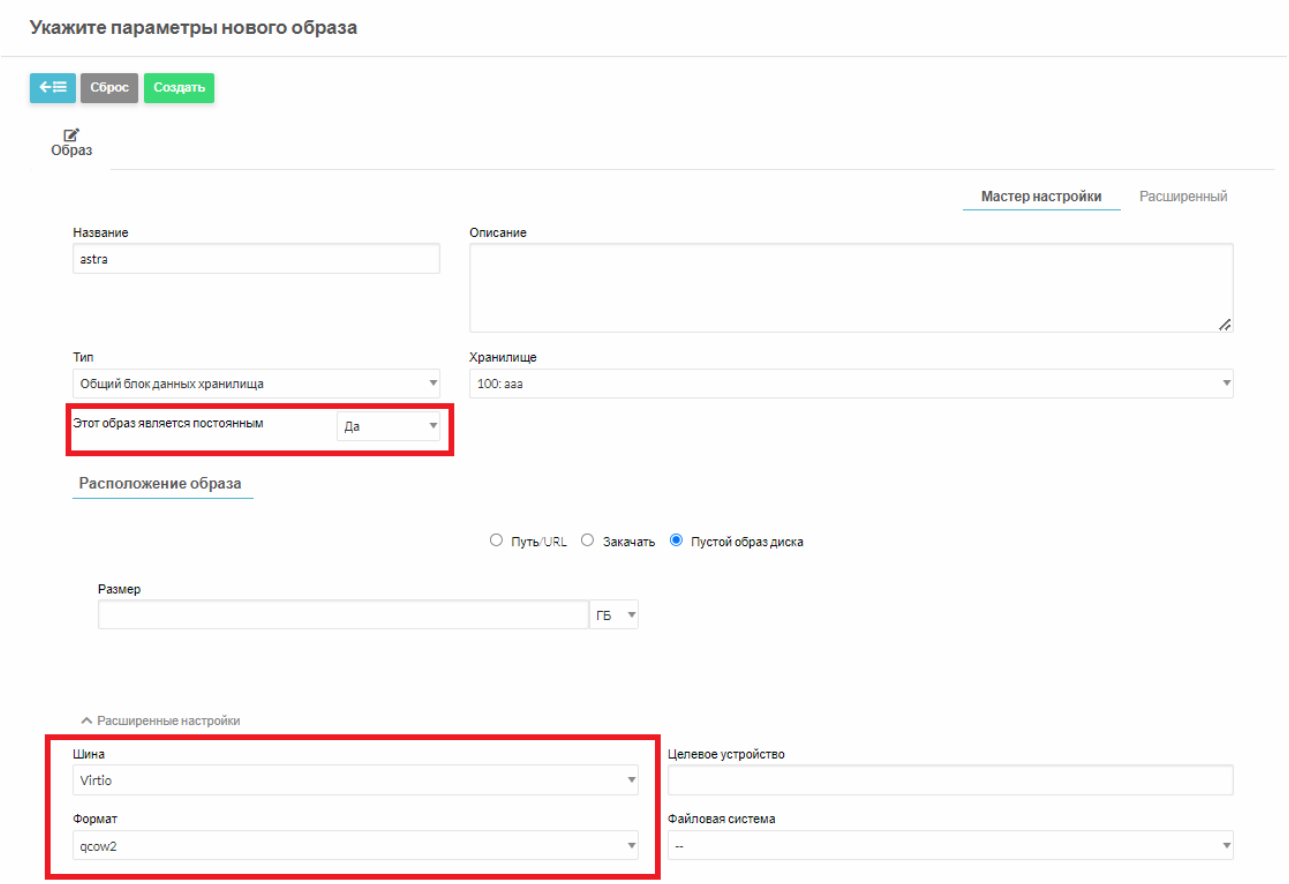


Рисунок 39. Окно назначения параметров образа диска в ПК СВ Брест

Значение в поле «Формат» зависит от типа подключенного к ПК СВ Брест хранилища.

В настройках шаблона ВМ следует:

- перейти «Хранилище - Расширенные настройки», в поле «Шина» выбрать значение «Virtio» (см. рисунок Окно назначения расширенных параметров диска шаблона ВМ);
- в поле «ID Образа» указать идентификатор (ID) подключенного к шаблону ВМ образа диска;
- поля «Имя образа» и «Имя пользователя владельца образа» очистить от любых значений;

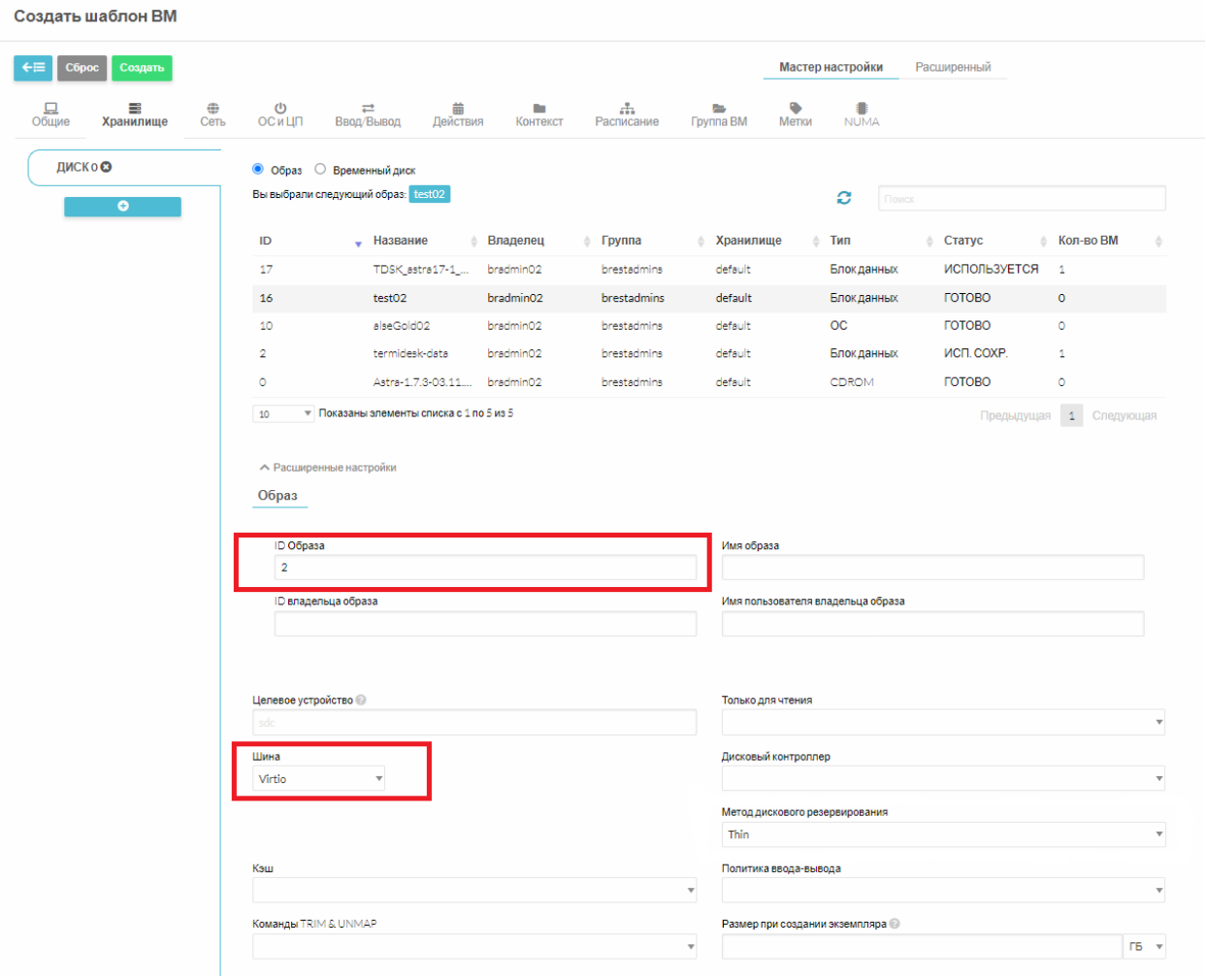


Рисунок 40. Окно назначения расширенных параметров диска шаблона ВМ

- перейти в «Ввод/Вывод», затем в поле «Средства графического доступа» выбрать значение «SPICE», а в поле «Видеокарта» выбрать значение «QXL» (см. рисунок Окно назначения средств графического доступа шаблона ВМ);

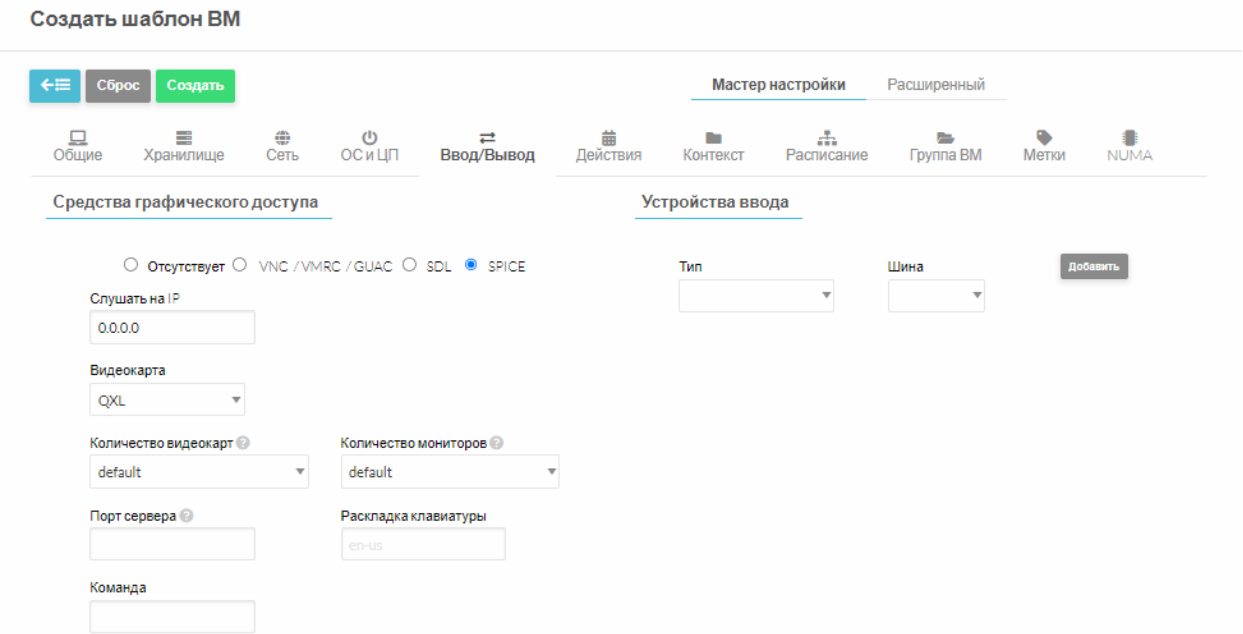


Рисунок 41. Окно назначения средств графического доступа шаблона ВМ

- в случае многомониторной конфигурации необходимо в выпадающем списке «Количество мониторов» выбрать соответствующее значение для гостевой ОС Astra Linux, а в выпадающем списке «Количество видеокарт» выбрать соответствующее значение для гостевой ОС Microsoft Windows;
- перейти во вкладку «ОС и ЦП», в поле «Архитектура CPU» следует оставить значение по умолчанию (не менять).

В случае, если необходим автоматический запуск ВМ, то после создания шаблона ВМ в панели управления ПК СВ Брест следует перейти в созданный шаблон и задать для параметра «Служебная ВМ» значение на «Да» (см. рисунок Расположение параметра «Служебная ВМ»).

При добавлении ПК СВ Брест как поставщика ресурсов Termidesk VDI должен быть активирован параметр «Запуск от имени служебного пользователя;

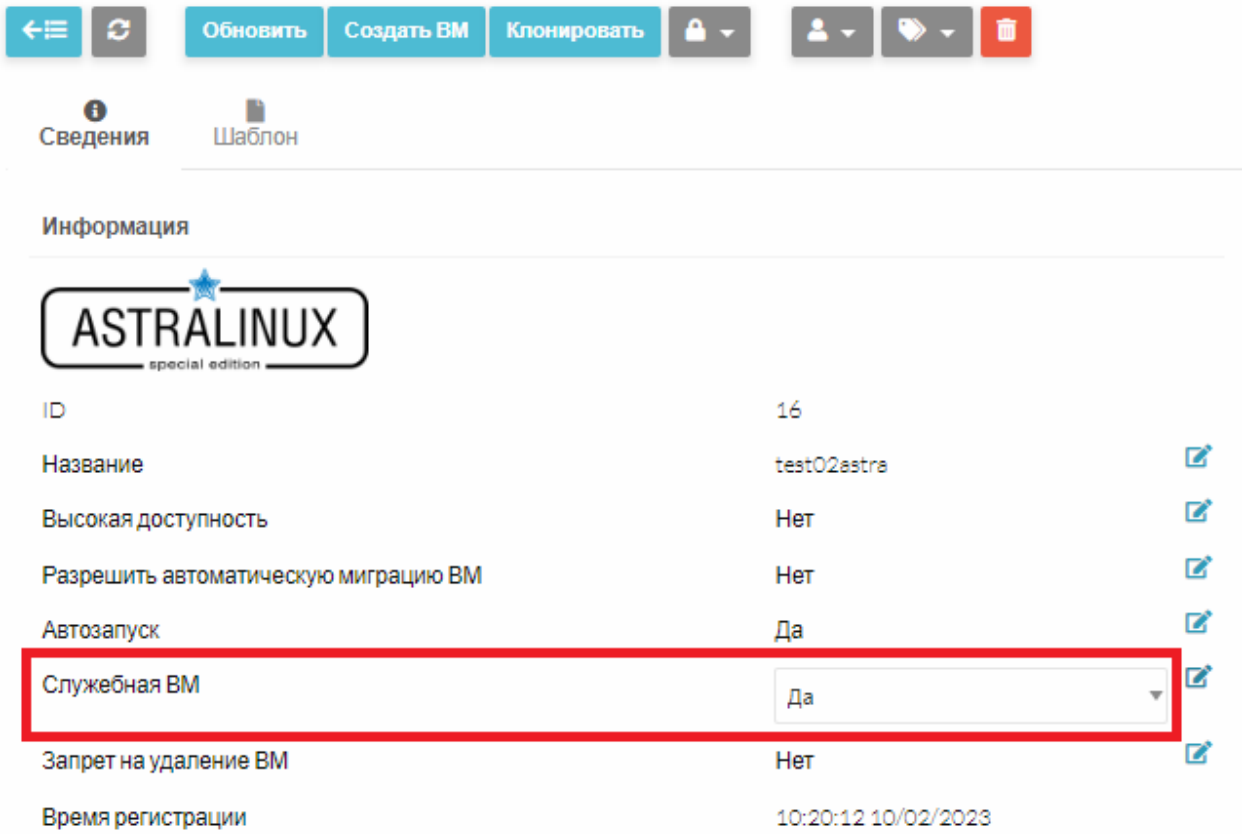


Рисунок 42. Расположение параметра «Служебная ВМ»

Подготовка базового шаблона ВМ на примере VMmanager

Описание по подготовке базового шаблона актуальна для случая, если сервер VMmanager установлен на ОС Astra Linux 1.7.4.

При создании базового шаблона ВМ в платформе управления виртуализации VMmanager необходимо учесть следующее:

- при добавлении конфигурации ВМ необходимо установить технологию вирутализации KVM, активировать параметры «Разрешить подключения по протоколу SPICE» и «Интеграция с TERMIDESK» (см. рисунок Окно добавления конфигурации в VMmanager);
- для стабильной работы ВМ рекомендуется назначать ресурсы в соответствии с минимальными системными требованиями, установленными производителем ОС;

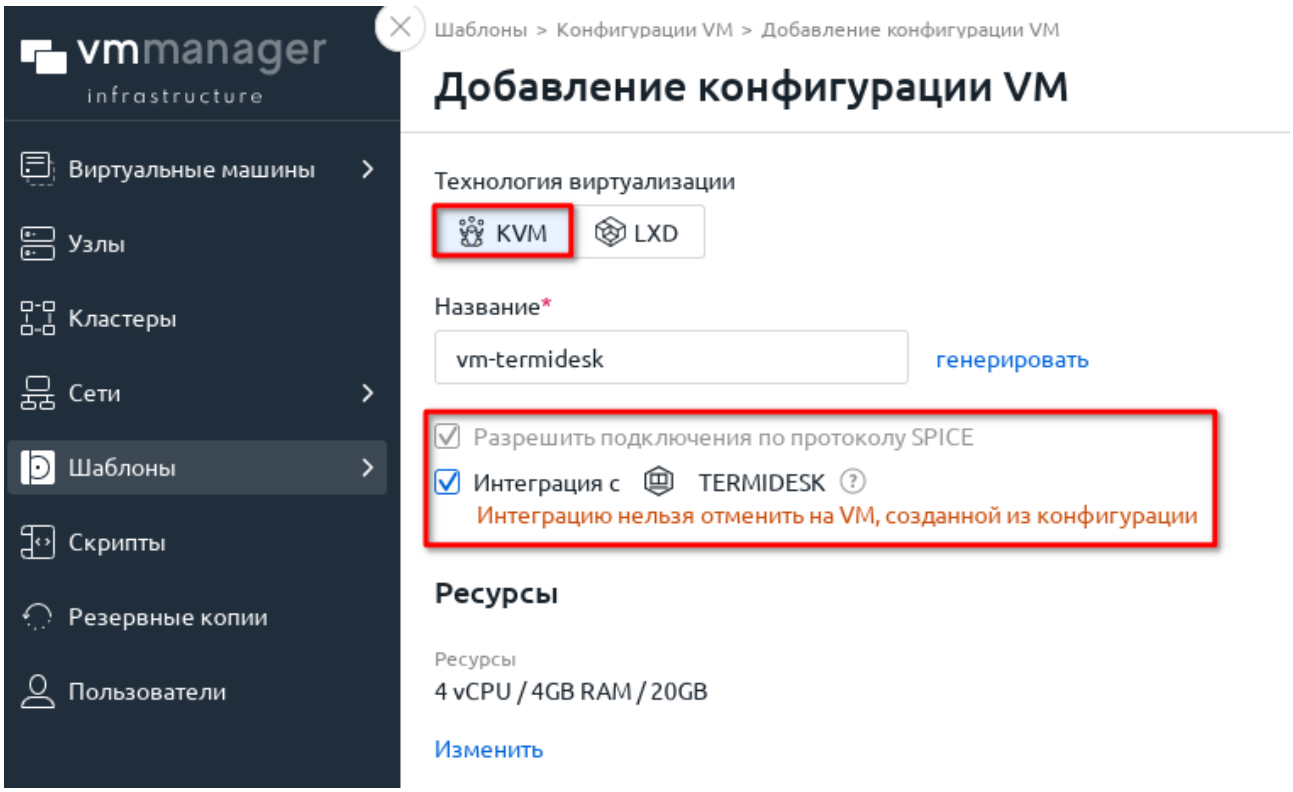


Рисунок 43. Окно добавления конфигурации в VMmanager

- при создании ВМ необходимо:
  - выбрать ОС. В случае выбора ОС Windows 10 необходимо использовать ОС Windows 10 RUS GPT для корректной работы автоматической выдачи IP-адресов;
  - выбрать созданную конфигурацию для работы с Termidesk VDI (см. рисунок Окно создания новой ВМ в VMmanager);
  - в блоке настроек «Приложение и скрипты» установить «без скрипта»;
  - настроить узел, сеть;
  - назначить название ВМ и пароль.

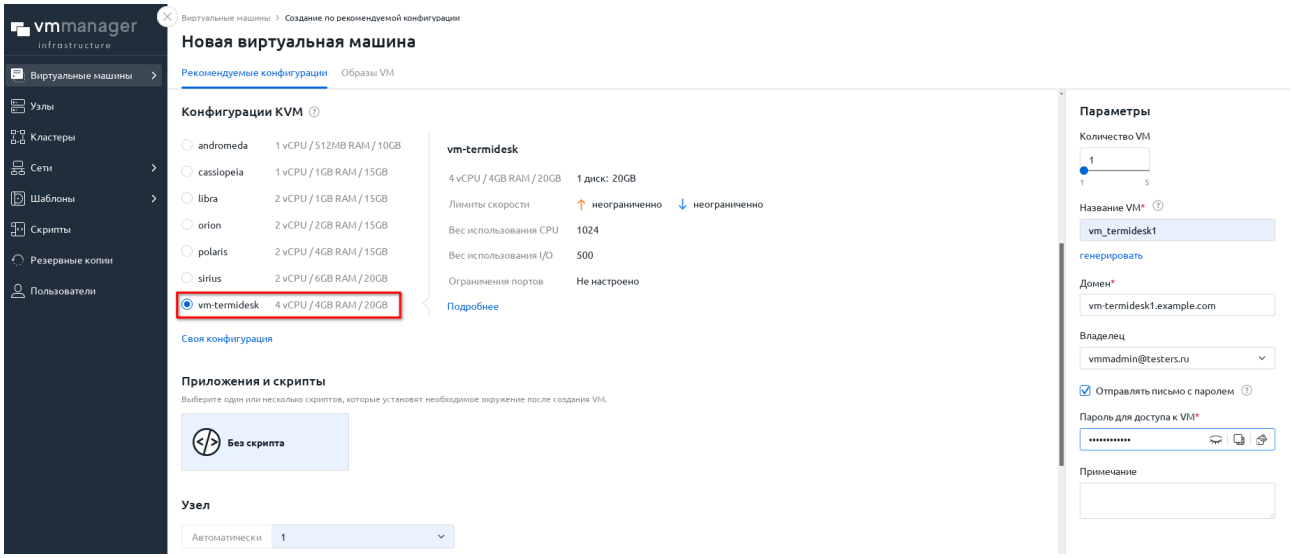


Рисунок 44. Окно создания новой ВМ в VMmanager

НАСТРОЙКА ГОСТЕВОЙ ОС РМ

Обязательные настройки гостевой ОС РМ

Обязательные настройки

Для подготовки необходимо:

- в созданной ранее ВМ выполнить настройку гостевой ОС в зависимости от типа ОС;
- выполнить установку и настройку компонента «Агент виртуального рабочего места»;
- для активации функционала перенаправления видеокамеры и смарт-карт выполнить установку и настройку компонентов «Видеоагент» и «Агент виртуальных смарт-карт»;
- для активации возможности подключения к сессии пользователя через компонент «Удаленный помощник» выполнить установку клиентской части «Удаленного помощника».

Базовое ВРМ в домен вводить не нужно: процесс ввода контролируется параметрами гостевых ОС, которые указываются при создании фонда РМ.

Обязательная настройка гостевой ОС Astra Linux

Настройка гостевой ОС Astra Linux сводится к выполнению следующих действий:

> Перечень протестированных и поддерживаемых комбинаций протоколов удаленного доступа и гостевых ОС приведен в подразделе **Общие сведения о протоколах доставки**.

- для возможности подключения по протоколу SPICE:
  - установить пакеты `qemu-guest-agent`, `spice-vdagent`, `xserver-xorg-video-qxl`:

```
sudo apt install -y qemu-guest-agent spice-vdagent xserver-xorg-video-qxl
```

  - для включения возможности перенаправления каталога по протоколу SPICE установить пакеты `spice-webdavd` и `davfs2`:

```
sudo apt install -y spice-webdavd davfs2
```

> Для предоставления пользователям возможности перенаправления каталога необходимо также выполнить настройки, указанные в подразделе **Настройка перенаправления каталога из пользовательской рабочей станции в РМ**.

- для возможности подключения по протоколу RDP (в сценарии использования терминального сервера с компонентом «Сервер терминалов Astra Linux»):
  - установить «Сервер терминалов Astra Linux»;
  - при использовании ОС Astra Linux Special Edition 1.8 для корректного отображения размера шрифтов нужно изменить файл `/etc/xdg/kdeglobals`, добавив строку:

```
[KScreen]
```

```
ScreenScaleFactors=rdp0=1;
```

- для возможности подключения по протоколу TERA установить TERA;
- привести файл `/etc/acpi/events/powerbtn-acpi-support` к виду:

```
event=button/power
action=/sbin/poweroff
```

- для возможности ввода ОС Astra Linux в домен MS AD установить пакет `astra-ad-sssd-client`:

```
sudo apt install -y astra-ad-sssd-client
```

- для возможности ввода ОС Astra Linux в домен FreeIPA установить пакет `astra-freeipa-client`:

```
sudo apt install -y astra-freeipa-client
```

- для возможности ввода ОС Astra Linux в домен ALD Pro нужно:
  - подключить необходимый репозиторий согласно документации на программный комплекс ALD Pro;
  - установить пакеты `astra-freeipa-client` и `aldpro-client`:

    ```
    sudo apt install -y astra-freeipa-client aldpro-client
    ```

  - если используется гостевая ОС Astra Linux Special Edition 1.8 нужно:
    - создать файл `/etc/sssd/conf.d/10_short_names.conf` со следующим содержимым (в примере `astra.domain` - наименование домена):

      ```
      [domain/astra.domain]
      use_fully_qualified_names = False
      ```

    - задать права созданному файлу:

      ```
      chown root:root /etc/sssd/conf.d/10_short_names.conf
      chmod 600 /etc/sssd/conf.d/10_short_names.conf
      ```

После ввода гостевой ОС в домен необходимо убедиться, что для конфигурационных файлов службы `sssd` (`/etc/sssd/conf.d/*.conf`) установлены корректные права доступа. При необходимости следует изменить права на файлы:

```
sudo chmod 0600 <файл_конфигурации_sssd>
```

На ОС Astra Linux Special Edition в зависимости от версии права доступа на файлы могут отличаться, поэтому следует руководствоваться документацией ОС.

При необходимости работы с vGPU по протоколу доставки Loudplay в гостевой ОС дополнительно должны быть установлены серверные драйверы NVIDIA и сервер Loudplay.

Для гостевой ОС Astra Linux 1.7 необходимо изменить способ назначения сетевых настроек:

- отключить (`systemctl --now mask`) и удалить (`apt remove`) встроенную программу для управления сетевыми соединениями `NetworkManager`:

```
sudo systemctl --now mask NetworkManager && sudo apt remove network-manager
```

- выполнить настройку сетевых интерфейсов при помощи конфигурационных файлов `/etc/network/interfaces.d/<имя интерфейса>.conf`. Необходимо создать конфигурационные файлы и описать их, воспользовавшись справочным центром Astra Linux: https://wiki.astralinux.ru/pages/viewpage.action?pageId=3277370;

Настройка должна быть выполнена для имен сетевых интерфейсов, а не их псевдонимов.

- отредактировать файл `/etc/network/interfaces`, добавив в него следующую строку, если ее нет:

```
source /etc/network/interfaces.d/*
```

- после изменения настроек выполнить перезапуск службы сети:

```
sudo systemctl restart networking
```

При стандартной настройке сетевой инфраструктуры предполагается, что IP-адрес DNS-сервера определяется DHCP-сервером. Однако если это не так, необходимо скорректировать файл `/etc/resolv.conf` в гостевой ОС Astra Linux:

- указать имя домена и IP-адрес DNS-сервера:

```
echo -e 'domain <имя_домена>\nsearch <имя_домена>\nnameserver <IP-адрес_DNS-
сервера>' | sudo tee /etc/resolv.conf
```

- для защиты файла `/etc/resolv.conf` от перезаписи нужно создать файл `/etc/dhcp/dhclient-enter-hooks.d/nodnsupdate`:

```
sudo touch /etc/dhcp/dhclient-enter-hooks.d/nodnsupdate
```

- отредактировать его содержимое, приведя к виду:

```
#!/bin/bash
make_resolv_conf() {
        :
}
```

- сохранить файл и закрыть.

Вернуть возможность перезаписи файла `/etc/resolv.conf` можно, удалив ранее созданный файл `/etc/dhcp/dhclient-enter-hooks.d/nodnsupdate` и выполнив перезапуск сетевой службы:

```
sudo systemctl restart networking
```

Обязательная настройка гостевой ОС РЕД

Настройка гостевой ОС РЕД сводится к выполнению следующих действий:

Перечень протестированных и поддерживаемых комбинаций протоколов удаленного доступа и гостевых ОС приведен в подразделе **Общие сведения о протоколах доставки**.

- для корректного отображения в Termidesk VDI статуса РМ нужно задать полное доменное имя гостевой ОС РЕД:

```
hostnamectl set-hostname workplace.termdiesk.local
```

где:

`workplace.termidesk.local` - полное доменное имя гостевой ОС;

- для возможности подключения по протоколу SPICE установить пакеты `qemu-guest-agent`, `spice-vdagent`, `xorg-x11-drv-qxl`:

```
sudo dnf install qemu-guest-agent spice-vdagent xorg-x11-drv-qxl
```

- для включения возможности перенаправления каталога по протоколу SPICE установить пакеты `spice-webdavd` и `davfs2`:

```
sudo dnf install spice-webdavd davfs2
```

Для предоставления пользователям возможности перенаправления каталога необходимо также выполнить настройки, указанные в подразделе **Настройка перенаправления каталога из**

пользовательской рабочей станции в РМ.

- привести файл /etc/acpi/events/powerbtn-acpi-support к виду:

```
event=button/power
action=/sbin/poweroff
```

- для ввода ОС РЕД в домен FreeIPA нужно:
  - установить пакет ipa-client:

```
sudo dnf install ipa-client
```

  - для FreeIPA из состава ОС Astra Linux Special Edition внести изменения в файл /usr/lib/python3/site-packages/ipalib/constants.py:

```
sudo sed -i "s/^NAME_REGEX.*$/NAME_REGEX = r'[a-z][_a-z0-9\\\-]*[a-z0-9]$|[a-z]$'/g" $(sudo find / -name constants.py -type f | grep -FzZ 'ipalib/constants.py')
```

Команда осуществляет поиск файла constants.py в корневой директории и учитывает, что найденный путь к файлу должен содержать каталог «ipalib». В найденный файл вносится изменение переменной NAME_REGEX. Путь к файлу зависит от используемой ОС Linux и версии Python и может отличаться от указанного. Для определения пути к файлу можно воспользоваться утилитой find:

```
sudo find / -name constants.py -type f
```

В зависимости от дистрибутива ОС Linux команды могут отличаться от приведенных.

- для возможности ввода ОС РЕД 8 в домен MS AD нужно:
  - установить пакеты realmd, sssd, krb5-workstation, krb5-libs, oddjob, oddjob-mkhomedir, samba-common:

```
sudo dnf install realmd sssd krb5-workstation krb5-libs oddjob oddjob-mkhomedir samba-common
```

  - указать IP-адрес контроллера домена MS AD в файле /etc/resolv.conf, пример:

```
nameserver 192.0.2.1
```

Для гостевой ОС РЕД необходимо также изменить способ назначения сетевых настроек.

При стандартной настройке сетевой инфраструктуры предполагается, что IP-адрес DNS-

сервера определяется DHCP-сервером. Однако если это не так, необходимо скорректировать файл `/etc/resolv.conf`:

- указать имя домена и IP-адрес DNS-сервера:

```
echo -e 'domain <имя_домена>\nsearch <имя_домена>\nameserver <IP-адрес_DNS-сервера>' | sudo tee /etc/resolv.conf
```

- защитить файл `/etc/resolv.conf` от перезаписи:

```
sudo chattr +i /etc/resolv.conf
```

Вернуть возможность перезаписи файла `/etc/resolv.conf` можно командой:

```
sudo chattr -i /etc/resolv.conf
```

Обязательная настройка других гостевых ОС Linux

Настройка других гостевых ОС Linux сводится к выполнению следующих действий:

Перечень протестированных и поддерживаемых комбинаций протоколов удаленного доступа и гостевых ОС приведен в подразделе **Общие сведения о протоколах доставки**.

- для возможности подключения по протоколу SPICE установить пакеты `qemu-guest-agent`, `spice-vdagent`, `xserver-xorg-video-qxl`:

В зависимости от дистрибутива ОС Linux, а именно пакетного менеджера, команда установки может отличаться от приведенной.

Например:

```
sudo yum -y install <наименование_пакета>
```

```
sudo apt install -y qemu-guest-agent spice-vdagent xserver-xorg-video-qxl
```

- установить пакеты `spice-webdavd` и `davfs2` для включения возможности перенаправления каталога из пользовательской рабочей станции по протоколу SPICE:

```
sudo apt install -y spice-webdavd davfs2
```

Для предоставления пользователям возможности перенаправления каталога необходимо также выполнить настройки, указанные в подразделе **Настройка перенаправления каталога из пользовательской рабочей станции в РМ**.

- привести файл /etc/acpi/events/powerbtn-acpi-support к виду:

```
event=button/power
action=/sbin/poweroff
```

- при необходимости ввода ОС в домен FreeIPA нужно:
  - для FreeIPA из состава ОС Astra Linux Special Edition внести изменения в файл /usr/lib/python3/site-packages/ipalib/constants.py:

    ```
    sudo sed -i "s/^NAME_REGEX.*$/NAME_REGEX = r'[a-z][_a-z0-9\\\-]*[a-z0-9]$|[a-z]$'/g" $(sudo find / -name constants.py -type f | grep -FzZ 'ipalib/constants.py')
    ```

    Команда осуществляет поиск файла constants.py в корневой директории и учитывает, что найденный путь к файлу должен содержать каталог «ipalib». В найденный файл вносится изменение переменной NAME_REGEX. Путь к файлу зависит от используемой ОС Linux и версии Python и может отличаться от указанного. Для определения пути к файлу можно воспользоваться утилитой find:

    ```
    sudo find / -name constants.py -type f
    ```

    В зависимости от дистрибутива ОС Linux команды могут отличаться от приведенных.

  - настроить создание домашнего каталога для новых пользователей. Для этого выполнить:

    ```
    sudo pam-auth-update
    ```

  - в псевдографическом интерфейсе активировать пункт «Create home directory on login» и нажать экранную кнопку **[Ok]**. Это добавит модуль pam_mkhomedir.so в файл /etc/pam.d/common-session;
- при необходимости ввода ОС CentOS в домен нужно:
  - для ввода в домен FreeIPA установить пакеты realm, ipa-client и выполнить действия по исправлению constants.py, приведенные выше;
- при необходимости ввода ОС Альт Рабочая станция 10 и Альт Рабочая станция 11 в домен нужно:
  - для ввода в Альт Домен установить пакеты realmd, task-auth-ad-sssd:

    ```
    sudo apt install -y realmd task-auth-ad-sssd
    ```

  - для ввода в домен MS AD установить пакеты task-auth-ad-sssd, gpupdate и gpresult:

```
sudo apt install -y task-auth-ad-sssd gpupdate gpresult
```

- для ввода в домен FreeIPA установить пакет `freeipa-client` и выполнить действия по исправлению `constants.py`, приведенные выше;
- для ввода в домен ALD Pro установить пакет `freeipa-client` и выполнить действия по исправлению `constants.py`, приведенные выше.

Обязательная настройка гостевой ОС Microsoft Windows

Настройка гостевой ОС Microsoft Windows сводится к выполнению следующих действий:

> Перечень протестированных и поддерживаемых комбинаций протоколов удаленного доступа и гостевых ОС приведен в подразделе **Общие сведения о протоколах доставки**.

- отключить режим гибернации;
- отключить выключение дисплея и жесткого диска в дополнительных параметрах схемы электропитания;

> Установку приложений `qemu-guest-agent for Windows`, `spice-guest-tools`, `spice-webdavd` нужно пропустить, если ВРМ реализовано на базе поставщика ресурсов VMware vSphere. Подключиться к такому ВРМ можно только по протоколам RDP или TERA.

- установить приложения `qemu-guest-agent for Windows` (доступ: https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/archive-qemu-ga/qemu-ga-win-106.0.1-1.el9/) и `spice-guest-tools` (доступ: https://www.spice-space.org/download/windows/spice-guest-tools/);
- установить пакет `spice-webdavd` для ОС Microsoft Windows (доступ: https://www.spice-space.org/download/windows/spice-webdavd/) для включения возможности перенаправления каталога из пользовательской рабочей станции в ВРМ. Перенаправление каталогов из пользовательской рабочей станции в ВРМ с установкой пакета `spice-webdavd` работает только для протокола SPICE;
- включить возможность удаленного подключения по протоколу RDP. Для этого:
  - в меню «Пуск» выбрать путь «Параметры - Система - Удаленный рабочий стол» и нажать экранную кнопку **[Включить удаленный рабочий стол]**;
  - убрать активацию параметра (снять галочку) «Разрешить подключения только с компьютеров, на которых работает удаленный рабочий стол с проверкой подлинности на уровне сети» (рекомендуется выполнить для ОС Microsoft Windows 7, а также при подключении по протоколу RDP с пользовательской рабочей станции на основе ОС Linux);
- для возможности подключения по протоколу TERA установить TERA;
- для возможности перенаправления принтеров из пользовательской рабочей станции с ОС Microsoft Windows необходимо установить драйвер Microsoft Software Printer Driver. Для этого:
  - перейти «Принтеры и сканеры - Свойства сервера печати - Драйверы» и нажать экранную кнопку **[Добавить]**;
  - после выбора типа архитектуры нужно указать изготовителя «Microsoft» и выбрать «Microsoft Software Printer Driver»;
- для возможности перенаправления принтеров из пользовательской рабочей станции с ОС Linux необходимо установить драйвер MS Publisher Imagesetter. Для этого:

- «Принтеры и сканеры - Свойства сервера печати - Драйверы» и нажать экранную кнопку **[Добавить]**;
- после выбора типа архитектуры нужно указать изготовителя «Generic» и выбрать «MS Publisher Imagesetter»;

- в настройках восстановления служб `spice-agent` (`Spice Agent`), `vdservice` (`SPICE VDAgent`) и `TermideskService` (`Termidesk Agent Daemon`) назначить значение «Перезапуск служб» для действий при сбое. Для этого перейти «Диспетчер задач» - «Службы» - «Открыть службы», правой кнопкой мыши нажать на нужное наименование и перейти «Свойства» - «Восстановление» (см. рисунок Дополнительные свойства служб для ОС Microsoft Windows).

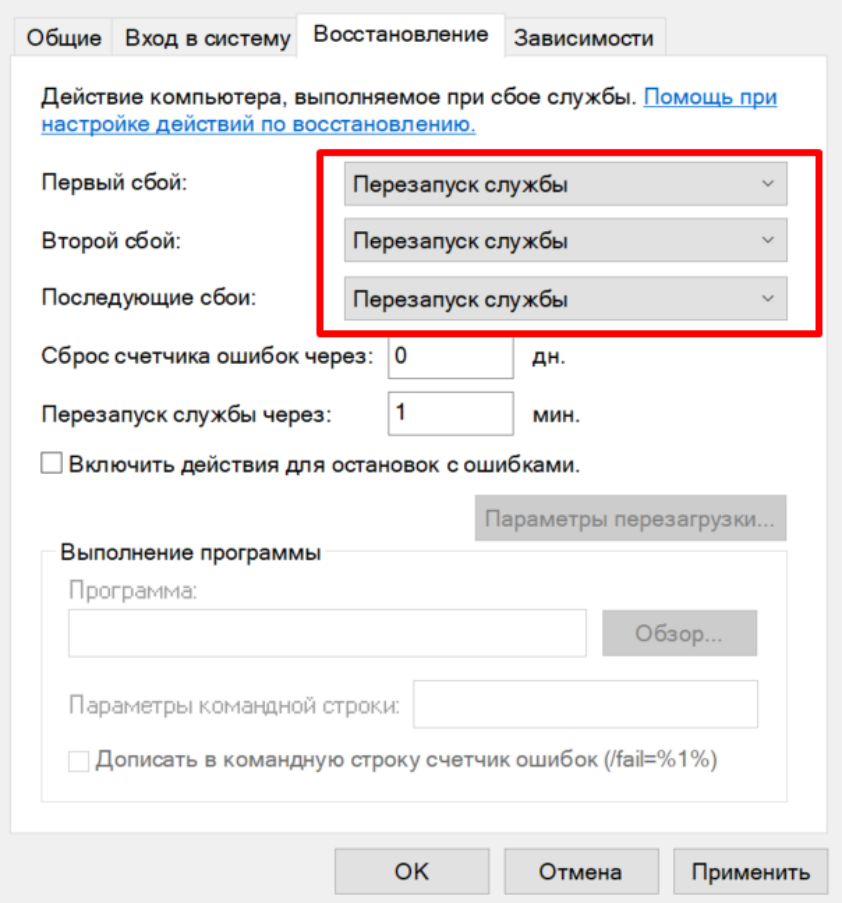


Рисунок 45. Дополнительные свойства служб для ОС Microsoft Windows

Опциональные настройки функционала для гостевой ОС РМ

Опциональные настройки выполняются для выполнения сценариев использования РМ, определенных в организации.

Автоматическое масштабирование экрана в ОС Astra Linux

Условия, при которых автоматическое масштабирование экрана должно работать при подключении пользователя к гостевой ОС Astra Linux:

- для протокола SPICE: запущенный процесс `spice-vdagent` в сессии пользователя. Дополнительно нужно выполнить настройку, описанную ниже, в том числе для экрана приветствия;
- для протокола TERA: запущенный процесс `tera-vdagent` в сессии пользователя. Дополнительные настройки могут выполняться при установке TERA.

Для настройки автоматического масштабирования экрана для протокола SPICE нужно:

- отредактировать файл /etc/udev/rules.d/50-spice-vdagent.rules, создав правило для udev:

```
ACTION=="change", KERNEL=="card0", SUBSYSTEM=="drm", RUN+="/usr/local/bin/x-resize"
```

- перезапустить сервис udev командой:

```
sudo systemctl restart udev
```

- создать исполняемый файл /usr/local/bin/x-resize:

Исполняемый файл x-resize поддерживает автоматическое масштабирование экрана ОС как в одномониторной, так и в многомониторной конфигурации.

```
#!/bin/sh
PATH=/usr/bin:/bin
LOG_FILE="/tmp/xrandr_script.log"

# Функция логирования
log_message() {
    echo "$(date '+%Y-%m-%d %H:%M:%S') - $1" >> "$LOG_FILE"
}

# Начало выполнения скрипта
log_message "Starting X11 display configuration script"

# Определение дисплея и пользователя графической сессии
desktopuser=""
display=""
log_message "Searching for active X11 sessions..."

session_ids=$(loginctl show-seat seat0 | grep Sessions= | cut -d'=' -f2)
log_message "Found session IDs: $session_ids"

for id in $session_ids
do
    log_message "Checking session $id"
    session_info=$(loginctl show-session $id --p Id --p Remote --p Name --p Type
--p Class --p Active --p IdleHint --p LockedHint)
    session_line=$(echo "$session_info" | tr '\n' ' ')
    log_message "Session $id info: $session_line"

    if echo "$session_line" | grep -E
"Remote=no.*Class=(user|greeter).*(Active=yes|LockedHint=yes)" >/dev/null 2>&1
    then
        display="$(loginctl show-session $id --p Display | cut -d'=' -f2)"
        desktopuser="$(loginctl show-session $id --p Name | cut -d'=' -f2)"
```

```
        log_message "Found active session: user=$desktopuser, display=$display"
        break
    fi
done

# Проверка что есть DISPLAY и он один
if [ $(echo "$display" | tr -cd ':' | wc -c) -ne 1 ]; then
    log_message "ERROR: No single DISPLAY X-session found or multiple displays
detected"
    exit 1
fi

# Установка найденного display-кода в переменную DISPLAY
export DISPLAY="$display"
log_message "Setting DISPLAY to: $DISPLAY"

# Определение auth
xauth=""
log_message "Searching for Xauth file..."

# Обработка процессов Xorg
xauth_candidates=$(pgrep -x Xorg | while read pid; do
    /bin/ps -o cmd= -p $pid | awk -F "-auth" '{print $2}' | awk '{print $1}'
done)

log_message "Xauth candidates from Xorg processes: $xauth_candidates"

# Поиск xauth файла, точно соответствующего DISPLAY
found_xauth=""
display_num="${DISPLAY#:}"
log_message "Searching for xauth matching DISPLAY number: $display_num"

for candidate in $xauth_candidates; do
    if [ -r "$candidate" ]; then
        if echo "$candidate" | grep -q ":[^0-9]*\<${display_num}\>[^0-9]" ||
           echo "$candidate" | grep -q ":[^0-9]*\<${display_num}\>$"; then
            found_xauth="$candidate"
            log_message "Found xauth exactly matching DISPLAY: $found_xauth"
            break
        fi
    fi
done

if [ -z "$found_xauth" ]; then
    log_message "No xauth file found matching DISPLAY $DISPLAY in Xorg processes"
fi

xauth="$found_xauth"
```

```
# Если не нашли в процессах, пробуем домашнюю директорию пользователя
if [ -z "$xauth" ] || [ ! -r "$xauth" ]; then
    if [ -n "$desktopuser" ]; then
        user_home=$(eval echo "~$desktopuser")
        xauth="$user_home/.Xauthority"
        log_message "Trying user Xauth file: $xauth"
    fi
fi

# Финальная проверка доступности xauth
if [ -z "$xauth" ] || [ ! -r "$xauth" ]; then
    log_message "ERROR: Cannot access xauth file: $xauth"
    exit 1
fi

export XAUTHORITY=$xauth
log_message "Setting XAUTHORITY to: $XAUTHORITY"

# Применение xrandr ко всем подключенных мониторам
log_message "Starting monitor configuration..."

connected_monitors=$(xrandr | awk '/ connected/ {print $1}')
log_message "Found connected monitors: $connected_monitors"

if [ -z "$connected_monitors" ]; then
    log_message "ERROR: No connected monitors found"
    exit 1
fi

for monitor in $connected_monitors; do
    log_message "Configuring monitor: $monitor"
    if xrandr --output "$monitor" --auto; then
        log_message "Successfully configured monitor: $monitor"
    else
        log_message "ERROR: Failed to configure monitor: $monitor"
    fi
done

log_message "X11 display configuration completed successfully"
```

- сделать файл исполняемым:

```
sudo chmod +x /usr/local/bin/x-resize
```

Для масштабирования экрана приветствия для протокола SPICE выполнить:

- заблокировать автостарт `kscreen`, переименовав расширение или удалив данные файлы из указанных директорий: `/usr/share/fly-dm/autostart/greeter/kscreend_autostart.desktop`,

/usr/share/fly-dm/preload/greeter/kscreend_preload.desktop;

- сделать символьную ссылку на ярлык для автозапуска spice-vdagent для экрана приветствия:

```
sudo ln -s /etc/xdg/autostart/spice-vdagent.desktop /usr/share/fly-
dm/autostart/greeter/spice-vdagent.desktop
```

- перезапустить процесс fly-dm командой:

```
sudo systemctl restart fly-dm
```

Если файл /usr/bin/fly-monitor-hotplug.sh не является исполняемым или удален, то на экране приветствия масштабирование не выполняется.

Ограничение числа интерактивных сессий на РМ

Termidesk VDI поддерживает ограничение числа сессий пользователя, подключенного к РМ:

- для терминальных сессий Метапоставщика ограничение задается на этапе создания или редактирования сервисного фонда;
- для ВРМ и автономных машин число сессий ограничено одной. При этом для ОС Linux должна быть выполнена настройка модуля PAM (см. подраздел **Настройка модуля PAM без монтирования Перемещаемых Профилей**). Ограничение применяется после прохождения аутентификации пользователя на РМ и выполняется в следующей последовательности:
  - пользователь аутентифицируется на сервере Termidesk VDI;
  - пользователь аутентифицируется в гостевой ОС РМ;
  - модуль PAM выполняет аутентификацию и авторизацию по модулям, включая модуль «Агента виртуального рабочего места» - pam_tdsk;
  - модуль pam_tdsk получает значения, ограничивающие число сессий, у «Агента виртуального рабочего места»;
  - модуль pam_tdsk получает фактическое количество активных сессий в ОС;
  - в зависимости от полученных и фактических значений подключение пользователя будет разрешено или запрещено.

Настройка вызова виртуальной клавиатуры в ОС Astra Linux

Настройка позволяет отображать виртуальную клавиатуру в гостевой ОС Astra Linux. Это нужно для случаев, когда ОС не реагирует на передачу данных с физической клавиатуры пользовательской рабочей станции.

Настройка сочетания клавиш для вызова виртуальной клавиатуры применяется к пользователю, который подключается удаленно. При подготовке базового образа или терминального сервера необходимо задать системную настройку для всех подключающихся пользователей.

Для использования этой функции администратор может назначить сочетание клавиш **<Win>** + **<Ctrl>** + **<O>** команде fly-vkbd в пользовательских сессиях графического интерфейса Fly.

> После завершения настроек следует убедиться, что вызов виртуальной клавиатуры через ПО Termidesk Viewer доступен новым и ранее зарегистрированным пользователям.

Настроить отображение виртуальной клавиатуры можно одним из способов:

- добавить назначение сочетания клавиш в конфигурационный файл пользователя `~/.fly/keyshortcutrc`:

```
echo 'Mod4|Ctrl|o="fly-vkbd"' >> ~/.fly/keyshortcutrc
```

- назначить сочетание клавиш в графическом интерфейсе ОС Astra Linux. Для этого:
  - перейти «Звезда - Панель управления - Рабочий стол» и выбрать ярлык «Горячие клавиши Fly» (см. рисунок Расположение ярлыка «Горячие клавиши Fly»);

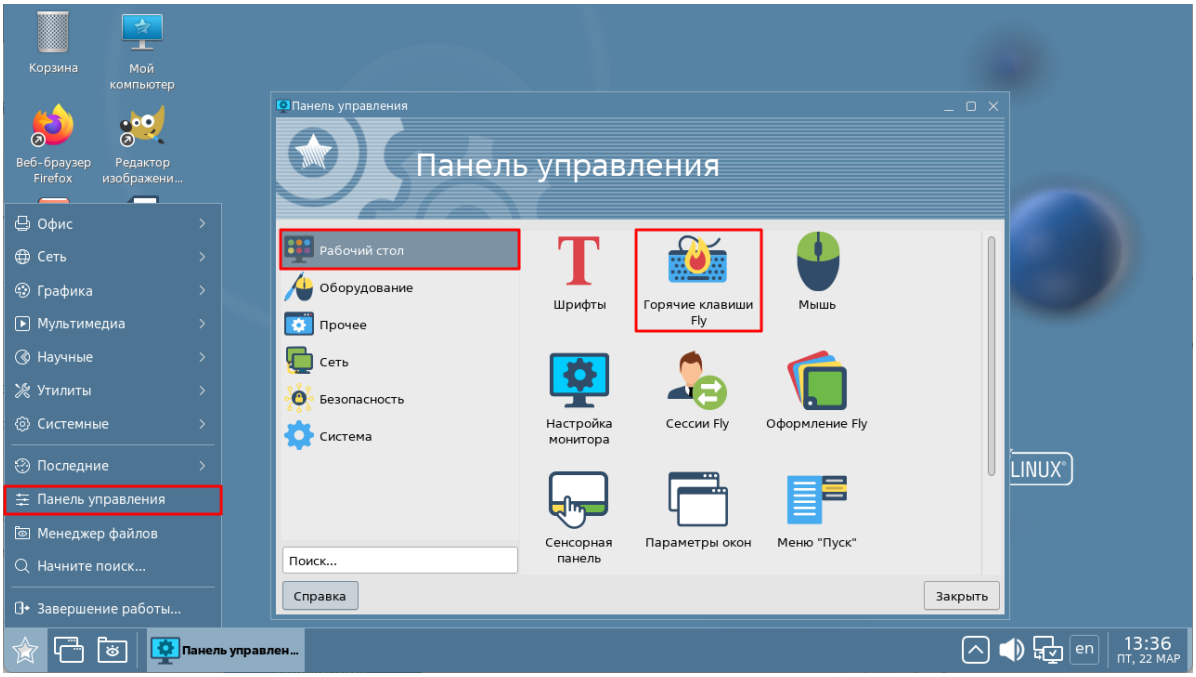


Рисунок 46. Расположение ярлыка «Горячие клавиши Fly»

  - в окне «Редактор горячих клавиш Fly» выбрать список «Клавиши для приложений» и нажать экранную кнопку **[+]** (см. рисунок Добавление команды вызова виртуальной клавиатуры);

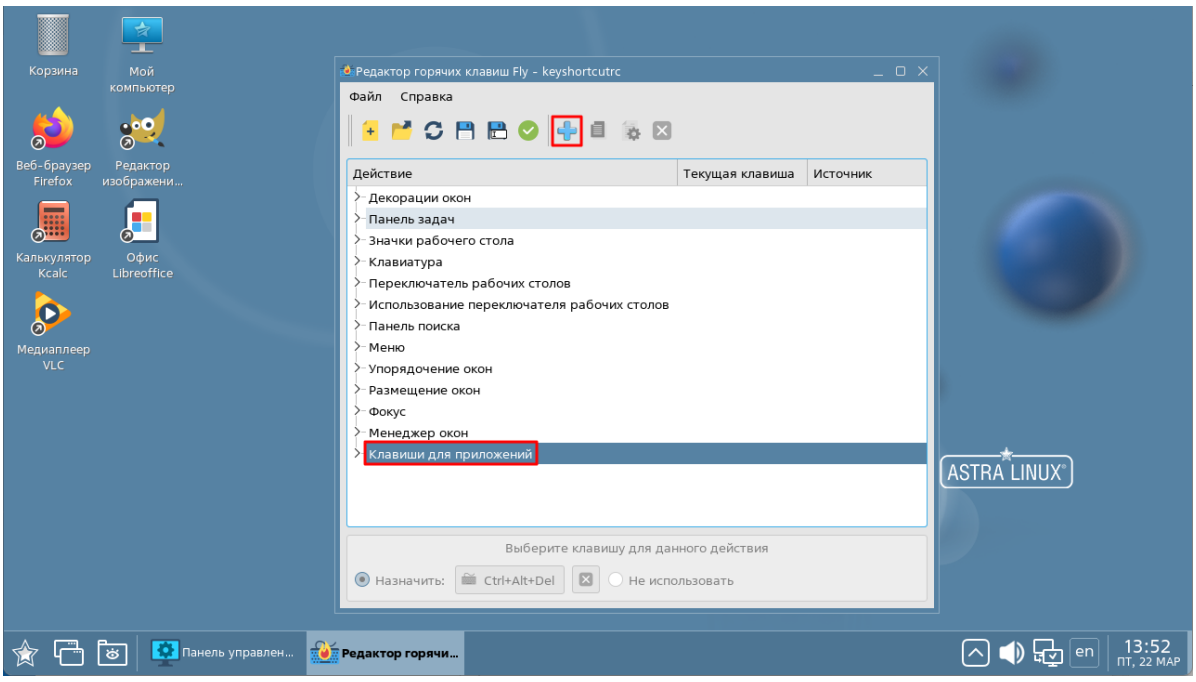


Рисунок 47. Добавление команды вызова виртуальной клавиатуры

- в окне «Выбор команды» ввести команду вызова виртуальной клавиатуры `fly-vkbd` и нажать экранную кнопку **[Да]** (см. рисунок Ввод команды вызова виртуальной клавиатуры);

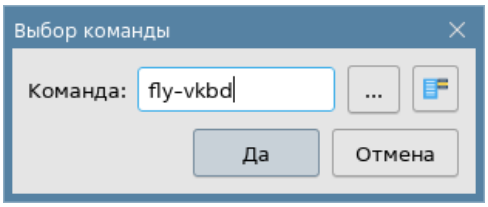


Рисунок 48. Ввод команды вызова виртуальной клавиатуры

- выделить созданное действие, в области «Выберите клавишу для данного действия» выбрать параметр «Назначить», нажать сочетание клавиш **<Win>** + **<Ctrl>** + **<O>** и нажать экранную кнопку **[Применить]** (см. рисунок Назначение сочетания клавиш вызова виртуальной клавиатуры).

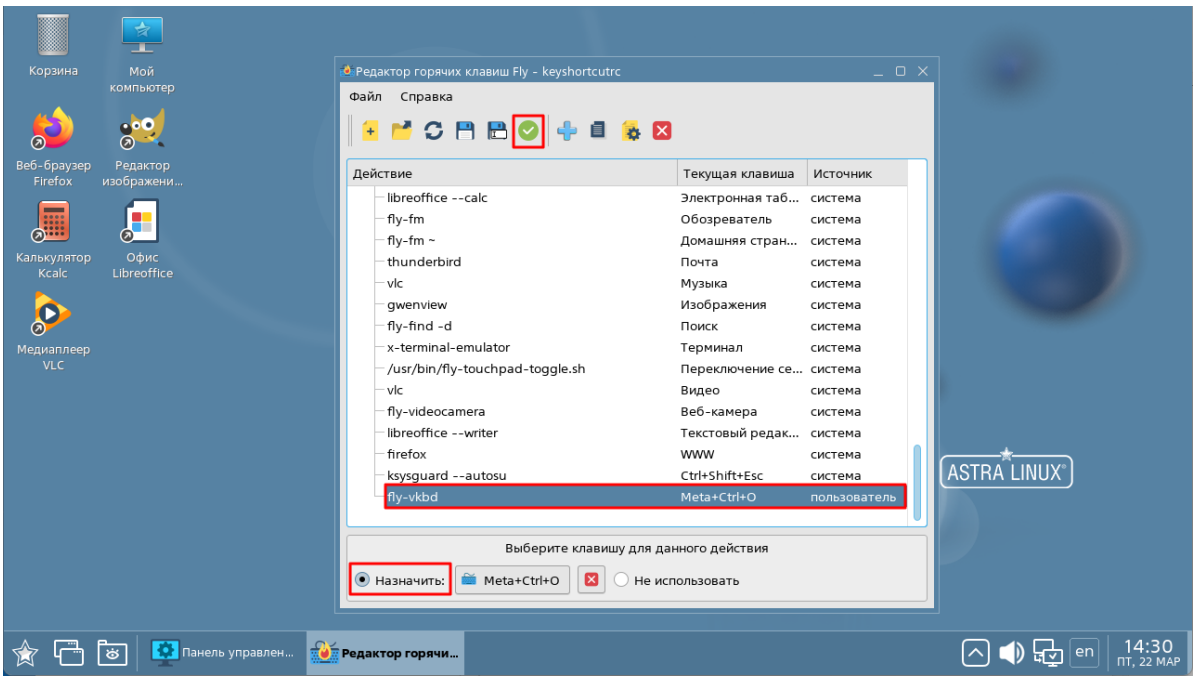


Рисунок 49. Назначение сочетания клавиш вызова виртуальной клавиатуры

Настройки для перенаправления принтеров

Для перенаправления принтера должны быть выполнены условия:

- в ОС пользовательской рабочей станции должен быть добавлен нужный принтер. Поддерживается перенаправление программных принтеров (например, программный виртуальный принтер PDF/XPS);
- в гостевой ОС РМ должен быть установлен нативный драйвер используемого принтера. При перенаправлении принтера в РМ через ПО Termidesk Viewer будет использован соответствующий драйвер:
  - «generic raw» - если печать будет выполняться в STAL или BPM;
  - нативный драйвер - при использовании полного функционала принтера;
- при использовании терминального сервера MS RDSH нужно разрешить перенаправление принтера в групповых политиках. Для этого:
  - открыть редактор групповой политики;
  - перейти «Конфигурация компьютера - Административные шаблоны - Компоненты Windows - Службы удаленных рабочих столов - Узел сеансов удаленных рабочих столов - Перенаправление принтеров» («Computer Configuration - Administrative Templates - Windows Components - Remote Desktop Services - Remote Desktop Session Host - Printer Redirection» в английской локализации);
  - задать параметру «Не разрешать перенаправление для клиентского принтера» значение «Отключена» («Do not allow client printer redirection» значение «Disabled» в английской локализации).

По умолчанию добавление принтера в гостевую ОС РМ не требуется.

Ручное добавление принтера может быть выполнено одним из способов:

- через существующую в гостевой ОС оснастку (например, «Менеджер печати Fly» для ОС Astra Linux Special Edition);
- через веб-интерфейс службы CUPS (для гостевой ОС Linux).

Для ручного добавления принтера через веб-интерфейс службы CUPS нужно:

- открыть в браузере URL-адрес: http://127.0.0.1:631/;
- перейти во вкладку «Администрирование». Выбрать пункт «Добавить принтер» и авторизоваться, использовав логин и пароль для входа в гостевую ОС;
- доступные принтеры будут отображены в списке «Найденные сетевые принтеры» (см. рисунок Список найденных сетевых принтеров). Выбрать принтер для добавления;

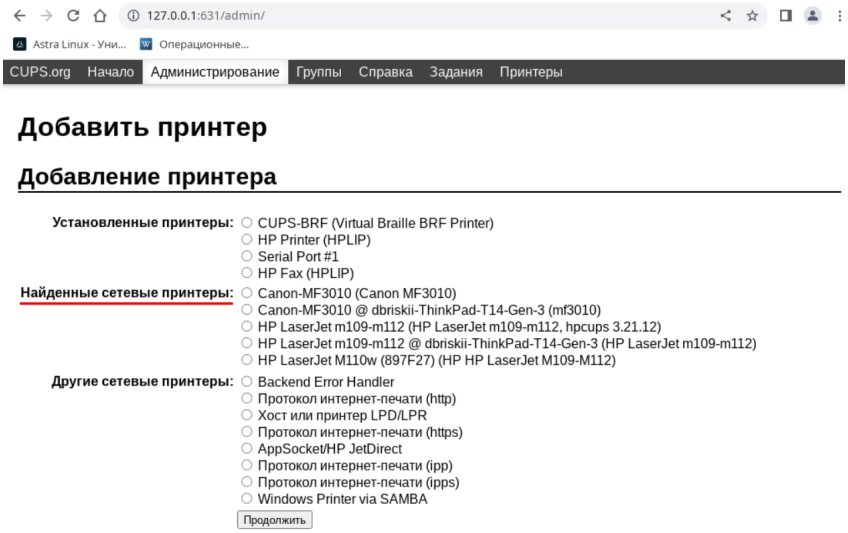


Рисунок 50. Список найденных сетевых принтеров

- убедиться, что в строке «Подключение» (см. рисунок Проверка URL) адрес начинается с «tdsk-prt»;

Настройка «tdsk-prt» актуальна при подключении по протоколу SPICE.

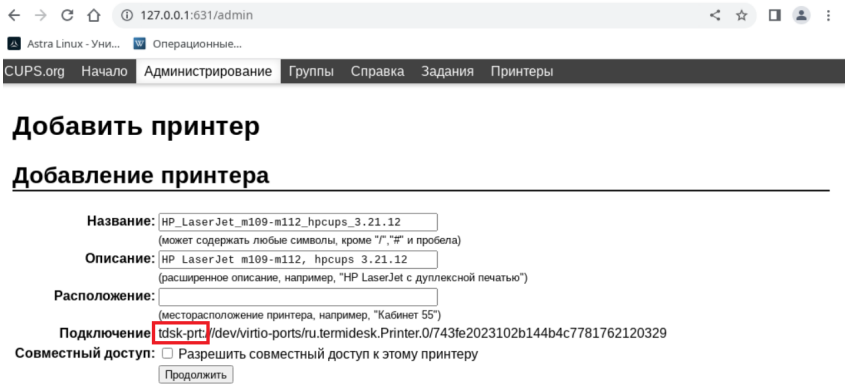


Рисунок 51. Проверка URL

- выбрать модель принтера из списка (см. рисунок Выбор модели принтера) или использовать файл драйвера принтера PPD;

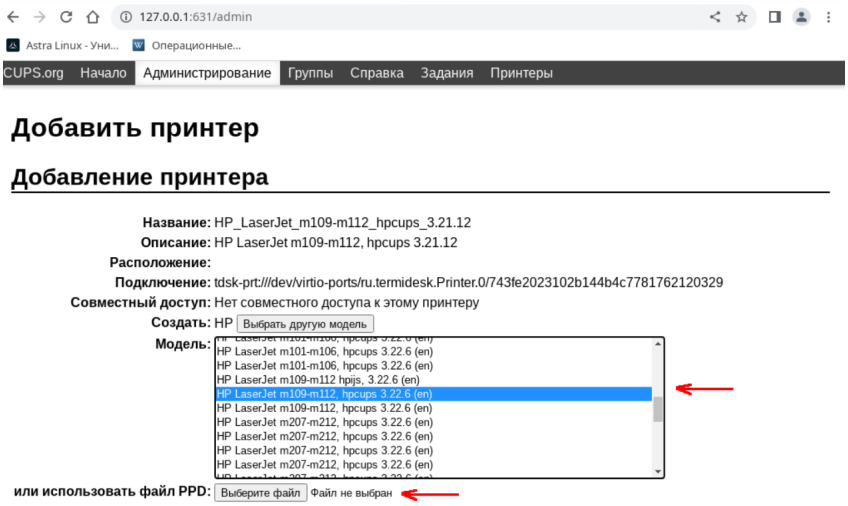


Рисунок 52. Выбор модели принтера

- завершить добавление принтера.

Если список «Найденные сетевые принтеры» пуст:

Настройка актуальна при подключении по протоколу SPICE.

- выбрать значение «Termidesk Virtual Printer» в списке «Другие сетевые принтеры» (см. рисунок Выбор другого сетевого принтера);

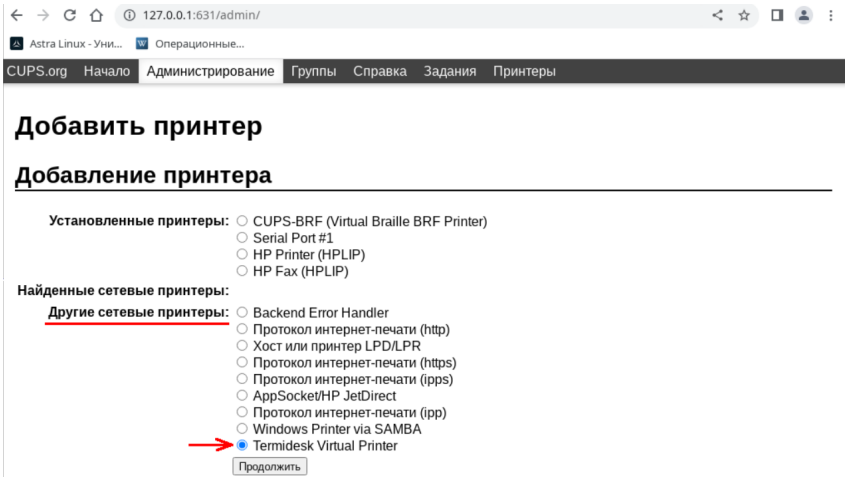


Рисунок 53. Выбор другого сетевого принтера

- перейти к интерфейсу командной строки (открыть программу «Терминал Fly») и выполнить:

```
cd /usr/lib/cups/backend
sudo ./tdsk-prt
```

- выбрать адрес нужного принтера и скопировать его в поле «Подключение» в браузере;

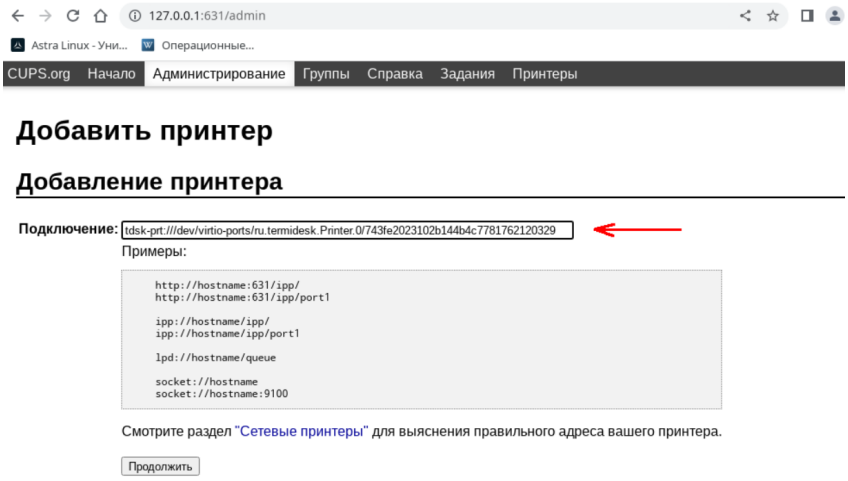


Рисунок 54. Добавление адреса принтера

- завершить добавление принтера аналогично описанию выше, когда список «Найденные сетевые принтеры» содержал записи.

Добавленный принтер должен отобразиться в менеджере печати (например, «Менеджер печати Fly») гостевой ОС.

При перенаправлении принтера из пользовательской рабочей станции на ОС Microsoft Windows в ВРМ на ОС Microsoft Windows доступны следующие конфигурации драйверов:

Настройка актуальна при подключении по протоколу RDP.

- использование нативных драйверов: установка нативных драйверов на пользовательской рабочей станции и ВРМ позволяет использовать весь функционал принтера, включая двустороннюю печать. Для корректного перенаправления принтера версии драйверов должны совпадать;
- использование универсального драйвера Microsoft Software Printer Driver: универсальный драйвер позволяет избежать установки драйверов для каждого принтера. При этом драйвер поддерживает только одностороннюю печать.

Для использования универсального драйвера на пользовательской рабочей станции с установленным ПО Termidesk Viewer нужно создать переменную окружения `TDSK_RDP_PRT_UNIVERSAL`. Для перенаправления принтера с использованием нативного драйвера переменную нужно удалить.

Настройка перенаправления каталога из пользовательской рабочей станции в РМ

Перенаправление каталога из пользовательской рабочей станции в РМ работает для протоколов SPICE, TERA и RDP. При этом:

- для протоколов RDP и TERA:
  - для ВРМ и терминального сервера STAL дополнительная настройка не выполняется;
  - для терминального сервера MS RDSH выполняется дополнительная настройка, как приведено ниже;
- для протокола SPICE выполняется дополнительная настройка гостевой ОС ВРМ, как приведено ниже;
- управление возможностью перенаправления осуществляется через политику «Перенаправление дисков и папок (RDP, SPICE, TERA)».

Для протокола TERA, установленного в ОС Linux необходимо убедиться, что в гостевой ОС соответствующие службы запущены:

```
sudo systemctl status tera-mounting-shdir-service
sudo systemctl --user status tera-webdav-service.service
```

Для гостевой ОС Astra Linux Special Edition:

- должны быть установлены пакеты `spice-webdavd`, `davfs2`, `autofs`:

```
sudo apt install -y spice-webdavd davfs2 autofs
```

- должны быть запущены службы `spice-webdavd.service` и `autofs.service`:

```
sudo systemctl status spice-webdavd.service autofs.service
```

- далее создать каталог для монтирования:

```
sudo mkdir /media/davfs
```

- создать файл `/etc/auto.master.d/spice-webdav.autofs` следующего содержания:

```
/-  /etc/auto.master.d/auto.localwebdav.mount
```

где:

`/-` - опция, указывающая утилите `autofs` выполнять монтирование по существующему пути вместо автоматического создания подкаталогов в корневой точке монтирования;

- создать файл `/etc/auto.master.d/auto.localwebdav.mount` следующего содержания:

```
/media/davfs -fstype=davfs,rw,dir_mode=0777,file_mode=666 :http\://localhost\:9843
```

где:

`/media/davfs` - каталог, в который будет происходить монтирование;

`-fstype=davfs,rw` - тип смонтированной файловой системы с правами на чтение и запись в нее (`rw`);

`dir_mode=0777,file_mode=666` - права, с которыми будут доступны файлы и каталоги. Рекомендуется не менять указанные значения для исключения случаев монтирования файловой системы от пользователя `root` и недоступности файлов при подключении через программу доставки РМ (ПО Termidesk Viewer);

- отредактировать файл `/etc/davfs2/secrets`, добавив строку:

```
"http://localhost:9843/" "" ""
```

где:

http://localhost:9843/ - место размещения файловой системы, по которому определяется устройство хранения для монтирования;

"" "" - логин и пароль пользователя, по умолчанию пусты для утилиты spice-webdav;

- перезапустить службу автоматического монтирования:

```
sudo systemctl restart autofs
```

Для гостевой ОС РЕД:

- установка пакетов spice-webdavd, davfs2, autofs выполняется через пакетный менеджер dnf:

```
sudo dnf install -y spice-webdavd davfs2 autofs
```

- остальные настройки перенаправления каталога по протоколу SPICE выполняются аналогично настройкам, приведенным для ОС Astra Linux Special Edition.

Для гостевой ОС Microsoft Windows:

- для ВРМ должен быть установлен пакет spice-webdavd (доступ: https://www.spice-space.org/download/windows/spice-webdavd/spice-webdavd-x64-latest.msi);
- для терминального сервера MS RDSH должен быть установлен модуль WebDAV Redirector. Установка выполняется через мастер добавления ролей и компонентов в ОС Misrosoft Windows Server. Для этого:
  - открыть мастер добавления ролей и компонентов;
  - в разделе «Компоненты» выбрать «Перенаправитель WebDAV»;
  - нажать экранную кнопку **[Установить]**;
- для терминального сервера MS RDSH нужно скорректировать ограничение на размер копируемых файлов (по умолчанию 50 МБ). Для этого:
  - перейти в реестре по пути HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters;
  - задать параметру FileSizeLimitInBytes нужный размер (в байтах).

После установки пакета в гостевой ОС Microsoft Windows произойдет следующее:

- будет добавлен сетевой диск;
- перенаправляемый каталог будет монтироваться в добавленный сетевой диск.

Перенаправление видеокамеры

Перенаправление видеокамеры позволяет передать по сети сжатое алгоритмом кодирования видео от устройств видеозахвата, подключенных к USB-шине пользовательской рабочей станции, на удаленное устройство, такое как ВРМ или терминальный сервер.

Виртуальная видеокамера определяется как видеоустройство веб-браузерами, программами видеоконференцсвязи, диагностическими утилитами и иными программами, работающими с устройствами захвата видео.

Для реализации функционала перенаправления видеокамеры:

- в гостевую ОС РМ должен быть установлен компонент «Видеоагент»;
- пользователю необходимо использовать специализированный клиент подключений - ПО Termidesk Viewer.

Возможность перенаправления видеокамеры определяется политикой «Перенаправление веб-камеры (RDP, SPICE, TERA)».

Перенаправление смарт-карты

Перенаправление смарт-карты позволяет передать подключенную к USB-шине пользовательской рабочей станции смарт-карту на удаленное устройство, такое как ВРМ или терминальный сервер.

Виртуальная смарт-карта определяется диагностическими утилитами и иными программами, работающими с устройствами подобного типа.

Для реализации функционала перенаправления смарт-карт:

- в гостевой ОС РМ должен быть установлен компонент «Агент виртуальных смарт-карт»;
- пользователю необходимо использовать специализированный клиент подключений - ПО Termidesk Viewer.

Возможность перенаправления смарт-карт определяется политикой «Перенаправление смарт-карт (RDP, SPICE, TERA)».

Аутентификация пользователей через носитель TouchMemory

Компонент «Клиент» Termidesk VDI поддерживает аутентификацию пользователя через носитель TouchMemory, а именно - через программный продукт «Сетевой модуль ТМ-аутентификации WinNET» производства ООО «Фирма ИнфоКрипт».

Поддерживаемые ОС:

- для пользовательской рабочей станции: ОС Microsoft Windows, Debian (только с графическим окружением GNOME);
- для ВРМ: ОС Microsoft Windows.

Для реализации функционала администратору необходимо установить в гостевую ОС ВРМ:

- ПО WinNET 3.1, при установке выбрать значение «Сервер с MsTS»;
- ПО Vitamin (сервер).

Функционал перенаправления часового пояса и синхронизации времени в РМ

Termidesk VDI поддерживает перенаправление часового пояса из пользовательской рабочей станции в РМ и синхронизацию времени между ними. Это происходит при создании пользовательской сессии: если функционал активирован, то при подключении пользователя из другого часового пояса время в его сессии не будет отличаться от локального времени пользовательской рабочей станции.

Функционал поддерживается для протоколов:

- RDP;
- TERA;
- SPICE.

Для работы функционала необходимо, чтобы:

- была активирована политика «Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)». «Агент виртуального рабочего места» получит значение временной зоны из запроса SSO и выставит его при создании пользовательской сессии;
- для гостевой ОС Linux были выполнены настройки, приведенные ниже. Для ОС Microsoft Windows дополнительная настройка не требуется.

Управление перенаправлением часового пояса осуществляется политикой «Перенаправление часового пояса пользователя (RDP, TERA, SPICE)».

Для работы механизма перенаправления часового пояса в ВРМ на базе ОС Linux необходимо выполнить настройку модуля `PAM` (`pam_tdsk`) в гостевой ОС. Для этого:

- убедиться, что выполнена подготовка базового ВРМ;
- создать файл `/usr/share/pam-configs/pam_tdsk` со следующим содержимым:

```
Name: Termidesk VDI PAM Timezone
Default: yes
Priority: 900
Session-Type: Additional
Session:
    optional pam_exec.so quiet /usr/bin/pam_tdsk --setenvonly
    optional pam_env.so user_readenv=1
```

- выполнить обновление профилей модуля `PAM`:

```
sudo pam-auth-update
```

- убедиться, что в файле `/etc/pam.d/common-session` появились строки с модулем `pam_tdsk`:

```
session      optional     pam_exec.so quiet /usr/bin/pam_tdsk --setenvonly
session      optional     pam_env.so user_readenv=1
```

Функционал выполнения скриптов в РМ

Функционал выполнения скриптов в РМ позволяет автоматизировать задачи, связанные с развертыванием РМ.

Скрипты размещаются в сетевом хранилище и запрашиваются при инициализации компонента «Агент виртуального рабочего места». Компонент должен иметь права на чтение каталога хранилища скриптов для корректного получения файлов и их выполнения на РМ.

Функционал передачи скриптов будет работать, если компоненты «Агент виртуального рабочего места» и «Универсальный диспетчер» настроены на взаимную аутентификацию по протоколу mTLS.

Поддерживаемые типы хранилищ скриптов перечислены в таблице (см. таблицу Список поддерживаемых хранилищ скриптов).

Таблица 12. Список поддерживаемых хранилищ скриптов

ОС РМ	Список поддерживаемых хранилищ скриптов
Linux	• NFS; • SMB
Microsoft Windows	• SMB

Для работы функционала нужно:

- убедиться, что выполнена подготовка базового ВРМ. Дополнительные настройки в ОС Microsoft Windows не требуются. В ОС Linux пакеты `nfs-utils` и `smbclient` являются рекомендуемыми зависимостями компонента «Агент виртуального рабочего места» и по умолчанию устанавливаются в ОС. Если пакеты отсутствуют в репозитории ОС, нужновыполнить настройки, приведенные ниже;
- для возможности получения скриптов из NFS-хранилища установить пакет `nfs-client`:

```
sudo apt install nfs-client
```

- запустить службу `rpc-statd`:

```
sudo systemctl start rpc-statd
```

- проверить монтирование каталога сетевого хранилища, выполнив:

```
mount -t nfs -o ro,soft nfs.termidesk.local:/var/scripts /tmp/scripts
```

где:

`-t nfs` - тип файловой системы сетевого хранилища;

`-o ro,soft` - монтирование каталога сетевого хранилища в режиме «только чтение» с мягкой обработкой ошибок;

`nfs.termidesk.local:/var/scripts` - IP-адрес или FQDN сетевого хранилища с указанием монтируемого каталога;

`/tmp/scripts` - каталог для монтирования файловой системы сетевого хранилища в РМ.

- для возможности получения скриптов из SMB-хранилища установить пакет `smbclient`:

```
sudo apt install smbclient
```

- проверить получение скрипта из SMB-хранилища, выполнив:

```
/usr/bin/smbclient //smb.termidesk.local/scripts -N -c 'get demo.sh
/var/run/termidesk/scripts/demo.sh'
```

где:

`//smb.termidesk.local/scripts` - путь к каталогу хранения скриптов на сетевом хранилище;

`-N` - флаг, отключает запрос данных для подключения к SMB-хранилищу;

`-c 'get demo.sh /var/run/termidesk/scripts/demo.sh'` - команда получает скрипт `demo.sh` и сохраняет его в каталог `/var/termidesk/scripts/`.

Настройка модуля PAM без монтирования Перемещаемых Профилей

Настройка модуля `PAM` (`pam_tdsk`) необходима для изменения конфигурации системы аутентификации, что требуется, например, при включении политики фонда РМ «Подключение с отличающимся именем пользователя».

Для настройки модуля `PAM` в гостевой ОС базового ВРМ нужно:

- выполнить подготовку базового ВРМ;
- создать файл `/usr/share/pam-configs/pam_tdsk` со следующим содержимым:
  - если требуется аутентификация через файл паролей `/etc/htpasswd`:

    ```
    Name: Termidesk VDI PAM
    Default: yes
    Priority: 901
    Auth-Type: Primary
    Auth:
    sufficient pam_exec.so expose_authtok quiet /usr/bin/pam_tdsk --htpasswd
    /etc/htpasswd
    ```

  - в остальных случаях:

    ```
    Name: Termidesk VDI PAM
    Default: yes
    Priority: 901
    Session-Type: Additional
    Session:
    required pam_exec.so quiet /usr/bin/pam_tdsk
    ```

- выполнить обновление профилей `PAM`:

```
sudo pam-auth-update
```

- убедиться, что в соответствующих файлах появилась строка с модулем `pam_tdsk`:
  - если использовался файл паролей `/etc/htpasswd`, то строка появится в `/etc/pam.d/common-auth`:

```
auth    sufficient pam_exec.so expose_authtok quiet /usr/bin/pam_tdsk
--htpasswd /etc/htpasswd
```

  - в остальных случаях строка появится в файле `/etc/pam.d/common-session`:

```
session    required pam_exec.so quiet /usr/bin/pam_tdsk
```

Настройка аутентификации пользователей ВРМ через файл

Действия по настройке аутентификации пользователей ВРМ через файл паролей сводятся к следующей последовательности шагов, выполняемых в гостевой ОС:

- задание файла для хранения паролей в модуле PAM;
- включение механизма автоматической авторизации в гостевую ОС. Механизм автоматической авторизации включается аналогично подразделу **Настройка технологии единого входа в гостевой ОС ВМ для протокола SPICE**.

> Termidesk VDI интегрирован со встроенным комплексом средств защиты информации ОС Astra Linux Special Edition. Идентификация и аутентификация, а также защита аутентификационной информации осуществляется средствами ОС.

Для задания файла хранения паролей в модуле PAM нужно отредактировать файл `/etc/pam.d/fly-dm`, добавив следующую строку перед секцией `@include common-auth`:

```
auth sufficient pam_exec.so expose_authtok quiet /usr/bin/pam_tdsk --htpasswd
/etc/htpasswd
```

Где `/etc/htpasswd` - путь к файлу с парами «логин:пароль» пользователей, имеющих право на автоматический вход в сессию.

Пример файла `/etc/pam.d/fly-dm`:

```
#%PAM-1.0
auth required pam_parsec_mac.so

auth    requisite       pam_nologin.so

auth    required        pam_env.so readenv=1
auth    required        pam_env.so readenv=1 envfile=/etc/default/locale
auth sufficient pam_exec.so expose_authtok quiet /usr/bin/pam_tdsk --htpasswd
/etc/htpasswd

@include common-auth
```

```
-auth   optional        pam_gnome_keyring.so
-auth   optional        pam_kwallet5.so

session required pam_parsec_mac.so unshare_root_only
session required        pam_limits.so
session  required       pam_loginuid.so

@include common-account
account required pam_parsec_mac.so labelselect=appset
@include common-session
session required pam_parsec_cap.so
session required pam_parsec_aud.so
session required pam_parsec_mac.so
-session optional       pam_gnome_keyring.so auto_start
-session optional       pam_kwallet5.so auto_start
@include common-password
```

Технология единого входа

Настройка технологии единого входа в гостевой ОС ВМ для протокола SPICE

Технология единого входа (автоматической авторизации) пользователя в гостевую ОС для протокола SPICE работает для:

- ОС Astra Linux Special Edition. При этом начиная с Termidesk VDI версии 4.3 достаточно только включить механизм автоматической авторизации в гостевую ОС, как написано ниже;
- ОС Microsoft Windows. При этом необходимо установить пакет переносимых библиотек из состава Visual Studio C++ в гостевую ОС: https://aka.ms/vs/17/release/vc_redist.x64.exe.

Технология управляется политикой фонда РМ «Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)».

Механизм автоматической авторизации в ОС Linux может быть включен через задание переменной `DM_LOGIN_AUTOMATION` со значением `1` в файле `/lib/systemd/system/fly-dm.service`.

Активация автоматической авторизации в ОС Linux влияет на настройку автоматического масштабирования экрана. Поэтому после активации этого механизма нужно проверить значение переменной окружения `DISPLAY` и скорректировать файл `/usr/local/bin/x-resize`, указав правильное значение для нее (см. подраздел **Автоматическое масштабирование экрана в ОС Astra Linux**).

Пример файла:

```
[Unit]
Description=The FLY login manager

#replaces getty
#Conflicts=getty@tty1.service
#After=getty@tty1.service
```

```
#replaces plymouth-quit  since it quits plymouth on its own
#Conflicts=plymouth-quit.service
#After=plymouth-quit.service

After=rc-local.service plymouth-start.service dbus.service systemd-user-
sessions.service libflygetexe-bin.service

#resposible for plymouth stopping, so if fails then make sure plymouth still stop
OnFailure=plymouth-quit.service

[Service]
ExecStartPre=/bin/bash -c /usr/bin/fly-dm-prepare.sh
ExecStart=/usr/bin/fly-dm vt7

IgnoreSIGPIPE=no

EnvironmentFile=-/etc/default/locale
Environment="DM_LOGIN_AUTOMATION=1"

[Install]
Alias=display-manager.service
```

После включения автоматической авторизации необходимо выполнить перезапуск конфигурации загруженных модулей:

```
sudo systemctl daemon-reload
```

Настройка технологии единого входа в гостевой ОС ВМ для протокола TERA

Технология единого входа (автоматической авторизации) пользователя в гостевую ОС для протокола TERA работает для:

- ОС Astra Linux Special Edition. При этом достаточно только включить механизм автоматической авторизации в гостевую ОС аналогично протоколу SPICE. Технология управляется политикой фонда РМ «Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)»;
- ОС Microsoft Windows. Для использования технологии нужно:
  - активировать параметр `TERA_CRED_PROVIDER` в каталоге реестра `HKEY_LOCAL_MACHINE\SOFTWARE\UVEON\Termidesk TERA` (см. подраздел **Каталог реестра `HKEY_LOCAL_MACHINE\SOFTWARE\UVEON\Termidesk TERA`** документа СЛЕТ.10001-01 90 09 «Руководство администратора. Настройка компонента TERA»);
  - политике фонда РМ «Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)» присвоить значение «Включен».

Настройка технологии единого входа в гостевой ОС ВМ для протокола RDP

Технология единого входа (автоматической авторизации) пользователя в гостевую ОС для протокола RDP поддерживается средствами самого протокола.

Автоматический вход включается для RDP при использовании хотя бы одного из условий:

- использование функционала PKINIT (аутентификация по смарт-карте) в свойствах домена аутентификации;
- использование в политике «Аутентификация на уровне сети (RDP)» значения «NLA» или «TLS».

Активация технологии единого входа на терминальном сервере MS RDS

Для включения SSO на MS RDS необходимо выполнить следующую последовательность шагов:

- на контроллере домена MS AD создать групповую политику с названием SSO;
- в созданную групповую политику внести следующие изменения:
  - в редакторе групповой политики перейти «Конфигурация компьютера - Административные шаблоны - Система - Передача учетных данных», выбрать параметр «Разрешить передачу учетных данных, установленных по умолчанию» и присвоить ему значение «Включено». Затем нажать экранную кнопку **[Добавить серверы в список]** и задать значение «TERMSRV/disp.termidesk.local», где `disp.termidesk.local` - имя узла с «Универсальным диспетчером» Termidesk VDI. Далее нажать экранные кнопки **[OK]** и **[Применить]** (см. рисунок Редактирование параметра «Разрешить передачу учетных данных, установленных по умолчанию» групповых политик);
  - в этом же списке выбрать параметр «Разрешить передачу новых учетных данных с проверкой подлинности сервера «только NTLM» и присвоить ему значение «Включено». Затем нажать экранную кнопку **[Добавить серверы в список]** и задать значение «TERMSRV/disp.termidesk.local». Далее нажать экранные кнопки **[OK]** и **[Применить]**;
  - в редакторе групповой политики перейти «Конфигурация компьютера - Административные шаблоны - Компоненты Windows - Службы удаленных рабочих столов - Клиент подключения к удаленному рабочему столу», выбрать параметр «Запрашивать учетные данные на клиентском компьютере» и присвоить ему значение «Отключено».

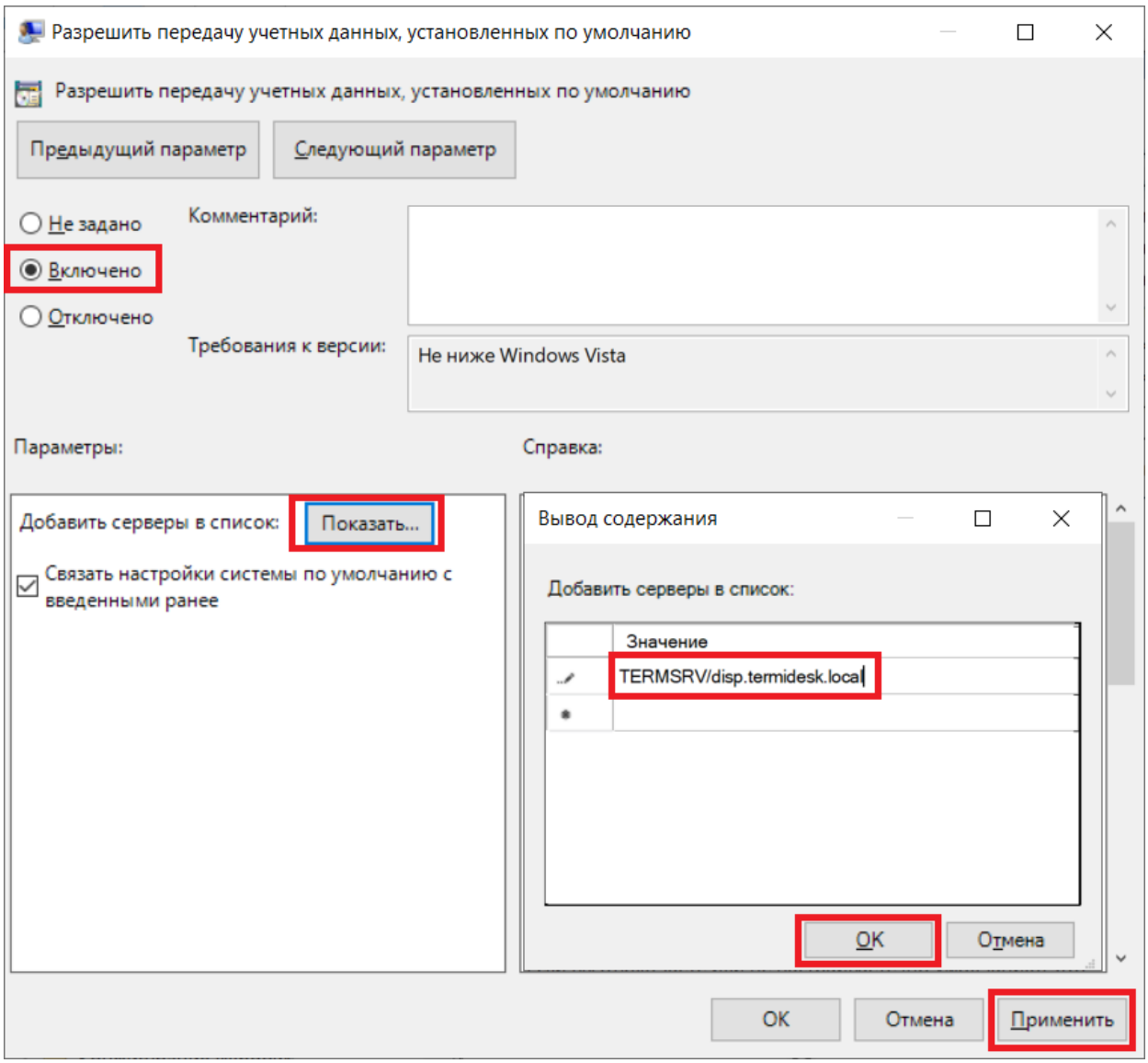


Рисунок 55. Редактирование параметра «Разрешить передачу учетных данных, установленных по умолчанию» групповых политик

По умолчанию время гарантированного автоматического применения изменений соответствует интервалу 90 – 120 минут после обновления файлов групповых политик на контроллере домена. Если необходимо форсировать применение политики, то на контроллере домена, MS RDS и рабочих станциях пользователей необходимо выполнить команду `gpupdate /force`.

Настройка технологии единого входа для Kerberos-аутентификации

Единый вход для Kerberos-аутентификации поддерживается для сценариев домена MS AD:

- протокол RDP:
  - подключение из ОС Astra Linux Special Edition в гостевую ОС Microsoft Windows, терминальный сервер MS RDSH, терминальный сервер STAL;
  - подключение из ОС Microsoft Windows в гостевую ОС Microsoft Windows, терминальный сервер MS RDSH, терминальный сервер STAL;
- протокол TERA:
  - подключение из ОС Astra Linux Special Edition в гостевую ОС Astra Linux Special Edition;
  - подключение из ОС Microsoft Windows в гостевую ОС Astra Linux Special Edition.

Работа для гостевой ОС Astra Linux Special Edition 1.7 (в частности 1.7.8) не гарантируется ввиду отсутствия в составе репозитория модуля проверки подлинности пользователя с помощью GSSAPI совместно с SSSD (`pam_sss_gss.so`).

Настройка TERA для Kerberos-аутентификации приведена в подразделе **Kerberos-аутентификация** документа СЛЕТ.10001-01 90 08 «Руководство администратора. Настройка компонента TERA».

Настройка терминального сервера STAL для Kerberos-аутентификации приведена в подразделе **Kerberos-аутентификация в STAL** документа СЛЕТ.10001-01 90 07 «Руководство администратора. Настройка компонента «Сервер терминалов».

Для корректной аутентификации гостевая ОС:

- должна быть введена в соответствующий домен аутентификации Kerberos, используемый в ферме Termidesk VDI и указанный в «Портале администратора». Настройка ввода в домен осуществляется из «Параметров гостевых ОС» в «Портале администратора»;
- должна быть предварительно настроена согласно описанию ниже.

Технология единого входа управляется политикой «Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)».

Для гостевой ОС Astra Linux Special Edition 1.8:

- убедиться, что в файле конфигурации службы `sssd` (`/etc/sssd/conf.d/*.conf`) заданы строки в секции настроек домена (если строк нет, то добавить):

```
ad_gpo_access_control = permissive
ad_gpo_ignore_unreadable = True
pam_gssapi_services = fly-dm
```

- убедиться, что в файле профиля PAM `/etc/pam.d/fly-dm` задана строка перед `@include common-auth` (если ее нет, то добавить):

```
auth sufficient pam_sss_gss.so
```

Для гостевой ОС Microsoft Windows (в том числе для терминального сервера MS RDSH) нужно настроить делегирование учетных данных:

- либо через групповую политику:
  - открыть редактор групповой политики;
  - перейти «Конфигурации компьютера - Административные шаблоны - Система - Передача учетных данных («Computer Configuration - Administrative Templates - System - Credentials Delegation» в английской локализации);
  - задать параметру «Удаленный узел позволяет делегирование неэскортируемых учетных данных» значение «Включена» («Remote host allows delegation of nonexportable credentials» значение «Enabled» в английской локализации);
- либо через реестр ОС Microsoft Windows, если настройка групповой политики по каким-либо причинам не применима:
  - открыть реестр и перейти к `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`;

- назначить параметру DisableRestrictedAdmin значение 0 (тип REG_DWORD).

Перемещаемые профили

Общие сведения по Перемещаемым Профилям

Перемещаемый Профиль - это средство для сохранения настроек и документов пользователя между сеансами работы в РМ. Он представляет собой образ диска или каталога с пользовательскими данными и настройками РМ.

В зависимости от ОС РМ реализация Перемещаемых Профилей может различаться:

- ОС Linux: рекомендуется использовать компонент Termidesk Profiles при размещении домашнего каталога пользователя на диске в qcow2-формате, расположенном в сетевом хранилище. Информация по назначению и установке компонента приведена в документе СЛЕТ.10001-01 90 11 «Установка и настройка Termidesk Profiles» (см. подразделы документа **Termidesk Profiles. Общие сведения**, **Подготовка среды функционирования**, **ОС Astra Linux Special Edition**);
- ПК СВ Брест (ОС Astra Linux Special Edition): может применяться альтернативный способ, подразумевающий настройку атрибутов диска и модуля PAM;
- ОС Microsoft Windows: Перемещаемые Профили размещаются во вложенных каталогах общего сетевого ресурса.

Настройка Перемещаемого Профиля для ПК СВ Брест

Общие действия по настройке

Существующие ограничения:

- функционал будет работать только для ОС Astra Linux Special Edition («Орел»);
- один диск Перемещаемого Профиля может быть подключен только к одной ВМ фонда РМ.

Действия по настройке Перемещаемого Профиля сводятся к следующей последовательности:

- создание базового образа диска для Перемещаемого Профиля в ПК СВ Брест;
- задание созданному образу атрибута TDSK_SHARED_TYPE со значением PRIVATE;
- настройка модуля PAM (pam_tdsk) в базовом ВРМ;
- активация механизма Перемещаемого Профиля в Termidesk VDI;
- активация политики «Отделяемый пользовательский профиль (RDP, SPICE, TERA)».

Создание базового образа диска в ПК СВ Брест

Для создания Перемещаемого Профиля (диска) на платформе ПК СВ Брест нужно:

- создать постоянный диск требуемого размера и подключить его к ВМ с установленной ОС Astra Linux. При создании выбрать шину SCSI (DEV_PREFIX=sd) или Virtio (DEV_PREFIX=vd);

При создании образа на шине Virtio может появиться сообщение об ошибке «Error attaching new VM Disk: Could not attach /var/lib/one/datastores/0/248/disk.2 (vdb) to one-248» при подключении диска в ПК СВ Брест версии 2.9. В случае возникновения такой ошибки нужно изменить атрибут DEV_PREFIX в свойствах образа диска.

- создать текстовый файл `/tmp/sfdisk.gpt` и привести его к виду:

```
label:gpt
type=773f91ef-66d4-49b5-bd83-d683bf40ad16
```

Тип раздела должен быть 773f91ef-66d4-49b5-bd83-d683bf40ad16.

- внести изменения в таблицу разделов на диске в соответствии с файлом `/tmp/sfdisk.gpt` при помощи утилиты `sfdisk`:

```
sudo sfdisk /dev/sdb < /tmp/sfdisk.gpt
```

В примерах используется обозначение диска `/dev/sdb`. Чтобы узнать, какое обозначение присвоено диску, необходимо воспользоваться утилитой `lsblk`.

- преобразовать новый раздел диска в формат `ext4`:

```
sudo mkfs.ext4 /dev/sdb1
```

- проверить успешность создания диска:

```
sudo lsblk -JO /dev/sdb1
```

где:

`-JO` - ключ для вывода всех столбцов в формате JSON.

Задание атрибутов созданному диску

Для задания атрибутов созданному ранее диску нужно:

- выключить ВМ и отключить диск от нее;
- в свойствах диска добавить атрибут `TDSK_SHARED_TYPE` со значением `PRIVATE`. Запомнить идентификатор (ID) диска (см. рисунок Окно просмотра ID диска в ПК СВ Брест).

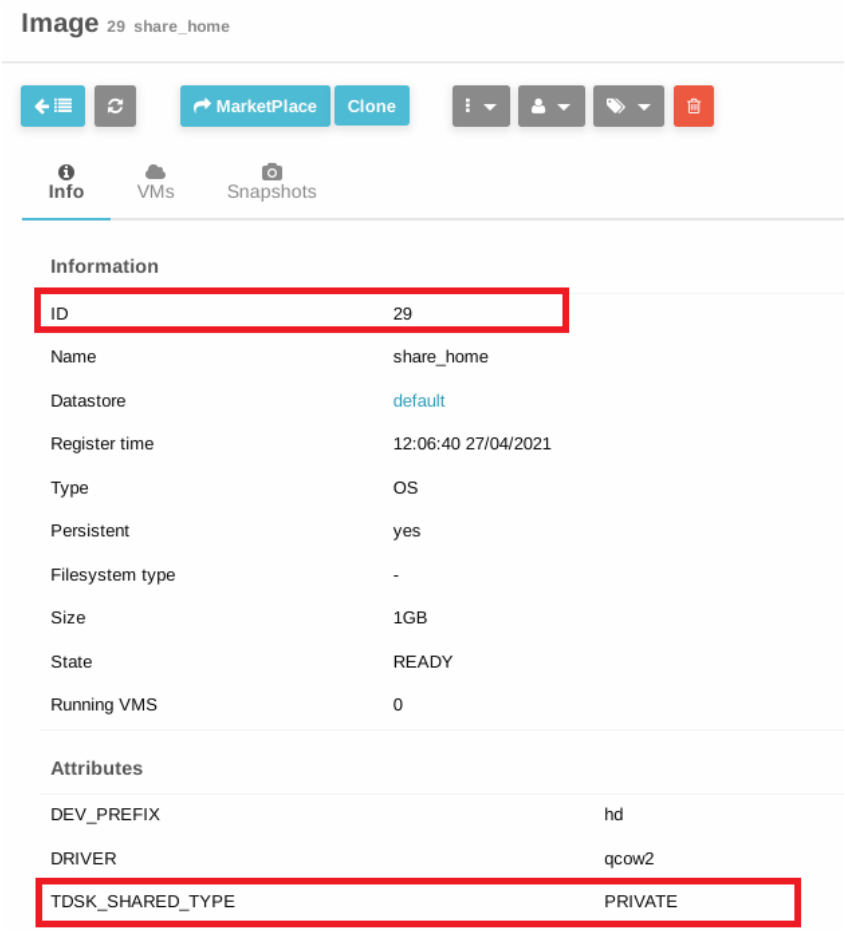


Рисунок 56. Окно просмотра ID диска в ПК СВ Брест

Настройка модуля PAM в базовом ВРМ

Для настройки модуля PAM в гостевой ОС базового ВРМ нужно:

- выполнить подготовку базового ВРМ;
- создать файл `/usr/share/pam-configs/pam_tdsk` со следующим содержимым:

```
Name: Termidesk VDI session
Default: yes
Priority: -1
Session-Interactive-Only: yes
Session-Type: Additional
Session:
required        pam_exec.so     /usr/bin/pam_tdsk --autofs --skel=/etc/skel
--chmod=700 --uid-ext-range 65536-2000000000
```

Параметр `--uid-ext-range` должен иметь минимальное значение `65 536`, максимальное значение `4 000 000 000`.

Максимальная граница диапазона зависит от используемого домена в сети, от настроек отображения идентификаторов пользователей домена в идентификаторы пользователей ВРМ.

Приоритет `Priority: -1` задан для того, чтобы домашний каталог (файл

> /usr/share/pam-configs/mkhomedir, Priority: 0) был создан прежде, чем будет выполнено подключение диска.

- выполнить обновление профилей PAM:

```
sudo pam-auth-update
```

- убедиться, что в файле /etc/pam.d/common-session появилась строка с модулем pam_tdsk:

```
session required        pam_exec.so     /usr/bin/pam_tdsk --autofs --skel=/etc/skel
--chmod=700 --uid-ext-range 65536-2000000000
```

Активация механизма Перемещаемого Профиля в Termidesk

Для активации механизма Перемещаемого Профиля в «Портале администратора» Termidesk VDI нужно перейти «Системные параметры - Системные настройки - Общие», затем в параметре «Список шаблонов подключаемых профилей в ПК СВ Брест» указать идентификатор образа диска для хранения Перемещаемого Профиля.

> Ранее активация механизма Перемещаемого Профиля выполнялась в конфигурационном файле /etc/opt/termidesk-vdi/termidesk.conf в параметре TDSK_AUTOFS_IMAGES_ID.

Активация политики в интерфейсе Termidesk

Для активации политики «Отделяемый пользовательский профиль (RDP, SPICE, TERA)» в «Портале администратора» Termidesk VDI следует перейти «Рабочие места - Глобальные политики», затем параметру «Отделяемый пользовательский профиль (RDP, SPICE, TERA)» присвоить значение «Включен».

Настройка Перемещаемых Профилей для ОС Microsoft Windows

Настройка Перемещаемых Профилей является опциональной. Действия по настройке сводятся к следующей последовательности:

- подготовка сетевого ресурса для централизованного хранения Перемещаемых Профилей пользователей, позволяющего им получать доступ к одному и тому же Профилю на всех серверах узла сеансов удаленных рабочих столов, настроенных на использование этого общего сетевого хранилища;
- включение в настройках фонда РМ политик «Использование обязательных профилей на сервере узла сеанса удаленных рабочих столов (RDP)» и «Путь для перемещаемого профиля пользователя служб удаленного рабочего стола (RDP)». Есть особенности работы политик фермы Termidesk VDI и политик контроллера домена (см. подраздел **Политики**);
- публикация фонда РМ.

Перемещаемые Профили пользователей будут содержаться во вложенных каталогах на указанном в политике «Путь для перемещаемого профиля пользователя служб удаленного рабочего стола (RDP)» сетевом ресурсе. Каталоги будут созданы автоматически после подключения пользователей и названы по имени учетной записи каждого пользователя %USERNAME%.

Технология бездисковой (сетевой) загрузки

Назначение бездисковой загрузки

Бездисковая загрузка - метод, позволяющий загружать ОС РМ, не имеющих собственного жесткого диска с предустановленным дистрибутивом, и предоставлять их пользователям для подключения через компонент «Клиент».

Корневая файловая система РМ хранится удаленно и транслируется по сети, что упрощает администрирование и централизованное управление РМ.

При использовании метода исключается необходимость установки ОС на машине РМ: все они используют единый эталонный образ системы, а вносимые изменения хранятся локально в слоях, специфичных для каждой машины.

с одного эталонного образа системы может загружаться несколько машин РМ. Например, для автономных машин это настраивается перечислением MAC-адресов машин в шаблоне РМ поставщика ресурсов (см. подраздел **Шаблон РМ для автономной машины с сетевой загрузкой**).

Компоненты инфраструктуры бездисковой загрузки

Для работы бездисковой загрузки требуется выделенный сервер, предоставляющий среду для сетевой загрузки. Он состоит из трех основных служб, работающих в изолированной подсети РМ (во избежание пересечения потоков данных с трафиком управления фермы Termidesk VDI):

- DHCP-сервер: работает в подсети машин РМ бездисковой загрузки. При загрузке выдает машинам IP-адреса и критически важные параметры, указывающие путь к следующим компонентам загрузки (TFTP и серверу Termidesk VDI);
- TFTP-сервер: хранит и передает машинам РМ по запросу первоначальный загрузчик и сопутствующие файлы (конфигурации, сертификаты и пр.). Автономная машина получает эту информацию на основе данных, предоставленных DHCP;
- iSCSI-сервер (транслятор блочных устройств): транслирует в сеть блочное устройство, которое воспринимается автономной машиной как локальный диск. В качестве источника выступает файл-образ (`.img`), содержащий эталонную корневую файловую систему. Доступ настраивается через конфигурационный файл сервера.

Состав тестового стенда для быстрого развертывания приведен в таблице (см. таблицу Состав тестового стенда для бездисковой (сетевой) загрузки).

Сервер для бездисковой (сетевой) загрузки может настраиваться на уже существующем узле, но с соблюдением требований к DHCP- и DNS-сервисам:

- наличие в конфигурации DHCP-опции `93`. Это обязательное значение кода, зарезервированное программно, указывает на архитектуру загрузки, Legacy или UEFI: `option arch code 93 = unsigned integer 16`;
- наличие в конфигурации DHCP-опции `224`. Значение кода может быть другим при необходимости, оно указывает на адрес сервера Termidesk: `option termidesk-server code 224 = text`;
- наличие в конфигурации DHCP-опции `225`. Значение кода может быть другим при необходимости, оно указывает на версию API «Универсального диспетчера»: `option termidesk-api-version code 225 = text`;
- наличие в конфигурации DHCP-опции `226`. Значение кода может быть другим при необходимости, оно указывает на адрес Syslog-сервера:

`option syslog-server code 226 = text`;

- наличие в конфигурации отдельного пространства DHCP-опций для iPXE: `option space ipxe`;
- наличие в конфигурации DHCP-опции `176` для iPXE-загрузчика. Это значение кода зарезервировано проектом iPXE и указывает на режим выполнения дополнительного PXE-DHCP-запроса: `option ipxe.no-pxedhcp code 176 = unsigned integer 8`;
- наличие отдельной подсети для загрузки машин РМ.

Указанные опции передаются машинам РМ при загрузке по сети.

Таблица 13. Состав тестового стенда для бездисковой (сетевой) загрузки

Узел	Описание
Серверная часть	
Сервер для бездисковой (сетевой) загрузки	Узел, предоставляющий сервисы DHCP, DNS и iSCSI. Может быть реализован на ВМ или на физическом узле. Требования: • установленная чистая ОС Astra Linux Special Edition 1.8.4; • наличие свободного сетевого интерфейса для создания подсети автономных машин (в примерах используется подсеть 172.16.0.0/24); • наличие минимум 60 Гб свободного объема диска для создания iSCSI-диска; • наличие сетевого интерфейса с доступом к сети Интернет для работы с репозиториями и зависимостями пакетов. Может быть реализован на втором сетевом интерфейсе
Сервер Termidesk	Узел с установленным компонентом «Универсальный диспетчер» («Портал администратора», «Портал пользователя» - могут быть установлены как на одном узле, так и на отдельных). Требования: • наличие доступа к подсети машин РМ
Узел подготовки образа для блочного устройства	

Узел	Описание
Узел с подключенным образом ОС Astra Linux Special Edition	Узел для подготовки образа ОС на удаленном iSCSI-устройстве. В общем случае может быть как ВМ, так и физической машиной. Подготовленный образ будет использоваться при загрузке РМ. В дальнейшем узел не используется. При необходимости изменения образа узел можно сконфигурировать повторно. Требования: • наличие подключенного Live-образа ОС Astra Linux Special Edition 1.8.4, узел должен быть загружен с него; • наличие сетевого интерфейса, подключенного к подсети машин РМ (172.16.0.0/24); • наличие сетевого интерфейса с доступом к сети Интернет для загрузки исходного кода iPXE-загрузчиков, работы с репозиториями и зависимостями пакетов
Машина РМ	
ВМ или физическая машина	Узел, являющийся РМ для подключения пользователя. Этот узел: • получает блочное устройство по сети; • загружается с полученного устройства. Требования: • наличие не менее 2 локальных дисков (они могут быть неформатированными). Суммарный размер каждого из них должен быть не менее размера корневой системы (root-слоя); • наличие сетевого интерфейса, подключенного к подсети автономных машин (172.16.0.0/24); • загрузка по сети должна быть включена в свойствах машины. Например, если в тестовом стенде используется ВМ с VirtualBox: в свойствах ВМ перейти к опциям загрузки и активировать загрузку с интерфейса «NIC»
Пользовательская часть	
Пользовательская рабочая станция	Узел, использующийся пользователем для подключения к серверу Termidesk и получения доступа к РМ

Процесс сетевой загрузки

Загрузка происходит строго по цепочке:

- машина РМ получает по DHCP IP-адрес и адрес TFTP-сервера;
- машина РМ загружает с TFTP-сервера начальный загрузчик;
- загрузчик инициализируется на машине РМ и отправляет запрос к серверу Termidesk VDI, передавая свой MAC-адрес;
- сервер Termidesk VDI идентифицирует машину РМ и отправляет ей конфигурацию с режимом загрузки;
- загрузчик подключается к iSCSI-серверу и получает доступ к образу корневой системы. Машина РМ воспринимает этот сетевой ресурс как обычное блочное устройство и начинает с него загрузку.

Технология наслоения (Overlay FS и работа с дисками)

Централизованное хранение системы требует наличие механизма, позволяющего каждому пользователю вносить изменения, не затрагивая общий эталонный образ. Для этого используется технология Overlay и минимум два локальных диска на машине РМ.

У каждой машины РМ должно быть два локальных диска. Они могут быть форматированными или неформатированными и не обязаны совпадать по размеру с корневым образом ОС.

После монтирования корневого раздела (только для чтения), поверх него накладываются слои для записи на локальных дисках машины РМ:

- слой 1 (read-only): эталонный корневой образ ОС с iSCSI-сервера. Является самым нижним слоем. Не может изменяться пользователем;
- слой 2 (read-write, слой установки): локальный диск. Хранит уникальную конфигурацию машины: hostname, сетевые настройки, ключи шифрования, хеши, «Агент виртуального рабочего места» и другие параметры, получаемые при первоначальной настройке;
- слой 3 (read-write, пользовательский слой): второй локальный диск. Создается после завершения конфигурации. Служит «черновиком» для всех изменений, вносимых пользователем и ОС в процессе работы: системные и прикладные журналы, временные файлы, данные пользовательских домашних каталогов (`/home`) и т.д.

Размер диска, выделенного под write-слой (слой 2 или 3), подбирается исходя из ожидаемого объема устанавливаемых пакетов и пользовательской работы. Общие рекомендации:

- слой 2 (read-write, слой установки): объем записываемых данных минимален, поэтому для него достаточно диска размером от 512 МБ (рекомендуемый минимум — 1 ГБ). Практика показывает, что занято может быть не более 30 МБ;
- слой 3 (read-write, пользовательский слой): размер задается исходя из ожидаемой пользовательской работы и не привязан к размеру корневого образа. Например, при корневом образе в 25 ГБ пользовательский диск может быть и 10 ГБ - это зависит от потребностей конкретного РМ.

Жизненный цикл и режимы загрузки

Управление машиной РМ осуществляется централизованно через сервер Termidesk («Универсальный диспетчер»), который определяет, в каком режиме загружать машину.

Режим настройки (Setup) используется при первом включении или для переконфигурации машины. Процесс выглядит следующим образом:

- загрузчик по команде с «Универсального диспетчера» монтирует слой 1 (root) и слой 2 (установки);
- загружается ОС, активируется «Агент виртуального рабочего места»;
- «Агент виртуального рабочего места» связывается с «Универсальным диспетчером», синхронизирует ключи, получает имя узла, настройки и сохраняет их на слой 2;
- процесс может потребовать нескольких циклов перезагрузки. «Универсальный диспетчер» будет отправлять машину в режим Setup до тех пор, пока «Агент виртуального рабочего места» не отправит сигнал о полной готовности.

Пользовательский режим (User) является рабочим режимом для конечного пользователя. Процесс выглядит следующим образом:

- после подтверждения готовности от «Агента виртуального рабочего места» «Универсальный диспетчер» при следующей загрузке отправит загрузчику команду на создание слоя 3;
- система загружается со всеми тремя слоями: поверх слоя установки (слой 2) накладывается пользовательский слой (слой 3). Пользователь может выполнять любые операции на машине, подключаясь к ней через ПО Termidesk Viewer. Все изменения записываются в слой 3.

Администратор может в любой момент очистить пользовательский слой 3, вернув машину в исходное состояние, или перевести ее обратно в режим Setup для изменения конфигурации слоя 2.

Настройка стека серверов для бездисковой загрузки

Установка необходимого набора пакетов

Для подготовки узла сервера для бездисковой (сетевой загрузки) выполнить:

- обновить список репозиториев:

```
apt-get update
```

- обновить дистрибутив ОС:

```
apt-get dist-upgrade -y
```

- установить набор пакетов:

```
apt-get install -y \
    isc-dhcp-server \
    tftpd-hpa \
    tgt \
    git \
    parted \
    unbound \
    curl \
    rsyslog
```

После установки у пакета `isc-dhcp-server` имеется набор конфигурационных файлов, которые необходимо удалить, предварительно сохранив их под другим именем:

```
mv -v /etc/dhcp/dhcpd6.conf /etc/dhcp/dhcpd6.conf.bak
mv -v /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.bak
```

Настройка конфигураций

Для упрощения настройки примеры конфигурации будут приводиться с учетом установки всех служб на одном узле.

> Файлы настройки конфигурации сделаны таким образом, чтобы при изменении версии API Termidesk VDI, или изменении IP-адресации, или изменении других параметров новые значения указывались только в одном месте конфигурации и через переменные автоматически применялись к другим конфигурациям, в которых они задаются.

DHCP (`isc-dhcp-server`)

Для настройки необходимо создать новый конфигурационный файл `/etc/dhcp/dhcpd.conf`:

```
cat > /etc/dhcp/dhcpd.conf <<EOF
# DHCP-опция 93 — Client System Architecture.
# Используется PXE-машинами для указания архитектуры загрузки.
#
# Примеры:
#   00:00 — BIOS / Legacy PXE
#   00:07 — UEFI x86_64
#
# По этой опции ниже выбирается загрузочный файл:
#   undionly.kpxe — для Legacy BIOS
#   ipxe.efi      — для UEFI
option arch code 93 = unsigned integer 16;


# ------------------------------------------------------------------------------
# Пользовательские DHCP-опции для Dynamic Diskless Loader / Termidesk
# ------------------------------------------------------------------------------

# DHCP-опция 224.
# Адрес Termidesk-сервера.
option termidesk-server code 224 = text;

# DHCP-опция 225.
# Версия API Termidesk-сервера.
option termidesk-api-version code 225 = text;

# DHCP-опция 226.
# Адрес Syslog-сервера.
option syslog-server code 226 = text;


# ------------------------------------------------------------------------------
# Пространство опций iPXE
# ------------------------------------------------------------------------------

# Объявление отдельного пространства DHCP-опций для iPXE.
option space ipxe;

# iPXE-опция 176 — no-pxedhcp.
#
```

```
# Значение 1 запрещает iPXE выполнять дополнительный PXE-DHCP-запрос.
option ipxe.no-pxedhcp code 176 = unsigned integer 8;


# ------------------------------------------------------------------------------
# Общие настройки DHCP-сервера
# ------------------------------------------------------------------------------

# Время аренды IP-адреса по умолчанию.
default-lease-time 600;

# Максимальное время аренды IP-адреса.
max-lease-time 7200;

# Отключение динамических DNS-обновлений.
ddns-update-style none;

# DHCP-сервер считается авторитетным для этой сети.
authoritative;


# ------------------------------------------------------------------------------
# Подсеть 172.16.0.0/24
# ------------------------------------------------------------------------------

subnet 172.16.0.0 netmask 255.255.255.0 {

    # ---------------------------------------------------------------------------
    # Статические DHCP-привязки
    # ---------------------------------------------------------------------------

    # Узел iSCSI-сервера с MAC-адресом 52:54:00:74:6d:a5 всегда будет получать
    # IP-адрес 172.16.0.2.
    host termidesk-iscsi-server {
        hardware ethernet 52:54:00:74:6d:a5;
        fixed-address 172.16.0.2;
    }


    # ---------------------------------------------------------------------------
    # Основные сетевые параметры
    # ---------------------------------------------------------------------------

    # Шлюз по умолчанию для машин этой подсети.
    option routers 172.16.0.1;

    # Маска подсети.
    option subnet-mask 255.255.255.0;
```

```
# DNS-сервер для клиентов.
#
# Он должен уметь разрешать имена, например:
#   termidesk.local
#   main.local
option domain-name-servers 172.16.0.1;

# DNS-домен для машин.
#
# Например, короткое имя:
#   termidesk
#
# может быть дополнено до:
#   termidesk.local
option domain-name "local";

# Динамический диапазон адресов.
#
# DHCP-сервер будет выдавать машинам адреса:
#   172.16.0.10 - 172.16.0.100
range 172.16.0.10 172.16.0.100;

# MTU интерфейса.
#
# 1400 может быть полезен для туннелей, VPN, overlay-сетей
# или проблем с фрагментацией.
option interface-mtu 1400;

# Время аренды IP-адреса именно для этой подсети.
default-lease-time 600;

# Максимальное время аренды именно для этой подсети.
max-lease-time 1800;


# ---------------------------------------------------------------------------
# Параметры iPXE
# ---------------------------------------------------------------------------

# Отключает дополнительный PXE-DHCP-запрос со стороны iPXE.
#
# Это делает загрузку предсказуемее, если все нужные параметры
# отдаёт этот DHCP-сервер.
option ipxe.no-pxedhcp 1;


# ---------------------------------------------------------------------------
# Параметры Dynamic Diskless Loader / Termidesk
# ---------------------------------------------------------------------------
```

```
# Адрес Termidesk-сервера.
#
# Передаётся машине PM через DHCP-опцию 224.
#
# Так как указано DNS-имя termidesk.local,
# машине нужен рабочий DNS-сервер 172.16.0.1.
option termidesk-server "termidesk.local";

# Версия API Termidesk.
#
# Передаётся клиенту через DHCP-опцию 225.
option termidesk-api-version "7.0";

# Адрес syslog-сервера.
#
# Вариант с DNS-именем:
#   option syslog-server "main.local";
#
# Вариант с IP-адресом надёжнее на ранней стадии загрузки,
# потому что не зависит от DNS.
#option syslog-server "main.local";
option syslog-server "172.16.0.1";


# ---------------------------------------------------------------------------
# Выбор загрузочного файла по архитектуре PXE-машины PM
# ---------------------------------------------------------------------------

# Если машина PM сообщила архитектуру 00:00,
# значит это Legacy BIOS / обычный PXE.
#
# Для него отдаём undionly.kpxe.
if option arch = 00:00 {
    filename "undionly.kpxe";

# Все остальные архитектуры считаем UEFI.
#
# Для UEFI отдаём ipxe.efi.
} else {
    filename "ipxe.efi";
}


# ---------------------------------------------------------------------------
# Список DHCP-опций, которые нужно отдать iPXE-машине PM
# ---------------------------------------------------------------------------

# Проверяем, что машина PM уже является iPXE.
```

```
#
# Обычно первый этап:
#   PXE firmware -> получает undionly.kpxe или ipxe.efi
#
# Второй этап:
#   iPXE -> снова делает DHCP-запрос с user-class = "iPXE"
#
# В этом блоке явно указываем, какие DHCP-опции iPXE должен запросить
# и получить от DHCP-сервера.
#if exists user-class and option user-class = "iPXE" {
    option dhcp-parameter-request-list
        1,    # subnet-mask
              # Маска подсети.

        3,    # routers
              # Шлюз по умолчанию.

        6,    # domain-name-servers
              # DNS-серверы.

        15,   # domain-name
              # DNS-домен, например local.

        26,   # interface-mtu
              # MTU интерфейса.

        66,   # tftp-server-name
              # Имя или IP-адрес TFTP-сервера.

        67,   # bootfile-name
              # Имя загрузочного файла.

        224,  # termidesk-server
              # Пользовательская опция с адресом сервера Termidesk.

        225,  # termidesk-api-version
              # Пользовательская опция с версией API Termidesk.

        226;  # syslog-server
              # Пользовательская опция с адресом syslog-сервера.
#}


# ---------------------------------------------------------------------------
# TFTP/PXE параметры
# ---------------------------------------------------------------------------

# IP-адрес next-server.
#
```

```
    # Для PXE это сервер, с которого машина PM должна забирать загрузочный файл.
    # Обычно это TFTP-сервер.
    next-server 172.16.0.1;

    # DHCP-опция 66 — tftp-server-name.
    #
    # Явно сообщает машине PM адрес TFTP-сервера.
    option tftp-server-name "172.16.0.1";
}
EOF
```

Затем указать серверу `isc-dhcp-server` имя сетевого интерфейса, на котором будет активирована конфигурируемая подсеть (в примере - `enp5s0`):

```
echo 'INTERFACESv4="enp5s0"' > /etc/default/isc-dhcp-server
```

DNS (`unbound`)

Для настройки необходимо создать новый конфигурационный файл `/etc/unbound/unbound.conf.d/diskless.conf`:

```
cat > /etc/unbound/unbound.conf.d/diskless.conf <<EOF
# ------------------------------------------------------------------------------
# Основной блок настроек DNS-сервера Unbound
# ------------------------------------------------------------------------------

server:

    # IP-адрес, на котором Unbound будет слушать DNS-запросы.
    #
    # В данном случае DNS-сервер доступен только на интерфейсе/адресе:
    #   172.16.0.1
    #
    # Это хорошо для изолированной загрузочной сети 172.16.0.0/24.
    interface: 172.16.0.1

    # Порт DNS-сервера.
    #
    # Стандартный DNS-порт:
    #   53
    port: 53


    # ------------------------------------------------------------------------------
    # Доступ к DNS-серверу
    # ------------------------------------------------------------------------------

    # Разрешить DNS-запросы с localhost.
```

```
#
# Нужно, чтобы сам сервер мог обращаться к локальному Unbound:
#   dig @127.0.0.1 termidesk.local
access-control: 127.0.0.0/8 allow

# Разрешить DNS-запросы из загрузочной сети.
#
# Машина из подсети 172.16.0.0/24 смогут использовать этот Unbound
# как DNS-сервер.
access-control: 172.16.0.0/24 allow


# ---------------------------------------------------------------------------
# Защита приватных адресов
# ---------------------------------------------------------------------------

# Запрещает получать приватные адреса 172.16.0.0/24 из внешнего DNS.
#
# Это защита от DNS rebinding и мусорных внешних ответов.
#
# Важно:
#   private-address не запрещает локальные записи local-data.
#
# Поэтому записи ниже:
#   termidesk.local -> 172.16.0.2
#   main.local      -> 172.16.0.1
#
# будут работать нормально.
private-address: 172.16.0.0/24


# ---------------------------------------------------------------------------
# Локальная DNS-зона
# ---------------------------------------------------------------------------

# Объявляет локальную DNS-зону local.
#
# Точка в конце обязательна:
#   "local."
#
# Тип static означает:
#   - Unbound сам отвечает за имена внутри зоны local.
#   - Если имени нет в local-data, Unbound вернёт NXDOMAIN.
#   - Запросы вида unknown.local не будут пересылаться наружу.
#
# Это правильно для внутренней зоны, где все нужные имена
# должны быть явно описаны.
local-zone: "local." static
```

```
    # ---------------------------------------------------------------------------
    # Локальные DNS-записи
    # ---------------------------------------------------------------------------

    # DNS-запись для сервера Termidesk.
    #
    # Полное имя:
    #   termidesk.local.
    #
    # IP-адрес:
    #   172.16.0.2
    #
    # В DHCP это имя используется здесь:
    #   option termidesk-server "termidesk.local";
    local-data: "termidesk.local. IN A 172.16.0.2"

    # DNS-запись для основного сервера загрузочной сети.
    #
    # Полное имя:
    #   main.local.
    #
    # IP-адрес:
    #   172.16.0.1
    #
    # Обычно на этом адресе находятся:
    #   - DHCP
    #   - DNS / Unbound
    #   - TFTP
    #   - iSCSI
    #   - syslog
    local-data: "main.local. IN A 172.16.0.1"


# ------------------------------------------------------------------------------
# Пересылка внешних DNS-запросов
# ------------------------------------------------------------------------------

forward-zone:

    # Зона "." означает корневую DNS-зону.
    #
    # То есть все запросы, которые Unbound не обслуживает локально,
    # будут пересылаться на forward-addr ниже.
    #
    # Например:
    #   google.com
    #   debian.org
    #   ntp.org
```

```
    name: "."

    # Основной upstream DNS-сервер.
    #
    # В данном случае это скорее роутер или DNS-сервер
    # во внешней сети 192.168.0.0/24 (это только пример).
    forward-addr: 192.168.0.1

    # Резервный внешний DNS-сервер.
    #
    # Будет использоваться, если 192.168.0.1 недоступен
    # или не отвечает.
    forward-addr: 8.8.8.8
EOF
```

Удаленный журнал (`rsyslog`)

Для настройки необходимо создать новый конфигурационный файл `/etc/rsyslog.d/diskless.conf`:

```
# Прием syslog по UDP/514
module(load="imudp")
input(type="imudp" port="514" ruleset="remote")

# Прием syslog по TCP/514
module(load="imtcp")
input(type="imtcp" port="514" ruleset="remote")

# Шаблон: складывать удаленные журналы по IP-адресу отправителя
template(name="RemoteByIP" type="string"
         string="/var/log/remote/%FROMHOST-IP%/syslog.log")

# Правила для удаленных журналов
ruleset(name="remote") {
    action(
        type="omfile"
        dynaFile="RemoteByIP"
        createDirs="on"
        dirCreateMode="0755"
        fileCreateMode="0644"
    )
    stop
}
EOF
```

Сервер `tftp`

iPXE-загрузчик может отправлять RRQ-запрос на TFTP-сервер с параметром размера блока (`blksize`) в 1468 байт. Сам TFTP-сервер может отбросить запрос с ошибкой: `tftp: client does`

`not accept options`.

В процессе договора между TFTP-сервером и iPXE-загрузчиком сервер отправляет OACK, а загрузчик по какой-то причине может не принимать согласование. В таком случае для решения проблемы стоит запустить TFTP-сервер с параметром `--refuse blksize`, который позволит передавать данные с размером блока в 512 байт:

```
sed -i 's/^TFTP_OPTIONS="--secure"$/TFTP_OPTIONS="--refuse blksize --secure"/'
/etc/default/tftpd-hpa
```

В результате:

- с `blksize`: iPXE-загрузчик запросит ускоренный режим, TFTP-сервер согласится, но машина РМ не загрузится (нештатная работа);
- без `blksize`: iPXE-загрузчик запросит ускоренный режим, TFTP-сервер проигнориует ускорение - произойдет обычная TFTP-передача, машина РМ загрузится (штатная работа).

Настройка сетевого интерфейса

Для настройки сетевого интерфейса выполнить:

В примере используются:

- имя сетевого интерфейса - enp5s0;
- имя профиля соединения - static-enp5s0;
- IP-адрес и маска подсети в формате CIDR: 172.16.0.1/24.

```
nmcli connection delete "static-enp5s0" >/dev/null 2>&1 || true
nmcli --offline connection add type ethernet \
    con-name "static-enp5s0" \
    ifname "enp5s0" \
    ipv4.addresses "172.16.0.1/24" \
    ipv4.method manual \
    > "/etc/NetworkManager/system-connections/static-enp5s0.nmconnection"
chmod 600 "/etc/NetworkManager/system-connections/static-enp5s0.nmconnection"
nmcli connection reload
nmcli connection up "static-enp5s0"
```

Перезапуск служб

После завершения настройки необходимо выполнить перезапуск соответствующих служб:

```
sudo systemctl restart isc-dhcp-server
sudo systemctl restart unbound
sudo systemctl restart rsyslog
sudo systemctl restart tftpd-hpa
```

Проверка работы настроенных служб

Для проверки работы воспользоваться командой:

```
netstat -tulnp
```

И убедиться, что в выводе команды есть информация о PID настроенных служб.

Сборка iPXE-загрузчика

Для сборки нужно:

- клонировать скрипт-инструмент для сборки образа из репозитория gitflic:

```
git clone https://gitflic.ru/project/azhirov-astralinux-ru/ipxe-tool.git
/root/ipxe-tool
```

- собрать образ с инструментами разработчика:

```
/root/ipxe-tool/ipxe.sh image build
```

- собрать iPXE-загрузчик:

```
mkdir -pv /srv/tftp
/root/ipxe-tool/ipxe.sh build --out-dir /srv/tftp -- --efi --legacy --default
--force
```

Для работы с iPXE-загрузчиком нужно сохранить базовую конфигурацию в `/srv/tftp`:

```
cat > /srv/tftp/boot.ipxe <<'EOF'
#!ipxe

# ------------------------------------------------------------------------------
# Определяем интерфейс, через который был получен PXE/iPXE-скрипт.
#
# Признак загрузочного интерфейса — наличие переменной filename.
# Обычно она появляется на том интерфейсе, через который DHCP/TFTP отдал
# начальный загрузочный файл.
# ------------------------------------------------------------------------------

echo Detect PXE boot interface...

# Проверяем net0.
# Если у интерфейса есть filename, считаем его загрузочным.
isset ${net0/filename} && set bootif net0 && goto bootif_found ||

# Проверяем net1.
```

```
# Если у интерфейса есть filename, считаем его загрузочным.
isset ${net1/filename} && set bootif net1 && goto bootif_found ||

# Если ни на одном интерфейсе filename не найден, значит iPXE не смог
# надёжно определить, через какой интерфейс была получена загрузка.
echo ERROR: PXE boot interface not found

# Показываем состояние всех сетевых интерфейсов для диагностики.
ifstat

# Оставляем пользователя в shell для ручной отладки.
shell


# ------------------------------------------------------------------------------
# Загрузочный интерфейс найден.
# ------------------------------------------------------------------------------

:bootif_found

echo Boot interface: ${bootif}

# Переходим в секцию настройки конкретного интерфейса:
#   net0 -> :net0_setup
#   net1 -> :net1_setup
goto ${bootif}_setup


# ------------------------------------------------------------------------------
# Настройка загрузки через net0.
# ------------------------------------------------------------------------------

:net0_setup

echo Use only net0

# Закрываем второй интерфейс, чтобы iPXE не пытался ходить через него.
# Это важно при нескольких сетевых картах, когда маршруты или DNS могут переехать.
ifclose net1

# Открываем net0.
ifopen net0 || goto failed

# Повторно получаем DHCP-настройки именно на net0.
# Так мы гарантируем, что IP, gateway, DNS, next-server и custom options
# относятся к нужному интерфейсу.
dhcp net0 || goto failed

# MAC-адрес загрузочного интерфейса в обычном виде.
```

```
set boot_mac ${net0/mac}

# MAC-адрес в hex/text-виде для передачи в URL.
set boot_mac_txt ${net0/mac:hex}

# IP-адрес, полученный по DHCP.
set boot_ip ${net0/ip}

# Gateway, полученный по DHCP.
set boot_gw ${net0/gateway}

# DHCP next-server, обычно адрес TFTP/boot-сервера.
set boot_next_server ${net0/next-server}

# DHCP option 226 — syslog-сервер.
# Не пишем сразу в переменную syslog, сначала сохраняем отдельно.
set syslog_server ${net0/226:string}

set termidesk_server ${net0/224:string}
set termidesk_api_version ${net0/225:string}

goto boot


# ------------------------------------------------------------------------------
# Настройка загрузки через net1.
# ------------------------------------------------------------------------------

:net1_setup

echo Use only net1

# Закрываем первый интерфейс, чтобы исключить случайную работу через net0.
ifclose net0

# Открываем net1.
ifopen net1 || goto failed

# Повторно получаем DHCP-настройки именно на net1.
dhcp net1 || goto failed

# MAC-адрес загрузочного интерфейса в обычном виде.
set boot_mac ${net1/mac}

# MAC-адрес в hex/text-виде для передачи в URL.
set boot_mac_txt ${net1/mac:hex}

# IP-адрес, полученный по DHCP.
set boot_ip ${net1/ip}
```

```
# Gateway, полученный по DHCP.
set boot_gw ${net1/gateway}

# DHCP next-server, обычно адрес TFTP/boot-сервера.
set boot_next_server ${net1/next-server}

# DHCP option 226 — syslog-сервер.
# Не пишем сразу в переменную syslog, сначала сохраняем отдельно.
set syslog_server ${net1/226:string}

set termidesk_server ${net1/224:string}
set termidesk_api_version ${net1/225:string}

goto boot


# ------------------------------------------------------------------------------
# Основная загрузка.
# ------------------------------------------------------------------------------

:boot

echo MAC: ${boot_mac}
echo IP: ${boot_ip}
echo GW: ${boot_gw}
echo Next server: ${boot_next_server}
echo Syslog DHCP option 226: ${syslog_server}

# Если DHCP option 226 не пришла, используем резервный syslog-сервер.
isset ${syslog_server} || set syslog_server 172.16.0.1

# Включаем syslog.
# После этой строки echo-сообщения должны уходить в syslog,
# если iPXE собран с поддержкой CONSOLE_SYSLOG.
set syslog ${syslog_server} || goto syslog_failed

echo Syslog enabled: ${syslog_server}
goto build_url


# ------------------------------------------------------------------------------
# Ошибка настройки syslog не должна обязательно ломать загрузку.
# Поэтому просто пишем предупреждение и продолжаем.
# ------------------------------------------------------------------------------

:syslog_failed

echo WARNING: failed to enable syslog: ${syslog_server}
```

```
goto build_url


# ------------------------------------------------------------------------------
# Формирование URL загрузочного скрипта.
# ------------------------------------------------------------------------------

:build_url

# Собираем URL запроса к Termidesk.
# MAC кодируем через uristring, чтобы символы вроде ':' корректно попали в URL.
set url
http://${termidesk_server}/api/agent/v${termidesk_api_version}/boot_script?mac=${bo
ot_mac_txt:uristring}

echo Chain: ${url}

# Загружаем следующий iPXE-скрипт с сервера.
chain ${url} || goto failed

# Если chain завершился успешно и вернулся обратно, завершаем работу.
exit


# ------------------------------------------------------------------------------
# Общая обработка ошибки загрузки.
# ------------------------------------------------------------------------------

:failed

echo ERROR: boot failed

# Показываем состояние интерфейсов.
ifstat

# Показываем таблицу маршрутизации.
route

# Оставляем shell для ручной диагностики.
shell
EOF
```

Настройка iSCSI (`tgt`)

Для настройки выполнить:

- создать диск машины РМ для iSCSI:

```
mkdir -pv /var/iscsi
```

```
fallocate -v -l "25G" /var/iscsi/test-disk.img
```

- создать конфигурацию:

```
cat > /etc/tgt/conf.d/test-disk.conf <<'EOF'
<target iqn.2026-06.local.ipxe:test-disk>
    <backing-store "/var/iscsi/test-disk.img">
        lun 1
        allow-in-use yes
    </backing-store>
</target>
EOF
```

- перечитать конфигурацию tgt:

```
tgt-admin --update ALL
tgtadm --mode target --op show
```

Для последующего обслуживания диска, при необходимости изменить конфигурацию ОС на нем, используется скрипт `mdisk`, доступный в Интернет-репозитории Termidesk: https://repos.termidesk.ru/Addons/Scripts/.

Скрипт монтирует `IMG`-диск для возможности его изменения.

Для использования скрипта нужно:

- скопировать его в файловую систему iSCSI-сервера. Для того чтобы при вызове скрипта не запрашивалось повышение прав пользователя, его можно разместить в каталоге `/usr/sbin`;
- перейти в каталог размещения скрипта командой `cd`;
- задать скрипту флаг выполнения:

```
sudo chmod +x mdisk
```

- вызывать скрипт и передать ему путь к iSCSI-диску:

```
sudo ./mdisk -i <путь_к_диску> -t /mnt
```

Например:

```
sudo ./mdisk -i /var/iscsi/test-disk.img -t /mnt
```

Где:

`-t /mnt` - точка монтирования, в примере используется каталог `/mnt`

Для вызова справки по работе со скриптом выполнить:

```
sudo ./mdisk --help
```

Для ввода РМ с бездисковой загрузкой в домен установить в гостевую ОС соответствующие пакеты:

- для домена MS AD - пакет `astra-ad-sssd-client`:

```
sudo apt install -y astra-ad-sssd-client
```

- для домена FreeIPA - пакет `astra-freeipa-client`;
- для домена ALD Pro - пакеты `astra-freeipa-client` и `aldpro-client`.

Инструкции по настройке гостевой ОС Astra Linux Special Edition для всех типов доменов приведены в разделе **Обязательная настройка гостевой ОС Astra Linux**.

Подготовка образа РМ ОС Astra Linux Special Edition на удаленном iSCSI-устройстве

Предварительные требования

К узлу подготовки образа должен быть подключен Live-образ ОС Astra Linux Special Edition 1.8.4 и узел должен быть загружен с него перед выполнением последующих действий.

Общие сведения о подготовке образа

Процесс подготовки образа выполняется пакетом `cdi` по специализированному сценарию, ориентированному на сетевые хранилища:

- подключение к целевому устройству: установщик инициализирует сетевое подключение к iSCSI-серверу. После успешного обнаружения целевого узла (Target) и логического тома (LUN) этот диск становится доступен для выбора в качестве основного носителя;
- стандартная установка: все последующие этапы (разметка диска, создание разделов, форматирование, копирование системных файлов) выполняются штатными средствами установщика;
- предварительная конфигурация: в процессе установки задаются базовые параметры системы: имя пользователя ОС и его пароль, а также уникальное сетевое имя узла (hostname) для его идентификации в инфраструктуре.

Критически важным этапом является настройка способности системы загружаться с сетевого ресурса. Поскольку корневой раздел находится удаленно, необходимо, чтобы iSCSI-подключение устанавливалось на самых ранних стадиях загрузки, до монтирования корневой файловой системы. Эту задачу решает специализированный пакет `ddl` (Dynamic Diskless Loader).

Интеграция пакета в образ происходит на этапе установки:

- установщику передается пакет `ddl`, уже содержащийся в пакете `cdi`;
- пакет `ddl` устанавливается в целевую систему, обеспечивая в дальнейшем корректную инициализацию iSCSI-соединения при каждом старте.

Весь процесс установки инициируется и контролируется штатным консольным

установщиком `astra-installer-console`. Его работа строится на основе заранее подготовленного `preseed`-файла, содержащего исчерпывающий набор предустановленных параметров, ответов на запросы и инструкций, что позволяет исключить ручной ввод и выполнить развертывание в автоматическом режиме.

Результатом установки является готовая ОС Astra Linux Special Edition на iSCSI-устройстве, сконфигурированная по заданным параметрам и способная к самостоятельной загрузке с сетевого хранилища. После завершения установки рекомендуется проверить настройки автоматического подключения iSCSI в готовой ОС и убедиться в корректности конфигурации загрузчика.

Установка необходимого набора пакетов

Для установки пакета `cdi` нужно:

- подключить Интернет-репозиторий Termidesk, либо скачать пакет напрямую из него: https://repos.termidesk.ru/astra/dists/1.8_x86-64/pool/non-free/vats/;
- выполнить:

```
sudo apt install -y <путь_к_пакету>
```

- в запросе установщика нажать экранную кнопку **[Продолжить]**.

В процессе установки потребуется:

В случае неожиданного завершения работы псевдографического интерфейса установки рекомендуется уменьшить окно консольного терминала.

- настроить подключение к удаленному iSCSI-устройству:
  - «Адрес»: IP-адрес или доменное имя iSCSI-сервера;
  - «Порт»: порт подключения. По умолчанию 3260;
- если параметры подключения были введены правильно и доступ к iSCSI-устройству есть, то на следующем шаге появится список целей (Target), доступных для дальнейшего подключения. Потребуется выбрать цель: если настройка сервера выполнялась по стандартным примерам конфигураций, то цель будет `iqn.2026-06.local.ipxe:test-disk`;
- выбрать блочное устройство для установки (например, `sda`). Количество блочных устройств зависит от настройки iSCSI-сервера (параметр `LUN`);
- настроить параметры ОС образа:
  - «Пользователь»: имя создаваемого пользователя ОС;
  - «Пароль»: пароль пользователя ОС;
  - «Имя компьютера»: имя узла (hostname);
- указать используемый пакет `ddl`:
  - «Использовать встроенный в CDI deb-пакет DDL»: будет использоваться пакет по-умолчанию;
- указать используемый пакет `termidesk-agent`
  - «Использовать встроенный в CDI deb-пакет Termidesk Agent»: будет использоваться пакет по-умолчанию;
- настроить подключение к серверу Termidesk VDI:

- «Адрес[:порт]»: IP-адрес или FQDN компонента «Универсальный диспетчер» («Портал администратора»);
- «Порт Агента»: порт «Агента виртуального рабочего места», который будет использоваться для взаимодействия;
- «Мастер ключ»: значение мастер-ключа для взаимодействия с компонентом «Универсальный диспетчер». Значение мастер-ключа можно получить в «Портале администратора», перейдя в «Системные параметры - Системные настройки - Безопасность» и скопировав значение параметра «Мастер-ключ»;

- настроить конфигурацию опций DHCP (настройка сервера выполнялась ранее):
  - «DNS-домен»: имя доменной зоны;
  - «Опция Termidesk сервера»: опция, настроенная на DHCP-сервере, отвечающая за адрес сервера Termidesk VDI;
  - «Опция Termidesk API версии»: опция, настроенная на DHCP-сервере, отвечающая за версию сервера Termidesk VDI («Универсального диспетчера»);
  - «Опция Syslog сервера»: опция, настроенная на DHCP-сервере, отвечающая за адрес Syslog-сервера;
- нажать экранную кнопку **[Начать установку]** и дождаться завершения установки и настройки образа ОС;
- по завершению установки нажать экранную кнопку **[Завершить]**, затем **[Выйти]**.

На этом этапе подготовка образа завершена. Далее необходимо перейти к настройке непосредственно сервера Termidesk.

Параметры работы утилиты `cdi`

Для гибкой настройки версий пакетов, управляемых через `cdi`, предусмотрена возможность вызова утилиты с указанием параметров, перечисленных в таблице (см. таблицу Доступные параметры утилиты `cdi`).

Просмотр справки по утилите `cdi` выполняется командой:

```
sudo cdi --help
```

Таблица 14. Доступные параметры утилиты `cdi`

Параметр	Описание
`--version`	Вывод версии утилиты
`-v`	Включение отладочного уровня журналирования. Подробность журналирования настраивается количеством указанных параметров (поддерживается 7 уровней): например, `-vv` будет выводить более подробные события, чем `-v`
`-l`, `--log-path`	Путь к файлу журнала. По умолчанию: `/var/log/cdi.log`
`-d`, `--ddl-value`	Путь к `deb`-пакету `ddl`, предоставляющего iPXE-загрузчик. Поддерживается указание URL-пути (с устройства должен быть доступ к этому URL)
`-a`, `--agent -path`	Путь к `deb`-пакету `termidesk-agent` («Агент виртуального рабочего места»). Поддерживается указание URL-пути (с устройства должен быть доступ к этому URL). По умолчанию в пакет `cdi` включен пакет `termidesk-agent` версии 6.1.1

Настройка узла сервера Termidesk

Настройка сводится к:

- добавлению поставщика ресурсов в зависимости от сценария использования.

Поддерживаются: «Автономные машины», «VMware vSphere»;

- добавлению шаблона «Сетевая загрузка (MAC)» в выбранном поставщике ресурсов (см. подразделы **Шаблон РМ для автономной машины с сетевой загрузкой**, **Шаблон РМ машины с сетевой загрузкой для платформы VMware vSphere**);
- созданию фонда РМ «Сетевая загрузка (MAC)» (см. подраздел **Добавление фонда сетевой загрузки**);
- выполнить настройку узла «Универсального диспетчера»:
  - добавить параметр `IPXE_SCRIPT_PATH` в файл `opt/termidesk/share/termidesk-vdi/src/config.py`:

    ```
    IPXE_SCRIPT_PATH=/opt/termidesk/share/termidesk-vdi/src/private/script.ipxe
    ```

  - создать файл `/opt/termidesk/share/termidesk-vdi/src/private/script.ipxe` со следующим содержимым:
    - для EFI-загрузки:

      ```
      #!ipxe
      sanboot --filename \EFI\astra\grubx64.efi {iscsi_target_name} || reboot
      ```

    - для Legacy-загрузки:

      ```
      #!ipxe
      sanboot {iscsi_target_name} || reboot
      ```

ДОМЕНЫ АУТЕНТИФИКАЦИИ

Добавление доменов аутентификации

Общие сведения о доменах аутентификации

Домен аутентификации - объект Termidesk VDI, являющийся источником сведений о субъектах и их полномочиях.

В Termidesk VDI поддерживаются следующие домены аутентификации:

- FreeIPA;
- ALD Pro;
- SAML;
- IP-аутентификация;
- MS AD или LDAP;
- RADIUS;
- OIDC;
- Альт Домен.

Доступность некоторых доменов аутентификации зависит от типа редакции Termidesk VDI.

Для обеспечения доступности одного и того же РМ для пользователя, авторизовавшегося с разных доменов аутентификации, используется особый объект Termidesk VDI - метадомен аутентификации.

Поддержка некоторых доменов аутентификации может добавляться в режиме экспериментальных функций.

Для отображения списка добавленных доменов аутентификации следует перейти «Системные параметры - Домены аутентификации». Основные параметры списка приведены в таблице (см. таблицу Параметры списка доменов аутентификации).

Таблица 15. Параметры списка доменов аутентификации

Параметр	Описание
«Приоритет»	Приоритет отображения в списке доменов аутентификации для пользователя
«Название»	Текстовое наименование домена аутентификации в Termidesk
«Тип»	Тип домена аутентификации
«Пользователи»	Число пользователей домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения домена аутентификации
«Теги»	Список тегов, назначенных домену аутентификации. При выборе тега выполняется переход к разделу «Системные параметры – Управление тегами» со списком объектов, которым назначен данный тег

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом

для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Для добавления в Termidesk VDI домена аутентификации используется экранная кнопка **[Создать]**.

Доступны следующие действия над доменами аутентификации:

- редактирование. Для этого нужно пометить домен аутентификации и нажать на экранную кнопку **[Изменить]**;
- удаление. Для этого нужно пометить домен аутентификации и нажать на экранную кнопку **[Удалить]**;
- назначение тегов домену аутентификации. Для этого нужно пометить домен аутентификации и нажать экранную кнопку **[Теги]**. Общее описание по применению тегов приведено в подразделе **Общие сведения о тегах**.

Для удаления метадомена аутентификации он не должен использоваться в других доменах аутентификации.

Каждый домен аутентификации описывается перечнем параметров, требуемых для получения идентификаторов субъектов и информации о полномочиях. Проверить корректность указанных параметров можно при помощи экранной кнопки **[Тест]**, расположенной в том же окне. Для сохранения параметров конфигурации нужно использовать экранную кнопку **[Сохранить]**.

Следует предусмотреть, что в целях безопасности учетная запись для биндинга (подключения) к домену не должна иметь прав на удаление или изменение объекта типа «пользователь».

Добавление метадомена аутентификации

Метадомен аутентификации - особый объект в Termidesk VDI, обеспечивающий доступность одного и того же РМ для пользователя, авторизовавшегося с использованием разных доменов аутентификации.

Функционал работает следующим образом:

- если создан объект «Метадомен аутентификации (экспериментальный)» и он указан в параметрах других доменов, то в нем будет создан метапользователь (или метапользователи) после авторизации пользователя в «Портале пользователя»;
- если опубликовано несколько фондов РМ, к каждому из которых привязаны разные домены аутентификации, то пользователь получит несколько фондов вне зависимости от того, из какого домена аутентификации он авторизовался. При этом РМ будет привязано к метапользователю;
- сопоставление пользователя в разных доменах аутентификации производится по его имени. Задача администратора - корректно настроить домены аутентификации так, чтобы при авторизации в них пользователь использовал одинаковое имя.

Пользователь должен предварительно авторизоваться для каждого из доменов аутентификации (в Termidesk VDI должна появиться запись о нем). Допустим, есть фонд «А» с доменом аутентификации «А» и фонд «Б» с доменом аутентификации «Б». Если пользователь авторизовался из домена «А», но при этом не авторизовался из домена «Б», то ему не отобразится фонд «Б».

Метадомен аутентификации не поддерживается для домена «IP аутентификация».

Для добавления метадомена аутентификации администратору Termidesk VDI следует перейти «Системные параметры - Домены аутентификации», а затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «Метадомен аутентификации (экспериментальный)».

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления метадомена аутентификации).

Таблица 16. Данные для добавления метадомена аутентификации

Параметр	**Описание**
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения домена аутентификации
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий. Порядок отображения доменов зависит от приоритета домена и его наименования: • чем ниже приоритет, тем выше домен в списке; • при наличии доменов с одинаковым приоритетом действует сортировка по алфавиту
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных. Параметр используется для поиска аналогичного домена «Универсального диспетчера», поэтому должен быть одинаковым как на портале «Агрегатор» (при его использовании), так и на «Универсальном диспетчере». Поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)

Параметр	Описание
«Субъекты»	Выбор субъектов, для которых будет доступен домен аутентификации. Для метадомена аутентификации возможен выбор только значения «Система». Возможные значения: • «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»; • «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»; • «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»; • «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала

Параметр	Описание
«Порталы»	Выбор порталов фермы Termidesk VDI, для которых будет доступен домен аутентификации. Если портал не выбран, то домен аутентификации не будет доступен для него. В списке доступных значений отображаются все узлы со страницы «Инфраструктура - Порталы» с их полным доменным именем. Администратору нужно выбирать узел в соответствии со значением, указанным в параметре «Субъекты». Примеры: • если в параметре «Субъекты» указано «Пользователи», то в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Администраторы и персонал», в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу администратора», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Все», то в параметре «Порталы» может быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу администратора», либо «Порталу универсальному». Значение выбирается исходя из потребностей в разделении доменов аутентификации для того или иного субъекта. При изменении списка узлов на странице «Инфраструктура - Порталы»: • если узел удален, то он автоматически удалится из списка доступных значений для этого параметра. Уже назначенное значение удалится из свойств домена аутентификации; • если узел добавлен, то он автоматически добавится в список доступных значений для этого параметра, но не будет автоматически выбран для использования. В случае, если в параметре «Порталы» был указан единственный узел, который затем был удален из «Инфраструктура - Порталы», то этот домен аутентификации не будет доступен ни в каком из порталов. Для выбора всех порталов используется значение «Все»

Параметр	Описание

«Динамическая проверка членства пользователя в группах»	Управление динамической проверкой вхождения пользователя в группу службы каталогов.
	
	Параметр определяет, как будет происходить проверка нахождения пользователя в группе службы каталогов при аутентификации в Termidesk VDI и получении ресурсов.
	
	Особенности функционирования:
	
	• если пользователю уже назначено РМ, то проверяется вхождение пользователя в группу, указанную в свойствах фонда РМ. Проверка выполняется каждый раз при доступе к ресурсу. При этом если у пользователя отозваны права на доступ, то он:
	  - либо не увидит скрытый ресурс в зависимости от настройки «Скрывать недоступные ресурсы»;
	  - либо увидит, но не сможет получить доступ к нему;
	  - либо получит доступ к назначенному РМ, если права доступа были назначены на другую группу, в которую входит пользователь и которая указана в свойствах фонда РМ;
	  - либо получит доступ к назначенному РМ, если оно назначено на учетную запись пользователя напрямую.
	
	Возможные значения:
	
	• «Режим совместимости 6.0» (по умолчанию) - при аутентификации пользователя происходит запрос к службе каталогов для проверки его вхождения в группы. После этого группы пользователя актуализируются в БД. При попытке получить ресурс из фонда доступ определяется на основе информации из БД (БД не обновляется);
	• «Периодическое обновление» - если пользователя нет в БД и он впервые аутентифицируется, то происходит запрос к службе каталогов для получения актуальной информации о нем. Если пользователь есть в БД, то информация берется из нее. Актуализация пользователей и групп для всех доменов аутентификации с этим значением выполняется периодической фоновой задачей раз в 24 часа;
	• «Динамическая проверка» - при аутентификации пользователя или получении ресурсов происходит запрос к службе каталогов для получения актуальной информации о нем. При обращении к службе каталогов информация о полученных группах кешируется во внутренней памяти. Время кеширования определяется системным параметром «Таймаут кеша хранения групп домена, с»

Добавление домена аутентификации FreeIPA

Получение и добавление файла `keytab`

`Keytab`-файлы используются для аутентификации в системах, использующих механизм Kerberos. Для получения `keytab`-файла на контроллере домена и добавления его на сервер, где установлен Termidesk VDI, необходимо выполнить ряд действий.

Действия на контроллере домена (например, FreeIPA или ALD Pro):

- получить доступ к контроллеру домена в режиме интерфейса командной строки;
- получить `kerberos-ticket` для пользователя с полномочиями администратора домена при помощи команды:

```
sudo kinit admin
```

- выполнить команду для добавления узла:

```
sudo ipa host-add --force --ip-address=192.0.2.30 disp.termidesk.local
```

где:

`--force` - флаг для принудительного создания;

`--ip-address` - задание IP-адреса целевого узла;

`192.0.2.30` - IP-адрес сервера, где установлен Termidesk VDI,

`disp.termidesk.local` - мнимый FQDN узла в текущем домене (в примере `termidesk.local`);

> Здесь и далее примеры IP-адресов приведены в соответствии с RFC 5737. Указанные IP-адреса должны быть заменены на актуальные, используемые согласно схеме адресации, принятой в инфраструктуре организации. Мнимый FQDN означает, что он не обязательно должен быть привязан к действительно существующему узлу.

- выполнить команду добавления службы для нового сервисного аккаунта:

```
sudo ipa service-add HTTP/disp.termidesk.local
```

- создать файл `termidesk.keytab` для сервисного аккаунта:

```
sudo ipa-getkeytab -s freeipa.termidesk.local -p HTTP/disp.termidesk.local -k
/home/user/termidesk.keytab
```

где:

`-s freeipa.termidesk.local` - задание FQDN сервера-контроллера домена FreeIPA;

`-p HTTP/disp.termidesk.local` - указание ранее созданного субъекта-службы;

`-k /home/user/termidesk.keytab` - сохранение в файл `termidesk.keytab`;

> Неважно, для какого узла создан `keytab`, необходимо само его наличие.

- передать полученный файл `termidesk.keytab` на узел Termidesk VDI, например, воспользовавшись командой:

```
sudo scp termidesk.keytab localuser@192.0.2.30:termidesk.keytab
```

где:

`localuser` - имя пользователя целевого узла;

`192.0.2.30` - IP-адрес сервера, где установлен Termidesk VDI.

После передачи файла на узле Termidesk VDI необходимо выполнить следующее:

- переместить файл `termidesk.keytab` в каталог `/etc/opt/termidesk-vdi`:

```
sudo mv /home/user/termidesk.keytab /etc/opt/termidesk-vdi/
```

- сделать владельцем этого файла пользователя `termidesk`:

```
sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/termidesk.keytab
```

- перезапустить службу `termidesk-vdi`:

```
sudo systemctl restart termidesk-vdi
```

Перечень параметров для добавления домена аутентификации FreeIPA

При необходимости ввода в домен FreeIPA, развернутый на ОС Astra Linux Special Edition, ВРМ с другой гостевой ОС Linux, необходимо внести изменения в файл `/usr/lib/python3.6/site-packages/ipalib/constants.py` (см. подраздел **Обязательные настройки гостевой ОС РМ**).

Для добавления аутентификации через FreeIPA администратору Termidesk VDI следует перейти «Системные параметры - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «FreeIPA». Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления аутентификации через FreeIPA).

При добавлении второго домена аутентификации необходимо создать новый файл `keytab` и задать ему имя, отличное от уже существующего. Добавление второго домена аутентификации не отличается от добавления первого.

Termidesk VDI поддерживает авторизацию пользователей, находящихся во вложенных доменных группах FreeIPA.

Таблица 17. Данные для добавления аутентификации через FreeIPA

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях

Параметр	Описание
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий. Порядок отображения доменов зависит от приоритета домена и его наименования: • чем ниже приоритет, тем выше домен в списке; • при наличии доменов с одинаковым приоритетом действует сортировка по алфавиту
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk VDI. Начиная с Termidesk VDI версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)
«Субъекты»	Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: • «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»; • «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»; • «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»; • «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала

Параметр	Описание
«Порталы»	Выбор порталов фермы Termidesk VDI, для которых будет доступен домен аутентификации. Если портал не выбран, то домен аутентификации не будет доступен для него. В списке доступных значений отображаются все узлы со страницы «Инфраструктура - Порталы» с их полным доменным именем. Администратору нужно выбирать узел в соответствии со значением, указанным в параметре «Субъекты». Примеры: • если в параметре «Субъекты» указано «Пользователи», то в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Администраторы и персонал», в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу администратора», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Все», то в параметре «Порталы» может быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу администратора», либо «Порталу универсальному». Значение выбирается исходя из потребностей в разделении доменов аутентификации для того или иного субъекта. При изменении списка узлов на странице «Инфраструктура - Порталы»: • если узел удален, то он автоматически удалится из списка доступных значений для этого параметра. Уже назначенное значение удалится из свойств домена аутентификации; • если узел добавлен, то он автоматически добавится в список доступных значений для этого параметра, но не будет автоматически выбран для использования. В случае, если в параметре «Порталы» был указан единственный узел, который затем был удален из «Инфраструктура - Порталы», то этот домен аутентификации не будет доступен ни в каком из порталов. Для выбора всех порталов используется значение «Все»
«Сервисный аккаунт»	Название сервисного аккаунта, созданного в службе каталогов FreeIPA
«Домен»	Идентификатор области Kerberos для аутентификации

Параметр	Описание
«Keytab»	Путь к файлу с ключами для сервисного аккаунта (пример формирования файла приведен в подразделе **Получение и добавление файла** `keytab`). Каждая генерация `keytab` должна производиться в новый файл. При необходимости повторного использования имени файла существующий файл **обязательно** должен быть удален перед генерацией. Неважно, для какого узла создан `keytab`, необходимо само его наличие. Пример задания значений: • в случае стандартного хранения файла: «/etc/opt/termidesk-vdi/termidesk.keytab»; • в случае хранения файла в хранилище hvac: «hvac-kv://secret#termidesk-admin/keytabs/termidesk». Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Если используется хранилище, то сгенерированный на контроллере домена `keytab`-файл должен быть преобразован к формату BASE64
«Сервер FreeIPA»	FQDN ресурса, являющегося источником сведений о субъектах и их полномочиях
«Проверка SSL»	Проверка использования SSL
«Метадомен аутентификации»	Выбор метадомена аутентификации, в который будет входить добавляемый домен. Метадомен аутентификации должен быть предварительно создан (см. подраздел **Добавление метадомена аутентификации**)

Параметр	Описание

«Динамическая проверка членства пользователя в группах»	Управление динамической проверкой вхождения пользователя в группу службы каталогов.
	
	Параметр определяет, как будет происходить проверка нахождения пользователя в группе службы каталогов при аутентификации в Termidesk VDI и получении ресурсов.
	
	Особенности функционирования:
	
	• если пользователю уже назначено РМ, то проверяется вхождение пользователя в группу, указанную в свойствах фонда РМ. Проверка выполняется каждый раз при доступе к ресурсу. При этом если у пользователя отозваны права на доступ, то он:
	  - либо не увидит скрытый ресурс в зависимости от настройки «Скрывать недоступные ресурсы»;
	  - либо увидит, но не сможет получить доступ к нему;
	  - либо получит доступ к назначенному РМ, если права доступа были назначены на другую группу, в которую входит пользователь и которая указана в свойствах фонда РМ;
	  - либо получит доступ к назначенному РМ, если оно назначено на учетную запись пользователя напрямую.
	
	Возможные значения:
	
	• «Режим совместимости 6.0» (по умолчанию) - при аутентификации пользователя происходит запрос к службе каталогов для проверки его вхождения в группы. После этого группы пользователя актуализируются в БД. При попытке получить ресурс из фонда доступ определяется на основе информации из БД (БД не обновляется);
	• «Периодическое обновление» - если пользователя нет в БД и он впервые аутентифицируется, то происходит запрос к службе каталогов для получения актуальной информации о нем. Если пользователь есть в БД, то информация берется из нее. Актуализация пользователей и групп для всех доменов аутентификации с этим значением выполняется периодической фоновой задачей раз в 24 часа;
	• «Динамическая проверка» - при аутентификации пользователя или получении ресурсов происходит запрос к службе каталогов для получения актуальной информации о нем. При обращении к службе каталогов информация о полученных группах кешируется во внутренней памяти. Время кеширования определяется системным параметром «Таймаут кеша хранения групп домена, с»

Для возможности подключения двухфакторной аутентификации (2FA) нужно выбрать домен аутентификации «FreeIPA (native 2FA)» - пользователям потребуется вручную отправлять QR-код для настройки двухфакторной аутентификации.

Двухфакторная аутентификация доступна только при входе в Termidesk VDI через веб-интерфейс. Для ее прохождения необходимо установить приложение FreeOTP Authenticator на мобильные устройства пользователей.

Termidesk VDI не реализует непосредственно механизм аутентификации. На контроллере домена FreeIPA должна быть подключена двухфакторная аутентификация, только после этого ее необходимо добавить в Termidesk VDI.

Добавление домена аутентификации ALD Pro

Для добавления аутентификации через ALD Pro администратору Termidesk VDI следует перейти «Системные параметры - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «ALD Pro». Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей на таблицы (см. таблицу Данные для добавления аутентификации через ALD Pro).

При добавлении второго домена аутентификации необходимо создать новый файл `keytab` и задать ему имя, отличное от уже существующего. Добавление второго домена аутентификации не отличается от добавления первого.

Termidesk VDI поддерживает авторизацию пользователей, находящихся во вложенных доменных группах ALD Pro.

Таблица 18. Данные для добавления аутентификации через ALD Pro

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий. Порядок отображения доменов зависит от приоритета домена и его наименования: • чем ниже приоритет, тем выше домен в списке; • при наличии доменов с одинаковым приоритетом действует сортировка по алфавиту
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk VDI. Начиная с Termidesk VDI версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)

Параметр	Описание
«Субъекты»	Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: • «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»; • «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»; • «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»; • «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала

Параметр	Описание
«Порталы»	Выбор порталов фермы Termidesk VDI, для которых будет доступен домен аутентификации. Если портал не выбран, то домен аутентификации не будет доступен для него. В списке доступных значений отображаются все узлы со страницы «Инфраструктура - Порталы» с их полным доменным именем. Администратору нужно выбирать узел в соответствии со значением,указанным в параметре «Субъекты». Примеры: • если в параметре «Субъекты» указано «Пользователи», то в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Администраторы и персонал», в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу администратора», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Все», то в параметре «Порталы» может быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу администратора», либо «Порталу универсальному». Значение выбирается исходя из потребностей в разделении доменов аутентификации для того или иного субъекта. При изменении списка узлов на странице «Инфраструктура - Порталы»: • если узел удален, то он автоматически удалится из списка доступных значений для этого параметра. Уже назначенное значение удалится из свойств домена аутентификации; • если узел добавлен, то он автоматически добавится в список доступных значений для этого параметра, но не будет автоматически выбран для использования. В случае, если в параметре «Порталы» был указан единственный узел, который затем был удален из «Инфраструктура - Порталы», то этот домен аутентификации не будет доступен ни в каком из порталов. Для выбора всех порталов используется значение «Все»
«Сервисный аккаунт»	Название сервисного аккаунта, созданного при добавлении поставщика ресурсов
«Домен»	Идентификатор области Kerberos для аутентификации

Параметр	Описание
«Keytab»	Путь к файлу с ключами для сервисного аккаунта (пример формирования файла приведен в подразделе **Получение и добавление файла** `keytab`). Каждая генерация `keytab` должна производиться в новый файл. При необходимости повторного использования имени файла существующий файл **обязательно** должен быть удален перед генерацией. Неважно, для какого узла создан `keytab`, необходимо само его наличие. Пример задания значений: • в случае стандартного хранения файла: «/etc/opt/termidesk-vdi/termidesk.keytab»; • в случае хранения файла в хранилище hvac: «hvac-kv://secret#termidesk-admin/keytabs/termidesk».Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Если используется хранилище, то сгенерированный на контроллере домена `keytab`-файл должен быть преобразован к формату BASE64
«Сервер ALD Pro»	IP-адрес или FQDN ресурса, являющегося источником сведений о субъектах и их полномочиях. Можно указать до пяти ресурсов, разделенных символом «;». Ресурсы будут использоваться в указанном порядке: обращение к следующему будет выполняться при недоступности предыдущего
«Проверка SSL»	Проверка использования SSL
«Порт PKINIT»	TCP/UDP порт, на котором запущена служба Kerberos. Значение по умолчанию: «88»

Параметр	Описание
«Использовать PKINIT»	Использовать механизм аутентификации Kerberos PKINIT при аутентификации пользователя. PKINIT - механизм, позволяющий использовать сертификаты X.509 в качестве метода аутентификации. Предполагается, что механизм аутентификации Kerberos PKINIT настроен в инфраструктуре организации и пользователю выданы соответствующие сертификаты и ключи для подключения (персональный сертификат, закрытый ключ к нему и корневой сертификат ЦС, на котором выпущен персональный сертификат). При активации механизма аутентификации Kerberos PKINIT нужно указать актуальный порт в параметре «Порт PKINIT». Для корректной работы PKINIT следует задать альтернативное имя пользователя (Subject Alternative Name) в сертификате как: • либо только UPN (UserPrincipalName); • либо UPN и атрибут RFC822 Name - Email. Возможные значения: • «Да» - использовать механизм; • «Нет» (по умолчанию) - не использовать механизм
«Метадомен аутентификации»	Выбор метадомена аутентификации, в который будет входить добавляемый домен. Метадомен аутентификации должен быть предварительно создан (см. подраздел **Добавление метадомена аутентификации**)

Параметр	Описание

«Динамическая проверка членства пользователя в группах»	Управление динамической проверкой вхождения пользователя в группу службы каталогов.
	
	Параметр определяет, как будет происходить проверка нахождения пользователя в группе службы каталогов при аутентификации в Termidesk VDI и получении ресурсов.
	
	Особенности функционирования:
	
	• если пользователю уже назначено РМ, то проверяется вхождение пользователя в группу, указанную в свойствах фонда РМ. Проверка выполняется каждый раз при доступе к ресурсу. При этом если у пользователя отозваны права на доступ, то он:
	  - либо не увидит скрытый ресурс в зависимости от настройки «Скрывать недоступные ресурсы»;
	  - либо увидит, но не сможет получить доступ к нему;
	  - либо получит доступ к назначенному РМ, если права доступа были назначены на другую группу, в которую входит пользователь и которая указана в свойствах фонда РМ;
	  - либо получит доступ к назначенному РМ, если оно назначено на учетную запись пользователя напрямую.
	
	Возможные значения:
	
	• «Режим совместимости 6.0» (по умолчанию) - при аутентификации пользователя происходит запрос к службе каталогов для проверки его вхождения в группы. После этого группы пользователя актуализируются в БД. При попытке получить ресурс из фонда доступ определяется на основе информации из БД (БД не обновляется);
	• «Периодическое обновление» - если пользователя нет в БД и он впервые аутентифицируется, то происходит запрос к службе каталогов для получения актуальной информации о нем. Если пользователь есть в БД, то информация берется из нее. Актуализация пользователей и групп для всех доменов аутентификации с этим значением выполняется периодической фоновой задачей раз в 24 часа;
	• «Динамическая проверка» - при аутентификации пользователя или получении ресурсов происходит запрос к службе каталогов для получения актуальной информации о нем. При обращении к службе каталогов информация о полученных группах кешируется во внутренней памяти. Время кеширования определяется системным параметром «Таймаут кеша хранения групп домена, с»

Добавление домена аутентификации LDAP

Получение и добавление `keytab`-файла для Kerberos-аутентификации

Для получения `keytab`-файла на контроллере домена MS AD нужно:

- заранее создать учетную запись (сервисный аккаунт), от имени которой будет работать служба. Для создания учетной записи нужно на КД перейти в стандартную утилиту «Active Directory - пользователи и компьютеры»;

- в свойствах учетной записи во вкладке «Account» активировать параметр «This account supports Kerberos AES 256 bit encryption» (см. рисунок Активация параметра «This account supports Kerberos AES 256 bit encryption»);

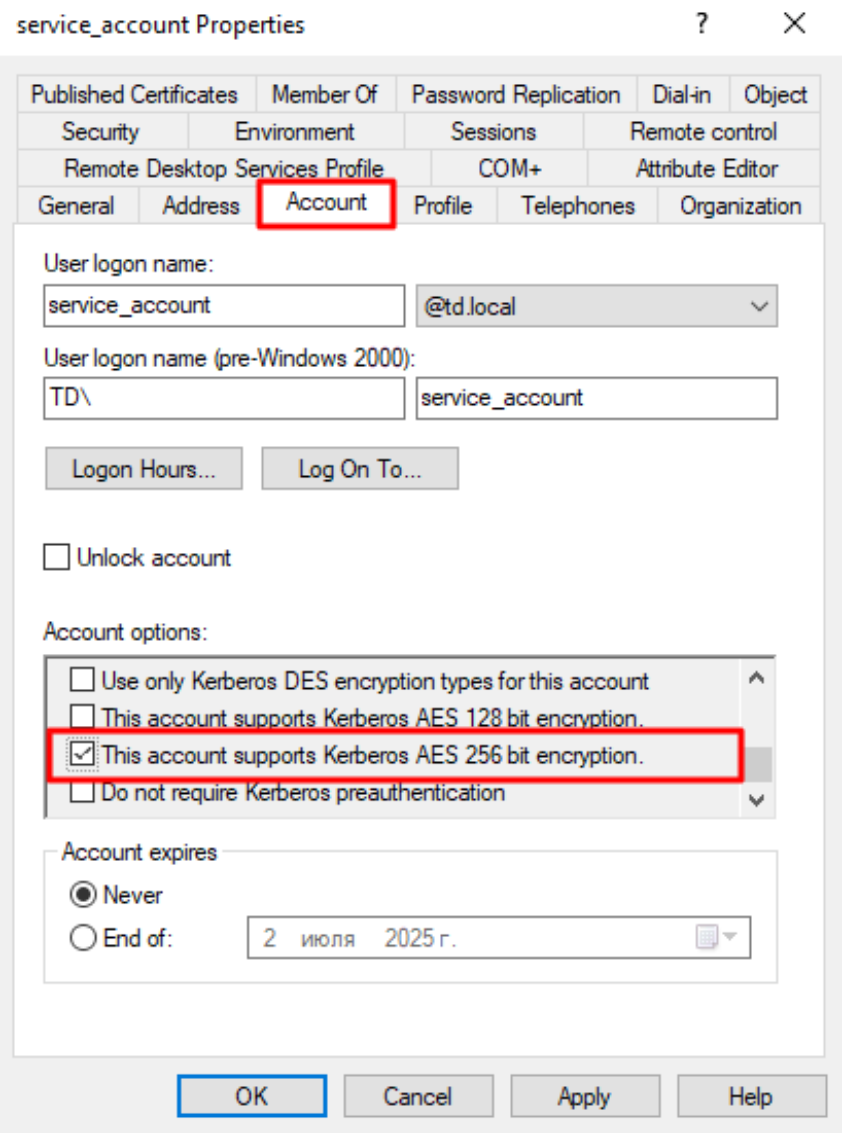


Рисунок 57. Активация параметра «This account supports Kerberos AES 256 bit encryption»

- открыть интерфейс командной строки PowerShell и выполнить команду добавления службы для сервисного аккаунта:

```
setspn -A HTTP/disp.termidesk.local service_account
```

где:

`service_account` - наименование сервисного аккаунта;

- для просмотра списка служб сервисного аккаунта можно воспользоваться командой:

```
setspn -L service_account
```

- создать файл `termidesk-msad.keytab` для сервисного аккаунта:

```
ktpass -princ HTTP/disp.termidesk.local@TERMIDESK.LOCAL -mapuser
service_account@TERMIDESK.LOCAL -pass <пароль_сервисного_аккаунта> -ptype
KRB5_NT_PRINCIPAL -out termidesk-msad.keytab -crypto AES256-SHA1
```

где:

`HTTP/disp.termidesk.local` - указание ранее созданного субъекта-службы;

`service_account@TERMIDESK.LOCAL` - наименование сервисного аккаунта;

`-out termidesk-msad.keytab` - сохранение в файл `termidesk-msad.keytab`;

`-crypto AES256-SHA1` - алгоритм для преобразования `keytab`-файла.

Алгоритм преобразования `keytab`-файла следует выбирать согласно установленным политикам безопасности MS AD.

Полученный файл `termidesk-msad.keytab` следует передать на целевой узел для хранения. Файл может быть сохранен в файловой системе узла Termidesk VDI или в хранилище OpenBao.

Для передачи файла на целевой узел нужно выполнить команду:

```
scp C:\Windows\System32\termidesk-msad.keytab localuser@192.0.2.30:termidesk-
msad.keytab
```

где:

`C:\Windows\System32\termidesk-msad.keytab` - путь к `keytab`-файлу;

`localuser` - имя пользователя целевого узла;

`192.0.2.30` - IP-адрес целевого узла.

После передачи файла необходимо выполнить ряд действий в зависимости от выбранного хранилища.

При хранении файла в файловой системе узла Termidesk VDI:

- переместить файл `termidesk-msad.keytab` в каталог `/etc/opt/termidesk-vdi`:

```
sudo mv /home/user/termidesk-msad.keytab /etc/opt/termidesk-vdi/
```

- сделать владельцем этого файла пользователя `termidesk`:

```
sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/termidesk-msad.keytab
```

- перезапустить службу `termidesk-vdi`:

```
sudo systemctl restart termidesk-vdi
```

При хранении файла в хранилище OpenBao:

- запустить интерпретатор Python:

```
sudo python3
```

- перевести файл в формат base64:

```
import base64 with open('/home/user/termidesk-msad.keytab', 'rb') as file:
keytab_bytes = file.read() keytab_base64 =
base64.b64encode(keytab_bytes).decode('utf-8') keytab_base64
```

где:

`/home/user/termidesk-msad.keytab` - путь к `keytab`-файлу;

- сохранить результат выполнения команды в хранилище OpenBao:

```
bao kv put secret/termidesk/ldap
keytab='BQIAAABGAAIAC1VTVVA0MDcuTEFOAARIVFRQABJ0ZXJtaWRlc2subXlkb21h
aW4AAAABAAAAAAUAFwAQhKQHwhUvWGEJk92QgI/tNA=='
```

где:

`termidesk` - значение переменной `SECRETS_OPENBAO_TERMIDESK_PATH`, заданной в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf`;

`ldap` - путь к хранилищу OpenBao, где следует сохранить результат выполнения команды.

Перечень параметров для добавления домена аутентификации MS AD (LDAP)

Для добавления аутентификации MS AD (LDAP) администратору Termidesk VDI следует перейти «Системные параметры - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «Microsoft AD DS/LDAP».

Затем необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления аутентификации через MS AD (LDAP)).

Таблица 19. Данные для добавления аутентификации через MS AD (LDAP)

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения домена аутентификации

Параметр	Описание
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий. Порядок отображения доменов зависит от приоритета домена и его наименования: • чем ниже приоритет, тем выше домен в списке; • при наличии доменов с одинаковым приоритетом действует сортировка по алфавиту
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных. Параметр используется для поиска аналогичного домена «Универсального диспетчера», поэтому должен быть одинаковым как на портале «Агрегатор» (при его использовании), так и на «Универсальном диспетчере». Поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)
«Субъекты»	Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: • «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»; • «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»; • «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»; • «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала

Параметр	Описание
«Порталы»	Выбор порталов фермы Termidesk VDI, для которых будет доступен домен аутентификации. Если портал не выбран, то домен аутентификации не будет доступен для него. В списке доступных значений отображаются все узлы со страницы «Инфраструктура - Порталы» с их полным доменным именем. Администратору нужно выбирать узел в соответствии со значением, указанным в параметре «Субъекты». Примеры: • если в параметре «Субъекты» указано «Пользователи», то в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Администраторы и персонал», в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу администратора», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Все», то в параметре «Порталы» может быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу администратора», либо «Порталу универсальному». Значение выбирается исходя из потребностей в разделении доменов аутентификации для того или иного субъекта. При изменении списка узлов на странице «Инфраструктура - Порталы»: • если узел удален, то он автоматически удалится из списка доступных значений для этого параметра. Уже назначенное значение удалится из свойств домена аутентификации; • если узел добавлен, то он автоматически добавится в список доступных значений для этого параметра, но не будет автоматически выбран для использования. В случае, если в параметре «Порталы» был указан единственный узел, который затем был удален из «Инфраструктура - Порталы», то этот домен аутентификации не будет доступен ни в каком из порталов. Для выбора всех порталов используется значение «Все»
«Сервер LDAP»	IP-адрес или доменное имя сервера службы каталогов, являющегося источником сведений о субъектах и их полномочиях
«Порт»	TCP-порт, на котором запущена служба каталогов. Возможные стандартные значения: • «389» (по умолчанию). Используется, если доступ к службе каталогов осуществляется по протоколу LDAP; • «636». Используется, если доступ к службе каталогов осуществляется по протоколу LDAPS; • «3268». Альтернативный порт. Используется, если доступ к службе каталогов осуществляется по протоколу LDAP; • «3269». Альтернативный порт. Используется, если доступ к службе каталогов осуществляется по протоколу LDAPS. Для ускорения поиска пользователей в службе каталогов рекомендуется указывать альтернативный порт
«Использовать SSL»	Использовать защищенное соединение при взаимодействии со службой каталогов

Параметр	Описание

«Проверять SSL»	Выполнять проверку цепочки сертификатов и имени (hostname) сервера службы каталогов.
	
	Возможные значения:
	
	• «Да» (по умолчанию для создаваемых доменов) - использовать механизм проверки. Если при этом выключен параметр «Использовать SSL», то значение «Проверять SSL» не применяется (то есть, проверка сертификатов отключена). Если используется защищенное соединение и включен механизм проверки, то TLS-соединение будет установлено только при отсутствии ошибок проверки сертификатов и имя сервера службы каталогов;
	• «Нет» (по умолчанию для уже созданных ранее доменов) - не использовать механизм проверки. Если при этом включен параметр «Использовать SSL», то ошибки при проверке сертификатов не влияют на подключение (TLS-соединение все равно будет установлено)
	
	Корневой сертификат УЦ должен быть добавлен на узел «Портала администратора» (см. подраздел **Установка корневого сертификата центра сертификации**). При этом:
	
	• сертификат должен быть задан в формате `Base64`, пример:
	
	`-----BEGIN CERTIFICATE-----`
	`MIIDVzCCAj+gAwIBAgIQPvc7pjfSf5VLzNdgExZPxzANBgkqhkiG9w0`
	`BAQsFADA+`
	`MRMwEQYKCZImiZPyLGQBGRYDbGFuMRIwEAYKCZImiZPyLGQBGRYCc2Q`
	`xEzARBgNV`
	`....`
	`-----END CERTIFICATE-----`
	
	• использование параметра `REQUESTS_CA_BUNDLE` конфигурационного файла `termidesk.conf` опционально: достаточно добавить корневой сертификат в системное хранилище ОС, но работа с параметром также поддерживается.

«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/msad/»

Параметр	Описание

«Механизм подключения»	Механизм подключения к службе каталогов.
	
	Возможные значения:
	
	• «SASL Bind» - безопасный механизм подключения с использованием протокола SASL. При выборе этого значения потребуется:
	  заполнить параметр «Путь до Keytab», при этом вводить сервер Termidesk VDI в домен не требуется (необходимо только задание и наличие `keytab`-файла);
	  убедиться, что на узле существует файл `/etc/krb5.conf`, в котором заданы настройки доменов для подклчений к ним. Пример файла `/etc/krb5.conf` приведен после таблицы;
	• «Simple Bind» - небезопасный механизм подключения, передающий данные для подключения в открытом виде.
	
	Значение по умолчанию: «SASL Bind»

«Учётная запись»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Учетная запись в формате Distinguished Name (DN) в домене MS AD (LDAP), используемая для подключения к службе каталогов. Пример: «CN=admin,OU=user,DC=test,DC=desk»
«Пароль учётной записи»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Набор символов, подтверждающий полномочия объекта для подключения к службе каталогов
«Время ожидания соединения, с»	Время ожидания (в секундах) ответа от службы каталогов. Значение по умолчанию: «10»
«Корень поиска»	Корень поиска в службе каталогов в формате DN. Параметру следует задавать значение, соответствующее записи верхнего уровня в иерархии службы каталогов (без указания OU). Вводимое значение не должно содержать пробелов: • в начале и конце строки; • рядом с разделителями (запятыми); • в элементах пути (например, «DC=company name,DC=de»). Пример: «DC=test,DC=desk»
«Имя класса пользователя»	Атрибут класса пользователя в службе каталогов. Для корректного заполнения данного поля необходимо указать значение «person»

Параметр	Описание
«Атрибут идентификатора пользователя»	Атрибут уникального имени или идентификатора пользователя в службе каталогов. Для корректного заполнения данного поля необходимо указать: • значение «name», если активирован параметр «Использовать PKINIT»; Атрибут идентификатора пользователя задается с учетом того, какой шаблон использовался при выдаче сертификата пользователя. Например, значение «name» для механизма аутентификации Kerberos PKINIT указывается в том случае, если сертификат для подключения выдан на имя пользователя. • значение «userPrincipalName», если в параметре «Формат имени пользователя для аутентификации» используется «userPrincipalName»; • значение «SamAccountName» в остальных случаях
«Список атрибутов пользователя»	Список атрибутов, содержащий уникальные данные пользователя, разделенные запятыми. Для корректного заполнения данного поля необходимо указать значение: • «userPrincipalName», если в параметре «Формат имени пользователя для аутентификации» используется «userPrincipalName»; • «name», если в параметре «Формат имени пользователя для аутентификации» используется «sAMAccountName»
«Формат имени пользователя для аутентификации»	Формат имени пользователя, заданный в службе каталогов. Если на пользовательской рабочей станции установлен компонент «Клиент» версии, младше 6.0, то он будет поддерживать только формат «sAMAccountName». Возможные значения: • «sAMAccountName» (по умолчанию) - имя пользователя без доменной части; • «userPrincipalName» - имя пользователя с доменной частью
«Имя атрибута группы»	Атрибут принадлежности к группе в службе каталогов. Для корректного заполнения данного поля необходимо указать значение «group»

Параметр	Описание
«Атрибут имени группы»	Атрибут идентификатора группы, к которой относится субъект в службе каталогов. Для корректного заполнения данного поля необходимо указать: • значение «distinguishedname», если включены параметры «Использовать рекурсивный поиск групп» или «Использовать обратный порядок проверки членства пользователей»; • значение «name», если активирован параметр «Использовать PKINIT» или «Использовать Kerberos»; Атрибут имени группы задается с учетом того, какой шаблон использовался при выдаче сертификата пользователя. Например, значение «name» для механизма аутентификации Kerberos PKINIT указывается в том случае, если сертификат для подключения выдан на имя пользователя. • значение «cn» в остальных случаях. Если используется значение «distinguishedname», то при добавлении группы в домен аутентификации по пути «Системные параметры - Домены аутентификации - Наименование домена - Группы» нужно указывать длинные имена групп, например: «CN=RootGroup,CN=Users,DC=test,DC=desk». Если используется значение «cn», то нужно указывать короткие имена групп. Если параметр «Атрибут имени группы» был изменен, то необходимо заново добавить группы, используя соответствующие имена групп: для «cn» - короткие имена, для «distinguishedname» - длинные имена
«Атрибут членства в группе»	Идентификатор группы для назначения полномочий субъекту. Для корректного заполнения данного поля необходимо указать значение «member»
«Атрибут групп для LDAP-запросов»	Атрибут, определяющий группы пользователя при запросах к службе каталогов. Возможные значения: «objectClass», «objectCategory»
«Время хранения дополнительных атрибутов учетной записи пользователей, сут»	Срок хранения (в сутках) дополнительных атрибутов учетной записи пользователей в БД. При наступлении срока данные будут очищены. Возможные значения: • «0» (по умолчанию) - не хранить дополнительные атрибуты; • числовое значение - хранить дополнительные атрибуты на протяжении заданного срока
«Рекурсивный поиск групп»	При запросе групп пользователя будут учтены его родительские группы, в которых он состоит неявно. При этом проверяется вхождение пользователя только в те группы, которые добавлены в домен аутентификации в Termidesk VDI. Если дополнительно включен параметр «Использовать обратный порядок проверки членства пользователей», то параметр «Использовать рекурсивный поиск групп» можно не включать. Возможные значения: • «Да» - использовать рекурсивный поиск; • «Нет» (по умолчанию) - не использовать рекурсивный поиск

Параметр	Описание
«Использовать обратный порядок проверки членства пользователей»	Проверка соответствия членства пользователя в группах службы каталогов членству в группах домена аутентификации. Для работы функционала необходимо, чтобы был задан параметр «Атрибут имени группы». Этот параметр нужно включить при большом количестве групп непосредственно на службе каталогов MS AD. В этом случае сначала будет проверяться вхождение пользователя в группы домена аутентификации (в том числе рекурсивно), затем будет происходить проверка найденных групп в службе каталогов MS AD. При выключении этого параметра применяется настройка выбора «Атрибут групп для LDAP-запросов»: «objectClass» или «objectCategory». При включении этого параметра всегда применяется настройка выбора «Атрибут групп для LDAP-запросов»: «objectClass». Возможные значения: • «Да» - использовать обратный порядок; • «Нет» (по умолчанию) - не использовать обратный порядок

Параметр	Описание

«Динамическая проверка членства пользователя в группах»	Управление динамической проверкой вхождения пользователя в группу службы каталогов.
	
	Параметр определяет, как будет происходить проверка нахождения пользователя в группе службы каталогов при аутентификации в Termidesk VDI и получении ресурсов.
	
	Особенности функционирования:
	
	• если пользователю уже назначено РМ, то проверяется вхождение пользователя в группу, указанную в свойствах фонда РМ. Проверка выполняется каждый раз при доступе к ресурсу. При этом если у пользователя отозваны права на доступ, то он:
	  - либо не увидит скрытый ресурс в зависимости от настройки «Скрывать недоступные ресурсы»;
	  - либо увидит, но не сможет получить доступ к нему;
	  - либо получит доступ к назначенному РМ, если права доступа были назначены на другую группу, в которую входит пользователь и которая указана в свойствах фонда РМ;
	  - либо получит доступ к назначенному РМ, если оно назначено на учетную запись пользователя напрямую.
	
	Возможные значения:
	
	• «Режим совместимости 6.0» (по умолчанию) - при аутентификации пользователя происходит запрос к службе каталогов для проверки его вхождения в группы. После этого группы пользователя актуализируются в БД. При попытке получить ресурс из фонда доступ определяется на основе информации из БД (БД не обновляется);
	• «Периодическое обновление» - если пользователя нет в БД и он впервые аутентифицируется, то происходит запрос к службе каталогов для получения актуальной информации о нем. Если пользователь есть в БД, то информация берется из нее. Актуализация пользователей и групп для всех доменов аутентификации с этим значением выполняется периодической фоновой задачей раз в 24 часа;
	• «Динамическая проверка» - при аутентификации пользователя или получении ресурсов происходит запрос к службе каталогов для получения актуальной информации о нем. При обращении к службе каталогов информация о полученных группах кешируется во внутренней памяти. Время кеширования определяется системным параметром «Таймаут кеша хранения групп домена, с»

Параметр	Описание
«Использовать PKINIT»	Использовать механизм аутентификации Kerberos PKINIT при аутентификации пользователя. PKINIT - механизм, позволяющий использовать сертификаты X.509 в качестве метода аутентификации. Предполагается, что механизм аутентификации Kerberos PKINIT настроен в инфраструктуре организации и пользователю выданы соответствующие сертификаты и ключи для подключения (персональный сертификат, закрытый ключ к нему и корневой сертификат ЦС, на котором выпущен персональный сертификат). При активации механизма аутентификации Kerberos PKINIT нужно указать актуальный порт в параметре «Порт PKINIT», а также указать нужные значения параметров «Атрибут имени группы» и «Атрибут идентификатора пользователя». Настройки параметров «Атрибут имени группы» и «Атрибут идентификатора пользователя», и связанных с ними «Формат имени пользователя для аутентификации» и «Список атрибутов пользователя» задаются с учетом того, какой шаблон использовался при выдаче сертификата пользователя. Поскольку служба каталогов MS AD использует шаблон с форматом «userPrincipalName», то рекомендуется использовать в настройках параметров этот формат (там, где он применим). Возможные значения: • «Да» - использовать механизм; • «Нет» (по умолчанию) - не использовать механизм
«Порт PKINIT»	TCP/UDP порт, на котором запущена служба Kerberos. Значение по умолчанию: «88»

Параметр	Описание
«Использовать Kerberos»	Использовать механизм аутентификации по билету Kerberos. Доступность функционала зависит от типа редакции Termidesk VDI. Предполагается, что механизм аутентификации по билету Kerberos настроен в инфраструктуре организации (см. подразделы **Получение и добавление keytab -файла для Kerberos-аутентификации** и **Настройка пользовательской рабочей станции для Kerberos-аутентификации**). Для работы аутентификации по билету Kerberos на терминальных серверах MS RDS, необходимо выполнить дополнительную настройку «Сессионного агента», задав значения параметрам MASTER_KEY и URL_BALANCER в его конфигурационном файле. Если используется аутентификация Kerberos, то нужно: • заполнить параметр «Путь до Keytab»; • убедиться, что задано значение «Полному доменному имени (FQDN)» для параметра «Подключаться к BPM по» в «Системные параметры - Системные настройки», раздел «Общие». Потребуется правильная настройка параметров «Атрибут имени группы», «Атрибут идентификатора пользователя», «Формат имени пользователя для аутентификации», «Список атрибутов пользователя». Поскольку служба каталогов MS AD использует шаблон с форматом «userPrincipalName», то рекомендуется использовать в настройках параметров этот формат (там, где он применим). Возможные значения: • «Да» - использовать механизм; • «Нет» (по умолчанию) - не использовать механизм
«Путь до Keytab»	Путь к файлу с ключами для сервисного аккаунта. В зависимости от места хранения файла следует указать путь в формате: • в случае стандартного хранения файла: «/etc/opt/termidesk-vdi/termidesk.keytab»; • в случае хранения файла в хранилище hvac: «hvac-kv://secret#termidesk-admin/keytabs/kerberos». Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Если используется хранилище, то сгенерированный на контроллере домена keytab-файл должен быть преобразован к формату BASE64
«Метадомен аутентификации»	Выбор метадомена аутентификации, в который будет входить добавляемый домен. Метадомен аутентификации должен быть предварительно создан (см.подраздел **Добавление метадомена аутентификации**)

Для подключения к службе каталогов учетная запись должна иметь как минимум следующие привилегии:

- право на чтение объектов пользователей;

- право на чтение Base DN;
- право на чтение атрибутов групп.

Пример файла `/etc/krb5.conf` при выборе значения «SASL Bind» в параметре «Механизм подключения»:

Приведен только пример, требуется изменить файл при внедрении в соответствии с инфраструктурой организации.

```
[libdefaults]
  default_realm = TEST.LOC
  dns_lookup_realm = true
  rdns = false
  dns_canonicalize_hostname = false
  dns_lookup_kdc = true
  ticket_lifetime = 24h
  forwardable = true
  udp_preference_limit = 0
  default_ccache_name = KEYRING:persistent:%{uid}
#canonicalize = true
[realms]
  TEST.LOC = {
    pkinit_anchors = FILE:/var/lib/ipa-client/pki/kdc-ca-bundle.pem
    pkinit_pool = FILE:/var/lib/ipa-client/pki/ca-bundle.pem  }
    TST.LOC = {
        kdc = tst.loc
        kdc = msad.tst.loc
        admin_server = tst.loc
        default_domain = tst.loc
[domain_realm]
  .test.loc = TEST.LOC
  test.loc = TEST.LOC
  tdsk.test.loc = TEST.LOC
    tst.loc = TST.LOC
    .tst.loc = TST.LOC
```

Настройка пользовательской рабочей станции для Kerberos-аутентификации

Для корректной аутентификации пользовательская рабочая станция должна быть введена в соответствующий домен аутентификации Kerberos, используемый в ферме и указанный в портале.

Пользователь не может быть локальным администратором при доступе через Kerberos-аутентификацию.

По умолчанию билет Kerberos выдается автоматически при аутентификации пользователя в системе. Однако, если билет не был выдан автоматически, нужно:

- просмотреть список билетов:

```
klist
```

- получить билет Kerberos:

```
kinit -f termidesk@TERMIDESK.LOCAL
```

где:

`termidesk@TERMIDESK.LOCAL` - учетная запись, для которой запрашивается билет.

Kerberos-аутентификация через веб-браузер требует настройки параметров безопасности в зависимости от используемой ОС и типа браузера.

На пользовательской рабочей станции с ОС Microsoft Windows:

- при использовании веб-браузера, основанного на Chromium, нужно настроить его параметры безопасности для зоны, в которой находится сервер Termidesk VDI. Для этого:
  - перейти «Панель управления - Свойства браузера - Безопасность»;
  - в разделе «Выберите зону для параметры ее параметров безопасности» выбрать зону «Местная интрасеть», нажать экранную кнопку **[Сайты]**;
  - в окне «Местная интрасеть» нажать экранную кнопку **[Дополнительно]**;
  - в поле «Добавить в зону следующий узел» ввести FQDN сервера Termidesk VDI, нажать экранную кнопку **[Добавить]** (см. рисунок Добавление FQDN компонента «Универсальный диспетчер» в зону «Местная интрасеть»);

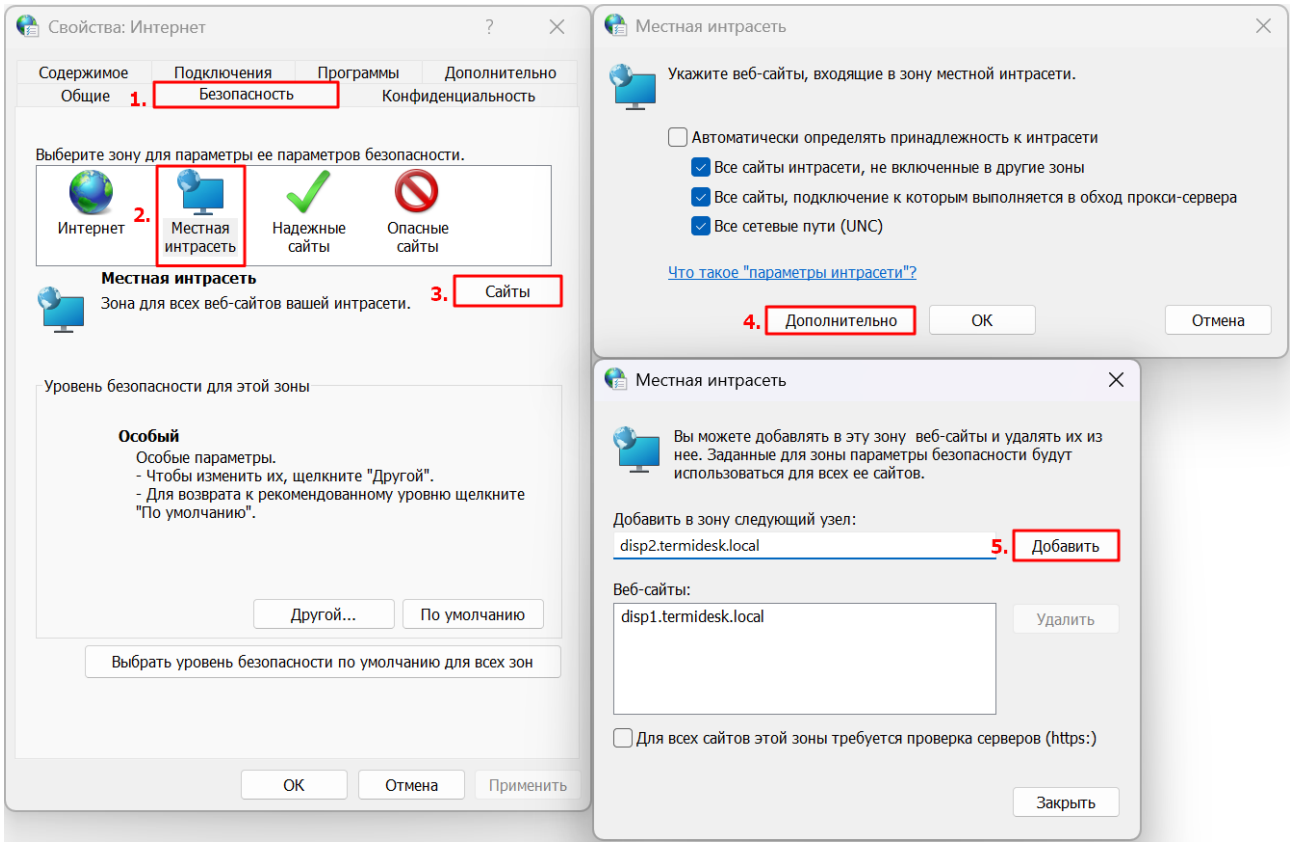


Рисунок 58. Добавление FQDN компонента «Универсальный диспетчер» в зону «Местная интрасеть»

- при использовании в ОС Microsoft Windows веб-браузера Mozilla Firefox нужно:
  - в адресной строке ввести `about:config`;
  - присвоить соответствующие значения параметрам, перечисленным в таблице (см. таблицу Данные для настройки Kerberos-аутентификации через веб-браузер Mozilla Firefox в ОС Microsoft Windows).

Таблица 20. Данные для настройки Kerberos-аутентификации через веб-браузер Mozilla Firefox в ОС Microsoft Windows

Параметр	Значение
`network.negotiate-auth.allow-proxies`	`True`
`network.negotiate-auth.delegation-uris`	`.termidesk.local`
`network.negotiate-auth.trusted-uris`	`.termidesk.local`

На пользовательской рабочей станции с ОС Astra Linux Special Edition:

- для работы технологии единого входа с Kerberos-аутентификацией изменить файл `/etc/krb5.conf`, добавив в раздел `libdefaults` параметр `forwardable = true`:

```
[libdefaults]
forwardable = true
...
```

- для настройки веб-браузера Chromium нужно:
  - в файл `/etc/chromium/policies/managed/policies.json` добавить строки:

```
{
    "AuthServerAllowlist": "*.termidesk.local" ,
    "AuthNegotiateDelegateAllowlist": "*.termidesk.local"
}
```

  где:

  `*.termidesk.local` - имя домена, для которого применяется Kerberos-аутентификация;

- для настройки веб-браузера Яндекс.Браузер нужно:
  - создать каталог `/etc/opt/yandex/browser/policies/managed`:

```
mkdir -p /etc/opt/yandex/browser/policies/managed
```

  - создать файл `/etc/opt/yandex/browser/policies/managed/policies.json` следующего содержания:

```
{
    "AuthServerAllowlist": "*.termidesk.local",
    "AuthNegotiateDelegateAllowlist": "*.termidesk.local"
```

```
}
```

- для настройки веб-браузера Mozilla Firefox нужно:
  - в адресной строке ввести `about:config`;
  - присвоить соответствующие значения параметрам, перечисленным в таблице (см. таблицу Данные для настройки Kerberos-аутентификации через веб-браузер Mozilla Firefox в ОС Astra Linux Special Edition).

Таблица 21. Данные для настройки Kerberos-аутентификации через веб-браузер Mozilla Firefox в ОС Astra Linux Special Edition

Параметр	Значение
`network.negotiate-auth.allow-proxies`	`True`
`network.negotiate-auth.delegation-uris`	`.termidesk.local`
`network.negotiate-auth.trusted-uris`	`.termidesk.local`

Добавление домена аутентификации Альт Домен

Для добавления домена аутентификации Альт Домен администратору Termidesk VDI следует перейти «Системные параметры - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «Альт Домен».

Затем необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления аутентификации через Альт Домен).

Таблица 22. Данные для добавления аутентификации через Альт Домен

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения домена аутентификации
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий. Порядок отображения доменов зависит от приоритета домена и его наименования: • чем ниже приоритет, тем выше домен в списке; • при наличии доменов с одинаковым приоритетом действует сортировка по алфавиту
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных. Параметр используется для поиска аналогичного домена «Универсального диспетчера», поэтому должен быть одинаковым как на портале «Агрегатор» (при его использовании), так и на «Универсальном диспетчере». Поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)

Параметр	Описание
«Субъекты»	Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: • «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»; • «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»; • «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»; • «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала

Параметр	Описание
«Порталы»	Выбор порталов фермы Termidesk VDI, для которых будет доступен домен аутентификации. Если портал не выбран, то домен аутентификации не будет доступен для него. В списке доступных значений отображаются все узлы со страницы «Инфраструктура - Порталы» с их полным доменным именем. Администратору нужно выбирать узел в соответствии со значением, указанным в параметре «Субъекты». Примеры: • если в параметре «Субъекты» указано «Пользователи», то в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Администраторы и персонал», в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу администратора», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Все», то в параметре «Порталы» может быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу администратора», либо «Порталу универсальному». Значение выбирается исходя из потребностей в разделении доменов аутентификации для того или иного субъекта. При изменении списка узлов на странице «Инфраструктура - Порталы»: • если узел удален, то он автоматически удалится из списка доступных значений для этого параметра. Уже назначенное значение удалится из свойств домена аутентификации; • если узел добавлен, то он автоматически добавится в список доступных значений для этого параметра, но не будет автоматически выбран для использования. В случае, если в параметре «Порталы» был указан единственный узел, который затем был удален из «Инфраструктура - Порталы», то этот домен аутентификации не будет доступен ни в каком из порталов. Для выбора всех порталов используется значение «Все»
«Сервер LDAP»	IP-адрес или доменное имя сервера службы каталогов, являющегося источником сведений о субъектах и их полномочиях

Параметр	Описание
«Порт»	TCP-порт, на котором запущена служба каталогов. Возможные стандартные значения: • «389» (по умолчанию). Используется, если доступ к службе каталогов осуществляется по протоколу LDAP; • «636». Используется, если доступ к службе каталогов осуществляется по протоколу LDAPS; • «3268». Альтернативный порт. Используется, если доступ к службе каталогов осуществляется по протоколу LDAP; • «3269». Альтернативный порт. Используется, если доступ к службе каталогов осуществляется по протоколу LDAPS. Для ускорения поиска пользователей в службе каталогов рекомендуется указывать альтернативный порт
«Использовать SSL»	Использовать защищенное соединение при взаимодействии со службой каталогов

Параметр	Описание

«Проверять SSL»	Выполнять проверку цепочки сертификатов и имени (hostname) сервера службы каталогов.
	
	Возможные значения:
	
	• «Да» (по умолчанию для создаваемых доменов) - использовать механизм проверки. Если при этом выключен параметр «Использовать SSL», то значение «Проверять SSL» не применяется (то есть, проверка сертификатов отключена). Если используется защищенное соединение и включен механизм проверки, то TLS-соединение будет установлено только при отсутствии ошибок проверки сертификатов и имя сервера службы каталогов;
	• «Нет» (по умолчанию для уже созданных ранее доменов) - не использовать механизм проверки. Если при этом включен параметр «Использовать SSL», то ошибки при проверке сертификатов не влияют на подключение (TLS-соединение все равно будет установлено)
	
	Корневой сертификат УЦ должен быть добавлен на узел «Портала администратора» (см. подраздел **Установка корневого сертификата центра сертификации**). При этом:
	
	• сертификат должен быть задан в формате `Base64`, пример:
	
	`-----BEGIN CERTIFICATE-----`
	`MIIDVzCCAj+gAwIBAgIQPvc7pjfS`
	`f5VLzNdgExZPxzANBgkqhkiG9w0B`
	`AQsFADA+`
	`MRMwEQYKCZImiZPyLGQBGRYDbGFu`
	`MRIwEAYKCZImiZPyLGQBGRYCc2Qx`
	`EzARBgNV`
	`....`
	`-----END CERTIFICATE-----`
	
	• использование параметра `REQUESTS_CA_BUNDLE` конфигурационного файла `termidesk.conf` опционально: достаточно добавить корневой сертификат в системное хранилище ОС, но работа с параметром также поддерживается.

Параметр	Описание
«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/msad/»
«Учётная запись»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Учетная запись в формате Distinguished Name (DN) в домене MS AD (LDAP), используемая для подключения к службе каталогов. Пример: «CN=admin,OU=user,DC=test,DC=desk»
«Пароль учётной записи»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Набор символов, подтверждающий полномочия объекта для подключения к службе каталогов
«Время ожидания соединения, с»	Время ожидания (в секундах) ответа от службы каталогов. Значение по умолчанию: «10»
«Корень поиска»	Корень поиска в службе каталогов в формате DN. Параметру следует задавать значение, соответствующее записи верхнего уровня в иерархии службы каталогов (без указания OU). Вводимое значение не должно содержать пробелов: • в начале и конце строки; • рядом с разделителями (запятыми); • в элементах пути (например, «DC=company name,DC=de»). Пример: «DC=test,DC=desk»
«Имя класса пользователя»	Атрибут класса пользователя в службе каталогов. Для корректного заполнения данного поля необходимо указать значение «person»

Параметр	Описание
«Атрибут идентификатора пользователя»	Атрибут уникального имени или идентификатора пользователя в службе каталогов. Для корректного заполнения данного поля необходимо указать: • значение «name», если активирован параметр «Использовать PKINIT»; Атрибут идентификатора пользователя задается с учетом того, какой шаблон использовался при выдаче сертификата пользователя. Например, значение «name» для механизма аутентификации Kerberos PKINIT указывается в том случае, если сертификат для подключения выдан на имя пользователя. • значение «userPrincipalName», если в параметре «Формат имени пользователя для аутентификации» используется «userPrincipalName»; • значение «SamAccountName» в остальных случаях
«Список атрибутов пользователя»	Список атрибутов, содержащий уникальные данные пользователя, разделенные запятыми. Для корректного заполнения данного поля необходимо указать значение: • «userPrincipalName», если в параметре «Формат имени пользователя для аутентификации» используется «userPrincipalName»; • «name», если в параметре «Формат имени пользователя для аутентификации» используется «sAMAccountName»
«Формат имени пользователя для аутентификации»	Формат имени пользователя, заданный в службе каталогов. Если на пользовательской рабочей станции установлен компонент «Клиент» версии, младше 6.0, то он будет поддерживать только формат «sAMAccountName». Возможные значения: • «sAMAccountName» (по умолчанию) - имя пользователя без доменной части; • «userPrincipalName» - имя пользователя с доменной частью

Параметр	Описание
«Имя атрибута группы»	Атрибут принадлежности к группе в службе каталогов. Для корректного заполнения данного поля необходимо указать значение «group»
«Имя атрибута группы»	Атрибут принадлежности к группе в службе каталогов. Для корректного заполнения данного поля необходимо указать значение «group»
«Атрибут имени группы»	Атрибут идентификатора группы, к которой относится субъект в службе каталогов. Для корректного заполнения данного поля необходимо указать: • значение «distinguishedname», если включены параметры «Использовать рекурсивный поиск групп» или «Использовать обратный порядок проверки членства пользователей»; • значение «name», если активирован параметр «Использовать PKINIT» или «Использовать Kerberos»; Атрибут имени группы задается с учетом того, какой шаблон использовался при выдаче сертификата пользователя. Например, значение «name» для механизма аутентификации Kerberos PKINIT указывается в том случае, если сертификат для подключения выдан на имя пользователя. • значение «cn» в остальных случаях. Если используется значение «distinguishedname», то при добавлении группы в домен аутентификации по пути «Системные параметры - Домены аутентификации - Наименование домена - Группы» нужно указывать длинные имена групп, например: «CN=RootGroup,CN=Users,DC=test,DC=desk». Если используется значение «cn», то нужно указывать короткие имена групп. Если параметр «Атрибут имени группы» был изменен, то необходимо заново добавить группы, используя соответствующие имена групп: для «cn» - короткие имена, для «distinguishedname» - длинные имена
«Атрибут членства в группе»	Идентификатор группы для назначения полномочий субъекту. Для корректного заполнения данного поля необходимо указать значение «member»
«Атрибут групп для LDAP-запросов»	Атрибут, определяющий группы пользователя при запросах к службе каталогов. Возможные значения: «objectClass», «objectCategory»

Параметр	Описание
«Время хранения дополнительных атрибутов учетной записи пользователей, сут»	Срок хранения (в сутках) дополнительных атрибутов учетной записи пользователей в БД. При наступлении срока данные будут очищены. Возможные значения: • «0» (по умолчанию) - не хранить дополнительные атрибуты; • числовое значение - хранить дополнительные атрибуты на протяжении заданного срока
«Использовать рекурсивный поиск групп»	При запросе групп пользователя будут учтены его родительские группы, в которых он состоит неявно. Если дополнительно включен параметр «Использовать обратный порядок проверки членства пользователей», то параметр «Использовать рекурсивный поиск групп» можно не включать. Возможные значения: • «Да» - использовать рекурсивный поиск; • «Нет» (по умолчанию) - не использовать рекурсивный поиск
«Использовать обратный порядок проверки членства пользователей»	Проверка соответствия членства пользователя в группах службы каталогов членству в группах домена аутентификации. Для работы функционала необходимо, чтобы был задан параметр «Атрибут имени группы». Этот параметр нужно включить при большом количестве групп непосредственно на службе каталогов. В этом случае сначала будет проверяться вхождение пользователя в группы домена аутентификации (в том числе рекурсивно), затем будет происходить проверка найденных групп в службе каталогов. При выключении этого параметра применяется настройка выбора «Атрибут групп для LDAP-запросов»: «objectClass» или «objectCategory». При включении этого параметра всегда применяется настройка выбора «Атрибут групп для LDAP-запросов»: «objectClass». Возможные значения: • «Да» - использовать обратный порядок; • «Нет» (по умолчанию) - не использовать обратный порядок
«Метадомен аутентификации»	Выбор метадомена аутентификации, в который будет входить добавляемый домен. Метадомен аутентификации должен быть предварительно создан (см. подраздел **Добавление метадомена аутентификации**)

Параметр	Описание

«Динамическая проверка членства пользователя в группах»	Управление динамической проверкой вхождения пользователя в группу службы каталогов.
	
	Параметр определяет, как будет происходить проверка нахождения пользователя в группе службы каталогов при аутентификации в Termidesk VDI и получении ресурсов.
	
	Особенности функционирования:
	
	• если пользователю уже назначено РМ, то проверяется вхождение пользователя в группу, указанную в свойствах фонда РМ. Проверка выполняется каждый раз при доступе к ресурсу. При этом если у пользователя отозваны права на доступ, то он:
	  - либо не увидит скрытый ресурс в зависимости от настройки «Скрывать недоступные ресурсы»;
	  - либо увидит, но не сможет получить доступ к нему;
	  - либо получит доступ к назначенному РМ, если права доступа были назначены на другую группу, в которую входит пользователь и которая указана в свойствах фонда РМ;
	  - либо получит доступ к назначенному РМ, если оно назначено на учетную запись пользователя напрямую.
	
	Возможные значения:
	
	• «Режим совместимости 6.0» (по умолчанию) - при аутентификации пользователя происходит запрос к службе каталогов для проверки его вхождения в группы. После этого группы пользователя актуализируются в БД. При попытке получить ресурс из фонда доступ определяется на основе информации из БД (БД не обновляется);
	• «Периодическое обновление» - если пользователя нет в БД и он впервые аутентифицируется, то происходит запрос к службе каталогов для получения актуальной информации о нем. Если пользователь есть в БД, то информация берется из нее. Актуализация пользователей и групп для всех доменов аутентификации с этим значением выполняется периодической фоновой задачей раз в 24 часа;
	• «Динамическая проверка» - при аутентификации пользователя или получении ресурсов происходит запрос к службе каталогов для получения актуальной информации о нем. При обращении к службе каталогов информация о полученных группах кешируется во внутренней памяти. Время кеширования определяется системным параметром «Таймаут кеша хранения групп домена, с»

Добавление домена аутентификации OIDC

OIDC - это механизм, позволяющий приложению связаться со службой идентификации IdP, получить данные о пользователе и вернуть их обратно в приложение. Таким образом OIDC обеспечивает аутентификацию администраторов и пользователей без необходимости ввода логина и пароля.

Служба идентификации IdP (например, keycloak) должна быть предварительно настроена в инфраструктуре организации для возможности использования OIDC как домена аутентификации.

Поддерживаются следующие типы аутентификации:

- по идентификатору и секрету. В этом случае используются параметры «Client ID» и «Client Secret», заданные в службе идентификации IdP;
- по подписанному JWT-токену. В этом случае используются параметры «Client ID» и «Signed Jwt», заданные в службе идентификации IdP. Закрытый ключ, использующийся для подписи JWT-токена, должен быть загружен на узлы «Универсального диспетчера» («Портал администратора», «Портал пользователя»).

Для добавления домена аутентификации OIDC следует перейти «Системные параметры - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «OIDC».

Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления аутентификации через OIDC).

Для сохранения параметров конфигурации использовать экранную кнопку **[Сохранить]**.

Таблица 23. Данные для добавления аутентификации через OIDC

Параметр	Описание
«Название»	Параметр обязателен для заполнения. Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Приоритет использования домена аутентификации при проверке субъекта и его полномочий. Порядок отображения доменов зависит от приоритета домена и его наименования: • чем ниже приоритет, тем выше домен в списке; • при наличии доменов с одинаковым приоритетом действует сортировка по алфавиту
«Метка»	Параметр обязателен для заполнения. Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk VDI. Начиная с Termidesk VDI версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)

Параметр	Описание
«Субъекты»	Параметр обязателен для заполнения. Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: • «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»; • «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»; • «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»; • «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала

Параметр	Описание
«Порталы»	Параметр обязателен для заполнения. Выбор порталов фермы Termidesk VDI, для которых будет доступен домен аутентификации. Если портал не выбран, то домен аутентификации не будет доступен для него. В списке доступных значений отображаются все узлы со страницы «Инфраструктура - Порталы» с их полным доменным именем. Администратору нужно выбирать узел в соответствии со значением, указанным в параметре «Субъекты». Примеры: • если в параметре «Субъекты» указано «Пользователи», то в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Администраторы и персонал», в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу администратора», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Все», то в параметре «Порталы» может быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу администратора», либо «Порталу универсальному». Значение выбирается исходя из потребностей в разделении доменов аутентификации для того или иного субъекта. При изменении списка узлов на странице «Инфраструктура - Порталы»: • если узел удален, то он автоматически удалится из списка доступных значений для этого параметра. Уже назначенное значение удалится из свойств домена аутентификации; • если узел добавлен, то он автоматически добавится в список доступных значений для этого параметра, но не будет автоматически выбран для использования. В случае, если в параметре «Порталы» был указан единственный узел, который затем был удален из «Инфраструктура - Порталы», то этот домен аутентификации не будет доступен ни в каком из порталов. Для выбора всех порталов используется значение «Все»
«Client ID»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Уникальный идентификатор приложения, полученный от службы идентификации IdP. Пример: «openid-test-cl»

Параметр	Описание
«Client secret»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Ключ приложения, полученный от службы идентификации IdP. Параметр должен быть пустым, если задан параметр «Приватный Ключ»
«Приватный Ключ»	Путь к закрытому ключу, использующемуся для подписи JWT-токена. Закрытый ключ, используемый в службе идентификации IdP, должен быть добавлен на сервер Termidesk VDI. Для этого: • скопировать его в каталог `/etc/opt/termidesk-vdi/`; • назначить владельцем файла пользователя `termidesk`: `sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.key` Пример: «/etc/opt/termidesk-vdi/client.key»
«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Требуется использовать статические данные (префикс `hvac-kv`). Пример: «hvac-kv://secret#termidesk-admin/oidc/»
«Authorization endpoint»	Параметр обязателен для заполнения. URL-адрес авторизации службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/auth»
«Logout endpoint»	Параметр обязателен для заполнения. URL-адрес получения информации о завершении сессии пользователя от службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/logout»

Параметр	Описание
«Token endpoint»	Параметр обязателен для заполнения. URL-адрес получения токена службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/token»
«Userinfo endpoint»	Параметр обязателен для заполнения. URL-адрес получения информации о пользователе от службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/userinfo»
«JWKS URI»	URL-адрес получения сертификатов службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/certs»
«Scope»	Параметр обязателен для заполнения. Набор областей действия, поддерживаемый в службе идентификации IdP. Области действия определяются спецификацией протокола OAuth 2.0. Неполный список возможных значений (указываются через пробел): • «openid» (обязательное значение для OIDC) - запуск аутентификации с использованием OIDC; • «profile» - доступ к профилю пользователя; • «email» - доступ к адресу электронной почты пользователя; • «offline_access» - обновление токена доступа без необходимости повторной аутентификации; • «groups» - доступ к списку ролей пользователя. Значение по умолчанию: «openid email profile groups». Если нужно указать другой набор значений, следует убедиться, что он поддерживается используемой службой идентификации IdP
«Атрибут имени пользователя»	Имя атрибута, в котором хранится имя пользователя (логин) в службе идентификации IdP. Значение по умолчанию: «email»
«Проверка SSL»	Проверка использования SSL
«Метадомен аутентификации»	Выбор метадомена аутентификации, в который будет входить добавляемый домен. Метадомен аутентификации должен быть предварительно создан (см. подраздел **Добавление метадомена аутентификации**)

Параметр	Описание

«Динамическая проверка членства пользователя в группах»	Управление динамической проверкой вхождения пользователя в группу службы каталогов.
	
	Параметр определяет, как будет происходить проверка нахождения пользователя в группе службы каталогов при аутентификации в Termidesk VDI и получении ресурсов.
	
	Особенности функционирования:
	
	• если пользователю уже назначено РМ, то проверяется вхождение пользователя в группу, указанную в свойствах фонда РМ. Проверка выполняется каждый раз при доступе к ресурсу. При этом если у пользователя отозваны права на доступ, то он:
	  - либо не увидит скрытый ресурс в зависимости от настройки «Скрывать недоступные ресурсы»;
	  - либо увидит, но не сможет получить доступ к нему;
	  - либо получит доступ к назначенному РМ, если права доступа были назначены на другую группу, в которую входит пользователь и которая указана в свойствах фонда РМ;
	  - либо получит доступ к назначенному РМ, если оно назначено на учетную запись пользователя напрямую.
	
	Возможные значения:
	
	• «Режим совместимости 6.0» (по умолчанию) - при аутентификации пользователя происходит запрос к службе каталогов для проверки его вхождения в группы. После этого группы пользователя актуализируются в БД. При попытке получить ресурс из фонда доступ определяется на основе информации из БД (БД не обновляется);
	• «Периодическое обновление» - если пользователя нет в БД и он впервые аутентифицируется, то происходит запрос к службе каталогов для получения актуальной информации о нем. Если пользователь есть в БД, то информация берется из нее. Актуализация пользователей и групп для всех доменов аутентификации с этим значением выполняется периодической фоновой задачей раз в 24 часа;
	• «Динамическая проверка» - при аутентификации пользователя или получении ресурсов происходит запрос к службе каталогов для получения актуальной информации о нем. При обращении к службе каталогов информация о полученных группах кешируется во внутренней памяти. Время кеширования определяется системным параметром «Таймаут кеша хранения групп домена, с»

Добавление домена аутентификации RADIUS

Для добавления домена аутентификации RADIUS администратору Termidesk VDI следует перейти «Системные параметры - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «RADIUS».

Затем необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления аутентификации Radius).

Таблица 24. Данные для добавления аутентификации Radius

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий. Порядок отображения доменов зависит от приоритета домена и его наименования: • чем ниже приоритет, тем выше домен в списке; • при наличии доменов с одинаковым приоритетом действует сортировка по алфавиту
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk VDI. Начиная с Termidesk VDI версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)
«Субъекты»	Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: • «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»; • «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»; • «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»; • «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала

Параметр	Описание
«Порталы»	Выбор порталов фермы Termidesk VDI, для которых будет доступен домен аутентификации. Если портал не выбран, то домен аутентификации не будет доступен для него. В списке доступных значений отображаются все узлы со страницы «Инфраструктура - Порталы» с их полным доменным именем. Администратору нужно выбирать узел в соответствии со значением, указанным в параметре «Субъекты». Примеры: • если в параметре «Субъекты» указано «Пользователи», то в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Администраторы и персонал», в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу администратора», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Все», то в параметре «Порталы» может быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу администратора», либо «Порталу универсальному». Значение выбирается исходя из потребностей в разделении доменов аутентификации для того или иного субъекта. При изменении списка узлов на странице «Инфраструктура - Порталы»: • если узел удален, то он автоматически удалится из списка доступных значений для этого параметра. Уже назначенное значение удалится из свойств домена аутентификации; • если узел добавлен, то он автоматически добавится в список доступных значений для этого параметра, но не будет автоматически выбран для использования. В случае, если в параметре «Порталы» был указан единственный узел, который затем был удален из «Инфраструктура - Порталы», то этот домен аутентификации не будет доступен ни в каком из порталов. Для выбора всех порталов используется значение «Все»

Параметр	Описание
«RADIUS сервер»	IP-адрес или доменное имя ресурса, являющегося источником сведений о субъектах и их полномочиях (сервер RADIUS) Если осуществляется подключение к серверу NPS (Network Policy Server), то доменное имя ресурса нужно указывать заглавными символами.
«Аутентификационный порт»	Порт для обработки запросов на аутентификацию
«Секрет»	Набор символов (пароль), подтверждающий подключение к серверу RADIUS
«NAS-Identifier»	Идентификатор фермы Termidesk VDI, используемый при отправке запросов на сервер RADIUS. Значение по умолчанию: «termidesk-server»
«Время ожидания соединения, с»	Максимальное время ожидания (в секундах) для установки соединения
«Регистрозависимость»	Учитывать регистр символов в имени пользователя при аутентификации. Активация параметра позволяет обрабатывать имена пользователей с отличающимся регистром как разные учетные записи. При этом выполняется создание новых учетных записей в интерфейсе Termidesk VDI, а каждому пользователю может быть назначено отдельное РМ. Отключение параметра позволяет обрабатывать имена пользователей с отличающимся регистром как одну учетную запись. При этом создание новых учетных записей в интерфейсе Termidesk VDI не выполняется, а пользователь подключается к одному и тому же РМ. Возможные значения: • «Да» - регистр символов учитывается; • «Нет» (по умолчанию) - регистр символов не учитывается
«Использовать OTP»	Использовать при аутентификации пользователя OTP - механизм, позволяющий применять одноразовые пароли для дополнительной аутентификации. Сервер RADIUS должен быть настроен на аутентификацию пользователей с использованием OTP. Возможные значения: • «Да» - использовать механизм; • «Нет» (по умолчанию) - не использовать механизм

Параметр	Описание
«Режим аутентификации»	Выбор режима, который будет использован при аутентификации пользователя. Для работы функционала нужно активировать параметр «Использовать OTP». На сервере RADIUS должен быть настроен соответствующий режим аутентификации (примеры настроек приведены в подразделе интеграции с системами сайта документации Termidesk VDI: **Примеры параметров конфигурации сервера RADIUS для работы в различных режимах аутентификации**). Возможные значения: • «Одноэтапный (только Access-Request)» (по умолчанию) - пароль и OTP пользователя передаются для проверки одновременно. Проверка учетных данных выполняется за один этап аутентификации; • «Многоэтапный (Access-Request + Access-Challenge)» - пароль и OTP пользователя передаются для проверки последовательно. Проверка учетных данных выполняется за несколько этапов аутентификации
«Метадомен аутентификации»	Выбор метадомена аутентификации, в который будет входить добавляемый домен. Метадомен аутентификации должен быть предварительно создан (см. подраздел **Добавление метадомена аутентификации**)

Параметр	Описание

«Динамическая проверка членства пользователя в группах»	Управление динамической проверкой вхождения пользователя в группу службы каталогов.
	
	Параметр определяет, как будет происходить проверка нахождения пользователя в группе службы каталогов при аутентификации в Termidesk VDI и получении ресурсов.
	
	Особенности функционирования:
	
	• если пользователю уже назначено РМ, то проверяется вхождение пользователя в группу, указанную в свойствах фонда РМ. Проверка выполняется каждый раз при доступе к ресурсу. При этом если у пользователя отозваны права на доступ, то он:
	  - либо не увидит скрытый ресурс в зависимости от настройки «Скрывать недоступные ресурсы»;
	  - либо увидит, но не сможет получить доступ к нему;
	  - либо получит доступ к назначенному РМ, если права доступа были назначены на другую группу, в которую входит пользователь и которая указана в свойствах фонда РМ;
	  - либо получит доступ к назначенному РМ, если оно назначено на учетную запись пользователя напрямую.
	
	Возможные значения:
	
	• «Режим совместимости 6.0» (по умолчанию) - при аутентификации пользователя происходит запрос к службе каталогов для проверки его вхождения в группы. После этого группы пользователя актуализируются в БД. При попытке получить ресурс из фонда доступ определяется на основе информации из БД (БД не обновляется);
	• «Периодическое обновление» - если пользователя нет в БД и он впервые аутентифицируется, то происходит запрос к службе каталогов для получения актуальной информации о нем. Если пользователь есть в БД, то информация берется из нее. Актуализация пользователей и групп для всех доменов аутентификации с этим значением выполняется периодической фоновой задачей раз в 24 часа;
	• «Динамическая проверка» - при аутентификации пользователя или получении ресурсов происходит запрос к службе каталогов для получения актуальной информации о нем. При обращении к службе каталогов информация о полученных группах кешируется во внутренней памяти. Время кеширования определяется системным параметром «Таймаут кеша хранения групп домена,с»

Валидация заданных параметров экранной кнопкой **[Тест]** проверяет корректность заданного имени сервера (возможность получить IP-адрес, используя DNS), доступность сервера (корректный порт, работоспособность сервера RADIUS).

После добавления домена аутентификации RADIUS необходимо перейти в созданный объект и указать актуальный список групп, пользователи которых могут производить вход в Termidesk VDI.

При дальнейшей эксплуатации сервер Termidesk VDI, обрабатывая запрос на аутентификацию, получает актуальный список групп пользователя и сравнивает со своей

конфигурацией. Если ни одного совпадения не обнаружено, то пользователю будет отказано в доступе.

Конфигурация сервера RADIUS должна учитывать передачу списка групп пользователя в атрибуте с ключом 25 (Class) в ответе со статусом авторизации.

Для корректного получения списка групп на Termidesk VDI сервер RADIUS может быть настроен следующим образом:

Пример настройки приведен для сервера freeRADIUS.

- файл `/etc/freeradius/3.0/mods-enabled/ldap` должен содержать конструкцию вида:

```
ldap {
...
  update {
     ...
     reply:memberOf                  += 'memberOf'
  }
...
}
```

- в файл `/etc/freeradius/3.0/dictionary` необходимо добавить строку:

```
ATTRIBUTE       memberOf                3001    string
```

- в файле `/etc/freeradius/3.0/sites-enabled/default` необходимо найти секцию `post-auth` и добавить регулярное выражение, фильтрующее название группы из получаемых от сервера атрибутов:

```
foreach &reply:memberOf {
       if ("%{Foreach-Variable-0}" =~ /cn=([^,=]+)/i)
           }
```

- в файле `/etc/freeradius/3.0/mods-enabled/exec` указать для параметра `wait` значение `yes`:

```
wait = yes
```

Для корректной работы автоматического входа пользователя (SSO) нужно настроить конфигурацию сервера RADIUS:

- скорректировать файл `/etc/freeradius/3.0/mods-available/ldap`, добавив фильтр в секции `user`:

```
user {
                base_dn = "${..base_dn}"
```

```
...
                # Фильтр: поиск по sAMAccountName ИЛИ по userPrincipalName (UPN)
                filter = "(|(sAMAccountName=%{%{Stripped-User-Name}:-%{User-
Name}})(userPrincipalName=%{User-Name}))"
...
}
```

- остальные параметры настроить аналогично примеру выше.

Добавление аутентификации через SAML

Провайдер SAML - это единая точка входа пользователей в распределенной системе, позволяющей аутентифицироваться в разных и несвязных между собой частях системы посредством веб-браузера. Независимо от того, какой используется тип биндинга (binding), всегда происходит перенаправление на страницу аутентификации «Провайдер SAML».

Для добавления аутентификации через SAML администратору Termidesk VDI следует перейти «Системные параметры - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «SAML».

Затем необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления аутентификации через SAML).

Для работы с сертификатами при получении метаданных от домена аутентификации SAML необходимо установить корневой сертификат центра сертификации и настроить Termidesk VDI на работу с сертификатами (см. подраздел **Установка корневого сертификата центра сертификации**).

Таблица 25. Данные для добавления аутентификации через SAML

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Приоритет использования домена аутентификации при проверке субъекта и его полномочий. Порядок отображения доменов зависит от приоритета домена и его наименования: • чем ниже приоритет, тем выше домен в списке; • при наличии доменов с одинаковым приоритетом действует сортировка по алфавиту
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk VDI. Начиная с Termidesk VDI версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)

Параметр	Описание
«Субъекты»	Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: • «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»; • «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»; • «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»; • «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала

Параметр	Описание
«Порталы»	Выбор порталов фермы Termidesk VDI, для которых будет доступен домен аутентификации. Если портал не выбран, то домен аутентификации не будет доступен для него. В списке доступных значений отображаются все узлы со страницы «Инфраструктура - Порталы» с их полным доменным именем. Администратору нужно выбирать узел в соответствии со значением, указанным в параметре «Субъекты». Примеры: • если в параметре «Субъекты» указано «Пользователи», то в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Администраторы и персонал», в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу администратора», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Все», то в параметре «Порталы» может быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу администратора», либо «Порталу универсальному». Значение выбирается исходя из потребностей в разделении доменов аутентификации для того или иного субъекта. При изменении списка узлов на странице «Инфраструктура - Порталы»: • если узел удален, то он автоматически удалится из списка доступных значений для этого параметра. Уже назначенное значение удалится из свойств домена аутентификации; • если узел добавлен, то он автоматически добавится в список доступных значений для этого параметра, но не будет автоматически выбран для использования. В случае, если в параметре «Порталы» был указан единственный узел, который затем был удален из «Инфраструктура - Порталы», то этот домен аутентификации не будет доступен ни в каком из порталов. Для выбора всех порталов используется значение «Все»
«ID клиента»	Уникальный идентификатор клиента на сервисе аутентификации SAML
«URL метаданных»	URL для подключения к сервису аутентификации SAML
«Проверка SSL»	Проверка использования SSL
«Тип Биндинга»	Способ отправки ответа сервисом SAML на запрос аутентификации. Поддерживаются следующие типы: HTTP-Redirect, HTTP-POST
«Тип Биндинга в ответе»	Выбор типа биндинга для обратного перенаправления в SAML-запросе. Поддерживаются следующие типы: HTTP-Redirect, HTTP-POST
«Приватный ключ»	Набор символов приватного ключа для подписи SAML-запросов

Параметр	Описание
«Формат Name ID»	Формат сопоставления идентификаторов имен SAML у поставщиков удостоверений и поставщиков услуг
«Group Attr Name»	Тип атрибута пользователя (обычно в этом поле указывается значение «Group»)
«Время ожидания соединения, с»	Время ожидания (в секундах) ответа от SAML
«Метадомен аутентификации»	Выбор метадомена аутентификации, в который будет входить добавляемый домен. Метадомен аутентификации должен быть предварительно создан (см. подраздел **Добавление метадомена аутентификации**)

Параметр	Описание

«Динамическая проверка членства пользователя в группах»	Управление динамической проверкой вхождения пользователя в группу службы каталогов.
	
	Параметр определяет, как будет происходить проверка нахождения пользователя в группе службы каталогов при аутентификации в Termidesk VDI и получении ресурсов.
	
	Особенности функционирования:
	
	• если пользователю уже назначено РМ, то проверяется вхождение пользователя в группу, указанную в свойствах фонда РМ. Проверка выполняется каждый раз при доступе к ресурсу. При этом если у пользователя отозваны права на доступ, то он:
	  - либо не увидит скрытый ресурс в зависимости от настройки «Скрывать недоступные ресурсы»;
	  - либо увидит, но не сможет получить доступ к нему;
	  - либо получит доступ к назначенному РМ, если права доступа были назначены на другую группу, в которую входит пользователь и которая указана в свойствах фонда РМ;
	  - либо получит доступ к назначенному РМ, если оно назначено на учетную запись пользователя напрямую.
	
	Возможные значения:
	
	• «Режим совместимости 6.0» (по умолчанию) - при аутентификации пользователя происходит запрос к службе каталогов для проверки его вхождения в группы. После этого группы пользователя актуализируются в БД. При попытке получить ресурс из фонда доступ определяется на основе информации из БД (БД не обновляется);
	• «Периодическое обновление» - если пользователя нет в БД и он впервые аутентифицируется, то происходит запрос к службе каталогов для получения актуальной информации о нем. Если пользователь есть в БД, то информация берется из нее. Актуализация пользователей и групп для всех доменов аутентификации с этим значением выполняется периодической фоновой задачей раз в 24 часа;
	• «Динамическая проверка» - при аутентификации пользователя или получении ресурсов происходит запрос к службе каталогов для получения актуальной информации о нем. При обращении к службе каталогов информация о полученных группах кешируется во внутренней памяти. Время кеширования определяется системным параметром «Таймаут кеша хранения групп домена, с»

Добавление IP-аутентификации

Домен «IP аутентификация» позволяет определять назначение прав на основе сетевых адресов. Для добавления IP-аутентификации администратору Termidesk VDI следует перейти «Системные параметры - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «IP аутентификация».

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления IP-аутентификации).

Таблица 26. Данные для добавления IP-аутентификации

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения домена аутентификации
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий. Порядок отображения доменов зависит от приоритета домена и его наименования: • чем ниже приоритет, тем выше домен в списке; • при наличии доменов с одинаковым приоритетом действует сортировка по алфавиту
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk VDI. Начиная с Termidesk VDI версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)
«Субъекты»	Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: • «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»; • «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»; • «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»; • «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала

Параметр	Описание
«Порталы»	Выбор порталов фермы Termidesk VDI, для которых будет доступен домен аутентификации. Если портал не выбран, то домен аутентификации не будет доступен для него. В списке доступных значений отображаются все узлы со страницы «Инфраструктура - Порталы» с их полным доменным именем. Администратору нужно выбирать узел в соответствии со значением, указанным в параметре «Субъекты». Примеры: • если в параметре «Субъекты» указано «Пользователи», то в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Администраторы и персонал», в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу администратора», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Все», то в параметре «Порталы» может быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу администратора», либо «Порталу универсальному». Значение выбирается исходя из потребностей в разделении доменов аутентификации для того или иного субъекта. При изменении списка узлов на странице «Инфраструктура - Порталы»: • если узел удален, то он автоматически удалится из списка доступных значений для этого параметра. Уже назначенное значение удалится из свойств домена аутентификации; • если узел добавлен, то он автоматически добавится в список доступных значений для этого параметра, но не будет автоматически выбран для использования. В случае, если в параметре «Порталы» был указан единственный узел, который затем был удален из «Инфраструктура - Порталы», то этот домен аутентификации не будет доступен ни в каком из порталов. Для выбора всех порталов используется значение «Все»

Действия над группами в домене аутентификации

Группы – перечень объектов домена аутентификации, определяющих разрешения пользователей на доступ к фондам ВРМ. Перечень групп, доступных для добавления в Termidesk VDI, запрашивается у домена аутентификации.

Для просмотра групп следует перейти «Системные параметры - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации.

Доступны следующие действия над группами домена аутентификации:

- создание (добавление существующей в службе каталогов группы в Termidesk VDI). Для этого нужно нажать экранную кнопку **[Создать]**;
- редактирование. Для этого нужно пометить группу и нажать экранную кнопку **[Изменить]**. В режиме редактирования невозможно изменить идентификатор группы домена аутентификации, поскольку он получен автоматически от службы каталогов;
- удаление. Для этого нужно пометить группу и нажать экранную кнопку **[Удалить]**. Группа может быть удалена даже в том случае, если в ней есть пользователи;
- просмотр сведений таблицы «Группы»;

- назначение политик группе пользователей. Для этого нужно пометить группу и нажать экранную кнопку **[Политики]**. Значения по умолчанию наследуются от глобальных политик. Список политик и общее описание по применению политик приведено в подразделе **Политики**. Для разрешения ситуаций с порядком применения разного набора политик для объектов используется механизм приоритизации политик (параметр «Приоритет политик»);
- назначение тегов группе пользователей. Для этого нужно пометить группу и нажать экранную кнопку **[Теги]**. Общее описание по применению тегов приведено в подразделе **Общие сведения о тегах**.

Редактирование и удаление групп в домене аутентификации в «Портале администратора» Termidesk VDI не приводит к каким-либо изменениям объекта в службе каталогов.

Основные параметры списка групп приведены в таблице (см. таблицу Параметры списка групп домена аутентификации).

Таблица 27. Параметры списка групп домена аутентификации

Параметр	Описание
«Название»	Наименование группы
«Комментарий»	Информационное сообщение, используемое для описания группы
«Тип»	Тип группы
«Состояние»	Характеристика состояния субъектов группы
«Приоритет политик»	Приоритет действия политик для группы
«Теги»	Список тегов, назначенных группе. При выборе тега выполняется переход к разделу «Системные параметры – Управление тегами» со списком объектов, которым назначен данный тег

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом

для соответствующего столбца.

Для добавления доступны два типа групп:

- «Группа» - стандартная группа, созданная в службе каталогов и которая будет добавлена в Termidesk VDI (см. рисунок Окно добавления группы домена аутентификации);
- «Метагруппа» - группа, объединяющая несколько стандартных групп в Termidesk VDI (см. рисунок Окно добавления метагруппы домена аутентификации).

Для метагруппы недоступен функционал выбора политик группы. Создание метагруппы недоступно для домена аутентификации «IP аутентификация».

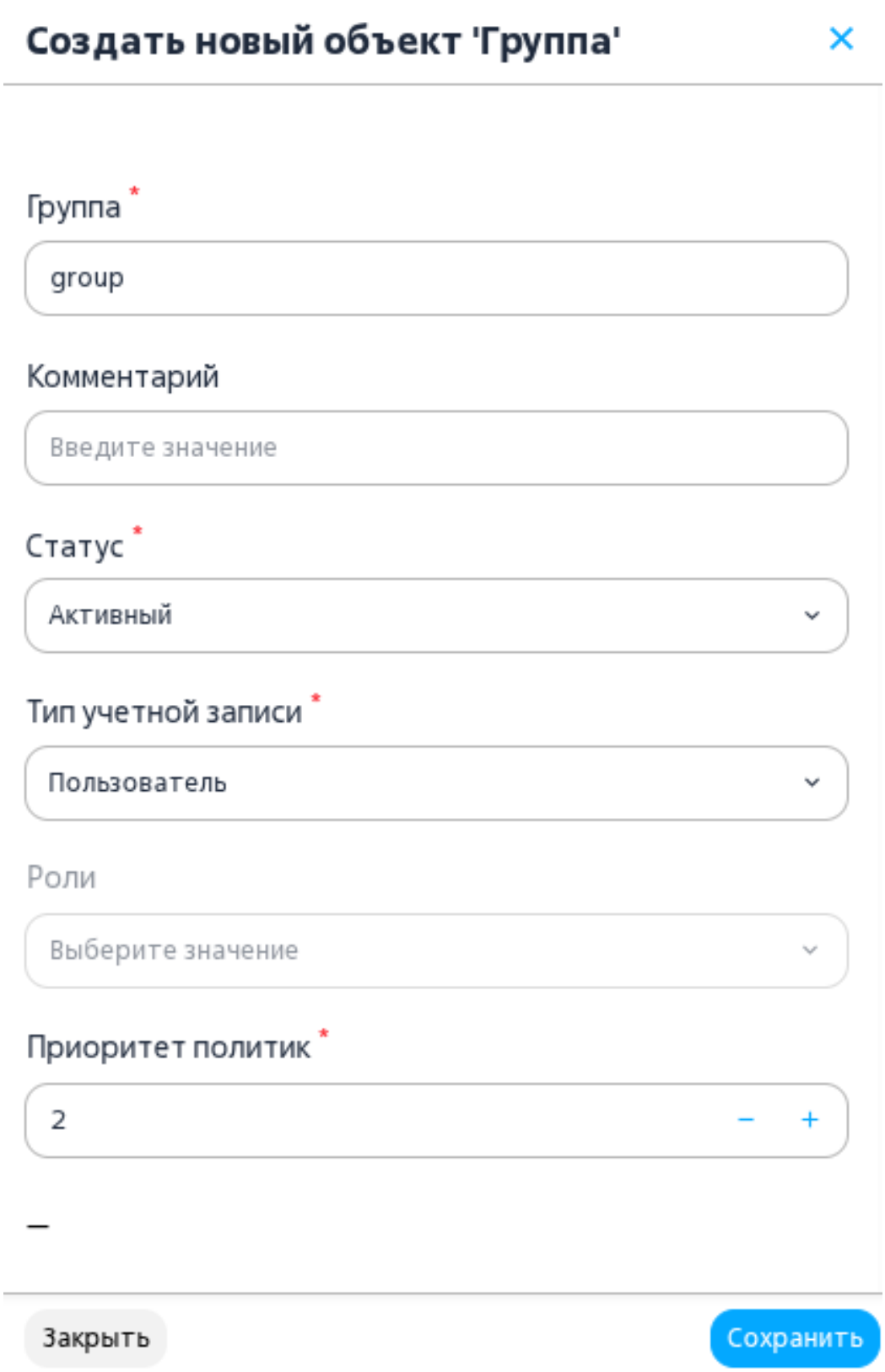


Рисунок 59. Окно добавления группы домена аутентификации

Для добавления группы администратору Termidesk VDI необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления группы домена аутентификации).

Таблица 28. Данные для добавления группы домена аутентификации

Параметр	Описание
«Группа»	Наименование группы, полученное от домена аутентификации. Для выбора группы из списка доступных необходимо начать ввод ее наименования
«Диапазон IP»	Параметр доступен только для домена аутентификации с типом «IP аутентификация». IP-адрес или IP-адреса группы. Может быть указан IP-адрес, диапазон IP-адресов, перечень IP-адресов. Пример: • «192.0.2.2»; • «192.0.2.0/24»; • «192.0.2.1/24, 192.0.2.5/24, 192.0.2.10/24»; • «192.0.2.2-192.0.2.253»
«Комментарий»	Информационное сообщение, используемое для описания группы
«Статус»	Характеристика состояния субъектов группы при доступе к фонду РМ. Доступные значения: • «Активный» - субъекты группы могут аутентифицироваться в Termidesk VDI; • «Неактивный» - субъекты группы не могут аутентифицироваться в Termidesk VDI; • «Временно заблокирован» - субъекты группы не могут аутентифицироваться в Termidesk VDI. Статус присваивается также по истечении попыток аутентификации, определенных в параметрах «Максимум попыток входа Администраторов», «Максимум попыток входа Персонала», «Максимум попыток входа Пользователей» на странице «Системные параметры - Системные настройки - Безопасность»
«Тип учетной записи»	Служебные функции субъектов группы при доступе к Termidesk VDI. Доступные значения параметра: • «Пользователь» - субъекты группы не будут иметь доступ к порталу администратора. При выборе этого значения параметр «Роли» будет пустым; • «Персонал» - субъекты группы будут иметь доступ к странице «Обзор» и будут обладать набором разрешений, определенных служебными функциями. При выборе этого значения в параметре «Роль» можно выбрать одно или несколько значений классов администратора, созданных на странице «Системные параметры - Управление ролями»; • «Администратор» - субъекты группы будут иметь полный доступ к порталу администратора. При выборе этого значения параметр «Роли» будет пустым
«Роли»	Назначение служебных функций пользователям группы. Доступность выбора значений зависит от параметра «Тип учетной записи» и того, созданы ли роли на странице «Системные параметры - Управление ролями»
«Приоритет политик»	Приоритет действия политик для группы пользователей. Чем меньше число, тем выше приоритет. Пример: пользователь состоит в двух группах домена аутентификации, для каждой из которой задан свой набор политик. В этом случае администратор должен настроить разные приоритеты применения политик для групп пользователя: одной группе задать приоритет выше, другой - ниже

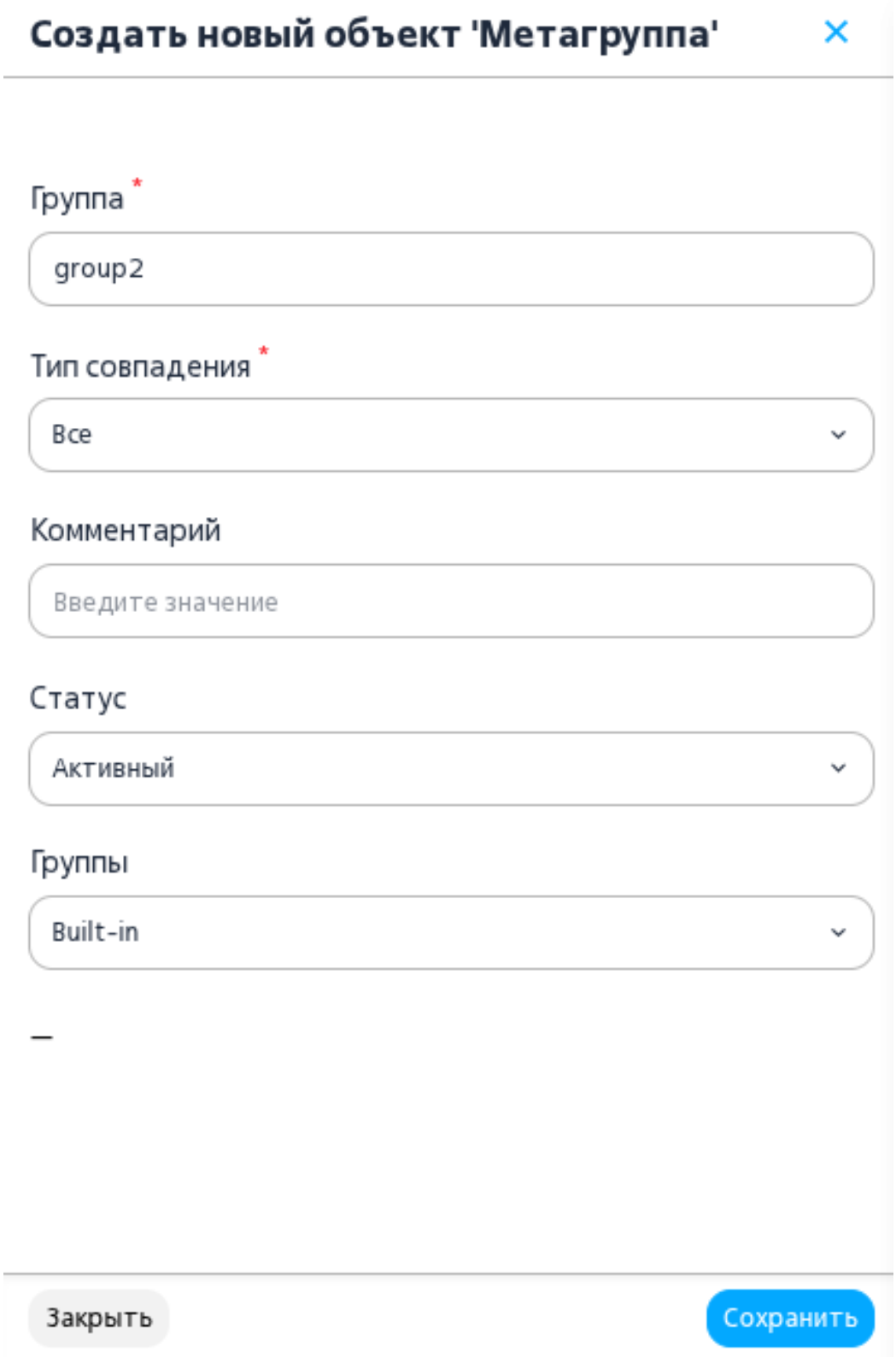


Рисунок 60. Окно добавления метагруппы домена аутентификации

Для добавления метагруппы администратору Termidesk VDI необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления метагруппы домена аутентификации).

Таблица 29. Данные для добавления метагруппы домена аутентификации

Параметр	Описание
«Группа»	Наименование группы

Параметр	Описание
«Диапазон IP»	Параметр доступен только для домена аутентификации с типом «IP аутентификация». IP-адрес или IP-адреса группы. Может быть указан IP-адрес, диапазон IP-адресов, перечень IP-адресов. Пример: • «192.0.2.2»; • «192.0.2.0/24»; • «192.0.2.1/24, 192.0.2.5/24, 192.0.2.10/24»; • «192.0.2.2-192.0.2.253»
«Тип совпадения»	Выбор способа определения принадлежности группы к метагруппе. Доступные значения: • «Любой» - любая из групп, перечисленных в параметре «Группы»; • «Все» (значение по умолчанию) - все группы, перечисленные в параметре «Группы»
«Комментарий»	Информационное сообщение, используемое для описания метагруппы
«Статус»	Характеристика состояния субъектов метагруппы при доступе к фонду ВРМ. Доступные значения: • «Активный» - субъекты метагруппы могут аутентифицироваться в Termidesk VDI; • «Неактивный» - субъекты метагруппы не могут аутентифицироваться в Termidesk
«Группы»	Наименования групп, к которым должна примениться метагруппа

Действия над пользователями в домене аутентификации

Пользователи – перечень объектов, имеющих в рамках домена аутентификации служебные функции на использование фондов РМ.

Создание учетной записи пользователя в Termidesk VDI выполняется после его первой авторизации на портале Termidesk VDI.

Администратору доступны следующие действия над пользователями внутри домена аутентификации:

- редактирование. Для редактирования пользователя следует выделить строку с именем пользователя и нажать экранную кнопку **[Изменить]**. Действие поддерживается и для домена аутентификации с типом «Встроенный»;
- удаление. Для удаления пользователя из домена аутентификации следует выделить строку с именем пользователя и нажать экранную кнопку **[Удалить]**. Действие поддерживается и для домена аутентификации с типом «Встроенный». Если у пользователя есть назначенное РМ, то его удаление будет недоступно;
- просмотр сведений.

Редактирование и удаление пользователя в домене аутентификации в указанных порталах Termidesk VDI не приводит к каким-либо изменениям объекта в службе каталогов.

В компоненте «Универсальный диспетчер» предусмотрена возможность

автоматической регистрации пользователей, запросивших опубликованные ресурсы через портал «Агрегатора». Для этого нужно, чтобы идентичные группы были добавлены как в доменах аутентификации портала «Агрегатор администратора», так и в доменах аутентификации «Портала администратора» Termidesk VDI. Если пользователь состоит в указанных группах, то после входа на портал «Агрегатора» и запроса ресурсов его учетная запись будет автоматически зарегистрирована для компонента «Универсальный диспетчер», использующегося в ферме Termidesk VDI.

Termidesk VDI хранит информацию о назначении прав пользователя в БД, поэтому в случае, если пользователь должен быть исключен из группы администрирования Termidesk VDI, то необходимо удалить пользователя из группы непосредственно в доменной службе каталогов и на стороне Termidesk VDI одновременно.

Для отображения списка пользователей следует перейти «Системные параметры - Домены аутентификации». Основные параметры списка приведены в таблице (см. таблицу Параметры списка пользователей).

Таблица 30. Параметры списка пользователей

Параметр	Описание
«Логин»	Идентификатор пользователя в домене аутентификации
«Имя»	Отображаемое имя пользователя в Termidesk
«Комментарий»	Информационное сообщение, используемое для описания назначения пользователя
«Тип пользователя»	Тип служебных функций, назначенный пользователю
«Состояние»	Характеристика состояния субъекта при доступе к фонду РМ
«Последний вход»	Временная метка, отражающая момент последней авторизации

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом

для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Для редактирования пользователя администратору Termidesk VDI необходимо заполнить данные, перечисленные в столбце «Параметр» следующей на таблицы (см. таблицу Данные для редактирования пользователя домена аутентификации).

Таблица 31. Данные для редактирования пользователя домена аутентификации

Параметр	Описание
«Логин»	Идентификатор субъекта в службе каталогов
«Имя»	Отображаемое имя субъекта в Termidesk
«Комментарий»	Информационное сообщение, используемое для описания назначения пользователя
«Статус»	Характеристика состояния субъекта при доступе к фонду РМ. Доступные значения: • «Активный» - субъект может аутентифицироваться в Termidesk VDI; • «Неактивный» - субъект не может аутентифицироваться в Termidesk VDI; • «Временно заблокирован» - субъект не может аутентифицироваться в Termidesk VDI. Статус присваивается также по истечении попыток аутентификации, определенных в параметрах «Максимум попыток входа Администраторов», «Максимум попыток входа Персонала», «Максимум попыток входа Пользователей» на странице «Системные параметры - Системные настройки - Безопасность». Время блокировки определяется параметром «Время блокировки входа» на странице «Системные параметры - Системные настройки - Общие»

Параметр	Описание
«Тип учетной записи»	Служебные функции субъекта при доступе к Termidesk VDI. Значение наследуется от группы, в которую входит пользователь. При этом по умолчанию тип учетной записи устанавливается в значение с более высоким уровнем прав. Пример: если пользователь одновременно состоит в группе с типом учетной записи «Администратор» и группе с типом «Пользователь», то по умолчанию для пользователя будет установлен тип учетной записи «Администратор». Доступные значения параметра: • «Пользователь» - субъект не будет иметь доступ к «Порталу администратора». При выборе этого значения параметр «Роли» будет пустым; • «Персонал» - субъект будет иметь доступ к странице «Обзор» и будет обладать набором разрешений, определенных служебными функциями. При выборе этого значения в параметре «Роль» можно выбрать одно или несколько значений классов администратора, созданных на странице «Системные параметры - Управление ролями»; • «Администратор» - субъект будет иметь полный доступ к «Порталу администратора». При выборе этого значения параметр «Роли» будет пустым Если пользователь состоит в группе администраторов Termidesk VDI, то ему автоматически будет присвоен тип учетной записи «Администратор» после первой авторизации на портале Termidesk VDI. Для того чтобы пользователь не обладал административными правами, нужно изменить для него параметр «Тип учетной записи» и удалить его из группы администраторов (либо изменить тип группы) Termidesk VDI.
«Группы»	Наименования групп, используемых для определения разрешений по доступу к фондам РМ. Назначение параметра «Группы» будет доступно, если «Тип учетной записи» соответствует «Персонал». Список групп пользователя будет получен автоматически от службы каталогов
«Роли»	Назначение служебной функции указанному пользователю. Доступность выбора значений зависит от параметра «Тип учетной записи» и того, созданы ли роли на странице «Системные параметры - Управление ролями». Назначение параметра «Роли» будет доступно, если «Тип учетной записи» соответствует «Персонал»

Просмотр данных о пользователе домена аутентификации

Для просмотра данных о пользователе домена аутентификации следует перейти «Системные параметры - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне перейти во вкладку «Пользователи» и нажать по ссылке с именем пользователя.

Для просмотра будут доступны таблицы:

- «Группы пользователя» - отображает информацию о вхождении пользователя в группы домена аутентификации;

- «Рабочие места пользователя» - отображает информацию о списке РМ пользователя;
- «Назначенные фонды» - отображает информацию о назначенных пользователю фондах;
- «Журнал» - отображает события аудита, связанные с действиями пользователя;
- «Атрибуты» - отображает атрибуты, назначенных пользователю.

Действия над атрибутами в домене аутентификации

Для домена аутентификации «Microsoft AD DS/LDAP» и «Альт Домен» поддерживается указание дополнительных атрибутов учетной записи пользователя, заданных в домене. Функционал предоставляет возможность сопоставлять учетные записи пользователей с различными объектами, например, подразделениями, в которые он входит.

Доступны следующие действия над атрибутами внутри домена аутентификации:

- создание;
- удаление.

Для просмотра списка атрибутов следует перейти «Системные параметры - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне перейти во вкладку «Атрибуты».

Основные параметры списка приведены в таблице (см. таблицу Параметры списка атрибутов домена аутентификации).

Таблица 32. Параметры списка атрибутов домена аутентификации

Параметр	Описание
«Атрибут»	Атрибут учетной записи пользователя из домена
«Название»	Отображаемое имя атрибута

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы;
- фильтрация записей таблицы через функцию «Умный фильтр».

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет

заблокирована, если нет изменений для возврата к исходному состоянию;

- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Для создания атрибута следует перейти «Системные параметры - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне перейти во вкладку «Атрибуты» и нажать экранную кнопку **[Создать]**.

Для добавления атрибута администратору Termidesk VDI необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления атрибута домена аутентификации).

Особенности функционирования:

- получение и сохранение атрибутов пользователя выполняется при первой авторизации;
- срок хранения атрибутов задается параметром «Время хранения дополнительных атрибутов учетной записи пользователей, сут»;
- очистка устаревших атрибутов пользователя производится периодической задачей каждые 24 часа.

Таблица 33. Данные для добавления атрибута домена аутентификации

Параметр	Описание
«Название»	Наименование добавляемого атрибута
«Атрибут»	Атрибут учетной записи пользователя из домена

ПОСТАВЩИКИ РЕСУРСОВ

Добавление поставщиков ресурсов

Общие сведения о поставщиках ресурсов

Поставщик ресурсов - это ОС, платформа виртуализации или терминальный сервер, предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения РМ.

Поддержка некоторых поставщиков ресурсов может добавляться в режиме экспериментальных функций. Доступность поставщиков ресурсов зависит от типа редакции Termidesk VDI.

В Termidesk VDI поддерживаются следующие поставщики ресурсов:

- ПК СВ Брест;
- платформа VMmanager;
- платформа zVirt;
- платформа oVirt;
- платформа РЕД Виртуализация;
- платформа OpenStack;
- платформа VMware vSphere;
- автономная машина;

- терминальный сервер (MS RDSH или STAL), подключаемый через функционал Метапоставщика;
- терминальные серверы MS RDSH и STAL.

Веб-интерфейс Termidesk VDI с установленной ролью «Портал администратора» обеспечивает следующие операции управления поставщиками ресурсов:

- добавление;
- редактирование;
- удаление;
- назначение тегов;
- техобслуживание;
- просмотр сведений;
- организация шаблона РМ.

Для добавления в Termidesk VDI поставщика ресурсов администратору Termidesk VDI следует перейти «Инфраструктура - Поставщики ресурсов», затем нажать на экранную кнопку **[Создать]** и выбрать из выпадающего списка нужный вариант.

Каждый поставщик ресурсов описывается перечнем параметров, требуемых Termidesk VDI для получения идентификаторов субъектов и информации о полномочиях. Проверить корректность указанных параметров можно при помощи экранной кнопки **[Тест]**, расположенной в том же окне. Для сохранения параметров конфигурации необходимо использовать экранную кнопку **[Сохранить]**.

Доступны следующие действия над поставщиками ресурсов:

- редактирование. Для этого нужно пометить поставщика ресурсов и нажать экранную кнопку **[Изменить]**;
- удаление. Для этого нужно пометить поставщика ресурсов и нажать экранную кнопку **[Удалить]**;
- назначение тегов поставщику ресурсов. Для этого нужно пометить поставщика ресурсов и нажать экранную кнопку **[Теги]**. Общее описание по применению тегов приведено в подразделе **Общие сведения о тегах**.

Поставщик ресурсов может быть удален только в том случае, если на нем не производится размещение фондов РМ.

Добавление поставщика ПК СВ БРЕСТ

Для добавления следует перейти «Инфраструктура - Поставщики ресурсов», нажать на экранную кнопку и выбрать из выпадающего списка «ПК СВ "Брест"».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления поставщика ресурсов ПК СВ Брест).

Таблица 34. Данные для добавления поставщика ресурсов ПК СВ Брест

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Версия ПК СВ Брест»	Выбор версии установленной платформы виртуализации

Параметр	Описание
«Адрес сервера»	IP-адрес или доменное имя фронтальной машины платформы виртуализации
«Домен»	Идентификатор области Kerberos для аутентификации. Если ПК СВ Брест используется в сервисном режиме, то параметр можно не заполнять
«Keytab»	Путь к файлу с ключами для сервисного аккаунта (пример формирования файла приведен в подразделе **Получение и добавление файла** `keytab`). Если ПК СВ Брест используется в сервисном режиме, то параметр можно не заполнять. Пример: • в случае стандартного хранения файла: «/etc/opt/termidesk-vdi/termidesk.keytab»; • в случае хранения файла в хранилище hvac: «hvac-kv://secret#termidesk-admin/keytabs/termidesk». Если используется хранилище, то сгенерированный на контроллере домена `keytab`-файл должен быть преобразован к формату BASE64
«Порт»	Номер порта для подключения к API платформы виртуализации. Значение по умолчанию: «2633», если на платформе не было указано иное
«Использовать SSL»	Управление использованием протокола SSL. Значение по умолчанию: «Нет»
«Проверка SSL»	Управление режимом строгой проверки SSL. Значение по умолчанию: «Да»
«Запуск ВМ от имени служебного пользователя»	Переключатель для запуска ВМ на платформе виртуализации от имени служебного пользователя. Если данный параметр активирован, то параметры «Делегация запуска ВМ», «Логин делегата», «Пароль делегата» настраивать не нужно. При активации параметра проверка аутентификации `kerberos` (`termidesk.keytab`) не производится, проверяется только доступность поставщика ресурсов и его версия. Значение по умолчанию: «Да»
«Логин»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Субъект, имеющий полномочия для управления платформой виртуализации
«Пароль»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Пароль субъекта с полномочиями для управления платформой виртуализации

Параметр	Описание
«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/brest/»
«Токен»	Электронный ключ субъекта с полномочиями для управления платформой виртуализации, который нужно скопировать из интерфейса управления платформой виртуализации. Для этого следует зайти в интерфейс управления платформой виртуализации с помощью логина и пароля указанного пользователя, в главном меню развернуть раздел «System» и выбрать строку «Users». В появившемся окне выбрать указанного пользователя, перейти на вкладку «Auth» и нажать экранную кнопку **[Manage login tokens]**, в появившейся форме скопировать значение из поля «Token»
«Делегация запуска ВМ»	Включение делегирования прав на запуск ВМ на платформе виртуализации другому пользователю. Значение по умолчанию: «Нет»
«Логин делегата»	Субъект, которому делегируется право на запуск ВМ на платформе виртуализации
«Пароль делегата»	Пароль субъекта, которому делегируется право на запуск ВМ на платформе виртуализации
«Подготавливать ВМ одновременно»	Максимальное число ВМ, создаваемых для всех фондов поставщика за одну проверку периодичностью «Интервал проверок кэша рабочих мест» (см. подраздел **Общие системные параметры Termidesk VDI**). Пример: для поставщика ресурсов созданы 4 фонда, в параметре «Подготавливать ВМ одновременно» задано «10», в параметре «Интервал проверок кэша рабочих мест» задано «19». Тогда за одну проверку (каждые 19 секунд) будет создано не более двух ВМ для каждого фонда (для расчета нужно выполнить целочисленное деление 10 ВМ на 4 фонда). Значение по умолчанию: «10»
«Удалять ВМ одновременно»	Максимальное число ВМ, удаляемых для всех фондов поставщика за одну проверку периодичностью 30 секунд. Значение по умолчанию: «5»
«Время ожидания соединения, с»	Максимальное время ожидания (в секундах) отклика от платформы виртуализации. Значение по умолчанию: «10»

Необходимо задать перечисленные параметры таким образом, чтобы использовался либо запуск ВМ от имени служебного пользователя (назначается параметр «Запуск ВМ от имени служебного пользователя»), либо запуск от имени пользователя-делегата (назначаются параметры «Делегация запуска ВМ», «Логин делегата», «Пароль делегата»). Использовать одновременно оба типа запуска запрещено.

Для управления платформой ПК СВ Брест субъект должен иметь привилегии, указанные в таблице (см. таблицу Перечень привилегий для роли в ПК СВ Брест).

Таблица 35. Перечень привилегий для роли в ПК СВ Брест

Путь к привилегии	Требуемые настройки

«Система - Группы»	Создать группу «termidesk», установив настройки:
	• на вкладке «Представление»:
	  отключить предоставление всех привилегий;
	• на вкладке «Права» предоставить привилегии:
	  ВМ;
	  образы;
	  шаблоны

«Система - Пользователи»	Создать пользователя «termidesk-tech» и добавить в группу «termidesk»
«Хранилища - Образы»	В разделе «Владелец» назначить: • «Владелец» - «termidesk-tech»; • «Группа» - «termidesk»
«Шаблоны - ВМ»	Отредактировать шаблон ВМ: • перейти: «Хранилище - Расширенные настройки - Образ»; • в строке «Имя пользователя владельца образа» указать нужного пользователя; • обновить шаблон ВМ

Добавление платформы oVirt

Для добавления следует перейти «Инфраструктура - Поставщики ресурсов», затем нажать на экранную кнопку **[Создать]** и выбрать из выпадающего списка «oVirt».

Платформа oVirt версии 4.0 и выше поддерживает интеграцию с Termidesk VDI без установки дополнительных пакетов.

Для корректной интеграции Termidesk VDI с платформой oVirt версии ниже 4.0 нужно:

- на хост oVirt Node установить дополнительный пакет `termidesk_zVirt_hook-<версия>-zvirt.noarch.rpm` (пакет предоставляется вендором платформы виртуализации):

```
rpm -i termidesk_zVirt_hook-<версия>-zvirt.noarch.rpm
```

- перезапустить сервис `ovirt-engine`:

```
service ovirt-engine restart
```

- на управляющей ВМ платформы oVirt убедиться, что каналы `ru.termidesk.PCSC.0`, `ru.termidesk.Printer.0`, `ru.termidesk.RealtimeStreaming.0`, `ru.termidesk.tvm.0` отображены в выводе команды:

```
ls /dev/virtio-ports
```

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления поставщика ресурсов oVirt).

Таблица 36. Данные для добавления поставщика ресурсов oVirt

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Версия oVirt»	Выбор используемой версии oVirt
«Адрес oVirt»	IP-адрес или доменное имя платформы виртуализации
«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/ovirt/»
«Логин»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Субъект, имеющий полномочия для управления платформой виртуализации. Указывается в формате: `login@internal`
«Пароль»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Подготавливать ВМ одновременно»	Максимальное число ВМ, создаваемых для всех фондов поставщика за одну проверку периодичностью 631 с. Пример: для поставщика ресурсов созданы 4 фонда, в параметре «Подготавливать ВМ одновременно» задано «10». Тогда за одну проверку будет создано не более двух ВМ для каждого фонда (для расчета нужно выполнить целочисленное деление 10 ВМ на 4 фонда). Значение по умолчанию: «10»
«Удалять ВМ одновременно»	Максимальное число ВМ, удаляемых для всех фондов поставщика за одну проверку периодичностью 30 секунд. Значение по умолчанию: «5»

Параметр	Описание
«Интервал опроса поставщика, мин»	Периодичность (в минутах) выполнения опроса платформы. После завершения предыдущего опроса следующий запустится через время, указанное в этом параметре. При превышении указанного интервала администратору будет отображено уведомление, если настроен системный параметр отправки уведомления (см. подраздел **Общие системные параметры Termidesk VDI**). Возможные значения: от 1 до 1140. Значение по умолчанию: «5»
«Нижний предел свободного места на хранилище (ГБ)»	Минимальный объем (в ГБ) хранилища, который должен быть доступен для последующего создания и размещения максимального числа ВРМ. Возможные значения: от 1 до 65000. Значение по умолчанию: «1000»
«Время ожидания соединения, с»	Максимальное время ожидания (в секундах) отклика от платформы виртуализации. Значение по умолчанию: «10»

Для платформы oVirt субъект должен иметь привилегии, указанные в таблице (см. таблицу Перечень привилегий для роли в oVirt).

В общем случае назначение ролей выглядит следующим образом: на сервере oVirt создается пользователь (например, «termidesk»), создается роль (в рамках oVirt употребляется термин «роль») («termidesk»). Пользователю «termidesk» выдается роль «termidesk».

Создать роль «termidesk» быстрее и проще через копирование существующей: «PowerUserRole» (необходимо перейти в графическом интерфейсе oVirt в «Administration - Configure - Roles, выбрать роль «PowerUserRole» и нажать **[Copy]**, изменить наименования на «termidesk»). Созданную роль затем изменить, добавив отсутствующие привилегии в соответствии с таблицей.

Роль «termidesk» с указанными привилегиями подходит только для управления ВМ, она не имеет прав доступа на администрирование oVirt.

Таблица 37. Перечень привилегий для роли в oVirt

Тип привилегий	Наименование привилегий
«System»: «Configure System»	«Login Permissions»
«Network»: «Configure vNIC Profile»	«Assign vNIC Profile to VM»
«Template»: «Provisioning Operations»	«Create» «Delete»

Тип привилегий	Наименование привилегий
«VM»: «Basic Operations»	«Reboot VM» «Reset VM» «Stop VM» «Shutdown VM» «Hibernate VM» «Run VM» «Change CD»
«VM»: «Provisioning Operations»	«Create» «Create Instance» «Delete»
«Disk»: «Provisioning Operations»	«Create» «Delete» «Attach» «Access Image Storage Domains»
«Disk»: «Disk Profile»	«Attach Disk Profile»

Добавление платформы zVirt

Для добавления платформы zVirt следует перейти «Инфраструктура - Поставщики ресурсов», затем нажать на экранную кнопку **[Создать]** и выбрать из выпадающего списка «zVirt».

Для корректной интеграции Termidesk VDI с платформой zVirt нужно:

- установить на всех хостах пакет `vdsm-hook-qemucmdline` (пакет предоставляется вендором платформы виртуализации):

```
sudo dnf install vdsm-hook-qemucmdline
```

- если пакет не найден, следует выполнить активацию:

```
sudo dnf config-manager --enable "zvirt*"
```

и повторить установку.

Затем на управляющей машине («HostedEngine»):

- выполнить:

```
sudo engine-config -s "UserDefinedVMProperties=qemu_cmdline=^.*$"
```

- на запрос выбора версии указать версию кластера zVirt;
- выполнить перезапуск службы:

```
sudo service ovirt-engine restart
```

Далее подготовить образ ВМ, затем для него выполнить:

- перейти в меню редактирования свойств образа, нажав экранную кнопку **[Edit]**. В разделе «Console» активировать пункты «USB Enabled» и «Smartcard Enabled»;
- перейти в раздел «Custom Properties». В правом меню нажать на выпадающий список «Please select a key...». Выбрать «qemu_cmdline» и в соседнем поле ввести (обязательно с сохранением квадратных скобок):
  - для zVirt 4.3:

```
["-device", "ich9-intel-hda,bus=pcie.0,addr=0x5",
 "-device", "hda-duplex",
 "-device", "nec-usb-xhci,id=xhci,bus=pcie.0,addr=0x7",
 "-device", "usb-host,hostbus=2,hostport=3,id=usb23",
 "-spice", "jpeg-wan-compression=always",
 "-device", "virtio-serial,bus=pcie.0,addr=0x8",
 "-chardev", "spiceport,id=WebDavPort,name=org.spice-
space.webdav.0",
 "-device",
"virtserialport,chardev=WebDavPort,name=org.spice-
space.webdav.0",
 "-chardev",
"socket,path=/tmp/termidesk/tvmd.sock,server=off,reconnect=1,
mux=on,id=ru_termidesk_tvm",
 "-device",
"virtserialport,chardev=ru_termidesk_tvm,name=ru.termidesk.tv
m.0",
 "-chardev",
"spiceport,id=RealtimeStreamingPort,name=TDSK_STREAM",
 "-device",
"virtserialport,chardev=RealtimeStreamingPort,name=ru.termide
sk.RealtimeStreaming.0",
 "-chardev", "spiceport,id=PrinterPort,name=TDSK_PRINTER",
 "-device",
"virtserialport,chardev=PrinterPort,name=ru.termidesk.Printer
.0",
 "-chardev", "spiceport,id=SmardCardPort,name=TDSK_PCSC",
 "-device",
"virtserialport,chardev=SmardCardPort,name=ru.termidesk.PCSC.
0"]
```

  - для zVirt ниже 4.3:

```
["-device", "ich9-intel-hda",
 "-device", "hda-duplex",
 "-device", "nec-usb-xhci,id=xhci",
 "-device", "usb-host,hostbus=2,hostport=3,id=usb23",
 "-spice", "jpeg-wan-compression=always",
 "-device", "virtio-serial",
 "-chardev", "spiceport,id=WebDavPort,name=org.spice-
space.webdav.0",
 "-chardev",
"socket,path=/tmp/termidesk/tvmd.sock,server=off,reconnect=1,
mux=on,id=ru_termidesk_tvm",
 "-device",
"virtserialport,chardev=ru_termidesk_tvm,name=ru.termidesk.tv
m.0",
 "-chardev",
"spiceport,id=RealtimeStreamingPort,name=TDSK_STREAM",
 "-device",
"virtserialport,chardev=RealtimeStreamingPort,name=ru.termide
sk.RealtimeStreaming.0",
 "-chardev", "spiceport,id=PrinterPort,name=TDSK_PRINTER",
 "-device",
"virtserialport,chardev=PrinterPort,name=ru.termidesk.Printer
.0",
 "-chardev", "spiceport,id=SmardCardPort,name=TDSK_PCSC",
 "-device",
"virtserialport,chardev=SmardCardPort,name=ru.termidesk.PCSC.
0"]
```

- нажать экранную кнопку **[Ok]** и сохранить изменения.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления платформы zVirt).

Таблица 38. Данные для добавления платформы zVirt

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Версия zVirt»	Выбор используемой версии zVirt
«Адрес zVirt»	IP-адрес или доменное имя платформы виртуализации
«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/zvirt/»

Параметр	Описание
«Логин»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Субъект, имеющий полномочия для управления платформой виртуализации. Указывается в формате: • для zVirt 4.3: `admin@zvirt@internalsso`; • для zVirtv ниже 4.3: `login@internal`
«Пароль»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Подготавливать ВМ одновременно»	Максимальное число ВМ, создаваемых для всех фондов поставщика за одну проверку периодичностью 631 с. Пример: для поставщика ресурсов созданы 4 фонда, в параметре «Подготавливать ВМ одновременно» задано «10». Тогда за одну проверку будет создано не более двух ВМ для каждого фонда (для расчета нужно выполнить целочисленное деление 10 ВМ на 4 фонда). Значение по умолчанию: «10»
«Удалять ВМ одновременно»	Максимальное число ВМ, удаляемых для всех фондов поставщика за одну проверку периодичностью 30 секунд. Значение по умолчанию: «5»
«Время ожидания соединения, с»	Максимальное время ожидания (в секундах) отклика от платформы виртуализации. В случае возникновения проблем с созданием ВМ нужно увеличить время ожидания отклика. Значение по умолчанию: «10»

Для платформы zVirt субъекту назначаются следующие роли:

В общем случае назначение ролей выглядит следующим образом: на сервере zVirt создается пользователь (например, «termidesk»), затем в графическом интерфейсе zVirt в «Управление - Пользователи» пользователь редактируется с указанием ролей в поле «Роли пользователя».

- «UserRole»;
- «PowerUserRole»;
- «UserVmManager»;
- «DiskOperator»;
- «DiskCreator»;
- «VmCreator»;
- «TemplateCreator»;
- «TemplateOwner»;
- «UserTemplateBasedVM»;
- «DiskProfileUser»;

- «UserProfileEditor»;
- «CpuProfileOperator»;
- «VnicProfileUser»;
- «MacPoolUser».

Добавление платформы «РЕД Виртуализация»

Для добавления платформы «РЕД Виртуализация» следует перейти «Инфраструктура - Поставщики ресурсов», затем нажать на экранную кнопку **[Создать]** и выбрать из выпадающего списка «РЕД Виртуализация».

Для корректной интеграции Termidesk VDI с платформой «РЕД Виртуализация» нужно установить на всех хостах пакет `vdsm-hook-qemucmdline` (пакет предоставляется вендором платформы виртуализации):

```
sudo dnf install vdsm-hook-qemucmdline
```

Затем на управляющей ВМ («HostedEngine»):

- выполнить:

```
sudo engine-config -s "UserDefinedVMProperties=qemu_cmdline=^.*$"
```

- на запрос выбора версии выбрать версию кластера «РЕД Виртуализация»;
- выполнить перезапуск службы:

```
sudo service ovirt-engine restart
```

Далее подготовить образ ВМ, затем для него выполнить:

- перейти в меню редактирования свойств образа, нажав экранную кнопку **[Edit]**. В разделе «Console» активировать пункты «USB Enabled» и «Smartcard Enabled»;
- перейти в раздел «Custom Properties». В правом меню нажать на выпадающий список «Please select a key...». Выбрать «qemu_cmdline» и в соседнем поле ввести (обязательно с сохранением квадратных скобок):

```
["-device", "ich9-intel-hda",
 "-device", "hda-duplex",
 "-device", "nec-usb-xhci,id=xhci",
 "-device", "usb-host,hostbus=2,hostport=3,id=usb23",
 "-spice", "jpeg-wan-compression=always",
 "-device", "virtio-serial",
 "-chardev", "spiceport,id=WebDavPort,name=org.spice-
space.webdav.0",
 "-chardev",
```

```
"socket,path=/tmp/termidesk/tvmd.sock,server=off,reconnect=1,mux=on,
id=ru_termidesk_tvm",
 "-device",
"virtserialport,chardev=ru_termidesk_tvm,name=ru.termidesk.tvm.0",
 "-chardev", "spiceport,id=RealtimeStreamingPort,name=TDSK_STREAM",
 "-device",
"virtserialport,chardev=RealtimeStreamingPort,name=ru.termidesk.Real
timeStreaming.0",
 "-chardev", "spiceport,id=PrinterPort,name=TDSK_PRINTER",
 "-device",
"virtserialport,chardev=PrinterPort,name=ru.termidesk.Printer.0",
 "-chardev", "spiceport,id=SmardCardPort,name=TDSK_PCSC",
 "-device",
"virtserialport,chardev=SmardCardPort,name=ru.termidesk.PCSC.0"]
```

- нажать экранную кнопку **[Ok]** и сохранить изменения.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления платформы «РЕД Виртуализация»).

Таблица 39. Данные для добавления платформы «РЕД Виртуализация»

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Версия REDVirt»	Выбор используемой версии платформы виртуализации
«Адрес REDVirt»	IP-адрес или доменное имя платформы виртуализации
«Логин»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Субъект, имеющий полномочия для управления платформой виртуализации. Указывается в формате: `login@internal`
«Пароль»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/red/»

Параметр	Описание
«Подготавливать ВМ одновременно»	Максимальное число ВМ, создаваемых для всех фондов поставщика за одну проверку периодичностью 631 с. Пример: для поставщика ресурсов созданы 4 фонда, в параметре «Подготавливать ВМ одновременно» задано «10». Тогда за одну проверку будет создано не более двух ВМ для каждого фонда (для расчета нужно выполнить целочисленное деление 10 ВМ на 4 фонда). Значение по умолчанию: «10»
«Удалять ВМ одновременно»	Максимальное число ВМ, удаляемых для всех фондов поставщика за одну проверку периодичностью 30 секунд. Значение по умолчанию: «5»
«Время ожидания соединения, с»	Максимальное время ожидания (в секундах) отклика от платформы виртуализации. Значение по умолчанию: «10»

Добавление поставщика VMmanager

Для добавления платформы VMmanager следует перейти «Инфраструктура - Поставщики ресурсов», затем нажать на экранную кнопку **[Создать]** и выбрать из выпадающего списка «VMmanager».

Начиная с Termidesk VDI версии 6.1 улучшено однозначное сопоставление ВМ, отображаемых в портале VMmanager, и фонда РМ. Для ВМ, создаваемых поставщиком VMmanager, при публикации фонда РМ будет добавлено поле «Примечание». При этом:

- в поле «Примечание» записывается название публикуемого фонда;
- если поле «Примечание» было непустым, то оно будет перезаписано без предупреждения.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей на таблицы (см. таблицу Данные для добавления поставщика ресурсов VMmanager).

Таблица 40. Данные для добавления поставщика ресурсов VMmanager

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Хост»	IP-адрес или полное доменное имя сервера VMmanager
«Порт»	Номер порта для подключения к VMmanager. Значение по умолчанию: «443», если на платформе не настроен другой
«Логин (эл. почта)»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Субъект, имеющий полномочия для управления платформой виртуализации VMmanager

Параметр	Описание
«Пароль»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий субъекта
«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/vmm/»
«Использовать SSL»	Включение использования протокола SSL. Значение по умолчанию: «Нет»
«Проверять SSL»	Включение строгой проверки SSL. Значение по умолчанию: «Нет»
«Подготавливать ВМ одновременно»	Максимальное число ВМ, создаваемых для всех фондов поставщика за одну проверку периодичностью 631 с. Пример: для поставщика ресурсов созданы 4 фонда, в параметре «Подготавливать ВМ одновременно» задано «10». Тогда за одну проверку будет создано не более двух ВМ для каждого фонда (для расчета нужно выполнить целочисленное деление 10 ВМ на 4 фонда). Значение по умолчанию: «10»
«Удалять ВМ одновременно»	Максимальное число ВМ, удаляемых для всех фондов поставщика за одну проверку периодичностью 30 секунд. Значение по умолчанию: «5»
«Интервал опроса поставщика, мин»	Периодичность (в минутах) выполнения опроса платформы. После завершения предыдущего опроса следующий запустится через время, указанное в этом параметре. При превышении указанного интервала администратору будет отображено уведомление, если настроен системный параметр отправки уведомления (см. подраздел **Общие системные параметры Termidesk VDI**). Возможные значения: от 1 до 1140. Значение по умолчанию: «5»
«Нижний предел свободного места на хранилище (ГБ)»	Минимальный объем (в Гб) хранилища, который должен быть доступен для последующего создания и размещения максимального числа ВРМ. Возможные значения: от 1 до 65000. Значение по умолчанию: «1000»
«Время ожидания соединения, с»	Максимальное время ожидания (в секундах) отклика от платформы виртуализации. Значение по умолчанию: «10»

Субъект должен иметь привилегии, указанные в таблице (см. таблицу Перечень привилегий для роли в VMmanager).

В общем случае назначение ролей выглядит следующим образом: на сервере VMmanager создается пользователь (например, «termidesk»), создается роль с типом «Продвинутый пользователь» (в рамках VMmanager употребляется термин «роль») («Termidesk»). Пользователю «termidesk» выдается роль «Termidesk».

Таблица 41. Перечень привилегий для роли в VMmanager

Тип привилегий	Наименование привилегий
Секция «Кластеры»	
«Для узлов»	«Запуск скриптов на узле»
Секция «Виртуальные машины»	
«Базовые операции»	«Переименование VM» «Изменение пароля» «Запуск и остановка VM» «Переустановка ОС» «Режим восстановления» «Подключение ISO» «Запуск скрипта» «Создание снимка» «Создание образа VM» «Открыть VNC» «Открыть SPICE»
«Продвинутые операции»	«Клонирование» «Создание дисков» «Редактирование дисков» «Отключение дисков» «Управление сетями» «Управление снимками» «Управление образами» «Работа с IP-адресами» «Тонкие настройки» «Примечание»

Тип привилегий	Наименование привилегий
«Административные операции»	«Создание VM» «Удаление VM» «Миграция» «Настройки защиты VM» «Балансировщик» «Настройка VNC / SPICE»
Секция «Общие права на управление разделами»	
«Разделы»	«Дашборд» «Скрипты» «Шаблоны» «IP-адреса» «Виртуальные сети» «Пользователи и группы» «Роли» «DNSBL» «Уведомления» «Список задач» «Настройки платформы» «Настройка внешних хранилищ» «Резервные копии VM»

Добавление платформы VMware vSphere

Для добавления следует перейти «Инфраструктура - Поставщики ресурсов», затем нажать на экранную кнопку **[Создать]** и выбрать из выпадающего списка «VMware vSphere».

При взаимодействии Termidesk VDI с платформой VMware необходимо наличие ВМ управления (vCenter). Начиная с версии Termidesk VDI 4.1 поддерживается работа как с кластерами данных в качестве системы хранения, так и с обычными хранилищами (Datastore).

Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления поставщика ресурсов VMware vSphere).

Таблица 42. Данные для добавления поставщика ресурсов VMware vSphere

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов

Параметр	Описание
«Версия платформы»	Выбор используемой версии платформы виртуализации. Значение по умолчанию: «6.7 - 9.0.0»
«Адрес сервера»	IP-адрес или доменное имя ВМ управления платформой виртуализации VMware (vCenter)
«Порт»	Номер порта для подключения к API платформы. Значение по умолчанию: «443»
«Использовать SSL»	Форсировать использование протокола SSL. Значение по умолчанию: «Да»
«Домен пользователя»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Доменное имя сервера службы каталогов, в который входит субъект, имеющий полномочия для управления платформой виртуализации VMware. Если параметр задан, то к имени пользователя будет добавлена доменная часть, если ее нет
«Логин»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Субъект, имеющий полномочия для управления платформой виртуализации VMware
«Пароль»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий субъекта
«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/vmware/»

Параметр	Описание
«Выбрать ресурсы платформы»	Активировать использование ресурсов платформы для размещения ВМ. После активации в параметрах «Кластер ресурсов», «Кластеры данных», «Сети» станет доступен выбор ресурсов, полученных от платформы виртуализации. Значение по умолчанию: «Нет» Перед активацией параметра нужно заполнить поля «Название», «Адрес сервера», «Порт» (при необходимости), «Логин», «Пароль» и нажать экранную кнопку **[Тест]**. Необходимо обязательно задать этот параметр!
«Кластер ресурсов»	Идентификатор ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд ВРМ. Доступные значения получены от платформы виртуализации Необходимо обязательно задать этот параметр!
«Кластеры данных»	Идентификатор кластера ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд ВРМ. Доступные значения получены от платформы виртуализации Необходимо обязательно задать этот параметр!
«Сети»	Выбор одной или нескольких сетей, созданных на платформе виртуализации VMware, адреса из которых могут быть назначены ВМ из фонда ВРМ Необходимо обязательно задать этот параметр!
«Подготавливать ВМ одновременно»	Максимальное число ВМ, создаваемых для всех фондов поставщика за одну проверку периодичностью 631 с. Пример: для поставщика ресурсов созданы 4 фонда, в параметре «Подготавливать ВМ одновременно» задано «10». Тогда за одну проверку будет создано не более двух ВМ для каждого фонда (для расчета нужно выполнить целочисленное деление 10 ВМ на 4 фонда). Значение по умолчанию: «10»
«Удалять ВМ одновременно»	Максимальное число ВМ, удаляемых для всех фондов поставщика за одну проверку периодичностью 30 секунд. Значение по умолчанию: «5»

Параметр	Описание
«Интервал опроса поставщика, мин»	Периодичность (в минутах) выполнения опроса платформы. После завершения предыдущего опроса следующий запустится через время, указанное в этом параметре. При превышении указанного интервала администратору будет отображено уведомление, если настроен системный параметр отправки уведомления (см. подраздел **Общие системные параметры Termidesk VDI**). Возможные значения: от 1 до 1140. Значение по умолчанию: «5»
«Нижний предел свободного места на хранилище (ГБ)»	Минимальный объем (в ГБ) хранилища, который должен быть доступен для последующего создания и размещения максимального числа ВРМ. Возможные значения: от 1 до 65000. Значение по умолчанию: «1000»
«Уведомлять об изменении MAC-адреса»	Управление синхронизацией MAC-адресов. Параметр необходим для корректного получения MAC-адреса РМ в случае, когда полученный от «Агента виртуального рабочего места» MAC-адрес не совпадает с первым адресом из списка, полученного от платформы. При активации параметра MAC-адрес РМ, сохраненный в БД, будет сравниваться со всем списком MAC-адресов, полученных от платформы. При этом из опроса MAC-адресов исключаются РМ, в шаблонах которых включена опция «Статический MAC-адрес». По умолчанию параметр активирован

Субъект должен иметь привилегии, указанные в таблице (см. таблицу Перечень привилегий для роли в VMware vCenter).

В общем случае назначение ролей выглядит следующим образом: на сервере vCenter создается пользователь (например, «termidesk»), создается группа («Termidesk Group») и класс (в рамках vCenter употребляется термин «роль») («Termidesk»). Созданной группе «Termidesk Group» выдается роль «Termidesk». Роль «Termidesk» состоит из сочетания встроенной группы «Virtual machine power user (sample)» и «VMware virtualization environments(Citrix)».

Таблица 43. Перечень привилегий для роли в VMware vCenter

Тип привилегий	Наименование привилегий
«Datastore»	«Allocate space» «Browse datastore» «Low level file operations»
«Global»	«Cancel task»
«Network»	«Assign network»
«Resource»	«Assign virtual machine to resource pool»

Тип привилегий	Наименование привилегий
«Scheduled task»	«Create tasks» «Modify task» «Remove task» «Run task»
«Virtual machine»: «Change Configuration»	«Acquire disk lease» «Add existing disk» «Add new disk» «Add or remove device» «Advanced configuration» «Change CPU count» «Change Memory» «Change Settings» «Change resource» «Modify device settings» «Remove disk» «Rename» «Reset guest information» «Upgrade virtual machine compatibility»
«Virtual machine»: «Edit Inventory»	«Create from existing» «Create new» «Remove»
«Virtual machine»: «Interaction»	«Answer question» «Configure CD media» «Configure floppy media» «Connect devices» «Console interaction» «Pause or Unpause» «Power off» «Power on» «Reset» «Suspend»

Тип привилегий	Наименование привилегий
«Virtual machine»: «Provisioning»	«Clone virtual machine» «Create template from virtual machine» «Deploy template» «Mark as template» «Mark as virtual machine»
«Virtual machine»: «Snapshot management»	«Create snapshot» «Remove snapshot» «Rename snapshot» «Revert to snapshot»

Добавление поставщика OpenStack

Для возможности добавления поставщика ресурсов OpenStack необходимо включить экспериментальный параметр `experimental.openstack.provider.enabled` в соответствии с подразделом **Управление экспериментальными параметрами Termidesk VDI**.

Затем перейти в «Инфраструктура - Поставщики ресурсов» и нажать на экранную кнопку **[Создать]**, выбрать из выпадающего списка «OpenStack». Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления поставщика ресурсов OpenStack).

Таблица 44. Данные для добавления поставщика ресурсов OpenStack

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Имя хоста»	IP-адрес или FQDN сервиса аутентификации
«Порт»	Порт для подключения к OpenStack. Значение по умолчанию: «5000»
«Путь»	Опциональная составляющая URI
«Использовать SSL»	Управление использованием протокола SSL. Значение по умолчанию: «Нет»
«Проверять SSL»	Управление режимом строгой проверки SSL. Значение по умолчанию: «Нет»
«Интерфейс доступа»	Идентификатор интерфейса доступа OpenStack. Значение по умолчанию: «public»
«Домен»	Идентификатор домена OpenStack
«Пользователь»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Субъект, имеющий полномочия для управления в OpenStack

Параметр	Описание
«Пароль»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/openstack/»
«Количество одновременно создаваемых ВМ»	Максимальное число ВМ, создаваемых для всех фондов поставщика за одну проверку периодичностью 631 с. Пример: для поставщика ресурсов созданы 4 фонда, в параметре «Подготавливать ВМ одновременно» задано «10». Тогда за одну проверку будет создано не более двух ВМ для каждого фонда (для расчета нужно выполнить целочисленное деление 10 ВМ на 4 фонда). Значение по умолчанию: «10»
«Количество одновременно удаляемых ВМ»	Максимальное число ВМ, удаляемых для всех фондов поставщика за одну проверку периодичностью 30 секунд. Значение по умолчанию: «5»
«Время ожидания соединения, с»	Максимальное время ожидания (в секундах) отклика от OpenStack. Значение по умолчанию: «15»

Для взаимодействия с OpenStack требуются привилегии «member» для доступа к API, перечисленным в таблице (см. таблицу Перечень API-запросов для привилегии «member»).

Привилегий «member» недостаточно для API-запроса `GET /os-console-auth-tokens/{console_token}` (получение узла и порта по токену для удаленной консоли) сервиса Nova (Compute Service).

Таблица 45. Перечень API-запросов для привилегии «member»

Сервис OpenStack	API-запрос	Описание API-запроса
Keystone (Identity Service)	`POST auth/tokens`	Получение токена аутентификации
	`GET users/{user_id}/projects`	Получение списка проектов пользователя
	`GET regions/`	Получение списка регионов
Glance (Image Service)	`GET /images?status=active`	Получение списка активных образов
	`GET /images/{image_id}`	Получение информации об образе

Сервис OpenStack	API-запрос	Описание API-запроса
Nova (Compute Service)	`GET /servers`	Получение списка серверов
	`GET /servers/detail`	Получение списка серверов с детальной информацией
	`GET /servers/{server_id}`	Получение информации о сервере
	`POST /servers`	Создание экземпляра ВМ из снимка диска
	`POST /servers/{server_id}/action`	Удаление экземпляра ВМ (forceDelete) Запуск экземпляра ВМ (os-start) Останов экземпляра ВМ (os-stop) Приостановка экземпляра ВМ (suspend) Возобновление экземпляра ВМ (resume) Перезагрузка экземпляра ВМ (reboot)
	`POST /servers/{server_id}/remote-consoles`	Получение консоли (SPICE/VNC)
	`GET /os-availability-zone`	Получение списка зон доступности
	`GET /flavors`	Получение списка конфигураций ВМ (flavors)
	`GET /os-security-groups`	Получение списка групп безопасности
Cinder (Block Storage Service)	`GET /volumes/detail`	Получение сведений о диске с детальной информацией
	`GET /volumes/{volume_id}`	Получение сведений о диске
	`POST /volumes`	Создание диска из снимка
	`DELETE /volumes/{volume_id}`	Удаление диска
	`GET /snapshots`	Получение списка снимков
	`POST /snapshots`	Создание снимка диска
	`GET /snapshots/{snapshot_id}`	Получение информации о снимке
	`PUT /snapshots/{snapshot_id}`	Обновление информации о снимке
	`DELETE /snapshots/{snapshot_id}`	Удаление снимка
	`GET /types`	Получение списка типов диска
Neutron (Networking Service)	`GET /networks`	Получение списка сетей
	`GET /ports`	Получение списка портов

Добавление автономной машины как поставщика ресурсов

Общие сведения об автономной машине

Автономная машина - это машина (физическая или виртуальная), которая является постоянной (статической) и не пересоздается для пользователей. То есть пользователи всегда подключаются к одной и той же машине.

Для подключения к автономной машине могут использоваться протоколы:

- RDP;
- TERA;
- Loudplay.

Для работы подключения в ВРМ должны быть установлены соответствующие пакеты поддержки на этапе подготовки гостевой ОС. В ОС автономной машины должен быть установлен:

- компонент «Агент виртуального рабочего места» для регистрации РМ в Termidesk;
- компонент «Сессионный агент», если автономная машина будет терминальным сервером.

Перечень параметров для добавления автономной машины

Для добавления поставщика ресурсов следует перейти в «Инфраструктура - Поставщики ресурсов», затем нажать на экранную кнопку **[Создать]** и выбрать из выпадающего списка «Автономные машины».

Поставщик ресурсов «Автономные машины» может использоваться для объединения нескольких терминальных серверов для предоставления дополнительных возможностей по работе с ними (см. подраздел **Добавление терминального сервера (MS RDS и STAL) в качестве поставщика ресурсов**).

Поставщик ресурсов «Автономные машины» доступен в лицензии с типом «Стандартный» или «Расширенный».

Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления автономных машин в качестве поставщика ресурсов).

Таблица 46. Данные для добавления автономных машин в качестве поставщика ресурсов

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов

Добавление терминального сервера (MS RDS и STAL) в качестве поставщика ресурсов

Для добавления следует перейти «Инфраструктура - Поставщики ресурсов», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «Сервер терминалов».

Для взаимодействия с терминальным сервером (MS RDS или STAL) необходимо установить:

- компонент «Сессионный агент»;
- (опционально, если дополнительно используется поставщик «Автономные машины») компонент «Агент виртуального рабочего места».

Терминальный сервер для ОС Astra Linux Special Edition реализуется компонентом «Сервер терминалов Astra Linux» (STAL) Termidesk VDI, который может быть установлен на узел совместно с Termidesk VDI.

Следует использовать отдельные установки терминальных серверов:

- на одном сервере MS RDS или STAL – публикация только приложений;
- на другом MS RDS или STAL – только терминальных сессий.

Поддерживается расширенный сценарий добавления терминальных серверов: помимо использования поставщика ресурсов «Сервер терминалов» добавить поставщик «Автономные машины», который будет объединять несколько узлов и выполнять роль служебного (не виден пользователю, но предоставляет ему ресурсы). Таким образом может быть несколько «Серверов терминалов», и одна «Автономная машина», в шаблоне которой будут заданы терминальные серверы, что предоставляет дополнительные возможности:

- поддержка нескольких сессий пользователя в рамках одного сервера. Каждой сессии пользователя назначается свой идентификатор, который передается в заголовке `X-TDSK-SID`;
- поддержка отправки сообщений в сессию пользователя терминального сервера. Сессия пользователя определяется по ее идентификатору, переданному в заголовке `X-TDSK-SID`;
- поддержка сбора метрик узла терминального сервера.

Работа с MS RDS поддерживается как в варианте подключения через «Шлюз» Termidesk VDI, так и без него, если:

- либо терминальный сервер MS RDS развернут без полнофункциональной инфраструктуры через поставщик ресурсов «Метапоставщик»;
- либо развернута полнофункциональная инфраструктура MS RDS, при этом роль «Remote Desktop Gateway» развернута, но не используется. Каждая нода MS RDS должна быть подключена как отдельный поставщик ресурсов «Сервер терминалов» (то есть, коллекция MS RDS находится на том сервере, к которому идет подключение).

Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления сервера терминалов).

Таблица 47. Данные для добавления сервера терминалов

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов

Параметр	Описание
«Адрес сессионного агента»	FQDN узла, на котором установлен «Сессионный агент» Termidesk VDI. Для инфраструктуры MS RDS в этом параметре обязательно нужно указывать не IP-адрес, а FQDN узла. Для STAL: • если если используется Kerberos-аутентификация, то обязательно нужно указывать не IP-адрес, а FQDN узла; • если Kerberos-аутентификация не используется, то можно указать внешний IP-адрес узла. Если STAL установлен на одном узле с Termidesk VDI, нужно также указывать внешний IP-адрес узла. Перед изменением FQDN или IP-адреса STAL необходимо завершить все активные сессии. После смены FQDN или IP-адреса STAL активные сессии, связанные с предыдущим FQDN или IP-адресом, становятся недоступными. Для восстановления доступа к STAL необходимо удалить предыдущие сессии и выполнить новое подключение
«Порт сессионного агента»	Номер порта «Сессионного агента» Termidesk VDI. Значение по умолчанию: «31000»
«Домен»	Наименование домена для подключения к терминальному серверу
«Логин»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Субъект, имеющий полномочия для подключения к терминальному серверу: достаточно только прав для прохождения аутентификации. Отдельные права на чтение приложений не требуются. Для подключения STAL в домене MS AD необходимо указывать логин локального администратора ОС узла, на котором установлен STAL. В ином случае тест соединения для поставщика может пройти успешно, но шаблон РМ при этом добавить не получится
«Пароль»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/terminal/»
«Таймаут сессионного агента, с»	Время ожидания (в секундах) отклика от «Сессионного агента». Указанное значение также определяет время ожидания обработки запросов при подключении пользователя к STAL и отправляется на компонент «Клиент». Значение по умолчанию: «10»

Параметр	Описание
«Использовать HTTPS»	Выбор использования протокола HTTPS для запросов к «Сессионному агенту». При включении параметра на сервере терминалов должны быть добавлены валидные сертификаты и установлена опция `USE_HTTPS` в значение `True` в конфигурационном файле «Сессионного агента». В случае необходимости использовать протокол HTTP нужно отключить данный параметр и установить опцию `USE_HTTPS` в значение `False` в конфигурационном файле «Сессионного агента». Если используется протокол HTTP, то необходимо настроить «Универсальный диспетчер» на использование протокола HTTP, скорректировав файл `/etc/apache2/sites-available/termidesk.conf` (см. подраздел **Перенаправление на HTTPS**) Значение по умолчанию: «Нет»
«Валидация сертификата»	Выбор проверки подлинности сертификата при запросах к «Сессионному агенту». Значение по умолчанию: «Нет»

В инфраструктуре должна быть сетевая связанность между компонентами «Универсальный диспетчер» и «Сессионный агент» по IP-адресу. Если на узле «Универсального диспетчера» используется VPN с туннелированием, функционал оповещения и регистрации, приведенный ниже, между этими компонентами работать не будет.

После добавления сервера терминалов в Termidesk VDI будет зарегистрирован MAC-адрес узла, на котором установлен «Сессионный агент». В то же время непосредственно «Сессионный агент» сохранит IP-адрес «Универсального диспетчера», который отправил ему запрос. Поскольку MAC-адрес нужен для регистрации событий, то в случае его изменения «Универсальный диспетчер» перестанет принимать события от этого «Сессионного агента», однако подключение при этом будет работать.

Для исправления ситуации, когда MAC-адрес был изменен и от «Сессионного агента» перестали регистрироваться события, нужно:

- либо открыть поставщик ресурсов и нажать экранные кнопки **[Тест]** и **[Сохранить]** для перерегистрации «Сессионного агента»;
- либо создать новый поставщик ресурсов с указанием нужного «Сессионного агента»;
- либо выполнить на узле с «Универсальным диспетчером» команды:

```
sudo -u termidesk bash
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_refresh_ssa
```

Указанные команды выполняются также для регистрации «Сессионного агента» в случае, если компонент «Универсальный диспетчер» был обновлен раньше него.

Если после попытки проверить введенные данные экранной кнопкой **[Тест]** появляются сообщения об ошибке, то при создании шаблона РМ будет блокироваться возможность его сохранения (создания).

Для корректного подключения через компонент «Клиент» к серверу терминалов необходимо задать параметр «Аутентификация на уровне сети

(RDP)» в политиках конкретного фонда ВРМ («Рабочие места - Фонды») в соответствии с выбранным сервером:

- «TLS» или «RDP» - для подключения к STAL (если не используется Kerberos-аутентификация);
- «NLA» - для подключения к MS RDS.

Добавление поставщика «Метапоставщик»

Предварительная настройка для добавления терминального сервера Метапоставщика

Алгоритм подготовки для добавления терминального сервера Метапоставщика состоит в следующем:

- на платформе виртуализации создается ВМ терминального сервера («золотой образ»):
  - или с гостевой ОС Microsoft Windows Server;
  - или с гостевой ОС Astra Linux Special Edition (Server);
- в гостевой ОС ВМ устанавливается и настраивается компонент «Агент виртуального рабочего места» и компонент «Сессионный агент»;
- для ОС Microsoft Windows Server:
  - устанавливается роль сервера публикации приложений «Remote Desktop Session Host» из состава «Remote Desktop Services» (MS RDS);
  - выполняется активация роли через «Сессионный агент»;
  - если ОС Microsoft Windows Server не вводится в домен, то в ОС создается пользователь с правами доступа к удаленному рабочему столу;
- для ОС Astra Linux Special Edition:
  - устанавливается STAL;
- необходимые приложения публикуются вручную:
  - для MS RDS используется «Сессионный агент»: в веб-браузере перейти по адресу: `https://<IP-адрес_узла_агента>:31000/docs`. В разделе «Auth» раскрыть POST-запрос `/auth` и нажать экранную кнопку **[Try it out]**. В поле «Request body» заполнить логин, домен (при необходимости) и пароль для авторизации. После успешной авторизации перейти в раздел «Meta» и раскрыть POST-запрос `/meta/applications`, нажать экранную кнопку **[Try it out]**. В поле «Request body» перечислить список приложений (имя и путь к исполняемому файлу);
  - для ОС Astra Linux Special Edition (STAL) основной список приложений, ОС, уже доступен к публикации. При необходимости опубликовать нестандартное приложение следует обратиться к документации STAL;
- на этом этапе подготовка завершена, ВМ выключается.

Не допускается вмешательство (переустановка «Сессионного агента», удаление БД «Сессионного агента» и др.) в уже функционирующую ноду терминального сервера.

Обновление или переустановка «Сессионного агента» выполняется только на ВМ терминального сервера, которая является «золотым образом» для нод терминального сервера Метапоставщика.

В гостевой ОС должен быть настроен встроенный межсетевой экран для доступа по портам протокола RDP.

Далее нужно добавить соответствующие объекты в в веб-интерфейсе Termidesk VDI:

- создать поставщика ресурсов с той платформой виртуализации, на которой создана подготовленная ВМ терминального сервера;
- в поставщике ресурсов создать нужный шаблон РМ для выбранной платформы виртуализации. В параметре «Базовая ВМ» выбранного шаблона указать подготовленную ВМ терминального сервера;
- создать сервисный фонд РМ для шаблона РМ через мастер публикации «Виртуальные машины». В сервисном фонде не указываются группы пользователей, пользователи, протоколы доставки (их можно удалить после создания фонда). Сервисный фонд должен использовать кеш 1-го уровня (кеш 2-го уровня не используется);

Для сервисного фонда РМ обязательно нужно проверить используемое значение политики «Действие при выходе пользователя из ОС».

Хотя бы одно РМ должно получить статус «Действительный» во вкладке «Рабочие места» созданного фонда, иначе все дальнейшие действия будут завершаться ошибкой «Не удалось найти подходящую для подключения машину».

При понижении количества ВМ в кеше 1-го уровня сервисного фонда те ВМ, на которых есть активные сессии Метапоставщика, не будут удалены.

- добавить поставщик «Метапоставщик»;
- создать шаблон РМ для поставщика «Метапоставщик», выбрав тип в зависимости от того, что нужно опубликовать - терминальную сессию или приложение;
- добавить фонд РМ для Метапоставщика через мастер публикации «Публикация служб Метапоставщика».

Перечень параметров для добавления терминального сервера Метапоставщика

Для добавления поставщика ресурсов следует перейти «Инфраструктура - Поставщики ресурсов», затем нажать на экранную кнопку **[Создать]** и выбрать из выпадающего списка «Метапоставщик».

Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления терминального сервера (Метапоставщика)).

Сразу после создания поставщика ресурсов «Метапоставщик» будет создан шаблон рабочего места с наименованием «Meta Terminal Service».

Таблица 48. Данные для добавления терминального сервера (Метапоставщика)

Параметр	Описание
«Название»	Текстовое наименование поставщика ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения поставщика ресурсов
«Порт сессионного агента»	Номер порта «Сессионного агента» Termidesk VDI. Значение по умолчанию: «31000»
«Домен»	Наименование домена для подключения к серверу терминалов
«Логин»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Субъект, имеющий полномочия для управления сервером терминалов

Параметр	Описание
«Пароль»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/meta/»
«Фонд»	Выбор **сервисного фонда** для размещения. В качестве сервисного фонда может быть выбран фонд автономных машин. В списке отображаются только те сервисные фонды, которые не используются другим Метапоставщиком
«Таймаут сессионного агента, с»	Время ожидания (в секундах) отклика от «Сессионного агента». Указанное значение также определяет время ожидания обработки запросов при подключении пользователя к STAL и отправляется на компонент «Клиент». Значение по умолчанию: «10»
«Использовать HTTPS»	Выбор использования протокола HTTPS для запросов к «Сессионному агенту». При включении параметра на сервере терминалов должны быть добавлены валидные сертификаты и установлена опция `USE_HTTPS` в значение «True» в конфигурационном файле «Сессионного агента». В случае необходимости использования протокола HTTP нужно отключить данный параметр и установить опцию `USE_HTTPS` в значение «False» в конфигурационном файле «Сессионного агента». Если используется протокол HTTP, то необходимо настроить «Универсальный диспетчер» на использование протокола HTTP, скорректировав файл `/etc/apache2/sites-available/termidesk.conf` (см. подраздел **Перенаправление на HTTPS**). По умолчанию параметр выключен
«Проверка сертификата»	Выбор проверки подлинности сертификата при запросах к «Сессионному агенту». По умолчанию параметр выключен

Параметр	Описание
«Соиспользование сессий»	Выбор метода балансировки, основанного на совместном использовании сессии приложениями. Если параметр выключен, то подключение пользователя будет происходить на любую ноду (первую во внутреннем списке). При включении параметра будет производиться поиск и учет активной сессии пользователя. Если такая сессия найдена, приложение будет запущено на той же ноде. STAL не поддерживает функционал запуска нескольких разных приложений в одной сессии. Поддерживается только работа с несколькими профилями пользователя одновременно в рамках одного приложения (например, запуск второй вкладки веб-браузера в той же сессии, реализуемый через настройку «Сессионного агента» `APPS_SHARING_SESSIONS`). По умолчанию параметр включен

Параметр	Описание
«Балансировка по метрикам»	Выбор метода балансировки, основанного на полученных метриках, регулярно присылаемых от «Сессионного агента», установленного на Метапоставщике (MS RDS или STAL). Описание механизма балансировки приведено в подразделе **Балансировка подключений на основе загрузки терминальных серверов Метапоставщика**. Возможные значения: • «Да» - для балансировки будет рассчитываться нагрузка ноды Метапоставщика. Пользователю будет выдана для подключения та нода, которая имеет в момент запроса наименьшее значение нагрузки; • «Нет» - метод балансировки по метрикам использоваться не будет. В этом случае параметр «Предпочитать соиспользование сессий вместо балансировки» не проверяется Поведение при балансировке также зависит от значений других параметров: • если активированы «Балансировка по метрикам», «Соиспользование сессий», «Предпочитать соиспользование сессий вместо балансировки», то новая сессия пользователя будет направлена на ту же ноду Метапоставщика, на которой у пользователя есть хотя бы одна сессия. Значение нагрузки ноды будет проигнорировано; • если активированы только «Балансировка по метрикам» и «Соиспользование сессий», то будет проверено значение нагрузки ноды. Если нагрузка равна 10000, то новая сессия будет направлена на наименее загруженную ноду. Значение нагрузки ноды рассчитывается на основании значения индекса нагрузки, вычисляемого из имеющихся показателей метрик. В случае, если несколько нод имеют одинаковое наименьшее значение нагрузки, то подключение может быть выполнено на любую ноду. Механизм оповещения и связанный с ним механизм балансировки по метрикам передает IP-адрес «Универсального диспетчера» на «Сессионный агент», поэтому в инфраструктуре должна быть сетевая связанность между этими компонентами по IP-адресу. Если на узле «Универсального диспетчера» используется VPN с туннелированием, функционал балансировки по метрикам работать не будет. Оценка нагрузки при выборе этого метода балансировки происходит на основании параметров (метрик балансировки), заданных ниже. Периодичность отправки метрик определяется настройками, заданными на странице «Системные параметры - Системные настройки - Метрики» (см. подраздел **Настройка отправки метрик для «Сессионного агента»**)

Параметр	Описание
«Применить "Утилизпация ЦП"»	Использование возможно при активации параметра «Балансировка по метрикам». Управление использованием метрики при расчете нагрузки. Значение по умолчанию: «Да» (метрика используется)
«Утилизация ЦП»	Использование возможно при активации параметра «Балансировка по метрикам». Для формирования кеша метрик, на основании которых будет происходить балансировка, нужно активировать настройку «Применить "Использование ЦП"». Параметр задает предел загруженности процессора ноды Метапоставщика в процентах. Изменение применяется на компоненте «Сессионный агент» сразу. Диапазон значений: от 1 до 100. Значение по умолчанию: «100»
«Применить "Использование ОЗУ"»	Использование возможно при активации параметра «Балансировка по метрикам». Управление использованием метрики при расчете нагрузки. Значение по умолчанию: «Да» (метрика используется)
«Использование ОЗУ»	Использование возможно при активации параметра «Балансировка по метрикам». Для формирования кеша метрик, на основании которых будет происходить балансировка, нужно активировать настройку «Применить "Использование ОЗУ"». Параметр задает предел загруженности оперативной памяти ноды терминального сервера в процентах. Изменение применяется на компоненте «Сессионный агент» сразу. Диапазон значений: от 1 до 100. Значение по умолчанию: «100»

Параметр	Описание
«Применить "Сессий всего"»	Использование возможно при активации параметра «Балансировка по метрикам». Управление использованием параметром «Сессий всего» при расчете нагрузки. Если параметр выключен, то: • предел числа подключений пользователей будет определяться параметром `MAX_SESSIONS` конфигурационного файла компонента «Сессионный агент». Компонент «Сессионный агент» отправляет значение параметра вместе с метриками узла; • если число подключений пользователей достигло предела, заданного в параметре `MAX_SESSIONS`, то терминальный сервер считается полностью нагруженным и не может принимать новые подключения. Значение по умолчанию: «Да» (параметр используется)
«Сессий всего»	Использование возможно при активации параметра «Балансировка по метрикам». Параметр задает предел числа подключений пользователей к ноде Метапоставщика. При достижении заданного лимита новые подключения будут происходить к другой доступной ноде. Текущие пользователи, уже имеющие открытую сессию на ноде, будут подключены к ней же, если в настройках Метапоставщика активирован параметр «Соиспользование сессий». Изменение применяется на компоненте «Сессионный агент» сразу. Диапазон значений: от 1 до 181. Значение по умолчанию: «181»

Параметр	Описание
«Влияние входов в систему на нагрузку»	Использование возможно при активации параметра «Балансировка по метрикам». Параметр определяет, как сильно влияет процесс входа пользователя в ОС ноды на производительность ноды Метапоставщика. Используется для предотвращения перегрузки ноды в момент балансировки. Чем менее производительна нода, тем сильнее на нее влияет число подключившихся пользователей и тем выше будет нагрузка на нее. Для снижения нагрузки следует назначить более высокую степень влияния на производительность. Изменение применяется на компоненте «Сессионный агент» сразу. Возможные значения: • «Экстремальное (Extreme)»; • «Высокое (High)»; • «Выше среднего (Medium-High)»; • «Среднее (Medium)» (по умолчанию); • «Ниже среднего (Medium-Low)»; • «Не использовать» - при выборе этого значения параметр не будет учитываться при балансировке
«Предпочитать соиспользование сессий вместо балансировки»	Использование возможно при активации параметра «Балансировка по метрикам». Параметр переопределяет механизм балансировки при полной загрузке ноды Метапоставщика: будет использоваться механизм соиспользования сессий, а не балансировка по метрикам узла

Максимальное число подключений к ноде (одной) Метапоставщика, если не используется «Балансировка по метрикам», можно задать командой `termidesk-vdi-manage`, предварительно переключившись на пользователя `termidesk`:

```
sudo -u termidesk bash
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_config set --key
experimental.metasessionsprov.maxConnectionCount --value <значение>
```

В случае, если используется «Балансировка по метрикам» максимальное число подключений задается параметром «Сессий всего».

После добавления Метапоставщика в Termidesk VDI будет зарегистрирован MAC-адрес узла, на котором установлен «Сессионный агент». В то же время непосредственно «Сессионный агент» сохранит IP-адрес «Универсального диспетчера», отправившего ему запрос. Поскольку MAC-адрес нужен для регистрации событий, то в случае его изменения «Универсальный диспетчер» перестанет принимать события от этого «Сессионного агента», однако подключение при этом будет работать.

Для исправления ситуации, когда MAC-адрес был изменен и от «Сессионного агента» перестали регистрироваться события, нужно:

- либо открыть поставщик ресурсов и нажать экранные кнопки **[Тест]** и **[Сохранить]** для

перерегистрации «Сессионного агента»;

- либо создать новый поставщик ресурсов с указанием нужного «Сессионного агента»;
- либо выполнить на узле с «Универсальным диспетчером» команды:

```
sudo -u termidesk bash
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_refresh_ssa
```

Указанные команды выполняются также для регистрации «Сессионного агента» в случае, если компонент «Универсальный диспетчер» был обновлен раньше него.

Если в качестве сервисного фонда используется фонд автономных машин, то возможна ситуация, когда первое подключение к автономной машине будет неуспешным, если на ней изменился MAC-адрес. Для исправления ситуации следует выполнить повторное подключение.

Балансировка подключений на основе загрузки терминальных серверов Метапоставщика

Для эффективного распределения ресурсов терминальных серверов Метапоставщика реализована поддержка балансировки подключений на основе метрик, которые отправляет «Сессионный агент».

Балансировка подключений будет работать только при выборе протокола доставки «RDP терминальный». Более ранние протоколы доставки не поддерживаются.

Процесс балансировки состоит в следующем:

- «Сессионный агент», установленный на ноды Метапоставщика, собирает метрики узла и хранит их в своей БД;
- «Универсальному диспетчеру» передаются средние значения метрик ноды, подсчет которых задается через параметр «Размер кеша» (см. подраздел **Настройка отправки метрик для «Сессионного агента»**);
- на основе полученных метрик «Универсальный диспетчер» рассчитывает нагрузку на каждую ноду Метапоставщика. Расчет нагрузки хранится в таблице БД «Универсального диспетчера»;
- при запросе пользователя на подключение к Метапоставщику:
  - проверяет, установлен ли в его свойствах параметр «Соиспользование сессий». Если параметр активирован и у пользователя уже есть активная сессия, то Метапоставщик вернет адрес подключения той ноды, на которую терминирована сессия;
  - проверяет, активирован ли параметр «Балансировка по метрикам». Если параметр активирован, то Метапоставщик получит список всех нод и выполнит балансировку подключения, вернув пользователю ноду, имеющую минимальную нагрузку или любую, если несколько нод имеют одинаково наименьшее значение нагрузки. При этом во время балансировки будут проверены условия как получения метрик, так и их актуальности.

Если активированы оба параметра «Балансировка по метрикам» и «Соиспользование сессий», то проверяется параметр «Предпочитать соиспользование сессий вместо балансировки». В зависимости от его значения новая сессия либо будет направлена на ту же ноду, либо на наименее нагруженную.

Если метрики с какой-либо из нод не получены или стали неактуальны, такая нода будет переведена в режим техобслуживания, а соответствующее событие об этом будет

отражено в журнале «Универсального диспетчера» `/var/log/termidesk/termidesk.log`.

Следующие события, связанные с механизмом балансировки, регистрируются в журнале фонда Метапоставщика:

- достижение максимальной нагрузки ноды: «Значение индекса нагрузки достигло предела в 10000 slv. Узел <IP-адрес> не будет принимать новых пользователей до тех пор, пока нагрузка не снизится»;
- выбор наименее загруженной ноды (событие регистрируется для уровня DEBUG): «Пользователь будет перенаправлен на этот узел: <IP-адрес>, т.к. он наименее загружен»;
- вход пользователя на ноду: «Пользователь <Имя пользователя> успешно вошел в систему».

В журнале РМ отражаются события входа всех пользователей, добавленных в фонд Метапоставщика и подключившихся к одной ноде. Например, если в фонд добавлена группа с пользователями «user1» и «user2», тогда, несмотря на то, что пользователи получат разные РМ при подключении к одной ноде (назначенной ВМ), событие подключения «user2», присоединившегося позже, также зарегистрируется в журнале РМ «user1».

Из очереди балансировки исключаются поставщики ресурсов и фонды, находящиеся в режиме техобслуживания.

Режим техобслуживания поставщика ресурсов

Режим техобслуживания предназначен для проведения плановых регламентных или аварийных работ поставщика ресурсов. В режиме техобслуживания Termidesk VDI не использует поставщика ресурсов для размещения фондов РМ.

Состояние режима техобслуживания отображается в столбце «Техобслуживание» списка поставщиков ресурсов.

Для перевода поставщика ресурсов в режим техобслуживания следует перейти «Инфраструктура - Поставщики ресурсов», в столбце «Техобслуживание» установить переключатель в положение «Включен» для соответствующего поставщика ресурсов.

Для отключения режима техобслуживания нужно установить переключатель в положение «Выключен» для соответствующего поставщика ресурсов.

По завершении техобслуживания поставщик ресурсов может быть снова использован для размещения фондов РМ.

ШАБЛОНЫ РМ В ПОСТАВЩИКАХ РЕСУРСОВ

Общие сведения о шаблонах РМ

РМ в общем случае представляет собой гостевую ОС или ОС, установленную на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа. К РМ относится:

- ВРМ;
- терминальные серверы, к которым пользователь получает доступ (терминальная сессия или приложение).

В рамках документации принято, что сокращение ВРМ используется, когда речь идет о

классическом сценарии VDI, когда РМ - это развернутая на ВМ гостевая ОС с установленным «Агентом виртуального рабочего места» и необходимым прикладным ПО, доступ к которой реализуется с помощью протокола удаленного доступа.

Termidesk VDI выполняет подготовку РМ на основе заданных шаблонов. Шаблон РМ - совокупность параметров для создания ВМ на платформе виртуализации.

В случае с подготовкой ВРМ Termidesk VDI создает шаблон с префиксом «TDSK», а не из исходных шаблонов базового ВРМ, настроенных администратором на поставщике ресурсов.

Каждый поставщик ресурсов поддерживает свой набор типов шаблонов РМ. Поддерживаемый в Termidesk VDI список типов шаблонов:

Доступность функционала зависит от типа редакции Termidesk VDI.

- шаблон на основе связанного клона - предполагает создание ВРМ из базового образа на платформе виртуализации в режиме инкрементного копирования;
- шаблон на основе полного клона - предполагает создание ВРМ из базового образа на платформе виртуализации в режиме полного копирования;
- связанный клон на базе снапшота - предполагает создание ВРМ на основе снимка виртуального жесткого диска базовой ВМ. В этом случае на платформе виртуализации должна быть развернута непосредственно ВМ;
- шаблоны серверов терминалов - предполагают создание РМ на основе терминального доступа или доступа к опубликованным на терминальном сервере приложениям;
- шаблон на основе автономных машин - предполагает создание РМ на основе шаблона «Автономные машины», созданного для автономной машины.

Для добавления шаблона в веб-интерфейсе Termidesk VDI следует перейти «Инфраструктура - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне следует нажать на экранную кнопку **[Создать]**, а затем из выпадающего списка выбрать поддерживаемый в Termidesk VDI способ формирования шаблона РМ.

Созданные шаблоны можно:

- редактировать, для этого необходимо выбрать шаблон, а затем нажать на экранную кнопку **[Изменить]**;
- удалить, для этого необходимо выбрать шаблон, а затем нажать на экранную кнопку **[Удалить]**.

Шаблон может быть удален только в том случае, если он не используется фондом РМ.

Шаблоны ВРМ для ПК СВ Брест

Шаблон на основе связанного и полного клона для ПК СВ Брест

Для добавления шаблона следует перейти «Инфраструктура - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов «ПК СВ "Брест"».

Далее в открывшемся окне нужно нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать один из шаблонов «Полный клон» или «Связанный клон», затем заполнить

данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблонов на основе клонов для ПК СВ Брест).

Таблица 49. Данные для добавления шаблонов на основе клонов для ПК СВ Брест

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Хранилище»	Идентификатор ресурсов хранения, представленных в платформе виртуализации, используемых для размещения файлов ВМ, входящих в фонд РМ
«Базовый шаблон»	Единый базовый образ, используемый для создания точной копии, из которой будут создаваться ВРМ. Базовый образ составляет базовый шаблон ВМ, подготовленный в платформе виртуализации совместно с выполненными в гостевой ОС настройками
«Базовое имя»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого ВРМ. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (только строчных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера наименования, используемая в идентификаторе каждого ВРМ. Возможные значения: от 3 до 6
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: • «0-9» - числовой формат порядкового номера; • «a-z» - символьный формат порядкового номера

Шаблон на базе снапшота для ПК СВ Брест

Для добавления шаблона следует перейти «Инфраструктура - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов «ПК СВ "Брест"».

Далее в открывшемся окне нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Связанный клон на базе снимка», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона на базе снапшота для ПК СВ Брест).

Для возможности использования шаблона на базе снапшота в ПК СВ Брест нужно:

- создать базовый шаблон ВМ;
- создать экземпляр ВМ на основе базового шаблона;
- создать снимок диска экземпляра ВМ. Для этого на платформе виртуализации выбрать ВМ, перейти в раздел «Хранилище» и нажать на пиктограмму создания снимка в строке соответствующего диска.

Таблица 50. Данные для добавления шаблона на базе снапшота для ПК СВ Брест

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Хранилище»	Идентификатор ресурсов хранения, представленных в платформе виртуализации, используемых для размещения файлов ВМ, входящих в фонд РМ
«Базовая ВМ»	ВМ, на базе которой будут создаваться фонды РМ

Параметр	Описание
«Базовое имя»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого ВРМ. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (только строчных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера наименования, используемая в идентификаторе каждого ВРМ. Возможные значения: от 3 до 6
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: • «0-9» - числовой формат порядкового номера; • «a-z» - символьный формат порядкового номера

Шаблоны ВРМ для oVirt

Шаблон на основе полного клона для oVirt

Для добавления шаблона следует перейти «Инфраструктура - Поставщики ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Полный клон», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона на основе полного клона для oVirt).

Таблица 51. Данные для добавления шаблона на основе полного клона для oVirt

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Кластер»	Идентификатор кластера на платформе oVirt, используемый для размещения фондов РМ
«Хранилище»	Идентификатор ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд РМ
«Место (Гб)»	Минимально необходимое дисковое пространство на объекте «Хранилище» для размещения файлов ВМ, входящих в фонд РМ
«Базовая ВМ»	Единый базовый образ, используемый для создания точной копии, из которой будут созданы фонды РМ
«Память (Мб)»	Объем оперативной памяти, выделяемый ВРМ
«Гарантированная память (Мб)»	Минимальный объем оперативной памяти, резервируемый для ВРМ
«USB»	Политика разрешения доступа к USB-портам
«Дисплей»	Используемый протокол удаленного доступа к ВРМ
«Базовое имя»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого ВРМ. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (только строчных), цифр и знака «-» (дефис)

Параметр	Описание
«Длина суффикса»	Длина порядкового номера наименования, используемого в идентификаторе каждого ВРМ. Возможные значения: от 3 до 6. При настройке параметра будет отображено предупреждение: «Для создания максимально возможного числа машин в фонде не хватает XXXXX ГБ». Оно информирует о нехватке объема выбранного хранилища для публикации максимального числа машин из шаблона. Максимальное количество машин определяется типом и длиной суффикса. Пример: если в «Типе суффикса» задано значение «0-9», а в «Длине суффикса» задано значение «3», то из шаблона можно создать не более 1000 РМ
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: • «0-9» - числовой формат порядкового номера; • «a-z» - символьный формат порядкового номера

ВМ, из которой планируется создать шаблон, может отображаться с некоторой задержкой, следует немного подождать ее появления в параметре «Базовая ВМ».

Шаблон на основе связанного клона для oVirt

Для добавления шаблона следует перейти «Инфраструктура - Поставщики ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Связанный клон», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона на основе связанного клона для oVirt).

Таблица 52. Данные для добавления шаблона на основе связанного клона для oVirt

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Кластер»	Идентификатор кластера на платформе oVirt, используемый для размещения фондов РМ
«Хранилище»	Идентификатор ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд РМ
«Место (Гб)»	Минимально необходимое дисковое пространство на объекте «Хранилище» для размещения файлов ВМ, входящих в фонд РМ
«Базовая ВМ»	Единый базовый образ, используемый для создания точной копии, из которой будут созданы фонды РМ
«Память (Мб)»	Объем оперативной памяти, выделяемый ВРМ
«Гарантированная память (Мб)»	Минимальный объем оперативной памяти, резервируемый для ВРМ
«USB»	Политика разрешения доступа к USB-портам
«Дисплей»	Используемый протокол удаленного доступа к ВРМ

Параметр	Описание
«Базовое имя»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого ВРМ. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (только строчных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера наименования, используемого в идентификаторе каждого ВРМ. Возможные значения: от 3 до 6. При настройке параметра будет отображено предупреждение: «Для создания максимально возможного числа машин в фонде не хватает XXXXX ГБ». Оно информирует о нехватке объема выбранного хранилища для публикации максимального числа машин из шаблона. Максимальное количество машин определяется типом и длиной суффикса. Пример: если в «Типе суффикса» задано значение «0-9», а в «Длине суффикса» задано значение «3», то из шаблона можно создать не более 1000 РМ
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: • «0-9» - числовой формат порядкового номера; • «a-z» - символьный формат порядкового номера

ВМ, из которой планируется создать шаблон, может отображаться с некоторой задержкой, следует немного подождать ее появления в параметре «Базовая ВМ».

Создание снимка ВМ для oVirt

Для создания снимка ВМ (снапшота) следует перейти «Инфраструктура - Поставщики ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Перед созданием снимка ВМ, состояние которой нужно зафиксировать, должна быть выключена!

Далее в открывшемся окне нужно нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «Снимок», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления снимка ВМ для oVirt).

Таблица 53. Данные для добавления снимка ВМ для oVirt

Параметр	Описание
«Название»	Текстовое наименование создаваемого снимка ВМ
«Шаблон»	Выбор шаблона для поставщика oVirt, для которого будет сделан снимок ВМ. Шаблон для поставщика oVirt должен существовать к моменту создания снимка ВМ
«Комментарий»	Информационное сообщение, используемое для описания назначения создаваемого снимка ВМ

Шаблоны ВРМ для платформы «РЕД Виртуализация»

Шаблон на основе полного клона для платформы «РЕД Виртуализация»

Для добавления шаблона следует перейти «Инфраструктура - Поставщики ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование поставщика

ресурсов.

Далее в открывшемся окне нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Полный клон», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона на основе полного клона для платформы «РЕД Виртуализация»).

Таблица 54. Данные для добавления шаблона на основе полного клона для платформы «РЕД Виртуализация»

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Кластер»	Идентификатор кластера на платформе «РЕД Виртуализация», используемый для размещения фондов ВМ
«Хранилище»	Идентификатор ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд ВМ
«Место (Гб)»	Минимально необходимое дисковое пространство (в ГБ) на объекте «Хранилище» для размещения файлов ВМ, входящих в фонд ВМ
«Базовая ВМ»	Единый базовый образ, используемый для создания точной копии (реплики), из которой будут созданы фонды ВМ
«Память (Мб)»	Объем оперативной памяти (в МБ), выделяемый ВРМ
«Гарантированная память (Мб)»	Минимальный объем оперативной памяти (в МБ), резервируемый для ВРМ
«USB»	Политика разрешения доступа к USB-портам
«Дисплей»	Используемый протокол удаленного доступа к ВРМ
«Базовое имя»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого ВРМ. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (только строчных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера наименования, используемого в идентификаторе каждого ВРМ. Возможные значения: от 3 до 6. При настройке параметра будет отображено предупреждение: «Для создания максимально возможного числа машин в фонде не хватает XXXXX ГБ». Оно информирует о нехватке объема выбранного хранилища для публикации максимального числа машин из шаблона. Максимальное количество машин определяется типом и длиной суффикса. Пример: если в «Типе суффикса» задано значение «0-9», а в «Длине суффикса» задано значение «3», то из шаблона можно создать не более 1000 РМ
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: • «0-9» - числовой формат порядкового номера; • «a-z» - символьный формат порядкового номера

Шаблон на основе связанного клона для платформы «РЕД Виртуализация»

Для добавления шаблона следует перейти «Инфраструктура - Поставщики ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне нажать на экранную кнопку **[Создать]**, из выпадающего списка

выбрать шаблон «Связанный клон», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона на основе связанного клона для платформы «РЕД Виртуализация»).

Таблица 55. Данные для добавления шаблона на основе связанного клона для платформы «РЕД Виртуализация»

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Кластер»	Идентификатор кластера на платформе «РЕД Виртуализация», используемый для размещения фондов ВМ
«Хранилище»	Идентификатор ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд ВМ
«Место (Гб)»	Минимально необходимое дисковое пространство (в ГБ) на объекте «Хранилище» для размещения файлов ВМ, входящих в фонд ВМ
«Базовая ВМ»	Единый базовый образ, используемый для создания точной копии (реплики), из которой будут созданы фонды ВМ
«Память (Мб)»	Объем оперативной памяти (в МБ), выделяемый ВРМ
«Гарантированная память (Мб)»	Минимальный объем оперативной памяти (в МБ), резервируемый для ВРМ
«USB»	Политика разрешения доступа к USB-портам
«Дисплей»	Используемый протокол удаленного доступа к ВРМ
«Базовое имя»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого ВРМ. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (только строчных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера наименования, используемого в идентификаторе каждого ВРМ. Возможные значения: от 3 до 6. При настройке параметра будет отображено предупреждение: «Для создания максимально возможного числа машин в фонде не хватает XXXXX ГБ». Оно информирует о нехватке объема выбранного хранилища для публикации максимального числа машин из шаблона. Максимальное количество машин определяется типом и длиной суффикса. Пример: если в «Типе суффикса» задано значение «0-9», а в «Длине суффикса» задано значение «3», то из шаблона можно создать не более 1000 РМ
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: • «0-9» - числовой формат порядкового номера; • «a-z» - символьный формат порядкового номера

Создание снимка ВМ для платформы «РЕД Виртуализация»

Для создания снимка ВМ (снапшота) следует перейти «Инфраструктура - Поставщики ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Перед созданием снимка ВМ, состояние которой нужно зафиксировать, должна быть выключена!

Далее в открывшемся окне нужно нажать на экранную кнопку **[Создать]**, из выпадающего

списка выбрать «Снимок», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления снимка ВМ для платформы «РЕД Виртуализация»).

Таблица 56. Данные для добавления снимка ВМ для платформы «РЕД Виртуализация»

Параметр	Описание
«Название»	Текстовое наименование создаваемого снимка ВМ
«Шаблон»	Выбор шаблона для поставщика «РЕД Виртуализация», для которого будет сделан снимок ВМ. Шаблон для поставщика «РЕД Виртуализация» должен существовать к моменту создания снимка ВМ
«Комментарий»	Информационное сообщение, используемое для описания назначения создаваемого снимка ВМ

Шаблоны ВРМ для zVirt

Шаблон на основе полного клона для zVirt

Для добавления шаблона следует перейти «Инфраструктура - Поставщики ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне нужно на экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Полный клон», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона на основе полного клона для zVirt).

Таблица 57. Данные для добавления шаблона на основе полного клона для zVirt

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Кластер»	Идентификатор кластера на платформе zVirt, используемый для размещения фондов РМ
«Хранилище»	Идентификатор ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд РМ
«Место (Гб)»	Минимально необходимое дисковое пространство на объекте «Хранилище» для размещения файлов ВМ, входящих в фонд РМ
«Базовая ВМ»	Единый базовый образ, используемый для создания точной копии (реплики), из которой будут созданы фонды РМ
«Память (Мб)»	Объем оперативной памяти, выделяемый ВРМ
«Гарантированная память (Мб)»	Минимальный объем оперативной памяти, резервируемый для ВРМ
«USB»	Политика разрешения доступа к USB-портам
«Дисплей»	Используемый протокол удаленного доступа к ВРМ

Параметр	Описание
«Базовое имя»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого ВРМ. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (только строчных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера наименования, используемого в идентификаторе каждого ВРМ. Возможные значения: от 3 до 6. При настройке параметра будет отображено предупреждение: «Для создания максимально возможного числа машин в фонде не хватает XXXXX ГБ». Оно информирует о нехватке объема выбранного хранилища для публикации максимального числа машин из шаблона. Максимальное количество машин определяется типом и длиной суффикса. Пример: если в «Типе суффикса» задано значение «0-9», а в «Длине суффикса» задано значение «3», то из шаблона можно создать не более 1000 РМ
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: • «0-9» - числовой формат порядкового номера; • «a-z» - символьный формат порядкового номера

Шаблон на основе связанного клона для zVirt

Для добавления шаблона следует перейти «Инфраструктура - Поставщики ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне нужно на экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Связанный клон», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона на основе связанного клона для zVirt).

Таблица 58. Данные для добавления шаблона на основе связанного клона для zVirt

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Кластер»	Идентификатор кластера на платформе zVirt, используемый для размещения фондов РМ
«Хранилище»	Идентификатор ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд РМ
«Место (Гб)»	Минимально необходимое дисковое пространство на объекте «Хранилище» для размещения файлов ВМ, входящих в фонд РМ
«Базовая ВМ»	Единый базовый образ, используемый для создания точной копии (реплики), из которой будут созданы фонды РМ
«Память (Мб)»	Объем оперативной памяти, выделяемый ВРМ

Параметр	Описание
«Гарантированная память (Мб)»	Минимальный объем оперативной памяти, резервируемый для ВРМ
«USB»	Политика разрешения доступа к USB-портам
«Дисплей»	Используемый протокол удаленного доступа к ВРМ
«Базовое имя»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого ВРМ. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (только строчных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера наименования, используемого в идентификаторе каждого ВРМ. Возможные значения: от 3 до 6. При настройке параметра будет отображено предупреждение: «Для создания максимально возможного числа машин в фонде не хватает XXXXX ГБ». Оно информирует о нехватке объема выбранного хранилища для публикации максимального числа машин из шаблона. Максимальное количество машин определяется типом и длиной суффикса. Пример: если в «Типе суффикса» задано значение «0-9», а в «Длине суффикса» задано значение «3», то из шаблона можно создать не более 1000 РМ
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: • «0-9» - числовой формат порядкового номера; • «a-z» - символьный формат порядкового номера

Создание снимка ВМ для zVirt

Для создания снимка ВМ (снапшота) следует перейти «Инфраструктура - Поставщики ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Перед созданием снимка ВМ, состояние которой нужно зафиксировать, должна быть выключена!

Далее в открывшемся окне нужно нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «Снимок», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления снимка ВМ для zVirt).

Таблица 59. Данные для добавления снимка ВМ для zVirt

Параметр	Описание
«Название»	Текстовое наименование создаваемого снимка ВМ
«Шаблон»	Выбор шаблона для поставщика zVirt, для которого будет сделан снимок ВМ. Шаблон для поставщика zVirt должен существовать к моменту создания снимка ВМ
«Комментарий»	Информационное сообщение, используемое для описания назначения создаваемого снимка ВМ

Шаблоны ВРМ для VMmanager

Шаблон на основе образа ВМ для VMmanager

Для добавления шаблона следует перейти в «Инфраструктура - Поставщики ресурсов», в

столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне следует нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «ВМ из образа», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона на основе образа ВМ).

Для добавления шаблона на основе связанного клона для платформы VMmanager необходимо создать шаблон «ВМ из образа», в котором включить параметр «Создать как связанный клон».

Таблица 60. Данные для добавления шаблона на основе образа ВМ

Параметр	Описание
«Название»	Текстовое наименование шаблона. Параметр обязателен для заполнения
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Кластер»	Идентификатор кластера на платформе VMmanager, используемый для размещения фондов РМ. Параметр обязателен для заполнения
«Узел»	Идентификатор узла кластера на платформе VMmanager, используемый для размещения фондов РМ. Значение по умолчанию: «Автоматически» (размещением управляет платформа VMmanager)
«Образ ВМ»	Единый базовый образ, используемый для создания точной копии из которой будут созданы фонды РМ. Параметр обязателен для заполнения
«Количество ЦПУ»	Количество процессоров ВМ. Значение по умолчанию: «1»
«Объем памяти, Мб»	Объем оперативной памяти ВМ. Значение по умолчанию: «512»
«Объем диска, Мб»	Размер диска, выделяемый ВМ. Значение по умолчанию: «512»
«Использовать VxLAN»	Управление использованием виртуальной сети VxLAN. Следует включить параметр, если базовая ВМ создана с использованием виртуальной сети VxLAN. При использовании физической сети следует оставить значение по умолчанию. Значение по умолчанию: «Нет»
«Виртуальная сеть»	Выбор виртуальной сети, созданной в кластере платформы VMmanager, к которой будет подключена ВМ. Использование параметра возможно, если включен «Использовать VxLAN»

Параметр	Описание
«Локальная сеть»	Выбор локальной сети, к которой будет подключена ВМ. Использование параметра возможно, если включен «Использовать VxLAN». Параметр используется, если на платформе VMmanager создана дополнительная локальная сеть для виртуальной сети
«Подключить к бриджу»	Выбор сетевого моста (бриджа) узла кластера платформы VMmanager, к которому будет подключен сетевой интерфейс ВМ. Использование параметра возможно, если выключен «Использовать VxLAN»
«Использовать DHCP»	Управление использованием автоматического назначения IP-адресов по протоколу DHCP. Использование параметра возможно, если выключен «Использовать VxLAN». Значение по умолчанию: «Нет»
«Пул IP-адресов»	Идентификатор пула IP-адресов, настроенный на платформе VMmanager, из которого будут назначаться IP-адреса ВМ. Использование параметра возможно, если выключен «Использовать DHCP».
«Количество IP-адресов»	Количество IP-адресов, которое может быть выделено ВМ. Ограничение возможного количества определяется платформой VMmanager. Использование параметра возможно, если выключен «Использовать DHCP». Значение по умолчанию: «1»
«Пользовательский скрипт»	Выбор выполняемого пользовательского скрипта. Если пользовательский скрипт не используется, следует выбрать «Без скрипта». Параметр обязателен для заполнения
«Пароль root»	Пароль пользователя root гостевой ОС. Параметр необходим для подключения к ВМ и авторизации в гостевой ОС. Параметр обязателен для заполнения
«Доменное имя»	Имя домена для ВМ (требуется заполнить, если ВМ введена в домен). Параметр необходим для подключения к ВМ
«Базовое имя»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого ВРМ. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (только строчных), цифр и знака «-» (дефис). Параметр обязателен для заполнения

Параметр	Описание
«Длина суффикса»	Длина порядкового номера наименования, используемого в идентификаторе каждого ВРМ. Возможные значения: от 3 до 6. Значение по умолчанию: «5» При настройке параметра будет отображено предупреждение: «Для создания максимально возможного числа машин в фонде не хватает XXXXX ГБ». Оно информирует о нехватке объема выбранного хранилища для публикации максимального числа машин из шаблона. Максимальное количество машин определяется типом и длиной суффикса. Пример: если в «Типе суффикса» задано значение «0-9», а в «Длине суффикса» задано значение «3», то из шаблона можно создать не более 1000 РМ
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: • «0-9» (по умолчанию) - числовой формат порядкового номера; • «a-z» - символьный формат порядкового номера
«Создать как связанный клон»	Управление созданием ВМ в режиме связанного клона. Значение по умолчанию: «Нет»

Шаблоны ВРМ для VMware vSphere

Шаблоны на основе связанного или полного клона для платформы VMware vSphere

Для добавления шаблона следует перейти «Инфраструктура - Поставщики ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать один из доступных шаблонов «Полный клон» или «Связанный клон», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона для VMware vSphere).

Таблица 61. Данные для добавления шаблона для VMware vSphere

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Датацентр»	Параметр обязателен для заполнения! Идентификатор виртуального центра обработки данных, используемый для размещения ВМ
«Кластер ресурсов»	Параметр обязателен для заполнения! Идентификатор кластера ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд

Параметр	Описание
«Кластер данных»	Параметр обязателен для заполнения! Идентификатор ресурсов хранения, используемый для размещения файлов ВМ входящих в фонд.
«Пул ресурсов»	Параметр обязателен для заполнения! Идентификатор пула ресурсов, используемый для размещения ВМ
«Размещение ВМ»	Идентификатор каталога размещения создаваемых ВМ
«Место (Гб)»	Минимальный размер свободного пространства для размещения ВМ
«Базовая ВМ»	Единый базовый образ, используемый для создания точной копии, из которой будут созданы фонды
«Сети»	Выбор одной или нескольких сетей, которые будут использоваться для назначения создаваемым ВМ. Список доступных сетей определяется значениями параметра «Сети», заданного в параметрах поставщика ресурсов («Инфраструктура - Поставщики ресурсов»). При создании новой ВМ Termidesk VDI проверяет доступность указанных сетей (по порядку следования) и наличие в них свободного IP-адреса
«Максимальное количество ВРМ, подключаемых к каждой выбранной сети поставщика ресурсов»	Выбор максимального количества ВРМ для подключения к каждой сети, заданной в параметре «Сети». При добавлении фонда РМ для поставщика ресурсов VMware vSphere суммарное количество создаваемых ВРМ в кеше 1-го уровня не должно превышать установленное значение данного параметра. При достижении предельного количества подключаемых к сети ВРМ вновь создаваемые при публикации ВРМ будут отображаться с ошибкой «No available network found». Предельное количество подключаемых к сети ВРМ - это количество сетей, выбранных в параметре «Сети», умноженное на значение параметра «Максимальное количество ВРМ, подключаемых к каждой выбранной сети поставщика ресурсов»

Параметр	Описание
«Режим диска»	Выбор режима работы диска ВРМ. Возможные значения: • «Зависимый» - при таком режиме все изменения при работе пользователя с ВРМ записываются на основной диск. Механизм восстановления ВРМ для этого режима основывается на восстановлении снимка ВМ (снапшота); • «Независимый-Непостоянный» - при таком режиме на момент запуска ВМ (получения ВРМ пользователем) создается временный диск, являющийся копией основного. Все изменения при работе пользователя с ВРМ записываются на временный диск. При небезопасной перезагрузке или небезопасном выключении временный диск удаляется. Механизм восстановления ВРМ для этого режима происходит через небезопасное выключение ВМ
«Базовое имя»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого ВРМ. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (только строчных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера наименования, используемая в идентификаторе каждого ВРМ. Возможные значения: от 3 до 6. При настройке параметра будет отображено предупреждение: «Для создания максимально возможного числа машин в фонде не хватает XXXXX ГБ». Оно информирует о нехватке объема выбранного хранилища для публикации максимального числа машин из шаблона. Максимальное количество машин определяется типом и длиной суффикса. Пример: если в «Типе суффикса» задано значение «0-9», а в «Длине суффикса» задано значение «3», то из шаблона можно создать не более 1000 РМ
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: • «0-9» - числовой формат порядкового номера; • «a-z» - символьный формат порядкового номера
«Использовать статический MAC-адрес при создании»	Управление режимом назначения статического MAC-адреса для ВМ. Проверка на пересечение MAC-адресов проводится только между теми шаблонами, в которых включен этот параметр. Значение по умолчанию: «Нет»

Параметр	Описание
«Префикс диапазона MAC-адресов»	Задание префикса диапазона частных MAC-адресов, который будет использоваться для создания MAC-адреса ВМ. Использование возможно при: • активации параметра «Использовать статический MAC-адрес при создании»; • указании сети в параметре «Сети». В разных шаблонах РМ необходимо указывать разные префиксы MAC-адресов для исключения их дублирования. Если у ВМ будет несколько сетевых интерфейсов, то настройка префикса будет действовать только для первого интерфейса (eth0). Если используется переиспользование имен для ВМ (см. подраздел **Общие системные параметры Termidesk VDI**), то: • для ВМ с переиспользованным именем будет назначен ранее записанный в БД MAC-адрес; • для ВМ с переиспользованным именем будет назначен ранее записанный в БД IP-адрес. Значение префикса должно удовлетворять условиям: • допускается задание от 3 до 5 октетов; • запрещено использовать значение «00:05:56». Значение по умолчанию: «00:00:6C»

Создание снимка ВМ для платформы VMware vSphere

Для создания снимка ВМ (снапшота) следует перейти «Инфраструктура - Поставщики ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Перед созданием снимка ВМ, состояние которой нужно зафиксировать, должна быть выключена!

Далее в открывшемся окне нужно нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «Снимок», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления снимка ВМ для VMware vSphere).

Таблица 62. Данные для добавления снимка ВМ для VMware vSphere

Параметр	Описание
«Название»	Текстовое наименование создаваемого снимка ВМ
«Шаблон»	Выбор шаблона для поставщика VMware vSphere, для которого будет сделан снимок ВМ. Шаблон для поставщика VMware vSphere должен существовать к моменту создания снимка ВМ

Параметр	Описание
«Комментарий»	Информационное сообщение, используемое для описания назначения создаваемого снимка ВМ

Шаблон РМ машины с сетевой загрузкой для платформы VMware vSphere

Подробнее о технологии сетевой (бездисковой) загрузки и этапах подготовки инфраструктуры приведено в подразделе **Технология бездисковой (сетевой) загрузки**.

Для добавления шаблона следует перейти в «Инфраструктура - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне следует нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Сетевая загрузка», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона сетевой загрузки для VMware vSphere).

Таблица 63. Данные для добавления шаблона сетевой загрузки для VMware vSphere

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Датацентр»	Параметр обязателен для заполнения! Идентификатор виртуального центра обработки данных, используемый для размещения ВМ
«Кластер ресурсов»	Параметр обязателен для заполнения! Идентификатор кластера ресурсов хранения, используемый для размещения файлов ВМ, входящих в фонд
«Кластер данных»	Параметр обязателен для заполнения! Идентификатор ресурсов хранения, используемый для размещения файлов ВМ входящих в фонд.
«Пул ресурсов»	Параметр обязателен для заполнения! Идентификатор пула ресурсов, используемый для размещения ВМ
«Размещение ВМ»	Идентификатор каталога размещения создаваемых ВМ
«Место (Гб)»	Минимальный размер свободного пространства для размещения ВМ
«Базовая ВМ»	Единый базовый образ, используемый для создания точной копии, из которой будут созданы фонды

Параметр	Описание
«Сети»	Выбор одной или нескольких сетей, которые будут использоваться для назначения создаваемым ВМ. Список доступных сетей определяется значениями параметра «Сети», заданного в параметрах поставщика ресурсов («Инфраструктура - Поставщики ресурсов»). При создании новой ВМ Termidesk проверяет доступность указанных сетей (по порядку следования) и наличие в них свободного IP-адреса
«Максимальное количество ВРМ, подключаемых к каждой выбранной сети поставщика ресурсов»	Выбор максимального количества ВРМ для подключения к каждой сети, заданной в параметре «Сети». При добавлении фонда РМ для поставщика ресурсов VMware vSphere суммарное количество создаваемых ВРМ в кеше 1-го уровня не должно превышать установленное значение данного параметра. При достижении предельного количества подключаемых к сети ВРМ вновь создаваемые при публикации ВРМ будут отображаться с ошибкой «No available network found». Предельное количество подключаемых к сети ВРМ - это количество сетей, выбранных в параметре «Сети», умноженное на значение параметра «Максимальное количество ВРМ, подключаемых к каждой выбранной сети поставщика ресурсов»
«Режим диска»	Выбор режима работы диска ВРМ. Возможные значения: • «Зависимый» - при таком режиме все изменения при работе пользователя с ВРМ записываются на основной диск. Механизм восстановления ВРМ для этого режима основывается на восстановлении снимка ВМ (снапшота); • «Независимый-Непостоянный» - при таком режиме на момент запуска ВМ (получения ВРМ пользователем) создается временный диск, являющийся копией основного. Все изменения при работе пользователя с ВРМ записываются на временный диск. При небезопасной перезагрузке или небезопасном выключении временный диск удаляется. Механизм восстановления ВРМ для этого режима происходит через небезопасное выключение ВМ

Параметр	Описание
«Базовое имя»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого ВРМ. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (только строчных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера наименования, используемая в идентификаторе каждого ВРМ. Возможные значения: от 3 до 6. При настройке параметра будет отображено предупреждение: «Для создания максимально возможного числа машин в фонде не хватает XXXXX ГБ». Оно информирует о нехватке объема выбранного хранилища для публикации максимального числа машин из шаблона. Максимальное количество машин определяется типом и длиной суффикса. Пример: если в «Типе суффикса» задано значение «0-9», а в «Длине суффикса» задано значение «3», то из шаблона можно создать не более 1000 РМ
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: • «0-9» - числовой формат порядкового номера; • «a-z» - символьный формат порядкового номера
«Использовать статический MAC-адрес при создании»	Управление режимом назначения статического MAC-адреса для ВМ. Проверка на пересечение MAC-адресов проводится только между теми шаблонами, в которых включен этот параметр. Значение по умолчанию: «Нет»

Параметр	Описание
«Префикс диапазона MAC-адресов»	Задание префикса диапазона частных MAC-адресов, который будет использоваться для создания MAC-адреса ВМ. Использование возможно при: • активации параметра «Использовать статический MAC-адрес при создании»; • указании сети в параметре «Сети». В разных шаблонах РМ необходимо указывать разные префиксы MAC-адресов для исключения их дублирования. Если у ВМ будет несколько сетевых интерфейсов, то настройка префикса будет действовать только для первого интерфейса (eth0). Если используется переиспользование имен для ВМ (см. подраздел **Общие системные параметры Termidesk**), то: • для ВМ с переиспользованным именем будет назначен ранее записанный в БД MAC-адрес; • для ВМ с переиспользованным именем будет назначен ранее записанный в БД IP-адрес. Значение префикса должно удовлетворять условиям: • допускается задание от 3 до 5 октетов; • запрещено использовать значение «00:05:56». Значение по умолчанию: «00:00:6C»
«iSCSI хранилище»	Адрес подключения к iSCSI-хранилищу, на котором размещен базовый образ РМ. Задается в формате: `iscsi:<IP-адрес_хранилища>:<порт_подключения>:<тип_аутентификации>:<LUN>`. Данные параметры настраиваются при конфигурировании iSCSI для бездисковой загрузки (см. подраздел **Настройка стека серверов для бездисковой загрузки**). Пример: «iscsi:172.16.0.1:::1»

Параметр	Описание
«Имя целевого iSCSI устройства»	Имя iSCSI устройства, на котором размещен базовый образ РМ. Задается в формате iSCSI Qualified Name: `iqn.<гггг-мм>.<обратный_домен>:<уникальный_идентификатор>`. Где: • `iqn` - указывает на использование формата iSCSI Qualified Name; • `<гггг-мм>` - дата (год и месяц), когда было зарегистрировано доменное имя (например, 2026-05); • <обратный_домен> - обратное доменное имя организации (например, `local.ipxe`); • <уникальный_идентификатор> - строка, выбранная для идентификации конкретного устройства или сервера (например, `astra-disk-dev`). Данные параметры настраиваются при конфигурировании iSCSI для бездисковой загрузки (см. подраздел **Настройка стека серверов для бездисковой загрузки**). Пример: «iqn.2026-06.local.ipxe:test-disk»

Шаблоны РМ для терминальных серверов

Шаблон для доступа к опубликованным приложениям MS RDS

Для добавления шаблона следует перейти «Инфраструктура - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Приложение RDS», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона для доступа к приложениям MS RDS).

Таблица 64. Данные для добавления шаблона для доступа к приложениям MS RDS

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«RDS коллекция»	Название существующей в инфраструктуре MS RDS коллекции опубликованных приложений. В форме будет доступен поиск коллекции
«Удаленное приложение»	Наименование опубликованного в коллекции приложения. В форме будет доступен поиск приложения

Шаблон для доступа к терминальному серверу MS RDS

Для добавления шаблона следует перейти «Инфраструктура - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Рабочий стол RDS», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона

для доступа к терминальному серверу MS RDS).

Таблица 65. Данные для добавления шаблона для доступа к терминальному серверу MS RDS

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Терминал»	Наименование существующего терминала MS RDS. В форме будет доступен поиск терминала

Шаблон для доступа к опубликованным приложениям STAL

Для добавления шаблона следует перейти «Инфраструктура - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Приложение STAL», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона для доступа к приложениям STAL).

Таблица 66. Данные для добавления шаблона для доступа к приложениям STAL

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Удаленное приложение»	Наименование опубликованного в коллекции приложения. В форме будет доступен поиск приложения

Шаблон для доступа к терминальному серверу STAL

Для добавления шаблона следует перейти «Инфраструктура - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Рабочий стол STAL», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона для доступа к терминальному серверу STAL).

Таблица 67. Данные для добавления шаблона для доступа к терминальному серверу STAL

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона

Шаблоны РМ для Метапоставщика

Шаблон для терминальных сессий

Для добавления шаблона следует перейти «Инфраструктура - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов «Метапоставщик».

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Рабочий стол Метапоставщика», затем заполнить данные,

перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона терминальных сессий для Метапоставщика).

Таблица 68. Данные для добавления шаблона терминальных сессий для Метапоставщика

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона

Шаблон для публикации приложений

Для добавления шаблона следует перейти «Инфраструктура - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов «Метапоставщик».

Далее в открывшемся окне следует нажать экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Приложение Метапоставщика», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона публикации приложений для Метапоставщика).

Таблица 69. Данные для добавления шаблона публикации приложений для Метапоставщика

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Удаленное приложение»	Наименование опубликованного приложения

Шаблоны ВРМ для Openstack

Шаблон на основе образа ВМ для OpenStack

Для добавления шаблона следует перейти в «Инфраструктура - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне следует нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «ВМ из образа», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона на основе образа ВМ для OpenStack).

Таблица 70. Данные для добавления шаблона на основе образа ВМ для OpenStack

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Регион»	Идентификатор региона на платформе OpenStack, используемый для размещения фондов РМ
«Проект»	Единый базовый образ, используемый для создания точной копии, из которой будут созданы фонды РМ
«Зона доступности»	Выбор зоны доступности ВМ
«Образ диска»	Выбор базового образа диска, ограничен зоной доступности
«Сеть»	Выбор сети, в которой будет расположена ВМ

Параметр	Описание
«Тип диска»	Тип диска ВМ
«Размер диска»	Размер диска ВМ, в ГБ
«Конфигурация ВМ»	Выбор конфигурации ВМ, созданной в OpenStack
«Группа безопасности»	Выбор группы безопасности, созданной в OpenStack
«Базовое имя»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого ВРМ. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (как строчных, так и прописных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера наименования, используемого в идентификаторе каждого ВРМ. Возможные значения: от 3 до 6. При настройке параметра будет отображено предупреждение: «Для создания максимально возможного числа машин в фонде не хватает XXXXX ГБ». Оно информирует о нехватке объема выбранного хранилища для публикации максимального числа машин из шаблона. Максимальное количество машин определяется типом и длиной суффикса. Пример: если в «Типе суффикса» задано значение «0-9», а в «Длине суффикса» задано значение «3», то из шаблона можно создать не более 1000 РМ
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого ВРМ: • «0-9» - числовой формат порядкового номера; • «a-z» - символьный формат порядкового номера
«Состояние ВМ в кеше 2 уровня»	Выбор состояния ВМ по умолчанию в кеше 2-го уровня
«Метадата»	Информация о метаданных
«Cloud-init скрипт»	Скрипт cloud-init, выполняемый при создании ВМ

Шаблоны РМ для автономной машины

Шаблон РМ для автономной машины на основе статического IP-адреса

Для добавления шаблона следует перейти в «Инфраструктура - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

В ОС автономной машины должен быть установлен компонент «Агент виртуального рабочего места» для регистрации РМ в Termidesk VDI.

Далее в открывшемся окне следует нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Машины по IP», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона РМ на основе статического IP-адреса).

Таблица 71. Данные для добавления шаблона РМ на основе статического IP-адреса

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона

Параметр	Описание
«IP машин»	IP-адрес или IP-адреса добавляемого хоста. Может быть указан один IP-адрес, диапазон IP-адресов, перечень IP-адресов. Пример: • «192.0.2.1»; • «192.0.2.1, 192.0.2.1, 192.0.2.7»; • «192.0.2.1, 192.0.2.2-192.0.2.7, 192.0.2.10»; • «192.0.2.2-192.0.2.253»

Шаблон РМ для автономной машины на основе FQDN

Для добавления шаблона следует перейти в «Инфраструктура - Поставщики ресурсов», в столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

В ОС автономной машины должен быть установлен компонент «Агент виртуального рабочего места» для регистрации РМ в Termidesk VDI.

Далее в открывшемся окне следует нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Машины по FQDN», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона РМ на основе FQDN).

Таблица 72. Данные для добавления шаблона РМ на основе FQDN

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«FQDN машин»	FQDN добавляемого хоста или хостов. Может быть указано одно значение или перечень значений. FQDN указывается с доменным именем не ниже второго уровня. Пример: • «host1.tst.local»; • «host1.tst.local, host2.tst.local, host3.tst.local». Для добавления записей из `csv`-файла нужно нажать экранную кнопку **[CSV]** и указать путь к файлу. Требования к содержимому `csv`-файла: • первая строка должна быть пустой или содержать заголовок; • каждая строка должна содержать одно FQDN с доменным именем не ниже второго уровня; • размер файла не должен превышать 2 MB

Шаблон РМ для автономной машины с сетевой загрузкой

Подробнее о технологии сетевой (бездисковой) загрузки и этапах подготовки инфраструктуры приведено в подразделе **Технология бездисковой (сетевой) загрузки**.

Для добавления шаблона следует перейти в «Инфраструктура - Поставщики ресурсов», в

столбце «Название» сводной таблицы нажать на наименование поставщика ресурсов.

Далее в открывшемся окне следует нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать шаблон «Сетевая загрузка (MAC)», затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона РМ с сетевой загрузкой).

Таблица 73. Данные для добавления шаблона РМ с сетевой загрузкой

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«MAC-адреса машин»	MAC-адреса добавляемых хостов. Может быть указано одно значение или перечень значений через запятую
«Исключить MAC-адреса машин»	MAC-адреса исключенных хостов. Может быть указано одно значение или перечень значений через запятую
«Базовое имя»	Неизменяемая часть текстового наименования, используемая в идентификаторе каждого РМ. Базовое имя должно назначаться в соответствии с RFC 953: оно может состоять из букв латинского алфавита (только строчных), цифр и знака «-» (дефис)
«Длина суффикса»	Длина порядкового номера наименования, используемого в идентификаторе каждого РМ. Возможные значения: от 3 до 6
«Тип суффикса»	Параметр, задающий формат порядкового номера наименования в идентификаторе каждого РМ: • «0-9» - числовой формат порядкового номера; • «a-z» - символьный формат порядкового номера
«iSCSI хранилище»	Адрес подключения к iSCSI-хранилищу, на котором размещен базовый образ РМ. Задается в формате: `iscsi:<IP-адрес_хранилища>:<порт_подключения>:<тип_аутентификации>:<LUN>`. Данные параметры настраиваются при конфигурировании iSCSI для бездисковой загрузки (см. подраздел **Настройка стека серверов для бездисковой загрузки**). Пример: «iscsi:172.16.0.1:::1»
«Имя целевого iSCSI устройства»	Имя iSCSI устройства, на котором размещен базовый образ РМ. Задается в формате iSCSI Qualified Name: `iqn.<гггг-мм>.<обратный_домен>:<уникальный_идентификатор>`. Где: • `iqn` - указывает на использование формата iSCSI Qualified Name; • `<гггг-мм>` - дата (год и месяц), когда было зарегистрировано доменное имя (например, 2026-05); • <обратный_домен> - обратное доменное имя организации (например, `local.ipxe`); • <уникальный_идентификатор> - строка, выбранная для идентификации конкретного устройства или сервера (например, `astra-disk-dev`). Данные параметры настраиваются при конфигурировании iSCSI для бездисковой загрузки (см. подраздел **Настройка стека серверов для бездисковой загрузки**). Пример: «iqn.2026-06.local.ipxe:test-disk»

ПАРАМЕТРЫ ГОСТЕВЫХ ОС

Добавление параметров гостевых ОС

Общие сведения о параметрах гостевых ОС

Параметры гостевых ОС позволяют произвести автоматическую и идентичную настройку одного или нескольких РМ для использования в фонде РМ.

Веб-интерфейс Termidesk VDI с установленной ролью «Портал администратора» обеспечивает следующие операции управления параметрами гостевых ОС:

- добавление, для этого используется экранная кнопка **[Создать]** ;
- редактирование, для этого используется экранная кнопка **[Изменить]**;
- удаление, для этого используется экранная кнопка **[Удалить]**;
- просмотр сведений.

Параметры конфигурации гостевой ОС могут быть удалены только в том случае, если они не используются фондом РМ.

Для отображения списка добавленных параметров гостевых ОС следует перейти «Рабочие места - Параметры гостевых ОС». Основные параметры списка приведены в таблице (см. таблицу Параметры списка гостевых ОС).

Таблица 74. Параметры списка гостевых ОС

Параметр	Описание
«Название»	Текстовое наименование параметров гостевых ОС в Termidesk
«Используется»	Характеристика использования параметров гостевых ОС в каком-либо фонде
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевых ОС

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет

изменений для возврата к исходному состоянию;

- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Поддерживаемые комбинации ввода гостевых ОС в домен

Поддерживаемые комбинации ввода гостевых ОС в домен приведены в таблице (см. Комбинации ввода гостевых ОС в домен).

Таблица 75. Комбинации ввода гостевых ОС в домен

ОС/Домен	MS AD	ALD Pro	FreeIPA	Альт Домен
Astra Linux Special Edition 1.7, 1.8	□	□	□	
Microsoft Windows	□			
Альт Рабочая станция 10	□	□	□	□
Альт Рабочая станция 11	□	□	□	□
РЕД ОС 7	□		□	
РЕД ОС 8	□		□	

Параметры гостевой ОС Linux

Конфигурация ОС Linux без домена

Для добавления в Termidesk VDI параметров гостевой ОС на базе GNU/Linux без ввода в домен следует перейти «Рабочие места - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «ОС Linux».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для гостевой ОС Linux без ввода в домен).

Таблица 76. Данные для гостевой ОС Linux без ввода в домен

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС

Конфигурация ОС Linux при вводе в домен FreeIPA

Для добавления в Termidesk VDI параметров гостевой ОС на базе GNU/Linux с вводом в

домен FreeIPA следует перейти «Рабочие места - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «Linux FreeIPA».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для гостевой ОС Linux при вводе в домен FreeIPA).

Для ввода РМ с ОС Astra Linux в домен FreeIPA необходимо в гостевую ОС установить пакет `astra-freeipa-client`.

Таблица 77. Данные для гостевой ОС Linux при вводе в домен FreeIPA

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС
«Домен аутентификации»	Идентификатор домена FreeIPA
«Аккаунт»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Идентификатор субъекта, имеющий полномочия по добавлению РМ в домен
«Пароль»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/freeipa/»

Конфигурация ОС Linux при вводе в домен ALD Pro

Для добавления в Termidesk VDI параметров гостевой ОС на базе GNU/Linux с вводом в домен ALD Pro следует перейти «Рабочие места - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «Linux ALD Pro».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для гостевой ОС Linux при вводе в домен ALD Pro).

Для ввода РМ с ОС Astra Linux в домен ALD Pro необходимо в гостевую ОС установить пакеты `astra-freeipa-client` и `aldpro-client`.

Для корректного ввода РМ в домен нужно обеспечить корректное разрешение имен узлов в домене ALD Pro.

Таблица 78. Данные для гостевой ОС Linux при вводе в домен ALD Pro

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС

Параметр	Описание
«Домен аутентификации»	Идентификатор домена ALD Pro
«Аккаунт»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Идентификатор субъекта, имеющий полномочия по добавлению РМ в домен
«Пароль»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Путь к секретам»	NOTE:Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/aldpro/»

Конфигурация ОС Linux при вводе в домен MS AD

Для добавления в Termidesk VDI параметров гостевой ОС на базе GNU/Linux при вводе в домен MS AD следует перейти «Рабочие места - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «Linux MS AD DS».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для гостевой ОС Linux при вводе в домен MS AD).

Для ввода РМ с ОС Astra Linux в домен MS AD необходимо в гостевую ОС установить пакет `astra-ad-sssd-client`.

Таблица 79. Данные для гостевой ОС Linux при вводе в домен MS AD

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС
«Домен»	Доменное имя (DNS) службы каталогов MS AD
«Аккаунт»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Идентификатор субъекта, имеющий полномочия по добавлению РМ в домен. Для гостевых ОС Альт Рабочая станция 10 и 11 рекомендуется указывать аккаунт в формате «sAMAccountName»
«Пароль»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий

Параметр	Описание
«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/msad/»
«OU»	Идентификатор организационной единицы, в которую будут добавлены РМ. Следует учесть, что при вводе гостевой ОС в домен MS AD рекомендуется создавать обособленные подразделения домена, и не создавать учетные записи в подразделении «Computers». Если учетные записи используют подразделение «Computers», то ввод РМ в домен не гарантируется! Строка не должна быть пустой, если используется функционал удаления учетной записи при удалении фонда РМ. Если строка будет пустой, то учетная запись не будет удалена. Параметр «OU» должен принимать значения вида: «OU=Computers,DC=domain,DC=local», т.е. не должен использоваться Common Name (CN)

Конфигурация ОС Linux при вводе в Альт Домен

Для добавления в Termidesk VDI параметров гостевой ОС на базе GNU/Linux при вводе в Альт Домен следует перейти «Рабочие места - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «Linux Альт Домен».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для гостевой ОС Linux при вводе в Альт Домен).

Таблица 80. Данные для гостевой ОС Linux при вводе в Альт Домен

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС
«Домен»	Доменное имя (DNS) службы каталогов
«Аккаунт»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Идентификатор субъекта, имеющий полномочия по добавлению РМ в домен
«Пароль»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий

Параметр	Описание
«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/msad/»
«OU»	Идентификатор организационной единицы, в которую будут добавлены РМ. Следует учесть, что при вводе гостевой ОС в Альт Домен рекомендуется создавать обособленные подразделения домена, и не создавать учетные записи в подразделении «Computers». Если учетные записи используют подразделение «Computers», то ввод РМ в домен не гарантируется! Строка не должна быть пустой, если используется функционал удаления учетной записи при удалении фонда РМ. Если строка будет пустой, то учетная запись не будет удалена. Параметр «OU» должен принимать значения вида: «OU=Computers,DC=domain,DC=local», т.е. не должен использоваться Common Name (CN)

Конфигурация ОС Linux при использовании автономной машины

Для добавления в Termidesk VDI параметров ОС автономной машины следует перейти «Рабочие места - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «Автономные машины Linux».

Доступность функционала зависит от типа редакции Termidesk VDI.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для ОС Linux при использовании автономной машины).

Таблица 81. Данные для ОС Linux при использовании автономной машины

Параметр	Описание
«Название»	Текстовое наименование параметров ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров ОС

Параметры гостевой ОС Microsoft Windows

Конфигурация ОС Windows без домена

Для добавления в Termidesk VDI параметров гостевой ОС Microsoft Windows без ввода в домен следует перейти «Рабочие места - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «ОС Windows».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для гостевой ОС Microsoft Windows без ввода в домен).

Таблица 82. Данные для гостевой ОС Microsoft Windows без ввода в домен

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС

Конфигурация ОС Windows при вводе в Альт Домен

Для добавления в Termidesk VDI параметров гостевой ОС Microsoft Windows с вводом в Альт Домен следует перейти «Рабочие места - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «Windows Альт Домен».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для гостевой ОС Microsoft Windows при вводе в Альт Домен).

Таблица 83. Данные для гостевой ОС Microsoft Windows при вводе в Альт Домен

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС
«Домен»	Доменное имя (DNS) службы каталогов
«Аккаунт»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Идентификатор субъекта, имеющий полномочия по добавлению РМ в домен
«Пароль»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/msad/»
«OU»	Идентификатор организационной единицы, в которую будут добавлены РМ. Следует учесть, что при вводе гостевой ОС в Альт Домен рекомендуется создавать обособленные подразделения домена, и не создавать учетные записи в подразделении «Computers». Если учетные записи используют подразделение «Computers», то ввод РМ в домен не гарантируется! Строка не должна быть пустой, если используется функционал удаления учетной записи при удалении фонда РМ. Если строка будет пустой, то учетная запись не будет удалена. Параметр «OU» должен принимать значения вида: «OU=Computers,DC=domain,DC=local», т.е. не должен использоваться Common Name (CN)

Для ввода РМ в домен субъект должен иметь как минимум следующие привилегии:

- право на создание и удаление учетных записей;
- право на сброс паролей учетных записей;
- право на ввод РМ в домен.

Конфигурация ОС Windows при вводе в домен MS AD

Для добавления в Termidesk VDI параметров гостевой ОС Microsoft Windows с вводом в домен следует перейти «Рабочие места - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «Windows MS AD DS».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для гостевой ОС Microsoft Windows при вводе в домен MS AD).

Таблица 84. Данные для гостевой ОС Microsoft Windows при вводе в домен MS AD

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС
«Домен»	Доменное имя (DNS) службы каталогов MS AD
«Аккаунт»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Идентификатор субъекта, имеющий полномочия по добавлению РМ в домен
«Пароль»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Набор символов, подтверждающий назначение полномочий
«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/msad/»
«OU»	Идентификатор организационной единицы, в которую будут добавлены РМ. Следует учесть, что при вводе гостевой ОС в домен MS AD рекомендуется создавать обособленные подразделения домена, и не создавать учетные записи в подразделении «Computers». Если учетные записи используют подразделение «Computers», то ввод РМ в домен не гарантируется! Строка не должна быть пустой, если используется функционал удаления учетной записи при удалении фонда РМ. Если строка будет пустой, то учетная запись не будет удалена. Параметр «OU» должен принимать значения вида: «OU=Computers,DC=domain,DC=local», т.е. не должен использоваться Common Name (CN)

Для ввода РМ в домен субъект должен иметь как минимум следующие привилегии:

- право на создание и удаление учетных записей;

- право на сброс паролей учетных записей;
- право на ввод РМ в домен.

Конфигурация ОС Windows при использовании автономной машины

Для добавления в Termidesk VDI параметров ОС автономной машины следует перейти «Рабочие места - Параметры гостевых ОС», далее нажать на экранную кнопку **[Создать]**, из выпадающего списка выбрать «Автономные машины Windows».

Доступность функционала зависит от типа редакции Termidesk VDI.

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для ОС Windows при использовании автономной машины).

Таблица 85. Данные для ОС Windows при использовании автономной машины

Параметр	Описание
«Название»	Текстовое наименование параметров гостевой ОС
«Комментарий»	Информационное сообщение, используемое для описания назначения параметров гостевой ОС

Изменение изображения гостевых ОС

Графические изображения в Termidesk VDI применяются для визуальной идентификации используемых гостевых ОС в фондах РМ.

Для добавления графического изображения следует перейти «Рабочие места - Галерея» и нажать экранную кнопку **[Создать]**.

В окне добавления изображения нужно заполнить наименование добавляемого объекта, а также добавить само изображение, нажав экранную кнопку **[Нажмите для загрузки]**.

Требования к изображению:

- размер: от 16x16 до 256x256 пикселей;
- соотношение сторон: 1:1;
- поддерживаемые форматы: `.ico`, `.jpeg`, `.jpg`, `.png`.

После добавления изображений гостевых ОС в Termidesk VDI пользователь, подключившись к «Универсальному диспетчеру» Termidesk VDI через компонент «Клиент», увидит их в своем интерфейсе (см. рисунок Отображение назначенных изображений в сеансе пользователя).

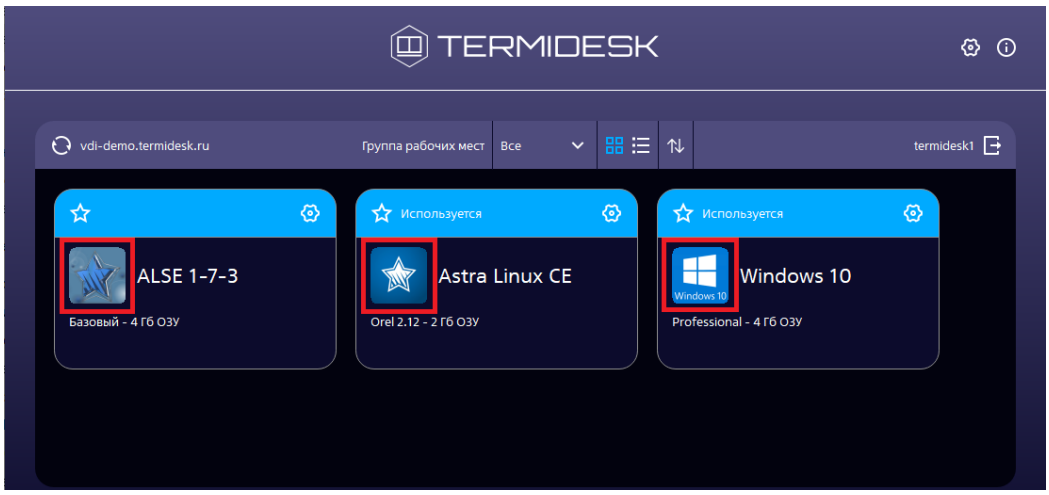


Рисунок 61. Отображение назначенных изображений в сеансе пользователя

Действие при выходе пользователя из ОС

Termidesk VDI поддерживает назначение действий с РМ при выходе пользователя из сессии в политике «Действие при выходе пользователя из ОС (RDP, SPICE, TERA)» (см. подраздел **Политики**).

Совместно с политикой «Действие при выходе пользователя из ОС (RDP, SPICE, TERA)» применяется политика «Удаление рабочего места».

СЕТИ

Общие сведения о сетях в Termidesk

Сети - это IP-адреса или диапазоны IP-адресов пользователей, подключающихся к Termidesk VDI. Сети используются для реализации «белого» или «черного» списка доступа на уровне:

- протокола доставки;
- фонда РМ.

Доступны следующие действия над сетями:

- просмотр списка сетей. Для отображения списка сетей следует перейти «Рабочие места - Сети»;
- создание. Для этого нужно нажать экранную кнопку **[Создать]**;
- редактирование. Для этого нужно пометить сеть и нажать экранную кнопку **[Изменить]**;
- удаление. Для этого нужно пометить сеть и нажать экранную кнопку **[Удалить]**;
- назначение политики для сети. Для этого нужно пометить сеть и нажать экранную кнопку **[Политики]**. Значения по умолчанию наследуются от глобальных политик. Список политик и общее описание по применению политик приведено в подразделе **Политики**;
- назначение тегов для сети. Для этого нужно пометить сеть и нажать экранную кнопку **[Теги]**. Общее описание по применению тегов приведено в подразделе **Общие сведения о тегах**.

Сеть должна быть добавлена в фонд РМ для работы алгоритма выбора значения политики (для учета политик сетей).

Для разрешения ситуаций с порядком применения разного набора политик для объектов используется механизм приоритизации политик (параметр «Приоритет политик»).

Политики сетей заново оцениваются и применяются, когда пользователь подключается к ранее запущенным на РМ сеансам.

Основные параметры списка сетей приведены в таблице (см. таблицу Параметры списка сетей).

Таблица 86. Параметры списка сетей

Параметр	Описание
«Название»	Наименование сети
«Диапазон»	IP-адреса или диапазоны IP-адресов, назначенных для сети
«Используется в фондах»	Характеристика использования сети в каком-либо фонде
«Используется в протоколах доставки»	Характеристика использования сети в каком-либо протоколе доставки
«Приоритет политик»	Приоритет действия политик для сети
«Теги»	Список тегов, назначенных сети. При выборе тега выполняется переход к разделу «Системные параметры – Управление тегами» со списком объектов, которым назначен данный тег

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Добавление сети

Для добавления сети следует перейти «Рабочие места - Сети», нажать экранную кнопку **[Создать]** и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления сети).

Таблица 87. Данные для добавления сети

Параметр	Описание
«Название»	Наименование сети
«Диапазон»	IP-адрес или диапазоны IP-адресов, назначаемые для сети. Может быть указан один IP-адрес или диапазон IP-адресов. Пример: • «192.0.2.1»; • «192.0.2.5/24»; • «192.0.2.2-192.0.2.253»
«Приоритет политик»	Приоритет действия политик для сети. Политики сети применяются только к фондам, к которым добавлена эта сеть. Чем меньше число, тем выше приоритет Пример: IP-адрес пользовательской рабочей станции попадает в диапазоны двух сетей, для каждой из которой задан свой набор политик. В этом случае администратор должен настроить разные приоритеты применения политик для сетей: одной группе задать приоритет выше, другой - ниже.

ПРОФИЛИ ШЛЮЗОВ

Общие сведения о профилях шлюзов

Профиль шлюза - это список параметров, задающих шлюз, который будет использоваться для подключения пользователей. Созданный профиль шлюза может быть указан в настройках протокола доставки.

Для отображения списка профилей шлюзов следует перейти «Рабочие места - Профили шлюзов». Основные параметры списка приведены в таблице (см. таблицу Параметры списка профилей шлюзов).

Отображение списка будет доступно администратору, если у него есть пользовательское разрешение «Просмотр профилей шлюзов».

Таблица 88. Параметры списка профилей шлюзов

Параметр	Описание
«Приоритет»	Приоритет отображения профиля шлюза в настройках протокола доставки
«Название»	Наименование профиля шлюза
«URL шлюза»	Адрес шлюза
«Используется»	Характеристика использования профиля шлюза в каком-либо протоколе доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения профиля шлюза

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Для добавления профиля шлюза следует перейти «Рабочие места - Профили шлюзов» и нажать экранную кнопку **[Создать]**.

Созданные профили шлюзов можно:

- редактировать, для этого нужно пометить его название, а затем нажать экранную кнопку **[Изменить]**;
- удалить, для этого нужно пометить его название, а затем нажать экранную кнопку **[Удалить]**.

Создание, редактирование и удаление будет доступно администратору, если у него есть пользовательское разрешение «Создание профилей шлюзов», «Редактирование профилей шлюзов» и «Удаление профилей шлюзов» соответственно.

Добавление профиля шлюза

Для добавления узла шлюза в список профилей следует перейти «Рабочие места - Профили шлюзов», нажать экранную кнопку **[Создать]**, выбрать «Профиль шлюза» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления профиля шлюза).

Таблица 89. Данные для добавления профиля шлюза

Параметр	Описание
«Название»	Наименование профиля шлюза
«Комментарий»	Информационное сообщение, используемое для описания назначения профиля шлюза
«Приоритет»	Приоритет отображения профиля шлюза в настройках протокола доставки
«URL шлюза»	Адрес узла шлюза, обеспечивающего формирование и поддержание соединения, заданный в формате: • `ws(s)://<IP-адрес_или_доменное_имя>:<порт>`; • или `ws(s)://<IP-адрес_или_доменное_имя>/<путь>`. Протокол WS (WebSocket) используется, если шлюз не настроен на защищенное соединение. Протокол WSS используется, если выполняется защищенное подключение к шлюзу. Пример: «wss://termidesk.loc/websockify»
«Время жизни wsp-токена, с»	Время жизни (в секундах) токена, используемого для взаимодействия «Универсального диспетчера» и шлюза. Возможные значения: диапазон значений от 0 до 960. Значение «0» делает время жизни токена бесконечным. Рекомендуемое значение: «70». Значение по умолчанию: «70»

Проверить корректность указанных параметров можно при помощи экранной кнопки **[Тест]**. Для сохранения параметров конфигурации необходимо использовать экранную кнопку **[Сохранить]**.

ПРОТОКОЛЫ ДОСТАВКИ

Общие сведения о протоколах доставки

Протокол доставки – это поддерживаемый в Termidesk VDI протокол удаленного доступа к РМ. Протоколы доставки обеспечивают подключение к ВРМ, а также к терминальным сессиям и приложениям, и могут выполнять доставку РМ как напрямую, так и через компонент «Шлюз».

Termidesk VDI поддерживает следующие протоколы удаленного доступа:

Доступность функционала зависит от типа редакции Termidesk VDI.

- SPICE, поддерживается, в том числе, при доставке ВРМ через HTML5-клиент;
- TERA, поддерживается, в том числе, при доставке ВРМ через HTML5-клиент;
- RDP;
- Loudplay.

Сравнительная таблица функциональных возможностей протоколов доставки приведена в подразделе характеристик сайта документации Termidesk VDI: **Функциональные возможности протоколов**.

Перечень протестированных и поддерживаемых комбинаций протоколов удаленного доступа и гостевых ОС представлен в таблице (см. таблицу Список поддерживаемых протоколов и ОС).

В таблице приняты обозначения:

- MS RDSH - терминальный сервер MS RDSH;
- STAL - терминальный сервер с установленным компонентом «Сервер терминалов Astra Linux»;
- ALSE - ОС Astra Linux Special Edition.

Версии ОС определяются поддерживаемыми ОС компонентов Termidesk VDI, установленными в них:

- для ВРМ и автономных машин - компонентом «Агент виртуального рабочего места»;
- для терминальных серверов с ОС Astra Linux Special Edition - компонентом «Сервер терминалов Astra Linux»;
- для терминальных серверов MS RDSH - компонентом «Сессионный агент».

Таблица 90. Список поддерживаемых протоколов и ОС

ОС	TERA	RDP	SPICE	Loudplay
STAL		□		
MS RDSH		□		
Microsoft Windows	□	□	□	□
ALSE	□		□	□
РЕД ОС			□	

Для отображения списка добавленных протоколов доставки следует перейти «Рабочие

места - Протоколы доставки». Основные параметры списка приведены в таблице (см. таблицу Параметры списка протоколов доставки).

Для добавления протокола доставки следует нажать на экранную кнопку **[Создать]** и выбрать из выпадающего списка поддерживаемый протокол.

Доступны следующие действия над протоколами доставки:

- редактирование. Для этого нужно пометить протокол доставки и нажать на экранную кнопку **[Изменить]**;
- удаление. Для этого нужно пометить протокол доставки и нажать на экранную кнопку **[Удалить]**;
- назначение тегов протоколу доставки. Для этого нужно пометить протокол и нажать экранную кнопку **[Теги]**. Общее описание по применению тегов приведено в подразделе **Общие сведения о тегах**.

Перед удалением протокола доставки следует убедиться, что он не является единственным назначенным протоколом для фонда РМ.

Таблица 91. Параметры списка протоколов доставки

Параметр	Описание
«Приоритет»	Приоритет отображения в списке протоколов доставки для пользователя
«Название»	Текстовое наименование протокола доставки в Termidesk
«Протокол»	Тип протокола доставки
«Используется»	Характеристика использования протокола доставки в каком-либо фонде
«Профиль шлюза»	Профиль, использующийся для протокола доставки при подключении через «Шлюз»
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Теги»	Список тегов, назначенных протоколу доставки. При выборе тега выполняется переход к разделу «Системные параметры – Управление тегами» со списком объектов, которым назначен данный тег

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы;
- экспорт записей таблицы в `csv`-файл. Можно выгрузить:
  - все записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт всех]**;
  - выбранные записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт выбранных]**.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Протокол доставки RDP

Прямое подключение по протоколу RDP

Для добавления прямого подключения по протоколу RDP следует перейти «Рабочие места - Протоколы доставки», нажать на экранную кнопку **[Создать]**, выбрать «RDP» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления прямого подключения по протоколу RDP).

В Termidesk VDI версии 7.0 некоторые устаревшие и перекрывающиеся политиками параметры протокола доставки были удалены.

Таблица 92. Данные для добавления прямого подключения по протоколу RDP

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Приоритет отображения в списке протоколов доставки для пользователя
«Порт»	Выбор порта для подключения. По умолчанию используется порт 3389
«Поддержка CredSSP»	Использовать технологию единого входа с помощью услуг безопасности Credential Security Service Provider

Параметр	Описание
«Параметры принтера»	Указать конфигурацию перенаправляемого принтера
«Параметры смарт-карты»	Указать конфигурацию смарт-карт
«Доступ из сетей»	Ограничение доступа для указанного диапазона сетей. Возможные значения: • «Да» - протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа); • «Нет» - протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к ВРМ. Указанные диапазоны должны быть созданы в «Рабочие места - Сети»
«Разрешенные устройства»	Идентификаторы ОС, которые могут быть использованы при подключении по протоколу RDP к ВРМ

Для проверки правильности заполнения формы подключения можно использовать экранную кнопку **[Тест]**.

Подключение через компонент «Шлюз» по протоколу RDP

Для добавления подключения по протоколу RDP через компонент «Шлюз» следует перейти «Рабочие места - Протоколы доставки», нажать на экранную кнопку **[Создать]**, выбрать «RDP через шлюз» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления подключения по протоколу RDP через «Шлюз»).

Начиная с Termidesk VDI версии 6.1 добавлен объект «Профиль шлюза». При обновлении с более старых версий (ранее не поддерживавших «Профиль шлюза») потребуется создать объект «Профиль шлюза» и указать его в протоколе доставки вручную.

В Termidesk VDI версии 7.0 некоторые устаревшие и перекрывающиеся политиками параметры протокола доставки были удалены.

Таблица 93. Данные для добавления подключения по протоколу RDP через «Шлюз»

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Приоритет отображения в списке протоколов доставки для пользователя
«Профиль шлюза»	Профиль, который будет использоваться для подключения через «Шлюз». Профиль должен быть предварительно добавлен. Параметр обязателен для заполнения, если требуется подключение через «Шлюз»
«Порт»	Выбор порта для подключения. По умолчанию используется порт 3389
«Поддержка CredSSP»	Использовать технологию единого входа с помощью услуг безопасности Credential Security Service Provider

Параметр	Описание
«Параметры принтера»	Указать конфигурацию перенаправляемого принтера
«Параметры смарт-карты»	Указать конфигурацию смарт-карт
«Доступ из сетей»	Ограничение доступа для указанного диапазона сетей. Возможные значения: • «Да» - протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа); • «Нет» - протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к ВРМ. Указанные диапазоны должны быть созданы в «Рабочие места - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении по протоколу RDP к ВРМ

Для проверки правильности заполнения формы подключения можно использовать экранную кнопку **[Тест]**.

Подключение по протоколу RDP для доступа к ресурсам сервера терминалов

Для добавления подключения для доступа к терминальному серверу администратору Termidesk VDI необходимо перейти «Рабочие места - Протоколы доставки», нажать на экранную кнопку **[Создать]**, выбрать «RDP (терминальный доступ)».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления подключения к серверу терминалов).

Начиная с Termidesk VDI версии 6.1 добавлен объект «Профиль шлюза». При обновлении с более старых версий (ранее не поддерживавших «Профиль шлюза») потребуется создать объект «Профиль шлюза» и указать его в протоколе доставки вручную.

В Termidesk VDI версии 7.0 некоторые устаревшие и перекрывающиеся политиками параметры протокола доставки были удалены.

Таблица 94. Данные для добавления подключения к серверу терминалов

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Преимущество использования протокола доставки в фонде ВРМ

Параметр	Описание
«Профиль шлюза»	Профиль, который будет использоваться для подключения через «Шлюз». Профиль должен быть предварительно добавлен. Параметр обязателен для заполнения, если требуется подключение через «Шлюз» Работа с MS RDS поддерживается как в варианте подключения через «Шлюз» Termidesk VDI, так и без него, если: • либо терминальный сервер MS RDS развернут без полнофункциональной инфраструктуры через поставщик ресурсов Метапоставщик; • либо развернута полнофункциональная инфраструктура MS RDS, при этом роль «Remote Desktop Gateway» развернута, но не используется. Каждая нода MS RDS должна быть подключена как отдельный поставщик ресурсов «Сервер терминалов» (то есть, коллекция MS RDS находится на том сервере, к которому идет подключение).
«Порт»	Выбор порта для подключения. По умолчанию используется порт 3389
«Поддержка CredSSP»	Использовать технологию единого входа с помощью услуг безопасности Credential Security Service Provider
«Параметры смарт-карты»	Указать конфигурацию смарт-карт
«Все принтеры»	Выполнить перенаправление всех устройств печати по протоколу RDP. При выключенном параметре «Разрешить принтеры» данный параметр игнорируется
«Доступ из сетей»	При выборе значения «Да» протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к ВРМ. Указанные диапазоны должны быть созданы в «Рабочие места - Сети»
«Разрешенные устройства»	Идентификаторы ОС, которые могут быть использованы при подключении по протоколу RDP к ВРМ

Для проверки правильности заполнения формы подключения можно использовать экранную кнопку **[Тест]**.

Протокол доставки SPICE

Для подключения пользователя по протоколу SPICE имена узлов платформы виртуализации должны корректно разрешаться в IP-адреса этих узлов. Подключение по протоколу SPICE происходит к гипервизору платформы виртуализации.

Для подключения по протоколу SPICE нужно:

- на узлах платформы виртуализации включить оптимизацию для протокола SPICE;
- на пользовательскую рабочую станцию установить ПО Termidesk Viewer.

Для добавления подключения по протоколу SPICE следует перейти «Рабочие места - Протоколы доставки», нажать на экранную кнопку **[Создать]**, выбрать «SPICE» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления подключения по SPICE).

Начиная с Termidesk VDI версии 6.1 добавлен объект «Профиль шлюза». При обновлении с более старых версий (ранее не поддерживавших «Профиль шлюза») потребуется создать объект «Профиль шлюза» и указать его в протоколе доставки вручную.

Таблица 95. Данные для добавления подключения по SPICE

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Приоритет отображения в списке протоколов доставки для пользователя
«Профиль шлюза»	Профиль, который будет использоваться для подключения через «Шлюз». Профиль должен быть предварительно добавлен. Параметр обязателен для заполнения, если требуется подключение через «Шлюз»
«Время ожидания соединения, с»	Время ожидания (в секундах) отклика шлюза
«Сертификат»	Информация о публичном ключе для доступа к платформе виртуализации (опционально)
«Доступ из сетей»	При выборе значения «Да» протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к ВРМ. Указанные диапазоны должны быть созданы в «Рабочие места - Сети»
«Разрешенные устройства»	Идентификаторы ОС, которые могут быть использованы при подключении по протоколу SPICE к ВРМ

Для проверки правильности заполнения формы подключения можно использовать экранную кнопку **[Тест]**.

Протокол доставки TERA

Подключение по протоколу TERA

Протокол TERA обеспечивает прямое подключение к гостевой ОС РМ независимо от используемой платформы виртуализации. TERA поддерживает безопасную аутентификацию пользователя по логину и паролю, передаваемого в преобразованном виде. Для безопасной аутентификации по умолчанию используются самоподписанные сертификаты.

Для подключения по протоколу TERA нужно:

- в гостевой ОС установить TERA для выбранного варианта использования (см. подразделы **ОС Astra Linux Special Edition**, **ОС Microsoft Windows** документа

СЛЕТ.10001-01 90 09 «Руководство администратора. Настройка компонента TERA»);

- на пользовательскую рабочую станцию установить ПО Termidesk Client.

Для добавления подключения по протоколу TERA следует перейти «Рабочие места - Протоколы доставки», нажать на экранную кнопку **[Создать]**, выбрать «TERA» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления подключения по TERA).

Начиная с Termidesk VDI версии 6.1 добавлен объект «Профиль шлюза». При обновлении с более старых версий (ранее не поддерживавших «Профиль шлюза») потребуется создать объект «Профиль шлюза» и указать его в протоколе доставки вручную.

Для проверки правильности заполнения формы подключения можно использовать экранную кнопку **[Тест]**.

Таблица 96. Данные для добавления подключения по TERA

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Приоритет отображения в списке протоколов доставки для пользователя
«UDP порт шлюза»	UDP-порт, заданный на шлюзе для TERA. Значение по умолчанию: «5900»
«Порт»	Порт для подключения к TERA. При использовании UDP в этом параметре указывается порт, заданный в настройках ПО tera-router (по умолчанию - 6000). Значение по умолчанию: «5900»
«Транспорт»	Выбор сетевого протокола, использующегося для подключения к TERA. Возможные значения: • «TCP и UDP» - для подключения будут использоваться протоколы TCP и UDP; • «TCP» - для подключения будет использоваться протокол TCP. Подключение по протоколу UDP рекомендуется выполнять напрямую, работа через шлюз не гарантируется. Значение по умолчанию: «TCP и UDP»

Параметр	Описание

«Аутентификация»	Управление режимом использования безопасной аутентификации пользователя (Simple Authentication and Security Layer, SASL).
	
	Возможные значения:
	
	• «Да» - при подключении по TERA используется механизм аутентификации SASL. При этом в параметре «Режим подключения» должно быть задано одно из следующих значений:
	  «Прямой режим с TLS»;
	  «Через шлюз с TLS». Профиль шлюза должен быть указан в параметре «Профиль шлюза»;
	  «Безопасный через шлюз с TLS». Профиль шлюза должен быть указан в параметре «Профиль шлюза».
	
	При использовании значения «Да» следует учитывать, что конфигурация TERA и гостевой ОС РМ должна быть настроена на использование SASL.
	
	• «Нет» - при подключении по TERA механизм аутентификации SASL не используется.
	
	Значение по умолчанию: «Нет»

«Профиль шлюза»	Профиль, который будет использоваться для подключения через шлюз. Профиль должен быть предварительно добавлен. Если требуется подключение через шлюз: • требуется заполнить профиль шлюза; • выбрать значение, предполагающее использование шлюза, в параметре «Режим подключения»

Параметр	Описание

«Режим подключения»	Выбор режима подключения к РМ с TERA.
	
	Возможные значения:
	
	• «Прямой режим» - подключение пользователя к РМ произойдет напрямую по протоколу TCP без преобразования данных. Рекомендуется использовать режим в случае, если пользовательская рабочая станция и РМ находятся в одной локальной сети. Профиль шлюза не должен указываться в параметре «Профиль шлюза»;
	• «Прямой режим с TLS» - подключение пользователя к РМ произойдет напрямую по протоколу TCP, но с преобразованием данных для их защиты. Рекомендуется использовать режим в случае, если пользовательская рабочая станция и РМ находятся в одной локальной сети, при этом требуется обеспечить безопасность передаваемых данных. При этом:
	  конфигурация TERA должна быть настроена на использование TLS;
	  профиль шлюза не должен указываться в параметре «Профиль шлюза»;
	• «Через шлюз» - подключение пользователя к РМ произойдет через шлюз по протоколу TCP с использованием WebSocket (WS). Рекомендуется использовать режим в случае, если РМ доступны только через шлюз и не требуется подключение с высоким уровнем безопасности. Профиль шлюза должен быть указан в параметре «Профиль шлюза»;
	• «Через шлюз с TLS» - подключение пользователя к РМ произойдет через шлюз по протоколу TCP через WS с преобразованием данных для их защиты. Рекомендуется использовать режим в случае, если РМ доступны только через шлюз и требуется обеспечить безопасность передаваемых данных. Преобразование данных через TLS происходит от шлюза до РМ. При этом:
	  конфигурация TERA должна быть настроена на использование TLS;
	  профиль шлюза должен быть указан в параметре «Профиль шлюза»;
	• «Безопасный через шлюз» - подключение пользователя к РМ произойдет через шлюз по протоколу TCP через WebSocket Secure (WSS). Рекомендуется использовать режим в случае, если РМ доступны только через шлюз и требуется обеспечить защищенное соединение только до шлюза. При этом:
	  конфигурация «Шлюза» должна быть настроена на использование TLS и WSS;
	  профиль шлюза должен быть указан в параметре «Профиль шлюза».
	• «Безопасный через шлюз с TLS» - подключение пользователя к РМ произойдет через шлюз по протоколу TCP через WSS с преобразованием данных для их защиты. Рекомендуется использовать этот режим в случае, если РМ доступны только через шлюз и требуется подключение с максимальным уровнем безопасности. Преобразование данных через TLS происходит как от пользователя к шлюзу, так и от шлюза до РМ. При этом:
	  конфигурация TERA и «Шлюза» должна быть настроена на использование TLS. «Шлюз» должен быть настроен на использование WSS;
	  профиль шлюза должен быть указан в параметре «Профиль шлюза».
	
	Значение по умолчанию: «Прямой режим с TLS»

Параметр	Описание
«Пароль»	Набор символов, подтверждающий подключение. Заполнение параметра зависит от настроек протокола TERA: • если в конфигурационном файле TERA задано использование пароля для подключения, то он должен быть задан в параметрах протокола доставки для успешного подключения пользователя к РМ; • если в конфигурационном файле TERA отключено использование пароля для подключения, то параметр в протоколе доставки можно не заполнять
«Приоритизация»	Управление режимом приоритизации каналов TERA. Возможные значения: • «Да» - при подключении пользователя по TERA будут использоваться приоритеты групп каналов TERA (см. подраздел **Группы каналов протокола TERA**); • «Нет» - при подключении пользователя по TERA приоритеты групп каналов TERA не используются. Значение по умолчанию: «Нет»
«Доступ из сетей»	При выборе значения «Да» протокол доставки будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол доставки будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола доставки для подключения к РМ. Указанные диапазоны должны быть созданы в «Рабочие места - Сети»
«Разрешенные устройства»	Идентификаторы ОС, которые могут быть использованы при подключении к РМ

Группы каналов протокола TERA

Протокол TERA поддерживает разделение каналов на несколько сетевых потоков и их приоритизацию на основе приоритетов сокетов для управления очередями пакетов (см. подраздел **Разделение каналов и их приоритизация в TERA** документа СЛЕТ.10001-01 90 09 «Руководство администратора. Настройка компонента TERA»).

Для назначения приоритетов каналам следует перейти «Рабочие места - Протоколы доставки», нажать на наименование протокола доставки TERA и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для заполнения групп каналов TERA).

Приоритизация будет применяться, если в свойствах протокола доставки активирован параметр «Приоритизация». Если параметр не активирован, то приоритизация отключена, все каналы будут иметь приоритет «0».

Если при обновлении с Termidesk VDI предыдущей версии каналы и приоритеты недоступны, то следует пересоздать протокол доставки, если он был создан ранее до обновления.

Таблица 97. Данные для заполнения групп каналов TERA

Параметр	Описание
«Приоритет»	Номер приоритета TERA. Номеру приоритета TERA соответствует текстовое наименование, задаваемое в параметре «Группа». Группировка приоритетов выполнена по следующему принципу: • «0» - соответствует группе канала «Background»; • «1» - соответствует группе канала «Bulk-Transfer»; • «2» - соответствует группе канала «Interactive»; • «3» - соответствует группе канала «Real-Time stream». Изменение номера приоритета доступно через изменение «Группы»: при изменении группы меняется и приоритет
«Каналы»	Тип канала, которому назначается приоритет: • «playback» - канал воспроизведения. Обеспечивает вывод звука с РМ на пользовательскую рабочую станцию; • «record» - канал записи. Обеспечивает аудиовход от пользовательской рабочей станции к РМ; • «display» - канал отображения. Обеспечивает обновление экрана и операции отрисовки; • «inputs» - канал ввода. Обеспечивает ввод с клавиатуры и мыши с пользовательской рабочей станции в РМ; • «cursor» - канал курсора. Обеспечивает обновление формы и положения курсора; • «webdav» - канал webdav. Обеспечивает перенаправление каталогов с пользовательской рабочей станции в РМ; • «smartcard» - канал смарт-карт. Обеспечивает перенаправление смарт-карт для аутентификации; • «usbredir» - канал USB-устройств. Обеспечивает перенаправление USB-устройств с пользовательской рабочей станции в РМ; • «port» - канал портов. Обеспечивает перенаправление устройств - веб-камер, принтеров. Дополнительно используется для взаимодействия по API (SDK TERA)

Параметр	Описание
«Группа»	Наименование группы каналов, соответствующей номеру приоритета TERA. Возможные значения: Очередь пакетов с более высоким приоритетом будет обработана раньше. • «Background» - фоновая передача данных, соответствует номеру приоритета «0». Приоритет обработки такого трафика - низкий. Используется для фоновых виртуальных каналов, например, печати; • «Bulk-Transfer» - массовая передача данных, соответствует номеру приоритета «1». Приоритет обработки такого трафика - средний. Используется для массовых виртуальных каналов, например, передачи файлов, перенаправления каталогов,; • «Interactive» - передача интерактивных данных, соответствует номеру приоритета «2». Приоритет обработки такого трафика - высокий. Используется для интерактивных каналов, например, графики, клавиатуры и мыши; • «Real-Time stream» - передача данных в реальном времени, соответствует номеру приоритета «3». Приоритет обработки такого трафика - самый высокий. Используется для каналов реального времени, например, аудио, видео и веб-камеры

Протокол доставки HTML5

Протокол доставки HTML5 SPICE

Протокол доставки HTML5 SPICE позволяет получить пользователю РМ по протоколу SPICE и работать с ним из веб-браузера, не устанавливая компонент «Клиент» на пользовательскую рабочую станцию. Подключение по протоколу SPICE происходит к гипервизору платформы виртуализации.

Для корректной работы протокола доставки HTML5 SPICE рекомендуется использовать компонент «Шлюз» версии 0.7.0 и выше.

Для добавления протокола доставки следует перейти «Рабочие места - Протоколы доставки», нажать на экранную кнопку **[Создать]**, выбрать «HTML5 SPICE» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления протокола HTML5).

Начиная с Termidesk VDI версии 6.1 добавлен объект «Профиль шлюза». При обновлении с более старых версий (ранее не поддерживавших «Профиль шлюза») потребуется создать объект «Профиль шлюза» и указать его в протоколе доставки вручную.

Таблица 98. Данные для добавления протокола HTML5

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Приоритет отображения в списке протоколов доставки для пользователя

Параметр	Описание
«Профиль шлюза»	Профиль, который будет использоваться для подключения через «Шлюз». Профиль должен быть предварительно добавлен. Параметр обязателен для заполнения. Для работы протокола доставки HTML5 SPICE по защищенному соединению со «Шлюзом» необходимо убедиться, что: • «Шлюз» настроен для подключения по защищенному соединению; • на узле «Шлюза» установлены валидные сертификаты (непосредственно сертификат SSL и корневой сертификат к нему)
«Время ожидания соединения, с»	Время ожидания (в секундах) отклика шлюза
«Доступ из сетей»	При выборе значения «Да» протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к РМ. Указанные диапазоны должны быть созданы в «Рабочие места - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении к РМ

Для проверки правильности заполнения формы подключения можно использовать экранную кнопку **[Тест]**.

Протокол доставки HTML5 TERA

Протокол доставки HTML5 TERA позволяет получить пользователю РМ по протоколу TERA и работать с ним из веб-браузера, не устанавливая компонент «Клиент» на пользовательскую рабочую станцию. Подключение по протоколу TERA происходит непосредственно к ВМ, обращением на IP-адрес или по имени узла (`hostname`).

Для корректной работы протокола доставки HTML5 TERA рекомендуется использовать компонент «Шлюз» версии 0.7.0 и выше.

Для добавления протокола доставки следует перейти «Рабочие места - Протоколы доставки», нажать на экранную кнопку **[Создать]**, выбрать «HTML5 TERA» и заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления протокола HTML5 TERA).

Начиная с Termidesk VDI версии 6.1 добавлен объект «Профиль шлюза». При обновлении с более старых версий (ранее не поддерживавших «Профиль шлюза») потребуется создать объект «Профиль шлюза» и указать его в протоколе доставки вручную.

Таблица 99. Данные для добавления протокола HTML5 TERA

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки

Параметр	Описание
«Приоритет»	Приоритет отображения в списке протоколов доставки для пользователя
«Профиль шлюза»	Профиль, который будет использоваться для подключения через «Шлюз». Профиль должен быть предварительно добавлен. Параметр обязателен для заполнения. Для работы протокола доставки HTML5 TERA по защищенному соединению со «Шлюзом» необходимо убедиться, что: • «Шлюз» настроен на подключение по защищенному соединению; • на узле «Шлюза» установлены валидные сертификаты (непосредственно сертификат SSL и корневой сертификат к нему).
«Время ожидания соединения, с»	Время ожидания (в секундах) отклика «Шлюза»
«Порт»	Порт подключения к TERA, заданный в настройках протокола
«Использовать TLS»	Управление режимом использования протокола TLS. Следует включить параметр, если используется защищенное подключение по протоколу TERA и параметры протокола настроены для него
«Пароль»	Пароль доступа к подключению, заданный в настройках протокола
«Доступ из сетей»	При выборе значения «Да» протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к РМ. Указанные диапазоны должны быть созданы в «Рабочие места - Сети»
«Разрешенные устройства»	Указать идентификаторы ОС, которые могут быть использованы при подключении к РМ

Для проверки правильности заполнения формы подключения можно использовать экранную кнопку **[Тест]**.

Протокол доставки Loudplay

Прямое подключение по протоколу Loudplay

Для подключения к РМ по протоколу доставки Loudplay нужно:

- на пользовательскую рабочую станцию дополнительно установить ПО LoudPlay-client, которое не входит в состав Termidesk VDI;
- в ОС РМ дополнительно установить серверные драйверы NVIDIA и сервер Loudplay.

Для возможности добавления протокола доставки Loudplay нужно включить экспериментальный параметр `experimental.loudplay.transports.enabled`. Процесс активации протокола доставки и параметры, доступные для его настройки, приведены в подразделе **Управление экспериментальными параметрами Termidesk VDI**.

После включения экспериментального параметра перейти в «Рабочие места - Протоколы доставки», затем нажать на экранную кнопку **[Создать]** и выбрать из выпадающего списка «Loudplay [экспериментальный]».

Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления прямого подключения по протоколу Loudplay).

Документация по настройкам протокола Loudplay доступна на официальном сайте разработчика: https://portal.vdi.loudplay.ru/. Конфигурация серверной части протокола доступна по ссылке: https://portal.vdi.loudplay.ru/docs/a/51-conf-reference.

Таблица 100. Данные для добавления прямого подключения по протоколу Loudplay

Параметр	Описание
«Название»	Текстовое наименование протокола доставки
«Комментарий»	Информационное сообщение, используемое для описания назначения протокола доставки
«Приоритет»	Приоритет отображения в списке протоколов доставки для пользователя
«Протокол передачи видео»	Выбор протокола для передачи видеопотока. Возможные значения: • «TCP» - передача видеопотока происходит по протоколу TCP; • «UDP» - передача видеопотока происходит по протоколу UDP. Значение по умолчанию: «TCP»
«Технология захвата»	Выбор технологии захвата изображения. Описание по используемым технологиям доступно на официальном сайте разработчика: https://portal.vdi.loudplay.ru/docs/a/51-conf-reference#heading-10. Возможные значения: • «FFmpeg DDA» - программный метод захвата; • «DDA» - аппаратный метод захвата; • «AMD DDA» - аппаратный метод захвата AMD; • «NVFBC» - аппаратный метод захвата NVIDIA. Значение по умолчанию: «FFmpeg DDA»
«Уровень логирования клиента LP»	Выбор категории сообщений, которые будут записываться в журнал клиента Loudplay. Возможные значения: • «Информационный»; • «Отладочный»; • «Предупреждения»; • «Критические ошибки»; • «Трассировка». Значение по умолчанию: «Отладочный»

Параметр	Описание
«Уровень журналирования модуля проброса USB»	Выбор категории сообщений, которые будут записываться в журнал клиента Loudplay при перенаправлении USB-устройств. Возможные значения: • «Информационный»; • «Отладочный». Значение по умолчанию: «INFO»
«Максимальная частота кадров видео»	Параметр позволяет задать максимально возможную частоту смены кадров (в секунду) видеопотока. Диапазон значений: от 1 до 120. Значение по умолчанию: «30»
«Скорость видеопотока (Kbit/s)»	Параметр позволяет задать максимально возможную скорость видеопотока (Kbit/s). Диапазон значений: от 50 до 100000. Значение по умолчанию: «5000»
«Автоматическое изменение скорости видеопотока»	Управление автоматическим изменением скорости видеопотока. Возможные значения: • «Да» - разрешить автоматическое изменение скорости видеопотока; • «Нет» - запретить автоматическое изменение скорости видеопотока
«Аппаратное ускорение»	Использование вычислительных ресурсов графического процессора (GPU) для обработки видеопотока. Возможные значения: • «Да» - разрешить использование вычислительных ресурсов GPU; • «Нет» - запретить использование вычислительных ресурсов GPU
«Выбор монитора на сервере»	Выбор приоритетного монитора для подключения в многомониторной конфигурации сервера. Возможные значения: • «0» - вывод изображения на первый монитор; • «1» - вывод изображения на второй монитор. Значение по умолчанию: «0»
«Выбор монитора пользовательского ПК»	Выбор приоритетного монитора на пользовательской рабочей станции для отображения клиента Loudplay. Возможные значения: • «0» - вывод изображения на первый монитор; • «1» - вывод изображения на второй монитор. Значение по умолчанию: «0»

Параметр	Описание
«Протокол передачи сигналов клавиатуры и мыши»	Выбор протокола для передачи сигналов клавиатуры и мыши. Возможные значения: • «TCP» - передача сигналов клавиатуры и мыши происходит по протоколу TCP; • «UDP» - передача сигналов сигналов клавиатуры и мыши происходит по протоколу UDP. Значение по умолчанию: «UDP»
«Помехоустойчивое кодирование»	Использование режима помехоустойчивого кодирования. При использовании значения «UDP» в параметре «Протокол передачи видео» режим помехоустойчивого кодирования обеспечивает непрерывную передачу видеоизображения на каналах с потерями до 30%. Возможные значения: • «Да» - разрешить использование помехоустойчивого кодирования; • «Нет» - запретить использование помехоустойчивого кодирования
«Доступ из сетей»	При выборе значения «Да» протокол будет разрешен только для перечисленных в параметре «Сети» диапазонов сетей (реализация «белого» списка доступа). При выборе значения «Нет» протокол будет запрещен для перечисленных в параметре «Сети» диапазонов сетей (реализация «черного» списка доступа)
«Сети»	Диапазон сетевых адресов, из которых будет разрешено или запрещено использование протокола для подключения к РМ. Указанные диапазоны должны быть созданы в «Рабочие места - Сети»
«Разрешенные устройства»	Идентификаторы ОС, которые могут быть использованы при подключении по протоколу Loudplay к РМ

Подключение через компонент «Шлюз» по протоколу Loudplay

Работа с протоколом Loudplay поддерживается только при прямом подключении.

ПОЛИТИКИ

Общие сведения о политиках

Политики - это набор правил и настроек, определяющих взаимодействие компонентов Termidesk VDI. Основное назначение политик - централизованное управление поведением Termidesk VDI для настройки доступа и использования ресурсов пользователями РМ.

Типы политик в Termidesk VDI и их иерархия (каждый последующий уровень переопределяет настройки предыдущего):

- глобальные политики - применяются ко всем фондам РМ и устанавливают общие настройки;
- политики фонда - устанавливают индивидуальные настройки для конкретного фонда РМ;
- политики группы - устанавливают индивидуальные настройки для конкретной группы

пользователей домена аутентификации;

- политики сетей - устанавливают индивидуальные настройки для конкретной сети.

Сеть должна быть добавлена в фонд РМ для работы алгоритма выбора значения политики (для учета политик сетей).

Политики сетей заново оцениваются и применяются, когда пользователь подключается к ранее запущенным на РМ сеансам.

Для разрешения ситуаций с порядком применения разного набора политик для объектов используется механизм приоритизации политик. Приоритизация политик осуществляется для:

- политик группы;
- политик сетей.

Пример: пользователь состоит в двух группах домена аутентификации, для каждой из которой задан свой набор политик. В этом случае администратор должен настроить разные приоритеты применения политик для групп пользователя: одной группе задать приоритет выше, другой - ниже.

Алгоритм выбора значения результирующей политики приведен на рисунке (см. рисунок Алгоритм выбора значения политики).

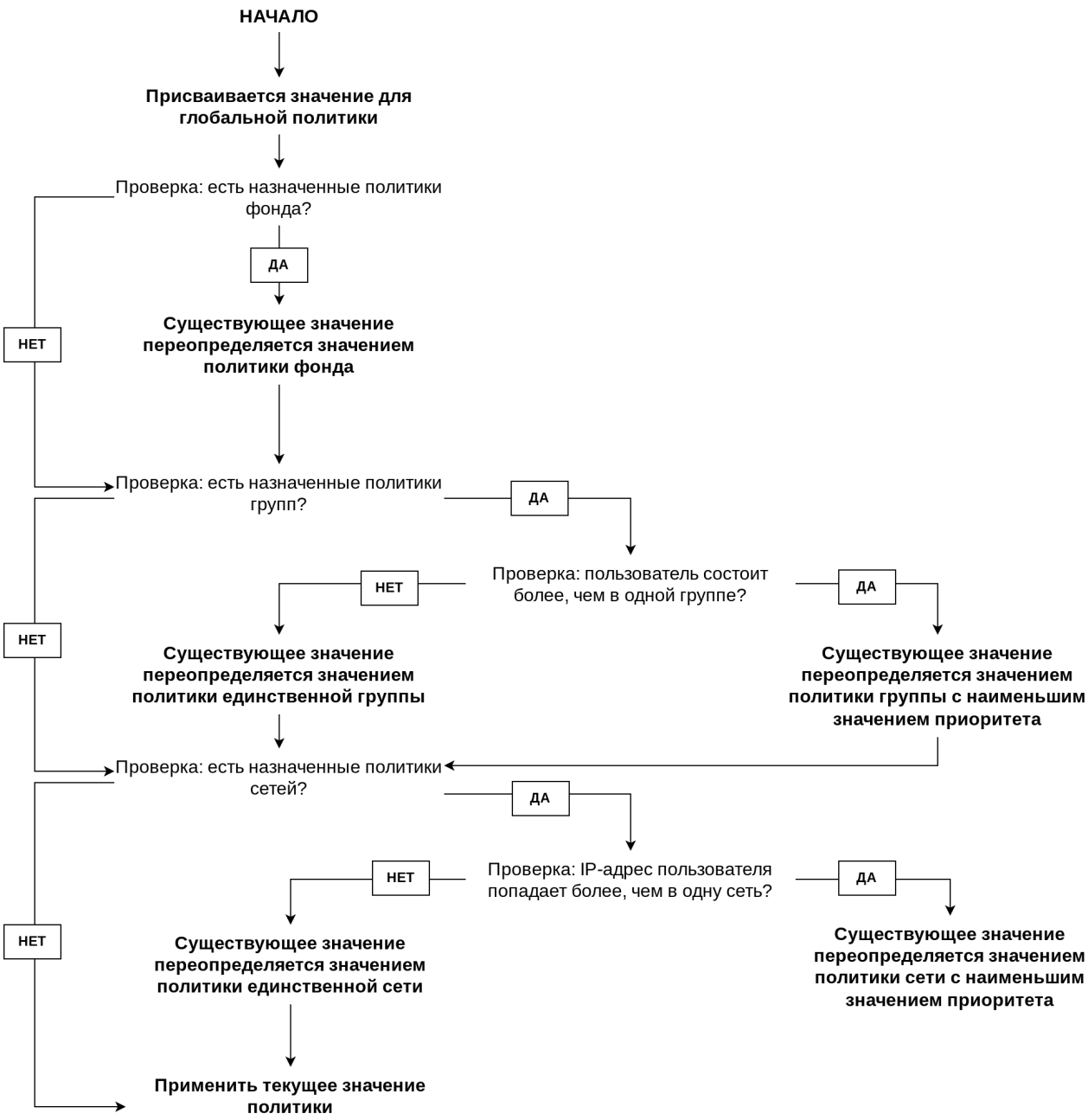


Рисунок 62. Алгоритм выбора значения политики

Список политик

Список глобальных политик представлен в таблице (см. таблицу Перечень доступных политик).

> Политики фонда РМ и групповые политики контроллера домена MS AD управляют одними и теми же ключами реестра. Поэтому рекомендуется использовать либо политики фермы Termidesk VDI, либо политики контроллера домена MS AD (но не из двух источников сразу). Для сохранения возможности управления параметрами подключения средствами контроллера домена MS AD следует назначать политике фонда РМ значение «Не задано».

Поддерживается:

- поиск записей по таблице;

- изменение внешнего вида таблицы;
- экспорт записей таблицы в `csv`-файл. Можно выгрузить:
  - все записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт всех]**;
  - выбранные записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт выбранных]**.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Таблица 101. Перечень доступных политик

Название политики	Тип политики	Описание
«UDP транспорт (TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление использованием транспортного протокола для протокола удаленного доступа TERA. Возможные значения: • «Не задано»; • «Использовать как UDP, так и TCP» (по умолчанию); • «Использовать только TCP»; • «Использовать либо UDP, либо TCP»

Название политики	Тип политики	Описание
«Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Политика определяет, должен ли пользователь вводить логин и пароль в гостевой ОС РМ (в ОС должна быть выполнена настройка SSO). Время ожидания (в секундах) для запуска ПО Termidesk Viewer при использовании технологии единого входа настраивается через системный параметр «Таймаут SSO, с» (см. подраздел **Общие системные параметры Termidesk VDI**). Политика не применяется к протоколу RDP. Автоматический вход включается для RDP при использовании хотя бы одного из условий: • использование функционала PKINIT (аутентификация по смарт-карте) в свойствах домена аутентификации; • использование в политике «Аутентификация на уровне сети (RDP)» значения «NLA» или «TLS». В целях обеспечения информационной безопасности политику необходимо выключить при подключении по протоколу TERA к физической машине (ПО x11tera): переподключения ПО Termidesk Viewer могут сопровождаться задержкой блокировки экрана физической машины, вследствие чего содержимое рабочего стола становится кратковременно доступным для визуального наблюдения. Применимость: • ВРМ (SPICE, TERA); • автономные машины (RDP, TERA). Возможные значения: • «Выключен» (по умолчанию) - учетные данные будут запрашиваться; • «Включен» - запрос учетных данных не происходит При активации политики: • если сессия ранее создана и существует, то при отключении пользователя и повторном подключении к РМ ему будет выдана уже существующая сессия; • если разблокировка сессии по каким-либо причинам не произошла, то пользователю потребуется ввести логин и пароль для входа в новую сессию или разблокировки существующей.

Название политики	Тип политики	Описание

«Аутентификация на уровне сети (RDP)»	Глобальная политика, политика фонда, политика группы, политика сети	Политика позволяет выбрать уровень безопасности для протокола RDP. Выбранный уровень безопасности влияет на способ запроса учетных данных пользователя.
		
		Применимость: все сценарии с протоколом RDP.
		
		Возможные значения:
		
		• «Автосогласование» (по умолчанию). Используется для автоматического согласования уровня безопасности. Этот параметр может не передаваться для некоторых программ доставки, поэтому следует учесть ограничения, приведенные ниже;
		• «RDP». Этот уровень безопасности не требует предварительной аутентификации пользователя до начала подключения по протоколу RDP;
		• «TLS». Используется для защиты подключения пользователя. Этот уровень безопасности преобразует передаваемые учетные данные пользователя в RDP-сессии для их сокрытия от злоумышленника, но при этом не требует предварительной аутентификации до начала подключения по протоколу RDP;
		• «NLA». Этот уровень безопасности предполагает, что пользователь должен быть аутентифицирован до начала подключения по протоколу RDP. Для NLA требуются, чтобы были переданы полные учетные данные пользователя для подключения.
		
		Ограничения для фондов:
		
		• для работы подключения к фондам терминальных серверов STAL должны использоваться:
		  значение «Автосогласование»: при любом типе аутентификации независимо от версии STAL;
		  значения «TLS» или «RDP»: при аутентификации пользователя по паролю независимо от версии STAL;
		  значение «NLA»: при Kerberos-аутентификации независимо от версии STAL. При аутентификации по паролю допустимо использование этого значения только с версией STAL 4.X (с поддержкой протокола NTLM);
		• для работы подключения к фондам терминальных серверов MS RDS должно использоваться:
		  значение «NLA»;
		• для фондов ВРМ, если пользователь использует программу доставки ПО Termidesk Viewer:
		  для подключения с ОС Microsoft Windows к ВРМ ОС Astra Linux Special Edition: значения «Автосогласование» или «TLS»;
		  для подключения с ОС Astra Linux Special Edition к ВРМ ОС Astra Linux Special Edition: значения «Автосогласование», или «RDP», или «TLS»

Название политики	Тип политики	Описание
«Буфер обмена (RDP, SPICE, TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление использованием буфера обмена в протоколах RDP, SPICE и TERA. Политика применяется и при подключении пользователя через веб-браузер, и при подключении непосредственно из компонента «Клиент». Применимость: все сценарии с протоколами SPICE, RDP, TERA. Возможные значения: • «Выключить перенаправление буфера»; • «Двустороннее перенаправление буфера» (по умолчанию); • «Перенаправление буфера только от сервера клиенту»; • «Перенаправление буфера только от клиента серверу»
«Время простоя рабочего места (RDP, SPICE, TERA)»	Глобальная политика, политика фонда	Разрешенное время простоя РМ (отсутствие действия пользователя с мышью и клавиатурой) в секундах. По достижении указанного времени сеанс будет отключен (disconnect). Политика распространяется на компонент «Агент виртуального рабочего места». Политика применяется к сессиям протокола Loudplay, если в Termidesk VDI активировано его использование. Применимость: • ВРМ (RDP, SPICE, TERA); • автономные машины (RDP, TERA). Значение «-1» означает неограниченное время простоя. Значение по умолчанию: «-1»

Название политики	Тип политики	Описание
«Выбор пользователем протокола доставки»	Глобальная политика, политика фонда, политика группы, политика сети	Определяет, может ли пользователь выбрать протокол доставки для подключения к РМ. Политика применяется как при подключении пользователя через веб-браузер, так и при подключении из компонента «Клиент». Возможные значения: • «Разрешен» (по умолчанию) - пользователь может выбирать протокол доставки при подключении к ресурсу; • «Запрещен» - пользователю будет доступен только один протокол доставки: либо высокоприоритетный, либо, если приоритет одинаков, первый по алфавиту
«Глубина цвета (RDP)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление максимально допустимым количеством цветов, отображаемых экраном РМ, для протокола RDP. Для подключения к STAL через стандартную утилиту Windows `mstsc` необходимо использовать значение «32 бит». Применимость: • ВРМ (RDP); • автономные машины (RDP); • терминальные сессии MS RDS; • опубликованные приложения MS RDS; • терминальные сессии Метапоставщика MS RDS; • опубликованные приложения Метапоставщика MS RDS. Возможные значения: • «15 бит»; • «16 бит» (по умолчанию); • «24 бит»; • «32 бит»; • «Не задано»

Название политики	Тип политики	Описание

«Действие при выходе пользователя из ОС (RDP, SPICE, TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Определяет действие после выхода пользователя из ОС.
		
		Применимость: ВРМ (RDP, SPICE, TERA). Политика неприменима для Метапоставщика и будет проигнорирована для сервисного фонда.
		
		Возможные значения:
		
		• «Не задано» (по умолчанию);
		• «Удалять рабочее место» - ВМ будет удалена. Периодичность проверки наличия назначенных, но неиспользуемых РМ для последующего их удаления, составляет 631 секунду;
		• «Не сохранять изменения» - ВМ будет возвращена к ранее созданному снимку. Значение политики применимо для фондов, основанных на шаблонах «Связанный клон» или «Полный клон» VMware vSphere или oVirt;
		• «Не сохранять изменения и назначение ВРМ» - ВМ будет перезагружена с возвратом к ранее созданному снимку (если он поддерживается для диска ВМ), назначение пользователя на ВРМ будет удалено. Значение политики применимо для фондов, основанных на шаблонах «Связанный клон» или «Полный клон» VMware vSphere или oVirt;
		• «Перезагрузить ВРМ» - ВМ будет перезагружена после завершения активной сессии пользователя. Действие применимо ко всем поставщикам ресурсов (которые размещают ВРМ), включая автономные ВМ. При этом:
		  будет выполнена безопасная перезагрузка через утилиты платформы виртуализации для гостевых ОС (например, VMware Tools для VMware vSphere). Однако следует учитывать, что разные платформы виртуализации поддерживают разные способы перезагрузки. Если платформа не поддерживает безопасную перезагрузку, то будет выполнена принудительная перезагрузка;
		  сброс состояния ВРМ не произойдет при перезагрузке ВМ из гостевой ОС или через функционал безопасной перезагрузки из фонда РМ;
		  для платформы VMware vSphere с выбранным режимом диска «Независимый - Непостоянный» будет выполнен сброс дельты диска ВМ.
		
		При применении значений в индивидуальных политиках фонда РМ может быть выведено уведомление «Данное значение политики не применимо к выбранному фонду», если у поставщика ресурсов фонда РМ нет возможности создавать снимки ВМ

Название политики	Тип политики	Описание
«Действие с ВРМ в кеше 2-го уровня»	Глобальная политика, политика фонда	Определяет состояние ВРМ в кеше второго уровня. Политика распространяется на платформы виртуализации, которые поддерживают приостановку ВМ: • ПК СВ Брест; • oVirt; • zVirt; • «РЕД Виртуализация»; • VMware vSphere; • VMmanager. Платформа VMmanager поддерживает приостановку ВМ, начиная с версии 2025.09.1. Возможные значения: • «Выключить машину после публикации» - ВРМ будут выключены после завершения их подготовки (после перехода в статус «Действительный»); • «Приостановить машину после публикации» (по умолчанию) - ВРМ будут приостановлены после завершения их подготовки (после перехода в статус «Действительный»). Изменение значения учитывается для новых ВРМ, создаваемых в кеше второго уровня. ВРМ, уже находящиеся в кеше второго уровня, не будут принудительно переводиться в другое состояние
«Домашний каталог пользователя служб удаленного рабочего стола (RDP)»	Глобальная политика, политика фонда	Политика указывает, будут ли службы удаленных рабочих столов использовать указанный сетевой ресурс или путь к локальному каталогу в качестве корневого каталога домашнего каталога пользователя для сеанса служб удаленных рабочих столов. Политика действует на ОС Microsoft Windows. Формат указания сетевого ресурса (пример): `\\имя_компьютера\имя_общего_ресурса\`. При изменении политики требуется перезагрузка терминальных серверов. Применимость: • терминальные сессии Метапоставщика MS RDS; • опубликованные приложения Метапоставщика MS RDS. Значение по умолчанию: «Не задан»

Название политики	Тип политики	Описание
«Завершение сеанса при достижении лимита времени (RDP, SPICE, TERA)»	Глобальная политика, политика фонда	Политика определяет, будет ли сессия пользователя сразу завершена (logoff) по истечении заданных лимитов времени, а не отключена (disconnect). Политика применяется к сессиям протокола Loudplay, если в Termidesk VDI активировано его использование. Применимость: • ВРМ (RDP, SPICE, TERA); • автономные машины (RDP, TERA); • терминальные сессии и опубликованные приложения Метапоставщика MS RDS; • терминальные сессии и опубликованные приложения Метапоставщика STAL. Работа политики не гарантируется для подключений по протоколу RDP, если в качестве RDP-сервера в РМ используется xRDP. Это связано с особенностями работы xRDP-сервера: события подключения и отключения сессий не отправляются в компонент «Агент виртуального рабочего места». Возможные значения: • «Не задано»; • «Выключено» (по умолчанию); • «Включено»

Название политики	Тип политики	Описание
«Интервал мониторинга кеша Перемещаемых Профилей пользователей (RDP)»	Глобальная политика, политика фонда	Политика позволяет ограничить интервал мониторинга (в минутах) размера кеша Перемещаемых Профилей пользователей для протокола RDP. Политика действует на ОС Microsoft Windows. Политика определяет, как часто проверяется размер всего кеша Перемещаемых Профилей пользователей, указанный в политике «Ограничение размера кеша Перемещаемых Профилей пользователей (RDP)». При изменении политики требуется перезагрузка ВМ или терминальных серверов. Применимость: • ВРМ (RDP); • автономные машины (RDP); • терминальные сессии и опубликованные приложения Метапоставщика MS RDS. Возможные значения (в минутах): от 15 до 10080. Значение по умолчанию: «900»
«Использование аудиосвязи в сеансе Удалённого Помощника»	Глобальная политика, политика фонда, политика группы, политика сети	Политика позволяет разрешить или запретить использование микрофона (голосового чата) и звука. Политика действует для всех сессий «Удаленного помощника». Возможные значения: • «Разрешено»; • «Запрещено» (по умолчанию)
«Использование веб-камеры в сеансе Удалённого Помощника»	Глобальная политика, политика фонда, политика группы, политика сети	Политика позволяет разрешить или запретить использование видеокамеры. Политика действует для всех сессий «Удаленного помощника». Возможные значения: • «Разрешено»; • «Запрещено» (по умолчанию)

Название политики	Тип политики	Описание
«Использование обязательных профилей на сервере узла сеанса удаленных рабочих столов (RDP)»	Глобальная политика, политика фонда	Политика позволяет указать, используют ли службы удаленных рабочих столов обязательный профиль для всех пользователей, удаленно подключающихся к серверу узла сеанса удаленных рабочих столов. Политика действует на ОС Microsoft Windows. При включении политики службы удаленных рабочих столов используют путь, указанный в политике «Путь для Перемещаемого Профиля пользователя служб удаленного рабочего стола (RDP)», в качестве корневого каталога для обязательного профиля пользователя. Все пользователи, удаленно подключающиеся к серверу узла сеансов удаленных рабочих столов, используют один и тот же профиль пользователя. При отключении политики обязательные профили пользователей не будут использоваться пользователями, удаленно подключающимися к серверу узла сеанса удаленных рабочих столов. При изменении политики требуется перезагрузка ВМ или терминальных серверов. Применимость: • ВРМ (RDP); • автономные машины (RDP); • терминальные сессии и опубликованные приложения Метапоставщика MS RDS. Возможные значения: • «Запрещено» (по умолчанию); • «Разрешено»

Название политики	Тип политики	Описание
«Композиция рабочего стола (RDP)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление отображением художественных эффектов рабочего стола. Для корректного отображения художественных эффектов в параметре «Глубина цвета (RDP)» требуется установить значение «32 бита». Политика применяется только при подключении по протоколу RDP к гостевой ОС Microsoft Windows. Применимость: • ВРМ (RDP); • автономные машины (RDP). Возможные значения: • «Разрешена»; • «Запрещена» (по умолчанию)

Название политики	Тип политики	Описание
«Лимит времени для активных сеансов (RDP, SPICE, TERA)»	Глобальная политика, политика фонда	Политика задает максимальное время для активного сеанса, по истечении которого он будет отключен (disconnect). Для ВРМ с ОС Microsoft Windows действие политики (завершение сеанса вместо его отключения) может быть изменено через: • «Завершение сеанса при достижении лимита времени (RDP, SPICE, TERA)»; • «Лимит времени для отключенных сеансов (RDP, TERA)». Для ВРМ с ОС Linux данная политика будет всегда завершать сеанс, а не отключать его. Для ВРМ с ОС Microsoft Windows политика применяется в момент авторизации пользователя в ОС. Политика распространяется на компонент «Агент виртуального рабочего места». Применимость: • ВРМ (RDP, SPICE, TERA); • автономные машины (RDP, TERA); • терминальные сессии и опубликованные приложения Метапоставщика MS RDS; • терминальные сессии и опубликованные приложения Метапоставщика STAL. Возможные значения: • «Нет ограничений» (по умолчанию; сессии будут оставаться активными без ограничений по времени); • «Не задано»; • выбор: «1 мин», «5 мин», «10 мин», «15 мин», «30 мин», «1 час», «2 часа», «3 часа», «4 часа», «5 часов», «6 часов», «7 часов», «8 часов», «9 часов», «10 часов», «12 часов», «16 часов», «18 часов», «1 день», «2 дня», «3 дня», «4 дня», «5 дней»

Название политики	Тип политики	Описание
«Лимит времени для выхода из сеансов RemoteApp (RDP)»	Глобальная политика, политика фонда	Политика позволяет указать, как долго сеанс пользователя при использовании RemoteApp (удаленного приложения) будет оставаться активным после закрытия всех программ RemoteApp. Если в течение указанного времени пользователь не запустит другое приложение RemoteApp, то сеанс завершится. Политика распространяется на компонент «Агент виртуального рабочего места» и действует для подключений по протоколу RDP к терминальному серверу Метапоставщика MS RDS. Если заданы другие политики с лимитами времени, то будет использоваться та, в которой задан более короткий период. Возможные значения: • «Никогда» (по умолчанию; при закрытии приложения сеанс будет отключен, но не завершен); • «Сразу»; • «Не задано»; • выбор: «1 мин», «5 мин», «10 мин», «15 мин», «30 мин», «1 час», «2 часа», «3 часа», «4 часа», «5 часов», «6 часов», «7 часов», «8 часов», «9 часов», «10 часов», «12 часов», «16 часов», «18 часов», «1 день», «2 дня», «3 дня», «4 дня», «5 дней»

Название политики	Тип политики	Описание
«Лимит времени для отключенных сеансов (RDP, TERA)»	Глобальная политика, политика фонда	Политика задает максимальное время, по истечении которого отключенная (disconnect) сессия будет завершена (logoff). Политика применяется к сессиям протокола Loudplay, если в Termidesk VDI активировано его использование. Политика распространяется на компонент «Агент виртуального рабочего места». Работает совместно с политикой «Завершение сеанса при достижении лимита времени (RDP, SPICE, TERA)». Применимость: • BPM (RDP, TERA). Возможные значения: • «Нет ограничений» (по умолчанию; сессия останется незавершенной без ограничения по времени); • «Не задано»; • выбор: «1 мин», «5 мин», «10 мин», «15 мин», «30 мин», «1 час», «2 часа», «3 часа», «4 часа», «5 часов», «6 часов», «7 часов», «8 часов», «9 часов», «10 часов», «12 часов», «16 часов», «18 часов», «1 день», «2 дня», «3 дня», «4 дня», «5 дней»

Название политики	Тип политики	Описание
«Максимальное количество устаревших шаблонов связанных клонов»	Глобальная политика, политика фонда	Политика определяет количество служебных шаблонов, хранящихся для каждого из фондов РМ. Служебный шаблон - это шаблон, используемый для создания РМ и размещаемый на платформе виртуализации. Если достигнуто заданное максимальное количество, то: • возможность новой публикации фонда РМ будет заблокирована; • для новой публикации нужно удалить некоторые существующие РМ или задать новое значение политике. Если будут удалены все РМ, принадлежащие служебному шаблону, то удалится и сам шаблон. При значении «-1» максимальное количество служебных шаблонов не ограничивается. Возможные значения: от -1 до 100. Значение по умолчанию: «10»
«Масштабирование экрана (RDP)»	Глобальная политика, политика фонда, политика группы, политика сети	Политика управления масштабированием экрана для протокола RDP. Применимость: • ВРМ (RDP); • автономные машины (RDP). Возможные значения: • «Выключено» (по умолчанию); • «Включено»

Название политики	Тип политики	Описание
«Многомониторный режим (RDP, SPICE, TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление многомониторным режимом при подключении к РМ по протоколам RDP, SPICE, TERA. Политика влияет на возможность пользователя использовать экран РМ на нескольких физических мониторах. Применимость: • ВРМ (RDP, SPICE, TERA); • автономные машины (RDP, TERA); • терминальные сессии STAL; • терминальные сессии MS RDS; • терминальные сессии Метапоставщика MS RDS; • терминальные сессии Метапоставщика STAL. При подключении к STAL через стандартную утилиту ОС Microsoft Windows (`mstsc.exe`) включать политику не рекомендуется. При подключении к ВРМ с ОС Astra Linux Special Edition или к STAL через стандартную утилиту ОС Linux (`xfreerdp`) рекомендуется использовать мониторы с одинаковым разрешением экрана. При подключении к STAL рекомендуется использовать конфигурацию, при которой основной монитор расположен слева от остальных. Возможные значения: • «Разрешен» - будет поддерживаться возможность вывода экрана РМ на нескольких дополнительных физических мониторах (если они подключены). При этом вариант использования экрана может быть различен в зависимости от дополнительных настроек программы доставки: дублирование, растяжение экрана и др.; • «Запрещен» (по умолчанию) - экран РМ будет выведен только на основном физическом мониторе, вариант использования которого может быть различен в зависимости от дополнительных настроек параметров в ОС

Название политики	Тип политики	Описание
«Ограничение полосы пропускания копирования файлов (TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Политика позволяет ограничить полосу пропускания при копировании файлов по протоколу TERA. Значение указывается в килобитах в секунду. Применимость: • ВРМ (TERA); • автономные машины (TERA). Значение по умолчанию: «0» (без ограничений)
«Ограничение размера буфера обмена (RDP, SPICE, TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Политика позволяет ограничить размер буфера обмена, доступный в обе стороны (от клиента к серверу и от сервера к клиенту). Значение указывается в килобайтах. Если размер передаваемых данных превышает заданный лимит, то будет передан только объем данных, соответствующий установленному лимиту. Для совместимости с предыдущими версиями программы доставки ПО Termidesk Viewer используется значение по умолчанию. Политика применяется и при подключении пользователя через веб-браузер, и при подключении непосредственно из компонента «Клиент». Применимость: все сценарии с протоколами RDP, SPICE, TERA. При этом для автономных машин только для протоколов RDP, TERA. Значение по умолчанию: «0» (без ограничений)

Название политики	Тип политики	Описание
«Ограничение размера кеша Перемещаемых Профилей пользователей (RDP)»	Глобальная политика, политика фонда	Политика позволяет ограничить размер всего кеша Перемещаемых Профилей пользователей на локальном диске. Политика действует на ОС Microsoft Windows. Для политики необходимо указать максимальный размер (в гигабайтах) для всего кеша Перемещаемых Профилей пользователей. Когда размер всего кеша Перемещаемых Профилей пользователей превысит указанную величину, самые давние по времени использования перемещаемые пользователей будут удаляться до тех пор, пока размер всего кеша Перемещаемых Профилей пользователей не станет меньше этого максимального размера. При изменении политики требуется перезагрузка ВМ или терминальных серверов. Зависит от политики «Интервал мониторинга кеша Перемещаемых Профилей пользователей (RDP)». Применимость: • ВРМ (RDP); • автономные машины (RDP); • терминальные сессии и опубликованные приложения Метапоставщика MS RDS. Возможные значения (в гигабайтах): от 5 до 10000. Значение по умолчанию: «600»

Название политики	Тип политики	Описание
«Ограничение разрешенных форматов буфера обмена (RDP, SPICE, TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Политика позволяет ограничить разрешенные форматы записи в буфер обмена «Клиента», сами форматы задаются в политике «Разрешенные форматы буфера обмена (RDP, SPICE, TERA)». Для совместимости с предыдущими версиями программы доставки ПО Termidesk Viewer используется значение по умолчанию. Политика применяется и при подключении пользователя через веб-браузер, и при подключении непосредственно из компонента «Клиент». Применимость: все сценарии с протоколами RDP, SPICE. При этом для автономных машин только для протоколов RDP. Возможные значения: • «Не задано» (по умолчанию); • «Выключено»; • «Включено»
«Отделяемый пользовательский профиль (RDP, SPICE, TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Использование отделяемого пользовательского профиля в ВРМ. Политика применяется при старте ВРМ. Применимость: ВРМ (RDP, SPICE, TERA). Возможные значения: • «Выключен» (по умолчанию); • «Включен»

Название политики	Тип политики	Описание
«Передача файлов (SPICE, TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление передачей файлов в протоколе SPICE и TERA. Применимость: ВРМ (SPICE, TERA). Политика применяется и при подключении пользователя через веб-браузер, и при подключении непосредственно из компонента «Клиент». Возможные значения: • «Разрешена» (по умолчанию); • «Запрещена»
«Перезапуск рабочего места по инициативе пользователя»	Глобальная политика, политика фонда, политика группы	Политика определяет возможность самостоятельного перезапуска ВРМ пользователем. Применимость: ВРМ (RDP, SPICE, TERA). Возможные значения: • «Разрешен» (по умолчанию); • «Запрещен». Для активации возможности перезапуска ВРМ, нужно установить политике значение «Разрешен». При этом пользователь сможет выполнить принудительный перезапуск назначенного ему ВРМ следующими способами: • через компонент «Клиент»; • через «Агрегатор пользователя»; • через «Портал пользователя»

Название политики	Тип политики	Описание
«Перенаправление PnP-устройств (RDP)»	Глобальная политика, политика фонда	Управление возможностью автоматически перенаправлять PnP-устройства для протокола RDP. Применимость: • ВРМ (RDP); • автономные машины (RDP). Возможные значения: • «Не задано» (по умолчанию); • «Разрешено»; • «Запрещено»

Название политики	Тип политики	Описание

«Перенаправление USB-устройств и фильтрация по PID/VID (RDP, SPICE, TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление перенаправлением USB-устройств и их фильтрацией по параметрам: «Vendor ID» (VID), «Product ID» (PID), класс устройства, его версия.
		
		Применимость:
		
		• ВРМ (RDP, SPICE, TERA) и автономные машины (RDP, TERA);
		• терминальные сессии и опубликованные приложения MS RDS;
		• терминальные сессии и опубликованные приложения Метапоставщика MS RDS.
		
		Возможные значения:
		
		• «0» (по умолчанию) - запрещено перенаправление всех устройств;
		• «1» - разрешено перенаправление всех устройств;
		• «A,B,C,D,E|.....|R,S,T,U,V» - перенаправление устройств в соответствии с фильтром. Каждые пять параметров, разделенных символом «|», составляют один фильтр. Число таких фильтров может быть произвольным.
		
		Правила составления фильтра USB-устройств:
		
		• параметры разделяются запятыми (без пробелов) и могут указываться как в шестнадцатеричном, так и в десятичном формате;
		• первый параметр («A») - класс USB-устройства. Например:
		  «0x01» (шестнад.), «01» (десятич.) - аудиоустройства;
		  «0x07» (шестнад.), «07» (десятич.) - принтеры;
		  «0x0b» (шестнад.), «11» (десятич.) - смарт-карты;
		• второй параметр («B») - идентификатор производителя, VID;
		• третий параметр («C») - идентификатор продукта, PID;
		• четвертый параметр («D») - версия продукта;
		• пятый параметр («E») - разрешить («1») или запретить («0») перенаправление USB-устройства.
		
		Для всех параметров, кроме последнего, разрядность чисел ограничена 16 битами и поддерживается использование значения «-1» (разрешено любое значение).
		
		Пример фильтров для разрешения аудиоустройств любых вендоров, продуктов и версий и запрет принтера с определенным идентификатором производителя:
		
		«0x01,-1,-1,-1,1|0x07,0xffff,-1,-1,0»

Название политики	Тип политики	Описание
«Перенаправление USB-устройств посредством RemoteFX (RDP)»	Глобальная политика, политика фонда, политика группы, политика сети	Политика активации механизма RemoteFX для протокола RDP. Механизм позволяет перенаправлять USB-устройства, подключенные к пользовательской рабочей станции в РМ, и обеспечивает возможность работы сервисов, требующих физического подключения устройства. Он также позволяет управлять доступностью устройств с помощью политик безопасности: Windows Group Policy в ОС Microsoft Windows и polkit в ОС Astra Linux Special Edition. Корректная работа перенаправления зависит от наличия драйверов устройств и используемой версии протокола RDP. Для активации возможности перенаправления USB-устройств из пользовательской рабочей станции в РМ, нужно установить политике значение «Разрешено». Применимость: • ВРМ (RDP); • автономные машины (RDP). Возможные значения: • «Запрещено» (по умолчанию); • «Разрешено»
«Перенаправление веб-камеры (RDP, SPICE, TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление перенаправлением видеокамеры для протоколов RDP, SPICE и TERA. Применимость: • ВРМ (RDP, SPICE, TERA); • автономные машины (RDP, TERA). Возможные значения: • «Разрешено» (по умолчанию); • «Запрещено»

Название политики	Тип политики	Описание
«Перенаправление воспроизведения и записи звука (RDP)»	Глобальная политика, политика фонда	Управление перенаправлением звука в протоколе RDP. Устройства воспроизведения и записи звука определяются на момент подключения к РМ и при их отключении или смене потребуется переподключиться к РМ. Применимость: • ВРМ (RDP); • автономные машины (RDP); • терминальные сессии MS RDS; • опубликованные приложения MS RDS; • терминальные сессии Метапоставщика MS RDS; • опубликованные приложения Метапоставщика MS RDS; • терминальные сессии Метапоставщика STAL; • опубликованные приложения Метапоставщика STAL. Возможные значения: • «Не используется» (по умолчанию); • «Разрешено»; • «Запрещено»

Название политики	Тип политики	Описание
«Перенаправление дисков и папок (RDP, SPICE, TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление перенаправлением дисков и каталогов. Применимость: • ВРМ (RDP, SPICE, TERA); • автономные машины (RDP, TERA); • терминальные сессии MS RDS; • опубликованные приложения MS RDS; • терминальные сессии STAL; • опубликованные приложения STAL; • терминальные сессии Метапоставщика MS RDS; • опубликованные приложения Метапоставщика MS RDS; • терминальные сессии Метапоставщика STAL; • опубликованные приложения Метапоставщика STAL. Возможные значения: • «Разрешено»; • «Запрещено» (по умолчанию)
«Перенаправление домашнего каталога пользователя (RDP)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление перенаправлением домашнего каталога пользователя в РМ. Политика зависит от значения, заданного в политике «Перенаправление дисков и папок (RDP, SPICE, TERA)»: • если задано «Разрешено», то будет учтено значение политики «Перенаправление домашнего каталога пользователя (RDP)»; • если задано «Запрещено», то перенаправление будет запрещено при любом значении политики «Перенаправление домашнего каталога пользователя (RDP)». Возможные значения: • «Разрешено» - при подключении пользователя к РМ его домашний каталог из пользовательской рабочей станции будет перенаправлен в РМ с правами на чтение и запись; • «Запрещено» (по умолчанию)

Название политики	Тип политики	Описание
«Перенаправление последовательных портов (RDP)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление перенаправлением последовательных портов для протокола RDP. Применимость: • ВРМ (RDP); • автономные машины (RDP). Возможные значения: • «Разрешено»; • «Запрещено» (по умолчанию)

Название политики	Тип политики	Описание
«Перенаправление принтеров (RDP, SPICE, TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление перенаправлением принтеров. Можно запретить перенаправление, разрешить перенаправлять все принтеры или только выбранные пользователем. Применимость: • ВРМ (RDP, SPICE, TERA); • автономные машины (RDP, TERA); • терминальные сессии MS RDS; • опубликованные приложения MS RDS; • терминальные сессии STAL; • опубликованные приложения STAL; • терминальные сессии Метапоставщика MS RDS; • опубликованные приложения Метапоставщика MS RDS; • терминальные сессии Метапоставщика STAL; • опубликованные приложения Метапоставщика STAL. Возможные значения: • «Не перенаправлять» (по умолчанию); • «Перенаправлять все»; • «Перенаправлять выбранные пользователем». Особенности работы с ОС Microsoft Windows (ВРМ, автономные машины) по протоколу RDP: • при назначении политики группы или политики сетей не требуется перезапуск РМ; • политика влияет на то, какие возможности перенаправления принтеров будут у пользователя, подключившегося через «Клиент»; • учитывается возможность переопределения перенаправления принтеров службой каталогов MS AD. Если политика изменилась, то «Агент виртуального рабочего места» зафиксирует событие в журнале РМ

Название политики	Тип политики	Описание
«Перенаправление смарт-карт (RDP, SPICE, TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление перенаправлением смарт-карт для протоколов RDP, SPICE, TERA. Применимость: • ВРМ (RDP, SPICE, TERA); • автономные машины (RDP, TERA); • терминальные сессии MS RDS; • опубликованные приложения MS RDS; • терминальные сессии STAL; • опубликованные приложения STAL; • терминальные сессии Метапоставщика STAL; • опубликованные приложения Метапоставщика STAL. Возможные значения: • «Разрешено» (по умолчанию); • «Запрещено»

Название политики	Тип политики	Описание

«Перенаправление часового пояса пользователя (RDP, TERA, SPICE)»	Глобальная политика, политика фонда	Управление перенаправлением часового пояса с пользовательской рабочей станции в сессию пользователя. Политика применяется при подключении пользователя (не применяется для HTML5 SPICE):
		• через компонент «Клиент»;
		• через веб-браузер (HTML5-клиент).
		
		Для работы должна быть активирована политика «Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)». Для гарантированного применения изменений нужно полностью перезапустить компонент «Клиента».
		
		Применимость:
		• ВРМ (RDP, SPICE, TERA) и автономные машины (RDP, TERA);
		• терминальные сессии и опубликованные приложения Метапоставщика MS RDS;
		• терминальные сессии и опубликованные приложения Метапоставщика STAL.
		
		Особенности работы с установленным «Агентом виртуального рабочего места» (ВРМ, автономные машины):
		• часовой пояс может быть изменен для существующей сессии, не только для новой;
		• если используется ОС Microsoft Windows, то для изменения часового пояса выполнится команда `tzutil`;
		• если используется ОС Linux, то для изменения часового пояса выполнится команда `timedatectl` (если она существует), либо создастся файл новой временной зоны. При этом:
		  если используется `systemd`, то перезапустятся службы (если они включены и работают): `rsyslog`, `syslog-ng`, `cron`, `anacron`, `systemd-timesyncd`, `chronyd`, `ntpd`, `ntp`, `openntpd`;
		  если `systemd` не используется, то перезапустятся службы (если они включены и работают): `cron`, `rsyslog`.
		
		Возможные значения:
		• «Не задано» (по умолчанию);
		• «Разрешено» - после подключения пользователя в его сессии установится часовой пояс, заданный на пользовательской рабочей станции. Если используется метапоставщик, то для всех пользовательских сессий установится часовой пояс того, кто подключился последним;
		• «Запрещено» - после подключения пользователя в его сессии установится часовой пояс, соответствующий системному в РМ. Часовой пояс пользовательской рабочей станции перенаправлен не будет

Название политики	Тип политики	Описание
«Подключение с отличающимся именем пользователя (SPICE, TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Для работы политики необходимо, чтобы в гостевой ОС ВРМ была настроен модуль PAM (см. подраздел **Настройка модуля PAM без монтирования Перемещаемых Профилей**). Политика управления подключением пользователя к ВМ. Применяется в случае, если вводимый в ВМ логин отличен от логина, введенного пользователем при аутентификации в Termidesk VDI. Применимость: • ВРМ (SPICE, TERA); • автономные машины (TERA). Возможные значения: • «Разрешено»; • «Запрещено» (по умолчанию)
«Показ обоев рабочего стола (RDP)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление отображением обоев рабочего стола РМ для протокола RDP. Применимость: • ВРМ (RDP); • автономные машины (RDP); • терминальные сессии MS RDS; • терминальные сессии Метапоставщика MS RDS. Возможные значения: • «Разрешен» - обои будут отображены; • «Запрещен» (по умолчанию) - обои не будут отображаться

Название политики	Тип политики	Описание
«Полноэкранный режим (SPICE, TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление работой в полноэкранном режиме для протоколов SPICE и TERA. Применимость: ВРМ (SPICE, TERA). Политика применяется и при подключении пользователя через веб-браузер, и при подключении непосредственно из компонента «Клиент». При подключении из веб-браузера политика действует ограниченно и ее штатное функционирование не гарантируется. Возможные значения: • «Включен» (по умолчанию) - при подключении пользователя к РМ ПО Termidesk Viewer при запуске будет работать в полноэкранном режиме; • «Выключен» - при подключении пользователя к РМ ПО Termidesk Viewer при запуске будет работать в оконном режиме

Название политики	Тип политики	Описание
«Путь для Перемещаемого Профиля пользователя служб удаленного рабочего стола (RDP)»	Глобальная политика, политика фонда	По умолчанию службы удаленных рабочих столов хранят все профили пользователей локально на сервере узла сеанса удаленных рабочих столов. Политика действует на ОС Microsoft Windows. Политика используется для указания общего сетевого ресурса, в котором профили пользователей могут храниться централизованно, позволяя пользователю получать доступ к одному и тому же профилю для сеансов на всех серверах узла сеансов удаленных рабочих столов, настроенных на использование общего сетевого ресурса для профилей пользователей. При задании значения для политики, службы удаленных рабочих столов будут использовать указанный путь в качестве корневого каталога для всех профилей пользователей. Непосредственно профили будут содержаться во вложенных каталогах, названных по имени учетной записи каждого пользователя `%USERNAME%`, которые появятся на сетевом ресурсе автоматически после подключения пользователя. При изменении политики требуется перезагрузка ВМ или терминальных серверов. Зависит от политики «Использование обязательных профилей на сервере узла сеанса удаленных рабочих столов (RDP)». Формат указания сетевого ресурса (пример): `\\имя_компьютера\имя_общего_ресурса\`. Применимость: • ВРМ (RDP); • автономные машины (RDP); • терминальные сессии Метапоставщика MS RDS; • опубликованные приложения Метапоставщика MS RDS. Значение по умолчанию: «Не задан»
«Разрешение веб-камеры (RDP, SPICE, TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Допустимые разрешения видеокамеры в протоколах RDP, SPICE, TERA. Применимость: • ВРМ (RDP, SPICE, TERA); • автономные машины (RDP, TERA). Значение по умолчанию: «320-2560x240-1440»

Название политики	Тип политики	Описание
«Разрешенные форматы буфера обмена (RDP, SPICE, TERA)»	Глобальная политика, политика фонда, политика группы, политика сети	Политика определяет разрешенный формат записей в буфере обмена. В зависимости от направления передачи перед отправкой или после получения данных из буфера обмена запрашивается их тип и сопоставляется с разрешенными значениями. В зависимости от типа данных передача данных разрешается или запрещается. Для совместимости с предыдущими версиями ПО Termidesk Viewer используется значение по умолчанию. Политика применяется и при подключении пользователя через веб-браузер, и при подключении непосредственно из компонента «Клиент». Применимость: • BPM (RDP, SPICE, TERA); • автономные машины (RDP, TERA); • терминальные сессии MS RDS; • опубликованные приложения MS RDS; • терминальные сессии STAL; • опубликованные приложения STAL; • терминальные сессии Метапоставщика MS RDS; • опубликованные приложения Метапоставщика MS RDS; • терминальные сессии Метапоставщика STAL; • опубликованные приложения Метапоставщика STAL. Возможные значения: • «Любой» (по умолчанию); • «Текст без форматирования»

Название политики	Тип политики	Описание
«Режим подключения администратора в Удалённом Помощнике»	Глобальная политика, политика фонда, политика группы, политика сети	Политика определяет значение параметра «Также разрешить управление мышью и клавиатурой» в диалоговом окне клиентской части «Удаленного помощника» при подключении администратора к сеансу. Если политике «Согласие пользователя для подключения администратора в Удалённом Помощнике» присвоено значение «Не требуется», то управление мышью и клавиатурой доступно администратору независимо от значения политики «Режим подключения администратора в Удалённом Помощнике». Применимость: • BPM (RDP, SPICE, TERA); • автономные машины (RDP, TERA); • терминальные сессии метапоставщика STAL. Возможные значения: • «Управление» - администратору доступно управление мышью и клавиатурой. Изменение параметра пользователю недоступно; • «Просмотр» - администратору доступен только просмотр сеанса. Изменение параметра пользователю недоступно; • «Запросить у пользователя» (по умолчанию) - возможность управления мышью и клавиатурой определяется пользователем при подключении администратора к сеансу

Название политики	Тип политики	Описание
«Сглаживание шрифтов (RDP)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление сглаживанием шрифтов, отображаемых экраном РМ, для протокола RDP. Применимость: • РМ (RDP); • автономные машины (RDP); • терминальные сессии MS RDS; • опубликованные приложения MS RDS; • терминальные сессии STAL; • опубликованные приложения STAL; • терминальные сессии Метапоставщика MS RDS; • опубликованные приложения Метапоставщика MS RDS; • терминальные сессии Метапоставщика STAL; • опубликованные приложения Метапоставщика STAL. Возможные значения: • «Разрешено» (по умолчанию); • «Запрещено»

Название политики	Тип политики	Описание
«Сжатие данных (RDP)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление использованием сжатия данных при взаимодействии с РМ по протоколу RDP. Применимость: • ВРМ (RDP); • автономные машины (RDP); • терминальные сессии MS RDS; • опубликованные приложения MS RDS; • терминальные сессии STAL; • опубликованные приложения STAL; • терминальные сессии Метапоставщика MS RDS; • опубликованные приложения Метапоставщика MS RDS; • терминальные сессии Метапоставщика STAL; • опубликованные приложения Метапоставщика STAL. Возможные значения: • «Включено» (по умолчанию); • «Выключено»; • «Не задано»
«Согласие пользователя для подключения администратора в Удалённом Помощнике»	Глобальная политика, политика фонда, политика группы, политика сети	Политика определяет необходимость согласия пользователя для подключения администратора к его сеансу через «Удаленный помощник». Возможные значения: • «Требуется» (по умолчанию) - запрос на подключение администратора отобразится пользователю в диалоговом окне клиентской части «Удаленного помощника». Администратор подключится к сеансу только после согласия пользователя. Имя подключившегося администратора отобразится у пользователя; • «Не требуется» - запрос на подключение администратора не будет отображен пользователю, т.к. подтверждение запроса не требуется. Уведомление о подключении администратора отобразится пользователю в клиентской части «Удаленного помощника». Имя подключившегося администратора отобразится у пользователя

Название политики	Тип политики	Описание
«Технология перенаправления дисков и папок (RDP)»	Глобальная политика, политика фонда, политика группы, политика сети	Выбор технологии для перенаправления дисков и каталогов в протоколе RDP. Политика зависит от значения, заданного в политике «Перенаправление дисков и папок (RDP, SPICE, TERA)»: • если задано «Разрешено», то будет учтено значение политики «Технология перенаправления дисков и папок (RDP)» для выбора технологии; • если задано «Запрещено», то перенаправление будет запрещено при любом значении политики «Технология перенаправления дисков и папок (RDP)». Возможные значения: • «RDP (по умолчанию) - будет использоваться стандартная технология для перенаправления; • «WebDAV» - будет использоваться оптимизированная технология перенаправления, отличающаяся более высокой скоростью передачи и обработки данных и предназначенная для работы с большими файлами

Название политики	Тип политики	Описание
«Тип сети (RDP)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление типом сетевого подключения, используемого при подключении к РМ по протоколу RDP. Применимость: • ВРМ (RDP); • автономные машины (RDP); • терминальные сессии MS RDS; • опубликованные приложения MS RDS; • терминальные сессии STAL; • опубликованные приложения STAL; • терминальные сессии Метапоставщика MS RDS; • опубликованные приложения Метапоставщика MS RDS; • терминальные сессии Метапоставщика STAL; • опубликованные приложения Метапоставщика STAL. Возможные значения: • «Модем»; • «Низкоскоростное широкополосное подключение»; • «Широкополосное подключение»; • «Высокоскоростное широкополосное подключение»; • «Глобальная сеть»; • «Локальная сеть»; • «Авто» (по умолчанию)

Название политики	Тип политики	Описание
«Удаление рабочего места»	Глобальная политика, политика фонда, политика группы, политика сети	Политика определяет событие, после которого будет произведено удаление РМ. Работает совместно с политикой «Действие при выходе пользователя из ОС (RDP, SPICE, TERA)». Применимость: • ВРМ (RDP, SPICE, TERA); • терминальные сессии Метапоставщика MS RDS; • опубликованные приложения Метапоставщика MS RDS. Возможные значения: • «После события выхода пользователя из ОС» (по умолчанию); • «После события завершения синхронизации профиля»

«Удаление устаревшей публикации»	Глобальная политика, политика фонда	Политика определяет действие, применимое к устаревшей публикации.
		
		Использование политики меняет поведение системного параметра «Срок действия устаревшей публикации, ч» на уровне фонда РМ.
		
		Возможные значения:
		
		• «Удалять по истечении срока действия» (по умолчанию) - устаревшие публикации будут удалены по истечении срока, заданного в параметре «Срок действия устаревшей публикации, ч»;
		• «Удалять немедленно» - при перепубликации фонда назначенная ВМ будет немедленно заменена на новую публикацию;
		• «Не удалять назначенные машины» - назначенные РМ не будут удалены при перепубликации (такие РМ будут требовать ручного удаления). Неназначенные РМ удаляются и публикуются заново. При этом значении:
		  - текущая публикация будет находиться в состоянии частичного удаления, пока существует хотя бы одно назначенное РМ;
		  - после удаления последнего назначенного РМ публикация будет переведена в статус «Публикация удалена». Новая публикация будет переведена в статус «Публикация успешно завершена», если она завершена успешно

Название политики	Тип политики	Описание
«Уровень сжатия (RDP)»	Глобальная политика, политика фонда, политика группы, политика сети	Управление уровнем сжатия данных, при взаимодействии с РМ по протоколу RDP. Применимость: • ВРМ (RDP); • автономные машины (RDP); • терминальные сессии MS RDS; • опубликованные приложения MS RDS; • терминальные сессии STAL; • опубликованные приложения STAL; • терминальные сессии Метапоставщика MS RDS; • опубликованные приложения Метапоставщика MS RDS; • терминальные сессии Метапоставщика STAL; • опубликованные приложения Метапоставщика STAL. Возможные значения: • «0»; • «1» (по умолчанию); • «2»; • «Не задано»

БИБЛИОТЕКА СКРИПТОВ

Общие сведения о библиотеке скриптов

Библиотека скриптов предназначена для централизованного управления скриптами автоматизации развертывания РМ.

Добавленный в библиотеку скрипт можно использовать для:

- назначения фонду РМ;
- ручного выполнения в нужном РМ;
- выполнения по заданному расписанию.

Для корректной работы скрипта требуется выполнить дополнительные настройки базового ВРМ.

Для отображения списка скриптов следует перейти «Рабочие места - Библиотека скриптов». Основные параметры списка приведены в таблице (см. таблицу Параметры списка скриптов).

Таблица 102. Параметры списка скриптов

Параметр	Описание
«Название»	Наименование скрипта
«Описание»	Информационное сообщение с описанием назначения скрипта
«Используется в фондах»	Список фондов, которым назначен скрипт
«Используется в расписаниях»	Список расписаний, которым назначен скрипт

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет

заблокирована, если нет изменений для возврата к исходному состоянию;

- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Для добавления скрипта в библиотеку следует перейти «Рабочие места - Библиотека скриптов» и нажать экранную кнопку **[Создать]**.

Созданные скрипты можно:

- редактировать, для этого нужно пометить название скрипта, а затем нажать экранную кнопку **[Изменить]**;
- удалить, для этого нужно пометить название скрипта, а затем нажать экранную кнопку **[Удалить]**.

Добавление скриптов в библиотеку

Для добавления скрипта в библиотеку нужно перейти «Рабочие места - Библиотека скриптов», затем нажать экранную кнопку **[Создать]**.

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления скрипта в библиотеку). Для сохранения параметров конфигурации нужно нажать экранную кнопку **[Сохранить]**.

Таблица 103. Данные для добавления скрипта в библиотеку

Параметр	Описание
«Название»	Наименование скрипта
«Файл скрипта»	Путь к файлу скрипта на сетевом хранилище SMB или NFS в формате URI. Для корректной работы параметра нужно выполнить настройки базового BPM (см. подраздел **Функционал выполнения скриптов в PM**). Пример использования: `nfs://nfs.termidesk.local/var/scripts/demo.sh`
«Строка запуска»	Путь к интерпретатору скриптов PM с параметрами запуска для выполнения скрипта. Пример использования: • в ОС Linux: `/usr/bin/bash` или `bash`; • в ОС Microsoft Windows: `cmd.exe /c`, `C:\Windows\System32\WindowsPowerShell\powershell.exe -File` или `poweshell` (если первый вариант не сработал)
«Аргументы»	Аргументы и переменные окружения, передаваемые скрипту при выполнении
«Описание»	Информационное сообщение, используемое для описания назначения скрипта

ТЕГИ

Общие сведения о тегах

Теги предназначены для классификации объектов Termidesk VDI и упрощения их поиска и управления.

Созданный тег может быть назначен:

- доменам аутентификации;
- группам домена аутентификации;
- порталам;
- поставщикам ресурсов;
- сетям;
- протоколам доставки;
- фондам РМ;
- ВРМ.

Существующие ограничения:

- в наименовании тегов допускается указывать прописные и строчные буквы, цифры, а также символы «.», «-» и «_». Использование пробелов не допускается;
- теги являются регистронезависимыми;
- просмотр страницы управления тегами будет доступен оператору, если у него есть пользовательское разрешение «Просмотр тегов»;
- управление тегами будет доступно оператору, если у него есть пользовательское разрешение «Управление тегами».

Для отображения списка тегов следует перейти «Системные параметры – Управление тегами». Основные параметры списка приведены в таблице (см. таблицу Параметры списка тегов).

Таблица 104. Параметры списка тегов

Параметр	Описание
«Имя тега»	Наименование тега
«Количество использований»	Количество объектов, которым назначен тег

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы;
- фильтрация записей таблицы через функцию «Умный фильтр»;
- экспорт записей таблицы в `csv`-файл. Можно выгрузить:
  - все записи таблицы, для этого нажать графический элемент , затем нажать

экранную кнопку **[Экспорт всех]**;

- выбранные записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт выбранных]**.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Для добавления тега в Termidesk VDI используется экранная кнопка **[Создать]**.

Доступны следующие действия над тегами:

- редактирование. Для этого нужно пометить тег и нажать экранную кнопку **[Изменить]**;
- удаление. Для этого нужно пометить тег и нажать экранную кнопку **[Удалить]**.

Удаление тега приводит к его удалению у всех связанных объектов.

После добавления тега можно перейти к просмотру связанных с ним объектов. Для этого в сводной таблице страницы «Управление тегами» в столбце «Имя тега» следует нажать на наименование тега. Подробные сведения о работе с тегами приведены в подразделе **Работа с тегами**.

Добавление тегов

Для добавления тега нужно перейти «Системные параметры - Управление тегами», затем нажать экранную кнопку **[Создать]**.

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления тега). Для сохранения параметров конфигурации нужно нажать экранную кнопку **[Сохранить]**.

Таблица 105. Данные для добавления тега

Параметр	Описание
«Теги»	Наименование тега

Работа с тегами

Для просмотра списка объектов, связанных с тегом нужно перейти «Системные параметры - Управление тегами», затем в столбце «Имя тега» сводной таблицы нажать на наименование тега.

На открывшейся странице будет представлен список объектов, связанных с выбранным тегом. Основные параметры списка приведены в таблице (см. таблицу Параметры списка тегированных объектов).

Таблица 106. Параметры списка тегированных объектов

Параметр	Описание
«Имя сущности»	Наименование объекта, которому назначен тег
«Тип сущности	Тип объекта
«Теги сущности	Список тегов, назначенных объекту

В зависимости от типа объекта поддерживаются следующие действия:

- для объектов с типом «Группа пользователей»:
  - управление политиками группы домена аутентификации;
  - редактирование группы домена аутентификации;
- для объектов с типом «Домен аутентификации»:
  - редактирование домена аутентификации;
- для объектов с типом «Портал»:
  - управление объектами не поддерживается;
- для объектов с типом «Поставщик ресурсов»:
  - редактирование поставщика ресурсов;
  - управление режимом техобслуживания поставщика ресурсов;
- для объектов с типом «Сети»:
  - управление политиками сети;
  - редактирование группы домена аутентификации;
- для объектов с типом «Протокол доставки»:
  - редактирование протокола доставки;
- для объектов с типом «Рабочее место»:
  - управление питанием РМ;
  - управление режимом техобслуживания РМ;
  - назначение владельца РМ;
  - выполнение скрипта в РМ;

- восстановление РМ;
- удаление РМ;

- для объектов с типом «Фонд»:
  - управление политиками фонда РМ;
  - редактирование фонда РМ;
  - управление режимом техобслуживания фонда РМ.

ФОНД РМ

Добавление фонда РМ

Общие сведения о фонде РМ

Фонд РМ – это совокупность подготовленных РМ для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей.

Для отображения списка фондов РМ следует перейти «Рабочие места - Фонды». Основные параметры списка приведены в таблице (см. таблицу Параметры списка фондов).

Таблица 107. Параметры списка фондов

Параметр	Описание
«Фонд рабочих мест»	Наименование фонда РМ
«Статус»	Состояние готовности фонда РМ Если фонд РМ находится в зависшем состоянии в статусах «Удален», «Отменен», «Ошибка», «Подготовка», «Создание» более 48 часов, то ВМ, вызвавшая это состояние, будет удалена периодической задачей, выполняемой раз в 24 часа. Фонд РМ также будет удален
«Места»	Общее количество РМ в фонде
«Готовятся»	Количество подготавливаемых РМ
«Выбор протокола»	Флаг возможности выбора пользователем протокола доставки при работе с фондом РМ. Значение определяется политикой фонда РМ «Выбор пользователем протокола доставки»
«Группа рабочих мест»	Принадлежность фонда группе РМ
«Поставщик ресурсов»	Поставщик ресурсов, примененный в фонде
«Комментарий»	Информационное сообщение, используемое для описания назначения фонда РМ
«Теги»	Список тегов, назначенных фонду РМ. При выборе тега выполняется переход к разделу «Системные параметры – Управление тегами» со списком объектов, которым назначен данный тег

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- поиск записей по таблице;
- изменение внешнего вида таблицы;
- фильтрация записей таблицы через функцию «Умный фильтр».

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Для добавления нового фонда РМ следует перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Создать]**.

Доступны следующие действия над фондами РМ:

- редактирование. Для этого нужно пометить фонд и нажать экранную кнопку **[Изменить]**;
- удаление. Для этого нужно пометить фонд и нажать экранную кнопку **[Удалить]**;
- назначение политик фонда. Для этого нужно пометить фонд и нажать экранную кнопку **[Политики]**. Значения по умолчанию наследуются от глобальных политик. Список политик и общее описание по применению политик приведено в подразделе **Политики**;
- назначение тегов фонду. Для этого пометить фонд и нажать экранную кнопку **[Теги]**. Общее описание по применению тегов приведено в подразделе **Общие сведения о тегах**.

После добавления фонда РМ можно перейти к его детальному просмотру. Для этого в сводной таблице окна «Фонды» в столбце «Фонд рабочих мест» следует нажать на наименование фонда РМ.

На открывшейся странице будут представлены следующие разделы:

- «Назначенные места» - список РМ, используемых субъектами;
- «Кеш» - список созданных и настроенных РМ;
- «Пользователи» - имена пользователей, используемые для определения разрешений по доступу к фондам РМ;
- «Группы» - наименование групп, используемые для определения разрешений по доступу к фондам РМ;
- «Сети» - сети, используемые для определения разрешений по доступу к фондам РМ;
- «Протоколы доставки» – доступные протоколы удаленного доступа, используемые при доставке РМ;
- «Скрипты» - скрипты, используемые для управления РМ;
- «Публикации» – актуальная информация о созданном фонде РМ. Раздел будет отсутствовать, если фонд используется для публикации приложений или для доступа к терминальным сессиям;
- «Журнал» – системные сообщения, связанные с жизненным циклом фонда РМ.

Настройка отдельных глобальных параметров по управлению фондами РМ (например, «Количество удаляемых рабочих мест за один проход») доступна в общих системных параметрах Termidesk VDI.

Добавление фонда ВМ

Для добавления фонда ВМ следует перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Создать]**, выбрать тип мастера публикации «Виртуальные машины».

Доступность функционала зависит от типа редакции Termidesk VDI.

Откроется мастер публикации фонда (см. рисунок Базовые настройки фонда в Мастере публикации). Необходимо заполнить параметры, указанные в таблице (см. таблицу Базовые настройки фонда), и нажать экранную кнопку **[Далее]**.

При нажатии экранной кнопки **[Закрыть]** или клавиши **<Esc>**, или иконки «Крестик», на любом из этапов работы произойдет закрытие мастера без сохранения настроек.

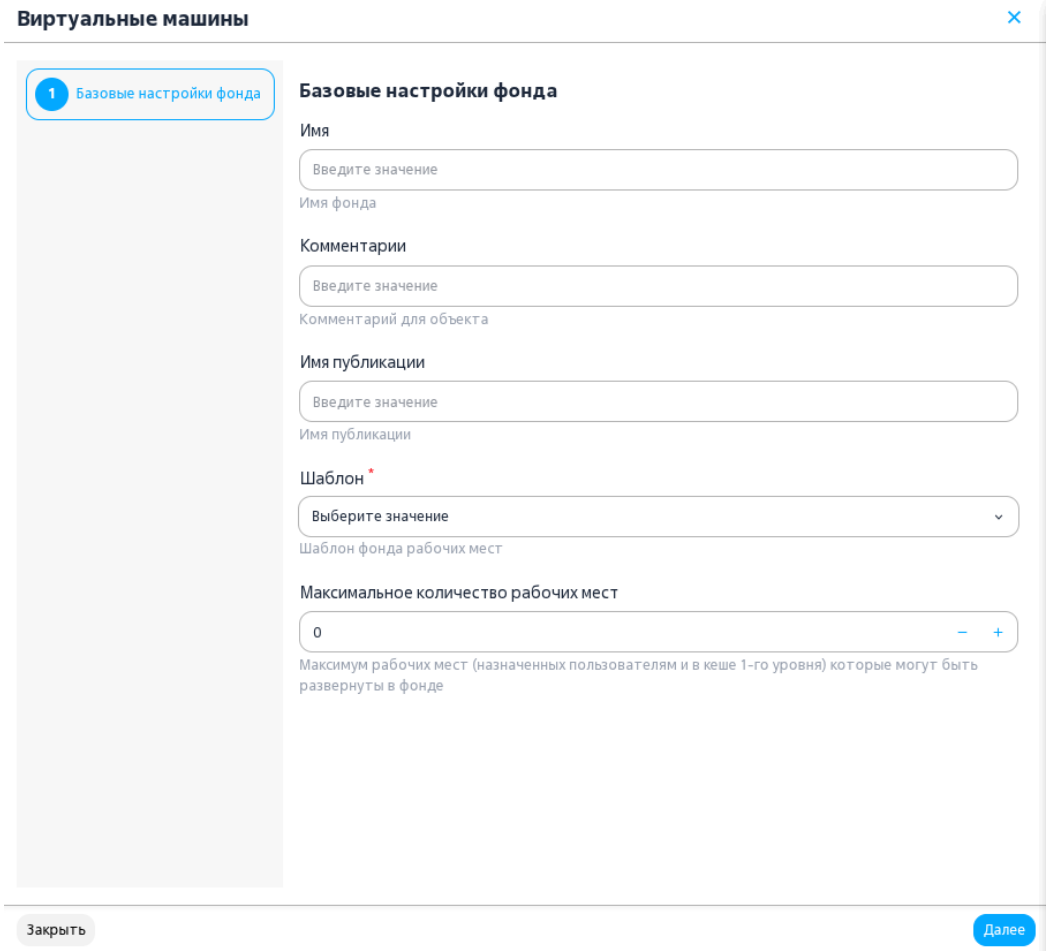


Рисунок 63. Базовые настройки фонда в Мастере публикации

Таблица 108. Базовые настройки фонда

Параметр	Описание
«Имя»	Текстовое наименование фонда. Наименование может содержать только буквы латинского алфавита, цифры, знаки «-» (дефис), пробел и «_» (нижнее подчеркивание). Параметр обязателен для заполнения
«Комментарии»	Информационное сообщение, используемое для описания назначения фонда
«Имя публикации»	Текстовое наименование публикации. Параметр применяется для георасределенной установки и позволяет отображать однообразные фонды РМ в виде единого ярлыка в компоненте «Клиент». Для этого на каждой из установок компонента «Универсальный диспетчер» в базовых настройках фонда следует задавать идентичное значение параметра. Параметр обязателен для заполнения
«Шаблон»	Шаблон РМ, который будет использоваться при создании РМ

Параметр	Описание
«Максимальное количество рабочих мест»	Максимальное количество РМ в фонде. При задании максимального количества следует руководствоваться следующим: • рекомендуется устанавливать значение, не равное 0; • при задании количества РМ в кеше рекомендуется хотя бы одному кешу (1-го или 2-го уровня) задавать значение, отличное от 0. Если значения обоих кешей будут равны 0, то РМ пользователю не будет выдано, даже если максимальное количество РМ отлично от 0. Таким образом функционал выдачи РМ пользователю по требованию (без наличия РМ в кеше) недоступен. Технически не ограничивается конфигурация, когда все три параметра (максимальное количество РМ, кеш 1-го и кеш 2-го уровня) заданы со значением 0. Однако при такой конфигурации РМ не будут созданы. При расчете количества РМ в фонде учитываются статусы РМ: • «Подготовка»; • «Действительный»; • «Техобслуживание»; • «Удаление»; • «Удаляется»; • «Отменяется»

Если обязательное поле не было заполнено или есть ошибка при заполнении, оно будет подсвечено красным цветом и будет выведено сообщение об ошибке после нажатия экранной кнопки **[Далее]**. Индикация цветом и сообщение не исчезнут после корректного заполнения поля.

Далее будет выполнен переход на следующий шаг настройки мастера публикации фонда (см. рисунок Дополнительные настройки фонда Мастера публикации), в котором нужно заполнить параметры, указанные в таблице (см. таблицу Дополнительные настройки фонда).

Поскольку во время перехода выполняется отправка данных на сервер, возможна ситуация, что при возвращении на предыдущий шаг появится сообщение об ошибке, если параметр «Протоколы доставки» не был заполнен. Отправка данных на сервер происходит всегда при переходе между шагами, кроме перехода назад с завершающего этапа.

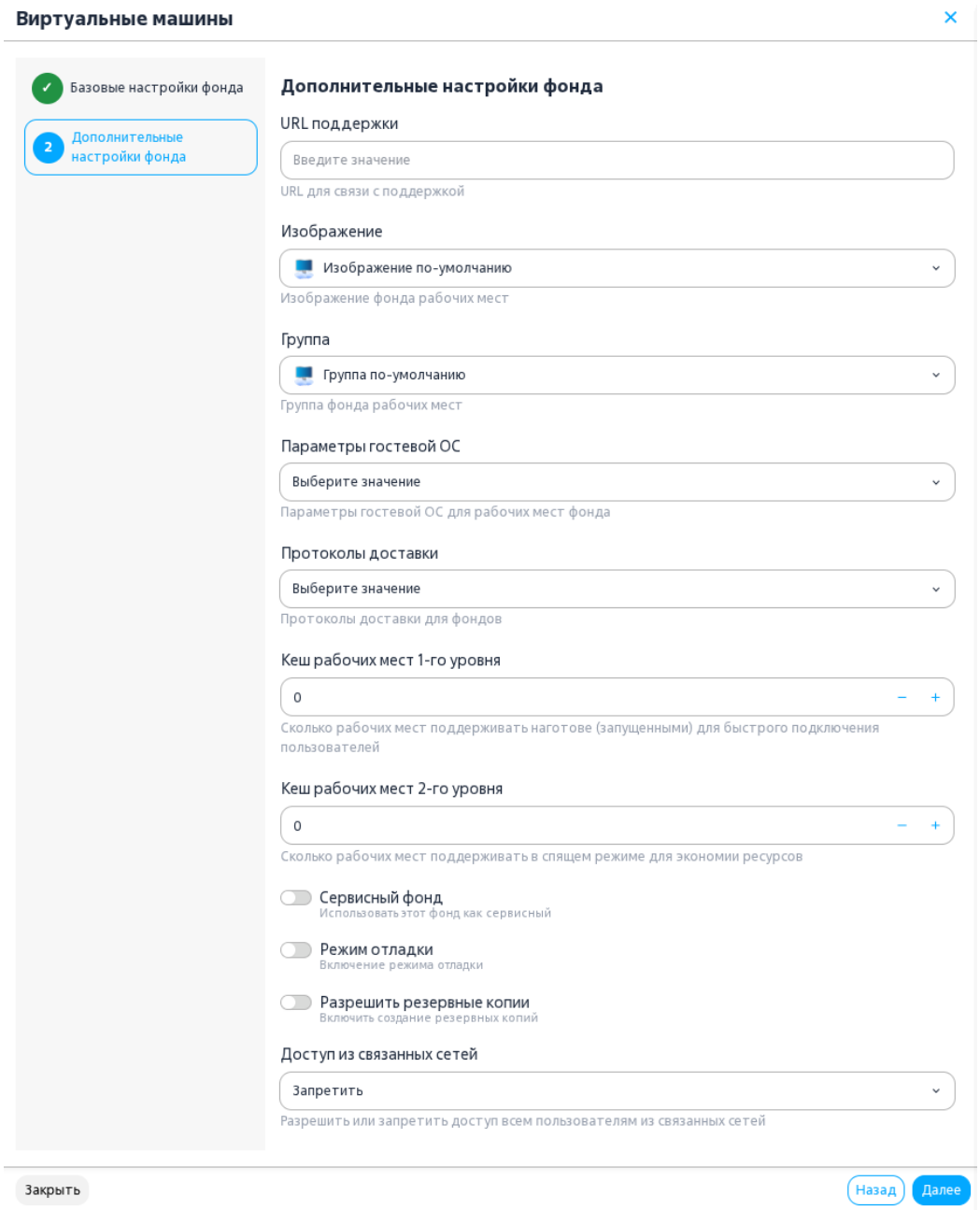


Рисунок 64. Дополнительные настройки фонда Мастера публикации

Таблица 109. Дополнительные настройки фонда

Параметр	Описание
«URL поддержки»	URL для связи с технической поддержкой. Адрес должен соответствовать стандарту кодирования URI. В случае задания некорректного URL, графический элемент для обращения в техническую поддержку в компоненте «Клиент» будет недоступен. Примеры схем для задания URL: • `http(s)://termidesk.local/support`; • `ws(s)://chat.termidesk.local`; • `file:///home/support/help.html`; • `mailto:support@termidesk.local`
«Изображение»	Графическое представление фонда
«Группа»	Группа рабочих мест, в которой будет отображаться созданный фонд
«Параметры гостевой ОС»	Параметры конфигурации гостевой ОС, которые будут использованы при создании РМ
«Протоколы доставки»	Один или несколько протоколов доставки, которые будут доступны для фонда
«Кеш рабочих мест 1-го уровня»	Количество созданных, настроенных и запущенных РМ в фонде Параметр не задается, если создается фонд РМ для терминальных серверов. Параметр может быть равен 0, но если одновременно с этим кеш 2-го уровня также будет 0, то РМ не будут созданы.
«Кеш рабочих мест 2-го уровня»	Количество созданных, настроенных и выключенных РМ Параметр не задается, если создается фонд РМ для терминальных серверов. Параметр может быть равен 0, но если одновременно с этим кеш 1-го уровня также будет 0, то РМ не будут созданы.
«Сервисный фонд»	Активация использования фонда как **сервисного** для Метапоставщика
«Режим отладки»	Активация более подробной детализации логов для фонда, по умолчанию режим отключен. При включении режима Termidesk VDI перестает удалять ВМ в фонде
«Разрешить резервные копии»	Активация режима резервного копирования ВМ фонда при использовании системы Rubackup. По умолчанию режим отключен

Параметр	Описание
«Доступ из связанных сетей»	Управление доступом пользователей из связанных сетей. Сети указываются в настройках фонда РМ после его создания. Параметр недоступен, если создается сервисный фонд. Возможные значения: • «Разрешить» - все пользователи из указанных сетей смогут подключаться к фонду РМ; • «Запретить» (по умолчанию) - всем пользователям из указанных сетей будет запрещено подключение к фонду РМ

После заполнения параметров нажать экранную кнопку **[Далее]**.

Если был активирован параметр «Сервисный фонд», то мастер публикации отобразит шаг «Настройки ограничения количества интерактивных сессий» (см. рисунок Настройки ограничений для сервисного фонда), в котором нужно заполнить параметры, указанные в таблице (см. таблицу Настройки ограничений по количеству интерактивных сессий).

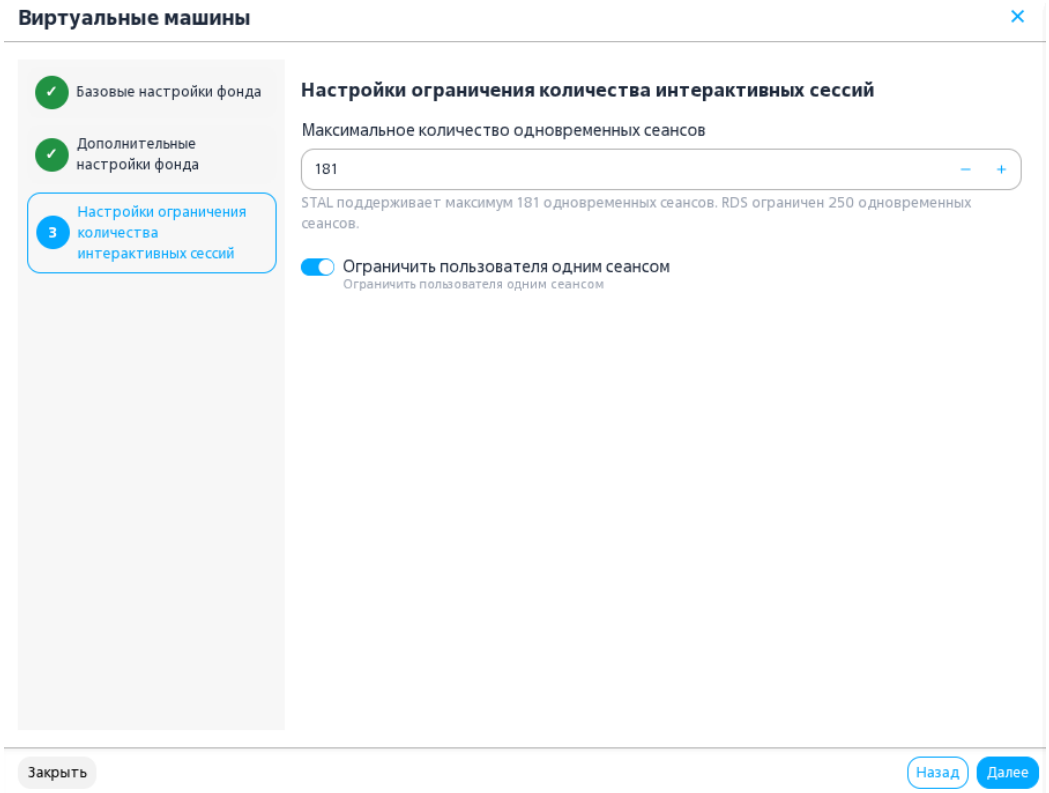


Рисунок 65. Настройки ограничений для сервисного фонда

Таблица 110. Настройки ограничений по количеству интерактивных сессий

Параметр	Описание
«Максимальное количество одновременных сеансов»	Количество одновременных сеансов на терминальном сервере. Параметр используется для ограничения количества одновременных сеансов на сервере. Максимальное количество сеансов ограничивается в соответствии с использующимся на терминальном сервере решением: • STAL – 181 одновременных сеансов; • MS RDSH – 250 одновременных сеансов. Ограничение количества сеансов повышает производительность, поскольку меньшее количество сеансов требует системных ресурсов. Значение по умолчанию: «181»
«Ограничить пользователя одним сеансом»	Активация ограничения пользователей одним сеансом терминального сервера. При активации параметра пользователи, подключающиеся к ОС терминального сервера, будут ограничены одним сеансом (активным или отключенным) на этом сервере. Если пользователь покидает сеанс в отключенном состоянии, он автоматически подключается к этому сеансу при следующем входе в систему. При деактивации параметра пользователям будет разрешено устанавливать неограниченное количество одновременных сеансов на сервере. Значение по умолчанию: «Да»

После заполнения параметров нажать экранную кнопку **[Далее]**.

В следующем окне завершить настройку фонда, нажав экранную кнопку **[Завершить]**. При успешном создании фонда в этом же окне отобразится сообщение «Фонд успешно создан!» (см. рисунок Успешное завершение настройки публикации фонда). Для выхода из мастера публикации нужно нажать экранную кнопку **[Закрыть]**.

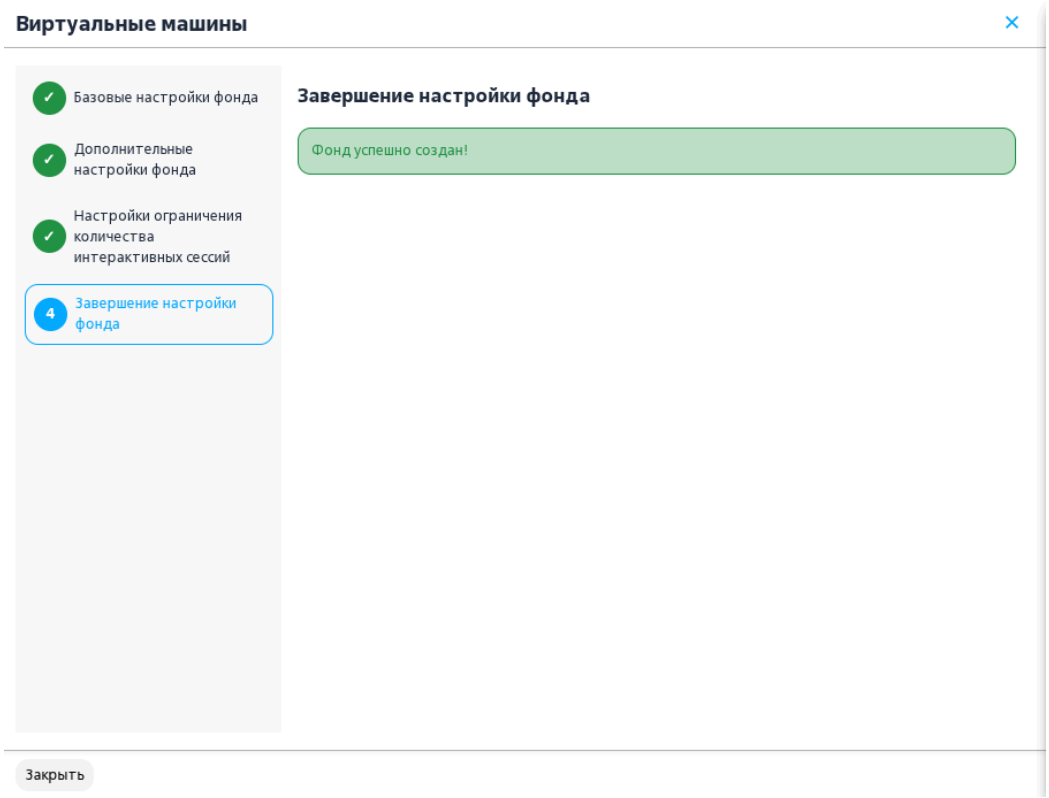


Рисунок 66. Успешное завершение настройки публикации фонда

Добавление фонда публикации служб «Метапоставщика»

Для добавления фонда следует перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Создать]**, выбрать тип мастера публикации «Приложение».

Доступность функционала зависит от типа редакции Termidesk VDI.

Сервисный фонд для Метапоставщика должен быть предварительно создан (см. подраздел **Предварительная настройка для добавления терминального сервера Метапоставщика**).

Хотя бы одно ВРМ из сервисного фонда должно получить статус «Действительный» во вкладке «Рабочие места».

Откроется мастер публикации фонда. Необходимо выбрать тип публикации (см. рисунок Выбор типа публикации):

- «Удаленный рабочий стол» - для публикации терминальной сессии;
- «Удалённое приложение» - для публикации приложения.

Затем нажать экранную кнопку **[Далее]**.

Экранная кнопка **[Закрыть]**, клавиша **<Esc>**, иконка «Крестик» на любом из этапов работы закрывает мастер без сохранения настроек.

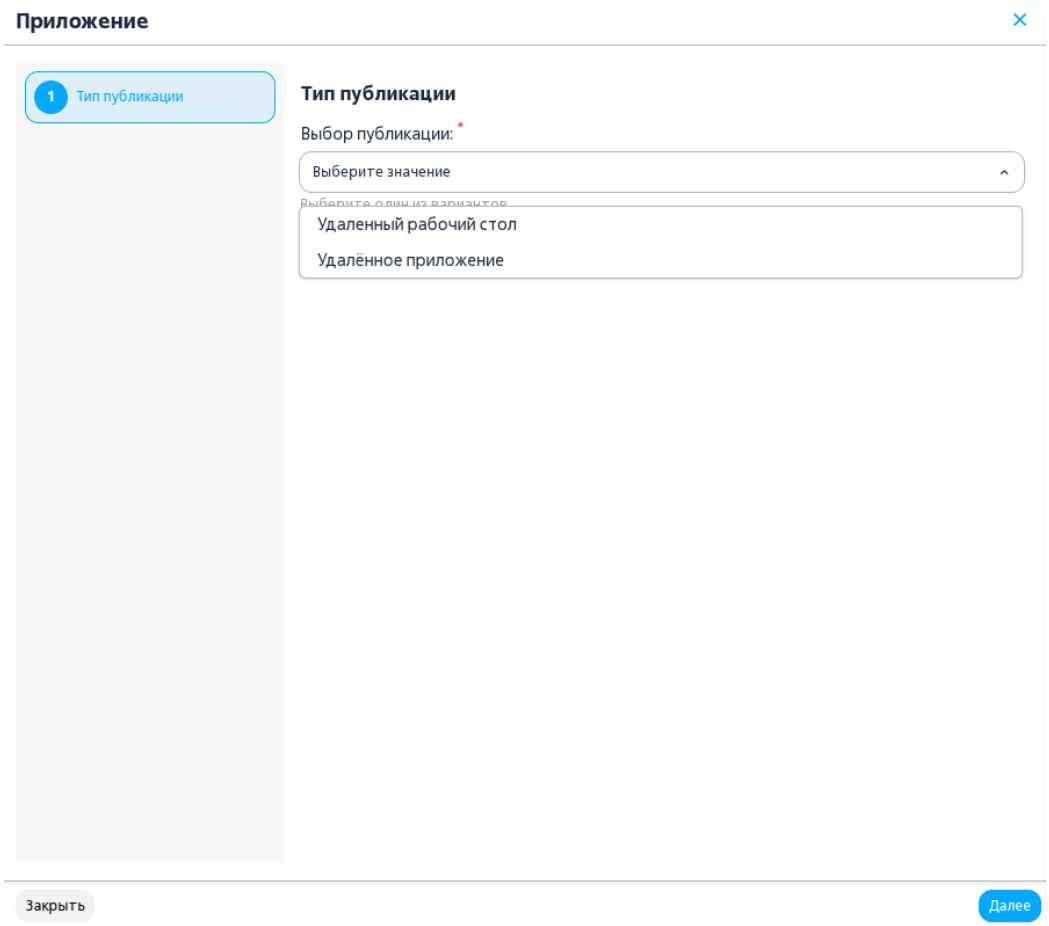


Рисунок 67. Выбор типа публикации

Далее нужно выбрать поставщик ресурсов с типом «Метапоставщик» для публикации (см. рисунок Выбор Метапоставщика для публикации). Если он не был создан ранее, выбрать «Новый поставщик ресурсов» и заполнить параметры для его создания.

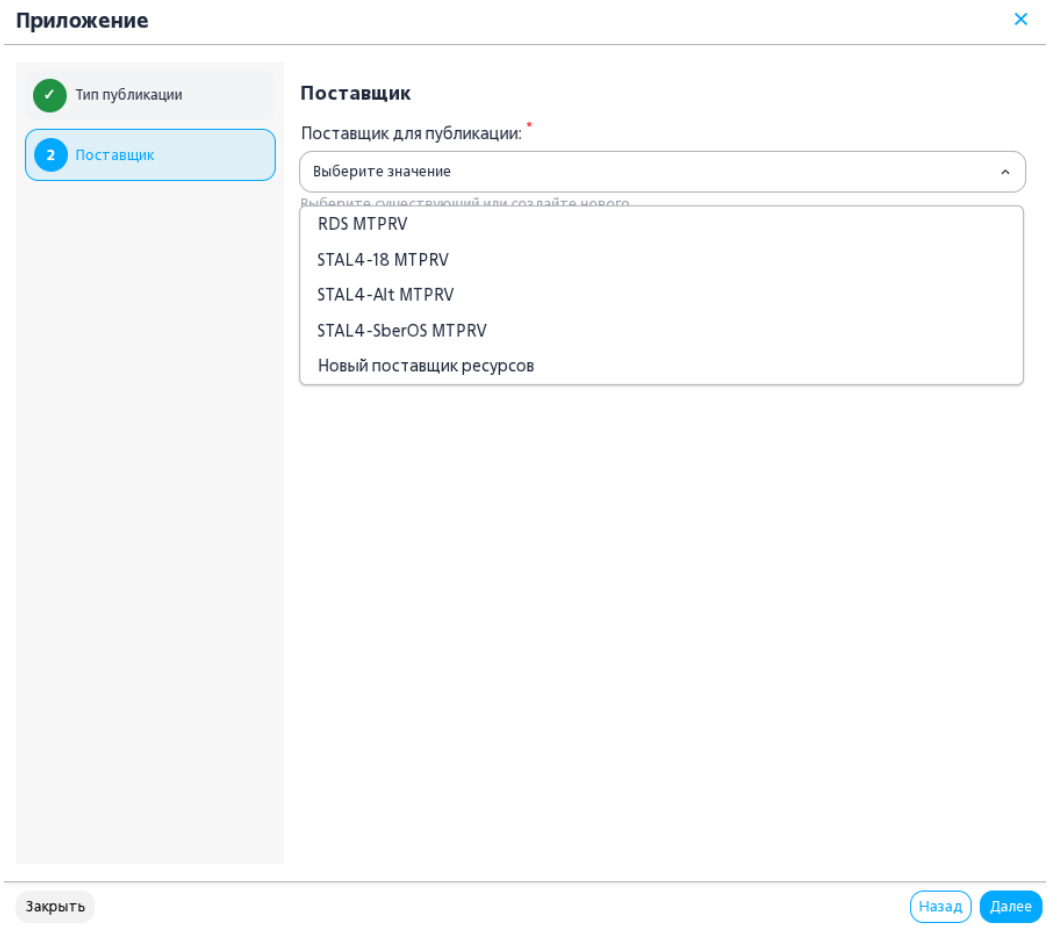


Рисунок 68. Выбор Метапоставщика для публикации

На следующем шаге задать (см. рисунок Ввод наименования сессии или приложения):

- или наименование приложения и выбрать приложение для публикации (если ранее был выбран тип публикации «Удаленное приложение»);
- или задать наименование терминальной сессии (если ранее был выбран тип публикации «Удаленный рабочий стол»).

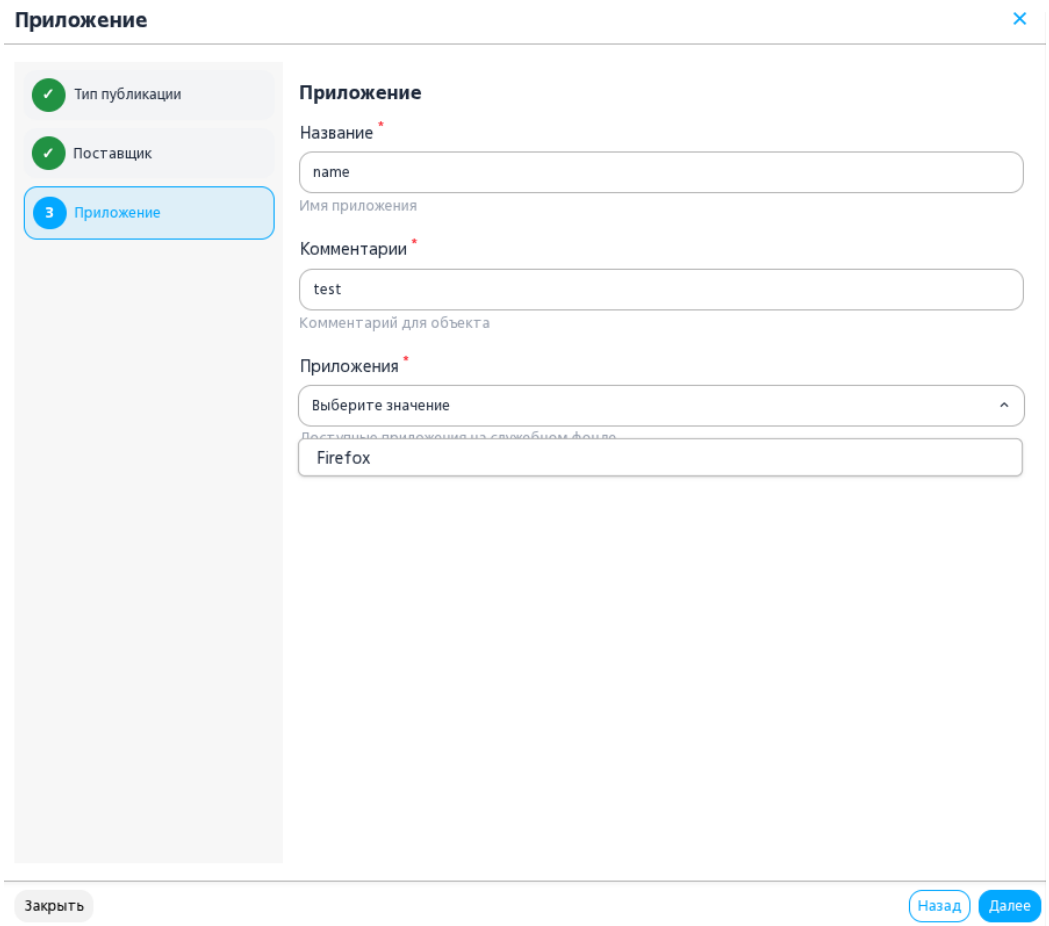


Рисунок 69. Ввод наименования сессии или приложения

Далее будет выполнен переход на следующий шаг настройки мастера публикации фонда (см. рисунок Настройка фонда публикации служб Метапоставщика), в котором нужно заполнить параметры, указанные в таблице (см. таблицу Настройки фонда публикации служб Метапоставщика).

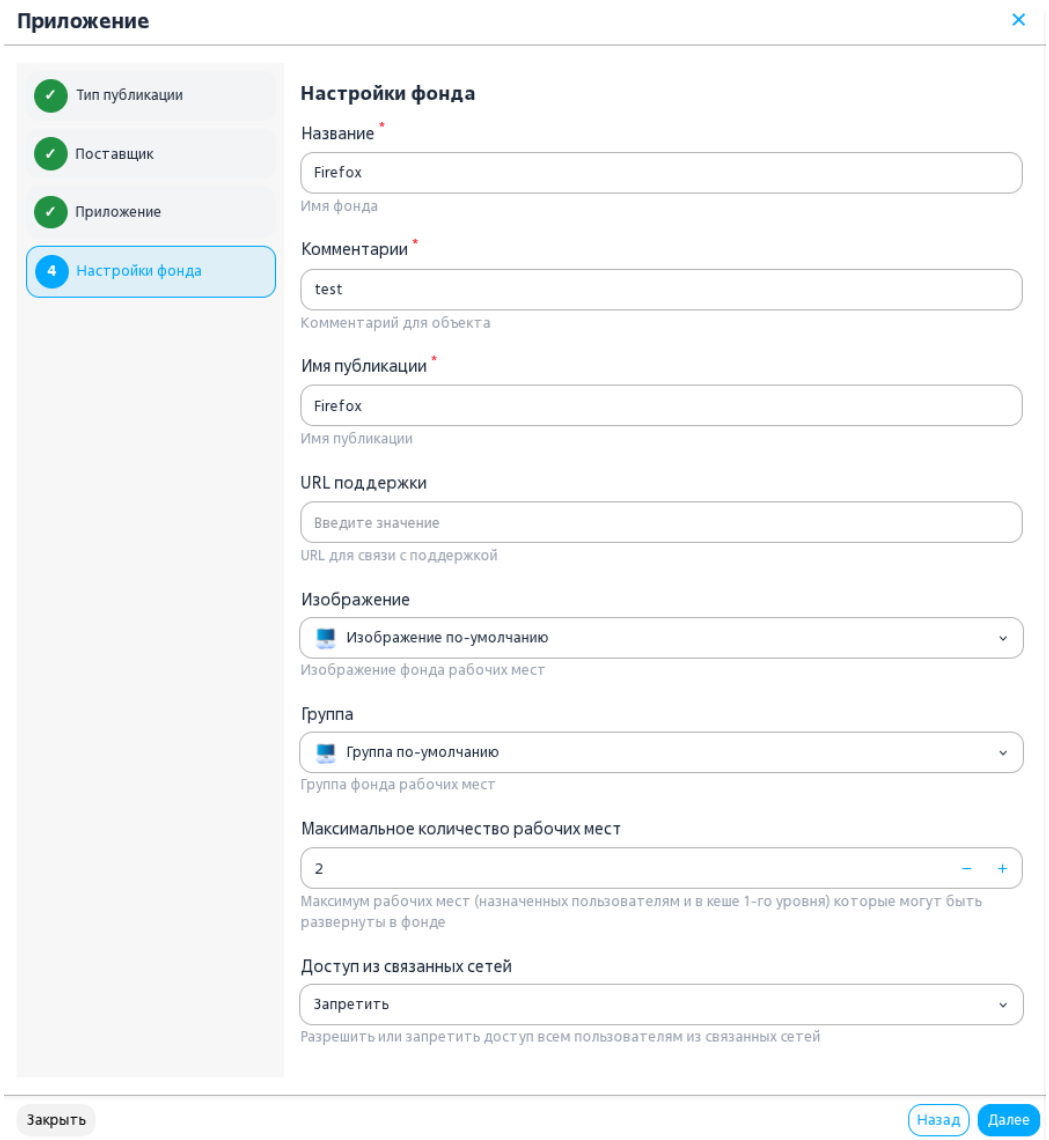


Рисунок 70. Настройка фонда публикации служб Метапоставщика

Таблица 111. Настройки фонда публикации служб Метапоставщика

Параметр	Описание
«Название»	Текстовое наименование фонда. Наименование может содержать только буквы латинского алфавита, цифры, знаки «-» (дефис), пробел и «_» (нижнее подчеркивание). Параметр обязателен для заполнения
«Комментарии»	Информационное сообщение, используемое для описания назначения фонда
«Имя публикации»	Текстовое наименование публикации. Параметр применяется для георасределенной установки и позволяет отображать однообразные фонды ВРМ в виде единого ярлыка в компоненте «Клиент». Для этого на каждой из установок компонента «Универсальный диспетчер» в базовых настройках фонда следует задавать идентичное значение параметра. Параметр обязателен для заполнения

Параметр	Описание
«URL поддержки»	URL для связи с технической поддержкой. Адрес должен соответствовать стандарту кодирования URI. В случае задания некорректного URL, графический элемент для обращения в техническую поддержку в компоненте «Клиент» будет недоступен. Примеры схем для задания URL: • `http(s)://termidesk.local/support`; • `ws(s)://chat.termidesk.local`; • `file:///home/support/help.html`; • `mailto:support@termidesk.local`
«Изображение»	Графическое представление фонда
«Группа»	Группа РМ, в которой будет отображаться созданный фонд
«Максимальное количество рабочих мест»	Максимальное количество РМ в фонде. При достижении указанного предела новые пользователи не смогут подключиться к фонду. При расчете количества РМ в фонде учитываются статусы РМ: • «Подготовка»; • «Действительный»; • «Техобслуживание»; • «Удаление»; • «Удаляется»; • «Отменяется»
«Доступ из связанных сетей»	Управление доступом пользователей из связанных сетей. Сети указываются в настройках фонда РМ после его создания. Возможные значения: • «Разрешить» - все пользователи из указанных сетей смогут подключаться к фонду РМ; • «Запретить» - всем пользователям из указанных сетей будет запрещено подключение к фонду РМ

На следующем шаге задать домен аутентификации и группу пользователей, входящую в этот домен, которым будет доступен фонд (см. рисунок Выбор домена аутентификации и группы пользователей). Для выбора будут доступны те домены аутентификации, для которых в параметре «Субъекты» задано значение «Пользователи» или «Все».

Шаг опционален: параметры можно добавить после завершения работы мастера публикации, в созданном фонде на странице «Рабочие места - Фонды».

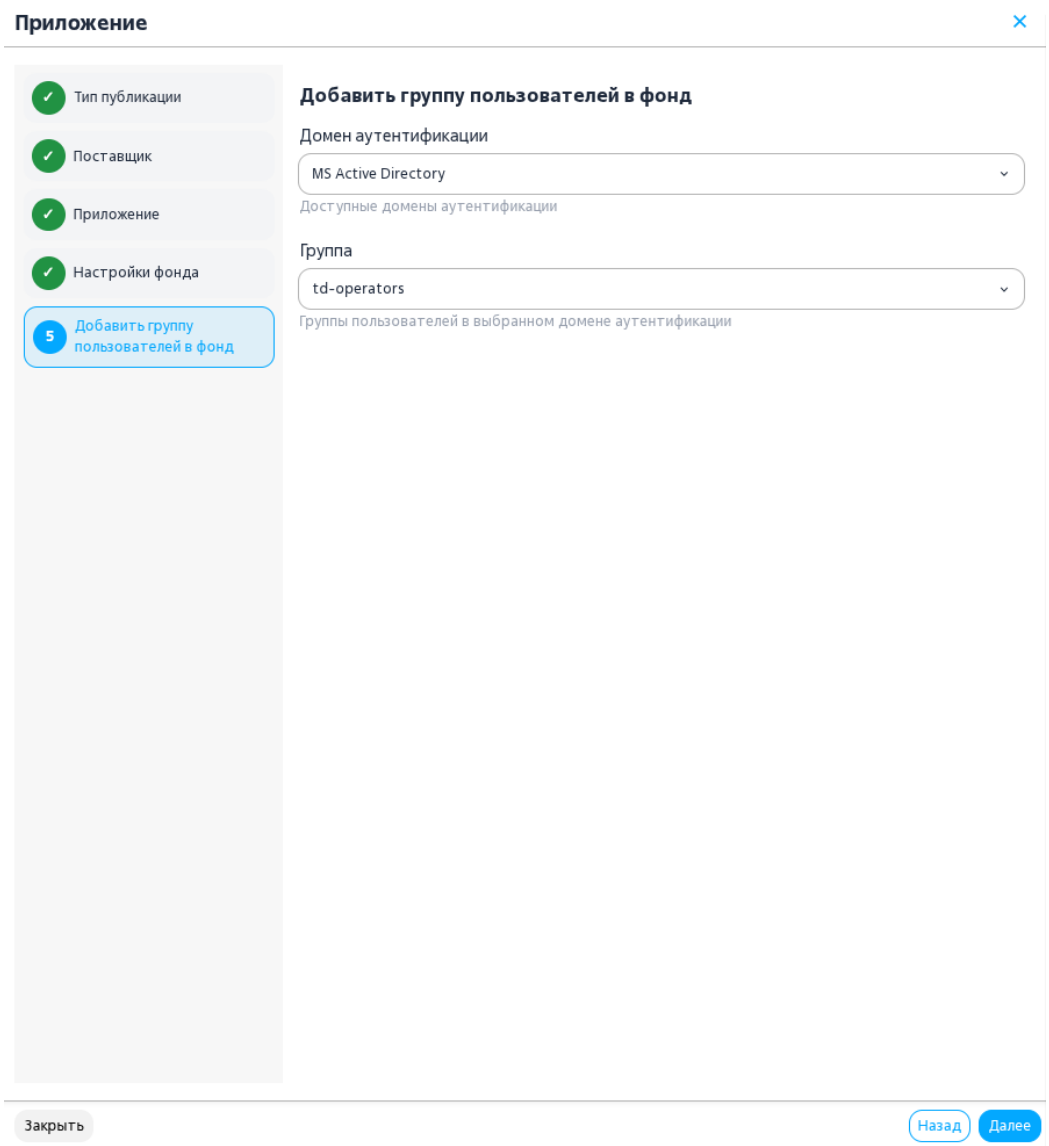


Рисунок 71. Выбор домена аутентификации и группы пользователей

Затем выбрать пользователя домена аутентификации (см. рисунок [Выбор-пользователей]).

Шаг опционален: параметры можно добавить после завершения работы мастера публикации, в созданном фонде на странице «Рабочие места - Фонды».

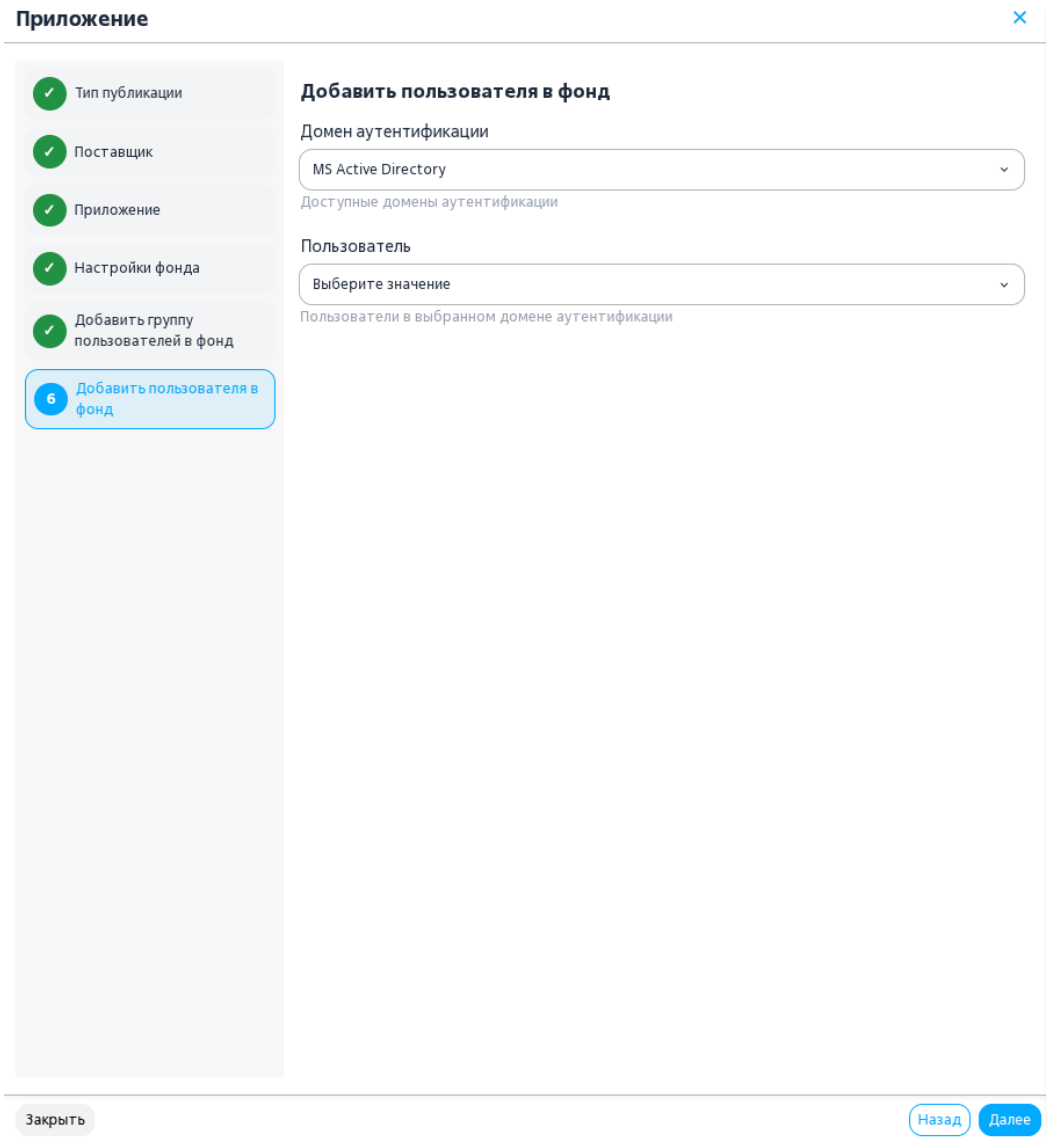


Рисунок 72. Выбор пользователей

Далее выбрать протокол доставки, который будет доступен для фонда (см. рисунок Выбор протокола доставки). Если он не был создан ранее, выбрать «Создать RDP (терминальный доступ)» и заполнить параметры для его создания.

Протокол доставки можно добавить и (или) изменить после завершения работы мастера публикации в созданном фонде на странице «Рабочие места - Фонды».

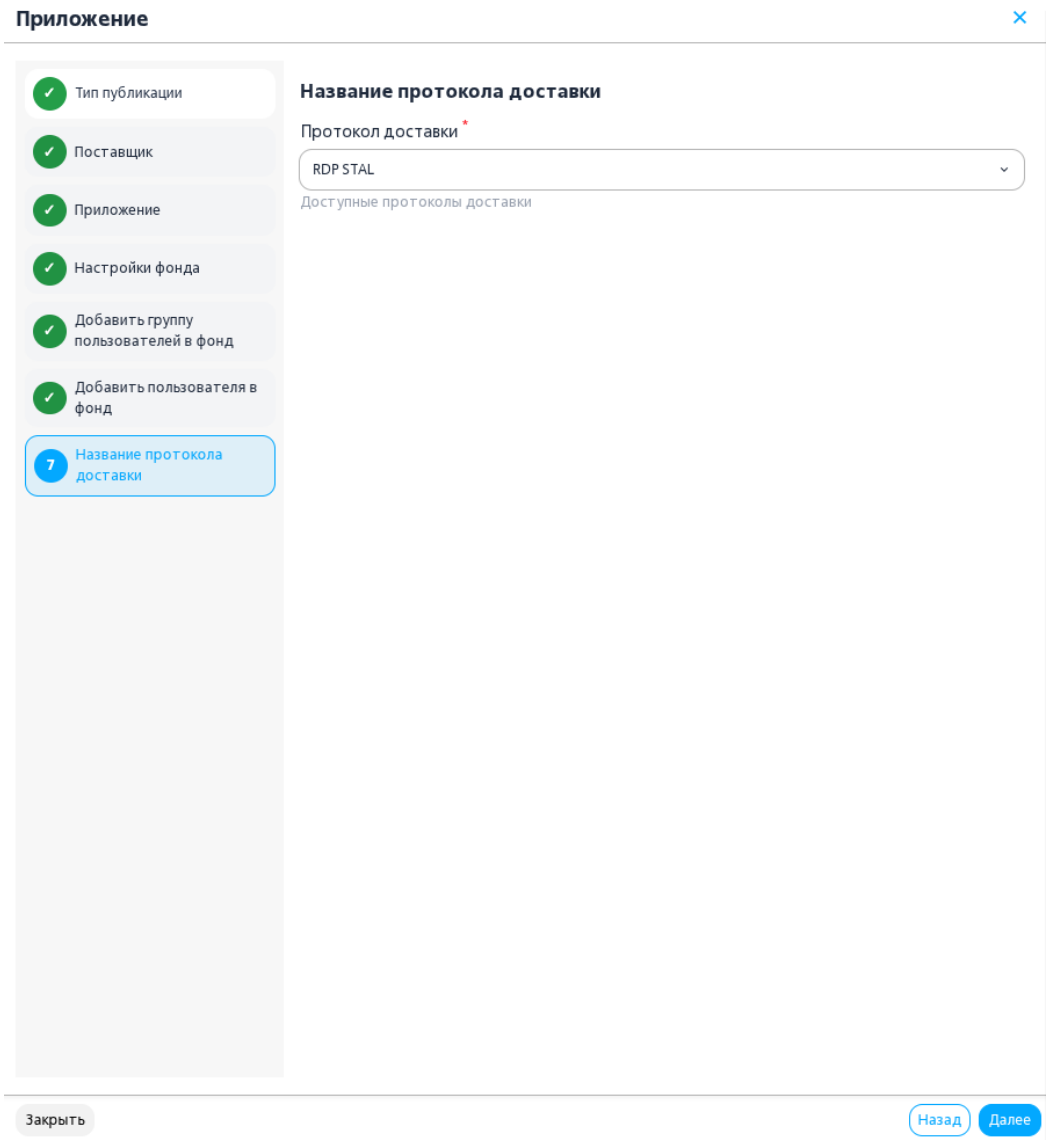


Рисунок 73. Выбор протокола доставки

В следующем окне ознакомиться с параметрами будущего фонда и завершить настройку, нажав экранную кнопку **[Завершить]** (см. рисунок Завершение настройки фонда). При успешном создании фонда в этом же окне отобразится сообщение «Фонд успешно создан!». Для выхода из мастера публикации нужно нажать экранную кнопку **[Закрыть]**.

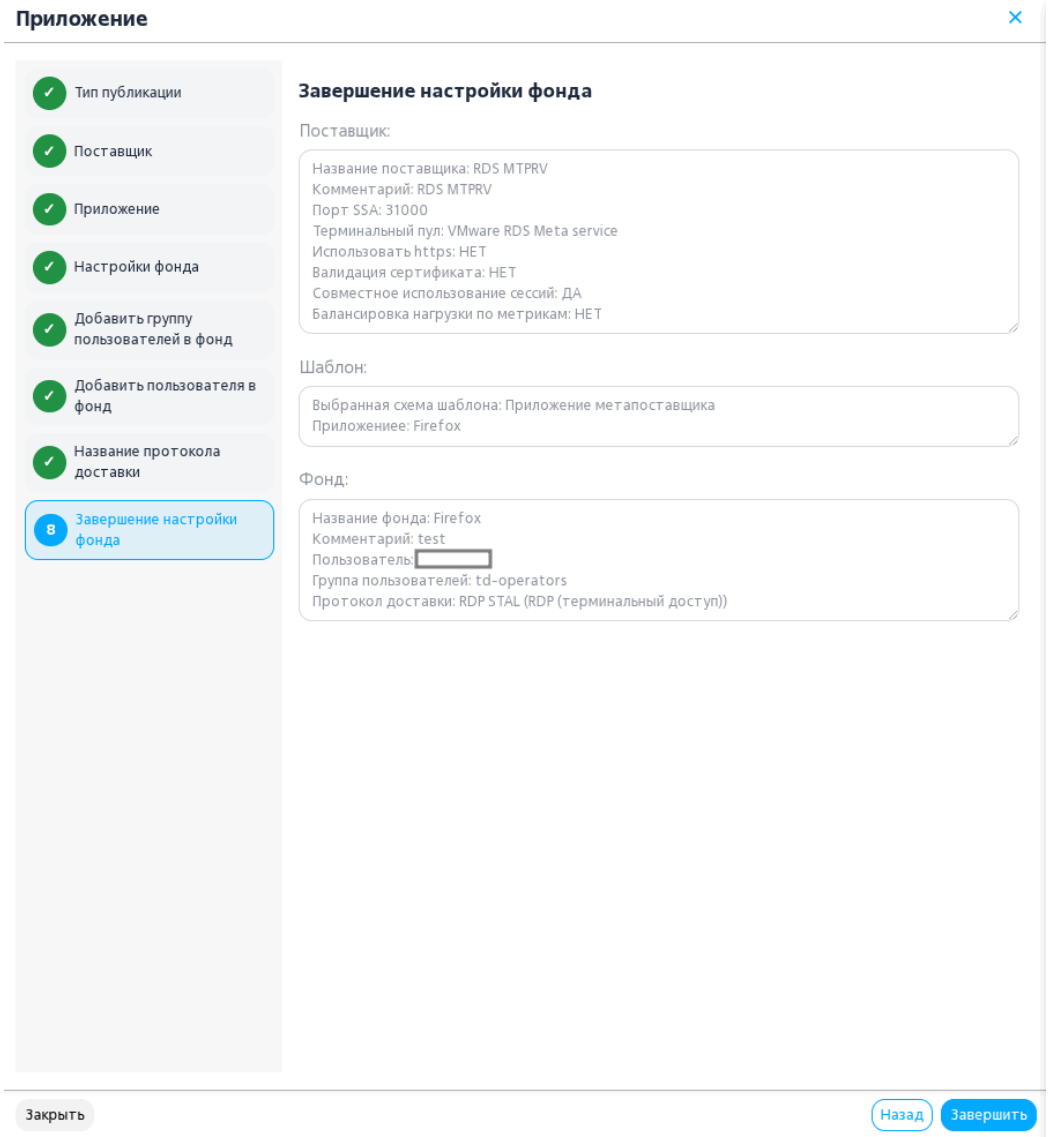


Рисунок 74. Завершение настройки фонда

После успешного завершения работы мастера публикации информация о создании фонда, добавленных пользователях и их группах, протоколах доставки будет отображена в журнале фонда. Для просмотра журнала нужно перейти на страницу «Рабочие места - Фонды», выбрать наименование фонда и перейти во вкладку «Журнал».

Добавление фонда автономных машин

Фонд автономных машин используется для публикации фонда, основанного на шаблонах автономных машин.

Для добавления фонда автономных машин следует перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Создать]**, выбрать тип мастера публикации «Автономные машины».

Откроется мастер публикации фонда (см. рисунок Базовые настройки фонда в Мастере публикации). Необходимо заполнить параметры, указанные в таблице (см. таблицу Базовые настройки фонда), и нажать экранную кнопку **[Далее]**.

При нажатии экранной кнопки **[Закрыть]** или клавиши **<Esc>**, или иконки «Крестик» на любом из этапов работы произойдет закрытие мастера без сохранения настроек.

При создании фонда автономных машин нужно следовать правилу «Один шаблон - один фонд». Создание фондов с одинаковыми шаблонами не допускается.

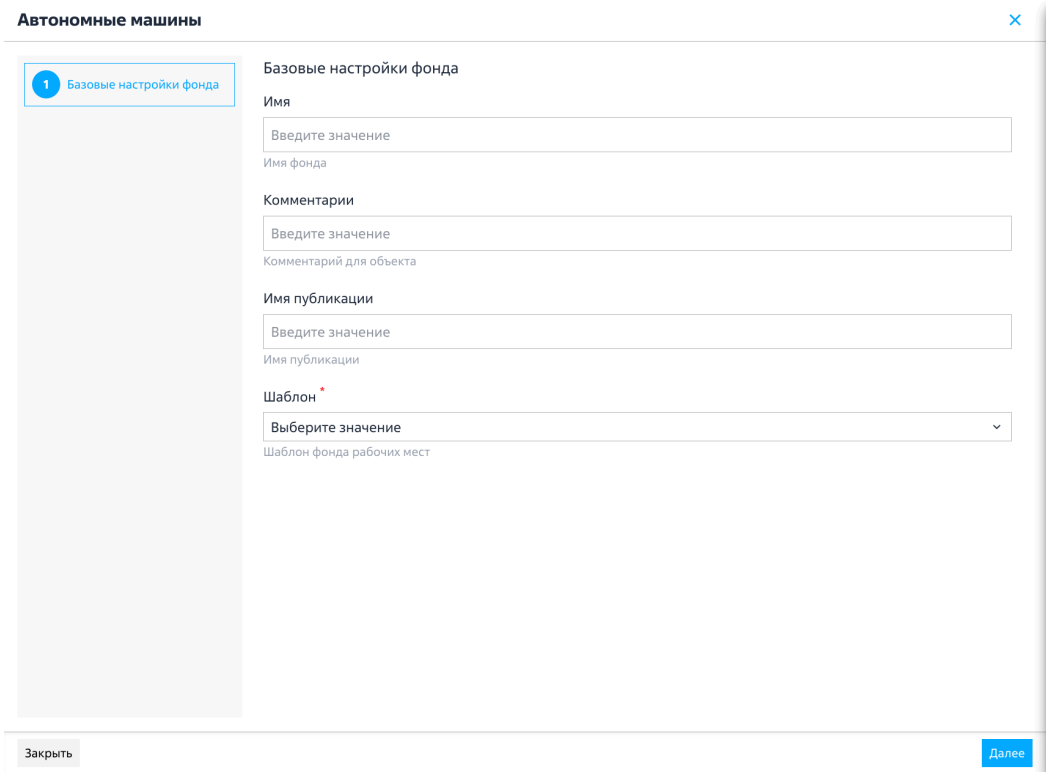


Рисунок 75. Базовые настройки фонда в Мастере публикации

Таблица 112. Базовые настройки фонда

Параметр	Описание
«Имя»	Текстовое наименование фонда. Параметр обязателен для заполнения
«Комментарии»	Информационное сообщение, используемое для описания назначения фонда
«Имя публикации»	Текстовое наименование публикации. Параметр применяется для георасределенной установки и позволяет отображать однообразные фонды в виде единого ярлыка в компоненте «Клиент». Для этого на каждой из установок компонента «Универсальный диспетчер» в базовых настройках фонда следует задавать идентичное значение параметра. Параметр обязателен для заполнения
«Шаблон»	Шаблон автономных машин, который будет использоваться при создании фонда. Выбор шаблонов, не относящихся к автономным машинам, не допускается. Параметр обязателен для заполнения

Если обязательное поле не было заполнено или есть ошибка при заполнении, оно будет подсвечено красным цветом и будет выведено сообщение об ошибке после нажатия экранной кнопки **[Далее]**. Индикация цветом и сообщение не исчезнут после заполнения поля.

Далее будет выполнен переход на следующий шаг настройки мастера публикации фонда (см. рисунок Дополнительные настройки фонда Мастера публикации), в котором нужно заполнить параметры, указанные в таблице (см. таблицу Дополнительные настройки фонда).

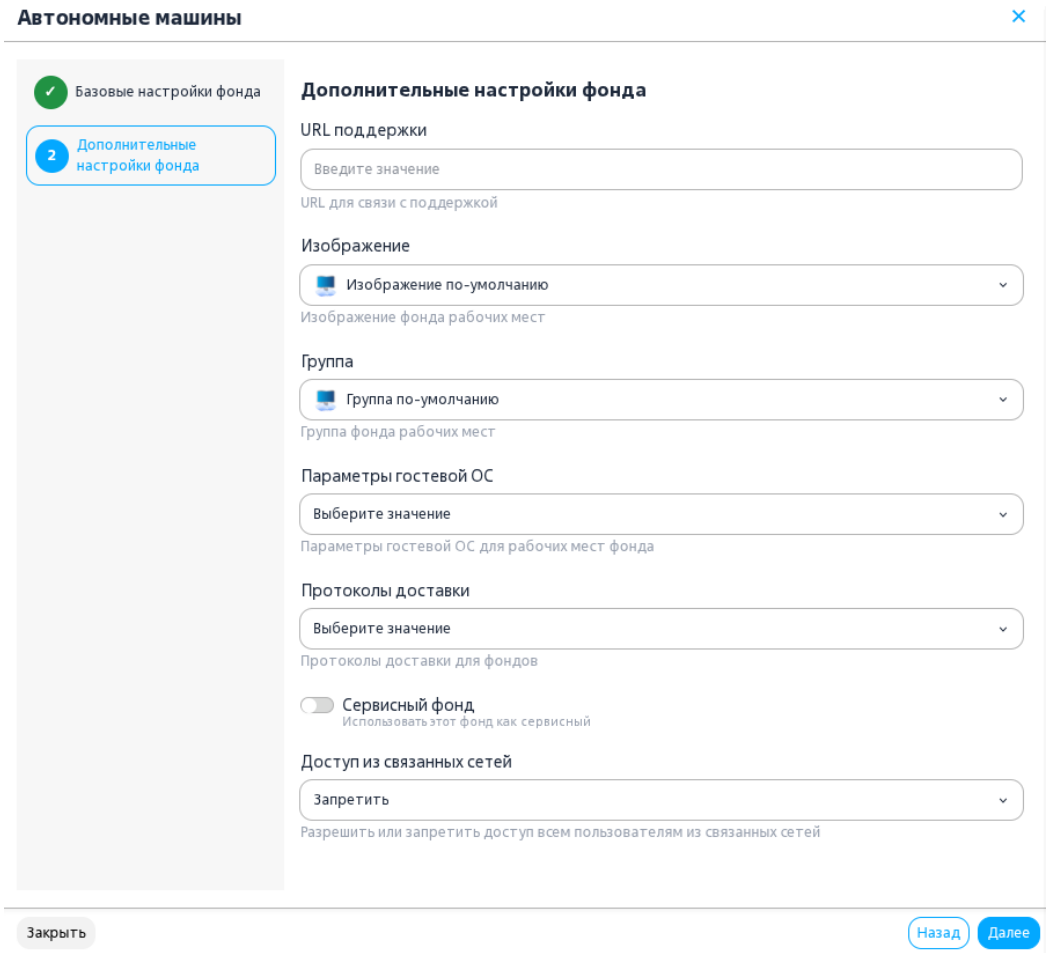


Рисунок 76. Дополнительные настройки фонда Мастера публикации

Таблица 113. Дополнительные настройки фонда

Параметр	Описание
«URL поддержки»	URL для связи с технической поддержкой. Адрес должен соответствовать стандарту кодирования URI. В случае задания некорректного URL, графический элемент для обращения в техническую поддержку в компоненте «Клиент» будет недоступен. Примеры схем для задания URL: • `http(s)://termidesk.local/support`; • `ws(s)://chat.termidesk.local`; • `file:///home/support/help.html`; • `mailto:support@termidesk.local`
«Изображение»	Графическое представление фонда
«Группа»	Группа РМ, в которой будет отображаться созданный фонд
«Параметры гостевой ОС»	Параметры конфигурации гостевой ОС автономных машин, которые будут использованы при создании фонда. Выбор параметров гостевой ОС, не относящихся к автономным машинам, не допускается
«Протоколы доставки»	Один или несколько протоколов доставки, которые будут доступны для фонда

Параметр	Описание
«Сервисный фонд»	Активация использования фонда как **сервисного** для Метапоставщика
«Доступ из связанных сетей»	Управление доступом пользователей из связанных сетей. Сети указываются в настройках фонда РМ после его создания. Возможные значения: • «Разрешить» - все пользователи из указанных сетей смогут подключаться к фонду РМ; • «Запретить» - всем пользователям из указанных сетей будет запрещено подключение к фонду РМ

После заполнения параметров нажать экранную кнопку **[Далее]**.

В следующем окне завершить настройку фонда, нажав экранную кнопку **[Завершить]** (см. рисунок Успешное завершение настройки публикации фонда). При успешном создании фонда в этом же окне отобразится сообщение «Фонд успешно создан!». Для выхода из мастера публикации нужно нажать экранную кнопку **[Закрыть]**.

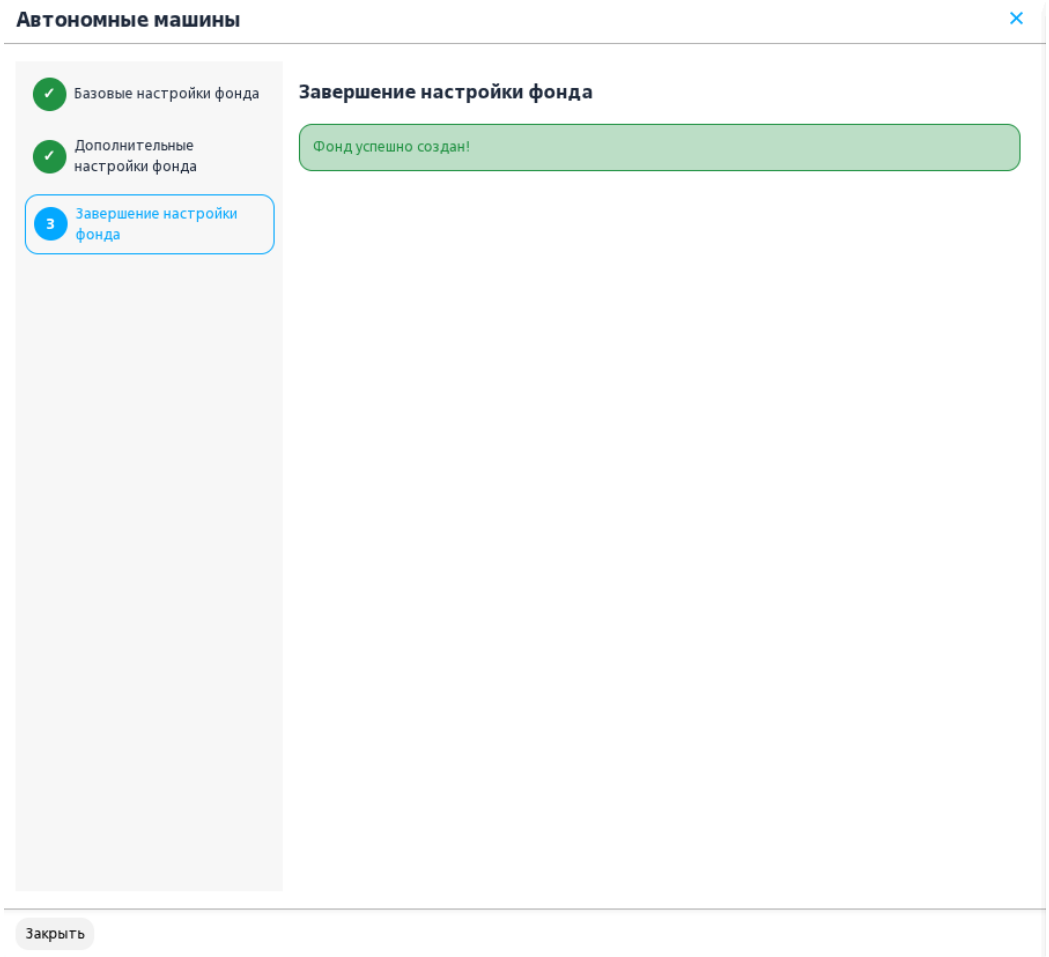


Рисунок 77. Успешное завершение настройки публикации фонда

Добавление составного фонда

Составной фонд в Termidesk VDI - абстракция, позволяющая объединить ВМ различных конфигураций (фонды РМ, фонды-участники) в единый фонд.

При использовании составного фонда требуется все управляющие действия (например, перевод в режим техобслуживания) выполнять в нем.

Преимущества использования составного фонда:

- предоставление пользователю, подключенного через компонент «Клиент» (или «Портал пользователя»), единого фонда. Фонды-участники при этом не будут отображаться пользователю;
- возможность использования в функционале Метапоставщика, что позволяет объединить ресурсы нескольких фондов.

Требования и рекомендации для использования составного фонда:

- для всех фондов-участников должна использоваться одинаковая гостевая ОС;
- для всех фондов-участников должны использоваться одинаковые службы каталогов, если РМ вводится в домен;
- для всех фондов-участников должны использоваться одинаковые параметры гостевых ОС;
- в параметрах всех фондов-участников не должны указываться протоколы доставки. Протоколы доставки задаются в составном фонде;
- в параметрах всех фондов-участников не должны указываться группы пользователей или пользователи. Группы и пользователи задаются в составном фонде;
- в параметрах всех фондов-участников не должны указываться сети. Сети задаются в составном фонде;
- в параметрах всех фондов-участников не должны указываться политики. Политики задаются в составном фонде;
- рекомендуется для всех ВМ в фондах-участниках использовать одинаковую конфигурацию процессора и оперативной памяти.

Особенности использования составного фонда:

- в составном фонде нельзя использовать другой составной фонд или фонд Метапоставщика;
- для удаления составного фонда нужно предварительно изменить его, исключив фонды-участники;
- для изменения параметров фонда-участника нужно:
  - перевести фонд-участник в режим техобслуживания (не требуется, если изменения касаются настроек кеша 1-го и 2-го уровней, режима отладки или настройки максимального количества рабочих мест);
  - удалить его из составного фонда;
  - выполнить изменение параметров;
  - вывести из режима техобслуживания;
  - вернуть его в составной фонд;
- при активации режима техобслуживания для составного фонда все фонды-участники переводятся в этот режим. При этом они перестают участвовать в выдаче РМ;

  Статус «Техобслуживание» не будет отображен для фондов-участников!

- для фондов-участников станут недоступны элементы, задающиеся только в составном фонде. Например, экранная кнопка **[Политики]** и вкладки в свойствах фонда: «Протоколы доставки», «Сети», «Пользователи и группы»;
- при активации расписания для составного фонда все фонды-участники задействуются в этом расписании.

Для добавления фонда РМ следует перейти «Рабочие места - Фонды» и нажать экранную

кнопку **[Создать]**, выбрать тип мастера публикации «Составной фонд».

Откроется мастер публикации фонда (см. рисунок Базовые настройки фонда в Мастере публикации). Необходимо заполнить параметры, указанные в таблице (см. таблицу Базовые настройки фонда), и нажать экранную кнопку **[Далее]**.

При нажатии экранной кнопки **[Закрыть]** или клавиши **<Esc>**, или иконки «Крестик» на любом из этапов работы произойдет закрытие мастера без сохранения настроек.

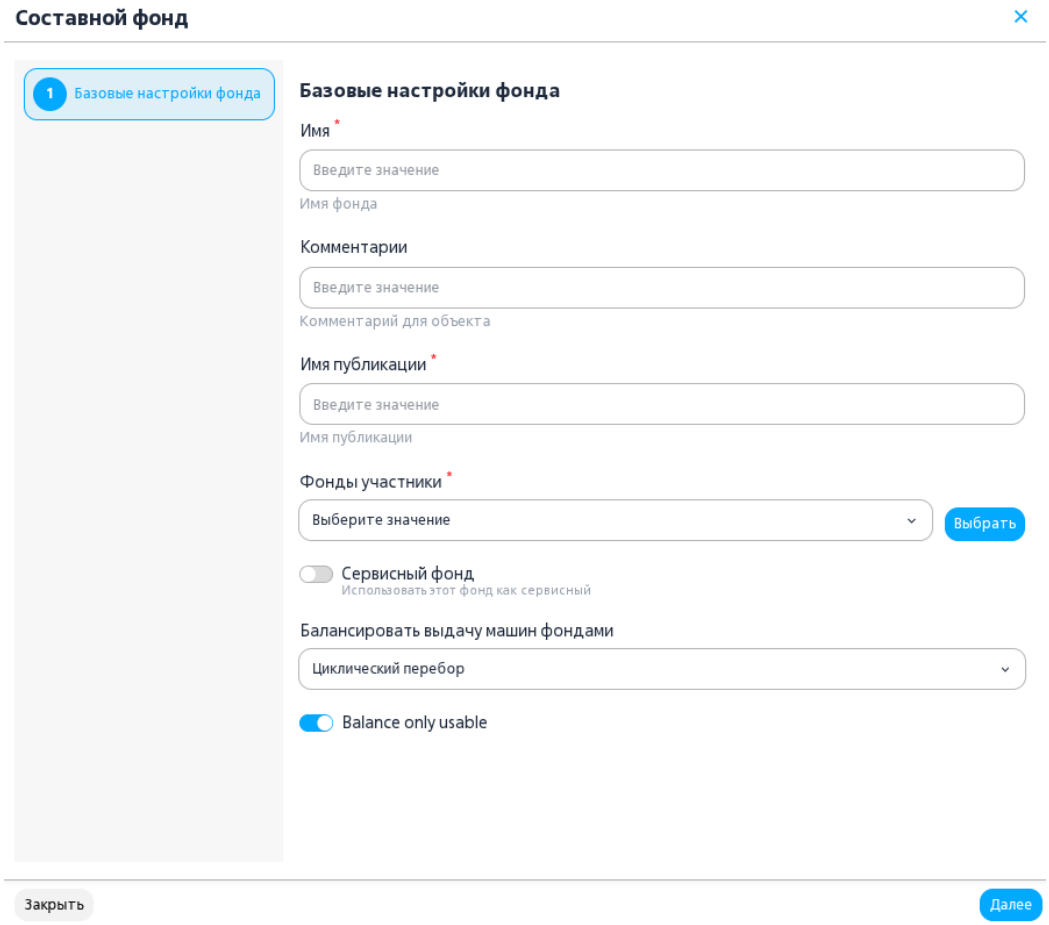


Рисунок 78. Базовые настройки фонда в Мастере публикации

Таблица 114. Базовые настройки фонда

Параметр	Описание
«Имя»	Текстовое наименование фонда. Наименование может содержать только буквы латинского алфавита, цифры, знаки «-» (дефис), пробел и «_» (нижнее подчеркивание). Параметр обязателен для заполнения
«Комментарии»	Информационное сообщение, используемое для описания назначения фонда

Параметр	Описание
«Имя публикации»	Текстовое наименование публикации. Параметр применяется для георасределенной установки и позволяет отображать однообразные фонды РМ в виде единого ярлыка в компоненте «Клиент». Для этого на каждой из установок компонента «Универсальный диспетчер» в базовых настройках фонда следует задавать идентичное значение параметра. Параметр обязателен для заполнения

«Фонды участники»	Выбор фондов РМ из списка, которые будут использоваться в составном фонде.
	
	Особенности:
	
	• в этом списке доступны фонды в статусе «Техобслуживание»;
	• в этом списке недоступны:
	  фонды, являющиеся либо частью Метапоставщика, либо частью другого составного фонда;
	  фонды, у которых есть пользователи или группы;
	  фонды, у которых есть протокол доставки;
	  фонды, у которых есть сети

«Сервисный фонд»	Активация использования фонда как **сервисного** для Метапоставщика

Параметр	Описание
«Балансировать выдачу машин фондами»	Выбор алгоритма выдачи РМ из фондов-участников. Возможные значения: • «Нет» - балансировка отключена. РМ выдаются из фондов-участников последовательно: сначала все РМ из первого по списку фонда, затем второго и т.д. Если используется параметр «Балансировать только между фондами с действительными машинами», то пользователь получит РМ из первого найденного фонда с действительными РМ; • «Циклический перебор» (по умолчанию) - РМ выдаются по схеме «round-robin»: сначала выбирается последний использованный фонд, затем следующий и т.д. Если используется параметр «Балансировать только между фондами с действительными машинами», то пользователь получит РМ из первого найденного фонда с действительными РМ; • «По наименьшему количеству выданных машин» - РМ выдаются по схеме «least connection»: выбирается фонд с наименьшим количеством выданных РМ. Если используется параметр «Балансировать только между фондами с действительными машинами», то пользователь получит РМ из фонда с действительными РМ и с наименьшим общим числом выданных РМ (назначенных пользователям). Статус РМ отфильтрует непригодные фонды, но не повлияет на расчет выданных РМ; • «По наименьшей относительной загрузке» - РМ выдаются из фонда с наименьшей нагрузкой: отношением числа выданных РМ (назначенных пользователям) к значению свойства фонда «Максимальное количество рабочих мест». Расчет нагрузки выполняется на каждый запрос по актуальным данным и не кешируется. Если используется параметр «Балансировать только между фондами с действительными машинами», то пользователь получит РМ из первого найденного фонда с действительными РМ и с наименьшей нагрузкой
«Балансировать только между фондами с действительными машинами»	Фильтрация РМ из полученного списка фондов-участников по статусу «Действительный». Если таких РМ несколько, то пользователю будет выдано то, что имеет наиболее раннюю дату создания. При использовании работает совместно с параметром «Балансировать выдачу машин фондами»: сначала обрабатывается фильтрация по статусу «Действительный», затем выполняется балансировка по выбранному алгоритму

После заполнения параметров нажать экранную кнопку **[Далее]**.

Если обязательное поле не было заполнено или есть ошибка при заполнении, оно будет подсвечено красным цветом и будет выведено сообщение об ошибке после нажатия экранной кнопки **[Далее]**. Индикация цветом и сообщение не исчезнут после корректного заполнения поля.

Далее будет выполнен переход на следующий шаг настройки мастера публикации фонда

(см. рисунок Дополнительные настройки фонда Мастера публикации), в котором нужно заполнить параметры, указанные в таблице (см. таблицу Дополнительные настройки фонда).

Поскольку во время перехода выполняется отправка данных на сервер, возможна ситуация, что при возвращении на предыдущий шаг появится сообщение об ошибке, если параметр «Протоколы доставки» не был заполнен. Отправка данных на сервер происходит всегда при переходе между шагами, кроме перехода назад с завершающего этапа.

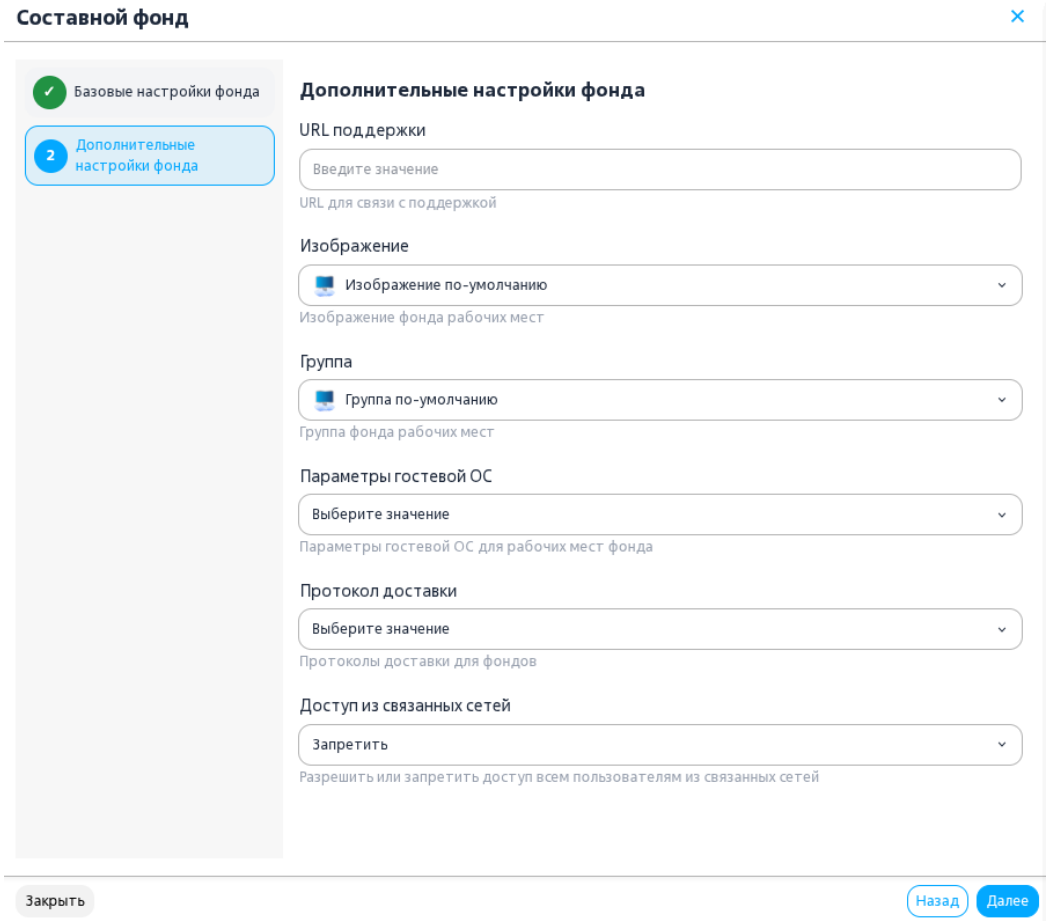


Рисунок 79. Дополнительные настройки фонда Мастера публикации

Таблица 115. Дополнительные настройки фонда

Параметр	Описание
«URL поддержки»	URL для связи с технической поддержкой. Адрес должен соответствовать стандарту кодирования URI. В случае задания некорректного URL, графический элемент для обращения в техническую поддержку в компоненте «Клиент» будет недоступен. Примеры схем для задания URL: • `http(s)://termidesk.local/support`; • `ws(s)://chat.termidesk.local`; • `file:///home/support/help.html`; • `mailto:support@termidesk.local`

Параметр	Описание
«Изображение»	Графическое представление фонда
«Группа»	Группа рабочих мест, в которой будет отображаться созданный фонд
«Параметры гостевой ОС»	Параметры конфигурации гостевой ОС, которые используются для РМ
«Протоколы доставки»	Один или несколько протоколов доставки, которые будут доступны для фонда
«Доступ из связанных сетей»	Управление доступом пользователей из связанных сетей. Сети указываются в настройках фонда РМ после его создания. Параметр недоступен, если создается сервисный фонд. Возможные значения: • «Разрешить» - все пользователи из указанных сетей смогут подключаться к фонду РМ; • «Запретить» (по умолчанию) - всем пользователям из указанных сетей будет запрещено подключение к фонду РМ

После заполнения параметров нажать экранную кнопку **[Далее]**.

В следующем окне завершить настройку фонда, нажав экранную кнопку **[Завершить]**. При успешном создании фонда в этом же окне отобразится сообщение «Фонд успешно создан!» (см. рисунок Успешное завершение настройки публикации фонда). Для выхода из мастера публикации нужно нажать экранную кнопку **[Закрыть]**.

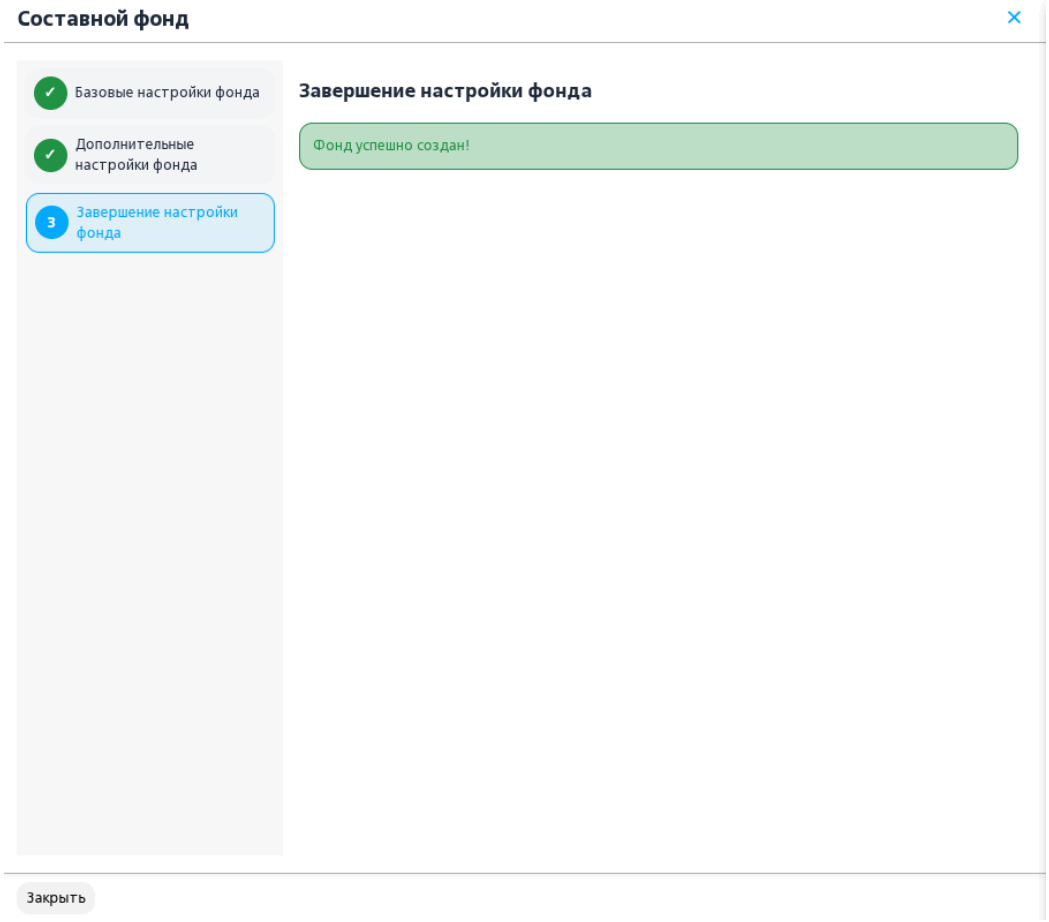


Рисунок 80. Успешное завершение настройки публикации фонда

Добавление фонда сетевой загрузки

Фонд сетевой загрузки используется для публикации фонда, основанного на шаблонах РМ «Сетевая загрузка (MAC)» (см. подраздел **Технология бездисковой (сетевой) загрузки**).

Для добавления фонда следует перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Создать]**, выбрать тип мастера публикации «Сетевая загрузка».

Откроется мастер публикации фонда. Необходимо заполнить параметры, указанные в таблице (см. таблицу Базовые настройки фонда), и нажать экранную кнопку **[Далее]**.

При нажатии экранной кнопки **[Закрыть]** или клавиши **<Esc>**, или иконки «Крестик» на любом из этапов работы произойдет закрытие мастера без сохранения настроек.

При создании фонда нужно следовать правилу «Один шаблон - один фонд». Создание фондов с одинаковыми шаблонами не допускается.

Таблица 116. Базовые настройки фонда

Параметр	Описание
«Имя»	Текстовое наименование фонда. Параметр обязателен для заполнения
«Комментарии»	Информационное сообщение, используемое для описания назначения фонда
«Имя публикации»	Текстовое наименование публикации. Параметр применяется для георасределенной установки и позволяет отображать однообразные фонды в виде единого ярлыка в компоненте «Клиент». Для этого на каждой из установок компонента «Универсальный диспетчер» в базовых настройках фонда следует задавать идентичное значение параметра. Параметр обязателен для заполнения
«Шаблон»	Шаблон РМ сетевой загрузки, который будет использоваться при создании фонда. Выбор шаблонов, не относящихся к сетевой загрузке, не допускается. Параметр обязателен для заполнения

Если обязательное поле не было заполнено или есть ошибка при заполнении, то будет выведено сообщение об ошибке после нажатия экранной кнопки **[Далее]**.

Далее будет выполнен переход на следующий шаг настройки мастера публикации фонда, в котором нужно заполнить параметры, указанные в таблице (см. таблицу Дополнительные настройки фонда).

Таблица 117. Дополнительные настройки фонда

Параметр	Описание
«URL поддержки»	URL для связи с технической поддержкой. Адрес должен соответствовать стандарту кодирования URI. В случае задания некорректного URL, графический элемент для обращения в техническую поддержку в компоненте «Клиент» будет недоступен. Примеры схем для задания URL: • `http(s)://termidesk.local/support`; • `ws(s)://chat.termidesk.local`; • `file:///home/support/help.html`; • `mailto:support@termidesk.local`
«Изображение»	Графическое представление фонда
«Группа»	Группа РМ, в которой будет отображаться созданный фонд
«Параметры гостевой ОС»	Параметры конфигурации гостевой ОС автономных машин, которые будут использованы при создании фонда. Выбор параметров гостевой ОС, не относящихся к автономным машинам, не допускается
«Протоколы доставки»	Один или несколько протоколов доставки, которые будут доступны для фонда
«Доступ из связанных сетей»	Управление доступом пользователей из связанных сетей. Сети указываются в настройках фонда РМ после его создания. Возможные значения: • «Разрешить» - все пользователи из указанных сетей смогут подключаться к фонду РМ; • «Запретить» (по умолчанию) - всем пользователям из указанных сетей будет запрещено подключение к фонду РМ

После заполнения параметров нажать экранную кнопку **[Далее]**.

В следующем окне завершить настройку фонда, нажав экранную кнопку **[Завершить]**. При успешном создании фонда в этом же окне отобразится сообщение «Фонд успешно создан!». Для выхода из мастера публикации нужно нажать экранную кнопку **[Закрыть]**.

Управление параметрами фонда РМ

Политики фонда РМ

Политики фонда РМ переопределяют настройки глобальных политик и устанавливают индивидуальные настройки доступа и использования ресурсов пользователями конкретного фонда РМ.

Список политик представлен в подразделе **Политики**. Доступны следующие действия над политиками фонда:

- просмотр политик. Для этого следует перейти «Рабочие места - Фонды», выбрать нужный фонд РМ, нажать экранную кнопку **[Политики]**;
- редактирование значения. Для этого нужно выбрать политику, нажать на значение политики или графический элемент ;

- сброс значения до значения по умолчанию. Для этого нужно выбрать политику, нажать на значение политики или графический элемент , затем нажать экранную кнопку **[Очистить]**.

> Во время обновления распределенной или отказоустойчивой конфигурации установки изменение политик нужно проводить после обновления на новую версию всех узлов Termidesk VDI.
>
> Если на ВРМ есть сессия пользователя, то политика применится после перезагрузки ВМ. Для терминального сервера перезагрузка обязательна!

Особенности применения политик:

- если при подключении к РМ пользователь использует ПО Termidesk Viewer, то администратор должен включить соответствующие политики фонда РМ для перенаправления ресурсов;
- политики, применимые к протоколу RDP, запрашиваются компонентом «Агент виртуального рабочего места» перед подключением пользователя к ВРМ по указанному протоколу и обновляются в реестре ОС в случае, если это гостевая ОС Microsoft Windows.

> Политики фонда РМ и групповые политики контроллера домена MS AD управляют одними и теми же ключами реестра. Поэтому рекомендуется использовать либо политики фермы Termidesk VDI, либо политики контроллера домена MS AD (но не из двух источников сразу). Для сохранения возможности управления параметрами подключения средствами контроллера домена MS AD следует назначать политике фонда РМ значение «Не задано».
>
> Действия по перезагрузке ОС после обновления реестра управляются компонентом «Агент виртуального рабочего места» через параметр `HKLMReboot`. Если параметр отсутствует, то:
>
> - для Агента ВРМ версии ниже 6.1 ОС будет перезагружаться после обновления реестра;
> - для Агента ВРМ версии 6.1 и выше ОС не будет перезагружаться после обновления реестра.

Назначение групп доступа фонду РМ

Фонду РМ можно назначать группы пользователей домена аутентификации, которым этот фонд будет доступен.

Для добавления новой группы к фонду РМ следует перейти «Рабочие места - Фонды» и в сводной таблице в столбце «Название» нажать на наименование фонда РМ.

На открывшейся странице в разделе «Группы» нужно нажать экранную кнопку **[Создать]**. В окне добавления объекта из выпадающего списка выбрать необходимый домен аутентификации, а затем требуемую для него группу.

> Для выбора будут доступны те домены аутентификации, для которых в параметре «Субъекты» задано значение «Пользователи» или «Все».

Для удаления группы из фонда используется экранная кнопка **[Удалить]**.

> Добавление группы пользователей домена будет возможно только в том

случае, если указанная группа существует в службе каталога и добавлена в домен аутентификации в Termidesk VDI.

Назначение пользователей фонду РМ

Фонду РМ можно назначать пользователей, которым этот фонд будет доступен.

Для добавления нового пользователя к фонду РМ следует перейти «Рабочие места - Фонды» и в сводной таблице в столбце «Название» нажать на наименование фонда. На открывшейся странице в разделе «Пользователи» нажать на экранную кнопку **[Создать]**. В форме добавления пользователя будет доступен его поиск в выбранном домене аутентификации.

Для выбора будут доступны те домены аутентификации, для которых в параметре «Субъекты» задано значение «Пользователи» или «Все».

Добавление пользователя домена будет доступно только в том случае, если пользователь хотя бы один раз осуществил вход в «Портал пользователя» под своей учетной записью.

Назначение протоколов фонду РМ

Фонду РМ можно назначать доступные для него протоколы доставки как на этапе настройки при помощи «Мастера публикации фонда», так и после.

Для добавления нового протокола доставки фонду РМ следует перейти «Рабочие места - Фонды» и в сводной таблице в столбце «Название» нажать на наименование фонда.

На открывшейся странице в разделе «Протоколы доставки» нужно нажать экранную кнопку **[Создать]**. В окне добавления объекта из выпадающего списка выбрать необходимый протокол доставки.

Добавление протокола доставки в фонд ВРМ будет доступно только в том случае, если настроен хотя бы один протокол доставки в «Рабочие места - Протоколы доставки».

Назначение сетей фонду РМ

Фонду РМ нужно назначить одну или несколько сетей, каждая из которых задает IP-адреса или диапазоны IP-адресов пользователей.

Отображение списка будет доступно администратору, если у него есть пользовательское разрешение «Управление списками сетей фондов рабочих мест».

Назначение сетей недоступно для **сервисного** фонда Метапоставщика.

Для добавления сетей фонду РМ следует:

- перейти «Рабочие места - Фонды» и в сводной таблице в столбце «Название» нажать на наименование фонда РМ;
- на открывшейся странице в разделе «Сети» нажать экранную кнопку **[Создать]**;
- в окне добавления объекта из выпадающего списка выбрать необходимую сеть и нажать экранную кнопку **[Сохранить]**. Для выбора будут доступны сети, предварительно заданные на странице «Рабочие места - Сети».

При этом:

- если в свойствах фонда параметру «Доступ из связанных сетей» задано значение «Разрешить», то подключение к фонду будет разрешено только для перечисленных на вкладке «Сети» диапазонов сетей (реализация «белого» списка доступа);
- если в свойствах фонда параметру «Доступ из связанных сетей» задано значение «Запретить», то подключение к фонду будет запрещено для перечисленных на вкладке «Сети» диапазонов сетей (реализация «черного» списка доступа);
- если ни одна сеть не будет задана, то подключение к фонду будет разрешено для всех сетей.

Для сокрытия недоступных пользователю фондов используется системный параметр «Скрывать недоступные ресурсы» (см. подраздел **Управление параметрами компонента «Клиент»**).

Для удаления сети из фонда используется экранная кнопка **[Удалить]**.

Для фондов, созданных в Termidesk VDI до версии 6.0, по умолчанию действует значение «Запретить» для параметра «Доступ из связанных сетей». Для изменения параметра нужно выбрать фонд на странице «Рабочие места - Фонды» и нажать экранную кнопку **[Изменить]**.

Если списки доступа заданы как на уровне фонда, так и на уровне протоколов доставки, то:

- в первую очередь проверка доступности будет происходить на уровне фонда, во вторую очередь проверяется ограничение сетей в протоколах доставки;
- будет применено наиболее строгое ограничение:
  - если в фонде РМ задан «белый» список с определенным IP-адресом, и на уровне протокола доставки задан «черный» список доступа, то фонд не будет доступен;
  - если в фонде РМ задан «белый» список, но в списке нет нужного IP-адреса, и на уровне протокола доставки задан «белый» список доступа, то фонд не будет доступен;
  - если в фонде РМ задан «белый» список, в котором есть нужный IP-адрес, и на уровне протокола доставки задан «белый» список доступа, то фонд будет доступен.

Назначение скриптов в фонде РМ

Для назначения скрипта фонду РМ нужно перейти «Рабочие места - Фонды» и в сводной таблице в столбце «Название» нажать на наименование фонда.

На открывшейся странице в разделе «Скрипты» нужно нажать экранную кнопку **[Создать]**.

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для назначения скрипта фонду РМ). Для сохранения параметров нужно нажать экранную кнопку **[Сохранить]**.

Таблица 118. Данные для назначения скрипта фонду РМ

Параметр	Описание
«Скрипт»	Выбор скрипта из списка
«Описание»	Информационное сообщение с описанием назначения скрипта

Параметр	Описание
«Выполнение»	Событие, при котором выполняется скрипт на РМ. Возможные значения: • «При первом включении РМ»; • «При каждом включении РМ»; • «При входе пользователя (в контексте пользователя)»; • «При входе пользователя»; • «При выходе пользователя (в контексте пользователя)»; • «При выходе пользователя»; • «При каждом выключении РМ»
«Приоритет»	Приоритет выполнения скрипта
«Активен»	Флаг использования скрипта в фонде

Назначение тегов в фонду РМ

Для назначения тегов фонду РМ нужно перейти «Рабочие места - Фонды», пометить фонд и нажать экранную кнопку **[Теги]**. Далее в поле «Теги» выбрать теги из списка (см. рисунок Назначение тегов фонду РМ). Для поиска тега нужно ввести полное или частичное наименование тега. Для удаления тега из списка назначенных тегов нужно нажать на иконку «Крестик» в графическом блоке тега.

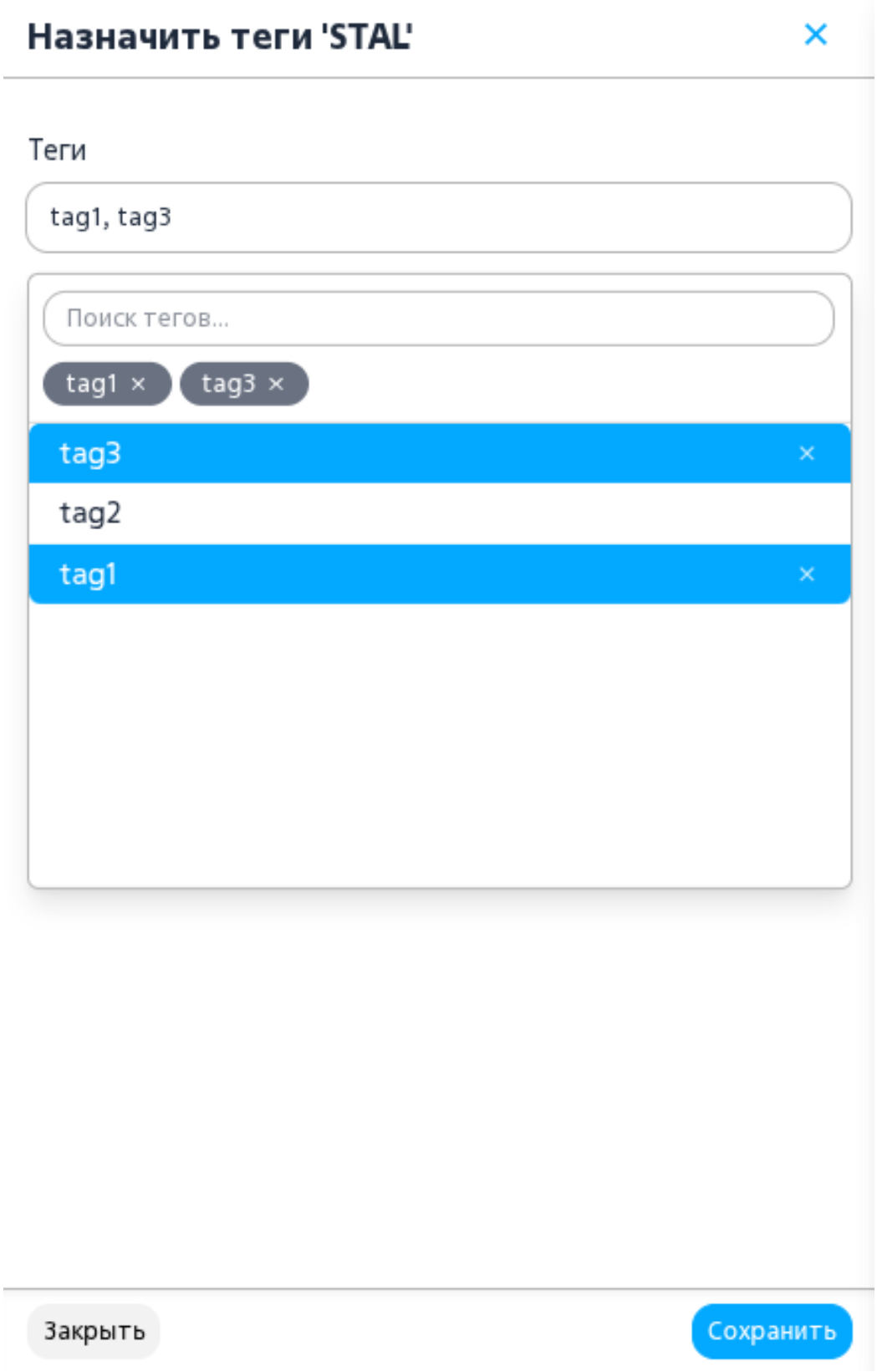


Рисунок 81. Назначение тегов фонду РМ

Объединение фондов в группы РМ

Группы РМ отображаются как самостоятельные разделы в интерфейсе пользователя. Группы РМ являются логическим признаком, по которому можно объединять отображение фондов РМ для пользователей.

Для добавления группы администратору Termidesk VDI следует перейти «Рабочие места - Группы рабочих мест» и нажать экранную кнопку **[Создать]**. Затем заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для объединения фондов ВРМ в группы).

Таблица 119. Данные для объединения фондов ВРМ в группы

Параметр	Описание
«Название»	Текстовое наименование группы РМ
«Комментарий»	Информационное сообщение, используемое для описания назначения группы РМ
«Приоритет»	Преимущество использования группы РМ в «Портале пользователя»

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Для редактирования группы РМ в Termidesk VDI нужно пометить необходимую группу и нажать экранную кнопку **[Изменить]**.

Для удаления группы РМ в Termidesk VDI нужно пометить необходимую группу и нажать экранную кнопку **[Удалить]**.

Режим техобслуживания фонда РМ

Режим техобслуживания фонда для ВРМ

Режим техобслуживания фонда для ВРМ - это запрет пользователям подключаться (создавать новую сессию) и/или переподключаться повторно в существующую сессию фонда РМ. Этот режим предназначен для проведения плановых регламентных или аварийных работ, например, когда нужно применить обновления или исправления для гостевых ОС или ВМ и требуется временно прекратить новые подключения к фонду.

Режим техобслуживания может применяться и к отдельным ВМ в выбранном фонде.

Для перевода фонда в режим техобслуживания следует перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Техобслуживание]** с выбором из выпадающего списка значения «Включить» (см. рисунок Перевод фонда ВРМ в режим техобслуживания). Затем подтвердить включение режима.

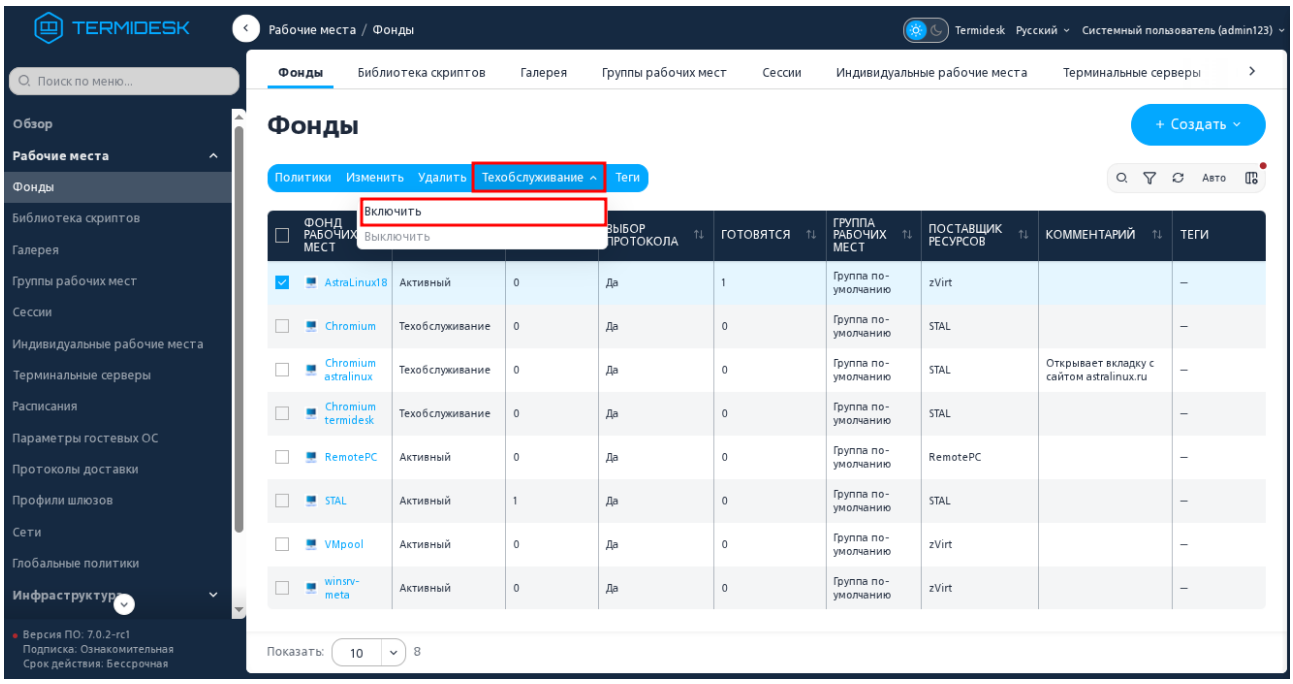


Рисунок 82. Перевод фонда ВРМ в режим техобслуживания

Состояние режима техобслуживания будет отображено в столбце «Статус» списка фондов.

Для отключения режима техобслуживания нужно выбрать фонд, нажать экранную кнопку **[Техобслуживание]**, а затем выбрать из выпадающего списка значение «Выключить». По завершении техобслуживания фонд может быть снова использован для размещения ВРМ.

Режим техобслуживания фонда терминального сервера

Режим техобслуживания фонда - это запрет пользователям подключаться (создавать новую сессию) и/или переподключаться повторно в существующую сессию фонда терминального сервера. Этот режим предназначен для проведения плановых регламентных или аварийных работ, например, когда нужно применить обновления или исправления для терминального сервера и требуется временно прекратить новые подключения к фонду.

Режим техобслуживания может применяться и к отдельному терминальному серверу в выбранном фонде.

Для перевода фонда в режим техобслуживания следует перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Техобслуживание]** с выбором из выпадающего списка значения «Включить» (см. рисунок Перевод фонда терминального сервера в режим техобслуживания). Затем подтвердить включение режима.

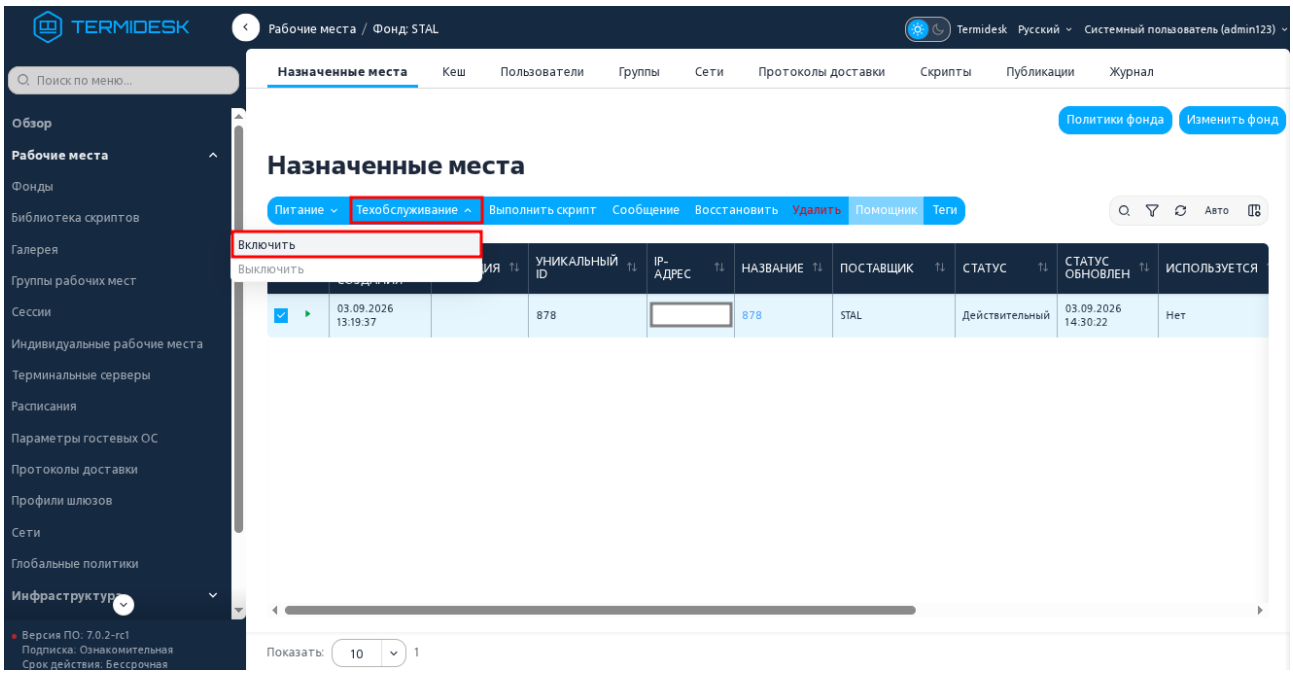


Рисунок 83. Перевод фонда терминального сервера в режим техобслуживания

Состояние режима техобслуживания будет отображено в столбце «Статус» списка фондов.

Для отключения режима техобслуживания нужно выбрать фонд терминального сервера, нажать экранную кнопку **[Техобслуживание]**, а затем выбрать из выпадающего списка значение «Выключить». По завершении техобслуживания фонд может быть снова использован.

Публикация фонда РМ

Публикация фонда РМ позволяет создать РМ внутри фонда в соответствии с заданным в настройках количеством или обновить уже имеющиеся внутри фонда РМ и подготовить их для дальнейшего использования.

Для публикации фонда РМ следует перейти «Рабочие места - Фонды» и в сводной таблице в столбце «Название» выбрать наименование фонда.

На открывшейся странице в разделе «Публикации» нажать экранную кнопку **[Создать]**. В окне создания публикации нажать экранную кнопку **[Создать]** для запуска задачи обновления фонда РМ.

При этом:

- для фондов, созданных на основе поставщиков ресурсов VMware vSphere, oVirt, zVirt, «РЕД Виртуализация» при публикации также доступен выбор снимка ВМ (снапшота), который будет использован для формирования РМ;
- для поставщиков ресурсов VMware vSphere, oVirt, zVirt, «РЕД Виртуализация» все наименования снапшотов будут содержать дату и время их создания. Активный снапшот будет помечен как «Active VM»;
- при публикации фонда РМ будет доступен выбор действия, применимого к учетной записи РМ. Описание действий приведено в параметре «Действие с учетной записью рабочего места» подраздела **Общие системные параметры Termidesk VDI**.

Публикация фонда РМ применима также к фонду автономных машин. При перепубликации фонда автономных машин назначенные машины не будут удалены.

Прогресс выполнения публикации будет отображен в этом же разделе. Индикатор прогресса учитывает количество назначенных ВМ (готовых и создаваемых).

Существуют несколько состояний публикации, отражаемых в столбце «Прогресс»:

- «Идёт создание ВМ», индикация зеленым цветом со статусом «Машин в прогрессе» - начало процесса публикации (см. рисунок Индикация прогресса выполнения публикации со статусом «Идет создание ВМ»);
- «Идёт создание ВМ», индикация зеленым цветом со статусом «Готово машин» - непосредственно процесс выполнения публикации, при котором выполняется обращение к поставщику ресурсов и создание ВМ;

Частота обновления прогресса зависит от значения интервала обновления для таблицы «Публикации». Отображаемый цвет и текст зависят от состояния публикации.

Максимальное время ожидания готовности РМ определяется системным параметром «Максимальное время инициализации рабочего места» (см. подраздел **Общие системные параметры Termidesk VDI**).

СОСТОЯНИЕ	ПРОГРЕСС	ПРИЧИНА
Удален	Публикация удалена	-
Действительный	Идёт создание ВМ... Машин в прогрессе: 2 из 2	-
Действительный	Идёт создание ВМ... Готово машин: 1 из 2	-

Рисунок 84. Индикация прогресса выполнения публикации со статусом «Идет создание ВМ»

- «Публикация успешно завершена», индикация зеленым на цветом (см. рисунок Индикация прогресса выполнения публикации со статусом «Публикация успешно завершена») - публикация ВМ в кеше завершена. При выдаче РМ из кеша прогресс вновь вернется на начало процесса публикации;

СОСТОЯНИЕ	ПРОГРЕСС	ПРИЧИНА
Действительный	Публикация успешно завершена ✓ Готово машин: 2 из 2	-

Рисунок 85. Индикация прогресса выполнения публикации со статусом «Публикация успешно завершена»

- «Во время публикации возникла ошибка», индикация серым цветом (см. рисунок Индикация возникновения ошибки при публикации) - процесс публикации завершился с ошибкой, текст ошибки отобразится в столбце «Причина»;

СОСТОЯНИЕ	ПРОГРЕСС	ПРИЧИНА
Ошибка	Во время публикации возникла ошибка Готово машин: 0 из 0	Machine must be in down state to publish it

Рисунок 86. Индикация возникновения ошибки при публикации

- «Публикация удалена», без индикации - информирование о завершении удаления публикации. Получить данное состояние можно при инициировании новой публикации (в таком случае старая публикация удаляется);
- «Публикация частично удалена», без индикации - информирование о частичном

удалении предыдущей публикации. В это состояние публикация переходит, если в фонде есть назначенная и используемая ВМ, и системному параметру «Срок действия устаревшей публикации» задано значение «-1»;

- «Нет машин в кеше 1-го и 2-го уровней», без индикации - информирование об отсутствии ВМ, поддерживаемых в кеше 1-го и 2-го уровней. Это означает, что в настройках фонда параметры «Кеш рабочих мест 1-го уровня» и «Кеш рабочих мест 2-го уровня» не заданы (для них выбрано значение «0»).

Состояние «Нет машин в кеше 1-го и 2-го уровней» не отображается для фонда автономных машин.

Для отмены существующей публикации фонда РМ следует перейти «Рабочие места - Фонды» и в сводной таблице в столбце «Название» выбрать наименование фонда.

На открывшейся странице в разделе «Публикации» нужно нажать экранную кнопку **[Отменить]**.

Отмена публикации возможна, если публикация не находится в статусе «Действительный». Отмена публикации удаляет РМ из фонда, а также параметры конфигурации фонда из Termidesk VDI.

Настройка автоматического подключения к фонду РМ

Автоматическое подключение к фонду РМ

Автоматическое подключение к фонду РМ позволяет компоненту «Клиент» выполнить поиск в сети компонента «Универсальный диспетчер» и реализовать автоматическое подключение к опубликованным фондам.

Для автоматического подключения к фонду РМ после настройки автоматического поиска сервера подключений на узле с установленным «Порталом администратора» следует перейти «Системные параметры - Системные настройки - Общие», активировать параметр «Автозапуск рабочего места» и нажать экранную кнопку **[Сохранить]**.

Для автоматического подключения к фонду РМ нужно настроить группы доступа к фондам так, чтобы пользователям из каждой группы был доступен только один фонд. Если пользователь является членом нескольких групп, и каждой из этих групп предоставлен доступ к отдельному фонду РМ, то пользователь получает доступ к нескольким фондам одновременно. В таком случае, автоматическое подключение невыполнимо. При этом возможность ручного подключения сохраняется.

Для корректной работы автоматического подключения к фонду РМ необходимо выполнить настройку службы DNS.

Настройка автоматического поиска в сети сервера Termidesk

Автоматический поиск сервера подключений позволяет компоненту «Клиент» выполнить поиск в сети компонента «Универсальный диспетчер».

Для этого на DNS-сервере должна быть внесена одна из записей:

- либо запись `daas` типа `TXT` с URL-адресом сервера Termidesk VDI,например: `https://termidesk.domain.local`;
- либо запись `vdi` типа `TXT` с URL-адресом сервера Termidesk VDI, например: `https://termidesk.domain.local`.

Управление расписанием задач

Расписание позволяет составить график задач, которые должны быть выполнены для фондов РМ.

Для отображения списка задач следует перейти «Рабочие места - Расписания». Основные параметры списка приведены в таблице (см. таблицу Параметры списка расписаний). Сортировка списка выполняется по столбцу «Название».

Доступность функционала зависит от типа редакции Termidesk VDI.

Таблица 120. Параметры списка расписаний

Параметр	Описание
«Название»	Текстовое наименование задачи
«Действие»	Действие, выполняемое в рамках расписания
«Фонды»	Список фондов, к которым будет применена задача
«Включено»	Управление выполнением задачи. Возможные значения: • «Да» - выполнять задачу по расписанию; • «Нет» - не выполнять задачу
«Комментарий»	Информационное сообщение, используемое для описания назначения задачи
«Дата активации»	Дата активации задачи
«Время начала»	Время начала очередного действия задачи
«Повтор»	Периодичность выполнения задачи
«Длительность»	Длительность (в минутах) выполнения задачи с момента, заданного в параметре «Время начала»

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;

- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Над созданными задачами можно выполнить следующие действия:

- отредактировать, для этого нажать экранную кнопку **[Изменить]**;
- удалить, для этого нажать экранную кнопку **[Удалить]**. При попытке удаления активной задачи будет отображено сообщение: «Вы уверены, что хотите удалить расписание, которое используется?». Удаление активной задачи производится без учета ее текущего выполнения;
- управлять состоянием задачи, для этого следует выбрать нужный объект в таблице, а затем воспользоваться переключателем в столбце «Включено».

Для добавления задачи в раскрывающемся списке экранной кнопки **[Создать]** следует выбрать тип действия, которое будет выполняться по расписанию:

- «Запуск» - включение ВМ, реализуется через гипервизор;
- «Перезагрузка» - перезагрузка ВМ, реализуется через гипервизор;
- «Перезагрузка (безопасная)» - перезагрузка ВМ, реализуется через гипервизор. В ВМ должен быть установлен пакет инструментов «Guest tools», который предоставляется производителем гипервизора;
- «Пауза» - приостанов ВМ, реализуется через гипервизор;
- «Останов (небезопасный)» - выключение ВМ, реализуется через гипервизор;
- «Выключение (безопасное)» - выключение ВМ, реализуется через гипервизор. В ВМ должен быть установлен пакет инструментов «Guest tools», который предоставляется производителем гипервизора;
- «Восстановление» (откат к снапшоту) - восстановление ВМ из базового снимка (снапшота), реализуется через гипервизор;
- «Техобслуживание» - отправка ВМ на техобслуживание;
- «Выполнение скрипта» - выполнение скрипта на РМ.

Действия, реализуемые через гипервизор, могут быть успешно выполнены только на гипервизорах, поддерживающих указанные команды.

Действие «Восстановление» будет доступно оператору, если у него есть пользовательское разрешение «Восстановление рабочих мест».

Действие «Выполнение скрипта» будет доступно оператору, если у него есть пользовательское разрешение «Выполнение скриптов фондов рабочих мест».

Для корректной работы расписаний для узлов Termidesk VDI должна быть настроена синхронизация времени.

Доступные для заполнения параметры перечислены в столбце «Параметр» следующей таблицы (см. таблицу Параметры расписаний). Для сохранения конфигурации нужно использовать экранную кнопку **[Сохранить]**.

Таблица 121. Параметры расписаний

Параметр	Описание
«Включено»	Управление состоянием задачи. Возможные значения: • «Да» (по умолчанию) - задача активирована; • «Нет» - задача деактивирована. Если задача уже успела активироваться, то при ее выключении (значение «Нет» переключателя параметра) действие будет применено в этот раз, но не в следующий
«Название»	Текстовое наименование создаваемой задачи
«Комментарий»	Информационное сообщение, используемое для описания назначения задачи
«Скрипт»	Выбор скрипта, который будет выполнен во время действия задачи. Доступен при выборе действия «Выполнение скрипта» в раскрывающемся списке экранной кнопки **[Создать]**.
«Фонды»	Выбор одного или нескольких фондов, к которым будет применена задача
«Дата активации расписания»	Дата активации задачи по расписанию Задачи по расписанию выполняются только по часовому поясу GMT+3. Выполнение задач не зависит от часового пояса, настроенного на сервере.
«Время начала»	Время начала очередного действия задачи по расписанию
«Длительность»	Длительность (в минутах) выполнения задачи с момента, заданного в параметре «Время начала». Возможные значения: • «1 мин.»; • «5 мин.»; • «15 мин.» (по умолчанию); • «30 мин.»; • «60 мин.»; • «180 мин. (3 ч.)»; • «360 мин. (6 ч.)»
«Повтор»	Выбор периодичности запуска задачи. Возможные значения: • «Дни недели»; • «Дни месяца»

Параметр	Описание
«Дни недели»	Выбор одного или нескольких дней недели, в которые будет запускаться задача. Доступен при выборе значения «Дни недели» в параметре «Повтор». Возможные значения: • «Понедельник»; • «Вторник»; • «Среда»; • «Четверг»; • «Пятница»; • «Суббота»; • «Воскресенье»
«Дни месяца»	Указание даты или дат (через запятую), в которые будет запускаться задача ежемесячно. Параметр доступен при выборе значения «Дни месяца» в параметре «Повтор». Допускается использование специального значения «*» - все дни месяца. Пример: «10,20,30»
«Включение всех назначенных рабочих мест»	Управление состоянием назначенных РМ. Доступен при выборе действия «Запуск» в раскрывающемся списке экранной кнопки **[Создать]**. Возможные значения: • «Да» (по умолчанию) - ВМ назначенных РМ будут включены; • «Нет» - ВМ назначенных РМ не будут включены
«Включение неназначенных рабочих мест»	Выбор того, как будут учитываться ВМ, которые были запущены до активации задачи и не были назначены пользователю. Доступен при выборе действия «Запуск» в раскрывающемся списке экранной кнопки **[Создать]**. Возможные значения: • «Процент от общего числа» (по умолчанию); • «Абсолютное число»
«Выключение рабочих мест»	Выбор того, как будут учитываться ВМ, которые были запущены до активации задачи. Доступен при выборе действия «Останов (небезопасный)» в раскрывающемся списке экранной кнопки **[Создать]**. Возможные значения: • «Процент от общего числа»; • «Абсолютное число» (по умолчанию)

Параметр	Описание
«Процент от общего числа»	Процент запускаемых или выключаемых ВМ, рассчитывается от общего числа ВМ в фонде. Доступен при выборе действия «Запуск» или «Останов (небезопасный)» в раскрывающемся списке экранной кнопки **[Создать]**. Параметр позволяет регулировать долю запускаемых или выключаемых ВМ в течение времени, заданного в параметре «Длительность». Например, если общее число ВМ составляет 100, и для параметра «Процент от общего числа» установлено значение «30», а для параметра «Длительность» установлено значение «15 мин.», то в течение 15 минут 30 ВМ будут запускаться или выключаться по 2 машины каждую минуту. Соотношение параметров «Длительность», «Процент от общего числа» и «Абсолютное число» позволяет оптимизировать нагрузку на платформу виртуализации. По умолчанию для действия «Запуск»: «20». По умолчанию для действия «Останов (небезопасный)»: «1»
«Абсолютное число»	Число запускаемых или выключаемых ВМ. Доступен при выборе действия «Запуск» или «Останов (небезопасный)» в раскрывающемся списке экранной кнопки **[Создать]**. Параметр позволяет регулировать количество запускаемых или выключаемых ВМ в течение времени, заданного в параметре «Длительность». Например, если для параметра «Абсолютное число» установлено значение «30», а для параметра «Длительность» установлено значение «15 мин.», то в течение 15 минут будут запускаться или выключаться по 2 машины каждую минуту. По умолчанию для действия «Запуск»: «20». По умолчанию для действия «Останов (небезопасный)»: «1»

СПИСКИ И СТАТУСЫ РМ

Список РМ из всех фондов

Отображение списка индивидуальных РМ

Для более эффективного администрирования Termidesk VDI предусмотрено отображение индивидуальных (однопользовательских) РМ из всех фондов ВМ и автономных машин, в том числе назначенных РМ, а также созданных и размещенных в кеше.

Для получения списка необходимо перейти «Рабочие места - Индивидуальные рабочие места» или перейти по ссылке «Рабочие места» из функции «Обзор» (см. рисунок Переход к списку РМ через функцию «Обзор»).

По умолчанию записи в представленном списке будут упорядочены согласно столбцу «Дата создания» по убыванию (см. рисунок Пример отображения списка РМ).

Подробная информация об управлении состоянием ВМ и ее индикации содержится в подразделе **Управление состоянием ВМ в назначенном фонде РМ**, информация по назначению владельца РМ приведена в подразделе **Назначение владельца РМ**.

Терминальные сессии, созданные не через Метапоставщик, также могут быть удалены экранной кнопкой **[Удалить]**.

Отображение списка будет доступно оператору, если у него есть разрешение «Просмотр фондов рабочих мест».

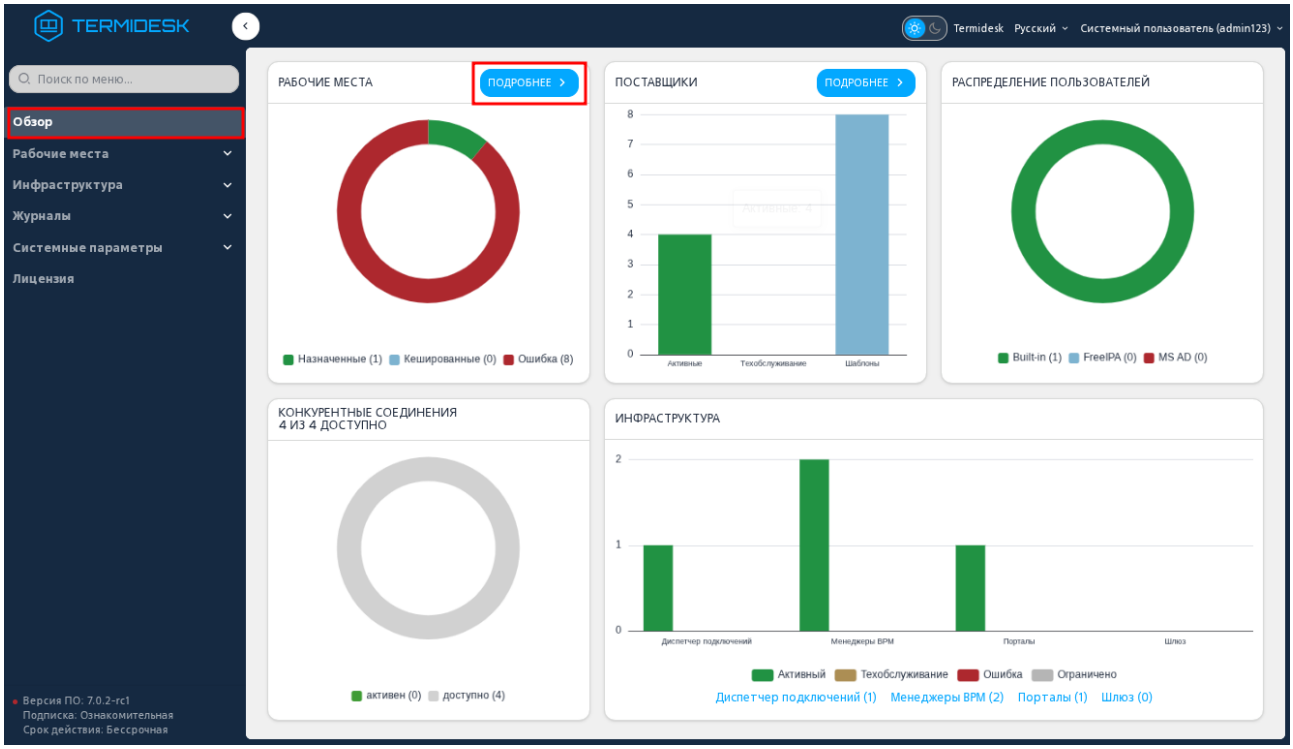


Рисунок 87. Переход к списку РМ через функцию «Обзор»

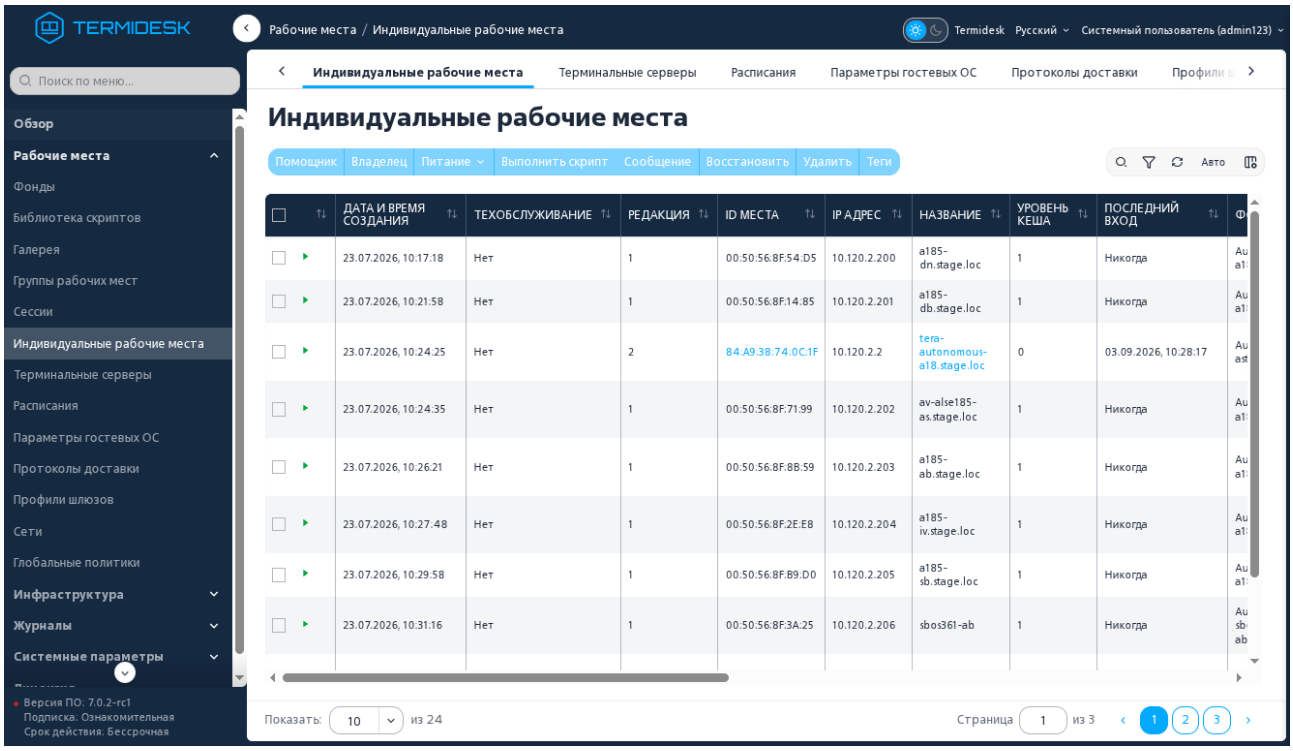


Рисунок 88. Пример отображения списка РМ

Основные параметры списка РМ приведены в таблице (см. таблицу Основные параметры списка РМ).

Таблица 122. Основные параметры списка РМ

Параметр	Описание
«Дата и время создания»	Временная метка выполнения публикации РМ
«Техобслуживание»	Управление режимом технического обслуживания РМ
«Редакция»	Порядковый номер версии публикации
«ID Места»	Уникальный идентификатор РМ и ссылка на метрики РМ. Значение идентификатора РМ определяется компонентом «Агент виртуального рабочего места». В качестве идентификатора РМ используется MAC-адрес сетевого интерфейса. При выборе идентификатора РМ отображается окно «Метрики сессии – Детали о ВРМ» со списком сведений о РМ
«IP-адрес»	IP-адрес сетевого интерфейса РМ. Значение определяется компонентом «Агент виртуального рабочего места»
«Название»	Наименование РМ и ссылка на метрики сессии. При выборе наименования РМ отображается окно «Метрики сессии – Ресурсы» со списком сведений о состоянии и нагрузке РМ
«Уровень кеша»	Уровень кеша, на котором находится РМ
«Последний вход»	Временная метка последней успешной аутентификации пользователя
«Фонд»	Наименование фонда РМ и ссылка на него
«Поставщик ресурсов»	Наименование поставщика ресурсов, в котором создано РМ
«Статус»	Флаг использования публикации РМ из фонда РМ
«Статус обновлен»	Временная метка обновления статуса
«Используется»	Флаг назначения РМ пользователю при наличии активной сессии. Значение «Нет» свидетельствует о том, что РМ не используется пользователем в данный момент. Значение «Да» может сохраниться на некоторое время даже при закрытии пользователем ПО Termidesk Viewer и обновится на «Нет» периодической задачей, выполняемой каждые 90 секунд
«Хост источника»	Наименование инициатора выдачи РМ
«IP источника»	IP-адрес инициатора выдачи РМ и ссылка на метрики компонента «Клиент». При выборе IP-адреса отображается окно «Метрики сессии – Сведения о клиенте» со списком сведений о компоненте «Клиент» и пользовательской рабочей станции
«Владелец»	Субъект, запросивший выдачу РМ и ссылка на метрики пользовательской сессии. При выборе субъекта отображается окно «Метрики сессии – Сведения о входе в сеть» со списком сведений о пользовательской сессии
«Версия агента»	Версия компонента «Агент виртуального рабочего места», установленного в гостевой ОС РМ
«Теги»	Список тегов, назначенных РМ. При выборе тега выполняется переход к разделу «Системные параметры – Управление тегами» со списком объектов, которым назначен данный тег

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- поиск записей по таблице;
- изменение внешнего вида таблицы;
- фильтрация записей таблицы через функцию «Умный фильтр».

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Если при множественном выборе ВМ операция управления состоянием неприменима для какого-то из них, то соответствующая экранная кнопка действия будет заблокирована независимо от применимости этой операции к другим ВМ.

Для отправки сообщения в РМ нужно:

- выбрать одно или несколько РМ;
- нажать экранную кнопку **[Сообщение]**. Отправка сообщения возможна, если параметр «Статус» имеет значение «Действительный» или «Подготовка». ВМ при этом необязательно должна находиться в состоянии «Включена» (например, ВМ может быть в состоянии «Приостановлена»).

Для массового восстановления РМ следует выбрать несколько строк с ВМ и нажать экранную кнопку **[Восстановить]**. Условия восстановления перечислены в подразделе **Управление состоянием ВМ в назначенном фонде РМ**.

Если при множественном выборе РМ операция управления состоянием неприменима для какого-то из них, то соответствующая экранная кнопка действия будет заблокирована независимо от применимости этой операции к другим РМ.

Отображение списка РМ терминальных серверов

Для более эффективного администрирования Termidesk VDI предусмотрено отображение РМ из всех фондов терминальных серверов, в том числе назначенных РМ, а также созданных и размещенных в кеше.

Для получения списка РМ терминальных серверов необходимо перейти «Рабочие места - Терминальные серверы».

В Termidesk VDI версии 7.0 на странице отображаются только терминальные серверы Метапоставщика.

Отображение списка будет доступно оператору, если у него есть разрешение «Просмотр фондов рабочих мест».

Основные параметры списка РМ терминальных серверов приведены в таблице (см. таблицу Основные параметры списка РМ терминальных серверов).

Подробная информация об управлении состоянием ВМ терминальных серверов содержится в подразделах **Управление состоянием терминальных серверов**, **Управление состоянием ВМ в назначенном фонде РМ**.

Таблица 123. Основные параметры списка РМ терминальных серверов

Параметр	Описание
«Дата и время создания»	Временная метка выполнения публикации РМ
«Редакция»	Порядковый номер версии публикации
«ID Места»	Уникальный идентификатор РМ: MAC-адрес сетевого интерфейса или номер сессии. Значение определяется компонентом «Агент виртуального рабочего места»
«IP-адрес»	IP-адрес сетевого интерфейса РМ. Значение определяется компонентом «Агент виртуального рабочего места»
«Название»	Наименование РМ и ссылка на метрики терминального сервера
«Сессии»	Количество активных сессий на терминальном сервере и ссылка на список активных сессий
«Индекс нагрузки»	Значение нагрузки для терминального сервера из сервисного фонда РМ, включенного в Метапоставщик
«Сервисный фонд»	Наименование сервисного фонда терминального сервера Метапоставщика
«Поставщик»	Наименование поставщика ресурсов, в котором создано РМ
«Статус»	Флаг использования публикации РМ из фонда РМ
«Статус обновлен»	Временная метка обновления статуса

Параметр	Описание
«Используется»	Флаг назначения РМ пользователю при наличии активной сессии. Значение «Нет» свидетельствует о том, что РМ не используется пользователем в данный момент
«Уровень кеша»	Значение уровня кеша РМ
«Версия агента»	Версия компонента «Агент виртуального рабочего места», установленного в гостевой ОС РМ

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- поиск записей по таблице;
- изменение внешнего вида таблицы;
- фильтрация записей таблицы через функцию «Умный фильтр».

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Фильтрация списка РМ

Для списка РМ доступен механизм фильтрации («Умный фильтр»). Фильтрация осуществляется путем задания значений для параметров «Атрибут», «Условие» и «Значение».

Чтобы применить установленные параметры фильтрации, следует нажать экранную кнопку **[Применить]**.

Экранная кнопка **[Очистить]** возвращает параметры фильтра к исходному состоянию: удаляются дополнительные строки фильтра, все значения сбрасываются, поля «Условие» и «Значение» блокируются.

Пример доступных параметров для механизма фильтрации страницы «Рабочие места - Индивидуальные рабочие места» приведен в таблице (см. таблицу Параметры фильтрации).

При ручном вводе данных в поле фильтра «Значение» допускается полный или частичный ввод только одного параметра фильтрации. При применении нескольких одинаковых фильтров к списку фильтрация выполняется с учетом только последнего заданного фильтра.

Таблица 124. Параметры фильтрации

Атрибут	Условия	Значение
«Дата и время создания»	Формирование списка РМ по времени создания: • «В пределах» - в указанном временном промежутке; • «Не в пределах» - исключая указанный временной промежуток	Ручной ввод посредством выбора даты и времени (графический элемент)
«Редакция»	Формирование списка РМ: • «Является» - включая указанную редакцию; • «Не является» - исключая указанную редакцию	Ручной ввод
«Уникальный ID»	Формирование списка РМ: • «Является» - по указанному идентификатору; • «Не является» - исключая указанный идентификатор; • «Начинается с» - по начальной части идентификатора; • «Оканчивается на» - по конечной части идентификатора; • «Содержит» - включая указанную часть идентификатора	Ручной ввод

Атрибут	Условия	Значение
«IP-адрес»	Формирование списка РМ: • «Является» - по указанному IP-адресу инициатора выдачи РМ; • «Не является» - исключая указанный IP-адрес инициатора выдачи РМ; • «Начинается с» - по начальной части IP-адреса инициатора выдачи РМ; • «Оканчивается на» - по конечной части IP-адреса инициатора выдачи РМ; • «Содержит» - включая указанную часть IP-адреса инициатора выдачи РМ	Ручной ввод
«Название»	Формирование списка РМ: • «Является» - по указанному наименованию РМ; • «Не является» - исключая указанное наименование РМ; • «Начинается с» - по начальной части наименования РМ; • «Оканчивается на» - по конечной части наименования РМ; • «Содержит» - включая указанную часть наименования РМ	Ручной ввод
«Фонд»	Формирование списка РМ: • «Является» - по указанному наименованию фонда РМ; • «Не является» - исключая указанное наименование фонда РМ; • «Начинается с» - по начальной части наименования фонда РМ; • «Оканчивается на» - по конечной части наименования фонда РМ; • «Содержит» - включая указанную часть наименования фонда РМ	Ручной ввод
«Поставщик ресурсов»	Формирование списка РМ: • «Является» - по указанному наименованию поставщика ресурсов; • «Не является» - исключая указанное наименование поставщика ресурсов; • «Начинается с» - по начальной части наименования поставщика ресурсов; • «Оканчивается на» - по конечной части наименования поставщика ресурсов; • «Содержит» - включая указанную часть наименования поставщика ресурсов	Ручной ввод

Атрибут	Условия	Значение
«Статус»	Формирование списка РМ: • «Является» - по указанному статусу РМ; • «Не является» - исключая указанный статус РМ	• «Подготовка»; • «Действительный»; • «Удаление»; • «Удаляется»; • «Удален»; • «Ошибка»; • «Отменяется»; • «Отменено»
«Статус обновлен»	Формирование списка РМ по времени обновления статуса: • «В пределах» - в указанном временном промежутке; • «Не в пределах» - исключая указанный временной промежуток	Ручной ввод посредством выбора даты и времени (графический элемент)
«Используется»	Формирование списка РМ: • «Является» - по используемым РМ; • «Не является» - исключая используемые РМ	• «Да»; • «Нет»
«Хост источника»	Формирование списка РМ: • «Является» - по указанному наименованию инициатора выдачи РМ; • «Не является» - исключая указанное наименование инициатора выдачи РМ; • «Начинается с» - по начальной части наименования инициатора выдачи РМ; • «Оканчивается на» - по конечной части наименования инициатора выдачи РМ; • «Содержит» - включая указанную часть наименования инициатора выдачи РМ	Ручной ввод
«IP источника»	Формирование списка РМ: • «Является» - по указанному IP-адресу инициатора выдачи РМ; • «Не является» - исключая указанный IP-адрес инициатора выдачи РМ; • «Начинается с» - по начальной части IP-адреса инициатора выдачи РМ; • «Оканчивается на» - по конечной части IP-адреса инициатора выдачи РМ; • «Содержит» - включая указанную часть IP-адреса инициатора выдачи РМ	Ручной ввод

Атрибут	Условия	Значение
«Владелец»	Формирование списка РМ: • «Является» - по указанному субъекту, инициировавшего выдачу РМ; • «Не является» - исключая указанный субъект, инициировавшего выдачу РМ; • «Начинается с» - по начальной части субъекта, инициировавшего выдачу РМ; • «Оканчивается на» - по конечной части субъекта, инициировавшего выдачу РМ; • «Содержит» - включая указанную часть субъекта, инициировавшего выдачу РМ	Ручной ввод
«Имя тега»	Формирование списка РМ: • «Является» - по указанному наименованию тега; • «Не является» - исключая наименование тега; • «Начинается с» - по начальной части наименования тега; • «Оканчивается на» - по конечной части наименования тега; • «Содержит» - включая указанную часть наименования тега	Ручной ввод
«Версия агента»	Формирование списка РМ: • «Является» - по указанной версии Агента; • «Не является» - исключая указанную версию Агента; • «Начинается с» - по начальной части версии Агента; • «Оканчивается на» - по конечной части версии Агента; • «Содержит» - включая указанную часть версии Агента	Ручной ввод
«Состояние»	Формирование списка РМ: • «Является» - по указанному состоянию ВМ; • «Не является» - исключая указанное состояние ВМ	• «Выключена»; • «Включена»; • «Спящий режим»; • «Неизвестно»
«Уровень кеша»	Формирование списка РМ: • «Является» - по указанному уровню кеша; • «Не является» - исключая указанный уровень кеша	• «0»; • «1»; • «2»

Атрибут	Условия	Значение
«Последний вход»	Формирование списка по времени последнего запуска РМ: • «В пределах» - в указанном временном промежутке; • «Не в пределах» - исключая указанный временной промежуток	Ручной ввод посредством выбора даты и времени (графический элемент)

Статусы РМ

Статусы позволяют отслеживать состояние РМ на разных этапах его жизненного цикла.

Возможные статусы, в которые может переходить РМ, приведены в таблице (см. таблицу Статусы РМ).

Таблица 125. Статусы РМ

Статус	Описание
«Подготовка»	Указывает на этап создания РМ. Статус назначается автоматически при запуске процесса создания РМ. Если РМ находится в этом статусе, то оно не готово к использованию и пользователь не может подключиться к нему. Если РМ успешно создано, то произойдет переход в статус «Действительный». Если во время создания РМ произошла ошибка, то произойдет переход в статус «Ошибка». Если РМ было удалено до окончания создания, то произойдет переход в статус «Отменено»
«Действительный»	Указывает на успешное завершение этапа подготовки РМ. Если РМ находится в этом статусе, то оно готово к использованию и пользователь может подключиться к нему. При наличии нескольких РМ с одинаковым статусом и при прочих равных условиях (например, уровень кеша) пользователю будет выдано РМ, созданное ранее остальных. РМ автоматически переходит в статус «Действительный» после успешного завершения одного из этапов: • «Подготовка»; • «Проверяется». Если инициирован процесс удаления РМ, то произойдет переход в статус «Удаление»

Статус	Описание
«Проверяется»	Указывает на этап проверки готовности РМ к подключению. Статус назначается автоматически при подключении пользователя к РМ через компонент «Клиент». Статус «Проверяется» не назначается РМ из фондов терминальных серверов и терминальных серверов Метапоставщика. Если РМ находится в этом статусе, то пользователь не может подключиться к нему. При нахождении РМ в этом статусе, выполняется проверка состояния компонента «Агент виртуального рабочего места». Если проверка состояния компонента «Агент виртуального рабочего места» завершилась успешно, то РМ переходит в статус «Действительный». Если проверка состояния компонента «Агент виртуального рабочего места» завершилась неуспешно, то РМ переходит в статус «Недействительный»
«Недействительный»	Указывает на неуспешное завершение этапа проверки готовности РМ к подключению. Статус назначается автоматически, если проверка состояния компонента «Агент виртуального рабочего места» завершилась ошибкой. При нахождении РМ в статусе «Недействительный» следует проверить состояние и настройки компонента «Агент виртуального рабочего места». Если РМ находится в этом статусе, то пользователь не может подключиться к нему. РМ в статусе «Недействительный» автоматически не удаляется. Удаление РМ в этом статусе выполняется вручную или при перепубликации фонда. Проверка состояния компонента «Агент виртуального рабочего места» для РМ в статусе «Недействительный» выполняется периодической задачей. Интервал проверки состояния компонента «Агент виртуального рабочего места» задается в параметре «Интервал проверки статуса 'Недействительный', с» (см. подраздел **Общие системные параметры Termidesk VDI**). Если периодическая проверка состояния компонента «Агент виртуального рабочего места» завершилась успешно, то РМ переходит в статус «Действительный»
«Удаление»	Указывает на ожидание удаления РМ. Статус назначается автоматически при инициировании процесса удаления РМ. Если РМ находится в этом статусе, то пользователь не может подключиться к нему. Если начато фактическое удаление РМ (процесс перешел в фазу исполнения), то произойдет переход в статус «Удаляется»
«Удаляется»	Указывает на процесс удаления РМ. Статус назначается автоматически при переходе процесса удаления РМ к исполнению. Если РМ находится в этом статусе, то пользователь не может подключиться к нему. Если удаление РМ успешно выполнено, то произойдет переход в статус «Удален». Если во время удаления РМ произошла ошибка, то произойдет переход в статус «Ошибка»

Статус	Описание
«Удален»	Указывает на успешное удаление РМ. Статус назначается автоматически после успешного завершения процесса удаления РМ. Если РМ находится в этом статусе, то пользователь не может подключиться к нему. Переход между статусами не предусмотрен
«Ошибка»	Указывает на неуспешное завершение одного из этапов: создания, удаления или отмены РМ. Статус назначается автоматически. Если РМ находится в этом статусе, то пользователь не может подключиться к нему. Переход между статусами не предусмотрен
«Отменяется»	Указывает на процесс отмены создания РМ. Статус назначается автоматически при удалении РМ, находящегося в статусе «Подготовка». Если РМ находится в этом статусе, то пользователь не может подключиться к нему. Если процесс отмены (удаления РМ) успешно завершился, то произойдет переход в статус «Отменено»
«Отменено»	Указывает на успешную отмену создания РМ. Статус назначается автоматически после успешного завершения процесса отмены создания РМ. Если РМ находится в этом статусе, то пользователь не может подключиться к нему. Переход между статусами не предусмотрен
«Техобслуживание»	Указывает на нахождение РМ в режиме техобслуживания. Режим техобслуживания активируется вручную. Статус назначается автоматически после активации режима. Если РМ выведено из режима техобслуживания, то произойдет переход в статус «Действительный»

УПРАВЛЕНИЕ СЕССИЯМИ И РМ

Управление сессиями подключенных к фондам пользователей

В графическом интерфейсе управления Termidesk VDI реализована возможность просмотра информации и управления текущими активными сессиями пользователей в фондах РМ.

Функционал управления сессиями (завершение, отключение) пользователя из страницы «Рабочие места - Сессии» доступен для терминальных сессий.

Для просмотра основных сведений об активных сессиях пользователей в фондах РМ следует перейти «Рабочие места - Сессии», после чего откроется сводная таблица (см. рисунок Просмотр сведений об активных сессиях пользователей в фондах ВРМ).

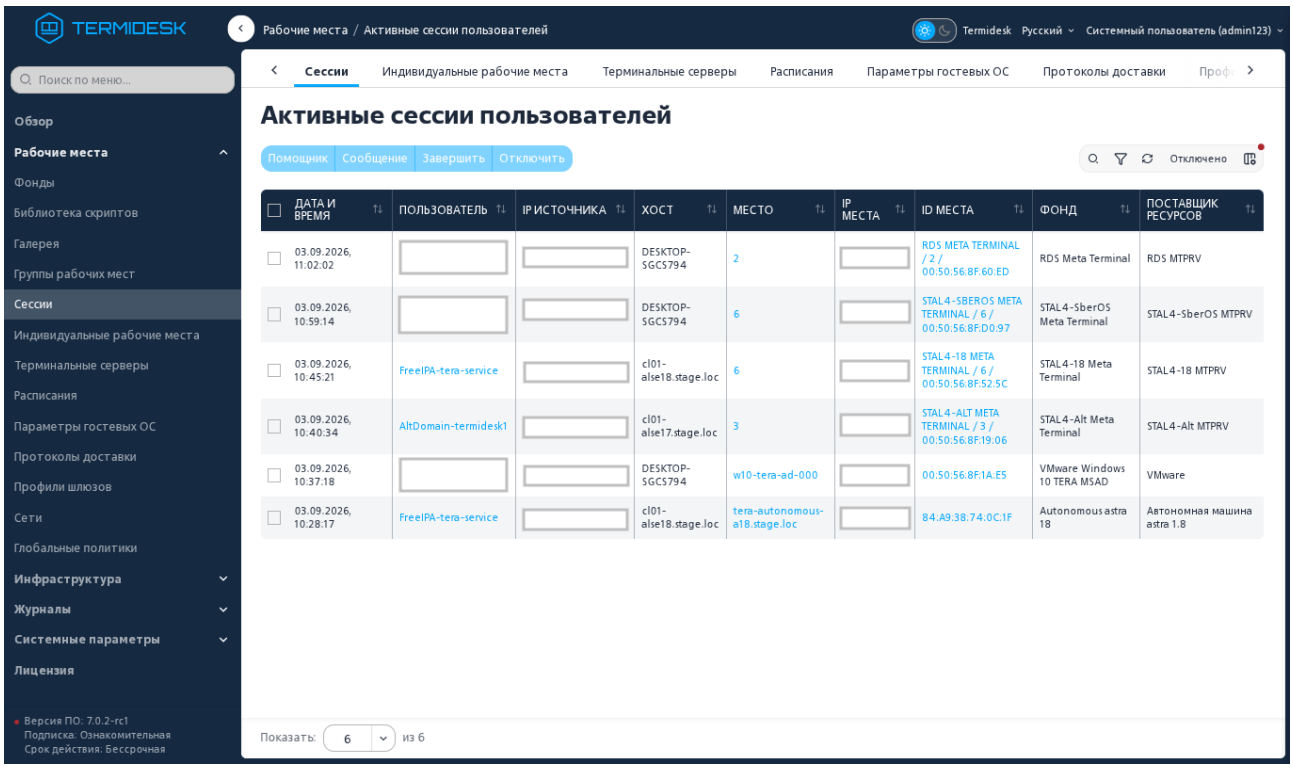


Рисунок 89. Просмотр сведений об активных сессиях пользователей в фондах ВРМ

Основные параметры сессий перечислены в столбце «Параметр» следующей таблицы (см. таблицу Основные параметры сессий пользователей).

Таблица 126. Основные параметры сессий пользователей

Параметр	Описание
«Дата и время»	Дата и время входа пользователя на РМ
«Пользователь»	Имя пользователя, которому было выдано РМ и ссылка на метрики пользовательской сессии. При выборе имени пользователя отображается окно «Метрики сессии – Сведения о входе в сеть» со списком сведений о пользовательской сессии
«IP источника»	IP-адрес инициатора сессии и ссылка на метрики компонента «Клиент». При выборе IP-адреса отображается окно «Метрики сессии – Сведения о клиенте» со списком сведений о компоненте «Клиент» и пользовательской рабочей станции
«Хост»	Наименование инициатора сессии
«Место»	Наименование РМ, выданного пользователю и ссылка на метрики сессии. При выборе наименования РМ отображается окно «Метрики сессии – Ресурсы» со списком сведений о состоянии и нагрузке РМ
«IP Места»	IP-адрес сетевого интерфейса РМ. Значение определяется компонентом «Агент виртуального рабочего места»

Параметр	Описание
«ID Места»	Уникальный идентификатор РМ и ссылка на метрики РМ. Значение идентификатора РМ определяется компонентом «Агент виртуального рабочего места». В качестве идентификатора РМ используется: • MAC-адрес сетевого интерфейса; • номер сессии. При выборе идентификатора РМ отображается окно «Метрики сессии – Детали о ВРМ» со списком сведений о РМ
«Фонд»	Название фонда, в составе которого находится выданное РМ
«Поставщик ресурсов»	Наименование поставщика ресурсов, в котором создано РМ

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- поиск записей по таблице;
- изменение внешнего вида таблицы;
- фильтрация записей таблицы через функцию «Умный фильтр».

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для

настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Для управления активной сессией пользователя предусмотрены следующие варианты управления (см. таблицу Управление активной сессией пользователя).

Сброс сессии для РМ будет работать для поставщика ПК СВ Брест, если выполнена дополнительная настройка «Агента узла виртуализации» (см. подраздел **Использование альтернативного механизма сброса сессий** документа СЛЕТ.10001-01 90 04 «Руководство администратора. Настройка компонента «Агент»).

Отключение сессии пользователя, подключенного по протоколу TERA, работает для гостевой ОС Astra Linux Special Edition, и применяется как для физической машины, так и для ВМ.

Таблица 127. Управление активной сессией пользователя

Параметр	Описание
«Помощник»	Подключает администратора к сессии пользователя. Следует пометить сессию пользователя и нажать экранную кнопку **[Помощник]**. Ввод данных для подключения не требуется: они будут заполнены автоматически. Доступность функционала зависит от типа редакции Termidesk VDI. Не рекомендуется устанавливать компонент «Удаленный помощник» (серверная часть) на узел с установленным компонентом «Универсальный диспетчер», поскольку оба компонента вносят изменения в конфигурацию веб-сервера Apache. Для работы подключения необходимо, чтобы: • в гостевой ОС был установлен компонент «Удаленный помощник» (клиентская часть); • в сетевой инфраструктуре организации существовал узел с установленным компонентом «Удаленный помощник» (серверная часть) и он был доступен для взаимодействия с «Универсальным диспетчером»; • в системных параметрах был установлен параметр «Адрес сервера удаленного помощника»

Параметр	Описание

«Сообщение»	Отправляет сообщение пользователю с подтверждением его получения со стороны пользователя и информированием администратора об успешности отправки сообщения. Факт прочтения пользователем сообщения фиксируется в журнале РМ.
	
	Отправка сообщения возможна, если параметр «Статус» имеет значение «Действительный» или «Подготовка». ВМ при этом необязательно должна находиться в состоянии «Включена» (например, ВМ может быть в состоянии «Приостановлена»).
	
	Отправка сообщений в терминальные сессии стандартных терминальных серверов (не созданных через Метапоставщик) возможна при использовании расширенного сценария добавления терминальных серверов (см. подраздел **Последовательность ввода в действие Termidesk VDI**). Отправка сообщений в терминальные сессии с опубликованными приложениями не поддерживается.
	
	Для отправки сообщения нужно:
	
	• заполнить его заголовок (параметр «Заголовок») и текст (параметр «Сообщение»), которые отобразятся пользователю;
	• выбрать уровень важности сообщения (параметр «Важность»):
	  - «informational» (по умолчанию) - информационное сообщение. Для пользователя отобразится сообщение с уровнем важности «informational»;
	  - «warning» - предупреждение. Для пользователя отобразится сообщение с уровнем важности «warning»;
	  - «error» - ошибка. Для пользователя отобразится сообщение с уровнем важности «error»;
	• указать необходимость запроса подтверждения о прочтении (параметр «Требовать подтверждения о прочтении»)

«Завершить»	Завершает сессию пользователя. Следует пометить сессию пользователя и нажать экранную кнопку **[Завершить]**. Принудительный штатный выход пользователя из ОС РМ произойдет в течение 30 секунд. Также сессия пользователя будет автоматически и принудительно завершена, если он был удален или домен аутентификации, в который входит этот пользователь, был отключен или удален
«Отключить»	Отключает сессию пользователя. Следует пометить сессию пользователя и нажать экранную кнопку **[Отключить]**. Сессия пользователя прервется, но если он снова подключится, то состояние сессии до отключения восстановится

Управление терминальными сессиями

В графическом интерфейсе управления Termidesk VDI предусмотрена возможность просмотра информации и управления терминальными сессиями пользователей.

Просмотр основных сведений о терминальных сессиях пользователей и управление ими возможен следующими способами:

- в меню навигации перейти «Рабочие места - Сессии» (см. подраздел **Управление сессиями подключенных к фондам пользователей**);
- в меню навигации перейти «Рабочие места - Фонды», затем выбрать нужный фонд терминального сервера, перейти во вкладку «Назначенные места» (см. рисунок Просмотр сведений о терминальных сессиях пользователей в назначенном фонде РМ). Основные параметры назначенных машин терминального сервера перечислены в столбце «Параметр» следующей таблицы (см. таблицу Основные параметры терминальных сессий).

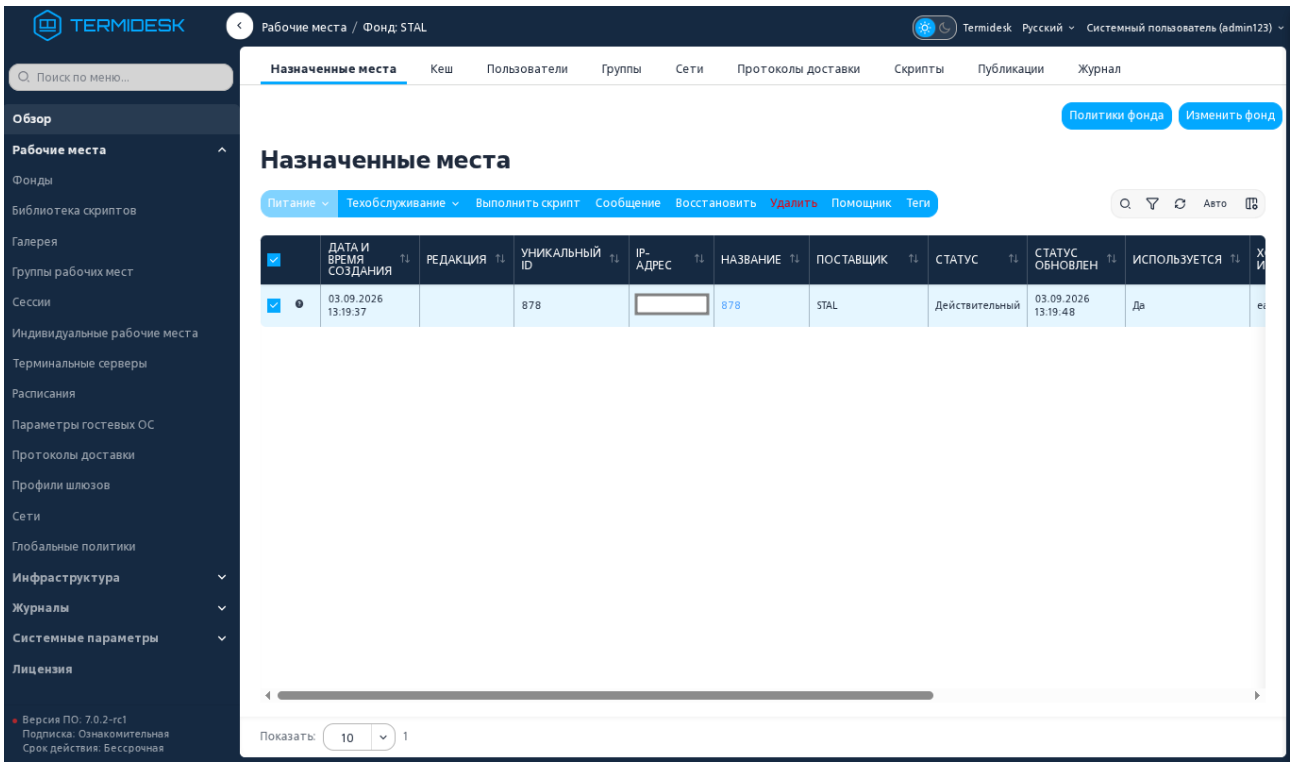


Рисунок 90. Просмотр сведений о терминальных сессиях пользователей в назначенном фонде РМ

Таблица 128. Основные параметры терминальных сессий

Параметр	Описание
«Дата и время создания»	Временная метка создания сессии
«Редакция»	Порядковый номер версии сессии
«Уникальный ID»	Уникальный идентификатор сессии
«IP-адрес»	IP-адрес терминального сервера, к которому установлено подключение сессии
«Название»	Номер сессии, выданной пользователю со ссылкой на журнал и метрики сессии
«Статус»	Флаг использования сессии. Частота обновления статусов терминальных сессий (в том числе сессий Метапоставщика) для небольшого количества машин составляет 2 секунды. Для терминальных сессий может возникнуть ситуация, при которой статус сессии отображен как «Действительный», но идентификатор ей не назначен. Такие сессии считаются неактивными и удаляются периодической задачей, которая срабатывает с интервалом 240 секунд
«Статус обновлен»	Временная метка обновления статуса
«Используется»	Флаг назначения РМ пользователю при наличии активной сессии. Значение «Нет» свидетельствует о том, что РМ не используется пользователем в данный момент
«Хост источника»	Наименование инициатора сессии
«IP источника»	IP-адрес инициатора сессии
«Владелец»	Субъект, инициировавший выдачу сессии
«Версия агента»	Версия компонента «Агент», установленного на терминальном сервере

Параметр	Описание
«Теги»	Список тегов, назначенных РМ. При выборе тега выполняется переход к разделу «Системные параметры – Управление тегами» со списком объектов, которым назначен данный тег

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- поиск записей по таблице;
- изменение внешнего вида таблицы;
- фильтрация записей таблицы через функцию «Умный фильтр».

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Для управления состоянием терминальных серверов используются элементы, аналогичные управлению ВМ (см. подраздел **Управление состоянием ВМ в назначенном фонде РМ**).

Управление состоянием терминальных серверов

Termidesk VDI поддерживает отображение РМ из всех фондов терминальных серверов и управление их состоянием.

Для получения списка терминальных серверов необходимо перейти «Рабочие места - Терминальные серверы» (см. подраздел **Отображение списка РМ терминальных серверов**).

Для управления состоянием терминальных серверов используются элементы, аналогичные управлению ВМ (см. подраздел **Управление состоянием ВМ в назначенном фонде РМ**).

Управление состоянием ВМ в назначенном фонде РМ

Termidesk VDI поддерживает управление состоянием назначенных ВМ для РМ, созданных для следующих поставщиков ресурсов:

- ПК СВ Брест (обязательна установка компонента «Агент узла виртуализации»);
- автономная машина;
- zVirt;
- РЕД Виртуализация;
- OpenStack;
- oVirt;
- VMware vSphere;
- VMmanager.

Для просмотра списка и управления состоянием ВМ в фонде РМ необходимо перейти «Рабочие места - Фонды», затем выбрать нужный фонд во вкладке «Назначенные места» (см. рисунок Страница управления состоянием назначенных ВМ).

Отображение списка будет доступно оператору, если у него есть пользовательское разрешение «Просмотр фондов рабочих мест».

Управление состоянием ВМ будет доступно оператору, если у него есть пользовательское разрешение «Управление питанием фондов рабочих мест».

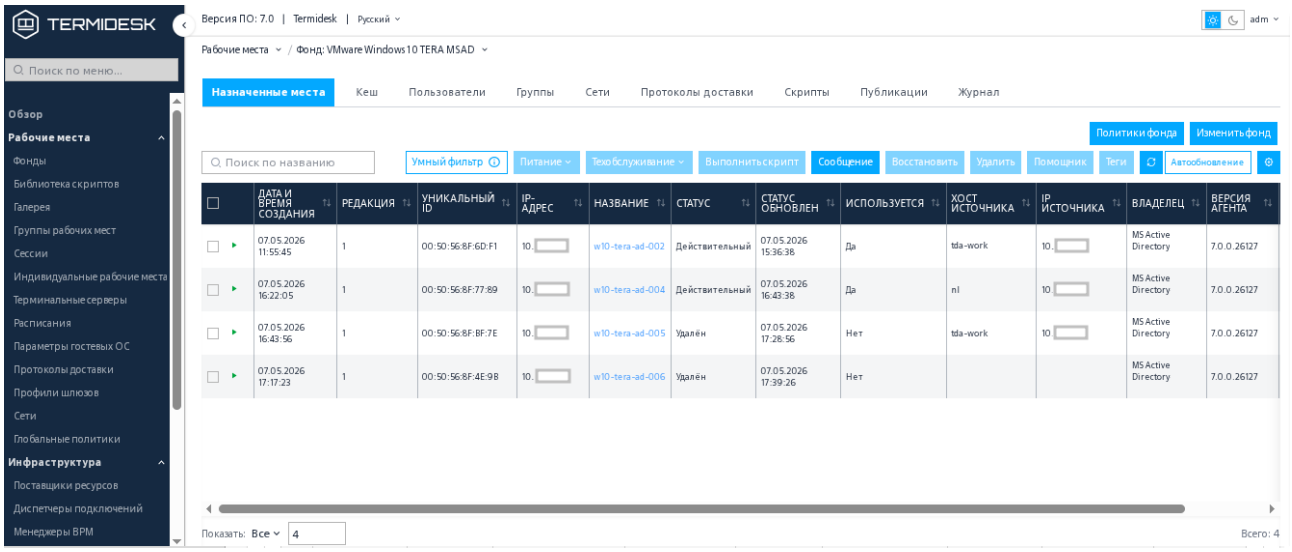


Рисунок 91. Страница управления состоянием назначенных ВМ

Основные параметры списка ВМ в назначенном фонде РМ перечислены в столбце «Параметр» следующей таблицы (см. таблицу Основные параметры списка ВМ в назначенном фонде РМ).

Таблица 129. Основные параметры списка ВМ в назначенном фонде РМ

Параметр	Описание
«Дата и время создания»	Временная метка выполнения публикации РМ
«Редакция»	Порядковый номер версии публикации
«Уникальный ID»	Уникальный идентификатор РМ: MAC-адрес сетевого интерфейса или номер сессии. Значение определяется компонентом «Агент виртуального рабочего места»
«IP-адрес»	IP-адрес сетевого интерфейса РМ. Значение определяется компонентом «Агент виртуального рабочего места»
«Название»	Наименование РМ со ссылкой на журнал и метрики РМ
«Индекс нагрузки»	Значение нагрузки для терминального сервера из сервисного фонда РМ, включенного в Метапоставщик
«Статус»	Флаг использования публикации РМ из фонда РМ
«Статус обновлен»	Временная метка обновления статуса
«Используется»	Флаг назначения РМ пользователю при наличии активной сессии. Значение «Нет» свидетельствует о том, что РМ не используется пользователем в данный момент. Значение «Да» может сохраниться на некоторое время даже при закрытии пользователем ПО Termidesk Viewer и обновится на «Нет» периодической задачей, выполняемой каждые 90 секунд
«Хост источника»	Наименование инициатора выдачи РМ
«IP источника»	IP-адрес инициатора выдачи РМ
«Владелец»	Субъект, инициировавший выдачу РМ
«Версия агента»	Версия компонента «Агент виртуального рабочего места», установленного в гостевой ОС РМ
«Теги»	Список тегов, назначенных РМ. При выборе тега выполняется переход к разделу «Системные параметры – Управление тегами» со списком объектов, которым назначен данный тег

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- поиск записей по таблице;
- изменение внешнего вида таблицы;
- фильтрация записей таблицы через функцию «Умный фильтр».

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Каждая запись списка сопровождается индикацией состояния ВМ (см. таблицу Индикация состояния ВМ).

Таблица 130. Индикация состояния ВМ

Индикация	Описание
	Состояние неизвестно. Статус появляется, когда состояние ВМ не подходит под приведенные ниже. Такое состояние также может свидетельствовать, что в фонде, которому принадлежит РМ, не поддерживается управление состоянием ВМ. Экранные кнопки **[Запуск]**, **[Пауза]**, **[Выкл (безопасно)]**, **[Перезагрузить (безопасно)]** будут недоступны для использования
	ВМ включена
	ВМ находится в спящем режиме
	ВМ выключена

Для изменения состояния ВМ предусмотрены следующие варианты управления состоянием (см. таблицу Управление состоянием ВМ). Управление состоянием ВМ будет доступно даже при переводе ВМ, фонда РМ или поставщика ресурсов в режим техобслуживания.

Таблица 131. Управление состоянием ВМ

Параметр	Описание
«Запуск»	Инициирует процесс старта ВМ. Параметр доступен при выборе экранной кнопки **[Питание]**
«Пауза»	Приостанавливает работу ВМ, с сохранением текущего состояния. Параметр доступен при выборе экранной кнопки **[Питание]**. Параметр будет недоступен, если поставщик ресурсов не поддерживает приостанов ВМ Параметр будет заблокирован, если поставщик ресурсов, на котором размещена ВМ, не поддерживает приостанов Для приостановки ВМ, размещенной на платформе VMmanager, версия VMmanager должна быть не ниже 2025.09.1.
«Выкл (безопасно)»	Инициирует процесс безопасного отключения ВМ, с завершением активных процессов и сохранением данных. Параметр доступен при выборе экранной кнопки **[Питание]**. Для безопасного отключения ВМ, размещенной на VMware, нужно дополнительно установить утилиты VMware Tools в гостевую ОС. Для принудительного выключения ВМ в раскрывающемся списке следует нажать экранную кнопку **[Выкл]** Принудительное выключение ВМ может привести к потере несохраненных данных или повреждению гостевой ОС.
«Перезагрузить (безопасно)»	Инициирует процесс безопасной перезагрузки ВМ, применяя изменения в конфигурации или гостевой ОС. Параметр доступен при выборе экранной кнопки **[Питание]**. Для безопасной перезагрузки ВМ, размещенной на VMware, нужно дополнительно установить утилиты VMware Tools в гостевую ОС. Для принудительной перезагрузки ВМ в раскрывающемся списке следует нажать экранную кнопку **[Перезагрузить]** Принудительная перезагрузка ВМ завершает активные сессии гостевой ОС и может привести к потере несохраненных данных. Для ВРМ, размещенного на поставщике ресурсов VMware vSphere и использующего диск с режимом «Независимый-Непостоянный», сброс состояния ВМ не происходит, если перезагрузка инициирована из гостевой ОС или через экранную кнопку **[Перезагрузить (безопасно)]**.

Параметр	Описание
«Техобслуживание»	Перевод ВМ в режим техобслуживания или вывод из него. Для выбора режима нужно отметить РМ в списке, затем нажать экранную кнопку **[Техобслуживание]**. Режим техобслуживания ВМ - это запрет пользователям подключаться и/или переподключаться к ВМ. Текущие подключения остаются до тех пор, пока пользователи не отключатся или не выйдут из ОС самостоятельно или при управляющем воздействии (активации политики фонда РМ или действии администратора). ВМ, находящаяся в режиме техобслуживания: • не назначается пользователю; • не удаляется, если зависла; • не может быть переведена в другое состояние из интерфейса портала Termidesk VDI; • не обновляет информацию о своем состоянии; • не переходит из кеша второго уровня в первый; • может быть удалена, однако ее удаление произойдет после вывода ВМ из режима техобслуживания
«Владелец»	Параметр доступен только для РМ из вкладки «Кеш». Назначает владельца РМ (см. подраздел **Назначение владельца РМ**)
«Выполнить скрипт»	Инициирует выполнение скрипта в выбранном РМ. Для выполнения скрипта нужно отметить РМ в списке, затем нажать экранную кнопку **[Выполнить скрипт]**, в открывшемся окне выбрать соответствующий скрипт в раскрывающемся списке и нажать экранную кнопку **[Выполнить]**

Параметр	Описание

«Сообщение»	Отправляет сообщение пользователю с подтверждением его получения со стороны пользователя и информированием администратора об успешности отправки сообщения. Факт прочтения пользователем сообщения фиксируется в журнале РМ.
	
	Отправка сообщения возможна, если параметр «Статус» имеет значение «Действительный» или «Подготовка». ВМ при этом необязательно должна находиться в состоянии «Включена» (например, ВМ может быть в состоянии «Приостановлена»).
	
	Отправка сообщений в терминальные сессии стандартных терминальных серверов (не созданных через Метапоставщик) возможна при использовании расширенного сценария добавления терминальных серверов (см. подраздел **Последовательность ввода в действие Termidesk VDI**). Отправка сообщений в терминальные сессии с опубликованными приложениями не поддерживается.
	
	Для отправки сообщения нужно:
	
	• заполнить его заголовок (параметр «Заголовок») и текст (параметр «Сообщение»), которые отобразятся пользователю;
	• выбрать уровень важности сообщения (параметр «Важность»):
	  «informational» (по умолчанию) - информационное сообщение. Для пользователя отобразится сообщение с уровнем важности «informational»;
	  «warning» - предупреждение. Для пользователя отобразится сообщение с уровнем важности «warning»;
	  «error» - ошибка. Для пользователя отобразится сообщение с уровнем важности «error»;
	• указать необходимость запроса подтверждения о прочтении (параметр «Требовать подтверждения о прочтении»)

«Восстановить»	Параметр доступен только для поставщиков ресурсов zVirt, oVirt, VMware vSphere, VMmanager. Производит возврат ВМ к снимку (снапшоту), созданному на завершающей стадии подготовки РМ, то есть к состоянию до момента затребования РМ пользователем. Восстановление может быть применимо и для неназначенных ВМ. Функционал восстановления ВМ будет доступен оператору, если у него есть пользовательское разрешение «Восстановление рабочих мест». Восстановление может быть применено, если есть снимок, к которому ВМ может быть возвращена. При повторной публикации фонда РМ возврат к снимку для ранних публикаций будет невозможен Для поставщика ресурсов VMware vSphere: • восстановление ВМ осуществляется через процедуру «выключить», а не «приостановить» («suspend»); • если диск ВМ создан в режиме «Зависимый», то механизм восстановления вернет состояние ВМ к снимку; • если диск ВМ создан в режиме «Независимый-Непостоянный», то механизм восстановления вернет состояние ВМ, актуальное до внесенных пользователем изменений (все изменения будут потеряны). Механизм восстановления для этого режима диска происходит через небезопасное выключение ВМ

Параметр	Описание
«Удалить»	Инициирует процесс полного удаления ВМ, включая все связанные с ней данные и конфигурации. Для удаления нужно отметить РМ в списке, затем нажать экранную кнопку **[Удалить]**. При удалении ВМ из фонда отобразится окно «Удалить объект». В раскрывающемся списке окна нужно выбрать действие, которое будет произведено над учетной записью РМ в службе каталогов: Список будет отображен, если действие над учетной записью применимо к РМ. • «Удалить» (по умолчанию) - при удалении РМ из фонда учетная запись будет удалена из службы каталогов. Применимость: MS AD, FreeIPA, ALD Pro; • «Сбросить пароль» - при удалении РМ из фонда у учетной записи будет сброшен пароль. Применимость: MS AD; • «Выключить» - при удалении РМ из фонда учетная запись будет отключена. Применимость: MS AD; • «Хранить» - при удалении РМ из фонда учетная запись будет сохранена в службе каталогов. Применимость: MS AD, FreeIPA, ALD Pro
«Помощник»	Параметр доступен только для РМ из вкладки «Назначенные места». Доступность функционала зависит от типа редакции Termidesk VDI. Подключает администратора к сессии пользователя. Следует пометить сессию пользователя и нажать экранную кнопку **[Помощник]**. Ввод данных для подключения не требуется: они будут заполнены автоматически. Не рекомендуется устанавливать компонент «Удаленный помощник» (серверная часть) на узел с установленным компонентом «Универсальный диспетчер», поскольку оба компонента вносят изменения в конфигурацию веб-сервера Apache. Для работы подключения необходимо, чтобы: • в гостевой ОС был установлен компонент «Удаленный помощник» (клиентская часть); • в сетевой инфраструктуре организации существовал узел с установленным компонентом «Удаленный помощник» (серверная часть) и он был доступен для взаимодействия с «Универсальным диспетчером»; • в системных параметрах был установлен параметр «Адрес сервера удаленного помощника»
«Теги»	Позволяет назначить теги для выбранного РМ. Для назначения тегов нужно отметить РМ в списке, затем нажать экранную кнопку **[Теги]**. Общее описание по применению тегов приведено в подразделе **Общие сведения о тегах**

Управление состоянием автономных машин в назначенном фонде

В графическом интерфейсе управления Termidesk VDI предусмотрена возможность просмотра информации и управления автономными машинами в назначенном фонде.

Для просмотра списка и управления состоянием автономных машин в фонде необходимо перейти «Рабочие места - Фонды», затем выбрать нужный фонд автономных машин,

перейти во вкладку «Назначенные машины».

Отображение списка будет доступно администратору, если у него есть пользовательское разрешение «Просмотр фондов рабочих мест».

Основные параметры списка машин в назначенном фонде перечислены в столбце «Параметр» следующей таблицы (см. таблицу Основные параметры списка физических машин).

Таблица 132. Основные параметры списка физических машин

Параметр	Описание
«Дата и время создания»	Временная метка выполнения публикации
«Редакция»	Порядковый номер версии публикации
«Уникальный ID»	Уникальный идентификатор РМ: MAC-адрес сетевого интерфейса автономной машины. Значение определяется компонентом «Агент виртуального рабочего места». В случае, если установленный на автономной машине «Агент виртуальных рабочих мест» запускается на VPN-соединении или сетевом адаптере без MAC-адреса, то он не сможет зарегистрироваться на «Универсальном диспетчере»
«IP-адрес»	IP-адрес сетевого интерфейса автономной машины. Значение определяется компонентом «Агент виртуального рабочего места»
«Название»	Наименование РМ со ссылкой на журнал и метрики РМ
«Статус»	Флаг использования публикации из фонда
«Статус обновлен»	Временная метка обновления статуса
«Используется»	Флаг назначения РМ пользователю при наличии активной сессии. Значение «Нет» свидетельствует о том, что РМ не используется пользователем в данный момент. Значение «Да» может сохраниться на некоторое время даже при закрытии пользователем ПО Termidesk Viewer и обновится на «Нет» периодической задачей, выполняемой каждые 90 секунд
«Хост источника»	Наименование инициатора выдачи РМ
«IP источника»	IP-адрес инициатора выдачи РМ
«Владелец»	Субъект, инициировавший выдачу РМ
«Версия агента»	Версия компонента «Агент виртуального рабочего места», установленного в ОС автономной машины

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- поиск записей по таблице;
- изменение внешнего вида таблицы;
- фильтрация записей таблицы через функцию «Умный фильтр».

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Для изменения состояния автономной машины предусмотрены параметры (см. таблицу Элементы управления автономными машинами).

Таблица 133. Элементы управления автономными машинами

Параметр	Описание
«Выкл (безопасно)»	Инициирует процесс безопасного отключения с завершением активных процессов и сохранением данных. Параметр доступен при выборе экранной кнопки **[Питание]**. Для безопасного отключения автономной машины, размещенной на VMware, нужно дополнительно установить утилиты (VMware Tools) в гостевую ОС. Экранная кнопка выпадающего списка **[Выключить]** не поддерживается
«Перезагрузить (безопасно)»	Инициирует процесс безопасной перезагрузки, применяя изменения в конфигурации или гостевой ОС. Параметр доступен при выборе экранной кнопки **[Питание]**.
«Сообщение»	Отправка сообщения пользователям РМ. Для отправки сообщения нужно отметить РМ в списке, затем нажать экранную кнопку **[Сообщение]**. Отправка сообщения возможна, если параметр «Статус» имеет значение «Действительный» или «Подготовка»

Параметр	Описание
«Техобслуживание»	Перевод автономной машины в режим техобслуживания или вывод из него. Для выбора режима нужно отметить РМ в списке, затем нажать экранную кнопку **[Техобслуживание]**. Режим техобслуживания - это запрет пользователям подключаться и (или) переподключаться к РМ. Текущие подключения остаются до тех пор, пока пользователи не отключатся или не выйдут из ОС самостоятельно или при управляющем воздействии (активации политики фонда или действии администратора). РМ, находящаяся в режиме техобслуживания: • не назначается пользователю; • не удаляется, если машина зависла; • не может быть переведено в другое состояние из интерфейса портала Termidesk VDI; • не обновляет информацию о своем состоянии; • не переходит из кеша второго уровня в первый; • может быть удалено, однако его удаление произойдет после вывода из режима техобслуживания
«Удалить»	Инициирует процесс полного удаления РМ, включая все связанные с ним данные и конфигурации. Для удаления нужно отметить РМ в списке, затем нажать экранную кнопку **[Удалить]**. Действие над учетной записью РМ в службе каталогов не поддерживается

Назначение владельца РМ

В Termidesk VDI предусмотрена возможность назначения владельца РМ для гарантированного закрепления за пользователем конкретной ВМ. В этом случае пользователь всегда будет получать одну и ту же ВМ при подключении к фонду РМ.

Назначение владельца возможно при соблюдении следующих условий:

- РМ находится в статусе «Подготовка» или «Действительный»;
- РМ находится в кеше 1-го уровня;
- для данного РМ отсутствует назначенный пользователь в столбце «Владелец» списка РМ.

Назначить владельца РМ можно:

- со страницы фонда. Для этого следует перейти «Рабочие места - Фонды», затем выбрать нужный фонд, перейти во вкладку «Кеш». Выбрать нужное РМ и нажать экранную кнопку **[Владелец]** (см. рисунок Назначение владельца РМ на странице фонда РМ). В открывшемся окне «Владелец» выбрать домен аутентификации и пользователя, которому будет назначено РМ. Выбранный пользователь автоматически добавится в фонд РМ и будет отображен во вкладке «Пользователи и группы»;
- со страницы «Рабочие места - Индивидуальные рабочие места».

Назначение владельца будет доступно только в том случае, если пользователь хотя бы один раз осуществил вход в «Портал пользователя» или подключился к «Универсальному диспетчеру» через компонент «Клиент» под своей учетной записью.

Для назначения владельца РМ требуются также права на просмотр доменов аутентификации.

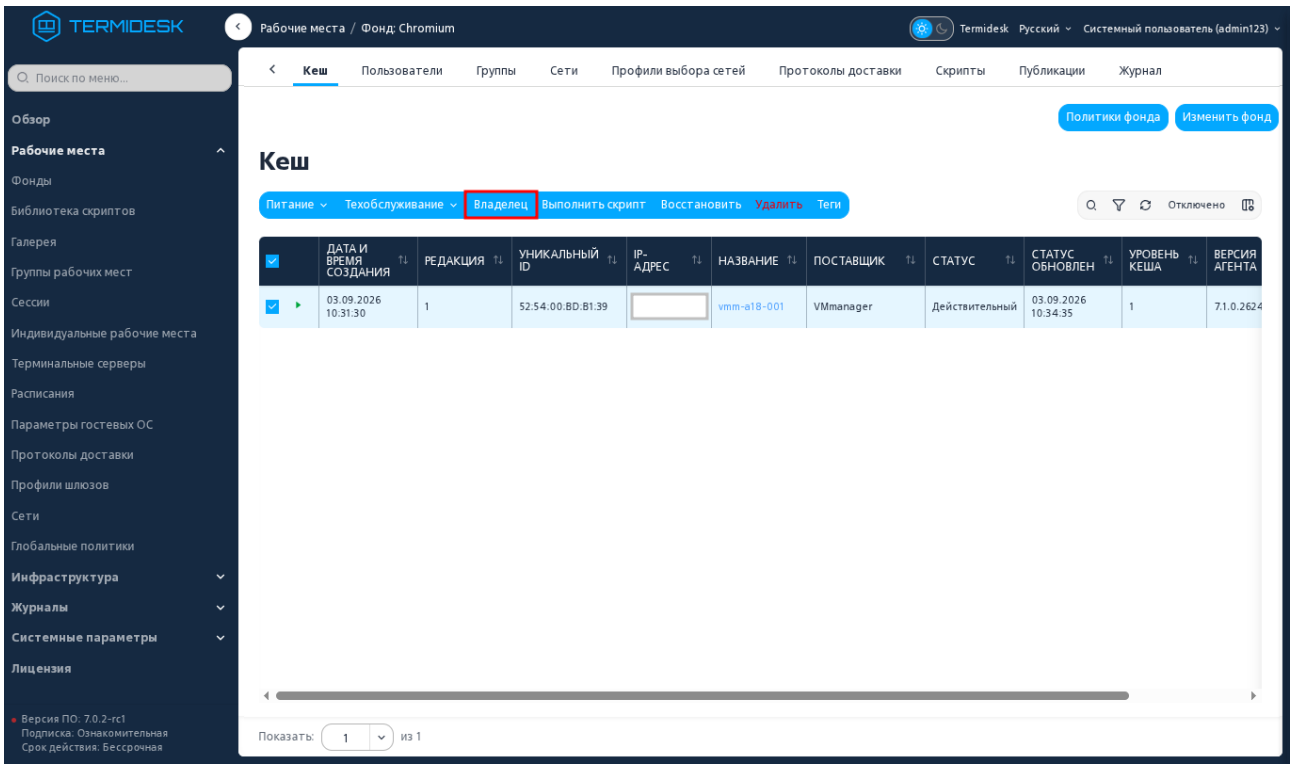


Рисунок 92. Назначение владельца РМ на странице фонда РМ

Фильтрация списка сессий

На страницах со списками РМ или сессий доступен механизм фильтрации. Фильтрация осуществляется путем задания значений для параметров «Атрибут», «Условие» и «Значение».

Для добавления дополнительного фильтра следует нажать экранную кнопку **[+]**. Для удаления фильтра нужно использовать экранную кнопку **[-]** в соответствующей строке. Максимально допустимое число фильтров - 15.

Чтобы применить установленные параметры фильтрации, следует нажать экранную кнопку **[Применить]**.

Экранная кнопка **[Очистить]** сбрасывает все фильтры, возвращая значения к исходному состоянию: удаляются дополнительные строки фильтра (остается только одна строка), все значения сбрасываются, поля «Условие» и «Значение» блокируются.

Пример возможного списка параметров механизма фильтрации для страницы «Рабочие места - Сессии» приведен в таблице (см. таблицу Параметры фильтрации списка сессий).

При ручном вводе данных в поле фильтра «Значение» допускается полный или частичный ввод только одного параметра фильтрации.

При применении нескольких одинаковых фильтров к списку, фильтрация выполняется с учетом только последнего заданного фильтра.

Таблица 134. Параметры фильтрации списка сессий

Атрибут	Условие	Значение
«Терминальный сервер (id)»	Формирование списка сессий: • «Является» - по указанному имени пользователя	Ручной ввод

Атрибут	Условие	Значение
«Дата и время»	Формирование списка сессий: • «В пределах» - в указанном временном промежутке; • «Не в пределах» - исключая указанный временной промежуток	Ручной ввод посредством выбора даты и времени (графический элемент)
«Пользователь»	Формирование списка сессий: • «Является» - по указанному имени пользователя; • «Не является» - исключая указанное имя пользователя; • «Начинается с» - по начальной части имени пользователя; • «Оканчивается на» - по конечной части имени пользователя; • «Содержит» - включая указанную часть имени пользователя	Ручной ввод
«IP-адрес»	Формирование списка сессий: • «Является» - по указанному IP-адресу инициатора сессии; • «Не является» - исключая указанный IP-адрес инициатора сессии; • «Начинается с» - по начальной части IP-адреса инициатора сессии; • «Оканчивается на» - по конечной части IP-адреса инициатора сессии; • «Содержит» - включая указанную часть IP-адреса инициатора сессии	Ручной ввод
«Хост»	Формирование списка сессий: • «Является» - по указанному наименованию инициатора сессии; • «Не является» - исключая указанное наименование инициатора сессии; • «Начинается с» - по начальной части наименования инициатора сессии; • «Оканчивается на» - по конечной части наименования инициатора сессии; • «Содержит» - включая указанную часть наименования инициатора сессии	Ручной ввод

Атрибут	Условие	Значение
«Место»	Формирование списка сессий: • «Является» - по указанному наименованию РМ, выданного пользователю; • «Не является» - исключая указанное наименование РМ, выданного пользователю; • «Начинается с» - по начальной части наименования РМ, выданного пользователю; • «Оканчивается на» - по конечной части наименования РМ, выданного пользователю; • «Содержит» - включая указанную часть наименования РМ, выданного пользователю	Ручной ввод
«IP Места»	Формирование списка сессий: • «Является» - по указанному IP-адресу РМ, выданного пользователю; • «Не является» - исключая указанный IP-адрес РМ, выданного пользователю; • «Начинается с» - по начальной части IP-адреса РМ, выданного пользователю; • «Оканчивается на» - по конечной части IP-адреса РМ, выданного пользователю; • «Содержит» - включая указанную часть IP-адреса РМ, выданного пользователю	Ручной ввод
«ID Места»	Формирование списка сессий: • «Является» - по указанному идентификатору РМ, выданного пользователю; • «Не является» - исключая указанный идентификатор РМ, выданного пользователю; • «Начинается с» - по начальной части идентификатора РМ, выданного пользователю; • «Оканчивается на» - по конечной части идентификатора РМ, выданного пользователю; • «Содержит» - включая указанную часть идентификатора РМ, выданного пользователю	Ручной ввод

Атрибут	Условие	Значение
«Фонд»	Формирование списка сессий: • «Является» - по указанному наименованию фонда, в котором находится РМ; • «Не является» - исключая указанное наименование фонда, в котором находится РМ; • «Начинается с» - по начальной части наименования фонда, в котором находится РМ; • «Оканчивается на» - по конечной части наименования фонда, в котором находится РМ; • «Содержит» - включая указанную часть наименования фонда, в котором находится РМ	Ручной ввод
«Поставщик ресурсов»	Формирование списка сессий: • «Является» - по указанному наименованию поставщика ресурсов, в котором находится РМ; • «Не является» - исключая указанное наименование поставщика ресурсов, в котором находится РМ; • «Начинается с» - по начальной части наименования поставщика ресурсов, в котором находится РМ; • «Оканчивается на» - по конечной части наименования поставщика ресурсов, в котором находится РМ; • «Содержит» - включая указанную часть наименования поставщика ресурсов, в котором находится РМ	Ручной ввод

РАЗГРАНИЧЕНИЕ ФУНКЦИЙ АДМИНИСТРАТОРОВ И ПОЛЬЗОВАТЕЛЕЙ

Разграничение функций

Предусмотрено следующее разграничение функций по управлению Termidesk VDI:

- функции администратора Termidesk VDI. Администратору Termidesk VDI доступны настройка и управление программным комплексом после успешного прохождения процедуры идентификации и аутентификации. По умолчанию с администратором ассоциируется локальный пользователь операционной системы (ОС) с полномочиями администратора на узле с установленным Termidesk VDI;
- функции пользователя Termidesk VDI. Пользователь Termidesk VDI использует компонент «Клиент» или «Портал пользователя» для получения доступа к РМ;
- функции персонала (оператора) Termidesk VDI. Персонал Termidesk VDI задается администратором Termidesk VDI. Ему доступен ограниченный администратором Termidesk VDI список полномочий по доступу в графический интерфейс управления.

Тип авторизованного пользователя отображается в правом верхнем углу веб-интерфейса управления:

- «Системный пользователь» - администратор Termidesk VDI;

- «Персонал» - персонал Termidesk VDI.

Пользователь Termidesk VDI не имеет доступа к веб-интерфейсу управления, ему доступен только «Портал пользователя» для подключения к РМ.

Termidesk VDI интегрирован со встроенным комплексом средств защиты информации ОС Astra Linux Special Edition. Идентификация и аутентификация, а также защита аутентификационной информации осуществляется средствами ОС.

Также поддерживаются следующие централизованные сетевые хранилища данных о субъектах и их полномочиях (см. подраздел **Добавление доменов аутентификации**).

Назначение служебных функций администраторам

Управление ролями

В Termidesk VDI для администраторов реализовано разделение доступных служебных функций.

Для назначения доступных служебных функций следует перейти «Системные параметры - Управление ролями» и нажать экранную кнопку **[Создать]** (см. рисунок Окно назначения пользовательских разрешений).

При добавлении функции необходимо ввести текстовое наименование создаваемого класса администратора, а также выбрать список назначаемых разрешений.

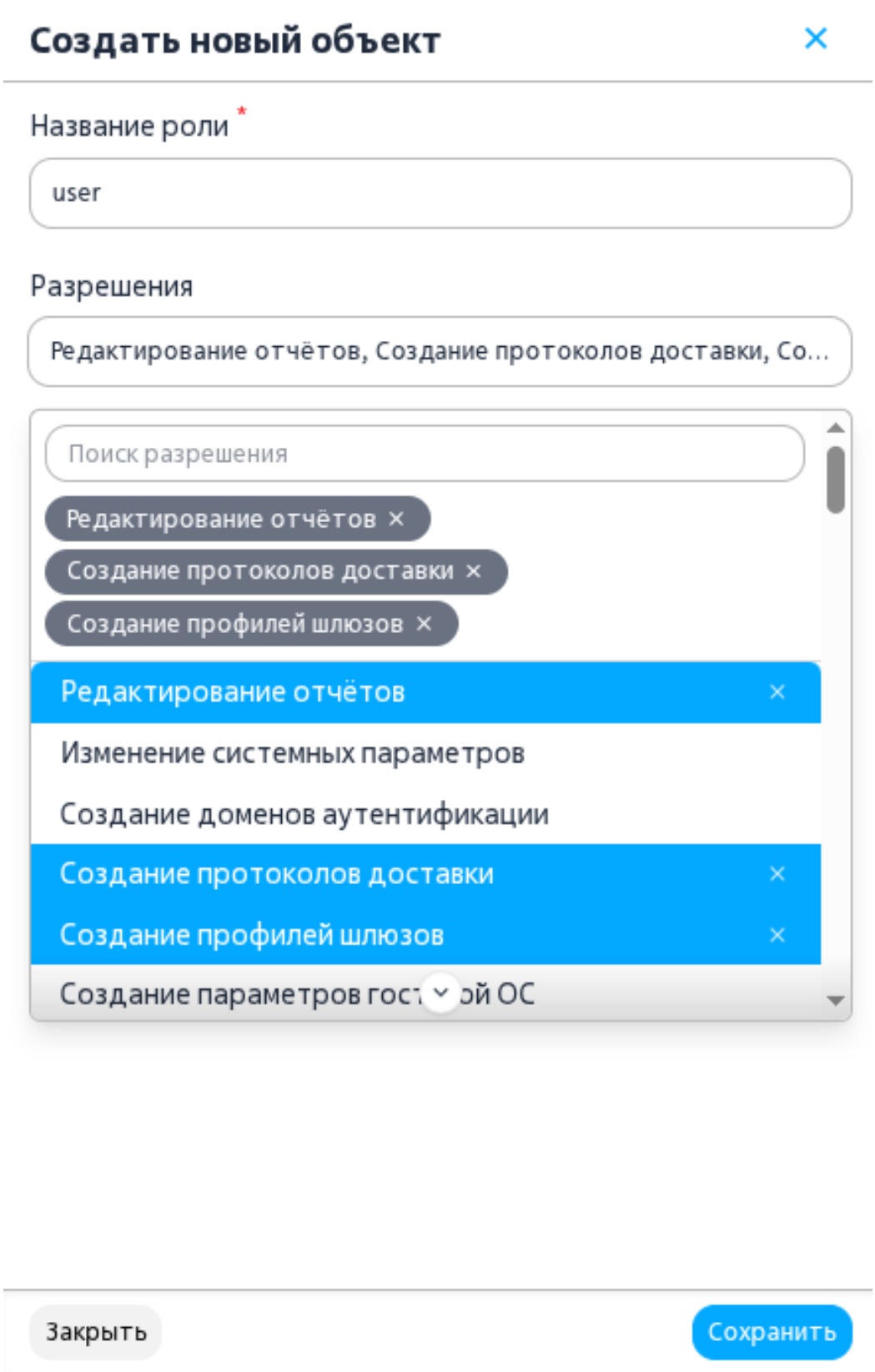


Рисунок 93. Окно назначения пользовательских разрешений

Список разрешений для назначения служебных функций администраторам перечислен в столбце «Разрешение» следующей таблицы (см. таблицу Список доступных для выбора разрешений).

Перед назначением разрешения на редактирование, создание, удаление или управление необходимо предоставить соответствующее разрешение

на просмотр страницы. Некоторые разрешения зависят от других, пример: для назначения владельца РМ потребуется предоставить права на просмотр доменов аутентификации.

Таблица 135. Список доступных для выбора разрешений

Разрешение	Описание
«Выполнение скриптов пула рабочих мест»	Разрешение позволяет выполнять скрипты на страницах: • «Рабочие места - Фонды»; • «Рабочие места - Индивидуальные рабочие места»
«Загрузка лицензии»	Разрешение позволяет загружать лицензии на странице «Лицензия»
«Изменение системных параметров»	Разрешение позволяет управлять системными параметрами на странице «Системные параметры - Системные настройки»
«Просмотр аудита»	Предоставляет доступ на чтение страницы «Журналы - Аудит»
«Просмотр групп рабочих мест»	Предоставляет доступ на чтение страницы «Рабочие места - Группы рабочих мест» для просмотра списка созданных групп РМ
«Просмотр доменов аутентификации»	Предоставляет доступ на чтение страницы «Системные параметры - Домены аутентификации». Разрешение позволяет выполнять просмотр: • пользователей домена, назначенных им групп, РМ, ВМ и журнал; • списка групп домена и пользователей, входящих в каждую группу; • журнала
«Просмотр логов фермы»	Предоставляет доступ на чтение страницы «Журналы - Журналы фермы»
«Просмотр изображений в галерее»	Предоставляет доступ на чтение страницы «Рабочие места - Галерея» для просмотра списка загруженных изображений
«Просмотр лицензии»	Предоставляет доступ на чтение страницы «Лицензия» для просмотра информации о лицензии и системе
«Просмотр объектов инфраструктуры»	Предоставляет доступ на чтение страниц раздела «Инфраструктура» для просмотра информации о статусе компонентов Termidesk
«Просмотр отчётов»	Предоставляет доступ на чтение страницы «Журналы - Отчеты», позволяет просматривать список существующих отчетов и их содержимого
«Просмотр параметров гостевой ОС»	Предоставляет доступ на чтение страницы «Рабочие места - Параметры гостевых ОС» для просмотра списка созданных параметров гостевых ОС
«Просмотр политик конфигурации»	Предоставляет доступ на чтение страницы «Рабочие места - Глобальные политики» для просмотра значений параметров политик
«Просмотр пользовательских сессий»	Предоставляет доступ на чтение страницы «Рабочие места - Сессии» для просмотра списка активных сессий пользователей

Разрешение	Описание
«Просмотр поставщиков ресурсов»	Предоставляет доступ на чтение страницы «Инфраструктура - Поставщики ресурсов». Разрешение позволяет выполнять просмотр: • список созданных поставщиков ресурсов; • список созданных шаблонов РМ
«Просмотр протоколов доставки»	Предоставляет доступ на чтение страницы «Рабочие места - Протоколы доставки» для просмотра списка созданных протоколов доставки
«Просмотр профилей шлюзов»	Предоставляет доступ на чтение страницы «Рабочие места - Профили шлюзов» для просмотра списка созданных профилей шлюзов
«Просмотр расписаний»	Предоставляет доступ на чтение страницы «Рабочие места - Расписания» для просмотра списка созданных расписаний
«Просмотр сертификатов»	Предоставляет доступ на чтение сертификатов со страниц объектов инфраструктуры
«Просмотр сетей»	Предоставляет доступ на чтение страницы «Рабочие места - Сети» для просмотра списка созданных сетей
«Просмотр системных логов»	Предоставляет доступ на чтение страницы «Журналы - Системные журналы»
«Просмотр системных параметров»	Предоставляет доступ на чтение страницы «Системные параметры» для просмотра заданных системных параметров
«Просмотр скриптов в библиотеке»	Предоставляет доступ на чтение страницы «Рабочие места - Библиотека скриптов»

«Просмотр фондов рабочих мест»	Предоставляет доступ на чтение страницы «Рабочие места - Фонды». Разрешение позволяет выполнять:
	• просмотр раздела «Фонды» и выполнять действия в разделе:
	  - просматривать список опубликованных фондов РМ;
	  - просматривать вкладки «Назначенные места», «Кеш» «Пользователи», «Сети», «Протоколы доставки», «Скрипты», «Публикации», «Журнал» при выборе опубликованного фонда РМ;
	• просмотр раздела «Индивидуальные рабочие места» для просмотра информации о назначенных ВМ

«Просмотр тегов»	Предоставляет доступ на чтение страницы «Системные параметры - Управление тегами» для просмотра списка созданных тегов
«Редактирование групп рабочих мест»	Разрешение позволяет редактировать параметры групп РМ
«Редактирование доменов аутентификации»	Разрешение позволяет редактировать параметры доменов аутентификации
«Редактирование изображений в галерее»	Разрешение позволяет редактировать параметры загруженных изображений в галерее
«Редактирование объектов инфраструктуры»	Разрешение позволяет редактировать параметры объектов инфраструктуры
«Редактирование отчётов»	Разрешение позволяет редактировать отчеты и просматривать список существующих
«Редактирование параметров гостевой ОС»	Разрешение позволяет редактировать параметры гостевых ОС

Разрешение	Описание
«Редактирование политик конфигурации»	Разрешение позволяет выполнять: • редактирование политик; • сброс значения политики
«Редактирование поставщика ресурсов»	Разрешение позволяет редактировать параметры поставщиков ресурсов
«Редактирование протоколов доставки»	Разрешение позволяет редактировать параметры протоколов доставки
«Редактирование профилей шлюзов»	Разрешение позволяет редактировать параметры профилей шлюзов
«Редактирование расписаний»	Разрешение позволяет редактировать параметры расписаний
«Редактирование сертификатов»	Разрешение позволяет редактировать сертификаты на страницах объектов инфраструктуры
«Редактирование сетей»	Разрешение позволяет редактировать параметры сетей
«Редактирование скриптов в библиотеке»	Разрешение позволяет редактировать параметры скриптов
«Редактировать фонды рабочих мест»	Разрешение позволяет редактировать параметры: • созданных фондов РМ; • индивидуальных РМ
«Создание групп рабочих мест»	Разрешение позволяет создавать группы РМ
«Создание доменов аутентификации»	Разрешение позволяет добавлять домены аутентификации
«Создание изображений в галерее»	Разрешение позволяет загружать изображения в галерею
«Создание объектов инфраструктуры»	Разрешение позволяет добавлять объекты инфраструктуры
«Создание отчётов»	Разрешение позволяет создавать отчёты и просматривать список существующих
«Создание параметров гостевой ОС»	Разрешение позволяет добавлять параметры гостевых ОС
«Создание поставщика ресурсов»	Разрешение позволяет добавлять поставщиков ресурсов
«Создание протоколов доставки»	Разрешение позволяет добавлять протоколы доставки
«Создание профилей шлюзов»	Разрешение позволяет добавлять профили шлюзов
«Создание расписаний»	Разрешение позволяет добавлять расписания
«Создание сетей»	Разрешение позволяет добавлять сети
«Создание скриптов в библиотеке»	Разрешение позволяет добавлять скрипты в библиотеку
«Создать фонды рабочих мест»	Разрешение позволяет создавать фонды РМ
«Удаление групп рабочих мест»	Разрешение позволяет удалять группы РМ
«Удаление доменов аутентификации»	Разрешение позволяет удалять домены аутентификации
«Удаление изображений из галереи»	Разрешение позволяет удалять изображения из галереи
«Удаление объектов инфраструктуры»	Разрешение позволяет удалять компоненты Termidesk VDI из таблиц раздела «Инфраструктура»
«Удаление отчётов»	Разрешение позволяет удалять отчеты и просматривать список существующих
«Удаление параметров гостевой ОС»	Разрешение позволяет удалять параметры гостевых ОС
«Удаление поставщика ресурсов»	Разрешение позволяет удалять поставщиков ресурсов
«Удаление протоколов доставки»	Разрешение позволяет удалять протоколы доставки

Разрешение	Описание
«Удаление профилей шлюзов»	Разрешение позволяет удалять профили шлюзов
«Удаление расписаний»	Разрешение позволяет удалять расписания
«Удаление сертификатов»	Разрешение позволяет удалять сертификаты
«Удаление сетей»	Разрешение позволяет удалять сети
«Удаление скриптов из библиотеки»	Разрешение позволяет удалять скрипты из библиотеки
«Удалить фонды рабочих мест»	Разрешение позволяет удалять фонды РМ
«Управление группами доменов аутентификации»	Разрешение позволяет выполнять действия: • добавление группы домена аутентификации; • редактирование группы домена аутентификации; • удаление группы домена аутентификации
«Управление пользовательскими сессиями»	Разрешение позволяет выполнять действия с активными сессиями пользователей: • отключение сессии; • завершение сессии
«Управление пользователями доменов аутентификации»	Разрешение позволяет выполнять действия: • добавление пользователя домена аутентификации; • редактирование пользователя домена аутентификации; • удаление пользователя домена аутентификации

«Управление ролями»	Разрешение позволяет выполнять:
	• просмотр раздела «Управление ролями» и выполнять действия в разделе:
	  - создавать роли;
	  - редактировать роли;
	  - удалять роли;
	• просмотр раздела «Управление ACL» и выполнять действия в разделе:
	  - создавать разрешения для объектов;
	  - редактировать разрешения для объектов;
	  - удалять разрешения для объектов

«Управление списками скриптов пула рабочих мест»	Разрешение позволяет выполнять:
	• просмотр раздела «Рабочие места - Библиотека скриптов» и выполнять действия в разделе:
	  - создавать скрипты;
	  - редактировать скрипты;
	  - удалять скрипты

«Управление шаблонами рабочих мест»	Разрешение позволяет выполнять действия: • создание шаблона РМ; • редактирование шаблона РМ; • удаление шаблона РМ

Разрешение	Описание
«Управление тегами»	Разрешение позволяет выполнять действия: • создание тега; • редактирование тега; • удаление тега

Для редактирования класса администратора нужно выбрать его, а затем нажать экранную кнопку **[Изменить]**.

Для удаления нужно выбрать созданный объект, а затем нажать экранную кнопку **[Удалить]**.

Класс администратора может быть удален только в том случае, если он не назначен пользователю.

Класс администратора может быть назначен определенному пользователю. Для назначения созданного класса следует перейти «Системные параметры - Домены аутентификации» и затем в столбце «Название» сводной таблицы выбрать домен аутентификации, в который входит пользователь. На открывшейся странице в таблице «Пользователи» нужно выбрать пользователя и нажать экранную кнопку **[Изменить]**. В открывшейся форме редактирования пользователя в поле «Роли» выбрать класс (см. рисунок Окно назначения пользовательских ролей).

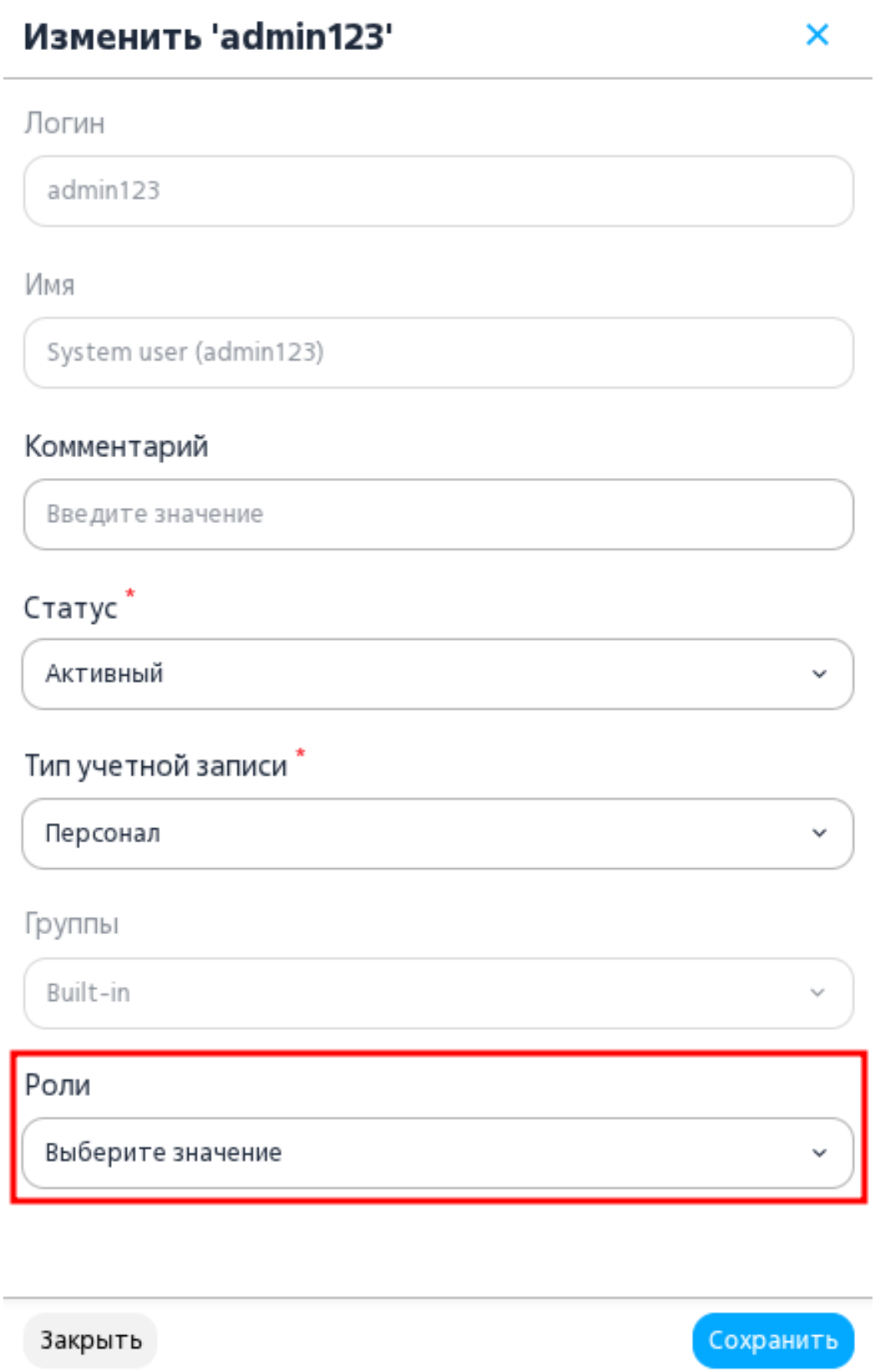


Рисунок 94. Окно назначения пользовательских ролей

Параметр «Персонал» указывает, что пользователь является оператором Termidesk VDI (класс администратора с ограниченными полномочиями в графическом интерфейсе Termidesk VDI).

Управление ACL

Созданным классам администраторов можно делегировать управление отдельными фондами РМ. Для добавления нового разрешения объекту следует перейти «Системные параметры - Управление ACL», нажать экранную кнопку **[Создать]** и выбрать «Фонд рабочих мест».

В режиме добавления нового разрешения для объекта администратору Termidesk VDI необходимо заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Доступные параметры при добавлении пользовательских разрешений для фондов РМ).

Таблица 136. Доступные параметры при добавлении пользовательских разрешений для фондов РМ

Параметр	Описание
«Роль»	Наименование заранее созданного и назначенного пользователю класса администратора
«Тип объекта»	Ранее созданный фонд РМ
«Права пользователя»	Выбор пользовательских разрешений, касающихся фондов РМ. Список всех доступных разрешений, можно выбрать несколько: • «Восстановить рабочие места»; • «Просмотр фондов рабочих мест»; • «Редактировать фонды рабочих мест»; • «Удалить фонды рабочих мест»; • «Управление питанием фонда рабочих мест»; • «Управление группами пользователей фонда рабочих мест»; • «Управление пользователями фонда рабочих мест»; • «Управление протоколами доставки фонда рабочих мест»; • «Управление публикациями фонда рабочих мест»; • «Управление рабочими местами в фонде»; • «Управление сетевыми списками фонда рабочих мест»

При изменении ранее созданного разрешения параметр «Объект» менять не рекомендуется. Если нужно изменить непосредственно объект, то следует создать новое разрешение.

СИСТЕМНЫЕ НАСТРОЙКИ

Конфигурационные файлы сервера Termidesk VDI

Конфигурационный файл `termidesk.conf`

Для настройки сервера Termidesk VDI («Универсальный диспетчер», «Агрегатор», «Менеджер рабочих мест», «Брокер сообщений TermideskMQ») используется конфигурационный файл `/etc/opt/termidesk-vdi/termidesk.conf`.

Каталог хранения конфигурационного файла `termidesk.conf` и указанные ниже параметры можно изменить через утилиту `termidesk-config`.

При установке пакета `termidesk-vdi` возможно активировать режим отладки инсталлятора через переменную окружения `TDSK_DEBUG=1`.

Полный перечень параметров, задающихся через файл, приведен в таблице (см. таблицу Параметры файла termidesk.conf).

Таблица 137. Параметры файла termidesk.conf

Параметр	Значение по умолчанию	Описание
Настройка режима работы ПО		
TERMIDESK_FARM_MODE	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора», «Брокера сообщений TermideskMQ». Определяет режим работы Termidesk VDI. Возможные значения: • BROKER - установка фермы «Универсального диспетчера»; • AGGREGATOR - установка фермы «Агрегатора». При обновлении Termidesk VDI пытается автоматически определить предыдущий режим установки и использовать нужное значение на узлах с «Порталами» «Универсального диспетчера». В случаях с другими узлами требуется указать значение вручную
Настройки установленных ролей Termidesk		
NODE_ROLES	Не задано	Параметр обязателен и задается на этапе установки на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора», «Брокера сообщений TermideskMQ». Определяет тип роли, с которой будет установлен Termidesk VDI. Возможные значения: • ADMIN - роль «Портал администратора» (ферма «Универсального диспетчера») или «Агрегатор администратора» (ферма «Агрегатора»); • USER - роль «Портал пользователя» (ферма «Универсального диспетчера») или «Агрегатор пользователя» (ферма «Агрегатора»); • CELERYMAN - роль «Менеджер рабочих мест»; • TERMQ - роль «Брокер сообщений». При переустановке значение параметра в конфигурационном файле будет перезаписано
Настройка языка сервера Termidesk		
LANGUAGE_CODE	en	Параметр обязателен и задается на этапе установки. Определяет язык сервера Termidesk VDI, использующийся по умолчанию. Значение соответствует коду языка согласно ISO-639-1
Настройка уникального имени узла		

Параметр	Значение по умолчанию	Описание
NODE_NAME	Не задано	Параметр обязателен и задается на этапе установки. Определяет уникальное имя узла для его идентификации в различных структурах Termidesk VDI. В частности: * для идентификации узлов «Агрегатора» во время балансировки подключений к ним; * для отображения узла в разделе «Инфраструктура» «Портала администратора» Следует задавать уникальное имя узла понятным и отражающим его роль, например «AdminPortal-01», «UserPortal-01». По умолчанию для заполнения параметра используется заданный в системе hostname и буквенно-числовой идентификатор
Настройка проверки данных при взаимодействии компонентов Termidesk		
DJANGO_SECRET_KEY	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Используется для проверки данных, пересылаемых между компонентами Termidesk VDI. Значение генерируется при установке Termidesk VDI и должно быть одинаковым для всех узлов при распределенной установке. Параметр может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: DJANGO_SECRET_KEY='hvac-kv://secret#termidesk-admin/django/key' Если параметр располагается в хранилище паролей, то все параметры, ранее заданные с преобразованными через утилиту scramble значениями, должны быть указаны с открытыми значениями (RABBITMQ_URL, DBPASS и др.). Это ограничение связано с тем, что при выборе на этапе установки хранилища для параметров подразумевается, что защита чувствительных данных реализуется только через хранилище
Настройки токена доступа к API для проверок состояния служб Termidesk		

Параметр	Значение по умолчанию	Описание
HEALTH_CHECK_ACCESS_KEY	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет токен доступа к API проверки состояния сервера. Начальное значение генерируется на этапе установки. При задании значения параметра следует руководствоваться правилом, что: • размер должен составлять от 0 до 64 символа; • должны использоваться символы в шестнадцатеричной системе (0-9, a-f). Значение также может быть сгенерировано через openssl: openssl rand -hex 32. Параметр может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: HEALTH_CHECK_ACCESS_KEY='hvac-kv://secret#termidesk-admin/tokens/healthcheck'
Настройки токена доступа к API получения метрик узла		
METRICS_ACCESS_KEY	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет токен доступа к API получения метрик узла. Начальное значение генерируется на этапе установки. При задании значения параметра следует руководствоваться правилом, что: • размер должен составлять от 0 до 64 символа; • должны использоваться символы в шестнадцатеричной системе (0-9, a-f). Значение также может быть сгенерировано через openssl: openssl rand -hex 32. Параметр может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: METRICS_ACCESS_KEY='hvac-kv://secret#termidesk-admin/tokens/metrics'
Настройки подключения к СУБД		
DB_CLUSTER_MODE	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет тип установки СУБД, к которой осуществляется подключение. Возможные значения: • single - подключение производится к отдельному серверу СУБД; • cluster - подключение производится к кластеру СУБД, адреса нод которого заданы в DBHOST, DBHOST2, DBHOST3. Termidesk VDI будет последовательно обращаться к заданным адресам нод, пока не подключится к мастер-ноде

Параметр	Значение по умолчанию	Описание
DBHOST	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет IP-адрес или FQDN СУБД PostgreSQL. Начальное значение задается на этапе подготовке среды функционирования и установки Termidesk
DBHOST2	Не задано	Параметр необязательный, может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет IP-адрес или FQDN дополнительного узла СУБД PostgreSQL, если используется подключение к кластеру СУБД (см. параметр DB_CLUSTER_MODE). Начальное значение задается на этапе установки Termidesk
DBHOST3	Не задано	Параметр необязательный, может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет IP-адрес или FQDN дополнительного узла СУБД PostgreSQL, если используется подключение к кластеру СУБД (см. параметр DB_CLUSTER_MODE). Начальное значение задается на этапе установки Termidesk
DBPORT	5432	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет порт соединения с сервером БД
DBSSL	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет протокол подключения к БД. Возможные значения: • Disable; • TLSv1.2; • TLSv1.3. Начальное значение задается на этапе установки Termidesk
DBNAME	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет имя БД. Начальное значение задается на этапе подготовки среды функционирования перед установкой Termidesk
DBUSER	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет имя пользователя, имеющего доступ к БД. Начальное значение задается на этапе подготовки среды функционирования перед установкой Termidesk

Параметр	Значение по умолчанию	Описание
DBPASS	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет пароль пользователя, имеющего доступ к БД. Начальное значение задается на этапе подготовки среды функционирования во время установки Termidesk VDI и хранится в конфигурационном файле termidesk.conf в преобразованном виде. В стандартных установках значение менять не следует. Чтобы получить преобразованное значение пароля, следует воспользоваться утилитой scramble: • для получения значения по стандартному алгоритму (не рекомендуется): /opt/termidesk/bin/scramble --value <пароль> --type AES256; • для получения значения с увеличенным числом итераций преобразования (рекомендуется): /opt/termidesk/bin/scramble --value <пароль> --type AES256_V2 Если значение пароля указывается в формате ключа (значение предваряется символом «-»), то следует изменить его передачу в параметр --value: /opt/termidesk/bin/scramble --value=←пароль> --type AES256_V2 Если конфигурационный файл termidesk.conf хранится в каталоге, отличном от /etc/opt/termidesk-vdi/, может потребоваться указание дополнительного параметра --config в утилите scramble.
DBCERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к клиентскому сертификату mTLS для защищенного подключения к БД. mTLS - метод обеспечения защищенного соединения с БД через двустороннюю аутентификацию с использованием сертификатов. Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt • установить корневой сертификат ЦС. Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: DBCERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'

Параметр	Значение по умолчанию	Описание
DBKEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к ключу mTLS для защищенного подключения к БД. Ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению: openssl rsa -in <путь_к_файлу_ключа.key> -out <путь_сохранения_преобразованного_ключа.key> Для использования ключа нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key • установить корневой сертификат ЦС, если ранее он не был установлен. Ключ может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: DBKEY='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/key'
DBCHAIN	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к промежуточному сертификату mTLS для защищенного подключения к БД. Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem • установить корневой сертификат ЦС, если ранее он не был установлен. Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему. Пример задания сертификата из хранилища: DBCHAIN='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/ca'

Параметр	Значение по умолчанию	Описание
DB_CONN_MAX_AGE	0	Максимально допустимое время (в секундах) существования одного подключения к БД. Параметр управляет жизненным циклом подключения к БД для Django. Для корректной работы это значение должно быть меньше аналогичной настройки на БД, которая может закрывать простаивающие подключения по истечении времени. Значение 0: • обеспечивает совместимость с предыдущими версиями Termidesk VDI; • определяет, что подключения к БД будут закрыты после обработки HTTP-запроса
CELERY_DB_REUSE_MAX	1000	Количество фоновых задач, которое может быть выполнено в рамках одного подключения к БД. По достижении этого количества подключение к БД пересоздастся. Параметр управляет жизненным циклом подключения к БД для служб celery «Менеджера рабочих мест»
DB_CONN_TIMEOUT	10	Время ожидания (в секундах) подключения к БД
Настройки «Менеджера рабочих мест» для распределенной установки		

CELERY_BEAT_PRIMARY_CHECK_INTERVAL	30	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».
		
		Определяет интервал (в секундах) проверки доступности главного процесса среди всех экземпляров «Менеджера рабочих мест» (службы termidesk-celery-beat).
		
		Параметры CELERY_BEAT_PRIMARY_CHECK_INTERVAL и CELERY_BEAT_PRIMARY_LOCK_TIMEOUT реализуют механизм корректной работы termidesk-celery-beat при распределенной установке:
		
		• при запуске нескольких экземпляров termidesk-celery-beat каждый из них пытается сделать запись в кеше БД. БД используется одна на все экземпляры;
		• если экземпляр termidesk-celery-beat:
		  - делает запись в БД, то он отправляет сообщения в очередь брокера сообщений;
		  - не делает запись в БД, то он ожидает своей очереди на добавление записи

CELERY_BEAT_PRIMARY_LOCK_TIMEOUT	45	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет время (в секундах) действия блокировки главного процесса среди всех экземпляров «Менеджера рабочих мест» (службы termidesk-celery-beat). Значение параметра CELERY_BEAT_PRIMARY_LOCK_TIMEOUT должно превышать значение CELERY_BEAT_PRIMARY_CHECK_INTERVAL. Это необходимо для возможности продления интервала проверки главным процессом termidesk-celery-beat
Настройка таймаутов задач «Менеджера рабочих мест»		

Параметр	Значение по умолчанию	Описание
REGISTRATIONS_PROVIDERS_TASK_RESOLVE_TIMEOUT	5	Параметр необязательный, может быть задан на узлах «Менеджера рабочих мест». Через утилиту termidesk-config не задается. Определяет время (в секундах) ожидания разрешения имени узла в IP-адрес в задаче синхронизации регистрации компонента «Сессионный агент» в Метапоставщиках
REGISTRATIONS_PROVIDERS_TASK_TIMEOUT	54	Параметр необязательный, может быть задан на узлах «Менеджера рабочих мест». Через утилиту termidesk-config не задается. Определяет время (в секундах) выполнения задачи синхронизации регистрации компонента «Сессионный агент» в Метапоставщиках. Если задача не завершится за отведенное время, то произойдет ожидание завершения последней блокирующей операции и остановка службы termidesk-celery-worker. Значение 0 отключает таймаут. При установке отрицательного значения задачи не будут выполнены.
CELERY_TASK_TIME_LIMIT	0	Параметр необязательный, может быть задан на узлах «Менеджера рабочих мест». Через утилиту termidesk-config не задается. Определяет глобальное время (в секундах) выполнения задач службы termidesk-celery-worker. Значение 0 отключает ограничение времени выполнения. Если задано ненулевое значение и в журнале службы появляются ошибки «TimeoutError: The read operation timed out», значение следует увеличить.
Настройка подключения к брокеру сообщений (RabbitMQ или TermideskMQ)		

Параметр	Значение по умолчанию	Описание
RABBITMQ_URL	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет URL-адрес подключения к серверам брокера сообщений. Параметр используется как для RabbitMQ, так и для TermideskMQ. Можно подключить до трех (включительно) серверов. Пароль подключения к брокеру сообщений, указанный в RABBITMQ_URL, хранится в конфигурационном файле termidesk.conf в преобразованном виде. Чтобы получить преобразованное значение пароля, следует воспользоваться утилитой scramble: • для получения значения по стандартному алгоритму (не рекомендуется): /opt/termidesk/bin/scramble --value <пароль> --type AES256; • для получения значения с увеличенным числом итераций преобразования (рекомендуется): /opt/termidesk/bin/scramble --value <пароль> --type AES256_V2. Если значение пароля указывается в формате ключа (значение предваряется символом «-»), то следует изменить его передачу в параметр --value: /opt/termidesk/bin/scramble --value=←пароль> --type AES256_V2 Если конфигурационный файл termidesk.conf хранится в каталоге, отличном от /etc/opt/termidesk-vdi/, может потребоваться указание дополнительного параметра --config. Для использования преобразованного значения следует указать его в RABBITMQ_URL и выполнить перезапуск служб. Начальное значение RABBITMQ_URL задается на этапе установки
RABBITMQ_SSL	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет протокол подключения к брокеру сообщений. Параметр используется как для RabbitMQ, так и для TermideskMQ. Возможные значения: Disable, TLSv1.2. Начальное значение задается на этапе установки
Настройки защищенного подключения к брокеру сообщений (RabbitMQ или TermideskMQ)		

Параметр	Значение по умолчанию	Описание
CELERY_BROKER_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к клиентскому сертификату mTLS для защищенного подключения к брокеру сообщений (RabbitMQ или TermideskMQ). Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt; • установить корневой сертификат ЦС, если ранее он не был установлен. Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: CELERY_BROKER_CERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'
CELERY_BROKER_KEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к закрытому ключу mTLS для защищенного подключения к брокеру сообщений (RabbitMQ или TermideskMQ). Ключ может иметь парольную защиту. Для использования в Termidesk VDI нужно преобразовать его к начальному значению: openssl rsa -in <путь_к_файлу_ключа.key> -out <путь_сохранения_преобразованного_ключа.key>. Для использования ключа нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key; • установить корневой сертификат ЦС, если ранее он не был установлен. Ключ может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: CCELERY_BROKER_KEY='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/key'

Параметр	Значение по умолчанию	Описание
CELERY_BROKER_CA	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к корневому сертификату ЦС mTLS для защищенного подключения к брокеру сообщений (RabbitMQ или TermideskMQ). Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt; • установить корневой сертификат ЦС. Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: CELERY_BROKER_CA='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/ca'
Настройки журналирования		
LOG_LEVEL	INFO	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет уровень журналирования сообщений. Возможные значения: DEBUG, INFO, WARNING, ERROR, CRITICAL. Включение уровня DEBUG может привести к повышенной нагрузке системы, поэтому после сбора подробных журналов следует вернуть значение к уровню INFO
LOG_ADDRESS	/dev/log	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет адрес отправки записей в системный журнал. Обычно это /dev/log для Linux-систем. Возможно указать IP-адрес и порт
LOG_FACILITY	local3	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет категорию сообщений syslog. Категория должна совпадать с настройками в конфигурационном файле /etc/syslog-ng/conffirst.d/termidesk.conf. При редактирование параметра через утилиту termidesk-config нужные значения в настройку syslog-ng будут подставлены автоматически
Настройки шаблонов для регистрации событий и журналирования (syslog-ng и logrotate)		

Параметр	Значение по умолчанию	Описание
LOG_DIR	/var/log/termidesk	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к каталогу с журналами, используется в настройках шаблонов logrotate и syslog-ng. Путь к шаблонам определен в файле /etc/default/termidesk-vdi.local. Каталог должен обладать следующими свойствами: • права доступа: rwxr-x--- (в восьмеричной записи - 750); • владелец и группа: root:termidesk. Рекомендуется выполнять изменение параметра через утилиту termidesk-config. Если изменение параметра выполнено вручную, то требуется выполнить команду: sudo /opt/termidesk/sbin/termidesk-config update_logger_config
LOG_OWNER	termidesk	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет владельца файлов журналов, используется в настройках шаблонов logrotate и syslog-ng. Путь к шаблонам определен в файле /etc/default/termidesk-vdi.local. Рекомендуется выполнять изменение параметра через утилиту termidesk-config. Если изменение параметра выполнено вручную, то требуется выполнить команду: sudo /opt/termidesk/sbin/termidesk-config update_logger_config
LOG_GROUP	adm	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет группу-владельца файлов журналов, используется в настройках шаблонов logrotate и syslog-ng. Путь к шаблонам определен в файле /etc/default/termidesk-vdi.local. Рекомендуется выполнять изменение параметра через утилиту termidesk-config. Если изменение параметра выполнено вручную, то требуется выполнить команду: sudo /opt/termidesk/sbin/termidesk-config update_logger_config
LOG_PERM	0440	Параметр может быть задан на узлах «Универсального диспетчера»,«Менеджера рабочих мест», «Агрегатора». Определяет права доступа к файлам журналов, используется в настройках шаблонов logrotate и syslog-ng. Путь к шаблонам определен в файле /etc/default/termidesk-vdi.local. Рекомендуется выполнять изменение параметра через утилиту termidesk-config. Если изменение параметра выполнено вручную, то требуется выполнить команду: sudo /opt/termidesk/sbin/termidesk-config update_logger_config

Параметр	Значение по умолчанию	Описание
LOG_DEEP	14	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет количество устаревеших файлов журналов, которое нужно хранить. Используется в настройках шаблонов logrotate и syslog-ng. Путь к шаблонам определен в файле /etc/default/termidesk-vdi.local. Рекомендуется выполнять изменение параметра через утилиту termidesk-config. Если изменение параметра выполнено вручную, то требуется выполнить команду: sudo /opt/termidesk/sbin/termidesk-config update_logger_config
INTERNAL_AUDIT	Disabled	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет включение или отключение записи событий аудита с анонимным пользователем в БД. Анонимный пользователь AnonymousUser(AnonymousAuth) указывается для запросов, выполняемых без аутентификации. Возможные значения: • Enabled - запись событий аудита с анонимным пользователем включена; • Disabled - запись событий аудита с анонимным пользователем отключена
Настройки защищенного подключения для проверок состояния служб «Менеджера рабочих мест»		
HEALTH_CHECK_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора» (в зависимости от варианта установки). Определяет путь к сертификату SSL/TLS для защищенного подключения к API проверки состояния служб «Менеджера рабочих мест». Для использования сертификата нужно: * скопировать его в каталог /etc/opt/termidesk-vdi/; * назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt; * изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt; * установить корневой сертификат ЦС, если ранее он не был установлен. Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: HEALTH_CHECK_CERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'

Параметр	Значение по умолчанию	Описание
HEALTH_CHECK_KEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера»,«Менеджера рабочих мест», «Агрегатора» (в зависимости от варианта установки). Определяет путь к ключу SSL/TLS для защищенного подключения к API проверки состояния служб «Менеджера рабочих мест». Ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению: openssl rsa -in <путь_к_файлу_ключа.key> -out <путь_сохранения_преобразованного_ключа.key> Для использования ключа нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key; • установить корневой сертификат ЦС, если ранее он не был установлен. Ключ может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: HEALTH_CHECK_KEY='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/key'
Настройки проверок состояния (health check)		
CELERY_BEAT_HEALTH_CHECK_PORT	8103	Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест». Определяет порт, на котором работает веб-сервер для обслуживания API проверки состояния компонента «Менеджер рабочих мест» (службы termidesk-celery-beat). Изначально параметр закомментирован (используется значение по умолчанию)
CELERY_BEAT_HEALTH_CHECK_IP	0.0.0.0	Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест». Определяет IP-адрес, с которым служба termidesk-celery-beat регистрируется в подсистеме проверки состояния на странице «Инфраструктура» Termidesk VDI. Опрос состояния службы будет проводиться по этому адресу. Если IP-адрес не задан, то будет использоваться имя (hostname) или FQDN узла. Изначально параметр закомментирован (используется значение по умолчанию)
CELERY_WORKER_HEALTH_CHECK_PORT	8104	Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест». Определяет порт, на котором работает веб-сервер для обслуживания API проверки состояния компонента «Менеджер рабочих мест» (службы termidesk-celery-worker). Изначально параметр закомментирован (используется значение по умолчанию)

Параметр	Значение по умолчанию	Описание
CELERY_WORKER_HEALTH_CHECK_IP	0.0.0.0	Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест». Определяет IP-адрес, с которым служба termidesk-celery-worker регистрируется в подсистеме проверки состояния на странице «Инфраструктура». Опрос состояния службы будет проводиться по этому адресу. Если IP-адрес не задан, то будет использоваться имя (hostname) или FQDN узла. Изначально параметр закомментирован (используется значение по умолчанию)
HEALTH_CHECK_TIMEOUT	10	Таймаут (в секундах) обработки запроса проверки состояния. По истечении указанного времени: • возвращается стандартная для health check структура ответа; • проверки, которые не успели завершиться, приобретают статус «fail» с причиной «timeout»
CELERY_HEALTH_CHECK_CHECKS	Не задано	Определяет список проверок состояния, выполняемые узлом «Менеджер рабочих мест» (службами termidesk-celery-beat и termidesk-celery-worker). Таймаут обработки запроса проверки состояния определяется параметром HEALTH_CHECK_TIMEOUT. Возможные значения: • db - проверка БД (проверяется подключение); • rabbit - проверка брокера сообщений (проверяется состояние); • fluentd - проверка компонента «Ретранслятор» (проверяется состояние и отправляется тестовое сообщение). Если значение не задано, то выполняются все проверки
TERMIDESK_HEALTH_CHECK_CHECKS	Не задано	Определяет список проверок состояния, выполняемые узлом «Универсальный диспетчер». Таймаут обработки запроса проверки состояния определяется параметром HEALTH_CHECK_TIMEOUT. Возможные значения: • celery - проверка компонента «Менеджер рабочих мест» (проверяется состояние обработчика); • db - проверка БД (проверяется подключение); • rabbit - проверка брокера сообщений (проверяется состояние); • fluentd - проверка компонента «Ретранлятор» (проверяется состояние и отправляется тестовое сообщение). Если значение не задано, то выполняются все проверки

Параметр	Значение по умолчанию	Описание
AGGREGATOR_HEALTH_CHECK_CHECKS	Не задано	Определяет список проверок состояния, выполняемые узлом «Агрегатор». Таймаут обработки запроса проверки состояния определяется параметром HEALTH_CHECK_TIMEOUT. Возможные значения: • celery - проверка компонента «Менеджер рабочих мест» (проверяется состояние обработчика); • db - проверка БД (проверяется подключение); • rabbit - проверка брокера сообщений (проверяется состояние); • fluentd - проверка компонента «Ретранлятор» (проверяется состояние и отправляется тестовое сообщение); • sites - проверка сайтов «Агрегатора» (проверяется состояние сайтов, в случае неактивности выполняется перевод в статус «warning»). Если значение не задано, то выполняются все проверки
Настройки подключения к серверу «Удаленного помощника»		
REMOTE_ASSISTANT_SERVER_CA	Не задано	Параметр может быть задан на узлах «Универсального диспетчера» («Портал администратора», «Портал пользователя»). Определяет путь к корневому сертификату SSL/TLS и используется для проверки подключения к «Удаленному помощнику» (проверка того, что подключение происходит к нужному серверу «Удаленного помощника»). Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem; • установить корневой сертификат ЦС, если ранее он не был установлен. Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: REMOTE_ASSISTANT_SERVER_CA='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'
Настройки доверенных корневых сертификатов		

Параметр	Значение по умолчанию	Описание
REQUESTS_CA_BUNDLE	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к файлу с доверенным корневым сертификатом, задается для настройки работы с сертификатами собственных ЦС. По умолчанию параметр не используется (закомментирован). Параметр является переменной окружения. Рекомендуется задать его в файле termidesk.conf и в /etc/default/termidesk-vdi.local, иначе его обработка не гарантируется
Настройка веб-сервера Apache		
HTTP_SERVER_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет путь к файлу с серверным сертификатом для веб-сервера Apache. Если для хранения чувствительной информации используется хранилище паролей OpenBao или Hashicorp Vault и заданы пути к сертификатам и ключам из хранилища, то они будут скопированы в каталог /dev/shm/: • /dev/shm/http.crt; • /dev/shm/http.key; • /dev/shm/http_ca.crt. При этом обновление сертификата, если такое предусмотрено, будет выполняться на веб-сервере автоматически через службу termidesk-watchdog.service и файл /lib/systemd/system/termidesk-watchdog.path. Если сертификаты и ключи не заданы в параметрах, то будут использоваться сертификаты и ключи по умолчанию (из ОС)
HTTP_SERVER_KEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет путь к файлу с закрытым ключом для веб-сервера Apache. Условия использования аналогичны параметру HTTP_SERVER_CERT
HTTP_SERVER_CA	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет путь к файлу с цепочкой сертификатов корневого и промежуточного УЦ для веб-сервера Apache. Условия использования аналогичны параметру HTTP_SERVER_CERT

Параметр	Значение по умолчанию	Описание
DJANGO_ALLOWED_HOSTS	*	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет список имен или IP-адресов узла, разделенных запятыми, на которые будет отвечать веб-сервер Apache. Рекомендуется использование параметра для повышения безопасности и снижения риска атак через HTTP-заголовки. По умолчанию разрешены любые узлы
DJANGO_SECURE_SSL_REDIRECT	True	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет режим обработки запросов: перенаправлять HTTP-запросы на HTTPS или нет. Возможные значения: • True - все HTTP-запросы перенаправятся на HTTPS; • False - перенаправление на HTTPS не осуществляется. Использование значения имеет практический смысл в случае, если в настройках веб-сервера Apache включена обработка HTTP-запросов
DJANGO_SECURE_HSTS_SECONDS	0	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет установку HTTP-заголовка Strict Transport Security. Если параметр задан ненулевым значением, то заголовок будет установлен во всех ответах, не содержащих его Настройка всех HSTS-параметров должна выполняться только после того, как узлу будет назначено корректное имя, а в настройках веб-сервера Apache будут заданы действующие сертификаты. В противном случае можно потерять доступ к веб-интерфейсу на время, указанное в DJANGO_SECURE_HSTS_SECONDS. Рекомендуется проверить корректность работы механизма на небольшом временном интервале и только после проверки устанавливать в параметре более длительное время.

Параметр	Значение по умолчанию	Описание
DJANGO_SECURE_HSTS_INCLUDE_SUBDOMAINS	False	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет установку директивы includeSubDomains в HTTP-заголовок Strict Transport Security. Возможные значения: • True - директива подставится в HTTP-заголовок; • False - директива не подставится в HTTP-заголовок Настройка всех HSTS-параметров должна выполняться только после того, как узлу будет назначено корректное имя, а в настройках веб-сервера Apache будут заданы действующие сертификаты. В противном случае можно потерять доступ к веб-интерфейсу на время, указанное в DJANGO_SECURE_HSTS_SECONDS.
DJANGO_SECURE_HSTS_PRELOAD	False	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет установку директивы preload в HTTP-заголовок Strict Transport Security. Возможные значения: • True - директива подставится в HTTP-заголовок; • False - директива не подставится в HTTP-заголовок Настройка всех HSTS-параметров должна выполняться только после того, как узлу будет назначено корректное имя, а в настройках веб-сервера Apache будут заданы действующие сертификаты. В противном случае можно потерять доступ к веб-интерфейсу на время, указанное в DJANGO_SECURE_HSTS_SECONDS.
Настройки, связанные с лицензированием		
EULA_ACCEPTED	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет принятие лицензионного соглашения при установке. В случае автоматизированной установки наличие параметра обязательно

Параметр	Значение по умолчанию	Описание
LICENSE_CACHE_TIME	0	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест». Определяет время (в секундах) кеширования данных о лицензии для внутренних процессов Termidesk VDI. Если срок кеширования истек, то следующее обращение к лицензии вызовет: • ее считывание из БД; • обновление времени кеширования. Возможные значения: • 0 - кеширование данных о лицензии отключено; • значение, большее 0 - кеширование данных о лицензии включено. Если была добавлена новая лицензия, то данные о ней не будут отображаться до истечения времени кеширования
Настройки узла «Агрегатора» и его взаимодействия с «Универсальным диспетчером»		
AGGREGATOR_JWT_SSL_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», использующихся в фермах, подключаемых к «Агрегатору». Обязателен для заполнения в случае, если в инфраструктуре используется «Агрегатор». Определяет путь к сертификату для получения значения JWT-токена «Агрегатора». Для использования сертификата нужно: * скопировать его в каталог /etc/opt/termidesk-vdi/; * назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem; * изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem; * установить корневой сертификат ЦС, если ранее он не был установлен. Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: AGGREGATOR_JWT_SSL_CERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'

Параметр	Значение по умолчанию	Описание
AGGREGATOR_JWT_SSL_CERT_SECOND	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», использующихся в фермах, подключаемых к «Агрегатору». Обязателен для заполнения в случае, если в инфраструктуре используется «Агрегатор». Определяет путь к резервному сертификату для получения значения JWT-токена «Агрегатора». Если сертификат, заданный в AGGREGATOR_JWT_SSL_CERT, станет невалидным, то будет использоваться сертификат, указанный в AGGREGATOR_JWT_SSL_CERT_SECOND. Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem; • установить корневой сертификат ЦС, если ранее он не был установлен. Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: AGGREGATOR_JWT_SSL_CERT_SECOND='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pemsecond'
AGGREGATOR_JWT_SSL_KEY	Не задано	Параметр обязателен и задается на узлах «Агрегатора» (портал «Агрегатор пользователя» и портал «Агрегатор администратора»), «Менеджера рабочих мест». Определяет путь к ключу для подписи JWT-токена «Агрегатора». Для использования ключа нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key; • установить корневой сертификат ЦС, если ранее он не был установлен. Ключ может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: AGGREGATOR_JWT_SSL_KEY='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/key'

Параметр	Значение по умолчанию	Описание
AGGREGATOR_YAML_FILE	Не задано	Параметр задается на узлах с установленным «Агрегатором». Параметр определяет путь к файлу mapping.yaml, содержащему сопоставление между именами узлов (NODE_NAME) «Агрегатора» и их полным доменным именем (FQDN) или IP-адресом. При работе с географической балансировкой (GSLB) файл должен быть одинаков на всех узлах распределенной установки «Агрегатора» для корректной обработки переключений между узлами и фермами «Агрегатора». Файл может располагаться в файловой системе узла или в хранилище чувствительной информации: AGGREGATOR_YAML_FILE='/etc/opt/termidesk-vdi/mapping.yaml'
Настройки подключения к хранилищу паролей OpenBao		
SECRETS_STORAGE_METHOD	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет способ хранения паролей подключения к СУБД и RabbitMQ: • config - пароли будут храниться в преобразованном виде в файле termidesk.conf; • hvac - для хранения паролей будет использоваться хранилище паролей OpenBao или Hashicorp Vault (хранилище должно быть заранее создано и настроено); • openbao - для хранения паролей будет использоваться хранилище паролей OpenBao (хранилище должно быть заранее создано и настроено). При этом пароли располагаются внутри хранилища, имена контейнеров хранения генерируются автоматически. Если для хранения чувствительной информации используется хранилище паролей OpenBao или Hashicorp Vault и в параметрах HTTP_SERVER_CERT, HTTP_SERVER_KEY, HTTP_SERVER_CA заданы пути к сертификатам и ключам из хранилища, то они будут скопированы для веб-сервера Apache (см. описание параметров). Хранилище паролей OpenBao должно быть реализовано в отказоустойчивом варианте, иначе Termidesk VDI не будет работать в период простоя узлов OpenBao. Начальное значение задается на этапе установки

Параметр	Значение по умолчанию	Описание
SECRETS_OPENBAO_URL	http://openbao:8200	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет IP-адреса или FQDN узла и порта с установленным хранилищем OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Формат: http://<IP-адрес или FQDN>:8200. Подключение может выполняться по протоколу HTTPS, если OpenBao настроен соответствующим образом. Начальное значение задается на этапе установки. Пример задания параметра: SECRETS_OPENBAO_URL='http://127.0.0.1:8200'
SECRETS_OPENBAO_KV_VERSION	1	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Используется для указания версии API OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Возможные значения: • 1 (по умолчанию); • 2. Начальное значение задается на этапе установки. Пример задания параметра: SECRETS_OPENBAO_KV_VERSION=1

Параметр	Значение по умолчанию	Описание
SECRETS_OPENBAO_CLIENT_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к сертификату mTLS для начального защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы. Особенности функционирования: • если параметры SECRETS_OPENBAO_CLIENT_CERT и SECRETS_OPENBAO_CLIENT_KEY заданы, то выполняется защищенное соединение по протоколу TLS; • если параметры SECRETS_OPENBAO_CLIENT_CERT и SECRETS_OPENBAO_CLIENT_KEY не заданы, то выполняется незащищенное соединение; • если помимо параметров SECRETS_OPENBAO_CLIENT_CERT, SECRETS_OPENBAO_CLIENT_KEY задан SECRETS_OPENBAO_SERVER_CERT, то выполняется защищенное соединение по протоколу mTLS; • сертификат должен размещаться в файловой системе узла (внешнее хранилище не используется). Начальное защищенное соединение настраивается в случаях, если сертификаты имеют продолжительный срок действия или их обновление производится средствами, отличными от OpenBao. В случае, если у сертифкатов непродолжительный срок действия или их обновление производится через OpenBao, следует выполнить настройку параметр SECRETS_OPENBAO_PKI_CERTS. Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt; • установить корневой сертификат ЦС, если ранее он не был установлен. Пример задания параметра: SECRETS_OPENBAO_CLIENT_CERT='/etc/opt/termidesk-vdi/openbao-client.crt'

Параметр	Значение по умолчанию	Описание
SECRETS_OPENBAO_CLIENT_KEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к ключу mTLS для начального защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы. Особенности функционирования: • если параметры SECRETS_OPENBAO_CLIENT_CERT и SECRETS_OPENBAO_CLIENT_KEY заданы, то выполняется защищенное соединение по протоколу TLS; • если параметры SECRETS_OPENBAO_CLIENT_CERT и SECRETS_OPENBAO_CLIENT_KEY не заданы, то выполняется незащищенное соединение; • если помимо параметров SECRETS_OPENBAO_CLIENT_CERT, SECRETS_OPENBAO_CLIENT_KEY задан SECRETS_OPENBAO_SERVER_CERT, то выполняется защищенное соединение по протоколу mTLS; • ключ должен размещаться в файловой системе узла (внешнее хранилище не используется). Начальное защищенное соединение настраивается в случаях, если сертификаты имеют продолжительный срок действия или их обновление производится средствами, отличными от OpenBao. В случае, если у сертифкатов непродолжительный срок действия или их обновление производится через OpenBao, следует выполнить настройку параметра SECRETS_OPENBAO_PKI_CERTS. Ключ может иметь парольную защиту. Для использования ключа в Termidesk VDI нужно преобразовать его к начальному значению: openssl rsa -in <путь_к_файлу_ключа.key> -out <преобразованный_ключ.key>. Для использования ключа нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key; • установить корневой сертификат ЦС, если ранее он не был установлен. Пример задания параметра: SECRETS_OPENBAO_CLIENT_KEY='/etc/opt/termidesk-vdi/openbao-client.key'

Параметр	Значение по умолчанию	Описание
SECRETS_OPENBAO_SERVER_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к промежуточному сертификату ЦС mTLS для начального защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы. Для работы защищенного соединения по протоколу mTLS требуется задать параметры SECRETS_OPENBAO_CLIENT_CERT, SECRETS_OPENBAO_CLIENT_KEY. Сертификат должен размещаться в файловой системе узла (внешнее хранилище не используется). Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem; • установить корневой сертификат ЦС, если ранее он не был установлен. Пример задания параметра: SECRETS_OPENBAO_SERVER_CERT='/etc/opt/termidesk-vdi/openbao-ca.pem'
SECRETS_OPENBAO_PKI_CERTS	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к клиентскому сертфикату и ключу, размещенному в OpenBao, для вторичной проверки подключения к OpenBao. В случае, если у сертифкатов непродолжительный срок действия или их обновление производится через OpenBao, следует использовать этот параметр. Пример задания параметра: SECRETS_OPENBAO_PKI_CERTS = 'hvac-pki://pki?common_name=www.my-website.com#example-dot-com/issuing_ca'
SECRETS_OPENBAO_TOKEN	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к файлу, содержащему одноразовый токен доступа к OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Пример задания параметра: SECRETS_OPENBAO_TOKEN='/etc/opt/termidesk-vdi/openbao.token'

Параметр	Значение по умолчанию	Описание
SECRETS_OPENBAO_DB_PATH	hvac-kv://secret#postgresql/	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь, настроенный на OpenBao и используемый для хранения данных подключения к СУБД. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Начальное значение задается на этапе установки. Данные могут быть расположены в специальном хранилище паролей, в этом случае указывается путь к ним: SECRETS_OPENBAO_DB_PATH='hvac-kv://secret#/postgresql/'
SECRETS_OPENBAO_ROLE_NAME	termidesk-role	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет роль (имя приложения), настроенную на OpenBao и имеющую доступ к логинам и паролям. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Начальное значение задается на этапе установки. Пример задания параметра: SECRETS_OPENBAO_ROLE_NAME='vdi-role'
SECRETS_OPENBAO_ROLE_ID	a877a491-71a4-bfe8-e24c-d5beff3dddd2	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет идентификатор роли, заданной в параметре SECRETS_OPENBAO_ROLE_NAME. Идентификатор должен быть получен на OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Пример задания параметра: SECRETS_OPENBAO_ROLE_ID='a877a491-71a4-bfe8-e24c-d5beff3dddd2'
SECRETS_OPENBAO_WATCHDOG_INTERVAL	10	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет интервал (в секундах) проверки актуальности одноразового токена (параметр SECRETS_OPENBAO_TOKEN). Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac
SECRETS_OPENBAO_TTL_DEADLINE	30	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет оставшееся время (в секундах) актуальности одноразового токена, по достижении которого он будет обновлен. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac

Параметр	Значение по умолчанию	Описание
SECRETS_OPENBAO_WRAP_TTL	10m	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет время актуальности (в минутах) одноразового токена. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac
SECRETS_OPENBAO_NAMESPACE	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет пространство имени, заданного на OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac
SECRETS_OPENBAO_RABBITMQ_PATH	hvac-kv://secret#rabbitmq/	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь, настроенный на OpenBao и используемый для хранения данных подключения к RabbitMQ. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Начальное значение задается на этапе установки. Данные могут быть расположены в специальном хранилище паролей, в этом случае указывается путь к ним: SECRETS_OPENBAO_RABBITMQ_PATH='hvac-kv://secret#/rabbitmq/'
SECRETS_OPENBAO_TERMIDESK_PATH	/termidesk	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь, настроенный на OpenBao для хранения паролей Termidesk VDI. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Начальное значение задается на этапе установки. Пример задания параметра: SECRETS_OPENBAO_TERMIDESK_PATH='hvac-kv://secret#/termidesk'
SECRETS_OPENBAO_CACHE_LIFETIME	5	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет время (в секундах) хранения пароля, полученного от OpenBao, во внутренней памяти. Позволяет сохранить полученный от OpenBao пароль на некоторое время в кеше для сокращения количества обращений к OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Начальное значение задается на этапе установки
Настройки взаимодействия с узлом «Ретранслятора»		

Параметр	Значение по умолчанию	Описание
FLUENTD_CACHE	15	Параметр может быть задан на узлах «Универсального диспетчера». Определяет время (в секундах) кеширования параметров подключения к узлу «Ретранслятора». По умолчанию после установки время кеширования составляет 15 секунд. В случае, если нужно изменить значение, следует раскомментировать параметр и задать ему новое значение
FLUENTD_TABLE	logs	Параметр может быть задан на узлах «Универсального диспетчера». Определяет таблицу хранения событий фермы. По умолчанию после установки «Универсальный диспетчер» обращается к таблице «logs» БД «Ретранслятора». В случае, если в БД «Ретранслятора» для хранения событий используется другая таблица, следует раскомментировать параметр и указать новое имя таблицы
FLUENTD_LOGGER_TIMEOUT	5	Параметр может быть задан на узлах «Универсального диспетчера». Определяет время (в секундах) ожидания подключения к узлу «Ретранслятора»
Настройки «Шлюза»		
WSPROXY_PUB_KEY_FILE	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет путь к открытому ключу id_rsa.pub. Используется для подписи токенов при взаимной аутентификации «Шлюза» и «Универсального диспетчера», «Агрегатора». По умолчанию создается при первой установке и хранится в каталоге /etc/opt/termidesk-vdi/wsproxy. Явно задавать путь следует только при использовани внешнего хранилища. Пример: WSPROXY_PUB_KEY_FILE='hvac-kv://secret#termidesk-admin/wsproxy/pub'
WSPROXY_PRIV_KEY_FILE	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет путь к закрытому ключу id_rsa. Используется для подписи токенов при взаимной аутентификации «Шлюза» и «Универсального диспетчера», «Агрегатора». По умолчанию создается при первой установке и хранится в каталоге /etc/opt/termidesk-vdi/wsproxy. Явно задавать путь следует только при использовани внешнего хранилища. Пример: WSPROXY_PRIV_KEY_FILE='hvac-kv://secret#termidesk-admin/wsproxy/priv'
Настройка защищенного взаимодействия сервера Termidesk VDI с другими компонентами по mTLS		

Параметр	Значение по умолчанию	Описание
MTLS_MODE	disabled	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет режим mTLS для взаимодействия между компонентами Termidesk VDI. В этом сценарии сервер Termidesk VDI выступает в роли клиента процесса взаимной аутентификации. Возможные значения: • disabled - результат проверки сертификата игнорируется. В этом режиме mTLS не используется; • permissive - нестрогий режим проверки сертификата. Проверка выполняется, но если сертификат не предоставлен или он недействительный, то в журнал записывается предупреждение. Запрос при этом выполняется; • strict - строгий режим проверки сертификата. Предоставление действительных сертификатов обязательно. Запрос отклоняется, когда сертификат не прошел проверку Если включен строгий режим проверки, то работа со всеми API (значение all_api параметра MTLS_CONNECTIONS) и «Агрегатором пользователя» (значение client_aggr_portal параметра MTLS_CONNECTIONS) будет запрещена.

Параметр	Значение по умолчанию	Описание
MTLS_CONNECTIONS	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет сценарий взаимодействия между компонентами Termidesk VDI по mTLS. Узлы должны быть настроены на использование mTLS: • должны быть загружены и использоваться валидные клиентские и серверные сертификаты; • должен быть активирован режим использования mTLS. Изменение параметра потребует перезапуска службы termidesk-vdi. Возможные значения: • va_agent - взаимодействие по mTLS осуществляется с «Агентом виртуального рабочего места»; • session_agent - взаимодействие по mTLS осуществляется с «Сессионным агентом»; • client_aggr_portal - взаимодействие по mTLS осуществляется со всеми видами порталов («Агрегатором пользователя», «Агрегатором администратора», «Порталом администратора», «Порталом пользователя»). Значение не должно использоваться, если включен строгий режим mTLS; • gateway - взаимодействие по mTLS осуществляется со шлюзом, обеспечивающим формирование и поддержание соединения; • all_api - взаимодействие по mTLS осуществляется для всех API-запросов «Универсального диспетчера». Значение не должно использоваться, если включен строгий режим mTLS; • health_check - взаимодействие по mTLS осуществляется для API-запроса /api/health/check «Универсального диспетчера»; • metrics - взаимодействие по mTLS осуществляется для API-запроса /api/health/metrics «Универсального диспетчера»
MTLS_CLIENT_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к клиентскому сертификату mTLS для защищенного подключения и взаимной аутентификации с другими компонентами (например, службами каталогов или платформами виртуализации). Для работы mTLS необходимо выбрать режим проверки и сценарии в параметрах MTLS_MODE и MTLS_CONNECTIONS. Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem

Параметр	Значение по умолчанию	Описание
MTLS_CLIENT_KEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к клиентскому ключу mTLS для защищенного подключения и взаимной аутентификации с другими компонентами (например, службами каталогов или платформами виртуализации). Для работы mTLS необходимо выбрать режим проверки и сценарии в параметрах MTLS_MODE и MTLS_CONNECTIONS. Для использования ключа нужно: * скопировать его в каталог /etc/opt/termidesk-vdi/; * назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key; * изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key
MTLS_CLIENT_CA	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к клиентскому корневому сертификату mTLS для защищенного подключения и взаимной аутентификации с другими компонентами (например, службами каталогов или платформами виртуализации). Для работы mTLS необходимо выбрать режим проверки и сценарии в параметрах MTLS_MODE и MTLS_CONNECTIONS. Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem
Настройка «Брокера сообщений TermideskMQ»		
TMQ_BASE_ADDRESS	0.0.0.0	IP-адрес прослушивания входящих подключений для «Брокера сообщений TermideskMQ»

Параметр	Значение по умолчанию	Описание

TMQ_BASE_PORT	5555	Номер базового порта «Брокера сообщений TermideskMQ».
		
		Если режим mTLS не используется, то:
		
		• действует правило выделения портов: <базовый_порт> + один последующий для IP-адреса, указанного в TMQ_BASE_ADDRESS;
		• базовый порт используется для приема сообщений, дополнительный порт - для отправки сообщений.
		
		Если режим mTLS используется, то:
		
		• в зависимости от базового порта будут определены внутренние TCP-порты для запуска «Брокера сообщений TermideskMQ» на localhost;
		• порты mTLS, использующиеся для IP-адреса, указанного в TMQ_BASE_ADDRESS:
		  - базовый порт (например, 5555);
		  - базовый порт +1 (например, 5556);
		• внутренние TCP-порты для запуска на localhost:
		  - базовый порт + 3 (например, 5558), используется для приема сообщений;
		  - базовый порт + 3 + 1 (например, 5559), используется для приема подключения и отправки сообщений

Настройка «Брокера сообщений TermideskMQ» для работы с mTLS		
TMQ_SERVER_CERT	Не задано	Определяет путь к серверному сертификату mTLS для «Брокера сообщений TermideskMQ». Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem
TMQ_SERVER_KEY	Не задано	Определяет путь к ключу для серверного сертификата mTLS для «Брокера сообщений TermideskMQ». Для использования ключа нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key

Параметр	Значение по умолчанию	Описание
TMQ_SERVER_CA	Не задано	Определяет путь к корневому сертификату mTLS для «Брокера сообщений TermideskMQ». Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem
Настройка высокодоступной конфигурации «Брокера сообщений TermideskMQ»		
TMQ_CLIENT_ID	default	Определяет идентификатор клиента «Брокере сообщений TermideskMQ». Для работы нескольких ферм Termidesk VDI (или ферм «Агрегатора») с одним кластером «Брокера сообщений TermideskMQ» нужно указать уникальный идентификатор для каждой фермы, в этом случае все клиенты в рамках нее полчат один идентификатор. Тип значения идентификатора - строка
TMQ_TIMEOUT_AWAIT_SENDING_MESSAGEL	10000	Определяет время ожидания ответа от узла кластера «Брокера сообщений TermideskMQ». При использования высокодоступной конфигурации требуется настройка «Брокера сообщений TermideskMQ» для работы с mTLS
TMQ_PUT_RETRY_COUNT	3	Определяет количество попыток выполнения запроса или отправки сообщения к узлу кластера «Брокера сообщений TermideskMQ». При использования высокодоступной конфигурации требуется настройка «Брокера сообщений TermideskMQ» для работы с mTLS
Настройки использования веб-интерфейса		
TERMIDESK_OLD_INTERFACE_ENABLED	True	Параметр может быть задан на узлах «Универсального диспетчера» («Портал администратора», «Портал пользователя»). Определяет использование старого веб-интерфейса. Возможные значения: • True - доступны старый и новый веб-интерфейсы; • False - доступен только новый веб-интерфейс. При этом будет окно авторизации для старого веб-интерфейса будет доступно, но не будет работать
Настройка взаимодействия со службой каталогов MS AD		

Параметр	Значение по умолчанию	Описание
AUTH_MSAD_META_USE_UPN	True	Параметр может быть задан на узлах «Универсального диспетчера». Определяет формат передачи имени метапользователя в службу каталогов MS AD. Возможные значения: • True - для имени метапользователя используется формат UPN; • False - для имени метапользователя не используется формат UPN
Настройка подключения пользователя к BPM		
CONNECTION_TICKET_VALIDITY	60	Параметр может быть задан на узлах «Универсального диспетчера». Определяет время валидности (в секундах) тикета для подключения пользователя к BPM. Значение следует менять только при возникновении ошибок подключения, связанных с долгой обработкой подключения

Пример файла конфигурации сервера OpenBao, который активирует строгую проверку клиентского SSL-сертификата:

```
listener "tcp" {
tls_min_version = "tls12"
tls_disable = "false"
address = "0.0.0.0:8200"
tls_cert_file = "/etc/bao/openbao.stand8.local.crt"
tls_key_file = "/etc/bao/openbao.stand8.local.key"
# Если включён, то будет проверять сертификат клиента на корректность
tls_require_and_verify_client_cert = "true"
# Если выключён, то будет требовать наличие сертификата клиента
tls_disable_client_certs = "false"
}
```

Файл /etc/default/termidesk-vdi.local

Для настройки путей хранения файлов конфигурации и некоторых других параметров, влияющих на установщик Termidesk и запуск службы termidesk-vdi, используется файл /etc/default/termidesk-vdi.local.

Перечень параметров, задающихся через файл, приведен в таблице (см. таблицу Параметры файла /etc/default/termidesk-vdi.local).

Если во время обновления Termidesk VDI было выбрано новое место хранения конфигурации, то:

- создастся (если не существовал) новый каталог для хранения конфигурации;
- в новый каталог будут скопированы (если не существовали) файлы из старого каталога (termidesk.conf, termidesk.cookie, CRYPTO_RSA_KEY,

/wsproxy/id_rsa, /wsproxy/id_rsa.pub).

Рекомендуется выполнять изменение путей к каталогам через утилиту termidesk-config.

Если изменение было сделано вручную, то потребуется:

- при изменении места хранения шаблонов выполнить:

```
sudo /opt/termidesk/sbin/termidesk-config update_logger_config
```

- при любых изменениях перезапустить службы Termidesk VDI (в зависимости от установленной роли узла список служб может отличаться).

Таблица 138. Параметры файла /etc/default/termidesk-vdi.local

Параметр	Значение по умолчанию	Описание
ETC	/etc/opt/termidesk-vdi	Параметр может быть задан на узлах «Универсального диспетчера»,«Менеджера рабочих мест», «Агрегатора». Определяет путь к каталогу с конфигурационными файлами (termidesk.conf, termidesk.cookie, CRYPTO_RSA_KEY, /wsproxy/id_rsa, /wsproxy/id_rsa.pub). Каталог должен обладать следующими свойствами: • права доступа: rwxr-x--- (в восьмеричной записи - 750); • владелец и группа: root:termidesk. Пример: ETC='/etc/opt/termidesk-vdi'
TEMPLATES_DIR	/etc/opt/termidesk-vdi/templates	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к каталогу с шаблонами для настройки регистрации событий и журналирования. Каталог должен обладать следующими свойствами: • права доступа: rwxr-x--- (в восьмеричной записи - 750); • владелец и группа: root:termidesk. Пример: TEMPLATES_DIR='/etc/opt/termidesk-vdi/templates'

Параметр	Значение по умолчанию	Описание
NON_INTERACTIVE_INSTALLATION	Не задано	Параметр определяет режим работы установщика при его запуске. Возможные значения: • yes - при запуске установщика (пакета termidesk-vdi) диалоги настройки параметров не отображаются. Значение рекомендуется использовать, если требуется выполнить установку без отображения псевдографического интерфейса установщика; • любое другое значение или пустое - при запуске установщика диалоги настройки параметров отображаются
GUNICORN_VDI_WORKERS	Не задано	Параметр определяет количество обработчиков запросов, используемых службой termidesk-vdi. По умолчанию параметр отсутствует и добавляется вручную. Значение параметра выбирается с учетом производительности сервера Termidesk VDI. Если переменная отсутствует или имеет значение меньше 1, то количество обработчиков автоматически рассчитывается по формуле: количество ядер CPU, умноженное на 3.

Общие системные параметры Termidesk VDI

Системные параметры позволяют задать основные значения, необходимые для успешного функционирования Termidesk VDI.

Для конфигурации общих системных параметров следует перейти «Системные параметры - Системные настройки», выбрать раздел «Общие».

Доступные для редактирования параметры перечислены в столбце «Параметр» следующей таблицы (см. таблицу Общие системные параметры Termidesk VDI).

Изменение системных параметров вступают в силу только после перезагрузки Termidesk VDI.

Экранная кнопка **[Сохранить]** сохраняет общие системные параметры.

Таблица 139. Общие системные параметры Termidesk VDI

Параметр	Описание
«Название фермы»	Наименование фермы, отображаемое в «Портале пользователя», «Портале администратора» и компоненте «Клиент»

Параметр	Описание
«Генератор имен»	Варианты использования имен при развертывании ВРМ. Возможные значения: • «С повторным использованием имени» (по умолчанию); • «Без переиспользования имен»

Параметр	Описание
«Действие с учетной записью рабочего места»	Выбор действия, которое будет произведено над учетной записью в службе каталогов при удалении ВРМ из фонда. DNS-сервер, указанный в настройках узла «Универсального диспетчера», должен иметь возможность разрешать имена узлов в зонах службы каталогов (MS AD, FreeIPA, ALD Pro). Для корректного сброса пароля учетной записи при удалении РМ из фонда на узле «Универсального диспетчера» требуется наличие сертификата, выпущенного центром сертификации для работы по протоколу LDAPS. Также на узле службы каталогов MS AD должны быть созданы соответствующие SRV-записи. Возможные значения: • «Удалить» (по умолчанию) - при удалении РМ из фонда учетная запись будет удалена из службы каталогов. Применимость: MS AD, FreeIPA, ALD Pro; • «Сбросить» - при удалении РМ из фонда у учетной записи будет сброшен пароль. Применимость: MS AD; • «Выключить» - при удалении РМ из фонда учетная запись будет отключена. Применимость: MS AD; • «Хранить» - при удалении РМ из фонда учетная запись будет сохранена в службе каталогов. Применимость: MS AD, FreeIPA, ALD Pro. Следует учесть, что при вводе гостевой ОС в MS AD: • если учетная запись РМ находится не в стандартном каталоге «Computers», то параметр «OU» должен принимать значения вида: «OU=Computers,DC=domain,DC=local», т.е. не должен использоваться Common Name (CN); • если учетная запись РМ находится в стандартном каталоге «Computers», то параметр «OU» должен принимать значения вида: «CN=Computers,DC=domain,DC=local», т.е. должен использоваться Common Name (CN)
«Автозапуск рабочего места»	Автоматическое подключение пользователя к фонду РМ через компонент «Клиент». Значение по умолчанию: «Нет»

Параметр	Описание
«Подключаться к ВРМ по»	Параметр определяет, какое значение в параметрах подключения к ВРМ «Универсальный диспетчер» должен передать компоненту «Клиент». Возможные значения: • «IP адреса» - в параметрах подключения будет передаваться IP-адрес ВРМ; • «Полному доменному имени (FQDN)» - в параметрах подключения будет передаваться FQDN ВРМ. При Kerberos-аутентификации это значение использовать обязательно. Действие параметра не распространяется на протокол подключения к терминальному серверу - при таком подключении всегда передается IP-адрес. При использовании Метапоставщика значение параметра будет учитываться: • при использовании значения «Полному доменному имени (FQDN)» Метапоставщик будет передавать FQDN ВМ из сервисного фонда; • при использовании значения «Сетевому адресу (IP)», Метапоставщик будет передавать IP-адрес ВМ из сервисного фонда
«Не учитывать максимальные ограничения»	Не учитывать ограничения, заданные в полях «Подготавливать ВМ одновременно» и «Удалять ВМ одновременно» поставщика ресурсов при формировании фондов. Если параметр активен, в фонде одновременно может создаваться и удаляться до 1000 ВМ. Значение по умолчанию: «Нет»
«Время хранения информационных объектов, с»	Время хранения (в секундах) информации о фондах в статусе «Удален», «Отменен», «Ошибка». Значение по умолчанию: «14401» Очистка фондов РМ, находящихся в статусах «Удалены», «Отменены», «Ошибка» происходит через время, указано в параметре «Время хранения информационных объектов». Периодичность удаления таких фондов составляет 30 секунд. Периодичность очистки фондов, находящихся в процессе удаления (ожидающих удаления и удаляемых), составляет 31 секунду

Параметр	Описание
«Время блокировки входа, с»	Время (в секундах) после истечения которого будет возможен повторный вход субъекта «Администратор», «Персонал» или «Пользователь» в случае превышения субъектом лимита неудачных попыток входа. По истечении этого времени пользователь продолжит визуально быть заблокированным (статус «Временно заблокирован») в списке пользователей в домене аутентификации. Статус сменится на «Активный» только после авторизации пользователя с правильным паролем или после смены статуса администратором. Значение по умолчанию: «300»
«URL входа»	URL-адрес начальной страницы графического интерфейса управления. Значение параметра менять не следует. Значение по умолчанию: «/login»
«Адрес сервера удаленного помощника»	URL-адрес узла с установленной серверной частью «Удаленного помощника». Для подключения можно использовать только протокол HTTPS (серверная часть «Удаленного помощника» должна быть настроена на работу по HTTPS). Пример: «https://192.168.0.2». По умолчанию значение не задано
«Максимальное время инициализации рабочего места, с»	Максимальное время (в секундах) ожидания готовности ВРМ, после истечения которого оно будет считаться зависшим. Если ВМ находятся в состоянии «Подготовка» или не назначена пользователю по истечении времени «Максимальное время инициализации рабочего места», то она будет очищена фоновой задачей, выполняемой каждые 60 секунд. Значение по умолчанию: «3601»
«Максимум записей в журнале для объектов»	Максимальное количество системных событий, добавляемых в журнал объекта. Значение по умолчанию: «100»
«Количество ошибок для ограничения фонда»	Пороговое значение количества ошибок, после которого фонд будет переведен в статус «Ограниченный». Значение по умолчанию: «3»
«Интервал отслеживания ошибок в фонде, с»	Периодичность отслеживания появления ошибок (в секундах), связанных с функционированием фонда. Значение по умолчанию: «600»

Параметр	Описание
«Срок действия устаревшей публикации, ч»	Время (в часах), по истечении которого ВМ будет удалена, если публикация фонда объявлена устаревшей. Поведение параметра переопределяется на уровне фонда РМ политикой «Удаление устаревшей публикации»: совместимость обеспечивается только при ее значении «Удалять по истечении срока действия», что соответствует значению «-1» этого параметра. При обновлении параметра его значение применяется к новым публикациям. Для публикаций, созданных до изменения параметра, будет действовать предыдущее значение параметра. Если значение параметра будет равным «-1», то при перепубликации фонда РМ произойдет следующее: • предыдущая публикация будет переведена в статус «Публикация частично удалена», если есть назначенная и используемая ВМ; • используемая ВМ автоматически не удалится, но при этом будет создана новая публикация. Если значение параметра будет равным «0», то при перепубликации фонда назначенная ВМ будет немедленно заменена на новую публикацию. Если значение параметра будет равным «1», то при перепубликации фонда назначенная ВМ будет доступна 1 час, после чего удалится. Значение по умолчанию: «24»
«Срок хранения статистики, сут»	Время (в сутках) хранения файлов журналов, по истечению которого журналы будут перезаписаны. Значение по умолчанию: «365»
«Количество удаляемых рабочих мест за один проход»	Максимальное количество ВРМ, помеченных к удалению, которые будут проверены и удалены при каждой итерации запуска фоновой задачи очистки. Значение по умолчанию: «3»

Параметр	Описание
«Отправлять уведомление при превышении лимита интервала опроса поставщика»	Управление возможностью отправки уведомлений администратору, если превышен интервал опроса, заданный в настройках поставщика ресурсов. Параметр также влияет на отправку почтовых уведомлений. Возможные значения: • «Да» - администратору будет отправлено почтовое уведомление и уведомление в веб-интерфейсе, если заданный интервал опроса превышен; • «Нет» (по умолчанию) - администратору не будут отправлены уведомления при превышении интервала опроса
«Заголовок access token»	Задает заголовок JWT-токена, предназначенный для настройки взаимодействия между «Агрегатором» и «Универсальным диспетчером». Значение по умолчанию: «Access»
«Дополнительная проверка заголовка JWT»	Управление дополнительной проверкой заголовка JWT-токена. Возможные значения: • «Да» - заголовок JWT-токена, полученный от «Агрегатора», будет проверяться; • «Нет» (по умолчанию) - заголовок JWT-токена, полученный от «Агрегатора», не будет проверяться
«Таймаут кеша хранения групп домена, с»	Определяет время кеширования (в секундах) информации о группах пользователя, полученной от службы каталогов, во внутренней памяти. Позволяет сохранить полученную от службы каталогов информацию на некоторое время в кеше для сокращения количества обращений к ней. Значение по умолчанию: «30»
«Список шаблонов подключаемых профилей в ПК СВ Брест»	Управление списком шаблонов Перемещаемых Профилей в ПК СВ Брест. В качестве значения используется идентификатор диска. Подробные сведения по настройке Перемещаемых Профилей приведены в подразделе **Настройка Перемещаемого Профиля для ПК СВ Брест**
«Время жизни тикета подключения к РМ, с»	Определяет время жизни (в секундах) токена, используемого для взаимодействия «Универсального диспетчера» с компонентом «Клиент». Значение по умолчанию: «60»

Параметр	Описание
«Таймаут обращения к серверу Удаленного помощника, с»	Определяет время ожидания (в секундах) ответа от серверной части компонента «Удаленный помощник». Если появляются ошибки недоступности серверной части компонента «Удаленный помощник», то рекомендуется увеличить значение параметра. Значение по умолчанию: «5»
«Таймаут обращения к агенту РМ, с»	Определяет время ожидания (в секундах) ответа от «Агента виртуального рабочего места». Если появляются ошибки недоступности «Агента виртуального рабочего места» и пользователь не может подключиться к РМ, то рекомендуется увеличить значение параметра. Значение по умолчанию: «15»
«Количество попыток проверки состояния РМ при выдаче»	Максимальное количество проверок готовности РМ к подключению. Количество попыток учитывается для каждого подключения к РМ отдельно, независимо от результатов предыдущих подключений. При достижении заданного количества проверок готовности РМ ему будет присвоен статус «Недействительный». При использовании Метапоставщика этот параметр определяет максимальное количество итераций при попытке выделить ВМ терминального сервера из пула балансировки. Механизм предназначен для автоматического «перебора» доступных ВМ в случае, если первый выбранный узел оказался недоступен. Если количество попыток исчерпано, то подключение не произойдет. Если узел недоступен, то он выводится из пула балансировки на время, указанное в параметре «Длительность исключения из балансировки недоступных РМ сервисного фонда, с». Значение по умолчанию: «5»
«Интервал проверки статуса 'Недействительный', с»	Периодичность (в секундах) отслеживания состояния РМ в статусе «Недействительный». Значение по умолчанию: «60»
«Длительность исключения из балансировки недоступных РМ сервисного фонда, с»	Время (в секундах), в течение которого недоступное РМ сервисного фонда временно выводится из распределения сессий. По истечении времени РМ с «Сессионным агентом» автоматически возвращается в пул балансировки для подключения пользователей. Параметр действует только при использовании Метапоставщика. Значение по умолчанию: «10»

Параметр	Описание
«Таймаут проверки компонентов инфраструктуры, с»	Определяет время ожидания (в секундах) ответа на запрос проверки состояния всех узлов инфраструктуры Termidesk VDI. Если появляются ошибки недоступности узлов инфраструктуры Termidesk VDI, то рекомендуется увеличить значение параметра. Значение по умолчанию: «10»
«Таймаут обработки запроса healthcheck, с»	Определяет время ожидания (в секундах) ответа на запрос проверки состояния отдельного узла инфраструктуры Termidesk VDI. Для корректной обработки запросов к отдельным узлам значение параметра должно быть больше значения, заданного в параметре «Таймаут проверки компонентов инфраструктуры, с». Если появляются ошибки проверки доступности узла, то рекомендуется увеличить значение параметра. Значение по умолчанию: «10»
«Время хранения приватного ключа Шлюза в кеше, с»	Определяет время кеширования (в секундах) токена, полученного от шлюза, во внутренней памяти. Позволяет сохранить полученный от шлюза токен на некоторое время в кеше для сокращения количества обращений к нему. Значение по умолчанию: «60»
«Время кеширования JWT сертификатов агрегатора, с»	Определяет время кеширования (в секундах) сертификатов для получения значения JWT-токена во внутренней памяти. Позволяет сохранить сертификат на некоторое время в кеше для сокращения количества обращений к источнику хранения сертификатов. Значение по умолчанию: «30»
«Таймаут аутентификации RADIUS, с»	Определяет время ожидания (в секундах) завершения всех этапов аутентификации пользователя на сервере RADIUS. Если появляются ошибки аутентификации пользователя на сервере RADIUS (например, после ввода OTP), то рекомендуется увеличить значение параметра. Значение по умолчанию: «60»

Параметр	Описание
«Таймаут SSO, с»	Определяет время ожидания (в секундах) для запуска ПО Termidesk Viewer при использовании технологии единого входа (SSO). Параметр передается компоненту «Клиент». Не рекомендуется назначать параметру предельно низкие значения. Минимальное значение, не вызывающее проблем с подключением в большинстве случаев: «30». Значение по умолчанию: «60»

Параметры безопасности Termidesk VDI

Для конфигурации системных параметров безопасности следует перейти «Системные параметры - Системные настройки», выбрать раздел «Безопасность».

Доступные для редактирования администратору Termidesk VDI параметры перечислены в столбце «Параметр» следующей таблицы (см. таблицу Параметры безопасности Termidesk VDI).

Таблица 140. Параметры безопасности Termidesk VDI

Параметр	Описание
«Мастер-ключ»	Идентификатор для регистрации РМ в Termidesk VDI. Значение идентификатора должно удовлетворять условиям: • длина должна составлять от 1 до 32 символов; • должны использоваться символы в шестнадцатеричной системе (0-9, a-f)
«Длительность сессии администратора, с»	Временной интервал сессии (в секундах), инициированной на «Портале администратора»
«Доступ к веб-части системным пользователем»	Возможность системному администратору подключаться к «Порталу администратора»
«Использовать анонсируемый IP клиента»	Использовать IP-адрес «Клиента», передаваемый в процессе входа в Termidesk VDI. Параметр необходимо включить, если узел «Универсального диспетчера» используется в ферме Termidesk VDI, подключаемой к порталу «Агрегатор». В противном случае при подключении пользователей к ресурсам ферм Termidesk VDI в журнале «Универсального диспетчера» будет отображен IP-адрес портала «Агрегатор», а не IP-адреса подключившихся пользователей
«GID системной группы администратора»	Идентификатор группы, в которую входит учетная запись администратора

Параметр	Описание
«Длительность сессии пользователя, с»	Временной интервал (в секундах) сессии пользователя. Параметр влияет на длительность сессии пользователя в «Портале пользователя». Начиная с Termidesk VDI версии 5.0 параметр также определяет общее время подключения пользователя к «Универсальному диспетчеру» Termidesk VDI. Вне зависимости от того, активен пользователь или нет, каждую секунду происходит уменьшение значения параметра на 1, при достижении значения 0 подключение пользователя завершится, при этом в системном трее на пользовательской рабочей станции отобразится уведомление от приложения «Клиент»: «Ваш сеанс завершился». В журнале «Клиента» отражаются события как получения параметра («userSessionLength»), так и завершения сессии по таймауту
«Максимум попыток входа Администраторов»	Пороговое положительное значение числа неудачных попыток входа администратора. Параметр может быть изменен только ролью «Администратор»: если права на изменение системных параметров будут выданы другой роли, то пользователь с этой ролью не сможет изменить параметр, т.к. он не будет отображен. Значение «0» эквивалентно «без ограничений»
«Максимум попыток входа Персонала»	Пороговое положительное значение числа неудачных попыток входа субъектов, не относящихся к администратору. Значение «0» эквивалентно «без ограничений»
«Максимум попыток входа Пользователей»	Пороговое положительное значение числа неудачных попыток входа пользователей. Значение «0» эквивалентно «без ограничений»
«Список доверенных прокси»	Настройка списка доверенных прокси-серверов в сети для определения доверенного клиентского IP-адреса из HTTP-заголовка X-Forwarded-For. Параметр позволяет: • исключить возможность подмены клиентского IP-адреса; • отображать в «Портале администратора« IP-адрес пользователя вместо IP-адреса балансировщика (если он указан в этом параметре). Поиск в списке клиентских IP-адресов производится с самого правого, пропуская все адреса из списка доверенных прокси-серверов. Первый несовпадающий IP-адрес будет целевым. Значение задается в виде списка IP-адресов, указанных через запятую. По умолчанию параметр пуст

Управление параметрами компонента «Клиент»

Управление авторизацией пользователя в компоненте «Клиент»

В Termidesk VDI предусмотрена возможность управления авторизацией пользователя в компоненте «Клиент».

Для изменения параметров авторизации следует перейти «Системные параметры - Системные настройки», выбрать раздел «Аутентификация» и настроить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Доступные параметры при настройке сохранения паролей в компоненте «Клиент»).

Для сохранения параметров авторизации нажать экранную кнопку **[Сохранить]**.

Таблица 141. Доступные параметры при настройке сохранения паролей в компоненте «Клиент»

Параметр	Описание
«Разрешить сохранение имени пользователя в клиенте»	Управление параметром сохранения имени пользователя в компоненте «Клиент» при подключении к «Универсальному диспетчеру». По умолчанию параметр активирован
«Разрешить сохранение пароля в клиенте»	Управление параметром сохранения пароля в компоненте «Клиент» при подключении к «Универсальному диспетчеру». Если параметр: • активирован, то пароль, ранее введенный пользователем при подключении к «Универсальному диспетчеру», будет сохранен в конфигурационном файле компонента «Клиент»; • не активирован, то пароль, ранее введенный пользователем при подключении к «Универсальному диспетчеру», не будет храниться в конфигурационном файле компонента «Клиент». Сохранение пароля невозможно без сохранения имени пользователя: если параметр «Разрешить сохранение имени пользователя в клиенте» не активирован, то параметр «Разрешить сохранение пароля в клиенте» также не активируется после нажатия экранной кнопки **[Сохранить]**. Влияние параметров сохранения пароля в различных сценариях приведено в таблице ниже (см. таблицу Влияние параметров, управляющих сохранением пароля или PIN-кода). По умолчанию параметр активирован

Параметр	Описание
«Использовать введённый пароль для подключения к РМ»	Сохранение пароля, введенного пользователем при подключении к «Универсальному диспетчеру», в оперативной памяти для дальнейшего подключения к РМ. Если параметр: • активирован, то пароль, ранее введенный пользователем при подключении к «Универсальному диспетчеру», будет использован для дальнейшего подключения к РМ; • не активирован, то пароль, ранее введенный пользователем при подключении к «Универсальному диспетчеру», не будет храниться и при подключении к РМ потребуется его ввести. Влияние параметров сохранения пароля в различных сценариях приведено в таблице ниже (см. таблицу Влияние параметров, управляющих сохранением пароля или PIN-кода). По умолчанию параметр активирован
«Использовать введённый PIN для подключения к РМ»	Сохранение PIN-кода смарт-карты, введенного пользователем при подключении к «Универсальному диспетчеру», в оперативной памяти для дальнейшего подключения к РМ. Если параметр: • активирован, то PIN-код, ранее введенный пользователем при подключении к «Универсальному диспетчеру», будет использован для дальнейшего подключения к РМ; • не активирован, то PIN-код, ранее введенный пользователем при подключении к «Универсальному диспетчеру», не будет храниться и при подключении к РМ потребуется его ввести. Влияние параметров сохранения PIN-кода в различных сценариях приведено в таблице ниже (см. таблицу Влияние параметров, управляющих сохранением пароля или PIN-кода). По умолчанию параметр активирован
«Доп. информация при ошибке входа»	Информационное сообщение, отображаемое при ошибке входа

В таблице приняты обозначения:

- параметр 1 - «Использовать введённый пароль для подключения к РМ»;
- параметр 2 - «Использовать введённый PIN для подключения к РМ»;
- параметр 3 - «Разрешить сохранение пароля в клиенте»;
- политика SSO - политика «Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)».

Таблица 142. Влияние параметров, управляющих сохранением пароля или PIN-кода

Параметр 1	Параметр 2	Параметр 3	Политика SSO	Результат подключения к РМ
Активирован	Активирован	Активирован	«Включен»	Выполняется SSO. Используется пароль, введенный пользователем при подключении
Активирован	Активирован	Активирован	«Выключен»	По требованию политики запрашивается пароль
Активирован	Активирован	Не активирован	«Включен»	Выполняется SSO. Используется пароль, введенный пользователем при подключении
Активирован	Активирован	Не активирован	«Выключен»	По требованию политики запрашивается пароль
Не активирован	Не активирован	Активирован	«Включен»	В отдельном окне запрашивается пароль, на этапе входа в ОС выполняется SSO
Не активирован	Не активирован	Активирован	«Выключен»	В отдельном окне запрашивается пароль, на этапе входа в ОС по требованию политики снова запрашивается пароль
Не активирован	Не активирован	Не активирован	«Включен»	В отдельном окне запрашивается пароль, на этапе входа в ОС выполняется SSO
Не активирован	Не активирован	Не активирован	«Выключен»	По требованию политики запрашивается пароль на этапе входа в ОС

Управление другими настройками компонента «Клиент»

В Termidesk VDI предусмотрена возможность управлять некоторыми настройками компонента «Клиент»:

- переподключением пользователя к сеансам (функционал перемещения сеансов);
- обновлением списка ресурсов (РМ, опубликованных приложений) пользователя;
- выбором программы доставки при подключении по RDP.

Для изменения настроек следует перейти «Системные параметры - Системные настройки», выбрать раздел «Клиент». Доступные для изменения параметры перечислены в столбце «Параметр» следующей таблицы (см. таблицу Доступные параметры для управления настройками компонента «Клиент»).

Для сохранения параметров после изменения нажать экранную кнопку **[Сохранить]**.

Отключенный сеанс - это сеанс работающего РМ без активного подключения со стороны программы доставки (например, ПО Termidesk Viewer). Активный сеанс, соответственно, предполагает активное подключение со стороны программы доставки.

Изменения системных параметров вступают в силу только после перезагрузки Termidesk VDI.

Таблица 143. Доступные параметры для управления настройками компонента «Клиент»

Параметр	Описание
«Скрывать недоступные ресурсы»	Управление отображением недоступных ресурсов пользователю. Недоступность ресурса определяется его статусов, при этом пользователю отображается в интерфейсе причина недоступности. Параметр действует как при подключении пользователя непосредственно через компонент «Клиент», так и при подключении через веб-браузер. Возможные значения: • «Да» (по умолчанию) - недоступные ресурсы будут скрыты от пользователя; • «Нет» - недоступные ресурсы будут отображены, но пользователь не сможет к ним подключиться
«Активировать управление перемещением сеансов»	Форсировать управление режимом повторного подключения пользователя. При активации параметра пользователь не сможет самостоятельно изменить настройку повторного подключения в интерфейсе «Клиента». Возможные значения: • «Да» (по умолчанию) - переподключение пользователя будет форсировано со стороны «Универсального диспетчера»; • «Нет» - переподключение пользователя будет управляться в интерфейсе «Клиента». При выборе этого значения в параметре «Использовать перемещение сеансов» будет всегда использоваться «Не назначено»
«Разрешать изменение адреса подключения в клиенте»	Управление возможностью изменения адреса подключения к «Универсальному диспетчеру» в интерфейсе «Клиента». Возможные значения: • «Да» (по умолчанию) - пользователь может изменять адрес подключения к «Универсальному диспетчеру»; • «Нет» - пользователь не может изменять адрес подключения к «Универсальному диспетчеру»

Параметр	Описание
«Использовать перемещение сеансов»	Использование возможно при активации параметра «Активировать управление перемещением сеансов». Управление повторным подключением пользователя к отключенным и активным сеансам. Функционал позволяет восстанавливать подключение после разрыва соединения или смены устройства (пользовательской рабочей станции). Таким образом пользователь сможет получить тот же сеанс, с которым работал ранее, не теряя прогресс работы. Возможные значения: • «Не назначено» - выбор режима будет задан пользователем в интерфейсе «Клиента»; • «Запрещено» - повторное переподключение не используется; • «Повторно подключаться к активным и отключенным сеансам» (по умолчанию). В этом случае при переподключении сначала будет произведена процедура отключения активного сеанса пользователя, после которой он будет повторно подключен к отключенному сеансу; • «Повторно подключаться только к отключенным сеансам». В этом случае переподключение пользователя будет происходить только к отключенным сеансам
«Повторно подключаться к сеансам при аутентификации»	Использование возможно при активации параметра «Активировать управление перемещением сеансов». Параметр определяет режим повторного подключения к ресурсам при активации параметра «Активировать управление перемещением сеансов». Возможные значения: • «Да» (по умолчанию) - переподключение будет происходить при аутентификации пользователя через «Клиент»; • «Нет» - переподключение не будет происходить при аутентификации пользователя

Параметр	Описание
«Повторно подключаться к сеансам при обновлении списка приложений»	Использование возможно при активации параметра «Активировать управление перемещением сеансов». Параметр определяет режим повторного подключения к ресурсам при активации параметра «Активировать управление перемещением сеансов». Возможные значения: • «Да» - переподключение будет происходить при обновлении списка ресурсов; • «Нет» (по умолчанию) - переподключение не будет происходить при обновлении списка ресурсов
«Периодичность фонового обновления списка ресурсов, с»	Параметр определяет периодичность (в секундах), с которой будет происходить обновление списка ресурсов в интерфейсе «Клиента». Возможные значения: от 60 до 28800. Поддерживается задание специального значения «-1» - периодичность будет задана пользователем в интерфейсе «Клиента». Значение по умолчанию: «-1»
«Обновлять список ресурсов при каждом запуске ресурса»	Управление режимом обновления списка ресурсов. Возможные значения: • «Не задано» (по умолчанию) - выбор режима будет задан пользователем в интерфейсе «Клиента»; • «Включено» - обновление списка ресурсов будет происходить при запуске какого-либо ресурса пользователем; • «Выключено» - обновление списка ресурсов не будет происходить при запуске какого-либо ресурса пользователем
«Соединение по RDP через Termidesk Viewer»	Управление режимом использования ПО Termidesk Viewer при подключении к РМ по протоколу RDP. Возможные значения: • «Не задано» - выбор режима будет задан пользователем в интерфейсе «Клиента». При подключении пользователя из веб-браузера используется встроенный веб-клиент Termidesk Web Viewer, использование сторонних программ настраивается через конфигурационный файл «Клиента» (`Termidesk Client.ini`); • «Включено» (по умолчанию) - при подключении к РМ по протоколу RDP будет использоваться ПО Termidesk Viewer; • «Выключено» - при подключении к РМ по протоколу RDP будут использоваться системные программы доставки РМ (`mstsc.exe`, `xfreerdp`)

Параметр	Описание
«Переподключаться при обрыве связи»	Управление режимом восстановления подключения. Возможные значения: • «Не переподключаться» (по умолчанию) - попытки восстановления связи выполняться не будут. При потере соединения подключение к РМ останавливается и не возобновляется; • «5» - при потере соединения выполняются 5 попыток для восстановления подключения; • «10» - при потере соединения выполняются 10 попыток для восстановления подключения; • «30» - при потере соединения выполняются 30 попыток для восстановления подключения; • «Не задано» - выбор режима будет задан пользователем в интерфейсе «Клиента»
«Интервал запросов состояния РМ клиентом, с»	Периодичность (в секундах), с которой будет запрашиваться проверка состояния РМ компонентом «Клиент». Значение по умолчанию: «3»

Настройка отправки метрик для «Сессионного агента»

Метрики узла «Сессионного агента» используются в механизмах балансировки терминальных серверов Метапоставщика, а также могут направляться в подключаемые внешние системы мониторинга.

Для настройки отправки метрик узла «Сессионного агента» следует перейти «Системные параметры - Системные настройки», выбрать раздел «Метрики». Доступные параметры перечислены в столбце «Параметр» следующей таблицы (см. таблицу Параметры отправки метрик узла «Сессионного агента»).

Конфигурацию параметров можно изменить также через утилиту `termidesk-vdi-manage`: функцию `tdsk_config` и секцию `Metrics`.

Таблица 144. Параметры отправки метрик узла «Сессионного агента»

Параметр	Описание
«Пороговое значение»	Предел индекса нагрузки, при достижении которого необходимо оповестить администратора. Для отправки уведомлений должны быть включены соответствующие параметры (см. подраздел **Настройка отправки уведомлений о системных событиях**). Уведомление будет отправлено, если указанный предел индекса нагрузки достигнут однократно, но длится в течение времени, указанного в параметре «Периодичность отправки среднего значения». Диапазон значений: «1-10000». Значение по умолчанию: «5000»

Параметр	Описание
«Периодичность проверки, с»	Периодичность (в секундах), с которой «Сессионный агент» опрашивает ОС и собирает метрики узла. Изменение параметра вступит в силу только после перезагрузки Termidesk VDI или перезапуска службы `termidesk-vdi`. Следует дождаться отправки обновленного значения на «Сессионный агент» (ориентировочно спустя период, заданный в параметре «Периодичность отправки среднего значения»). Когда «Сессионный агент» получит обновленное значение, нужно перезапустить его службу после появления следующего сообщения в журнале «Сессионного агента»: «Получены новые настройки. Для применения изменений потребуется перезагрузка приложения». Диапазон значений: «1-60». Значение по умолчанию: «5»
«Периодичность отправки среднего значения, с»	Периодичность (в секундах), с которой «Сессионный агент» отправляет средние значения метрик «Универсальному диспетчеру». Изменение параметра вступит в силу только после перезагрузки Termidesk VDI или перезапуска службы `termidesk-vdi`. Следует дождаться отправки обновленного значения на «Сессионный агент» (ориентировочно спустя период, заданный в параметре «Периодичность отправки среднего значения»). Когда «Сессионный агент» получит обновленное значение, нужно перезапустить его службу после появления следующего сообщения в журнале «Сессионного агента»: «Получены новые настройки. Для применения изменений потребуется перезагрузка приложения». Диапазон значений: 1-60. Значение по умолчанию: «30»

Параметр	Описание
«Размер кеша, записей»	Размер кеша (записей) на «Сессионном агенте» для хранения метрик. На основании этого параметра происходит подсчет средних значений для отправки. Изменение параметра вступит в силу только после перезагрузки Termidesk или перезапуска службы `termidesk-vdi`. Следует дождаться отправки обновленного значения на «Сессионный агент» (ориентировочно спустя период, заданный в параметре «Периодичность отправки среднего значения»). Когда «Сессионный агент» получит обновленное значение, нужно перезапустить его службу после появления следующего сообщения в журнале «Сессионного агента»: «Получены новые настройки. Для применения изменений потребуется перезагрузка приложения». Диапазон значений: «2-10». Значение по умолчанию: «10»

Брендирование Termidesk VDI

Брендирование позволяет настроить внешний вид графического интерфейса Termidesk VDI в соответствии с фирменным стилем организации.

Функционал брендирования доступен только для лицензии с типом «Расширенный».

В Termidesk VDI версии 7.0 функционал брендирования поддерживается в экспериментальном режиме.

Поддерживается:

- изменение логотипов;
- управление цветовой схемой графического интерфейса для светлой и темной тем оформления;
- резервное копирование и восстановление внешнего вида графического интерфейса.

Доступны следующие действия над параметрами брендирования:

- сохранение резервной копии. Для этого нужно нажать экранную кнопку **[Экспорт JSON]** и указать путь для сохранения файла;
- восстановление из резервной копии. Для этого нужно нажать экранную кнопку **[Импорт JSON...]**, указать путь к файлу и нажать экранную кнопку **[Сохранить]**;
- сохранение параметров. Для этого нужно нажать экранную кнопку **[Сохранить]**;
- сброс параметров. Для этого нужно нажать экранную кнопку **[Сбросить]**.

Для управления основными параметрами брендирования нужно перейти «Системные параметры - Системные настройки», выбрать раздел «Брендирование» и перейти во вкладку «Основное».

Основные параметры брендирования перечислены в столбце «Параметр» следующей таблицы (см. таблицу Основные параметры брендирования).

Таблица 145. Основные параметры брендирования

Параметр	Описание
«Название проекта»	В Termidesk VDI версии 7.0 параметр не оказывает влияния на графический интерфейс
«Ширина боковой панели»	Ширина (в пикселях) панели навигации при развернутом состоянии
«Скругление углов»	Скругление углов (в пикселях) кнопок, полей ввода и активных элементов графического интерфейса
«Полный логотип (светлая тема)»	Добавление логотипа для развернутого состояния панели навигации и светлой темы оформления. Для добавления логотипа нужно нажать экранную кнопку **[Перетащите файл сюда или нажмите для выбора]** и указать путь к логотипу. В Termidesk VDI версии 7.0 добавление логотипов через функцию drag-and-drop не поддерживается. Требования к изображению: • размер: до 2 Мб; • поддерживаемые форматы: `.jpeg`, `.jpg`, `.png`, `.svg`, `.webp`
«Полный логотип (тёмная тема)»	Добавление логотипа для развернутого состояния панели навигации и темной темы оформления. Для добавления логотипа нужно нажать экранную кнопку **[Перетащите файл сюда или нажмите для выбора]** и указать путь к логотипу. В Termidesk VDI версии 7.0 добавление логотипов через функцию drag-and-drop не поддерживается. Требования к изображению: • размер: до 2 Мб; • поддерживаемые форматы: `.jpeg`, `.jpg`, `.png`, `.svg`, `.webp`
«Компактный логотип (светлая тема)»	Добавление логотипа для свернутого состояния панели навигации и светлой темы оформления. Для добавления логотипа нужно нажать экранную кнопку **[Перетащите файл сюда или нажмите для выбора]** и указать путь к логотипу. В Termidesk VDI версии 7.0 добавление логотипов через функцию drag-and-drop не поддерживается. Требования к изображению: • размер: до 2 Мб; • поддерживаемые форматы: `.jpeg`, `.jpg`, `.png`, `.svg`, `.webp`

Параметр	Описание
«Компактный логотип (тёмная тема)»	Добавление логотипа для свернутого состояния панели навигации и темной темы оформления. Для добавления логотипа нужно нажать экранную кнопку **[Перетащите файл сюда или нажмите для выбора]** и указать путь к логотипу. В Termidesk VDI версии 7.0 добавление логотипов через функцию drag-and-drop не поддерживается. Требования к изображению: • размер: до 2 Мб; • поддерживаемые форматы: `.jpeg`, `.jpg`, `.png`, `.svg`, `.webp`

Для управления цветовой схемой светлой или темной темы оформления нужно перейти «Системные параметры - Системные настройки», выбрать раздел «Брендирование» и перейти во вкладку «Светлая тема» или «Тёмная тема».

Поддерживается:

- выбор цвета на цветовой палитре;
- выбор цвета с помощью графического элемента «Пипетка»;
- указание значений цвета в форматах RGB, HSL и HEX. Для переключения между форматами цвета нужно нажать на строку с текущим форматом цвета;
- управление прозрачностью цвета. Для этого нужно переместить ползунок параметра «Непрозрачность» в сторону уменьшения или увеличения.

Изменения цветовой схемы тем оформления отображаются в режиме предпросмотра. Для просмотра изменений неактивной темы оформления следует воспользоваться экранной кнопкой **[Переключить на светлую тему для предпросмотра]** или **[Переключить на тёмную тему для предпросмотра]**.

Основные параметры цветовой схемы перечислены в столбце «Параметр» следующей таблицы (см. таблицу Основные параметры цветовой схемы тем оформления).

Таблица 146. Основные параметры цветовой схемы тем оформления

Параметр	Описание
«Фон и типографика»	
«Белый»	Выбор цвета и прозрачности текста на активных вкладках
«Фон»	Выбор цвета и прозрачности фона графического интерфейса
«Фон контента»	Выбор цвета и прозрачности фона панели навигации раздела
«Текст»	Выбор цвета и прозрачности текста графического интерфейса
«Нейтральный»	Выбор цвета и прозрачности текста и элементов графического интерфейса без акцента
«Приглушённый нейтральный»	Выбор цвета и прозрачности второстепенных элементов графического интерфейса
«Текст подсказки и всплывающих окон»	Выбор цвета и прозрачности текста во всплывающих окнах графического интерфейса
«Акцент, поверхности и поля ввода»	

Параметр	Описание
«Основной (акцент)»	Выбор цвета и прозрачности экранных кнопок, ссылок и активных элементов графического интерфейса
«Основной (наведение)»	Выбор цвета и прозрачности экранных кнопок при наведении на них указателя мыши
«Приглушённый основной»	Выбор цвета и прозрачности фона уведомлений и активных блоков графического интерфейса
«Вторичный (наведение)»	Выбор цвета и прозрачности элементов графического интерфейса при наведении на них указателя мыши
«Третичный»	Выбор цвета и прозрачности фона вспомогательных элементов графического интерфейса (экранных кнопок, переключателей и областей загрузки файлов)
«Третичный (наведение)»	Выбор цвета и прозрачности фона вспомогательных элементов графического интерфейса (экранных кнопок, переключателей и областей загрузки файлов) при наведении на них указателя мыши
«Граница полей ввода»	Выбор цвета и прозрачности границ полей ввода
«Боковая панель, шапка и поиск»	
«Боковая панель»	Выбор цвета и прозрачности панели навигации
«Текст боковой панели (активный, наведение)»	Выбор цвета и прозрачности текста панели навигации в активном состоянии и при наведении на него указателя мыши
«Пункт меню (обычный)»	Выбор цвета и прозрачности текста разделов и подразделов панели навигации в неактивном состоянии
«Заголовок открытой ветки»	Выбор цвета и прозрачности текста раскрытых разделов панели навигации
«Заголовок активной открытой ветки»	Выбор цвета и прозрачности текста активного раздела панели навигации
«Фон шапки»	Выбор цвета и прозрачности фона системной панели
«Фон поиска в боковой панели»	Выбор цвета и прозрачности поля поиска панели навигации
«Текст поиска»	Выбор цвета и прозрачности текста в поле поиска панели навигации
«Плейсхолдер поиска»	Выбор цвета и прозрачности графического элемента «Лупа» в поле поиска панели навигации
«Статусы»	
«Успех»	Выбор цвета и прозрачности элементов графического интерфейса, отображающих успешное выполнение операций
«Приглушённый успех»	Выбор цвета и прозрачности фона уведомлений об успешной операции
«Предупреждение»	Выбор цвета и прозрачности элементов графического интерфейса, отображающих предупреждения
«Приглушённое предупреждение»	Выбор цвета и прозрачности фона предупреждающих уведомлений
«Опасность»	Выбор цвета и прозрачности элементов графического интерфейса, отображающих ошибки
«Приглушённая опасность»	Выбор цвета и прозрачности фона уведомлений об ошибках

Управление экспериментальными параметрами Termidesk VDI

Включение и отключение экспериментальных параметров Termidesk VDI производится из командной строки.

Для активации экспериментального параметра нужно:

- перейти в интерфейс командной строки;
- переключиться на пользователя `termidesk`:

```
sudo -u termidesk bash
```

- присвоить значение `True` ключу `--value`:

```
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_config set --key
experimental.2fa.enabled --value True
```

где:

`experimental.2fa.enabled` - наименование параметра.

Перечень экспериментальных параметров приведен в таблице (см. таблицу Экспериментальные параметры Termidesk VDI).

Таблица 147. Экспериментальные параметры Termidesk VDI

Параметр	Описание	Значение по умолчанию
`experimental.2fa.enabled`	Параметр поддержки двухфакторной аутентификации	`false`
`experimental.converted.transports.backup.path`	Параметр устанавливает путь сохранения файла формата `.json` с параметрами ранее существовавших протоколов доставки. Параметр менять не рекомендуется	`/opt/termidesk.backups`
`experimental.deviceauth.enabled`	Параметр поддержки авторизации устройств доступа	`false`
`experimental.html5.singleTab.enabled`	Параметр поддержки режима открытия HTML5-клиента в той же вкладке веб-браузера, из которой происходит его запуск	`false`
`experimental.loudplay.audioBitrate`	Параметр позволяет задать качество и объем передаваемых аудиоданных (Кб/с)	`128000`
`experimental.loudplay.bbrBitrateInitial`	Параметр позволяет задать начальную скорость видеопотока (Кб/с). Для управления параметром в «Портале администратора» в настройках протокола доставки Loudplay нужно активировать параметр «Автоматическое изменение скорости видеопотока». Диапазон значений: от 100 до 5000	`1000`
`experimental.loudplay.bbrBitrateMin`	Параметр позволяет задать минимально возможную скорость видеопотока (Кб/с). Для управления параметром в «Портале администратора» в настройках протокола доставки Loudplay нужно активировать параметр «Автоматическое изменение скорости видеопотока». Диапазон значений: от 50 до 3000	`50`

Параметр	Описание	Значение по умолчанию
experimental.loudplay.bbrBitrateMax	Параметр позволяет задать максимально возможную скорость видеопотока (Кб/с). Для управления параметром в «Портале администратора» в настройках протокола доставки Loudplay нужно активировать параметр «Автоматическое изменение скорости видеопотока». Диапазон значений: от 5000 до 100000	12000
experimental.loudplay.bbrCycleDelay	Параметр позволяет задать время (мс) между циклами расчета нового битрейта. Для управления параметром в «Портале администратора» в настройках протокола доставки Loudplay нужно активировать параметр «Автоматическое изменение скорости видеопотока». Диапазон значений: от 100 до 10000	8000
experimental.loudplay.bbrGainDrain	Параметр позволяет регулировать уровень уменьшения пропускной способности сети в зависимости от нагрузки. Диапазон значений: от 0.1 до 0.9	0.5
experimental.loudplay.bbrGainIncrease	Параметр позволяет регулировать скорость передачи данных в зависимости от пропускной способности сети. Диапазон значений: от 1.1 до 5	2
experimental.loudplay.bbrGainProbe	Параметр позволяет регулировать частоту увеличения пропускной способности сети в зависимости от нагрузки. Диапазон значений: от 1.1 до 1.3	1.15
experimental.loudplay.bbrGainStandby	Параметр позволяет регулировать уровень увеличения пропускной способности сети в режиме ожидания. Диапазон значений: от 0.1 до 0.9	0.75
experimental.loudplay.bbrPingDelay	Параметр позволяет задать время (мс) между циклами измерения состояния канала. Для управления параметром в «Портале администратора» в настройках протокола доставки Loudplay нужно активировать параметр «Автоматическое изменение скорости видеопотока». Диапазон значений: от 10 до 1000	50
experimental.loudplay.bbrPort	Параметр позволяет задать порт для управления сетевыми соединениями. Диапазон значений: от 0 до 65535	8556
experimental.loudplay.clipboardPort	Параметр позволяет задать порт для передачи данных буфера обмена. Диапазон значений: от 0 до 65535	8559

Параметр	Описание	Значение по умолчанию
`experimental.loudplay.controlEnable`	Параметр позволяет управлять включением или отключением передачи сигналов клавиатуры и мыши. Возможные значения: • `false` - запретить передачу сигналов клавиатуры и мыши; • `true` - разрешить передачу сигналов клавиатуры и мыши	`true`
`experimental.loudplay.controlForceAbsoluteCursor`	Параметр позволяет управлять определением абсолютных или относительных координат мыши. Отключение параметра рекомендуется в случаях, когда курсор мыши плохо позиционируется в приложениях. Возможные значения: • `false` - запретить определение абсолютных координат мыши; • `true` - разрешить определение абсолютных координат мыши	`true`
`experimental.loudplay.controlPort`	Параметр позволяет задать порт для передачи сигналов клавиатуры и мыши. Диапазон значений: от 0 до 65535	`8555`
`experimental.loudplay.controlPortTCP`	Параметр позволяет задать порт для передачи сигналов клавиатуры и мыши по протоколу TCP. Диапазон значений: от 0 до 65535	`8557`
`experimental.loudplay.fecRedundancy`	Параметр позволяет задать избыточность данных (в процентах) для обеспечения устойчивости к потерям в сети. Для управления параметром в «Портале администратора» в настройках протокола доставки Loudplay нужно активировать параметр «Помехоустойчивое кодирование». Диапазон значений: от 0 до 100	`20`
`experimental.loudplay.language`	Параметр задает язык интерфейса клиента Loudplay	`system`

Параметр	Описание	Значение по умолчанию
experimental.loudplay.logPath	Параметр определяет путь к файлу журнала клиента Loudplay Начиная с Termidesk VDI версии 7.0.2 указанное значение передается компоненту «Клиент» для переопределения файла журнала и его размещения по новому пути на стороне пользовательской рабочей станции: • ОС Microsoft Windows: C:\Users\<user>\AppData\Roaming\UVEON\logs\Loudplay_Client.log; • ОС Linux: /home/<user>/.config/UVEON/logs/Loudplay_Client.log Ротация журналов Loudplay выполняется средствами и настройками клиента Loudplay. Очистка журналов Loudplay находится в зоне ответственности пользователей Loudplay.	logs/lp_client.log
experimental.loudplay.peripheryPort	Параметр позволяет порт для перенаправления USB-устройств. Диапазон значений: от 0 до 65535	8558
experimental.loudplay.rtpAudioPort	Параметр позволяет задать порт для для передачи аудио. Для управления параметром в «Портале администратора» в настройках протокола доставки Loudplay нужно задать значение «UDP» параметру «Протокол передачи видео». Диапазон значений: от 0 до 65535	6972
experimental.loudplay.rtpRetransmission	Параметр позволяет управлять непрерывной передачей видеоизображения на каналах с потерями до 3%. Для управления параметром в «Портале администратора» в настройках протокола доставки Loudplay нужно активировать параметр «Помехоустойчивое кодирование». Отключение параметра rtpRetransmission, в сочетании с «Помехоустойчивым кодированием», рекомендуется в исключительных случаях, когда важна минимальная задержка отклика на стабильных каналах связи без потерь. Возможные значения: • false - запретить непрерывную передачу видеоизображения; • true - разрешить непрерывную передачу видеоизображения	true

Параметр	Описание	Значение по умолчанию
`experimental.loudplay.rtpVideoPort`	Параметр позволяет задать порт для передачи видео. Для управления параметром в «Портале администратора» в настройках протокола доставки Loudplay нужно задать значение «UDP» параметру «Протокол передачи видео». Диапазон значений: от 0 до 65535	`6970`
`experimental.loudplay.serverPort`	Параметр позволяет задать порт для подключения по протоколу Loudplay. Диапазон значений: от 0 до 65535	`8554`
`experimental.loudplay.showBadConnect`	Параметр активации отображения уведомлений при возникновении проблем с сетью. Возможные значения: • `false` - запретить отображение уведомлений; • `true` - разрешить отображение уведомлений	`false`
`experimental.loudplay.showResNotif`	Параметр активации отображения уведомлений при различии разрешений между экраном пользовательской рабочей станции и экраном РМ. Возможные значения: • `false` - запретить отображение уведомлений; • `true` - разрешить отображение уведомлений	`false`
`experimental.loudplay.transports.enabled`	Параметр поддержки протокола доставки Loudplay	`false`
`experimental.loudplay.x1`	Параметр позволяет запустить таймер с отсчетом времени бездействия (в секундах), по истечении которого активируется действие или событие	`0`
`experimental.metasessionsprov.maxConnectionCount`	Параметр позволяет задать максимальное количество подключений к ноде Метапоставщика	`181`
`experimental.mtls.mode`	Параметр позволяет задать режим mTLS для взаимодействия между компонентами Termidesk VDI. В этом сценарии сервер Termidesk VDI выступает в роли клиента процесса взаимной аутентификации. Возможные значения: • `disabled` - результат проверки сертификата игнорируется. В этом режиме mTLS не используется; • `permissive` - нестрогий режим проверки сертификата. Проверка выполняется, но если сертификат не предоставлен или он недействительный, то запрос выполняется, а в журнал записывается предупреждение; • `strict` - строгий режим проверки сертификата. Клиент обязан предоставить действительный сертификат. Запрос отклоняется, когда сертификат не прошел проверку	`disabled`
`experimental.openstack.provider.enabled`	Параметр поддержки поставщика ресурсов OpenStack	`false`

Параметр	Описание	Значение по умолчанию
`experimental.provider.physmachine.enabled`	Параметр поддержки поставщика ресурсов для физических машин	`false`
`experimental.t1cloud.provider.enabled`	Параметр поддержки поставщика ресурсов «Платформа T1cloud»	`false`
`experimental.vmware.netboot.service.enabled`	Параметр поддержки шаблона РМ «Сетевая загрузка» для поставщика ресурсов VMware vSphere	`false`

Хранение чувствительной информации с выбранным способом хранения «hvac»

Алгоритм работы

Способ хранения паролей выбирается на этапе установки Termidesk VDI. Способ хранения паролей «hvac» подразумевает, что будет использоваться хранилище OpenBao или Hashicorp Vault. Хранилище при этом должно быть заранее создано и настроено. При использовании Hashicorp Vault со схемой AD поддерживается автоматическое обновление паролей.

Termidesk VDI не выполняет ротацию паролей и другой чувствительной информации в хранилище: это возлагается на администраторов хранилища.

До начала установки Termidesk VDI администратору необходимо создать в хранилище контейнеры для хранения чувствительной информации. Эти контейнеры используются для подключения к элементам инфраструктуры, например для хранения учетных данных для подключения к MS AD. Формат хранения объектов и контейнеров в Termidesk VDI должен соответствовать формату, принятому в хранилище.

Администратором подготавливается конфигурационный файл Termidesk VDI `termidesk.conf`, в котором указываются значения для:

- `SECRETS_OPENBAO_URL`;
- `DJANGO_SECRET_KEY`;
- `SECRETS_OPENBAO_ROLE_ID`;
- `SECRETS_OPENBAO_TOKEN`;
- `SECRETS_OPENBAO_DB_PATH` и `SECRETS_OPENBAO_RABBITMQ_PATH`;
- `METRICS_ACCESS_KEY`;
- `HEALTH_CHECK_KEY`;
- опционально, для подключения к хранилищу по протоколу SSL:
  - `SECRETS_OPENBAO_CLIENT_CERT`;
  - `SECRETS_OPENBAO_CLIENT_KEY`;
  - `SECRETS_OPENBAO_SERVER_CERT`.

Хранение RSA-ключей (`id_rsa` и `id_rsa.pub`) может выполняться в отдельных объектах, заданных в хранилище.

Ограничений на длину имени хранимого объекта нет, однако есть ограничения в Termidesk VDI:

- если путь к объекту задается в веб-интерфейсе Termidesk VDI («Портал администратора»), то он должен быть меньше 255 символов;
- если путь к объекту задается на этапе установки Termidesk VDI, то он должен быть меньше 512 символов. При этом ограничений на длину строки параметра в конфигурационном файле termidesk.conf нет.

Алгоритм работы Termidesk VDI с хранилищем после установки Termidesk VDI или старта службы termidesk-vdi:

- первичный одноразовый токен доступа читается из файловой системы первой службой, получившей доступ к нему (termidesk-celery-beat или termidesk-celery-worker). Путь расположения файла указан в SECRETS_OPENBAO_TOKEN;
- первичный одноразовый токен доступа преобразуется к открытому виду (извлекается SECRET_ID) и используется для первичного подключения к хранилищу. При этом:
  - на основе SECRET_ID подготавливается новый «упакованный» (wrapped) токен и записывается в файл, указанный в SECRETS_OPENBAO_TOKEN. Этот токен используется службами, получившими доступ к нему;
  - при запуске служб «упакованный» токен обновляется на новый. Далее отдельный процесс отслеживает время жизни «упакованного» токена и, при истечении времени (время жизни задается в параметре SECRETS_OPENBAO_WRAP_TTL), обновляет его на новый. При штатной остановке службы «упакованный» токен также обновляется;
- используя полученный SECRET_ID и значение, заданное в SECRETS_OPENBAO_ROLE_ID, «Универсальный диспетчер» аутентифицируется для взаимодействия с хранилищем и получает ACCESS_TOKEN. ACCESS_TOKEN предоставляет доступ ко всей чувствительной информации, расположенной в хранилище для роли Termidesk VDI;
- при старте службы termidesk-vdi и перед подключением к БД и брокеру сообщений выполняется запрос информации из хранилища для получения:
  - DJANGO_SECRET_KEY;
  - SECRETS_OPENBAO_DB_PATH;
  - SECRETS_OPENBAO_RABBITMQ_PATH;
  - METRICS_ACCESS_KEY;
  - HEALTH_CHECK_KEY;
  - другой чувствительной информации (например для подключения к объектам инфраструктуры);
- после получения из хранилища DJANGO_SECRET_KEY и всей перечисленной выше чувствительной информации во внутренней структуре Termidesk VDI (временной памяти tmpfs) значения устанавливаются в полученные из хранилища и используются для взаимодействия с компонентами.

Время действия ACCESS_TOKEN определяется политикой хранилища, но до момента истечения его срока жизни выполняется процесс обновления со стороны Termidesk VDI. Алгоритм работы Termidesk VDI при обновлении ACCESS_TOKEN:

- проверка валидности ACCESS_TOKEN выполняется отдельным процессом, запускаемым после его получения (получение описано в алгоритме выше);
- периодичность проверки задается параметром SECRETS_OPENBAO_WATCHDOG_INTERVAL, заданным в termidesk.conf;
- если оставшееся время действия ACCESS_TOKEN меньше значения, определенного в параметре SECRETS_OPENBAO_TTL_DEADLINE конфигурационного файла termidesk.conf, то начинается процесс обновления:
  - из внутренней структуры Termidesk VDI читается SECRET_ID и преобразуется к «упакованному» (wrapped) виду. Время действия такого «упакованного» токена

определяется параметром SECRETS_OPENBAO_WRAP_TTL;

- SECRET_ID удаляется из внутренней структуры Termidesk VDI;
- процесс повторяется: происходит преобразование токена к открытому виду (извлечению SECRET_ID) и получение ACCESS_TOKEN.

Хранение данных в контейнерах и примеры

Чувствительная информация (имена учетных записей, пароли, открытые и закрытые ключи, keytab-файлы, токены) хранится в контейнерах, пути к которым задаются вручную.

В контейнерах может содержаться как динамически обновляемая чувствительная информация, так и статическая. Поэтому в Termidesk VDI для определения типа информации используются префиксы при задании пути к контейнеру хранения:

- hvac-ad:// - префикс используется для динамически обновляемой чувствительной информации. Может быть задан как для хранилища Hashicorp Vault, так и для OpenBao, но последний требует специфической настройки;
- hvac-kv:// - префикс используется для статической чувствительной информации. Может быть задан как для хранилища OpenBao, так и для Hashicorp Vault;
- hvac-pki:// - префикс используется для информации о сертификатах. Может быть задан как для хранилища OpenBao, так и для Hashicorp Vault.

Помимо указания префикса должна использоваться точка монтирования (mount point), заданная администратором в хранилище.

Для корректной работы Termidesk VDI со статической чувствительной информацией в хранилище должна быть повторена структура данных Active Directory. Контейнер, содержащий чувствительную информацию, должен содержать параметры:

- current_password - пароль учетной записи;
- username - имя учетной записи.

Пример:

```
{
    'current_password':
'?@09AZ3PlvTzMKhsvZ91YFyVjVRHceYQ34eizKcKhVNHPjQJ46kvGGdsBPSkRcE9',
    'username': 'adfs-s'
},
```

Таким образом общий формат указания пути к контейнеру хранениятчувствительной информации в Termidesk VDI выглядит следующим образом:

Символ «/» определяет, что должно быть возвращено все содержимое контейнера.

Если нужно вернуть значение конкретной переменной (key) контейнера, символ «/» не используется.

- если нужно вернуть всю информацию из контейнера:

```
<префикс> <точка_монтирования#> <путь_к_контейнеру>/
```

- если нужно вернуть только значение конкретного параметра:

```
<префикс> <точка_монтирования#> <путь_к_параметру_в_хранилище>
```

Допустим, в хранилище создан контейнер со статической информацией `termidesk` и точкой монтирования `secret`:

```
vault kv get secret/termidesk
```

Контейнер содержит следующие параметры:

```
========== Data ==========
Key                 Value
---                 -----
current_password    my_password
username            Администратор
```

В этом случае в Termidesk VDI следует указывать:

- для возврата всех параметров: `hvac-kv://secret#termidesk/` (будет возвращено: `{'current_password': 'my_password', 'username': 'Администратор'}`);
- для возврата значения параметра `username`: `hvac-kv://secret#termidesk/username` (будет возвращено: `'Администратор'`).

Схема взаимодействия с хранилищем приведена на рисунке (см. рисунок Схема взаимодействия с хранилищем).

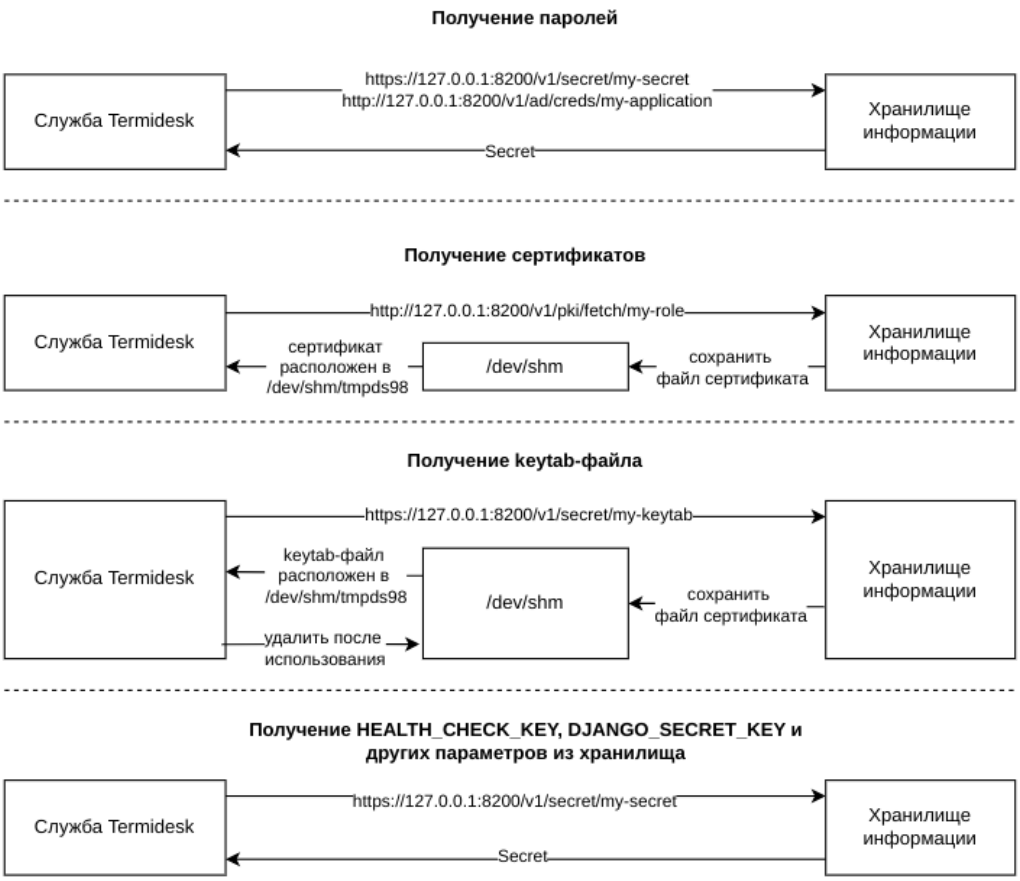


Рисунок 95. Схема взаимодействия с хранилищем

Дополнительные примеры приведены в таблице (см. таблицу Примеры указания путей к чувствительной информации в Termidesk).

Таблица 148. Примеры указания путей к чувствительной информации в Termidesk

Команда в хранилище	Указание пути в Termidesk
Команда записи роли в хранилище: `vault write ad/roles/vvddaa service_account_name="vvddaa@domain.local"`	`hvac-ad://ad#vvddaa/` Где: `hvac-ad://` - префикс; `ad#` - точка монтирования; `vvddaa/` - путь к роли
Команда записи сертификата в хранилище: `vault kv put secret/termidesk-admin/ssl-cert-snakeoil pem=@astra.local.pem` Команды вида `vault kv put` перезаписывают контейнер сразу целиком, поэтому если задание сертификата и ключа будет разделено на разные команды, то в контейнере окажется только то, что добавлялось последним	`hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem` Где: `hvac-kv://` - префикс; `secret#` - точка монтирования; `termidesk-admin/ssl-cert-snakeoil/` - путь к контейнеру; `pem` - сертификат

Команда в хранилище	Указание пути в Termidesk

Сгенерированный на контроллере домена keytab -файл должен быть преобразован к формату BASE64 для использования в хранилище:
 	
`base64 termidesk.keytab > termidesk.keytab.b64`
 	
Команда записи keytab-файла в хранилище:
 	
`vault kv put secret/termidesk-admin/keytabs termidesk=@kerberos.keytab.b64`
 	
Пример команды для преобразования файла и одновременной записи в хранилище:
 	
`vault kv put secret/termidesk-admin/keytabs termidesk="$(base64 -w 0 termidesk.keytab)"`
	hvac-kv://secret#termidesk-admin/keytabs/termidesk
	
	Где:
	
	hvac-kv:// - префикс;
	
	secret# - точка монтирования;
	
	termidesk-admin/keytabs/ - путь к контейнеру;
	
	termidesk - keytab-файл

Пример команды записи данных для подключения к СУБД в хранилище: `vault kv put secret/postgresql username=termidesk current_password=ksedimret`	hvac-kv://secret#/postgresql/ Где: hvac-kv:// - префикс; secret# - точка монтирования; postgresql/ - путь к контейнеру; username=termidesk - пользователь для подключения к СУБД; current_password=ksedimret - пароль для подключения к СУБД

Команда в хранилище	Указание пути в Termidesk

Пример команды записи данных для подключения к RabbitMQ в хранилище:
 	
`vault kv put secret/rabbitmq username=termidesk current_password=ksedimret`
 	
Поддерживается указание до трех пар имени и пароля пользователя для подключения к RabbitMQ.
 	
Пример использования:
 	
`vault kv put secret/rabbitmq username=termidesk1 current_password=ksedimret1 username=termidesk2 current_password=ksedimret2 username=termidesk3 current_password='qqq 111!#$%^&*()[]{}'`
	`hvac-kv://secret#/rabbitmq/`
	
	Где:
	
	`hvac-kv://` - префикс;
	
	`secret#` - точка монтирования;
	
	`rabbitmq/` - путь к контейнеру;
	
	`username=termidesk` - пользователь для подключения к RabbitMQ;
	
	`current_password=ksedimret` - пароль для подключения к RabbitMQ

Изменение способа хранения паролей на OpenBao

При стандартной настройке Termidesk VDI пароли хранятся в преобразованном виде в файле `/etc/opt/termidesk-vdi/termidesk.conf`. Начиная с Termidesk VDI версии 5.1 добавлен новый способ хранения паролей с использованием настроенного хранилища OpenBao.

Для изменения способа хранения паролей и перехода на использование хранилища OpenBao нужно:

- задать в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` параметру `SECRET_STORAGE_METHOD` значение `openbao`;
- задать остальные параметры конфигурационного файла `/etc/opt/termidesk-vdi/termidesk.conf`, относящиеся к OpenBao;
- в интерфейсе командной строки переключиться на пользователя `termidesk`:

```
sudo -u termidesk bash
```

- выполнить команду миграции:

```
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_openbao_migrate
```

При появлении ошибок после выполнения команды миграции нужно:

- изменить значение параметра `SECRET_STORAGE_METHOD` на `config`;
- повторить ввод паролей для параметров, указанных в ошибке;
- снова изменить значение `SECRET_STORAGE_METHOD` на `openbao`;

- выполнить команду миграции:

```
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_openbao_migrate
```

Для возврата к способу хранения паролей из конфигурационного файла нужно:

- убедиться, что в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` параметру `SECRET_STORAGE_METHOD` задано значение `openbao`;
- в интерфейсе командной строки переключиться на пользователя `termidesk`:

```
sudo -u termidesk bash
```

- выполнить команду миграции:

```
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_openbao_reverse_migrate
```

- задать в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` параметру `SECRET_STORAGE_METHOD` значение `config`.

Перенаправление на HTTPS

Для работы веб-интерфейса Termidesk VDI по безопасному протоколу HTTPS, используются настройки веб-сервера `apache` для перенаправления запроса с протокола HTTP на HTTPS.

Перенаправление на HTTPS настроено по умолчанию после установки Termidesk VDI. При необходимости использования незащищенного протокола HTTP администратор должен изменить файл `/etc/apache2/sites-available/termidesk.conf`, раскомментировав настройки VirtualHost и закомментировав настройки HTTPS. Шаблон файла для протокола HTTP представлен ниже.

Настройки перенаправления задаются в конфигурационном файле `/etc/apache2/sites-available/termidesk.conf`. После внесения любых изменений в этот файл необходимо перезапустить службу `apache2`:

```
sudo systemctl restart apache2
```

Шаблон части конфигурационного файла для протокола HTTPS:

Представлены только шаблоны конфигурационного файла! Изменение конфигурации не должно выполняться копированием представленного шаблона.

```
# Сайт для принудительного перенаправления на протокол HTTPS.
<VirtualHost *:80>
        ServerName #HOSTNAME#
        RewriteEngine On
        RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R=308,L]
```

```
        RequestHeader set X-Forwarded-Proto expr=%{REQUEST_SCHEME}
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

<IfModule mod_ssl.c>
<VirtualHost _default_:443>
    ServerName #HOSTNAME#
    DocumentRoot /opt/termidesk/share/termidesk-vdi/src

    Alias /media/ /opt/termidesk/share/termidesk-vdi/src/media/
    Alias /static/ /opt/termidesk/share/termidesk-vdi/src/static/

    <Directory /opt/termidesk/share/termidesk-vdi/src/static>
        Order deny,allow
        Allow from all
        Require all granted
    </Directory>

    <Directory /opt/termidesk/share/termidesk-vdi/src/media>
        Order deny,allow
        Allow from all
        Require all granted
    </Directory>

    RewriteEngine on
    ProxyTimeout 70
    ProxyPreserveHost On
    ProxyRequests Off

    ProxyPassMatch ^/media/ !
    ProxyPassMatch ^/static/ !

    ProxyPass / http://127.0.0.1:8000/
    ProxyPassReverse / http://127.0.0.1:8000/

    RequestHeader set X-Forwarded-Proto expr=%{REQUEST_SCHEME}

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    SSLEngine on
    SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
    SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

    RequestHeader set X-TDSK-SSL_CLIENT_FORMAT 'apache'
    RequestHeader set X-TDSK-SSL_CLIENT_S_DN expr=%{SSL_CLIENT_S_DN}
    RequestHeader set X-TDSK-SSL_CLIENT_VALIDITY_START expr=%{SSL_CLIENT_V_START}
    RequestHeader set X-TDSK-SSL_CLIENT_VALIDITY_END expr=%{SSL_CLIENT_V_END}
```

```
    RequestHeader set X-TDSK-SSL_CLIENT_VERIFY expr=%{SSL_CLIENT_VERIFY}
    RequestHeader set X-TDSK-SSL_CLIENT_CERT expr=%{SSL_CLIENT_CERT}
</VirtualHost>
</IfModule>
```

Шаблон части конфигурационного файла для работы по незащищенному протоколу HTTP (конфигурация HTTPS при этом должна быть закомментирована):

```
<VirtualHost *:80>
    ServerName #HOSTNAME#
    DocumentRoot /opt/termidesk/share/termidesk-vdi/src

    Alias /media/ /opt/termidesk/share/termidesk-vdi/src/media/
    Alias /static/ /opt/termidesk/share/termidesk-vdi/src/static/

    <Directory /opt/termidesk/share/termidesk-vdi/src/static>
        Order deny,allow
        Allow from all
        Require all granted
    </Directory>

    <Directory /opt/termidesk/share/termidesk-vdi/src/media>
        Order deny,allow
        Allow from all
        Require all granted
    </Directory>

    RewriteEngine on
    ProxyTimeout 70
    ProxyPreserveHost On
    ProxyRequests Off

    ProxyPassMatch ^/media/ !
    ProxyPassMatch ^/static/ !

    ProxyPass / http://127.0.0.1:8000/
    ProxyPassReverse / http://127.0.0.1:8000/

    RequestHeader set X-Forwarded-Proto expr=%{REQUEST_SCHEME}

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Замена SSL-сертификата веб-сервера

Для доступа к веб-интерфейсу по протоколу HTTPS на этапе установки веб-сервера автоматически генерируется самоподписанный сертификат и закрытый ключ к нему. В

некоторых случаях может понадобиться заменить эти сертификаты на другие.

Для замены SSL-сертификатов необходимо:

- получить новый сертификат и ключ к нему;
- поместить новый сертификат формата `.pem` в каталог `/etc/ssl/certs/`:

```
sudo cp <путь_к_сертификату> /etc/ssl/certs/
```

- поместить новый ключ формата `.key` в каталог `/etc/ssl/private/`:

```
sudo cp <путь_к_ключу> /etc/ssl/private/
```

Если сертификат и ключ находятся в PKCS12-контейнере (файл формата `.pfx`), необходимо сначала сконвертировать их в нужный формат:

```
openssl pkcs12 -in <путь_к_pfx-контейнеру> -out <путь_к_создаваемому_файлу.pem>
-nodes
openssl pkcs12 -in <путь_к_pfx-контейнеру> -nocerts -nodes  -out
<путь_к_создаваемому_файлу.key>
openssl rsa -in <путь_к_созданному_файлу_ключа.key> -out
<путь_сохранения_преобразованного_ключа.key>
```

- отредактировать файл `/etc/apache2/sites-available/termidesk.conf`, заменив путь к сертификату и ключу для параметров `SSLCertificateFile` и `SSLCertificateKeyFile` на новые:

```
SSLEngine on
SSLCertificateFile      /etc/ssl/certs/new_cert.pem
SSLCertificateKeyFile /etc/ssl/private/new_key.key
</VirtualHost>
```

- перезапустить веб-сервер:

```
sudo systemctl restart apache2
```

Установка корневого сертификата центра сертификации

Установка корневого сертификата центра сертификации (ЦС) может быть необходима при настройке доступа между компонентами по протоколу SSL. Предполагается, что инфраструктура открытых ключей (PKI) уже развернута в организации и ЦС установлен.

Для установки корневого сертификата ЦС (например, `CA.crt`) на «Универсальный диспетчер» Termidesk VDI, нужно:

- скопировать файл `CA.crt` на сервер Termidesk VDI;
- затем скопировать `CA.crt` в каталог `/usr/share/ca-certificates`:

```
sudo cp <путь_к_сертификату> /usr/share/ca-certificates/
```

- выполнить добавление корневого сертификата ЦС:

```
sudo dpkg-reconfigure ca-certificates
```

- на запрос «Доверять новым сертификатам удостоверяющих центров» ответить «Да»;
- убедиться, что сертификат `CA.crt` отмечен для активации;
- нажать экранную кнопку **[Ok]** и дождаться окончания операции.

Для настройки Termidesk VDI на работу с сертификатами нужно:

- добавить параметр `REQUESTS_CA_BUNDLE` в конфигурационный файл `termidesk.conf`. В параметре нужно указать путь к файлу с доверенным корневым сертификатом. Пример:

```
REQUESTS_CA_BUNDLE='/etc/ssl/certs/ca.crt'
```

- выполнить перезапуск службы `termidesk-vdi`:

```
sudo systemctl restart termidesk-vdi
```

Работа веб-интерфейса Termidesk VDI с протоколом TLS

Веб-интерфейс Termidesk VDI по умолчанию поддерживает работу на всех протоколах, кроме SSLv3. Для того чтобы включить поддержку только протоколов TLS1.2 и TLS 1.3 в веб-сервере Apache, нужно скорректировать файл конфигурации `/etc/apache2/mods-available/ssl.conf`.

Для этого:

- выполнить резервное копирование текущего файла конфигурации:

```
sudo cp /etc/apache2/mods-available/ssl.conf /etc/apache2/mods-
available/ssl.conf_bkp
```

- включить поддержку только протоколов TLS1.2 и TLS 1.3, внеся изменения в файл конфигурации `/etc/apache2/mods-available/ssl.conf`:

```
sudo sed -i 's/SSLProtocol all -SSLv3/SSLProtocol -all +TLSv1.2 +TLSv1.3/g'
/etc/apache2/mods-available/ssl.conf
sudo sed -i 's/SSLCipherSuite HIGH:!aNULL/SSLCipherSuite HIGH:!aNULL:!MD5:!3DES/g'
/etc/apache2/mods-available/ssl.conf
sudo sed -i 's/#SSLHonorCipherOrder on/SSLHonorCipherOrder on/g' /etc/apache2/mods-
available/ssl.conf
```

- выполнить обновление файлов конфигурации:

```
sudo systemctl reload apache2
```

Настройка mTLS

Конфигурирование веб-сервера Apache для mTLS

Для использования mTLS между компонентами Termidesk VDI нужно выполнить конфигурирование веб-сервера apache. Для этого:

- изменить конфигурационный файл `/etc/apache2/sites-available/termidesk.conf`, указав:

Указанные пути к сертификатам используются в качестве примера.

```
SSLEngine on
SSLCertificateFile      /home/cld/certs/server.cert.pem
SSLCertificateKeyFile   /home/cld/certs/server.key.pem
SSLCACertificateFile    /home/cld/certs/ca.cert.pem
#       SSLVerifyClient require
#       SSLVerifyClient optional
#       SSLVerifyClient none

#SSLVerifyClient require|optional|none

# Для корректной работы Termidesk VDI с MTLS необходимо настроить директивы ниже
# в соответствии с условиями и требованиями окружения инсталляции
# SSLCACertificateFile
# SSLVerifyClient
# SSLVerifyDepth

# Проброс параметров клиентского сертификата в Termidesk
# через набор собственных заголовков

RequestHeader set X-TDSK-SSL-CLIENT-FORMAT 'apache'
RequestHeader set X-TDSK-SSL-CLIENT-S-DN expr=%{SSL_CLIENT_S_DN}
RequestHeader set X-TDSK-SSL-CLIENT-I-DN expr=%{SSL_CLIENT_I_DN}
RequestHeader set X-TDSK-SSL-CLIENT-SERIAL expr=%{SSL_CLIENT_M_SERIAL}
RequestHeader set X-TDSK-SSL-CLIENT-VALIDITY-START expr=%{SSL_CLIENT_V_START}
RequestHeader set X-TDSK-SSL-CLIENT-VALIDITY-END expr=%{SSL_CLIENT_V_END}
RequestHeader set X-TDSK-SSL-CLIENT-VERIFY expr=%{SSL_CLIENT_VERIFY}
RequestHeader set X-TDSK-SSL-CLIENT-CERT "expr=%{escape:%{SSL_CLIENT_CERT}}"
```

- перезапустить веб-сервер:

```
sudo systemctl restart apache2
```

Конфигурирование компонентов Termidesk VDI для mTLS

Общие сведения о поддержке mTLS компонентами Termidesk

Termidesk VDI поддерживает взаимную аутентификацию между компонентами Termidesk VDI по протоколу mTLS.

В Termidesk VDI версии 7.0 настройка mTLS поддерживается в компонентах:

- «Универсальный диспетчер» для всех ролей («Портал администратора», «Портал пользователя», «Агрегатор администратора», «Агрегатор пользователя»);
- «Менеджер рабочих мест»;
- «Агент виртуального рабочего места»;
- «Сессионный агент»;
- TERA;
- «Шлюз», реализованный «Балансировщиком нагрузки Термидеск Коннект» (Termidesk Connect).

Для настройки нужно:

- загрузить сертификаты для mTLS на узел каждого компонента;
- указать ранее загруженные сертификаты в конфигурационных файлах каждого компонента, участвующего во взаимодействии по mTLS;
- выбрать сценарии подключений mTLS для сервера Termidesk VDI. Сценарии определяют, между какими компонентами будет использоваться взаимная аутентификация. Выбор сценариев задается в параметре `MTLS_CONNECTIONS` конфигурационного файла `/etc/opt/termidesk-vdi/termidesk.conf` (см. подраздел **Конфигурационный файл `termidesk.conf`**). При распределенной установке серверных компонентов Termidesk VDI параметр может быть задан на каждом узле:
  - узле «Универсального диспетчера»;
  - узле «Менеджер рабочих мест»;
- выбрать режим mTLS в конфигурации сервера Termidesk VDI и в каждом компоненте, с которым предполагается взаимодействие и который поддерживает mTLS:
  - для сервера Termidesk VDI («Универсальный диспетчер» и его ролей, «Менеджер рабочих мест») режим mTLS задается в параметре `MTLS_MODE` конфигурационного файла `/etc/opt/termidesk-vdi/termidesk.conf`;
  - для компонентов Termidesk VDI режим mTLS задается в конфигурационных файлах каждого компонента;
- выполнить настройку веб-сервера apache для mTLS (см. подраздел **Конфигурирование веб-сервера Apache для mTLS**);
- в настройках веб-браузера, из которого будет выполняться подключение к серверу Termidesk VDI, добавить корневой сертификат УЦ в список доверенных (пример для Mozilla Firefox):
  - перейти в меню «Настройки»;
  - выбрать раздел «Приватность и защита». На открывшейся странице переместиться к пункту «Защита - Сертификаты» и нажать экранную кнопку **[Просмотр сертификатов...]**;
  - в открывшемся окне перейти во вкладку «Центры сертификации» и нажать экранную кнопку **[Импортировать]**;
  - выбрать ранее сохраненный файл корневого сертификата УЦ и нажать экранную кнопку **[Открыть]**;

- в открывшемся окне загрузки сертификата выбрать цели импорта. Рекомендуется отметить все предложенные варианты и затем нажать экранную кнопку **[OK]**.

При настроенном режиме mTLS подключение к серверу Termidesk VDI выполняется по его FQDN.

Пример конфигурирования mTLS между компонентами «Универсальный диспетчер» и «Агент виртуального рабочего места»

Пример приведен для компонентов Termidesk VDI, установленных в ОС Astra Linux Special Edition 1.8.

Конфигурирование узла «Универсального диспетчера», установленного с ролями «Портал администратора», «Портал пользователя»:

- загрузить клиентские сертификаты и ключи для mTLS:
  - скопировать их в каталог `/etc/opt/termidesk-vdi/`;
  - назначить владельцем каждого файла пользователя `termidesk`, пример:

```
sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem
```

  - изменить права на каждый файл:

```
sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem
```

- указать клиентский сертификат, ключ к нему и корневой сертификат УЦ в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` в параметрах `MTLS_CLIENT_CERT`, `MTLS_CLIENT_KEY`, `MTLS_CLIENT_CA` соответственно;
- в параметре `MTLS_CONNECTIONS` задать значение `va_agent`;
- в параметре `MTLS_MODE` задать значение `permissive`;
- перезагрузить службу `termidesk-vdi`:

```
sudo systemctl restart termidesk-vdi
```

- выполнить настройку веб-сервера apache для mTLS (см. подраздел **Конфигурирование веб-сервера Apache для mTLS**).

Конфигурирование узла «Агента виртуального рабочего места»:

- загрузить серверные сертификаты и ключи для mTLS:
  - скопировать их в каталог `/etc/termidesk`;
  - назначить владельцем каждого файла пользователя `root`, пример:

```
sudo chown root:root /etc/termidesk/<имя>.pem
```

  - изменить права на каждый файл:

```
sudo chmod 600 /etc/termidesk/<имя>.pem
```

- загрузить клиентские сертификаты и ключи для mTLS аналогично пункту выше;
- в графическом интерфейсе ОС перейти «Звезда - Программы - Инструменты», выбрать ярлык «VDI Agent Configuration» и сконфигурировать параметры:

Предаполагается, что подключение к серверу Termidesk VDI уже было указано, поэтому здесь указаны только параметры, необходимые для mTLS.

  - «mTLS»: выбрать значение «Разрешительный режим»;
  - «Источник сертификатов»: выбрать значение «Файловая система»;
  - «Сервер»: указать в параметрах «Цепочка ЦС», «Сертификат», «Закрытый ключ» ранее загруженные файлы сертификатов и ключей. При необходимости заполнить параметр «Пароль» (если ключ защищен паролем) и отметить пункт «Использовать как клиентский сертификат» (если загруженный сертификат может использоваться и как серверный, и как клиентский);
  - «Клиент»: аналогично указать клиентские сертификаты. Если ранее был отмечен пункт «Использовать как клиентский сертификат», то выполнять действие не требуется;
- для проверки корректности подключения к серверу Termidesk VDI необходимо нажать экранную кнопку **[Проверить]**. Результатом проверки должно являться сообщение «Проверка успешно завершена».

В случае, если сертификаты узлов «Универсального диспетчера» и «Агента виртуального рабочего места» созданы в разных УЦ, то потребуется перечислить корневые и промежуточные сертификаты всех УЦ для компонента «Агента виртуального рабочего места». Пример:

- пусть файл корневого УЦ, выписавшего сертификаты, загруженные для «Универсального диспетчера», содержит информацию (приведен не полный текст сертификата):

```
-----BEGIN CERTIFICATE-----
IBAgIBATANBg
-----END CERTIFICATE-----
```

- пусть файл корневого УЦ, выписавшего сертификаты, загруженные для «Агента виртуального рабочего места», содержит информацию (приведен не полный текст сертификата):

```
-----BEGIN CERTIFICATE-----
MIIEfDCCAuSgAw
-----END CERTIFICATE-----
```

- тогда следует в файл корневого УЦ, выписавшего сертификаты, загруженные для «Агента виртуального рабочего места», добавить информацию об еще одном УЦ:

```
-----BEGIN CERTIFICATE-----
```

```
MIIEfDCCAuSgAw
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
IBAgIBATANBg
-----END CERTIFICATE-----
```

Настройки после распределенной установки фермы Termidesk VDI

Настройка балансировщика для работы с самоподписанными сертификатами

Создание самоподписанного SSL-сертификата

Для создания самоподписанного SSL-сертификата и ключа к нему нужно:

- получить доступ к интерфейсу командной строки;
- выполнить генерацию SSL-сертификата (`/etc/ssl/certs/nginx-selfsigned.crt`) и ключа к нему (`/etc/ssl/private/nginx-selfsigned.key`):

```
sudo openssl req -new -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/ssl/private/nginx-selfsigned.key -out /etc/ssl/certs/nginx-selfsigned.crt
```

Используемые ключи команды:

- `openssl` - базовый инструмент командной строки для создания и управления сертификатами, ключами и другими файлами OpenSSL;
- `req` - эта опция указывает, что на данном этапе нужно использовать запрос на подпись сертификата X.509 (CSR). X.509 – это стандарт инфраструктуры открытого ключа, которого придерживаются SSL и TLS при управлении ключами и сертификатами. Данная команда позволяет создать новый сертификат X.509;
- `new` - эта опция указывает, что будет создаваться новый запрос;
- `x509` - эта опция вносит поправку в предыдущую команду, сообщая утилите о том, что вместо запроса на подписание сертификата необходимо создать самоподписанный сертификат;
- `nodes` - ключ для пропуска опции защиты сертификата парольной фразой. Нужно, чтобы при запуске балансировщик нагрузки (nginx) имел возможность читать файл без вмешательства пользователя. Установив пароль, придется вводить его после каждой перезагрузки;
- `days 365` - эта опция устанавливает срок действия сертификата (в данном случае сертификат действителен в течение года);
- `newkey rsa:2048` - эта опция позволяет одновременно создать новый сертификат и новый ключ. Поскольку ключ, необходимый для подписания сертификата, не был создан ранее, нужно создать его вместе с сертификатом. Данная опция создаст RSA-ключ размером 2048 бит;
- `keyout` - эта опция сообщает OpenSSL, куда поместить сгенерированный файл ключа;
- `out` - эта опция сообщает OpenSSL, куда поместить созданный сертификат.

После исполнения команды надо последовательно ввести ряд параметров, запросы на которые отобразятся в командной строке:

- `Country Name (2 letter code) [AU]`;
- `State or Province Name (full name) [Some-State]`;
- `Locality Name (eg, city) []`;
- `Organization Name (eg, company) [Internet Widgits Pty Ltd]`;
- `Organizational Unit Name (eg, section) []`;
- `Common Name (e.g. server FQDN or YOUR name) []`;
- `Email Address []`.

Наиболее важным параметром является `Common Name` (необходимо ввести FQDN балансировщика). Как правило, в эту строку вносят доменное имя, с которым нужно связать сервер. В случае если доменного имени нет, нужно внести в эту строку IP-адрес сервера.

Файлы ключа и сертификата будут размещены в каталоге, указанном при вызове команды `openssl` в параметрах `keyout` и `out`.

При использовании OpenSSL необходимо также создать ключи Диффи-Хеллмана, для этого:

- открыть программу «Terminal Fly» и получить доступ к интерфейсу командной строки;
- сгенерировать ключи Диффи-Хеллмана длиной 4096 бит и сохранить их в файл `/etc/nginx/dhparam.pem`:

```
sudo openssl dhparam -out /etc/nginx/dhparam.pem 4096
```

Настройка nginx для поддержки SSL

Для настройки nginx нужно:

- создать новый пустой сниппет nginx в каталоге `/etc/nginx/snippets` для указания размещения сертификата и ключа:

```
sudo touch /etc/nginx/snippets/self-signed.conf
```

- отредактировать созданный файл, приведя его к виду:

```
ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;
ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;
```

- создать еще один пустой сниппет, предназначенный для настроек SSL (это позволит серверу nginx использовать надежный механизм преобразования и включит некоторые дополнительные функции безопасности):

```
sudo touch /etc/nginx/snippets/ssl-params.conf
```

- отредактировать созданный файл `ssl-params.conf`, приведя его к виду:

Следует настраивать TLS версии 1.2 и 1.3, т.к. некоторое компоненты могут использовать эти протоколы для связи.

```
ssl_protocols TLSv1.3 TLSv1.2;
ssl_prefer_server_ciphers on;
ssl_dhparam /etc/nginx/dhparam.pem;
ssl_ciphers ECDHE-RSA-AES256-GCM-SHA512:DHE-RSA-AES256-GCM-SHA512:ECDHE-RSA-AES256-
GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384;
ssl_ecdh_curve secp384r1; # Requires nginx >= 1.1.0
ssl_session_timeout  10m;
ssl_session_cache shared:SSL:10m;
ssl_session_tickets off; # Requires nginx >= 1.5.9
ssl_stapling on; # Requires nginx >= 1.3.7
ssl_stapling_verify on; # Requires nginx => 1.3.7
resolver 77.88.8.8 77.88.8.1 valid=300s;
resolver_timeout 5s;
# Disable strict transport security for now. You can uncomment the following
# line if you understand the implications.
# add_header Strict-Transport-Security "max-age=63072000; includeSubDomains;
preload";
add_header X-Frame-Options DENY;
add_header X-Content-Type-Options nosniff;
add_header X-XSS-Protection "1; mode=block";
```

Поскольку сертификат является самоподписанным, `SSL stapling` не будет использоваться. Сервер nginx выдаст предупреждение, отключит `stapling` для данного сертификата и продолжит работу.

Конфигурирование веб-сервера

Для конфигурирования веб-сервера нужно:

- создать пустой конфигурационный файл:

```
sudo touch /etc/nginx/sites-available/sampledomain.ru.conf
```

- отредактировать созданный файл, приведя его к виду:

Здесь и далее примеры IP-адресов приведены в соответствии с RFC 5737. Указанные IP-адреса должны быть заменены на актуальные, используемые согласно схеме адресации, принятой в инфраструктуре организации.

Для корректного отображения IP-адресов источника подключения следует в «Портале администратора» задать параметру «Использовать анонсируемый IP клиента» значение «Да» («Системные параметры - Системные настройки - Безопасность»).

```
upstream daas-upstream-ws {
 least_conn;
```

```
    # PROXY TERMIDESK

     server 192.0.2.41:5099;
     server 192.0.2.42:5099;
     server 192.0.2.43:5099;
     server 192.0.2.44:5099;

}

upstream daas-upstream-nodes {
 least_conn;
     # DISPATCHER TERMIDESK

     server 192.0.2.30:443;
     server 192.0.2.31:443;
     server 192.0.2.32:443;

 }

server {
 listen 0.0.0.0:80;
 listen 0.0.0.0:443 ssl;

  include snippets/self-signed.conf;
  include snippets/ssl-params.conf;

 location /websockify {
         # limit_req zone=fast nodelay;
        proxy_http_version 1.1;
        proxy_pass http://daas-upstream-ws/;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";

        # Connection timeout
        proxy_connect_timeout 1000;
        proxy_send_timeout 1000;
        proxy_read_timeout 1000;
        send_timeout 1000;

        # Disable cache
        proxy_buffering off;
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
 }

 location / {
        proxy_pass https://daas-upstream-nodes/;

        proxy_set_header Host $host;
```

```
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;

 }

}
```

IP-адреса, перечисленные в директиве daas-upstream-ws, являются адресами «Шлюзов» Termidesk VDI, а IP-адреса, перечисленные в директиве daas-upstream-nodes, являются адресами «Универсальных диспетчеров» Termidesk VDI.

- создать символическую ссылку на данный виртуальный хост из директории /etc/nginx/sites-available в директорию /etc/nginx/sites-enabled, чтобы nginx его обслуживал:

```
sudo ln -s /etc/nginx/sites-available/sampledomain.ru.conf /etc/nginx/sites-enabled/
```

- проверить корректность настроек:

```
sudo nginx -t
```

```
nginx: [warn] "ssl_stapling" ignored, issuer certificate not found
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

Веб-сервер возвращает предупреждение в случае использования самоподписанного сертификата, однако это не влияет на работу.

- если в синтаксисе обнаружены ошибки, необходимо исправить их, затем перезапустить веб-сервер:

```
sudo systemctl restart nginx
```

Генерация отчета по моделям данных и структурам БД Termidesk VDI

В Termidesk VDI реализована возможность генерации отчета по моделям данных и структурам БД с описанием полей таблиц, их значений и межтабличных связей.

Для генерации отчета следует перейти в интерфейс командной строки и выполнить следующее:

- если требуется сгенерировать отчет по модели данных и структуре БД приложения:

```
sudo /opt/termidesk/sbin/termidesk-vdi-manage tdsk_graph_models termidesk > <имя_файла_для_сохранения.html>
```

где:

termidesk - название приложения;

<имя_файла_для_сохранения.html> - имя и формат файла (html) для сохранения отчета.

Для генерации отчета по модели данных и структуре БД нескольких приложений их названия указываются через пробел.

- если требуется сгенерировать отчет по всей модели данных и структуре БД Termidesk VDI:

```
sudo /opt/termidesk/sbin/termidesk-vdi-manage tdsk_graph_models -a -g >
<имя_файла_для_сохранения.html>
```

где:

-a - ключ для генерации отчета, описывающего все доступные модели данных и структуры БД;

-g - ключ группировки таблиц в соответствии с их приложениями;

<имя_файла_для_сохранения.html> - имя и формат файла (html) для сохранения отчета.

Структура файла отчета приведена в таблице (см. таблицу Структура файла отчёта).

Таблица 149. Структура файла отчёта

Параметр	Описание
App	Название приложения, для которого представлена структура модели данных
Model	Идентификатор модели с представлением структуры данных
Abstract Model	Идентификатор модели, для которой представлена структура данных
<Информационная строка>	Строка содержит модель отчета с перечислением полей, либо дополнительную информацию о модели данных
NAME	Столбец содержит имена параметров
VALUE	Столбец содержит тип данных параметров
HELP TEXT	Столбец содержит описание параметров

РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ

Общие сведения о резервном копировании и восстановлении

Поскольку каждая установка компонентов Termidesk VDI может отличаться от других, подробные шаги по резервному копированию и восстановлению и используемые инструменты будут приведены только для некоторых компонентов. Резервное копирование и восстановление может выполняться как средствами и службами ОС, так и специализированными системами. Порядок выполнения и периодичность резервного копирования определяются эксплуатирующей организацией.

Резервному копированию подлежат:

- конфигурационные файлы компонента «Универсальный диспетчер» и административного и/или пользовательского порталов;

- конфигурационные файлы компонента «Шлюз»;
- конфигурационные файлы компонента «Менеджер рабочих мест»;
- конфигурационные файлы компонента «Сервер терминалов Astra Linux»;
- конфигурационные файлы компонента «Сессионный агент»;
- конфигурационные файлы балансировщика нагрузки;
- конфигурационные файлы, использующиеся для режима высокой доступности.

В качестве альтернативного варианта могут резервироваться целиком узлы компонентов, если они установлены на ВМ. Такой подход применяется, например, для резервирования компонента «Виртуальный модуль Termidesk».

Как правило, файлы компонентов «Удаленный помощник», «Клиент» не подлежат резервному копированию, т.к. повторная установка в большинстве случаев будет быстрее.

Действия с БД Termidesk

Резервное копирование БД

Резервное копирование БД, созданной СУБД PostgreSQL можно выполнить утилитой `pg_dump`:

```
pg_dump -d <наименование_БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь> -W
--format=t > <имя_файла_для_сохранения_БД.tar>
```

Где:

`-d <наименование_БД>` - имя БД. При стандартных настройках используется имя `termidesk`;

`-h <IP-адрес_хоста>` - IP-адрес узла, где расположена БД. Если БД устанавливалась локально, нужно указать `localhost`;

`-p <порт>` - порт для подключения к БД. При стандартных настройках используется `5432`;

`-U <пользователь>` - имя пользователя для подключения. При стандартных настройках используется имя `termideskdb`;

`-W` - запрос пароля для подключения к БД. При стандартных настройках при появлении запроса нужно указать `ksedimret`;

`--format=t` - ключ для экспорта БД в формате `tar`;

`<имя_файла_для_сохранения_БД.tar>` - имя и формат файла (tar) для сохранения БД;

Если указанная команда не помогла, то сделать резервную копию вторым способом:

- на узле с СУБД PostgreSQL переключиться на пользователя `postgres`:

```
sudo su postgres
```

- выполнить резервное копирование БД:

```
pg_dump -d <наименование_БД> > <имя_файла_для_сохранения_БД.sql>
```

где:

`-d <наименование_БД>` - имя БД. При стандартных настройках используется имя `termidesk`;

`<имя_файла_для_сохранения_БД.sql>` - имя и формат файла (`sql`) для сохранения БД.

Восстановление БД из резервной копии

Восстановление БД из резервной копии выполняется командой:

```
pg_restore -d <наименование БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь> -W
--format=t <файл_копии_БД.tar>
```

где:

`-d <наименование БД>` - имя БД. При стандартных настройках используется имя `termidesk`;

`-h <IP-адрес_хоста>` - IP-адрес узла, где расположена БД. Если используется локальная БД, нужно указать `localhost`;

`-p <порт>` - порт для подключения к БД. При стандартных настройках используется `5432`;

`-U <пользователь>` - имя пользователя для подключения. При стандартных настройках используется имя `termideskdb`;

`-W` - запрос пароля для подключения к БД. При стандартных настройках при появлении запроса нужно указать `ksedimret`;

`--format=t <файл_копии_БД.tar>` - ключ для восстановления БД из резервной копии в формате `tar`.

Если резервная копия сохранена в файле формата `.sql`, нужно:

- переключиться на пользователя `postgres`:

```
sudo su postgres
```

- восстановить БД из резервной копии:

```
psql -d <наименование_БД> -f <имя_файла_для_сохранения_БД.sql>
```

Действия с брокером сообщений RabbitMQ

Резервное копирование данных брокера сообщений RabbitMQ

Для брокера сообщений RabbitMQ следует:

- остановить службу `rabbitmq-server`:

```
sudo systemctl stop rabbitmq-server
```

- выполнить резервное копирование каталога /etc/rabbitmq/ вместе с его содержимым;
- выполнить резервное копирование каталога данных /var/lib/rabbitmq/mnesia/;
- запустить службу rabbitmq-server:

```
sudo systemctl start rabbitmq-server
```

Восстановление брокера сообщений RabbitMQ из резервной копии

Современные версии RabbitMQ (3.8.0+) поддерживают восстановление из резервной копии тогда, когда они восстанавливаются на узел RabbitMQ с точно таким же именем узла, с которого была создана резервная копия данных.

Для восстановления конфигурации RabbitMQ следует:

- остановить службу rabbitmq-server:

```
sudo systemctl stop rabbitmq-server
```

- восстановить резервные копии каталогов /etc/rabbitmq/ и /var/lib/rabbitmq/mnesia/;
- запустить службу rabbitmq-server:

```
sudo systemctl start rabbitmq-server
```

Действия с компонентом «Универсальный диспетчер»

Резервное копирование данных «Универсального диспетчера»

Для компонента «Универсальный диспетчер» следует выполнить резервное копирование:

- каталога /etc/opt/termidesk-vdi/ вместе с его содержимым;
- конфигурационного файла /etc/apache2/sites-available/termidesk.conf;
- ключей /etc/ssl/certs/ssl-cert-snakeoil.pem и /etc/ssl/private/ssl-cert-snakeoil.key, использующихся для защищенного подключения.

Восстановление «Универсального диспетчера» из резервной копии

Для восстановления конфигурации «Универсального диспетчера» следует:

- восстановить резервную копию каталога /etc/opt/termidesk-vdi/;
- восстановить резервные копии конфигурационного файла /etc/apache2/sites-available/termidesk.conf и ключей /etc/ssl/certs/ssl-cert-snakeoil.pem, /etc/ssl/private/ssl-cert-snakeoil.key;
- перезапустить службу termidesk-vdi:

```
sudo systemctl restart termidesk-vdi
```

- перезапустить веб-сервер:

```
sudo systemctl restart apache2
```

Действия с компонентом «Шлюз» (termidesk-gateway)

Резервное копирование данных «Шлюза»

Для компонента «Шлюз» следует выполнить резервное копирование:

- конфигурационного файла /etc/termidesk/gateway.yaml;
- ключей, использующихся для защищенного соединения, указанных в файле /etc/termidesk/gateway.yaml.

Восстановление «Шлюза» из резервной копии

Для восстановления конфигурации «Шлюза» следует:

- восстановить резервную копию файла /etc/termidesk/gateway.yaml и ключей указанных в этом файле;
- перезапустить службу termidesk-gateway:

```
sudo systemctl restart termidesk-gateway
```

Действия с компонентом «Менеджер рабочих мест»

Резервное копирование данных «Менеджера рабочих мест»

Для компонента «Менеджер рабочих мест» следует выполнить резервное копирование каталога /etc/opt/termidesk-vdi/ вместе с его содержимым.

Восстановление «Менеджера рабочих мест» из резервной копии

Для восстановления конфигурации «Менеджера рабочих мест» следует:

- восстановить резервную копию каталога /etc/opt/termidesk-vdi/;
- перезапустить службы:

```
sudo systemctl restart termidesk-celery-beat termidesk-celery-worker
```

Служба termidesk-taskman исключена из Termidesk VDI, начиная с версии 6.0.

Действия с компонентом «Сессионный агент»

Резервное копирование данных «Сессионного агента»

Для компонента «Сессионный агент» следует выполнить резервное копирование:

- каталога `/etc/opt/termidesk-ssa/` (для ОС Astra Linux Special Edition (Server));
- каталога `%ProgramData%\UVEON\Termidesk Session Agent\` (для ОС Microsoft Windows Server).

Восстановление «Сессионного агента» из резервной копии

Для восстановления конфигурации «Сессионного агента» следует:

- восстановить резервную копию каталога `/etc/opt/termidesk-ssa/` (для ОС Astra Linux Special Edition (Server)) или `%ProgramData%\UVEON\Termidesk Session Agent\` (для ОС Microsoft Windows Server);
- перезапустить службу `TermideskSessionAgentService` через оснастку «Службы» в ОС Microsoft Windows Server или командой в ОС Astra Linux Special Edition (Server):

```
sudo systemctl restart termidesk-session-agent
```

Действия с компонентом «Сервер терминалов Astra Linux»

Резервное копирование данных «Сервера терминалов Astra Linux»

Для компонента «Сервер терминалов Astra Linux» следует выполнить резервное копирование каталога `/etc/stal/` и компонента «Сессионный агент».

Восстановление «Сервера терминалов Astra Linux» из резервной копии

Для восстановления конфигурации «Сервера терминалов Astra Linux» следует:

- восстановить резервную копию каталога `/etc/stal/`;
- восстановить компонент «Сессионный агент»;
- перезапустить службы:

```
sudo systemctl restart termidesk-stal stal-proxy stal-rdpepc
```

Действия с балансировщиком нагрузки

Резервное копирование данных балансировщика нагрузки

Пример приведен для балансировщика nginx.

Для балансировщика нагрузки `nginx` следует выполнить резервное копирование:

- каталога `/etc/nginx/snippets`;
- каталога с ключами и сертификатами `/etc/ssl/`;
- каталога `/etc/nginx/sites-available/`;
- каталога `/etc/nginx/conf.d/`.

Восстановление балансировщика нагрузки из резервной копии

Для восстановления конфигурации балансировщика нагрузки `nginx` следует:

- восстановить резервные копии каталогов `/etc/nginx/snippets`, `/etc/ssl/`, `/etc/nginx/sites-available/`, `/etc/nginx/conf.d/`;
- перезапустить веб-сервер:

```
sudo systemctl restart nginx
```

Действия для режима высокой доступности

Резервное копирование конфигурации режима высокой доступности

Для режима высокой доступности, настраиваемого для отказоустойчивой или распределенной установки Termidesk VDI, следует выполнить резервное копирование каталога `/etc/keepalived/`.

Восстановление конфигурации режима высокой доступности из резервной копии

Для восстановления конфигурации режима высокой доступности следует:

- восстановить из резервной копии каталог `/etc/keepalived/`;
- перезапустить сервис `keeaplived`:

```
sudo systemctl restart keepalived
```

УПРАВЛЕНИЕ ИНФРАСТРУКТУРОЙ TERMIDESK

Общие сведения об инфраструктуре Termidesk

Раздел «Инфраструктура» предназначен для использования в качестве единого центра управления при распределенной установке Termidesk VDI. Он позволяет централизованно управлять компонентами и просматривать их статус на сервере.

Просмотр компонентов и их состояния также доступен в разделе «Обзор», наименования элементов в котором служат активной ссылкой на соответствующий подраздел веб-интерфейса (см. рисунок Отображение компонентов в разделе «Обзор»).

Состояние компонента визуализируется цветовой индикацией:

- - количество узлов, находящихся в статусе «ok» («Активный»), которое вернул запрос `healthcheck`;
- - количество узлов, находящихся в статусе «maintenance» («Техобслуживание»), которое вернул запрос `healthcheck`;
- - количество узлов, находящихся в статусе «error» («Ошибка»), которое вернул запрос `healthcheck`;
- - количество узлов, находящихся в статусе «unknown» («Ограничено»). Статус появляется, если после регистрации компонента еще не было ни одной попытки запроса состояния `healthcheck`.

По умолчанию запрос состояния компонентов производится с интервалом 60 секунд.

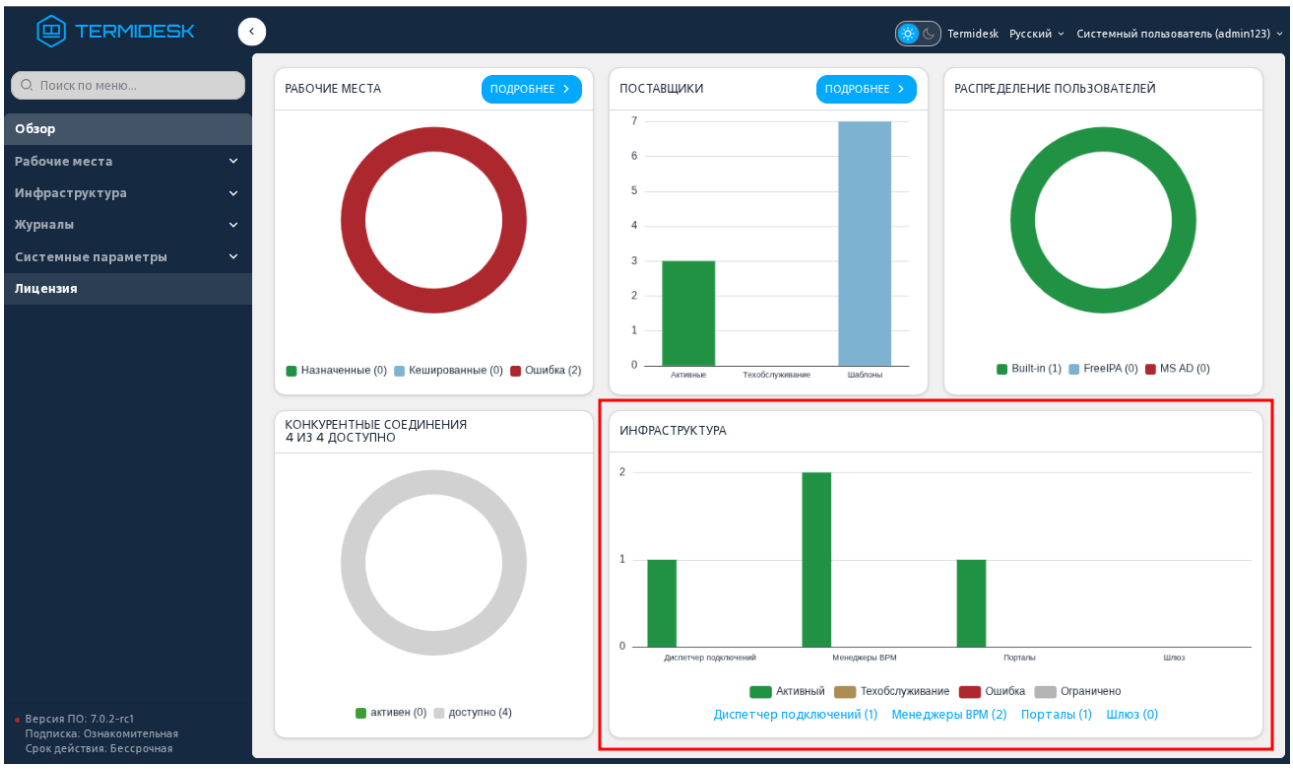


Рисунок 96. Отображение компонентов в разделе «Обзор»

Регистрация компонента Termidesk VDI в системе происходит через подключение к серверу RabbitMQ, передающему информацию об узле компоненту «Менеджер рабочих мест» для обработки и добавления в таблицу раздела «Инфраструктура». Регистрация компонентов происходит при их запуске (или при перезапуске их служб).

Управление списком узлов компонента «Универсальный диспетчер»

Для получения списка зарегистрированных узлов компонента «Универсальный диспетчер» нужно перейти «Инфраструктура - Диспетчеры подключений».

По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Имя». Отображение таблиц будет доступно оператору, если у него есть разрешение «Просмотр объектов инфраструктуры».

Для удаления узла компонента из таблицы следует выбрать нужный объект и нажать экранную кнопку **[Удалить]**. Удаление объекта из таблицы также удалит его из таблицы БД, однако при перезапуске службы компонента он зарегистрируется снова. Удаление объекта из таблицы будет доступно оператору, если у него есть разрешение «Удаление объектов инфраструктуры».

Основные регистрируемые параметры узлов приведены в таблице (см. таблицу Основные параметры списка узлов компонента «Универсальный диспетчер»).

Таблица 150. Основные параметры списка узлов компонента «Универсальный диспетчер»

Параметр	Описание
«Имя»	Наименование объекта и ссылка на метрики узла объекта

Параметр	Описание
«Статус»	Текущее состояние, может принимать значения: • «ok» - объект нормально функционирует; • «failed» - объект функционирует с ошибками; • «unknown» - состояние неизвестно или не поддерживается

«Полное доменное имя»	Полное доменное имя узла объекта.
	
	Необходимо обеспечить корректную передачу полного доменного имени (FQDN) узла в Termidesk VDI. Для этого:
	• убедиться, что на всех узлах инфраструктуры в файле `/etc/hosts` заданы FQDN;
	• обеспечить разрешение имен узлов:
	  убедиться, что в сетевой инфраструктуре развернуты и исправно функционируют службы доменных имен (DNS);
	  убедиться, что задана корректная настройка файла `/etc/resolv.conf` на каждом узле

«IP адрес(а)»	Список IP-адресов на узле объекта
«Изменено кем»	Наименование субъекта, который внес последние изменения
«Сертификат»	Статус сертификата объекта. Может быть: • «Истёк» - срок действия сертификата истек; • «Скоро истекает» - до окончания действия сертификата осталось менее 30 дней; • «В обработке» - любое переходное состояние (например, если ожидается ответ от ЦС); • «Действителен» - отсутствие проблем с сертификатом, сертификат действителен; • «Недействителен» - сертификат не прошел проверку подлинности. Для просмотра сертификата конкретного объекта используется экранная кнопка **[Сертификат]**. Сертификаты считываются из хранилища, используемого фермой Termidesk VDI. Список сертификатов, отображаемый для объекта, приведен в таблице ниже. Просмотр сертификата будет доступен, если: • узлы фермы Termidesk VDI используют способ хранения конфигурации «hvac» (выбирается на этапе установки Termidesk VDI); • у оператора есть разрешение «Просмотр сертификатов». Узлы фермы Termidesk VDI должны использовать единое хранилище конфигурации
«Дата изменения»	Дата внесения последних изменений
«Создано кем»	Наименование субъекта, который создал объект
«Дата создания»	Дата создания записи в таблице об объекте
«UUID ноды»	Системный UUID узла объекта
«Уникальный номер»	Уникальный идентификатор объекта

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы;
- экспорт записей таблицы в `csv`-файл. Можно выгрузить:
  - все записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт всех]**;
  - выбранные записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт выбранных]**.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Для объекта «Универсальный диспетчер» доступен список сертификатов, приведенный в таблице (см. таблицу Список сертификатов «Универсального диспетчера»).

Таблица 151. Список сертификатов «Универсального диспетчера»

Параметр	Описание
«Корневой сертификат БД»	Путь к корневому сертификату mTLS для защищенного подключения к БД
«Сертификат БД»	Путь к клиентскому сертификату mTLS для защищенного подключения к БД
«Закрытый ключ БД»	Путь к закрытому ключу mTLS для защищенного подключения к БД
«Сертификат сервера Удаленного помощника»	Путь к серверному сертификату SSL/TLS для проверки подключения к «Удаленному помощнику»
«Осн. серт. для расшифровки JWT-токена»	Путь к основному сертификату для получения значения JWT-токена «Агрегатора»
«Рез. серт. для расшифровки JWT-токена»	Путь к резервному сертификату для получения значения JWT-токена «Агрегатора»

Управление списком узлов компонента «Менеджер рабочих мест»

Для получения списка зарегистрированных узлов компонента «Менеджер рабочих мест» нужно перейти «Инфраструктура - Менеджеры BPM». По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Имя». Отображение таблиц будет доступно оператору, если у него есть разрешение «Просмотр объектов инфраструктуры».

Службы «Менеджера рабочих мест» регистрируются в «Инфраструктуре» отдельно как `CeleryBeat` и `CeleryWorker` и в интерфейсе отображаются имена этих служб, а не имена узлов (`NODE_NAME`).

Для удаления узла компонента из таблицы следует выбрать нужный объект и нажать экранную кнопку **[Удалить]**. Удаление объекта из таблицы также удалит его из таблицы БД, однако при перезапуске службы компонента он зарегистрируется снова. Удаление объекта из таблицы будет доступно оператору, если у него есть разрешение «Удаление объектов инфраструктуры».

Основные регистрируемые параметры узлов приведены в таблице (см. таблицу Основные параметры списка узлов компонента «Менеджер рабочих мест»).

Таблица 152. Основные параметры списка узлов компонента «Менеджер рабочих мест»

Параметр	Описание
«Имя»	Наименование объекта и ссылка на метрики узла объекта. В интерфейсе отображается имя службы (`CeleryBeat` или `CeleryWorker`), а не `NODE_NAME`
«Статус»	Текущее состояние, может принимать значения: • «ok» - объект нормально функционирует; • «failed» - объект функционирует с ошибками; • «unknown» - состояние неизвестно или не поддерживается
«Роль»	Тип узла, с которым установлен компонент «Менеджер рабочих мест». Может быть: «Taskman»

Параметр	Описание

«Полное доменное имя»	Полное доменное имя узла объекта.
	
	Необходимо обеспечить корректную передачу полного доменного имени (FQDN) узла в Termidesk VDI. Для этого:
	
	• убедиться, что на всех узлах инфраструктуры в файле `/etc/hosts` заданы FQDN;
	• обеспечить разрешение имен узлов:
	  - убедиться, что в сетевой инфраструктуре развернуты и исправно функционируют службы доменных имен (DNS);
	  - убедиться, что задана корректная настройка файла `/etc/resolv.conf` на каждом узле

«IP адрес(а)»	Список IP-адресов на узле объекта
«PID»	Идентификатор процесса объекта
«Изменено кем»	Наименование субъекта, который внес последние изменения
«Сертификат»	Статус сертификата объекта. Может быть: • «Истёк» - срок действия сертификата истек; • «Скоро истекает» - до окончания действия сертификата осталось менее 30 дней; • «В обработке» - любое переходное состояние (например, если ожидается ответ от ЦС); • «Действителен» - отсутствие проблем с сертификатом, сертификат действителен; • «Недействителен» - сертификат не прошел проверку подлинности. Для просмотра сертификата конкретного объекта используется экранная кнопка **[Сертификат]**. Сертификаты считываются из хранилища, используемого фермой Termidesk VDI. Список сертификатов, отображаемый для объекта, приведен в таблице ниже. Просмотр сертификата будет доступен, если: • узлы фермы Termidesk VDI используют способ хранения конфигурации «hvac» (выбирается на этапе установки Termidesk VDI); • у оператора есть разрешение «Просмотр сертификатов». Узлы фермы Termidesk VDI должны использовать единое хранилище конфигурации.
«Дата изменения»	Дата внесения последних изменений
«Создано кем»	Наименование субъекта, который создал объект
«Дата создания»	Дата создания записи в таблице об объекте
«UUID ноды»	Системный UUID узла объекта
«Уникальный номер»	Уникальный идентификатор объекта

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы;
- экспорт записей таблицы в `csv`-файл. Можно выгрузить:
  - все записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт всех]**;
  - выбранные записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт выбранных]**.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Для объекта «Менеджер рабочих мест» доступен список сертификатов, приведенный в таблице (см. таблицу Список сертификатов «Менеджера рабочих мест»).

Таблица 153. Список сертификатов «Менеджера рабочих мест»

Параметр	Описание
«Сертификат Celery Health Check»	Путь к сертификату SSL/TLS для защищенного подключения к API проверки состояния служб «Менеджера рабочих мест»
«Закрытый ключ Celery Health Check»	Путь к закрытому ключу SSL/TLS для защищенного подключения к API проверки состояния служб «Менеджера рабочих мест»

Параметр	Описание
«Закрытый ключ Celery»	Путь к закрытому ключу mTLS для защищенного подключения к RabbitMQ
«Сертификат Celery»	Путь к клиентскому сертификату mTLS для защищенного подключения к RabbitMQ
«Корневой сертификат Celery»	Путь к корневому сертификату mTLS для защищенного подключения к RabbitMQ

Управление списком узлов с ролями «Порталов»

Для получения списка зарегистрированных узлов с ролями «Порталов» нужно перейти «Инфраструктура - Порталы».

По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Имя». Отображение таблиц будет доступно оператору, если у него есть разрешение «Просмотр объектов инфраструктуры».

Доступны следующие действия над списком узлов:

- удаление. Для этого нужно пометить узел и нажать экранную кнопку **[Удалить]**. Удаление объекта из таблицы также удалит его из таблицы БД, однако при перезапуске службы компонента он зарегистрируется снова. Удаление объекта из таблицы будет доступно оператору, если у него есть разрешение «Удаление объектов инфраструктуры»;
- назначение тегов узлу. Для этого нужно пометить узел и нажать экранную кнопку **[Теги]**. Общее описание по применению тегов приведено в подразделе **Общие сведения о тегах**.

Основные регистрируемые параметры узлов приведены в таблице (см. таблицу Основные параметры списка узлов с ролями «Порталов»).

Таблица 154. Основные параметры списка узлов с ролями «Порталов»

Параметр	Описание
«Имя»	Наименование объекта и ссылка на метрики узла объекта
«Роль»	Тип портала, с которым установлен компонент «Универсальный диспетчер». Может быть: «admin» («Портал администратора»), «user» («Портал пользователя»), «universal» («Портал универсальный»)
«Статус»	Текущее состояние, может принимать значения: • «ok» - объект нормально функционирует; • «failed» - объект функционирует с ошибками; • «unknown» - состояние неизвестно или не поддерживается

«Полное доменное имя»	Полное доменное имя узла объекта.
	
	Необходимо обеспечить корректную передачу полного доменного имени (FQDN) узла в Termidesk VDI. Для этого:
	
	• убедиться, что на всех узлах инфраструктуры в файле `/etc/hosts` заданы FQDN;
	• обеспечить разрешение имен узлов:
	  - убедиться, что в сетевой инфраструктуре развернуты и исправно функционируют службы доменных имен (DNS);
	  - убедиться, что задана корректная настройка файла `/etc/resolv.conf` на каждом узле.

Параметр	Описание
«IP адрес(а)»	Список IP-адресов на узле объекта
«PID»	Идентификатор процесса объекта
«Сертификат»	Статус сертификата объекта. Может быть: • «Недействителен» - отображается при наличии проблем с сертификатом; • «Истёк» - отображается при истечении срока действия сертификата; • «Скоро истекает» - отображается, если до окончания действия сертификата осталось менее 30 дней; • «В обработке» - отображается при любом переходном состоянии (например, если ожидается ответ от ЦС); • «Действителен» - отображается при отсутствии проблем с сертификатом. Для просмотра сертификата конкретного объекта используется экранная кнопка **[Сертификат]**. Сертификаты считываются из хранилища, используемого фермой Termidesk VDI. Список сертификатов, отображаемый для объекта, приведен в таблице ниже. Просмотр сертификата будет доступен, если: • узлы фермы Termidesk VDI используют способ хранения конфигурации «hvac» (выбирается на этапе установки Termidesk VDI); • у оператора есть разрешение «Просмотр сертификатов». Узлы фермы Termidesk VDI должны использовать единое хранилище конфигурации
«Изменено кем»	Наименование субъекта, который внес последние изменения
«Дата изменения»	Дата внесения последних изменений
«Создано кем»	Наименование субъекта, который создал объект
«Дата создания»	Дата создания записи в таблице об объекте
«UUID ноды»	Системный UUID узла объекта
«Уникальный номер»	Уникальный идентификатор объекта
«Теги»	Список тегов, назначенных узлу объекта. При выборе тега выполняется переход к разделу «Системные параметры – Управление тегами» со списком объектов, которым назначен данный тег

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы;
- экспорт записей таблицы в `csv`-файл. Можно выгрузить:

все записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт всех]**;

выбранные записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт выбранных]**.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Управление списком узлов компонента «Шлюз»

Для получения списка зарегистрированных узлов компонента «Шлюз» нужно перейти «Инфраструктура - Шлюзы».

По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Имя». Отображение таблиц будет доступно оператору, если у него есть разрешение «Просмотр объектов инфраструктуры».

Для удаления узла компонента из таблицы следует выбрать нужный объект и нажать экранную кнопку **[Удалить]**. Удаление объекта из таблицы также удалит его из таблицы БД, однако при перезапуске службы компонента он зарегистрируется снова. Удаление объекта из таблицы будет доступно оператору, если у него есть разрешение «Удаление объектов инфраструктуры».

Основные регистрируемые параметры узлов приведены в таблице (см. таблицу Основные параметры списка узлов компонента «Шлюз»).

Таблица 155. Основные параметры списка узлов компонента «Шлюз»

Параметр	Описание
«Имя»	Наименование объекта
«Статус»	Текущее состояние, может принимать значения: • «ok» - объект нормально функционирует; • «failed» - объект функционирует с ошибками; • «unknown» - состояние неизвестно или не поддерживается

«Полное доменное имя»	Полное доменное имя узла объекта.
	
	Необходимо обеспечить корректную передачу полного доменного имени (FQDN) узла в Termidesk VDI. Для этого:
	• убедиться, что на всех узлах инфраструктуры в файле `/etc/hosts` заданы FQDN;
	• обеспечить разрешение имен узлов:
	  - убедиться, что в сетевой инфраструктуре развернуты и исправно функционируют службы доменных имен (DNS);
	  - убедиться, что задана корректная настройка файла `/etc/resolv.conf` на каждом узле

«IP адрес(а)»	Список IP-адресов на узле объекта
«Изменено кем»	Наименование субъекта, который внес последние изменения
«Сертификат»	Статус сертификата объекта. Может быть: • «Истёк» - срок действия сертификата истек; • «Скоро истекает» - до окончания действия сертификата осталось менее 30 дней; • «В обработке» - любое переходное состояние (например, если ожидается ответ от ЦС); • «Действителен» - отсутствие проблем с сертификатом, сертификат действителен; • «Недействителен» - сертификат не прошел проверку подлинности. Для просмотра сертификата конкретного объекта используется экранная кнопка **[Сертификат]**. Сертификаты считываются из хранилища, используемого фермой Termidesk VDI. Список сертификатов, отображаемый для объекта, приведен в таблице ниже. Просмотр сертификата будет доступен, если: • узлы фермы Termidesk VDI используют способ хранения конфигурации «hvac» (выбирается на этапе установки Termidesk VDI); • у оператора есть разрешение «Просмотр сертификатов». Узлы фермы Termidesk VDI должны использовать единое хранилище конфигурации.
«Дата изменения»	Дата внесения последних изменений
«Создано кем»	Наименование субъекта, который создал объект
«Дата создания»	Дата создания записи в таблице об объекте
«UUID ноды»	Системный UUID узла объекта

Параметр	Описание
«Уникальный номер»	Уникальный идентификатор объекта

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы;
- экспорт записей таблицы в `csv`-файл. Можно выгрузить:
  - все записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт всех]**;
  - выбранные записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт выбранных]**.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент

под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Для объекта «Шлюз» доступен список сертификатов, приведенный в таблице (см. таблицу

Список сертификатов «Шлюза»).

Таблица 156. Список сертификатов «Шлюза»

Параметр	Описание
«Сертификат шлюза»	Путь к сертификату «Шлюза»
«Закрытый ключ шлюза»	Путь к закрытому ключу «Шлюза»

Управление списком узлов компонента «Ретранслятор»

«Ретранслятор» - узел с установленным компонентом «Ретранслятор» Termidesk VDI, предназначенным для сбора и фильтрации записей журналов, поступающих от компонентов Termidesk VDI, и их перенаправления в централизованное хранилище журналов или БД.

Для установки и настройки компонента «Ретранслятор» следует обратиться к документу СЛЕТ.10001-01 90 05 «Руководство администратора. Настройка компонента «Ретранслятор».

В Termidesk VDI версии 6.1 отправка журналов поддерживается компонентами:

- «Сессионный агент». Требуется дополнительная настройка параметра `SEND_LOGS_TO_REPEATER` в конфигурационном файле компонента `session_agent.ini`;
- «Универсальный диспетчер» («Портал администратора», «Портал пользователя»). Дополнительные настройки для взаимодействия с «Ретранслятором» выполняются в конфигурационном файле `termidesk.conf`.

Для отображения списка «Ретрансляторов» следует перейти «Инфраструктура - Ретрансляторы». По умолчанию записи представлены табличном виде и упорядочены согласно столбцу «Имя». Отображение таблиц будет доступно оператору, если у него есть разрешение «Просмотр объектов инфраструктуры».

Доступность функционала зависит от типа редакции Termidesk VDI.

Над созданными «Ретрансляторами» можно выполнять следующие действия:

- редактировать, для этого следует выбрать нужный объект в таблице, а затем нажать экранную кнопку **[Изменить]**;
- удалить, для этого следует выбрать нужный объект в таблице, а затем нажать экранную кнопку **[Удалить]**. Удаление объекта из таблицы будет доступно оператору, если у него есть разрешение «Удаление объектов инфраструктуры».;
- управлять состоянием «Ретранслятора», для этого следует выбрать нужный объект в таблице, а затем воспользоваться переключателем в столбце «Включен».

Основные параметры списка приведены в таблице (см. таблицу Основные параметры списка «Ретрансляторов»).

Таблица 157. Основные параметры списка «Ретрансляторов»

Параметр	Описание
«Имя»	Наименование объекта
«Статус»	Текущее состояние объекта, может принимать значения: • «ok» - объект нормально функционирует; • «failed» - объект функционирует с ошибками; • «unknown» - состояние неизвестно или не поддерживается

Параметр	Описание
«Включен»	Управление использованием «Ретранслятора». Возможные значения: • «Включен» - «Ретранслятор» используется для сбора журналов; • «Выключен» - «Ретранслятор» не используется для сбора журналов

«Полное доменное имя»	Полное доменное имя узла, на котором функционирует «Ретранслятор»
	
	Необходимо обеспечить корректную передачу полного доменного имени (FQDN) узла в Termidesk VDI. Для этого:
	
	• убедиться, что на всех узлах инфраструктуры в файле `/etc/hosts` заданы FQDN;
	• обеспечить разрешение имен узлов:
	  - убедиться, что в сетевой инфраструктуре развернуты и исправно функционируют службы доменных имен (DNS);
	  - убедиться, что задана корректная настройка файла `/etc/resolv.conf` на каждом узле

«IP-адрес(а)»	Список IP-адресов на узле, на котором функционирует «Ретранслятор»
«Изменено кем»	Наименование субъекта, который внес последние изменения
«Дата изменения»	Дата внесения последних изменений
«Создано кем»	Наименование субъекта, который создал объект
«Дата создания»	Дата создания записи в таблице об объекте
«UUID ноды»	Системный UUID узла, на котором функционирует «Ретранслятор» Параметр имеет постоянное значение: «00000000-0000-0000-0000-000000000000»
«Уникальный номер»	Уникальный идентификатор объекта

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы;
- экспорт записей таблицы в `csv`-файл. Можно выгрузить:
  - все записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт всех]**;
  - выбранные записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт выбранных]**.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться

графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;

- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Для добавления «Ретранслятора» нужно перейти «Инфраструктура - Ретрансляторы» и нажать экранную кнопку **[Создать]**. Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления узла «Ретранслятора»).

Рекомендуется добавлять только один узел «Ретранслятора».

В отличие от компонентов Termidesk VDI, которые регистрируются в разделе «Инфраструктура» автоматически, «Ретранслятор» добавляется вручную.

Таблица 158. Данные для добавления узла «Ретранслятора»

Параметр	Описание
«Имя»	Текстовое наименование «Ретранслятора»
«Адрес»	IP-адрес или FQDN узла «Ретранслятора». Требуется указывать тот IP-адрес или FQDN узла «Ретранслятора» который доступен с любых узлов фермы Termidesk VDI. Значения «localhost» или «127.0.0.1» указывать запрещено
«Порт»	Порт, который будет использоваться при подключении к «Ретранслятору». Значение по умолчанию: «24224»

Параметр	Описание
«Включено»	Управление использованием «Ретранслятора». Возможные значения: • «Да» - использовать «Ретранслятор» для сбора журналов; • «Нет» - не использовать «Ретранслятор» для сбора журналов. Параметр предназначен для прекращения взаимодействия компонентов Termidesk VDI с узлом «Ретранслятора», который по каким-либо причинам выведен из стандартного рабочего состояния

Управление «Хранилищами журналов»

«Хранилище журналов» отображает список подключенных БД, в которые сохраняет события подключенный «Ретранслятор».

> Поскольку предполагается использование одного узла «Ретранслятора» с одной БД, то компоненты Termidesk VDI будут отправлять события на первый полностью работающий «Ретранслятор» и его БД.

Записанные «Ретранслятором» события в БД доступны для просмотра в разделе «Журналы - Журналы фермы».

В отличие от компонентов Termidesk VDI, регистрирующихся в разделе «Инфраструктура» автоматически, «Хранилище журналов» добавляется вручную.

Для отображения списка «Хранилищ журналов» нужно перейти «Инфраструктура - Хранилища журналов». По умолчанию записи представлены в табличном виде и упорядочены согласно столбцу «Название». Отображение таблиц будет доступно оператору, если у него есть разрешение «Просмотр объектов инфраструктуры».

Над созданными «Хранилищами журналов» можно выполнять следующие действия:

- редактировать, для этого следует выбрать нужный объект в таблице, а затем нажать экранную кнопку **[Изменить]**;
- удалить, для этого следует выбрать нужный объект в таблице, а затем нажать экранную кнопку **[Удалить]**. Удаление объекта из таблицы будет доступно оператору, если у него есть разрешение «Удаление объектов инфраструктуры»;
- управлять состоянием «Хранилища журналов», для этого следует выбрать нужный объект в таблице, а затем воспользоваться переключателем в столбце «Использование».

Основные параметры списка приведены в таблице (см. таблицу Основные параметры списка «Хранилищ журналов»).

Таблица 159. Основные параметры списка «Хранилищ журналов»

Параметр	Описание
«Название»	Наименование «Хранилища журналов»
«Использование»	Управление использованием «Хранилища журналов». Возможные значения: • «Включено» - объект используется для сбора журналов; • «Выключено» - объект не используется для сбора журналов

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы;
- экспорт записей таблицы в `csv`-файл. Можно выгрузить:
  - все записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт всех]**;
  - выбранные записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт выбранных]**.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент

под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Для добавления «Хранилища журналов» следует перейти «Инфраструктура - Хранилища журналов» и нажать экранную кнопку **[Создать]**.

Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления «Хранилища журналов»).

Таблица 160. Данные для добавления «Хранилища журналов»

Параметр	Описание
«Имя журнала»	Текстовое наименование «Хранилища журналов»
«Имя БД»	Наименование БД, в которой расположено «Хранилище журналов»
«УЗ БД»	Имя пользователя для подключения к БД «Хранилища журналов». Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Для обеспечения безопасного доступа к «Хранилищу журналов» рекомендуется создать учетные записи БД с нижеперечисленными ролями: • «Администратора» - учетная запись должна обладать правами на создание учетных записей «Ретранслятора» и «Читателя», задание паролей, создание БД для хранения событий; • «Ретранслятора» - учетная запись должна обладать правами на перенаправление событий из журналов компонентов Termidesk VDI в БД «Хранилища журналов» и управление сроком хранения данных в БД; • «Читателя» - учетная запись должна обладать правами на чтение данных из БД. В текущей версии Termidesk VDI для подключения к БД «Хранилища журналов» используется только учетная запись «Администратора»
«Пароль БД»	Пароль для подключения к БД «Хранилища журналов». Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config»
«Адрес БД»	IP-адрес или FQDN узла с установленной БД «Хранилища журналов»
«Порт»	Порт для подключения к БД «Хранилища журналов». Значение по умолчанию: «5432»
«Включено»	Управление использованием «Хранилища журналов». Возможные значения: • «Да» - использовать «Хранилище журналов» для сбора журналов; • «Нет» (по умолчанию) - не использовать «Хранилище журналов» для сбора журналов. Параметр предназначен для прекращения взаимодействия компонентов Termidesk VDI с узлом «Хранилища журналов», который по каким-либо причинам выведен из стандартного рабочего состояния
«Пороговый объём таблицы, ГБ»	Размер (в гигабайтах) таблицы БД, по достижении которого администратору будет отправлено оповещение. Для отправки оповещения должно быть включено уведомление «Уведомление о превышении порогового объёма таблицы журналов фермы» (см. подраздел **Настройка отправки уведомлений о системных событиях**). Значение по умолчанию: «1»
«Срок хранения данных, сут»	Срок (в сутках) хранения журналов в БД. По истечении срока будет запущена процедура управления жизненным циклом журналов (политика data retention в СУБД). Значение по умолчанию: «90»

Параметр	Описание
«Путь к секретам»	Путь к аутентификационным данным учетной записи, расположенным в хранилище. Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/fluent/»

Управление списком узлов компонента «Брокер сообщений»

«Брокер сообщений» - узел с установленным компонентом «Брокер сообщений TermideskMQ», предназначенным для взаимодействие между различными компонентами или приложениями Termidesk VDI, обеспечивая надежную асинхронную передачу данных.

Установка компонента выполняется из пакета `termidesk-vdi` (см. подраздел **Неавтоматизированная комплексная установка Termidesk VDI** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса».).

Для получения списка зарегистрированных узлов нужно перейти «Инфраструктура - Брокеры сообщений». Страница отображает сводную информацию о состоянии узлов TermideskMQ. Данные позволяют оценить загрузку системы по количеству накопленных задач и идентифицировать принадлежность клиента к конкретной ферме Termidesk VDI.

Основные регистрируемые параметры узлов приведены в таблице (см. таблицу Основные параметры списка узлов компонента «Брокер сообщений»).

Таблица 161. Основные параметры списка узлов компонента «Брокер сообщений»

Параметр	Описание
Общие параметры узлов	
«Всего сообщений в очередях кластера»	Суммарное количество всех неподтвержденных и готовых к отправке сообщений, находящихся во всех очередях всех узлов, входящих в состав кластера TermideskMQ. Оценка поведения: • рост значения указывает на накопление задач в брокере. Может свидетельствовать о недостаточной скорости обработки сообщений или о пиковой нагрузке; • нулевое значение указывает, что очереди пусты, брокер простаивает или работает в штатном режиме
«Количество сообщений (для идентификатора) фермы»	Количество сообщений в очередях кластера, отфильтрованных по значению заголовка (или свойства) сообщения, соответствующему идентификатору конкретной фермы Termidesk VDI. Параметр показывает уровень загруженности конкретной логической группы (фермы Termidesk VDI)
«Идентификатор клиента TermideskMQ фермы»	Уникальный идентификатор, который обозначает отдельную очередь в кластере брокера, с которой работают компоненты фермы Termidesk VDI. Этот идентификатор служит для маршрутизации: сообщения с определенной меткой направляются «подписчикам» брокера с этим идентификатором

Параметр	Описание
Индивидуальные параметры узла	

«FQDN»	Полное доменное имя брокера в кластере TermideskMQ.
	
	Необходимо обеспечить корректную передачу полного доменного имени (FQDN) узла в Termidesk VDI. Для этого:
	
	• убедиться, что на всех узлах инфраструктуры в файле `/etc/hosts` заданы FQDN;
	• обеспечить разрешение имен узлов:
	  - убедиться, что в сетевой инфраструктуре развернуты и исправно функционируют службы доменных имен (DNS);
	  - убедиться, что задана корректная настройка файла `/etc/resolv.conf` на каждом узле

«IP адрес»	IP-адрес брокера в кластере TermideskMQ
«Статус»	Текущее состояние, может принимать значения: • «Активен» - объект нормально функционирует; • «Недоступен» - объект не отправил свое состояние: он либо выключен, либо его состояние неизвестно
«Сертификат»	Время действия клиентского сертификата объекта, если используется mTLS. Цветовая индикация: • «Зеленый» - до окончания срока действия сертификата осталось больше 90 дней; • «Желтый» - до окончания срока действия сертификата осталось меньше 90 дней; • «Красный» - до окончания срока действия сертификата осталось 0 дней
«Корневой сертификат»	Время действия корневого сертификата объекта, если используется mTLS. Цветовая индикация аналогичная параметру «Сертификат»

МОНИТОРИНГ И УВЕДОМЛЕНИЯ

Настройка отправки уведомлений о системных событиях

Для настройки отправки уведомлений о системных событиях следует перейти «Системные параметры - Системные настройки», выбрать раздел «Уведомления».

Доступные для редактирования администратору Termidesk VDI параметры перечислены в столбце «Параметр» следующей таблицы (см. таблицу Параметры отправки уведомлений о событиях).

Таблица 162. Параметры отправки уведомлений о событиях

Параметр	Описание
«Вкл/выкл почтовых уведомлений»	Включение или отключение возможности отправки уведомлений о системных событиях по электронной почте

Параметр	Описание
«Хост»	IP-адрес или имя узла сервера исходящей электронной почты. Пример: «smtp.mail.ru»

«Порт»	Номер порта, на котором ведется прослушивание службой сервера электронной почты.
	
	При указании номера порта стоит руководствоваться правилами:
	
	• если используется порт 25, то параметру «Защита подключения» присвоить значение:
	  «Нет защиты» - при использовании незащищенного подключения;
	  «TLS» - при использовании защищенного подключения по протоколу STARTTLS;
	• если используется порт 465, то параметру «Защита подключения» присвоить значение «SSL»;
	• если используется порт 587, то параметру «Защита подключения» присвоить значение «TLS»;
	• если используется порт 2525, то параметру «Защита подключения» присвоить значение «TLS»

«Email отправителя»	Почтовый адрес отправителя сообщений на сервере электронной почты. Формат: `user@domain`. Пример: «user@mail.ru»
«Пользователь»	Идентификатор пользователя сервиса электронной почты
«Пароль»	Последовательность символов для подтверждения полномочий пользователя сервиса электронной почты
«Защита подключения»	Использование защищенного соединения при взаимодействии с сервером электронной почты. После обновления Termidesk VDI до версии 6.1 нужно повторно задать значение параметра. Возможные значения: • «Нет защиты»; • «SSL»; • «TLS»
«Таймаут, с»	Время ожидания (в секундах) ответа от сервера электронной почты. Возможные значения: от 1 до 180. Значение по умолчанию: «30»

Параметр	Описание
«Email получателей (через запятую)»	Перечень адресов электронной почты получателей уведомлений. Формат: `user@domain`. Пример: «user@mail.ru»
«Префикс для темы письма»	Текстовое поле, содержащее информацию для подстановки в тему электронного письма
«Уведомление о смене режима техобслуживания в поставщике ресурсов»	Управление режимом отправки уведомления по электронной почте о системном событии «Смена режима техобслуживания в поставщике ресурсов». Значение по умолчанию: «Нет» (уведомления не отправляются)
«Уведомление о смене режима техобслуживания в фонде рабочих мест»	Управление режимом отправки уведомления по электронной почте о системном событии «Смена режима техобслуживания в фонде рабочих мест». Значение по умолчанию: «Нет» (уведомления не отправляются)
«Уведомление о смене режима техобслуживания для рабочих мест»	Управление режимом отправки уведомления по электронной почте о системном событии «Смена режима техобслуживания для рабочих мест». Значение по умолчанию: «Нет» (уведомления не отправляются)
«Уведомление о возникновении ошибок с рабочими местами»	Управление режимом отправки уведомления по электронной почте о системном событии «Возникновение ошибок внутри фонда рабочих мест». Значение по умолчанию: «Нет» (уведомления не отправляются)
«Уведомление о превышении лицензированного количества подключений»	Управление режимом отправки уведомления по электронной почте о системном событии «Запрос подключения сверх лимита, установленного лицензией». Значение по умолчанию: «Нет» (уведомления не отправляются)
«Уведомление о превышении лицензированного количества пользователей»	Управление режимом отправки уведомления по электронной почте о системном событии «Запрос входа пользователя сверх лимита, установленного лицензией». Значение по умолчанию: «Нет» (уведомления не отправляются)

Параметр	Описание
«Порог для уведомления о превышении количества занятых лицензий, %»	Значение (в процентах) количества занятых лицензий, при достижении которого администратору будет отправлено уведомление о их превышении. Пример: лицензия выписана на 10 подключений, порог уведомления установлен в 50%. В этом случае: • если количество подключений увеличилось до 6 (соответствует 60%), то уведомление отправится; • если количество подключений увеличилось с 6 до 7 (соответствует 70%), то уведомление отправится; • если количество подключений уменьшилось с 7 до 6 (соответствует 60%), то уведомление не отправится; • если количество подключений уменьшилось с 6 до 5 (соответствует 50%), то уведомление не отправится
«Уведомление о превышении максимума индекса нагрузки»	Управление режимом отправки уведомления по электронной почте о системном событии «Превышение максимального индекса нагрузки». Значение по умолчанию: «Нет» (уведомления не отправляются)
«Уведомление о превышении порога индекса нагрузки»	Управление режимом отправки уведомления по электронной почте о системном событии «Превышение порога индекса нагрузки». Значение по умолчанию: «Нет» (уведомления не отправляются)
«Уведомление об истечении срока действия сертификата, сут»	Управление режимом отправки уведомления по электронной почте о системном событии «Истечение срока действия сертификата». Указывается значение (в сутках), определяющее временной промежуток до окончания срока действия сертификата, по достижении которого администратору будет отправлено уведомление. Поддерживается указание специального значения «-1» - отправка уведомления отключена. Значение по умолчанию: «30»
«Уведомление о превышении порогового объёма таблицы журналов фермы»	Управление режимом отправки уведомления по электронной почте о системном событии «Превышение порогового объема таблицы журналов фермы»

Также возможна регистрация и отправка событий, управляемая параметром «Отправлять уведомление при превышении лимита интервала опроса поставщика» в общих системных параметрах:

- о достижении предела свободного места на хранилище поставщика ресурсов;
- о недоступности хранилища поставщика ресурсов;
- о доступности хранилища поставщика ресурсов.

Шаблон для мониторинга Zabbix

Termidesk VDI поддерживает мониторинг состояния компонентов через ПО Zabbix.

Преднастроенные шаблоны для систем мониторинга размещены по ссылке: https://gitflic.ru/project/uveon/termidesk-zabbix.

Получение метрик узлов компонентов

Общие сведения о метриках

В Termidesk VDI реализован механизм API-запросов для получения метрик узлов, на которых установлены компоненты Termidesk VDI, что позволяет использовать полученные метрики во внешних системах мониторинга и непосредственно в Termidesk VDI. Например, метрики узла «Сессионного агента» используются в механизмах балансировки терминальных серверов Метапоставщика.

Для получения метрик узлов компонентов используется библиотека `psutil`, документация которой доступна на сайте: https://psutil.readthedocs.io/en/latest/.

Формат API-запроса получения метрик, а также список возвращаемых метрик приведен в описании REST API по каждому компоненту, поддерживающему эту функциональность, отдельно.

Поддерживается отправка метрик для следующих компонентов:

- «Универсальный диспетчер»;
- «Сессионный агент»;
- «Агент виртуального рабочего места»;
- «Шлюз».

В графическом интерфейсе Termidesk VDI поддерживается просмотр метрик:

- в назначенном фонде РМ;
- сессий;
- индивидуальных РМ;
- терминальных серверов Метапоставщика;
- узлов инфраструктуры.

В Termidesk VDI версии 7.0 просмотр метрик терминальных серверов не поддерживается.

Метрики фонда РМ

Для просмотра метрик из фонда РМ нужно перейти «Рабочие места - Фонды», затем выбрать нужный фонд РМ, в столбце «Название» нажать на наименование РМ. В открывшемся окне перейти во вкладку «Ресурсы».

Основные параметры метрик РМ из фонда РМ приведены в таблице (см. таблицу Основные параметры списка метрик РМ из фонда РМ).

Таблица 163. Основные параметры списка метрик РМ из фонда РМ

Параметр	Описание
«Использование CPU»	Уровень (в процентах) нагрузки на CPU РМ

Параметр	Описание
«Использование диска»	Объем (в процентах) используемого дискового пространства РМ
«Использование памяти»	Объем (в процентах) используемой оперативной памяти РМ
«Время работы»	Время непрерывной работы РМ
«IP-адрес»	IP-адрес РМ
«FQDN»	FQDN РМ
«Статус»	Статус РМ
«Версия агента»	Версия компонента «Агент виртуального рабочего места», установленного в РМ

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Метрики сессий

Просмотр метрик сессий доступен при переходе на страницу «Рабочие места - Сессии».

Для просмотра метрик сессии нужно выбрать значение одного из столбцов: «Пользователь», «IP источника», «Место» или «ID места».

Сведения о метриках выбранного объекта отобразятся в соответствующей вкладке окна «Метрики сессии».

Основные параметры метрик, регистрируемых в окне «Метрики сессии» приведены в таблице (см. таблицу Основные параметры списка метрик сессий).

Таблица 164. Основные параметры списка метрик сессий

Параметр	Описание
Вкладка «Сведения о клиенте»	
«IP-адрес»	IP-адрес пользовательской рабочей станции
«Имя клиента»	Наименование пользовательской рабочей станции
«Платформа клиента»	ОС пользовательской рабочей станции
«Версия клиента»	Версия компонента «Клиент», установленного на пользовательскую рабочую станцию
«Версия вьювера»	Версия ПО Termidesk Viewer, установленного на пользовательскую рабочую станцию
Вкладка «Сведения о входе в сеть»	
«Пользователь»	Имя пользователя, полученное от службы каталогов
«Домен аутентификации»	Наименование домена аутентификации
«GUSID»	Глобальный уникальный сессионный идентификатор
«URSI»	Текущий уникальный идентификатор запуска ресурса в сессии пользователя
«Статус»	Состояние учетной записи пользователя
«Статус сессии»	Состояние сессии пользователя
«Время простоя»	Время, прошедшее с момента последней активности пользователя в сессии
«Длительность сессии»	Время, прошедшее с момента начала пользовательской сессии
«Причина последнего переподключения»	Причина последнего переподключения пользователя к РМ
«Время входа»	Дата и время последнего входа пользователя
«Время изменения статуса»	Дата и время последнего изменения статуса
Вкладка «Детали о ВРМ»	
«Имя рабочего места»	Наименование РМ
«ОС»	ОС РМ
«FQDN»	FQDN РМ
«IP-адрес»	IP-адрес РМ
«Имя фонда»	Наименование фонда РМ
«Имя сервиса»	Наименование фонда РМ
«Опубликованное имя»	Наименование публикации фонда РМ
«Версия агента»	Версия компонента «Агент виртуального рабочего места», установленного в РМ
Вкладка «Ресурсы»	
«Использование CPU»	Уровень нагрузки (в процентах) на CPU РМ
«Время работы»	Время непрерывной работы РМ
«Использование памяти»	Объем (в процентах) используемой оперативной памяти РМ
«Использование диска»	Объем (в процентах) используемого дискового пространства РМ
Вкладка «Политики»	
«Источник»	Тип политики
«Политика»	Наименование политики
«Значение»	Значение политики

Параметр	Описание
«Описание»	Описание политики

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Метрики индивидуальных РМ

Просмотр метрик индивидуальных РМ доступен при переходе на страницу «Рабочие места - Индивидуальные рабочие места» или по ссылке «Рабочие места» из функции «Обзор».

Для просмотра метрик индивидуального РМ нужно выбрать значение одного из столбцов: «ID места», «Название», «IP источника» или «Владелец».

Сведения о метриках выбранного объекта отобразятся в соответствующей вкладке окна «Метрики сессии».

Основные параметры метрик, регистрируемых в окне «Метрики сессии» приведены в таблице (см. таблицу Основные параметры списка метрик индивидуальных РМ).

Таблица 165. Основные параметры списка метрик индивидуальных РМ

Параметр	Описание
Вкладка «Сведения о клиенте»	
«IP-адрес»	IP-адрес пользовательской рабочей станции
«Имя клиента»	Наименование пользовательской рабочей станции
«Платформа клиента»	ОС пользовательской рабочей станции

Параметр	Описание
«Версия клиента»	Версия компонента «Клиент», установленного на пользовательскую рабочую станцию
«Версия вьювера»	Версия ПО Termidesk Viewer, установленного на пользовательскую рабочую станцию
Вкладка «Сведения о входе в сеть»	
«Пользователь»	Имя пользователя, полученное от службы каталогов
«Домен аутентификации»	Наименование домена аутентификации
«GUSID»	Глобальный уникальный сессионный идентификатор
«URSI»	Текущий уникальный идентификатор запуска ресурса в сессии пользователя
«Статус»	Состояние учетной записи пользователя
«Статус сессии»	Состояние сессии пользователя
«Время простоя»	Время, прошедшее с момента последней активности пользователя в сессии
«Длительность сессии»	Время, прошедшее с момента начала пользовательской сессии
«Причина последнего переподключения»	Причина последнего переподключения пользователя к РМ
«Время входа»	Дата и время последнего входа пользователя
«Время изменения статуса»	Дата и время последнего изменения статуса
Вкладка «Детали о ВРМ»	
«Имя рабочего места»	Наименование РМ
«ОС»	ОС РМ
«FQDN»	FQDN РМ
«IP-адрес»	IP-адрес РМ
«Имя фонда»	Наименование фонда РМ
«Имя сервиса»	Наименование фонда РМ
«Опубликованное имя»	Наименование публикации фонда РМ
«Версия агента»	Версия компонента «Агент виртуального рабочего места», установленного в РМ
Вкладка «Ресурсы»	
«Использование CPU»	Уровень нагрузки (в процентах) на CPU РМ
«Время работы»	Время непрерывной работы РМ
«Использование памяти»	Объем (в процентах) используемой оперативной памяти РМ
«Использование диска»	Объем (в процентах) используемого дискового пространства РМ
Вкладка «Политики»	
«Источник»	Тип политики
«Политика»	Наименование политики
«Значение»	Значение политики
«Описание»	Описание политики

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий

список со значениями интервала в минутах, расположенный рядом с указанным элементом;

- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Метрики терминальных серверов

Для просмотра метрик терминальных серверов нужно перейти «Рабочие места - Терминальные серверы», в столбце «Название» нажать на наименование терминального сервера.

Сведения о метриках выбранного объекта отобразятся в окне «Метрики терминального сервера».

Основные параметры метрик терминальных серверов приведены в таблице (см. таблицу Основные параметры списка метрик терминальных серверов).

Таблица 166. Основные параметры списка метрик терминальных серверов

Параметр	Описание
«Использование CPU»	Уровень (в процентах) нагрузки на CPU терминального сервера
«Использование диска»	Объем (в процентах) используемого дискового пространства терминального сервера
«Использование памяти»	Объем (в процентах) используемой оперативной памяти терминального сервера
«Время работы»	Время непрерывной работы терминального сервера
«IP-адрес»	IP-адрес терминального сервера
«FQDN»	FQDN терминального сервера
«Статус»	Статус терминального сервера
«Версия агента»	Версия компонента «Агент виртуального рабочего места», установленного на сервер терминалов

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Метрики узлов инфраструктуры

Для просмотра метрик узлов инфраструктуры нужно перейти:

- «Инфраструктура - Диспетчеры подключений», в столбце «Имя» нажать на наименование узла для просмотра метрик узлов компонента «Универсальный диспетчер»;
- «Инфраструктура - Менеджеры BPM», в столбце «Имя» нажать на наименование узла для просмотра метрик узлов компонента «Менеджер рабочих мест»;
- «Инфраструктура - Порталы», в столбце «Имя» нажать на наименование узла для просмотра метрик узлов с ролями «Порталов».

Сведения о метриках выбранного объекта отобразятся в окне «Метрики узла».

Основные параметры метрик узлов инфраструктуры приведены в таблице (см. таблицу Основные параметры списка метрик узлов инфраструктуры).

Таблица 167. Основные параметры списка метрик узлов инфраструктуры

Параметр	Описание
«Версия компонента»	Версия компонента, установленного на узел
«Версия ОС»	Версия ОС, на которой установлен компонент
«Период в секундах, в течение которого система функционирует без проблем»	Время непрерывной работы узла
«Общая загрузка процессора в процентах»	Уровень (в процентах) нагрузки на CPU узла

Параметр	Описание
«Общая загрузка диска в процентах»	Объем (в процентах) используемого дискового пространства узла
«Общая загрузка виртуальной памяти в процентах»	Объем (в процентах) используемой оперативной памяти узла
«Пользовательские сессии (Портал)»	Количество пользовательских сессий в «Портале пользователя»
«Сессии администраторов (Портал)»	Количество пользовательских сессий в «Портале администратора»
«Сессии РМ (активные)»	Количество активных пользовательских сессий РМ
«Сессии РМ (отключенные)»	Количество отключенных пользовательских сессий РМ
«Сессии RDS/STAL (активные)»	Количество активных пользовательских сессий на серверах терминалов
«Сессии RDS/STAL (отключенные)»	Количество отключенных пользовательских сессий на серверах терминалов
«Всего РМ»	Общее количество РМ
«Ошибка запуска РМ»	Общее количество РМ в статусе «Ошибка»
«Зависшие РМ»	Общее количество зависших РМ
«Незарегистрированные агенты РМ»	Общее количество компонентов «Агент виртуального рабочего места», не зарегистрированных на «Универсальном диспетчере»

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом

для соответствующего столбца.

Отслеживание жизненного цикла сессий и ресурсов пользователей

Начиная с Termidesk VDI версии 5.0 поддерживается возможность отследить действия пользователя (или администратора) по идентификаторам, которыми маркируются все события, относящихся к работе с Termidesk VDI с момента аутентификации и до завершения работы:

- глобальный уникальный сессионный идентификатор (Global Unique Session ID, GUSID, также SUID) - позволяет однозначно сопоставить субъект (пользователя или администратора) и производимые им действия. Присваивается в момент аутентификации в Termidesk VDI;
- уникальный идентификатор запуска ресурса (Unique Resource Start ID, URSI) - позволяет однозначно сопоставить пользователя и конкретный ресурс, который он получает - РМ и/или приложение. Присваивается в момент запуска пользователем ресурса.

Последовательность присвоения и отправки идентификаторов представлена на рисунке (см. рисунок Последовательность присвоения и отправки GUSID и URSI).

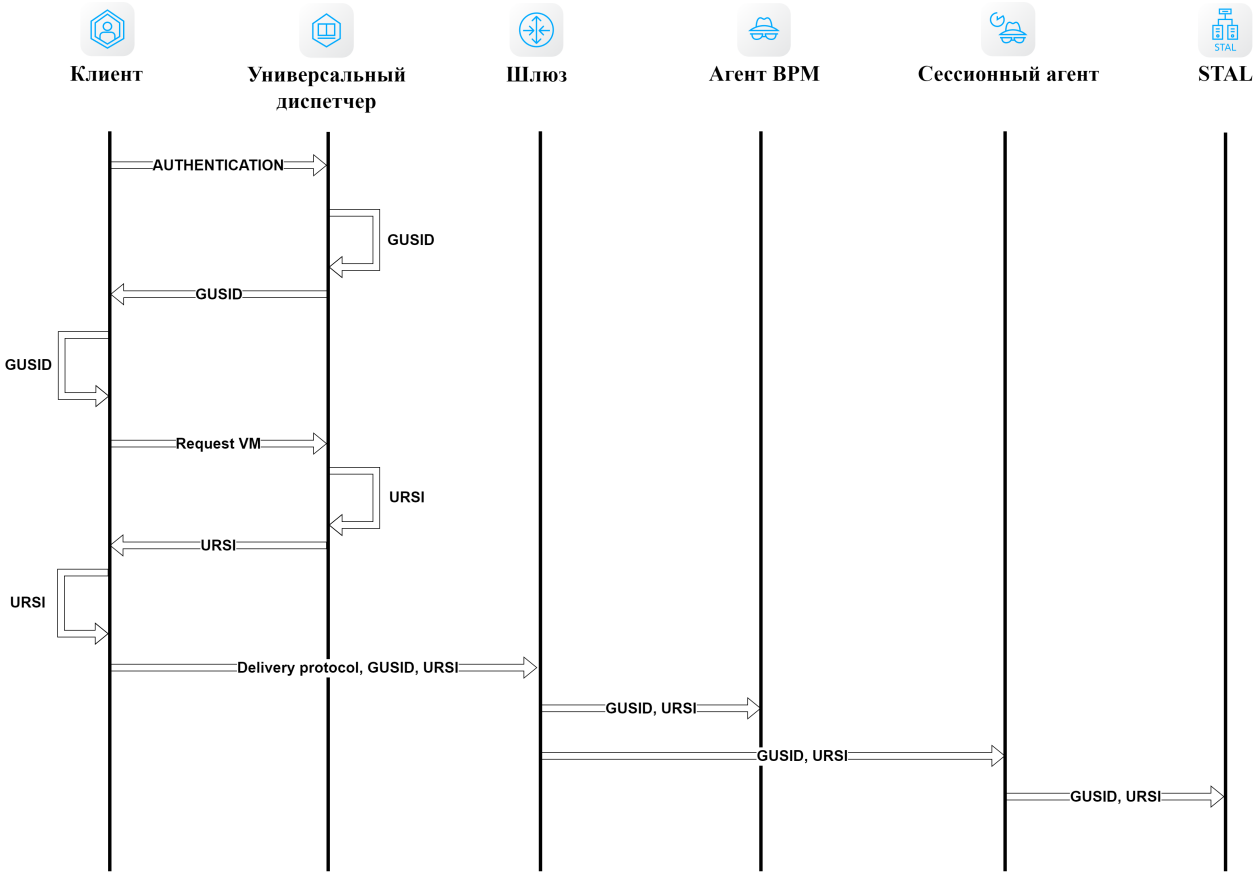


Рисунок 97. Последовательность присвоения и отправки GUSID и URSI

Аннулирование GUSID происходит при:

- завершении сессии по истечении времени, заданного параметром безопасности «Длительность сессии пользователя, с» или «Длительность сессии администратора, с»;
- отключении от «Универсального диспетчера»;
- закрытии компонента «Клиент» пользователем;

- запуске нового экземпляра компонента «Клиент» на той же пользовательской рабочей станции;
- невозможности восстановления подключения после обрыва связи - GUSID и URSI будут считаться недействительными и при следующем подключении к «Универсальному диспетчеру» будут назначены новые идентификаторы.

Аннулирование URSI происходит при:

- закрытии пользователем окна опубликованного приложения или выходе из сеанса РМ (`logoff`);
- отключении от сеанса РМ (`disconnect`);
- закрытии компонента «Клиент» и окна программы доставки РМ (ПО Termidesk Viewer);
- невозможности восстановления подключения после обрыва связи - GUSID и URSI будут считаться недействительными и при следующем подключении пользователя к «Универсальному диспетчеру» будут назначены новые идентификаторы.

GUSID и URSI регистрируются в журналах:

- компонента «Сессионный агент»;
- компонента «Агент виртуального рабочего места».

События, связанные с GUSID и URSI, хранятся в БД. Они доступны для просмотра в журнале на портале Termidesk VDI. Пример сообщения от источника «agent»:

«preConnect. User: u, Protocol: spice, GUSID: 93418bcd-5c95-5f46-ae1b-980a8519ae8f, URSI: 73fe89e3-5fe4-5b02-81a8-06b8e3bac2d1».

Рекомендации по настройке отслеживания состояния компонентов Termidesk VDI

Общие сведения по проверке состояния компонентов

Для отслеживания состояния компонентов Termidesk VDI и обращения к ним для выполнения проверок состояния (health check) используется API-запрос `/api/health`.

Начальная спецификация схемы HealthCheck API в формате OpenAPI соответствует описанию:

```
openapi: 3.0.3
info:
  title: Termidesk VDI health check api schema
  version: 0.1
paths:
  /api/health:
    get:
      responses:
        '200':
          description: Successful Response
          content:
            application/json:
              schema:
                type: object
                properties:
```

```
                  status:
                    type: string
                    enum: [pass, warn, fail]
                    example: fail
                    description: "Состояние компонента"
                  version:
                    type: string
                    example: 3.3
                    description: "Версия компонента"
                  description:
                    type: string
                    example: termidesk-celery
                    description: "Описание компонента"
                  output:
                    type: string
                    example: "django.db.utils.OperationalError: FATAL:  password
authentication failed for user 'termidesk'"
                    description: "Описание ошибки (если есть)"
                required:
                  - status
        '401':
          description: Authorization information is missing or invalid
```

Базовый URL для API: `/api/health`.

Тип контента: `application/json`.

Для каждого компонента Termidesk VDI механизм проверки состояния доступен на порте, заданном в конфигурационном файле:

> Для компонента «Универсальный диспетчер» порт определен настройками веб-сервера (по умолчанию используется 443).

- для компонента «Менеджер рабочих мест» - в файле `/etc/opt/termidesk-vdi/termidesk.conf`, в параметрах `CELERY_BEAT_HEALTH_CHECK_PORT` (по умолчанию используется 8103), `CELERY_WORKER_HEALTH_CHECK_PORT` (по умолчанию используется 8104);
- для компонента «Шлюз» (`termidesk-gateway`) - в файле `/etc/termidesk/gateway.yaml`, в параметре `${mgtServerPort:8102}` (по умолчанию используется 8102).

Для исключения злоупотреблением частыми вызовами API, способными создать нагрузку на систему, доступ к API-запросу контролируется отдельным токеном. Значение токена задается конфигурационным файлом:

- для компонентов «Универсальный диспетчер», «Менеджер рабочих мест» - в файле `/etc/opt/termidesk-vdi/termidesk.conf`, в параметре `HEALTH_CHECK_ACCESS_KEY`;
- для компонента «Шлюз» (`termidesk-gateway`) - в файле `/etc/termidesk/gateway.yaml`, в параметре `token: ${healthcheckaccesskey}`.

Пример `HEALTH_CHECK_ACCESS_KEY`:

```
HEALTH_CHECK_ACCESS_KEY = "9944b09199c62bcf9418ad846dd0e4bbdfc6ee4b"
```

Пример `token: ${healthcheckaccesskey}`:

```
${healthCheckAccessKey:9944b09199c62bcf9418ad846dd0e4bbdfc6ee4b}
```

Процесс автоматического опроса состояния компонентов осуществляется следующим образом:

- компонент Termidesk VDI помещает информацию о себе в очередь брокера сообщений RabbitMQ;
- служба `termidesk-celery-beat` (реализована в компоненте «Менеджер рабочих мест») с периодичностью в 60 секунд забирает из очереди RabbitMQ список всех узлов компонентов Termidesk VDI;
- служба `termidesk-celery-beat` создает задачу на опрос состояния;
- далее служба `termidesk-celery-worker` выполняет задачу на опрос состояния узлов. Полученные результаты служба `termidesk-celery-worker` записывает в БД.

Следующие порты должны быть доступны с узла «Менеджер рабочих мест»:

- 8102 (опрос компонента «Шлюз»);
- 8103 (опрос службы `termidesk-celery-beat`);
- 8104 (опрос службы `termidesk-celery-worker`);
- 443 (опрос компонента «Универсальный диспетчер», а именно - «Портала администратора» и «Портала пользователя»).

В случае если используются несколько узлов «Менеджера рабочих мест», опрос выполняет узел, первый забравший очередь из RabbitMQ. Опрос инициируется по времени:

- служба `termidesk-celery-beat` в 60 секунд подключается к очереди RabbitMQ для получения списка узлов;
- узлы, в свою очередь, раз в 60 секунд помещают информацию о себе в очередь RabbitMQ.

Состояние компонента «Универсальный диспетчер»

При распределенной установке Termidesk VDI экземпляры компонента «Универсальный диспетчер» могут быть установлены на нескольких узлах. Доступ к узлам организуется через балансировщик нагрузки, но для механизма проверок состояния нужно обращаться к каждому узлу напрямую.

Компонент изначально задействован для работы по протоколу HTTP, поэтому механизм проверки состояния реализуется отдельными вызовами REST API.

Пример команды проверки состояния компонента через утилиту `curl`:

```
curl --insecure -v -s -X 'GET' "https://$\{hostname}:443/api/health/check" -H
'accept: application/json' -H "Authorization: Token $\{health_check_access_key}"
```

Ключ `--insecure` используется для отключения проверки валидности сертификатов. Выполнение запроса без использования проверки SSL допустимо только на тестовых стендах. В производственной среде необходимо установить валидные сертификаты.

Состояние компонента «Шлюз» (termidesk-gateway)

При распределенной установке Termidesk VDI экземпляры компонента «Шлюз» (termidesk-gateway) могут быть установлены на нескольких узлах. Доступ к узлам организуется через балансировщик нагрузки, но для механизма проверок состояния нужно обращаться к каждому узлу напрямую.

Для исключения злоупотреблением частыми вызовами API, способными создать нагрузку на систему, доступ к API-запросу компонента «Шлюз» termidesk-gateway контролируется отдельным токеном. Значение токена задается при запуске службы «Шлюза» в параметре token: ${healthcheckaccesskey}.

Пример команды проверки состояния компонента через утилиту curl для компонента «Шлюз» termidesk-gateway (предполагается, что «Шлюз» настроен для работы по защищенному соединению):

```
curl --insecure -v -s -X 'GET' "https://$\{hostname}:8102/api/health" -H 'accept:
application/json' -H "Authorization: Token $\{healthcheckaccesskey}"
```

Состояние компонента «Менеджер рабочих мест»

При распределенной установке Termidesk VDI экземпляры компонента «Менеджер рабочих мест» могут быть установлены на нескольких узлах.

Для использования механизма проверки состояния компонента необходимо в конфигурационном файле /etc/opt/termidesk-vdi/termidesk.conf раскомментировать строки параметров:

- для непосредственно компонента «Менеджер рабочих мест», а именно службы termidesk-celery-beat: CELERY_BEAT_CHECK_IP, CELERY_BEAT_HEALTH_CHECK_PORT, HEALTH_CHECK_CERT, HEALTH_CHECK_KEY. Для параметров HEALTH_CHECK_CERT, HEALTH_CHECK_KEY нужно указать путь к сертификату и ключу, используемых для защищенного подключения, и выполнить перезапуск служб Termidesk VDI;
- для непосредственно компонента «Менеджер рабочих мест», а именно службы termidesk-celery-worker: CELERY_WORKER_CHECK_IP, CELERY_WORKER_HEALTH_CHECK_PORT, HEALTH_CHECK_CERT, HEALTH_CHECK_KEY. Для параметров HEALTH_CHECK_CERT, HEALTH_CHECK_KEY нужно указать путь к сертификату и ключу, используемых для защищенного подключения, и выполнить перезапуск служб Termidesk VDI.

Пример задания значений:

```
CELERY_BEAT_HEALTH_CHECK_PORT=8103
CELERY_BEAT_HEALTH_CHECK_IP='0.0.0.0'
CELERY_WORKER_HEALTH_CHECK_PORT=8104
CELERY_WORKER_HEALTH_CHECK_IP='0.0.0.0'
HEALTH_CHECK_CERT=/etc/opt/termidesk-vdi/healthcheck.pem
HEALTH_CHECK_KEY=/etc/opt/termidesk-vdi/healthcheck-decrypted.key
```

Пример команды проверки состояния компонента «Менеджер рабочих мест» через утилиту curl (предполагается, что «Менеджер рабочих мест» настроен для работы по защищенному соединению):

```
curl --insecure -v -s -X 'GET' "$\{hostname}:8103/api/health/check" -H 'accept:
```

```
application/json' -H "Authorization: Token $\{health_check_access_key}"
```

СИСТЕМА АУДИТА

Системные параметры аудита

Для конфигурации системных параметров аудита следует перейти «Системные параметры - Системные настройки», выбрать раздел «Аудит».

Доступные для редактирования администратору Termidesk VDI параметры перечислены в столбце «Параметр» следующей таблицы (см. таблицу Системные параметры аудита).

События аудита, регистрируемые Termidesk VDI, приведены в подразделе **Типы и шаблоны регистрируемых событий аудита**.

Таблица 168. Системные параметры аудита

Параметр	Описание
«Использовать "строгий" режим аудита»	Управление использованием «строгого» режима аудита. Этот режим аудита запрещает внесение изменений в часть настроек при недоступности БД Termidesk VDI (таблицы `termidesk_audit_event_log_v2`). Значение по умолчанию: «Нет»
«Использовать формат CEF»	Управление использованием формата CEF для записи событий аудита. События аудита в этом формате: • записываются в таблицу БД `termidesk_audit_event_log_v2`, если параметр «Сохранение в БД» активирован; • записываются в локальный файл журнала, если параметр «Сохранение в файл» активирован. Потребуется выполнить дополнительную настройку (см. подраздел **Формат CEF**); • отправляются на отдельный syslog-сервер, если параметр «Отправка в Syslog» активирован и заданы параметры syslog-сервера. Значение по умолчанию: «Нет»
«Сохранение в БД»	Выбор сохранения событий аудита в БД
«Сохранение в файл журнала»	Выбор сохранения событий аудита в отдельный файл журнала `/var/log/termidesk/audit.log`. Значение по умолчанию: «Нет»
«Время хранения записи в БД, сут»	Время хранения (в сутках) записей событий аудита в БД. Удаление устаревших записей аудита выполняется периодической задачей каждые 24 часа. Значение по умолчанию: «7»
«Максимум удаляемых событий»	Максимальное количество удаляемых событий в журнале аудита. Значение по умолчанию: «1000»

Параметр	Описание
«Количество архивных файлов (7-30)»	Максимальное количество архивных файлов журнала событий аудита, по достижении которого начинается перезапись. Возможные значения: от 7 до 30. Значение по умолчанию: «7»
«Отправка в Syslog»	Направление логирования на отдельный syslog-сервер. Значение по умолчанию: «Нет»
«Хост»	IP-адрес или имя узла, на котором развёрнута служба syslog-сервера. Значение по умолчанию: «localhost»
«Протокол»	Выбор протокола работы для службы syslog-сервера. Доступные значения: «UDP», «TCP», «TLS». При использовании протокола «TLS» необходимо установить на «Универсальный диспетчер» Termidesk VDI корневой сертификат ЦС, использующийся в syslog-сервере, согласно подразделу **Установка корневого сертификата центра сертификации**. Значение по умолчанию: «UDP»
«Порт»	Порт, на котором находится служба syslog-сервера. Значение по умолчанию: «514»
«Категория сообщения»	Выбор категории сообщений syslog, которые будут записываться в журнал аудита. Параметр не влияет на состав регистрируемых событий и не учитывается при записи в файл журнала. Значение по умолчанию: «local7»
«Интервал удаления устаревших записей аудита, с»	Периодичность (в секундах) удаления устаревших записей событий аудита в БД. Удаление записей выполняется после истечения срока хранения, заданного в параметре «Время хранения записи в БД, сут». Значение по умолчанию: «86400»

Описание шаблонов событий аудита

Типы данных регистрируемой информации событий аудита

При фиксации событий аудита используется ряд типов данных регистрируемой информации, состав которых может отличаться для разных событий (см. таблицу Типы данных регистрируемой информации).

Таблица 169. Типы данных регистрируемой информации

Тип данных	Описание
Дата/время	Дата и время указываются в формате: `DD.MM.YYYY, hh:mm:ss`, где: `DD.MM.YYYY` обозначает «день» - «месяц» - «год»; `hh:mm:ss` обозначает элементы времени «час» - «минута» - «секунда»; «`.`» и «`:`» используются как разделители в обозначениях даты и времени дня соответственно

Тип данных	Описание
Имя/логин	Идентификационные данные субъекта, совершающего доступ к объекту
Наименование параметра/секции/политики	Указывает объект, над которым производится действие
Значение	Указывается значение, которое принимал или принял объект после выполнения над ним операции
Тип объекта/сущности	Указывает тип объекта, над которым производится действие
Действие	Название операции, которую совершил субъект над объектом
Результат	Результат выполнения действия
Уровень важности	Показатель критичности события
Идентификатор	Указывают уникальную для соответствующего объекта последовательность чисел для его однозначной идентификации
IP-адрес	32-битовое число. Формой записи IP-адреса является запись в виде четырех десятичных чисел значением от 0 до 255, разделенных точками (например, 192.0.2.1)

Типы и шаблоны регистрируемых событий аудита

Список регистрируемых событий и шаблоны к ним приведены в таблице (см. таблицу Список типов и шаблонов регистрируемых событий аудита).

Формат записи событий аудита приведен в подразделе **Форматы регистрируемых событий аудита и их примеры**. Текст регистрируемого события зависит от выбранного формата.

Для запросов, выполняемых без аутентификации, указывается пользователь `AnonymousUser(AnonymousAuth)` (см. строку «Действия пользователя с API»). Включение записи таких событий управляется параметром `INTERNAL_AUDIT` в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf`.

Таблица 170. Список типов и шаблонов регистрируемых событий аудита

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Базовый класс событий		

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Изменение объектов пользователями base.InformationEvent	Регистрируется: • наименование домена аутентификации (user_auth); • имя пользователя (user_name); • тип учетной записи пользователя (user_type); • выполненное действие (action); • имя объекта, над которым произошло действие (obj_name); • тип объекта, над которым произошло действие (obj_type); • внутреннее наименование причины изменения (reason); • результат выполнения действия (result); • измененные данные (updated_data)	«[user_type] [user_name] из домена [user_auth] выполнил операцию [action] над объектом [obj_name] ([obj_type]) с помощью [reason]. Результат - [result]. Измененные данные: [updated_data]»
События, связанные с командной строкой		
Изменение системных параметров «Универсального диспетчера» через командную строку cli.SystemConfigChanged	Регистрируется: • имя пользователя (username); • название изменяемого параметра; (parameter_key); • новое значение параметра (parameter_value)	«Пользователь [username] изменил параметр системы [parameter_key]=[parameter_value] »
CRUD-операции с объектами через командную строку cli.EntityAction	Регистрируется: • имя системного пользователя, запустившего команду (username); • тип сущности (entity); • уникальный идентификатор (uuid); • тип объекта (subtype); • название объекта (name); • действие над объектом (action)	«Пользователь [username] выполнил операцию [action] для объекта [entity]([uuid]) [subtype] [name]»
Вход пользователя в систему через командную строку cli.UserLogin	Регистрируется: • наименование домена аутентификации (authenticator); • имя пользователя (username); • тип портала (portal); • идентификатор портала (portal_uuid)	«Пользователь [username] ([authenticator]) вошел в систему через [portal] ([portal_uuid])»

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Выход пользователя из системы через командную строку cli.UserLogout	Регистрируется: • наименование домена аутентификации (authenticator); • имя пользователя (username); • тип портала (portal); • идентификатор портала (portal_uuid)	«Пользователь [username] ([authenticator]) вышел из системы через [portal] ([portal_uuid])»
События, связанные с политиками		
Изменение глобальных политик policies.GlobalPolicyChanged	Регистрируется: • имя пользователя (username); • название домена аутентификации пользователя (authenticator_name); • тип учетной записи пользователя (user_type); • название политики (policy_name); • новое значение в дружественном к пользователю описании (value); • новое значение в оригинальном формате (value_raw)	«[user_type] [username] ([authenticator_name]) изменил значение глобальной политики [policy_name] на [value] ([value_raw])»
Изменение политик РМ policies.DeployedServicePolicyChanged	Регистрируется: • имя пользователя (username); • название домена аутентификации пользователя (authenticator_name); • название политики (policy_name); • название фонда РМ (deployed_service_name); • новое значение в дружественном к пользователю описании (value); • идентификатор домена аутентификации пользователя (authenticator_uuid); • идентификатор фонда РМ (deployed_service_uuid); • новое значение в оригинальном формате (value_raw)	«Пользователь [username] ([authenticator_name]) изменил значение политики [policy_name] для фонда [deployed_service_name] [value] на [value_raw]»

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Сброс политики РМ policies.DeployedServicePolicyDeleted	Регистрируется: • имя пользователя (username); • название домена аутентификации пользователя (authenticator_name); • название политики (policy_name); • название фонда РМ (deployed_service_name); • идентификатор домена аутентификации пользователя (authenticator_uuid); • идентификатор фонда РМ (deployed_service_uuid)	«Пользователь [username] ([authenticator_name]) сбросил значение политики [policy_name] для фонда [deployed_service_name]»
Сброс глобальных политик policies.GlobalPolicyDeleted	Регистрируется: • имя пользователя (username); • название домена аутентификации пользователя (authenticator_name); • тип учетной записи пользователя (user_type); • название политики (policy_name); • идентификатор домена аутентификации пользователя (authenticator_uuid)	«[user_type] [username] ([authenticator_name]) сбросил значение глобальной политики [policy_name]»
Изменение политик policies.SomeObjectPolicyChanged	Регистрируется: • имя пользователя (username); • название домена аутентификации пользователя (authenticator_name); • тип учетной записи пользователя (user_type); • название политики (policy_name); • тип сущности (instance_type); • имя сущности (instance_name); • новое значение в дружественном к пользователю описании (value); • новое значение в оригинальном формате (value_raw)	«[user_type] [username] ([authenticator_name]) изменил значение политики [policy_name] для [instance_type] [instance_name] на [value] ([value_raw])»

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Сброс политик policies.SomeObjectPolicyDeleted	Регистрируется: • имя пользователя (username); • название домена аутентификации пользователя (authenticator_name); • тип учетной записи пользователя (user_type); • название политики (policy_name); • тип сущности (instance_type); • имя сущности (instance_name)	«[user_type] [username] ([authenticator_name]) сбросил значение политики [policy_name] для [instance_type] [instance_name]»
Изменение политик фонда policies.ServicePoolPolicyChanged	Регистрируется: • имя пользователя (username); • название домена аутентификации пользователя (authenticator_name); • тип учетной записи пользователя (user_type); • название политики (policy_name); • тип сущности (instance_type); • имя сущности (instance_name); • новое значение в дружественном к пользователю описании (value); • новое значение в оригинальном формате (value_raw)	«[user_type] [username] ([authenticator_name]) изменил значение политики [policy_name] для [instance_type] [instance_name] на [value] ([value_raw])»
Сброс политик фонда policies.ServicePoolPolicyDeleted	Регистрируется: • имя пользователя (username); • название домена аутентификации пользователя (authenticator_name); • тип учетной записи пользователя (user_type); • название политики (policy_name); • тип сущности (instance_type); • имя сущности (instance_name)	«[user_type] [username] ([authenticator_name]) сбросил значение политики [policy_name] для [instance_type] [instance_name]»

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Изменение политик сети policies.NetworkPolicyChanged	Регистрируется: • имя пользователя (username); • название домена аутентификации пользователя (authenticator_name); • тип учетной записи пользователя (user_type); • название политики (policy_name); • тип сущности (instance_type); • имя сущности (instance_name); • новое значение в дружественном к пользователю описании (value); • новое значение в оригинальном формате (value_raw)	«[user_type] [username] ([authenticator_name]) изменил значение политики [policy_name] для [instance_type] [instance_name] на [value] ([value_raw])»
Сброс политик сети policies.NetworkPolicyDeleted	Регистрируется: • имя пользователя (username); • название домена аутентификации пользователя (authenticator_name); • тип учетной записи пользователя (user_type); • название политики (policy_name); • тип сущности (instance_type); • имя сущности (instance_name)	«[user_type] [username] ([authenticator_name]) сбросил значение политики [policy_name] для [instance_type] [instance_name]»

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Изменение политик группы пользователей policies.AuthGroupPolicyChanged	Регистрируется: • имя пользователя (username); • название домена аутентификации пользователя (authenticator_name); • тип учетной записи пользователя (user_type); • название политики (policy_name); • тип сущности (instance_type); • имя сущности (instance_name); • новое значение в дружественном к пользователю описании (value); • новое значение в оригинальном формате (value_raw)	«[user_type] [username] ([authenticator_name]) изменил значение политики [policy_name] для [instance_type] [instance_name] домена [authenticator_name] на [value] ([value_raw])»
Сброс политик группы пользователей policies.AuthGroupPolicyDeleted	Регистрируется: • имя пользователя (username); • название домена аутентификации пользователя (authenticator_name); • тип учетной записи пользователя (user_type); • название политики (policy_name); • тип сущности (instance_type); • имя сущности (instance_name)	«[user_type] [username] ([authenticator_name]) сбросил значение политики [policy_name] для [instance_type] [instance_name] домена [authenticator_name] на [value] ([value_raw])»
События, связанные с пользователем		
Подключение пользователя к РМ workplace.UserConnected	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • имя фонда РМ (workplace); • имя выданной ВМ (vm_name); • IP-адрес выданной ВМ (vm_ip); • протокол доставки (transport)	«Подключение к рабочему месту [vm_name]([vm_ip]) пула служб [workplace] пользователя [username]([authenticator]) было выполнено с использованием протокола [transport]»

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Отключение пользователя от РМ workplace.UserDisconnected	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • имя фонда РМ (workplace); • имя выданной ВМ (vm_name); • IP-адрес выданной ВМ (vm_ip); • протокол доставки (transport)	«Подключение к рабочему месту [vm_name]([vm_ip]) пула служб [workplace] пользователя [username]([authenticator]) через протокол [transport] разорвано»
Вход пользователя в ОС РМ workplace.UserLogin	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • имя пользователя гостевой ОС (guest_os_username); • IP-адрес, с которого был сделан запрос (ip); • имя фонда РМ (workplace); • имя выданной ВМ (vm_name); • IP-адрес выданной ВМ (vm_ip)	«Пользователь [username] ([authenticator]) вошел в ОС РМ [vm_name]([vm_ip]) фонда [workplace] как пользователь [guest_os_username] с IP-адреса [ip]»
Выход пользователя из ОС ВМ workplace.UserLogout	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • имя пользователя гостевой ОС (guest_os_username); • IP-адрес, с которого был сделан запрос (ip); • имя фонда РМ (workplace); • имя выданной ВМ (vm_name); • IP-адрес выданной ВМ (vm_ip)	«Пользователь [username] ([authenticator]) вышел из гостевой ОС РМ [vm_name]([vm_ip]) фонда [workplace] как пользователь [guest_os_username] с IP-адреса [ip]»

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Блокировка РМ workplace.UserLock	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • имя пользователя гостевой ОС (guest_os_username); • IP-адрес, с которого был сделан запрос (ip); • имя фонда РМ (workplace); • имя выданной ВМ (vm_name); • IP-адрес выданной ВМ (vm_ip)	«Пользователь [username] ([authenticator]) заблокировал гостевую ОС РМ [vm_name]([vm_ip]) фонда [workplace] как пользователь [guest_os_username] с IP-адреса [ip]»
Разблокировка РМ workplace.UserUnlock	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • имя пользователя гостевой ОС (guest_os_username); • IP-адрес, с которого был сделан запрос (ip); • имя фонда РМ (workplace); • имя выданной ВМ (vm_name); • IP-адрес выданной ВМ (vm_ip)	«Пользователь [username] ([authenticator]) разблокировал гостевую ОС РМ [vm_name]([vm_ip]) фонда [workplace] как пользователь [guest_os_username] с IP-адреса [ip]»
Пользователь неактивен workplace.UserIdle	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • имя пользователя гостевой ОС (guest_os_username); • IP-адрес, с которого был сделан запрос (ip); • имя фонда РМ (workplace); • имя выданной ВМ (vm_name); • IP-адрес выданной ВМ (vm_ip)	«Пользователь [username] ([authenticator]) не активен в гостевой ОС РМ [vm_name]([vm_ip]) фонда [workplace] как пользователь [guest_os_username] с IP-адреса [ip]»

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Пользователь активен workplace.UserActive	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • имя пользователя гостевой ОС (guest_os_username); • IP-адрес, с которого был сделан запрос (ip); • имя фонда РМ (workplace); • имя выданной ВМ (vm_name); • IP-адрес выданной ВМ (vm_ip)	«Пользователь [username] ([authenticator]) снова активен в гостевой ОС РМ [vm_name]([vm_ip]) фонда [workplace] как пользователь [guest_os_username] с IP-адреса [ip]»
Подключение пользователя к РМ и начало работы user.WorkplaceConnectionRequest	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • IP-адрес, с которого был сделан запрос (ip); • название фонда РМ (workplace); • имя выданной ВМ (vm_name); • название протокола доставки (transport)	«Пользователь [username] ([authenticator]) подключился к РМ [vm_name] фонда [workplace] по протоколу [transport] с IP-адреса [ip]»
Отправка сообщения в РМ user.WorkplaceMessageSent	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • тип учетной записи пользователя (user_type); • название фонда РМ (deployed_service_name); • название РМ (user_service_name); • уровень сообщения (msg_level); • текст сообщения (msg_text)	«[user_type] [username] ([authenticator]) отправил сообщение [msg_text] уровня [msg_level] на РМ [user_service_name] фонда [deployed_service_name]»
Назначение пользователя на РМ workplace.UserAssigned	Регистрируется: • имя пользователя (username); • тип учетной записи пользователя (user_type); • назначенный пользователь (assigned_to); • кем назначен пользователь (assigned_by)	«[user_type] [assigned_by] назначил рабочее место [assigned_to] пользователю [username]»

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Действие с учетными записями на сервере каталогов tasks.AudiDeregistrationAction	Регистрируется: • имя учетной записи (comp_name); • действие (action_deregistration)	«Выполнено действие [action_deregistration] с учётной записью компьютера [comp_name] на сервере каталогов»
Создание пользователя при логине authenticators.user.create	Регистрируется: • имя пользователя (created_user)	«При логине был создан пользователь [created_user]»
Изменение учетной записи пользователя домена аутентификации authenticators.user.updated	Регистрируется: • название домена аутентификации пользователя, который произвел изменения (authenticator); • имя пользователя, который произвел изменения (username); • тип учетной записи пользователя, который произвел изменения (user_type); • имя пользователя, над которым произвели изменения (modified_user_name); • идентификатор пользователя, над которым произвели изменения (modified_user_uuid); • название домена аутентификации измененного пользователя (auth_domain_name); • идентификатор домена аутентификации измененного пользователя (auth_domain_uuid); • IP-адрес, с которого произвели изменения (ip); • перечень изменений (changes)	«[user_type] [username] ([authenticator]) изменил учетную запись [modified_user_name] ([modified_user_uuid]) в домене аутентификации [auth_domain_name] ([auth_domain_uuid]) с IP-адреса [ip]. Изменения: [changes]»
События, связанные с веб-интерфейсом		
Неудачная попытка регистрации пользователя web.UserLoginForbidden	Регистрируется: • API метод (handler_path); • ошибка (error); • IP-адрес, с которого был сделан запрос (ip)	«Выполнена неудачная попытка регистрации пользователя api - [handler_path] ошибка - [error] ip - [ip]»

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Вход пользователя в систему через веб-интерфейс web.UserLogin	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • тип учетной записи пользователя (user_type); • IP-адрес, с которого был сделан запрос (ip); • тип портала (portal); • идентификатор портала (portal_uuid)	«[user_type] [username] ([authenticator]) вошел в систему с ip-адреса [ip] через [portal]([portal_uuid])»
Выход пользователя из веб-интерфейса web.UserLogout	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • тип учетной записи пользователя (user_type); • IP-адрес, с которого был сделан запрос (ip); • тип портала (portal); • идентификатор портала (portal_uuid)	«[user_type] [username] ([authenticator]) вышел из системы (ip-адрес [ip]) через [portal]([portal_uuid])»
Изменение системных параметров «Универсального диспетчера» web.SystemConfigChanged	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • IP-адрес, с которого был сделан запрос (ip); • старое значение параметра (old_value); • новое значение параметра (new_value); • имя параметра (name); • ключ параметра (key)	«[user_type] [username] ([authenticator]) изменил системный параметр [name] ([key]), старое значение - [old_value], новое значение - [new_value] (IP-адрес [ip])»

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
CRUD операции с объектами через REST API web.EntityAction	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • тип учетной записи пользователя (user_type); • IP-адрес, с которого был сделан запрос (ip); • тип сущности (entity); • идентификатор (uuid); • тип объекта (subtype); • название объекта (name); • действие над объектом (action)	«[user_type] [username] ([authenticator]) выполнил операцию [action] для объекта [entity] ([uuid]) [subtype] [name] (ip-адрес [ip])»
Загрузка файла лицензии через REST API web.LicenseUpdated	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • тип учетной записи пользователя (user_type); • IP-адрес, с которого был сделан запрос (ip); • имя файла лицензии (license_file_name)	«[user_type] [username] ([authenticator]) загрузил новый файл лицензии [license_file_name] с ip-адреса [ip]»
Удаление файла лицензии через REST API web.LicenseRemoved	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • тип учетной записи пользователя (user_type); • IP-адрес, с которого был сделан запрос (ip)	«[user_type] [username] ([authenticator]) удалил текущую лицензию с ip-адреса с ip-адреса [ip]»
Прекращение сессии пользователя по команде с сервера web.LogoffUserservice	Регистрируется: • имя пользователя (user); • тип учетной записи пользователя (user_type); • данные гостевой ВМ, сессию которой прекратили (userservice)	«[user_type] [user] подал запрос на прекращение сессии [userservice]»

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Сброс сессии пользователя по команде с сервера web.DisconnectUserservice	Регистрируется: • имя пользователя (user); • тип учетной записи пользователя (user_type); • данные гостевой ВМ, сессию которой прекратили (userservice)	«[user_type] [user] подал запрос на сброс сессии [userservice]»
Попытка повышения прав web.AdminAssigned	Регистрируется: • имя пользователя (assigned_to); • тип учетной записи пользователя (user_type); • пользователь, которому назначаются права (user1); • название домена аутентификации пользователя (authenticator)	«[user_type] [user] попытался установить тип учетной записи Администратор для пользователя [assigned_to] в домене аутентификации [authenticator]»
Пользователь обновил данные сущности web.EntityActionUpdate	Регистрируется: • имя пользователя (user); • название домена аутентификации пользователя (authenticator); • тип учетной записи пользователя (user_type); • обновленные данные (data); • объект (entity); • идентификатор объекта (uuid); • имя объекта (name); • IP-адрес, с которого был сделан запрос (ip)	«[user_type] [username] ([authenticator]) изменил свойства объекта [entity] [name] ([uuid]) - [data] (ip-адрес [ip])»

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Изменение правил балансировки web.LoadRules	Регистрируется: • имя пользователя (user); • название домена аутентификации пользователя (authenticator); • тип учетной записи пользователя (user_type); • правило (field); • объект (entity); • идентификатор объекта (uuid); • тип объекта (subtype); • имя объекта (name); • IP-адрес, с которого был сделан запрос (ip); • старое значение параметра (old_value); • новое значение параметра (new_value)	«[user_type] [username] ([authenticator]) изменил правило [field] для объекта [entity] ([uuid]) [subtype] [name] (ip-адрес [ip]). Старое значение: [old_value]. Новое значение: [new_value]»
Операция с публикациями фонда web.AuditPublication	Регистрируется: • действие публикации (action_pub); • фонд (pool)	«[action_pub] публикация фонда [pool]»
Операция с состоянием ВМ web.AuditMachineState	Регистрируется: • имя ВМ (name_vm); • новый статус ВМ (action_machine)	«Запрос на изменение статуса ВМ - [name_vm] статус - [action_machine]»
Подключение пользователя к сессии «Удаленного помощника» web.ConnectRASession	Регистрируется: • имя пользователя (user_name); • тип учетной записи пользователя (user_type); • данные ВМ, к сессии которой выполнен запрос на подключение (userservice)	«[user_type] [user_name] подал запрос на подключение к сессии [userservice]»

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Пользователь запросил метрики узла web.AuditMetrics	Регистрируется: • имя пользователя (user_name); • имя сущности, для которой запросили метрики (entity_name); • UUID сущности, для которой запросили метрики (entity_uuid); • FQDN сущности, для которой запросили метрики (entity_fqdn); • список метрик (metrics)	«Пользователь [user_name] запросил метрики для [entity_name] ([entity_fqdn], UUID: [entity_uuid]). Метрики: [metrics]»
Экспорт данных из таблицы веб-интерфейса в CSV web.DataExport	Регистрируется: • имя пользователя (username); • название домена аутентификации пользователя (authenticator); • тип учетной записи пользователя (user_type); • IP-адрес (ip); • код таблицы (table_code). Например: providers, audit_events; • имя таблицы (table_name); • формат выгрузки (export_format); • тип выгрузки (scopr). Например: all (все строки), selected (выбранные строки); • количество выгруженных строк (rows_cont)	«[user_type] [username] ([authenticator]) выполнил экспорт данных в формате [export_format] из таблицы [table_name] (table_code=[table_code], scope=[scope], rows_count=[rows_count], ip-адрес [ip])»
Изменение связей тегов web.TagRelationChanged	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • имя связанной сущности (name_relation_entity); • тип связанной сущности (type_relation_entity); • старые значения (old_value); • новые значения (new_value)	«[user_type] [username] ([authenticator]) изменил теги у сущности [name_relation_entity] ([type_relation_entity]), старое значение - [old_value], новое значение - [new_value]»

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Изменение режима техобслуживания фонда РМ web.EntityMaintenanceMode	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • тип учетной записи пользователя (user_type); • тип сущности (type_name); • имя сущности (name); • старое значение (old_value); • новое значение (new_value); • IP-адрес (ip)	«[user_type] [username] ([authenticator]) изменил состояние параметра Техобслуживание для сущности [type_name]([name]) новое значение - [new_value], старое значение - [old_value] (IP-адрес {ip})»
Изменение состояния расписания web.SchedulerActivationChange	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • тип учетной записи пользователя (user_type); • тип расписания (type_name); • имя расписания (name); • старое значение (old_value); • новое значение (new_value); • IP-адрес (ip)	«[user_type] [username] ([authenticator]) изменил состояние расписания [type_name]([name]) новое значение - [new_value], старое значение - [old_value] (IP-адрес {ip})»
Изменение состояния хранилища журналов web.JournalStorageActivationChange	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • тип учетной записи пользователя (user_type); • тип хранилища (type_name); • имя хранилища (name); • старое значение (old_value); • новое значение (new_value); • IP-адрес (ip)	«[user_type] [username] ([authenticator]) изменил состояние Хранилища Журналов [type_name]([name]) новое значение - [new_value], старое значение - [old_value] (IP-адрес {ip})»
	События, связанные с API	

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Действия пользователя с API (обращения Termidesk VDI к API от имени пользователя) `api.ApiViewAction`	Регистрируется: • название домена аутентификации пользователя (`authenticator`); • имя пользователя (`username`). Для запросов, выполняемых без аутентификации, указывается пользователь `AnonymousUser(AnonymousAuth)`; • тип учетной записи пользователя (`user_type`); • IP-адрес, с которого был сделан запрос (`ip`); • запрос(`action`); • URL-команда (`request_path`); • код ответа (`response_status`)	«`[user_type]` `[username]` (`[authenticator]`) выполнил запрос `[action]` для api `[request_path]` (статус код ответа - `[response_status]`) (ip-адрес `[ip]`)»
Неудачная попытка создать сессию API `api.ApiUserLoginForbidden`	Регистрируется: • метод (`handler_path`); • ошибка (`error`); • IP-адрес, с которого был сделан запрос (`ip`)	«Выполнена неудачная попытка регистрации пользователя api - `[handler_path]` ошибка - `[error]` ip - `[ip]`»
Вход пользователя в систему через API `api.UserLogin`	Регистрируется: • название домена аутентификации пользователя (`authenticator`); • имя пользователя (`username`); • тип учетной записи пользователя (`user_type`); • IP-адрес, с которого был сделан запрос (`ip`); • тип портала (`portal`); • идентификатор портала (`portal_uuid`); • тип учетной записи пользователя (`user_type`)	«`[user_type]` `[username]` (`[authenticator]`) вошел в систему с IP-адресом `[ip]` через `[portal]`(`[portal_uuid]`)»

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Выход пользователя из системы через API `api.UserLogout`	Регистрируется: • название домена аутентификации пользователя (`authenticator`); • имя пользователя (`username`); • тип учетной записи пользователя (`user_type`); • IP-адрес, с которого был сделан запрос (`ip`); • тип портала (`portal`); • идентификатор портала (`portal_uuid`); • тип учетной записи пользователя (`user_type`)	«`[user_type]` `[username]` (`[authenticator]`) вышел из системы с IP-адреса `[ip]` через `[portal]`(`[portal_uuid]`)»
Получение данных «Шлюзом» в ответ на отправку токена `api.WsproxyVerify`	Регистрируется: • IP-адрес, с которого был сделан запрос (`ip`); • результат выполнения (`result`): корректность получения данных или ошибка	«Попытка получения данных шлюзом `[ip]` результат - `[result]`»
События, связанные с пользовательскими сессиями		
Старт сессии пользователя `session.SessionStarted`	Регистрируется: • название домена аутентификации пользователя (`authenticator`); • имя пользователя (`username`); • GUSID (`suid`)	«Сессии пользователя `[username]`(`[authenticator]`) назначен GUSID `[suid]`»
Окончание сессии пользователя `session.SessionEnded`	Регистрируется: • название домена аутентификации пользователя (`authenticator`); • имя пользователя (`username`); • GUSID (`suid`)	«Сессия пользователя `[username]`(`[authenticator]`) с GUSID `[suid]` завершена по запросу»
Сессия пользователя завершена по сроку действия `session.SessionExpired`	Регистрируется: • название домена аутентификации пользователя (`authenticator`); • имя пользователя (`username`); • GUSID (`suid`)	«Сессия пользователя `[username]`(`[authenticator]`) с GUSID `[suid]` завершена по сроку действия»
События, связанные с поставщиком ресурсов		
Изменение конфигурации на стороне поставщика ресурсов `provider.ChangeConfiguration`	Регистрируется: • имя поставщика ресурсов (); • параметр (`changed_field`)	«Была изменена конфигурация `[provider]`. Был удален `[changed_field]`»

Наименование события	Состав регистрируемой информации	Шаблон регистрации события
Создание ВМ на стороне поставщика ресурсов provider.SuccessCreateVM	Регистрируется: • имя ВМ (vm_name)	«Успешно создалась виртуальная машина [vm_name]»
Удаление ВМ на стороне поставщика ресурсов provider.SuccessRemoveVM	Регистрируется: • имя ВМ (vm_name)	«Успешно удалена виртуальная машина [vm_name]»
	События, связанные с фондом РМ	
Изменение режима техобслуживания фонда РМ servicepool.MaintenanceModeChange	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • тип учетной записи пользователя (user_type); • имя фонда РМ (service_pool_name); • статус режима техобслуживания (maintenance_state)	«[user_type] [username] ([authenticator]) изменил режим техобслуживания для фонда рабочих мест [service_pool_name] на [maintenance_state]»

Форматы регистрируемых событий аудита и их примеры

Каждая запись аудита регистрируются в формате: [Дата и время][termidesk.audit.events.Наименование события] [Шаблон регистрации события] [Уровень важности]

Пример регистрации события аудита «Пользователь обновил данные сущности» в веб-портале:

Дата и время	Уровень	Событие	Описание
06.06.2025, 12:35:24	Высокий	termidesk.audit.events.workplace.EntityActionUpdate	«Пользователь "admin123(Встроенный)" обновил данные - "\{'tunnelWait': \{'старое_значение': 30, 'новое_значение': 29}}" для объекта Transport (ce5ecd63-041f-5d5e-99c9-9de93a7a663d) TERATransport "TERA" "(ip-адрес 10.10.100.11)"»

Termidesk VDI также поддерживает запись каждого события аудита в формате CEF (см. подраздел **Системные параметры аудита**):

[Дата и время]|[Узел]|[CEF:версия]|[Uveon]|[Termidesk]|[Версия Termidesk VDI]|[Идентификатор события]|[Наименование события]|[Объекты события]|[Уровень важности]

Пример события «Пользователь обновил данные сущности» в формате CEF:

```
2025-06-06T12:35:24.367115 localhost
CEF:0|Uveon|Termidesk|7.0|api/webui/draft/transports/:PUT|Пользователь обновил
данные сущности|6|suser=admin123 authenticator=Встроенный username=admin123
ip=10.10.100.11 entity=Transport uuid=ce5ecd63-041f-5d5e-99c9-9de93a7a663d
subtype=TERATransport name=TERA action=update updatedata={'tunnelWait':
```

```
{'старое_значение': 30, 'новое_значение': 29}} level=высокий
```

Формат CEF

Использование формата CEF

Termidesk VDI поддерживает запись каждого события аудита в формате Common Event Format (CEF).

Формат CEF описывается следующим набором обязательных полей:

- Version - версия формата CEF;
- Device Vendor, Device Product и Device Version - однозначная идентификация источника события;
- Signature ID - уникальный идентификатор типа события;
- Name - понятное описание события;
- Severity - важность события (от 0 до 10);
- Extension - набор пар «ключ - значение».

Для использования формата CEF нужно включить использование CEF в системных параметрах аудита «Портала администратора» (перейти «Системные параметры - Системные настройки», выбрать раздел «Аудит»).

Для того, чтобы события в формате CEF корректно сохранялись в локальный файл журнала, нужно:

- включить сохранение событий в файл в системных параметрах аудита «Портала администратора» (перейти «Системные параметры - Системные настройки», выбрать раздел «Аудит»);
- отредактировать шаблон отправки сообщений в каталоге `/etc/opt/termidesk-vdi/templates`:
  - закомментировать:

```
template t_termidesk_audit { template("[$ISODATE] $MESSAGE\n"); };
```

- раскомментировать:

```
template t_termidesk_audit { template("$MESSAGE\n"); };
```

- выполнить:

```
sudo /opt/termidesk/sbin/termidesk-config update_logger_config
```

- включить использование CEF в системных параметрах аудита «Портала администратора» (перейти «Системные параметры - Системные настройки», выбрать раздел «Аудит»).

ЖУРНАЛИРОВАНИЕ

Системные параметры журналирования

Для конфигурации системных параметров журналирования следует перейти «Системные параметры - Системные настройки», выбрать раздел «Логирование».

Доступные для редактирования администратору Termidesk VDI параметры перечислены в столбце «Параметр» следующей таблицы (см. таблицу Параметры журналирования Termidesk VDI).

Таблица 171. Параметры журналирования Termidesk VDI

Параметр	Описание
«Логирование Syslog»	Перенаправление потока событий журналов сервера Termidesk VDI на отдельный syslog-сервер. Syslog-сервер должен быть предварительно настроен для корректного получения событий журналов сервера Termidesk VDI. По умолчанию перенаправляются события журналов, перечисленных в разделе **Журналы сервера Termidesk VDI**. Значение по умолчанию: «Нет»
«Хост 1» — «Хост 3»	IP-адреса или имена узлов, на которых развернута служба syslog-сервера
«Протокол»	Выбор протокола работы для службы syslog-сервера. Доступные значения: «UDP», «TCP», «TLS». При использовании протокола «TLS» необходимо установить на узел с «Универсальным диспетчером» Termidesk VDI корневой сертификат ЦС, использующийся в syslog-сервере, согласно подразделу **Установка корневого сертификата центра сертификации**. Значение по умолчанию: «UDP»
«Категория сообщения»	Выбор категории сообщений syslog для их классификации при передаче в журнал мониторинга. Параметр не влияет на состав регистрируемых событий и запись сообщений в файл журнала. Значение по умолчанию: «user»
«Уровень логирования»	Выбор минимального уровня событий, записываемых в журнал мониторинга. Возможные значения: • «CRITICAL» - запись сообщений уровня «CRITICAL»; • «ERROR» - запись сообщений уровней «ERROR», «CRITICAL»; • «WARNING» - запись сообщений уровней «WARNING», «ERROR», «CRITICAL»; • «INFO» - запись сообщений уровней «INFO», «WARNING», «ERROR», «CRITICAL»; • «DEBUG» - запись сообщений уровней «DEBUG», «INFO», «WARNING», «ERROR», «CRITICAL». Значение по умолчанию: «INFO»

Параметр	Описание
«Тег ретранслятора»	Тег записи, обрабатываемый «Ретранслятором». Должен соответствовать параметру `Match`, указанному в конфигурационном файле «Ретранслятора». Значение по умолчанию: «termidesk»
«Суффикс тега ретранслятора»	Суффикс тега записи, обрабатываемый «Ретранслятором». Должен соответствовать параметру `Match`, указанному в конфигурационном файле «Ретранслятора». Значение по умолчанию: «termidesk»

Настройка уровня журналирования сервера Termidesk VDI

Уровень журналирования задается параметром `LOG_LEVEL` в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf`.

Для изменения уровня журналирования нужно:

- изменить параметр `LOG_LEVEL`;
- перезапустить службы Termidesk VDI:

```
sudo systemctl restart termidesk-vdi.service termidesk-celery-beat.service
termidesk-celery-worker.service
```

Журналы сервера Termidesk VDI

Журналы сервера Termidesk VDI хранятся в каталоге `/var/log/termidesk`.

Администратор может изменить каталог хранения через утилиту `termidesk-config` (см. подраздел **Утилита `termidesk-config`**).

Настройки ротации журналов определены в конфигурационном файле `/etc/logrotate.d/termidesk.conf` и формируются по шаблонам, указанным в каталоге `/etc/opt/termidesk-vdi/templates`. Каталог хранения шаблонов может быть изменен через утилиту `termidesk-config`.

Установлены следующие журналы Termidesk VDI, разделенные по типам событий, которые в них записываются:

- `broker.log` - записываются события «Брокера сообщений TermideskMQ». Поддерживается автоматическая ротация журнала для исключения возможности переполнения пространства диска;
- `celery-beat.log` - записываются события периодической проверки состояния обработчика заданий через брокера сообщений. Поддерживается автоматическая ротация журнала для исключения возможности переполнения пространства диска;
- `celery-worker.log` - записываются события обработчика заданий через брокера сообщений. Поддерживается автоматическая ротация журнала для исключения возможности переполнения пространства диска;
- `other.log` - записываются события, не попавшие в другие журналы;
- `termidesk.log` - записываются события работы «Универсального диспетчера» Termidesk

VDI;

- `workers.log` - записываются события обработчика фоновых задач;
- `gunicorn-access.log` - записываются события доступов к внутреннему серверу Gunicorn;
- `gunicorn-error.log` - записываются события функционирования внутреннего сервера Gunicorn.

Устаревшие журналы (`aggregator.log`, `auth.log`) допускается удалить вручную.

Просмотр журналов в «Портале администратора»

Просмотр системного журнала

Для просмотра общего журнала событий, связанного с функционированием Termidesk VDI, следует перейти «Журналы - Системные журналы», где визуализируются системные события с указанием уровня важности (CRITICAL, ERROR, WARNING, INFO, DEBUG) и источника возникновения события (см. рисунок Отображение общего журнала в графическом интерфейсе управления Termidesk VDI).

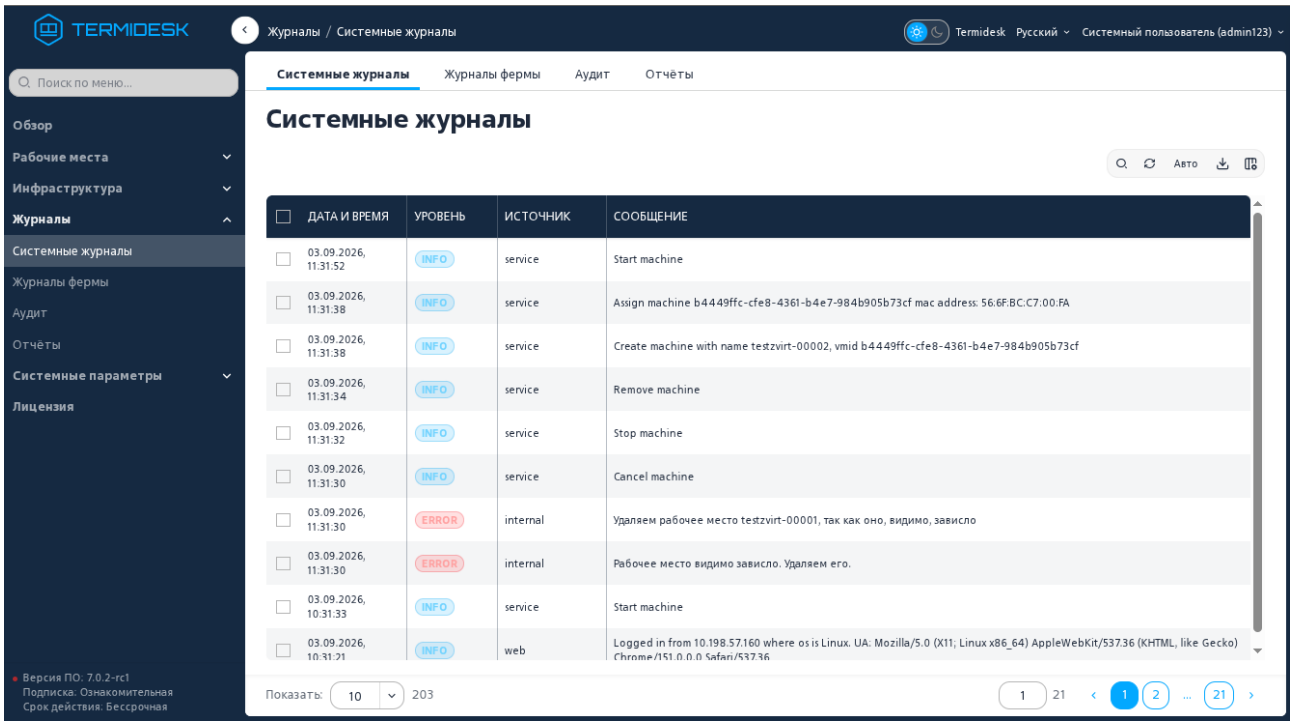


Рисунок 98. Отображение общего журнала в графическом интерфейсе управления Termidesk VDI

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;

- поиск записей по таблице;
- изменение внешнего вида таблицы;
- экспорт записей таблицы в `csv`-файл. Можно выгрузить:
  - все записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт всех]**;
  - выбранные записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт выбранных]**.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Просмотр журнала аудита

Для просмотра журнала событий, связанного с действиями субъектов доступа, следует перейти «Журналы - Аудит» (см. рисунок Отображение журнала аудита в графическом интерфейсе управления Termidesk VDI).

> Если события аудита не отображаются во вкладке «Журналы – Аудит», то необходимо убедиться, что в «Системные параметры - Системные настройки» во вкладке «Аудит» параметр «Сохранение в БД» имеет значение «Да».

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- поиск записей по таблице;
- изменение внешнего вида таблицы;
- экспорт записей таблицы в `csv`-файл. Можно выгрузить:
  - все записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт всех]**;
  - выбранные записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт выбранных]**.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

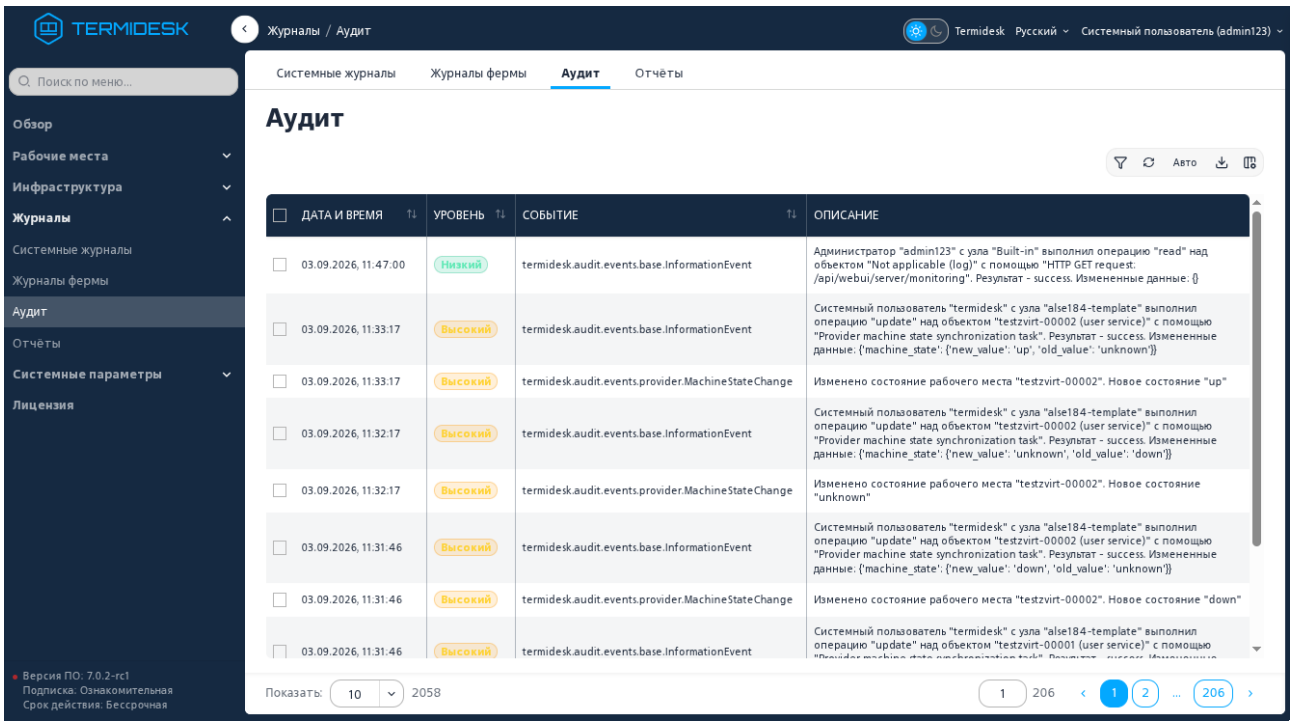


Рисунок 99. Отображение журнала аудита в графическом интерфейсе управления Termidesk VDI

Просмотр централизованных журналов фермы Termidesk VDI

Отображение централизованных журналов фермы

Для просмотра централизованных журналов событий, связанных с функционированием фермы Termidesk VDI, следует перейти «Журналы - Журналы фермы», где визуализируются события из «Хранилища журналов».

Для отображения событий нужно убедиться, что:

- добавлен и настроен «Ретранслятор»;
- добавлено «Хранилище журналов».

Если ранее узел «Ретранслятора» настраивался для Termidesk VDI версии младше 6.0, то его конфигурацию следует изменить.

По умолчанию записи событий представлены в табличном виде и упорядочены согласно столбцу «Дата и время» (записи в журнале сортируются по дате по убыванию) (см. рисунок Отображение централизованных журналов фермы).

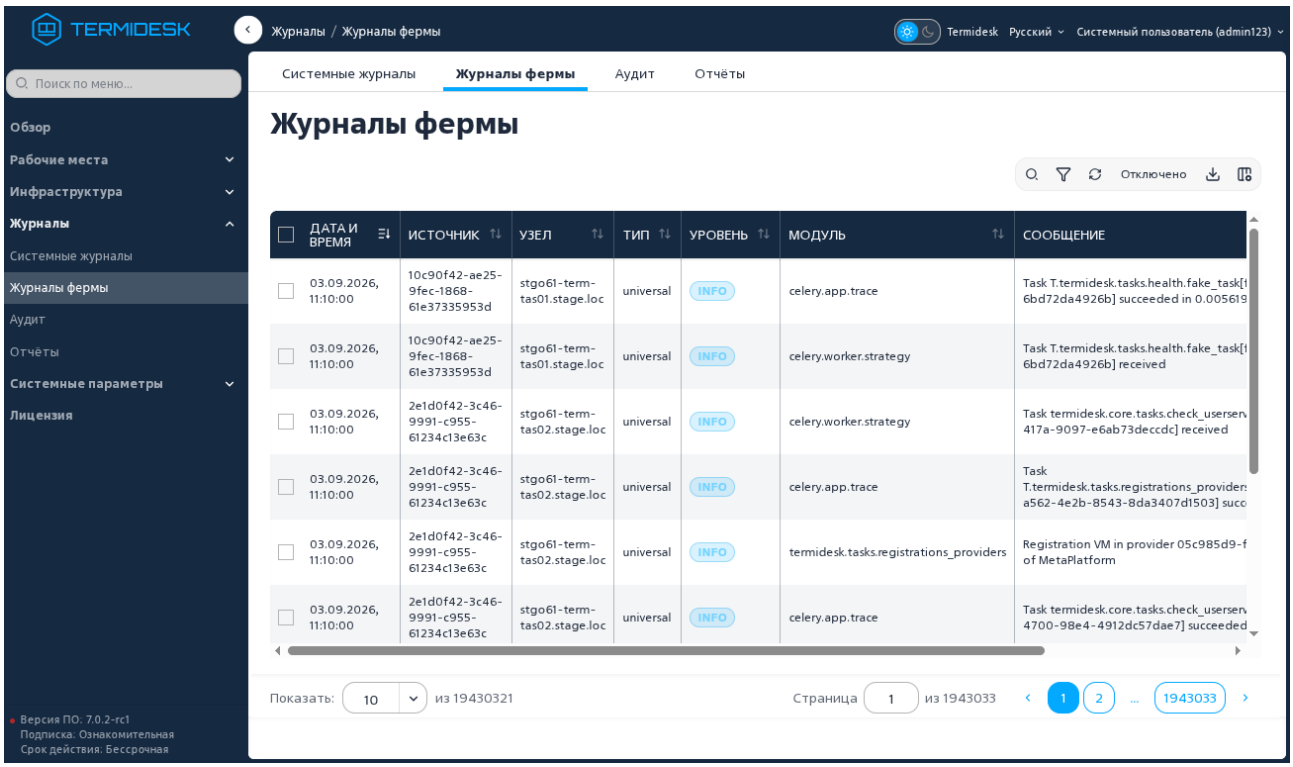


Рисунок 100. Отображение централизованных журналов фермы

Основные параметры списка приведены в таблице (см. таблицу Основные параметры списка событий централизованного журнала).

Таблица 172. Основные параметры списка событий централизованного журнала

Параметр	Описание
«Дата и время»	Дата и время регистрации события
«Источник»	Системный UUID узла, который зарегистрировал событие
«Узел»	Имя узла
«Тип»	Тип портала, который зарегистрировал событие. Может быть: «admin» («Портал администратора»), «user» («Портал пользователя»), «universal» («Портал универсальный»)
«Уровень»	Категория сообщения. Возможные значения:«INFO», «DEBUG», «WARNING», «ERROR»
«Модуль»	Служба Termidesk VDI, которая зарегистрировала событие
«Сообщение»	Подробное описание события

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;

- поиск записей по таблице;
- изменение внешнего вида таблицы;
- экспорт записей таблицы в `csv`-файл. Можно выгрузить:
  - все записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт всех]**;
  - выбранные записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт выбранных]**.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода.

Фильтрация списков событий журналов фермы

Для списка событий журналов фермы доступен механизм фильтрации («Умный фильтр»). Фильтрация осуществляется путем задания значений для параметров «Атрибут», «Условие» и «Значение».

Для добавления дополнительного фильтра следует нажать экранную кнопку **[+]**. Для удаления фильтра нужно использовать экранную кнопку **[-]** в соответствующей строке.

Чтобы применить установленные параметры фильтрации, следует нажать экранную кнопку **[Применить]**.

Экранная кнопка **[Очистить]** возвращает параметры фильтра к исходному состоянию:

удаляются дополнительные строки фильтра, все значения сбрасываются, поля «Условие» и «Значение» блокируются.

Подробное описание параметров механизма фильтрации списка событий приведено в таблице (см. таблицу Параметры фильтрации событий журналов фермы).

При ручном вводе данных в поле фильтра «Значение» допускается полный или частичный ввод только одного параметра фильтрации.

При применении нескольких одинаковых фильтров к списку фильтрация выполняется с учетом только последнего заданного фильтра.

Таблица 173. Параметры фильтрации событий журналов фермы

Атрибут	Условия	Значение
«Дата и время»	Формирование списка событий по времени создания: • «В пределах» - в указанном временном промежутке; • «Не в пределах» - исключая указанный временной промежуток	Ручной ввод посредством выбора даты и времени (графический элемент)
«Источник»	Формирование списка событий по источнику события: • «Является» - по указанному наименованию источника; • «Не является» - исключая указанное наименование источника; • «Начинается с» - по начальной части наименования источника; • «Оканчивается на» - по конечной части наименования источника; • «Содержит» - включая указанную часть наименования источника	Ручной ввод
«Тип»	Формирование списка событий по типу события: • «Является» - по указанному наименованию типа события; • «Не является» - исключая указанное наименование типа события; • «Начинается с» - по начальной части наименования типа события; • «Оканчивается на» - по конечной части наименования типа события; • «Содержит» - включая указанную часть наименования типа события	Ручной ввод

Атрибут	Условия	Значение
«Узел»	Формирование списка событий по имени узла: • «Является» - по указанному наименованию; • «Не является» - исключая указанное наименование; • «Начинается с» - по начальной части наименования; • «Оканчивается на» - по конечной части наименования; • «Содержит» - включая указанную часть наименования	Ручной ввод
«Уровень»	Формирование списка событий по уровню: • «Является» - по указанному уровню события; • «Не является» - исключая указанный уровень события	• «INFO»; • «DEBUG»; • «WARNING»; • «ERROR»
«Модуль»	Формирование списка событий по модулю: • «Является» - по указанному наименованию модуля; • «Не является» - исключая указанное наименование модуля; • «Начинается с» - по начальной части наименования модуля; • «Оканчивается на» - по конечной части наименования модуля; • «Содержит» - включая указанную часть наименования модуля	Ручной ввод
«Сообщение»	Формирование списка событий по сообщению: • «Является» - по указанному сообщению; • «Не является» - исключая указанное сообщение; • «Начинается с» - по начальной части сообщения; • «Оканчивается на» - по конечной части сообщения; • «Содержит» - включая указанную часть сообщения	Ручной ввод

Отчеты

Для формирования отчетов о событиях в графическом интерфейсе управления следует перейти «Журналы - Отчёты».

Можно сформировать следующие отчеты:

- отчет по последнему пользовательскому входу в систему;
- отчет по пользовательским сеансам;

- отчет по пользовательским подключениям.

Для формирования отчета по последнему пользовательскому входу в систему нажать экранную кнопку **[Создать]**, выбрать тип отчета «Отчет по последнему пользовательскому входу в систему» и заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Параметры для формирования отчета по последнему пользовательскому входу в Termidesk).

Таблица 174. Параметры для формирования отчета по последнему пользовательскому входу в Termidesk

Параметр	Описание
«Название»	Текстовое наименование отчета
«Комментарий»	Информационное сообщение, используемое для описания отчета
«Дата и время начала»	Дата и время начала события, от которых будет сформирован отчет. Ручной ввод посредством выбора даты и времени (графический элемент)

Если сформированные отчеты не содержат никакой информации (пустые), необходимо проверить, что системный параметр аудита «Сохранение в БД» установлен в значение «Да» .

Для формирования отчета по пользовательским сеансам нажать экранную кнопку **[Создать]**, выбрать тип отчета «Отчет по пользовательским сеансам» и заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Параметры для формирования отчета по пользовательским сеансам).

Таблица 175. Параметры для формирования отчета по пользовательским сеансам

Параметр	Описание
«Название»	Текстовое наименование отчета
«Комментарий»	Информационное сообщение, используемое для описания отчета
«Дата и время начала сеанса»	Дата и время начала события. Ручной ввод посредством выбора даты и времени (графический элемент)
«Дата и время завершения сеанса»	Дата и время завершения события. Ручной ввод посредством выбора даты и времени (графический элемент)
«Домен аутентификации»	Наименование домена аутентификации, по которому будет осуществлен поиск события
«Пользователь»	Логин пользователя, по которому будет осуществлен поиск события

Для формирования отчета по пользовательским подключениям нажать экранную кнопку **[Создать]**, выбрать тип отчета «Отчет по пользовательским подключениям» и заполнить параметры, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Параметры для формирования отчета по пользовательским подключениям).

Таблица 176. Параметры для формирования отчета по пользовательским подключениям

Параметр	Описание
«Название»	Текстовое наименование отчета
«Комментарий»	Информационное сообщение, используемое для описания отчета
«Дата и время начала подключения»	Дата и время начала события. Ручной ввод посредством выбора даты и времени (графический элемент)

Параметр	Описание
«Дата и время завершения подключения»	Дата и время завершения события. Ручной ввод посредством выбора даты и времени (графический элемент)

Для просмотра сформированного отчета следует перейти «Журналы - Отчёты» и выбрать название отчета. Откроется форма отчета в виде таблицы.

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- изменение внешнего вида таблицы;
- экспорт записей таблицы в `csv`-файл. Можно выгрузить:
  - все записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт всех]**;
  - выбранные записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Экспорт выбранных]**.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить видимость]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- порядок отображения столбцов. Для изменения порядка отображения столбцов нужно нажать и удерживать левую кнопку мыши на наименовании столбца, перемещая его вверх или вниз по списку. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Поддерживается выбор количества отображаемых записей на одной странице. Для настройки нужно:

- выбрать графический элемент Показать: 10 под таблицей. По умолчанию отображаются 10 записей на одной странице;
- выбрать одно из предлагаемых значений, отображаемых в выпадающем списке

графического элемента или ввести свой вариант в поле ввода.

ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ TERMIDESK

Утилита termidesk-vdi-manage

Утилита termidesk-vdi-manage используется для настройки «Универсального диспетчера» из интерфейса командной строки.

Для вызова утилиты следует:

- в интерфейсе командной строки переключиться на пользователя termidesk:

```
sudo -u termidesk bash
```

- вывести список команд утилиты:

```
/opt/termidesk/sbin/termidesk-vdi-manage help
```

Каждая подкоманда в приведенных ниже командах поддерживает вывод справки через ключ -h. В командах поддерживаются аргументы вывода:

- --version - вывод версии программы;
- -v {0,1,2,3}, --verbosity {0,1,2,3} - уровень детализации сообщений;
- --settings <настройки> - путь к модулю настроек Python;
- --pythonpath <каталог Python> - каталог, который нужно добавить в путь Python, например /home/djangoprojects/myproject;
- --traceback - вызов исключений;
- --no-color - вывод команды без подсвечивания;
- --force-color - вывод команды с принудительным подсвечиванием;
- --skip-checks - пропуск проверки системы.

Для управления параметрами поставщиков ресурсов, доменов аутентификации, протоколов доставки и других компонентов, настраиваемых через «Портал администратора» Termidesk VDI, следует обратиться к командам секции [termidesk].

Большая часть команд из вывода /opt/termidesk/sbin/termidesk-vdi-manage help предназначена для работы с БД и фреймворком Django и не приведена здесь.

Команды секции [termidesk] приведены в таблице (см. таблицу Команды секции [termidesk]).

Таблица 177. Команды секции [termidesk]

Параметр	Описание '
tdsk_auth	Управление доменами аутентификации. Для просмотра списка ключей следует воспользоваться аргументом -h: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_auth -h` Поддерживаются подкоманды: • create - создание домена аутентификации; • list - вывод списка доменов аутентификации; • remove - удаление домена аутентификации; • login - аутентификация в указанный домен; • logout - завершение сессии
tdsk_auth create	Создание домена аутентификации. Подкоманда create принимает аргументы: • --type - задание типа домена аутентификации. Доступны: IPAuth («IP аутентификация»), KerberosAuthenticatorPlugin («FreeIPA»), SAMLAuthenticator («SAML»), SimpleLdapAuthenticator («Microsoft AD DS/LDAP»); • --params - задание параметров домена аутентификации. Формат: имя1=значение1 имя2=значение2 и т.д. Доступные параметры для указанного типа домена аутентификации можно получить через команду --list , например: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_auth create --type IPAuth --name test --small_name test` • --list - вывод параметров домена аутентификации; • --test - проверка параметров без создания домена аутентификации; • --quiet - вывод только сообщений об ошибках; • --name <ИМЯ> - имя домена аутентификации; • --small_name <короткое имя> - короткое имя домена аутентификации. Допустимые символы: a-z, A-Z, 0-9. Максимальная длина 32 символа; • --priority <приоритет> - числовое значение приоритета домена аутентификации, по умолчанию «1»; • --comments <комментарий> - комментарий к создаваемому домену
tdsk_auth list	Вывод списка доменов аутентификации. Подкоманда list принимает аргумент --output json для вывода списка в формате JSON
tdsk_auth remove	Удаление домена аутентификации. Подкоманда remove принимает аргументы: • --output json - вывод параметров в формате JSON; • --silent - «тихое» удаление для выполнения команды из исполняемого файла; • --uuid <идентификатор> - идентификатор объекта для удаления.

Параметр	Описание '
tdsk_auth login	Аутентификация в указанный домен. Подкоманда login принимает аргументы: • --uuid <идентификатор> - идентификатор объекта для аутентификации; • --small_name <короткое имя> - короткое имя домена аутентификации; • --output json - вывод параметров в формате JSON.
tdsk_auth logout	Завершение сессии в указанном домене. Подкоманда logout принимает аргументы: • --token <токен> - токен сессии пользователя; • --output json - вывод параметров в формате JSON
tdsk_clear_cache	Удаляет ненужные кешированные данные. Для просмотра списка ключей следует воспользоваться аргументом -h: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_clear_cache -h`
tdsk_clearsessions	Порционная очистка сессий. Поддерживаются аргументы: • -chunk <количество> - количество сессий для удаления, по умолчанию 1000
tdsk_config	Управление системными настройками. Поддерживаются подкоманды: • list - вывод конфигурационных параметров и их значений; • set - установка значения конфигурационному параметру
tdsk_config set	Установка значения конфигурационному параметру. Подкоманда set принимает аргументы: • --key <ключ> - ключ параметра; • --value <значение> - значение параметра. Пример команды для смены значения параметра metrics.cacheSize («Размер кеша») секции Metrics на «9»: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_config set --key metrics.cacheSize --value 9`
tdsk_exp_2fa_add_statictoken	Добавление токена пользователю. Поддерживаются аргументы: • username - имя пользователя, с которым будет ассоциирован токен; • -t <токен>, --token <токен> - токен, который нужно добавить. Если этот параметр пропущен, он будет сгенерирован случайным образом; • --auth_uuid <идентификатор> - идентификатор домена аутентификации

Параметр	Описание '
tdsk_exp_2fa_clear_totpdevice	Удаление TOTP-устройства пользователя. Поддерживаются аргументы: • username - имя пользователя, которому нужно удалить TOTP-устройство; • --auth_uuid <идентификатор> - идентификатор домена аутентификаци
tdsk_gateways	Управление профилями шлюзов. Поддерживаются подкоманды: • create - создание профиля шлюза; • list - вывод списка профилей шлюзов; • remove - удаление профиля шлюза
tdsk_gateways create	Создание профиля шлюза. Для подкоманды create поддерживаются следующие аргументы: • --type - задание типа профиля шлюза. Доступен: TermideskGateway; • --params - задание параметров профиля шлюза. Формат: имя1=значение1 имя2=значение2 и т.д. Доступные параметры для указанного типа профиля шлюза можно получить через команду --list, например: /opt/termidesk/sbin/termidesk-vdi-manage tdsk_gateways create --type TermideskGateway --list --name test_gateway • --list - вывод параметров профиля шлюза; • --test - проверка параметров без создания профиля шлюза; • --quiet - вывод только сообщений об ошибках; • -- name <имя> - наименование профиля шлюза; • --comments <комментарий> - комментарий к создаваемому профилю шлюза; • --priority <приоритет> - числовое значение приоритета профиля шлюза. Пример создания профиля шлюза через подкоманду create: /opt/termidesk/sbin/termidesk-vdi-manage tdsk_gateways create --type TermideskGateway --params gatewayUrl=wss://192.0.2.1:10000 tunnelWait=35 --name test_gateway --priority 1

Параметр	Описание '
tdsk_graph_models	Создание файла GraphViz с описанием моделей БД для указанных имен приложений. Можно передать несколько имен приложений, и все они будут объединены в одну модель. Поддерживаются аргументы: • app_label - наименование приложения; • --pygraphviz - использование PyGraphViz для создания изображения; • --pydot - использование PyDot(Plus) для создания изображения; • --disable-fields, -d - не показывать поля; • --group-models, -g - сгруппировать модели в соответствии с их применением; • --all-applications, -a - включить все приложения для вывода модели; • --output <путь к файлу>, -o <путь к файлу> - запись вывода в файл; • --layout <макет>, -l <макет> - использование макета GraphViz для визуализации. Поддерживаются: circo, dot, fdpneato, nop, nop1, nop2, twopi; • --verbose-names, -n - использование подробных имен для моделей и полей; • --language <локализация>, -L <локализация> - указания языка, который будет использоваться для подробных имен; • --exclude-columns <столбцы>, -x <столбцы> - исключение определенных столбцов; • --exclude-models <модели>, -X <модели> - исключение определенных моделей; • --include-models <модели>, -I <модели> - ограничение только указанными моделями; • --inheritance, -e - включение наследования (используется по умолчанию); • --no-inheritance, -E - выключение наследования
tdsk_group	Управление группой РМ. Поддерживается подкоманда create
tdsk_group create	Создание группы РМ. Подкоманда create поддерживает следующие аргументы: • --quiet - вывод только сообщений об ошибках; • --name <имя> - имя создаваемой группы; • --comments <комментарий> - комментарий к создаваемой группе; • --priority <приоритет> - числовое значение приоритета группы
tdsk_license	Управление лицензией Termidesk VDI. Поддерживаются подкоманды: • install - установить лицензию; • show - вывести информацию об установленной лицензии; • remove - удалить лицензию из БД

Параметр	Описание '
tdsk_license install	Установка лицензии из файла, поддерживается относительный или абсолютный путь к файлу. Пример команды для установки лицензии: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_license install <путь к файлу лицензии>`
tdsk_license show	Вывод информации об установленной лицензии. Для вывода в формате JSON следует использовать аргумент --output: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_license show --output json`

tdsk_license remove	Удаление лицензии из БД. Перед выполнением команды необходимо авторизоваться:
	
	`/opt/termidesk/sbin/termidesk-vdi-manage tdsk_auth login`
	`/opt/termidesk/sbin/termidesk-vdi-manage tdsk_license remove`

tdsk_net	Управление объектом «Сеть». Поддерживается подкоманда create
tdsk_net create	Создание объекта «Сеть». Подкоманда create поддерживает следующие аргументы: • --quiet - вывод только сообщений об ошибках; • --name <имя> - имя создаваемой сети; • --netRange <диапазон> - диапазон IP-адресов. Допустимы различные форматы, например: A.B.C.*, A.B.C.D/N, A.B.C.D - E.F.G.D
tdsk_openbao_migrate	Миграция способа хранения паролей и переход с конфигурационного файла на использование хранилища OpenBao
tdsk_openbao_reverse_migrate	Миграция способа хранения паролей и переход с хранилища OpenBao на конфигурационный файл
tdsk_osm	Управление параметрами гостевой ОС. Поддерживается подкоманда create
tdsk_osm create	Создание параметров гостевой ОС. Подкоманда create поддерживает следующие аргументы: • --params - задание параметров гостевой ОС. Формат: имя1=значение1 имя2=значение2 и т.д.; • --list - вывод параметров гостевой ОС; • --test - проверка параметров без создания объекта; • --quiet - вывод только сообщений об ошибках; • --name <ИМЯ> - наименование параметров гостевой ОС; • --comments <комментарий> - комментарий к создаваемым параметрам

Параметр	Описание '
tdsk_pool	Управление фондами РМ. Поддерживаются подкоманды: • create - создание фонда РМ; • list - вывод списка фондов РМ
tdsk_pool create	Создание фонда РМ. Подкоманда create принимает аргументы: • --quiet - вывод только сообщений об ошибках; • --name <имя> - имя фонда РМ; • --comments <комментарий> - комментарий к создаваемому фонду РМ; • --published_name <имя> - имя публикации; • --service_id <идентификатор> - указание идентификатора шаблона РМ; • --osmanager_id <идентификатор> - указание идентификатора параметров гостевой ОС РМ; • --image_id <идентификатор> - указание идентификатора изображения гостевой ОС; • --servicesPoolGroup_id <идентификатор> - указание идентификатора группы РМ; • --cache_l1_srvs <значение> - количество РМ в кеше 1-го уровня; • --cache_l2_srvs <значение> - количество РМ в кеше 2-го уровня; • --max_srvs <значение> - максимальное количество РМ
tdsk_pool list	Вывод списка фондов РМ. Подкоманда list принимает аргумент --output json для вывода списка в формате JSON
tdsk_prov	Управление поставщиками ресурсов. Поддерживаются подкоманды: • create - создание поставщика ресурсов; • list - вывод списка поставщиков ресурсов; • id {id} - действия с поставщиком ресурсов с идентификатором id

Параметр	Описание '
`tdsk_prov create`	Создание поставщика ресурсов. Подкоманда `create` принимает аргументы: • `--type` - задание типа поставщика ресурсов. Доступны: RedVirtPlatform («РЕД Виртуализация»), SessionsPlatform («Сервер терминалов»), VMmanagerPlatform («VMmanager»), oVirtPlatform («oVirt»), pksvbrestPlatform («ПК СВ "Брест"»), vmwarePlatform («VMware vSphere»), zVirtPlatform («zVirt»), PhysicalMachinesServiceProvider («Автономная машина»); • `--params` - задание параметров поставщика ресурсов. Формат: `имя1=значение1 имя2=значение2` и т.д. Доступные параметры для указанного типа поставщика ресурсов можно получить через команду `--list` , например: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_prov create --type RedVirtPlatform --list --name test` • `--list` - вывод параметров поставщика ресурсов; • `--test` - проверка параметров без создания поставщика ресурсов; • `--quiet` - вывод только сообщений об ошибках; • `--name <имя>` - наименование поставщика ресурсов; • `--comments <комментарий>` - комментарий к создаваемому поставщику ресурсов
`tdsk_prov list`	Вывод списка поставщиков ресурсов. Подкоманда `list` принимает аргумент `--output json` для вывода списка в формате `JSON`
`tdsk_prov id {id}`	Действия с поставщиком ресурсов с идентификатором `id`. Подкоманда `id {id}` принимает: • `tpl create` - создание шаблона РМ в поставщике ресурсов; • `tpl list` - вывод списка шаблонов РМ поставщика ресурсов; • `tpl remove` - удаление шаблона РМ в поставщике ресурсов
`tdsk_refresh_ssa`	Регистрация «Сессионного агента» в БД Termidesk
`tdsk_setup`	Настройка Termidesk VDI после установки. Выполняет миграцию данных, создание таблицы кеша данных, сбор статических файлов, компиляцию файлов
`tdsk_trans`	Управление протоколами доставки. Поддерживаются подкоманды: • `create` - создание протокола доставки; • `list` - вывод списка протоколов доставки; • `remove` - удаление протокола доставки; • `convert` - конвертиртация протокола доставки

Параметр	Описание '
tdsk_trans create	Создание протокола доставки. Подкоманда create принимает аргументы: • --type - задание типа протокола. Доступны: HTML5Transport («HTML5»), LoudplayDirectTransport («Loudplay [экспериментальный]»), LoudplayTunneledTransport («Loudplay через шлюз (экспериментальный)»), RDPTransport («RDP»), TDSKSPICETransport («SPICE»), WSTRDPTransport («RDP через шлюз»), TERATransport («TERA»), TerminalTransport («RDP терминальный»); • --params - задание параметров протокола доставки. Формат: имя1=значение1 имя2=значение2 и т.д. Доступные параметры для указанного типа протокола доставки можно получить через команду --list. Например: /opt/termidesk/sbin/termidesk-vdi-manage tdsk_trans create --type RDPTransport --list --name test; • --list - вывод параметров протокола доставки; • --test - проверка параметров без создания протокола доставки; • --quiet - вывод только сообщений об ошибках; • --name <имя> - наименование протокола доставки; • --comments <комментарий> - комментарий к создаваемому протоколу доставки; • --priority <приоритет> - числовое значение приоритета протокола доставки; • --allowed_oss <перечень ОС> - перечень разрешенных ОС из списка: Android, CrOS, FreeBSD, iPad, iPhone, Linux, Mac, Windows, Windows Phone. Формат: имя1,имя2,имя3; • --nets_positive <yes/no> - указание, что протокол должен быть доступен только из сетей, указанных в параметре --networks. Может принимать значения не только yes или no, подходит в целом любое непустое значение; • --networks <наименования сетей> - перечень сетей, доступ из которых разрешен для создаваемого протокола доставки. Формат: имя1,имя2,имя3
tdsk_trans list	Вывод списка протоколов доставки. Подкоманда list принимает аргумент --output json для вывода списка в формате JSON
tdsk_trans remove	Удаление протокола доставки. Подкоманда remove принимает аргументы: • --output json - вывод списка в формате JSON; • --silent - выполнение в «тихом» режиме; • --uuid <идентификатор> - идентификатор объекта для удаления
tdsk_trans convert	Конвертиртация протокола доставки (RDSTransport, RDSWSTRDPTransport, STALTransport, STALWSTRDPTransport) в новый протокол TerminalTransport. Подкоманда convert принимает аргументы: • --uuid <идентификатор> - идентификатор протокола доставки, который необходимо конвертировать; • --all - ковернтировать все протоколы доставки MS RDS и STAL
tdsk_version	Получение версии Termidesk

Утилита termidesk-config

Утилита termidesk-config используется для переопределения настроек, заданных на этапе установки, и вносит изменения в конфигурационный файл termidesk.conf и /etc/default/termidesk-vdi.local.

Для вызова утилиты следует:

- в интерфейсе командной строки перейти в каталог /opt/termidesk/sbin/:

```
cd /opt/termidesk/sbin/
```

- выполнить запуск:

```
sudo ./termidesk-config
```

- откроется интерфейс утилиты (см. рисунок Интерфейс утилиты termidesk-config).

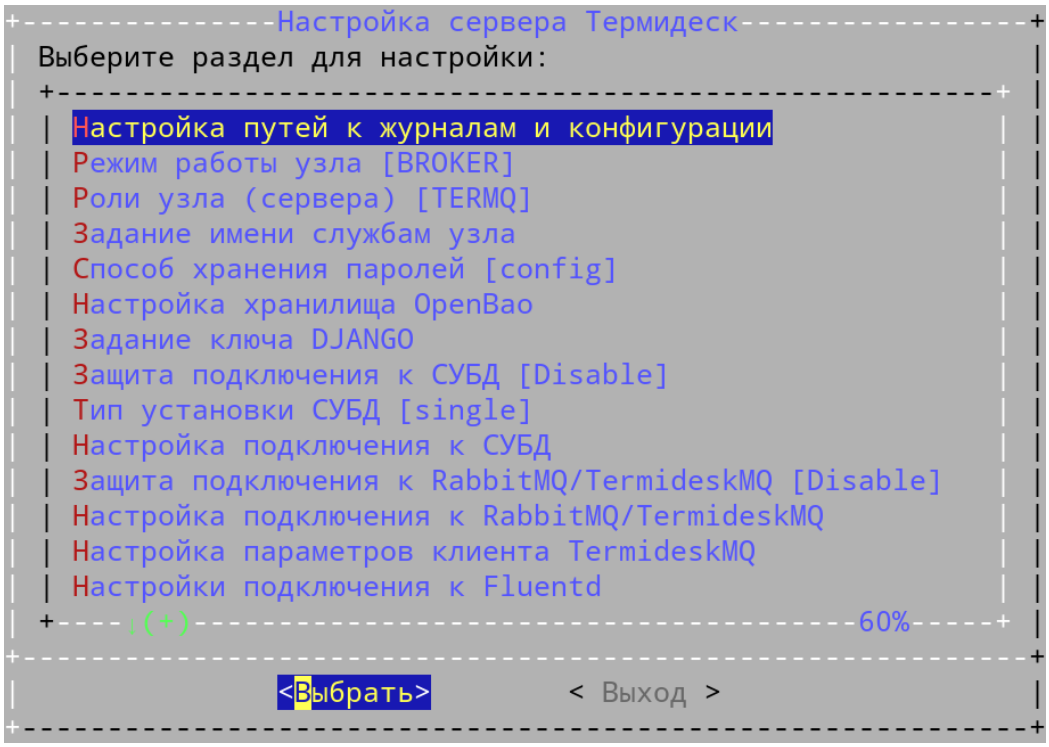


Рисунок 101. Интерфейс утилиты termidesk-config

Доступны следующие функции утилиты:

После выполнения изменений в любом из разделов рекомендуется воспользоваться пунктом «Перезапуск служб» для применения изменений.

- «Настройка путей к журналам и конфигурации: позволяет настроить каталоги для хранения конфигурации Termidesk VDI:
  - «Расположения конфигурации»: каталог, в котором будет расположен файл termidesk.conf (параметр ETC файла /etc/default/termidesk-vdi.local);
  - «Хранения журналов»: каталог, в котором будут расположены файлы журналов

(параметр LOG_DIR);

Параметр LOG_DIR доступен для изменения как в пункте «Место хранения журналов», так и в пункте «Настройка журналирования» - «Место хранения журналов». В обоих случаях фактически меняется значение только в параметре LOG_DIR конфигурационного файла termidesk.conf.

- «Шаблонов syslog/logrotate»: каталог, в котором будут расположены шаблоны для настройки регистрации событий и журналирования (параметр TEMPLATES_DIR файла /etc/default/termidesk-vdi.local);

- «Режим работы узла»: позволяет задать режим работы (параметр TERMIDESK_FARM_MODE):
  - «Диспетчер»: режим работы для фермы «Универсального диспетчера»;
  - «Агрегатор»: режим работы для фермы «Агрегатора»;

Установка «Агрегатора» должна производиться на узле, отличном от «Диспетчера».

Ранее установленный «Диспетчер» нельзя перенастроить на использование «Агрегатора».

- «Роли узла (сервера)»: позволяет изменить роли, которые запускаются на узле (параметр NODE_ROLES). Доступные роли:
  - «Портал администратора»;
  - «Портал пользователя»;
  - «Менеджер рабочих мест»;
  - «Брокер сообщений»;
- «Задание имени службам узла»: позволяет задать уникальное имя узла для его идентификации (параметр NODE_NAME);
- «Способ хранения паролей»: позволяет настроить способ хранения паролей подключения к СУБД и RabbitMQ (параметр SECRETS_STORAGE_METHOD):
  - «config» - пароли будут храниться в преобразованном виде в файле /etc/opt/termidesk-vdi/termidesk.conf;
  - «hvac» (рекомендуемый способ для безопасного хранения) - для хранения паролей будет использоваться хранилище паролей OpenBao или Hashicorp Vault (хранилище должно быть заранее создано и настроено);
  - «openbao» - для хранения паролей будет использоваться хранилище паролей OpenBao (хранилище должно быть заранее создано и настроено). В случае выбора «openbao» необходимо выполнить настройку подключения к хранилищу через функцию «Настройка хранилища OpenBao»;
- «Настройка хранилища OpenBao»: позволяет настроить параметры подключения к хранилищу и задать параметры, настроенные непосредственно на хранилище:
  - «URL хранилища» - IP-адрес или FQDN узла и порт с установленным хранилищем OpenBao (параметр SECRETS_OPENBAO_URL). Формат: http://<IP-адрес>:8200 или http://<FQDN>:8200. Подключение может выполняться по протоколу HTTPS, если OpenBao настроен соответствующим образом;
  - «Версия API OpenBao» - установленная версия API на OpenBao (параметр SECRETS_OPENBAO_KV_VERSION). Может принимать значения: 1 или 2;
  - «Путь к токену доступа к хранилищу» - путь к файлу с токеном доступа к хранилищу (параметр SECRETS_OPENBAO_TOKEN);
  - «Роль доступа Termidesk» - роль, настроенная на OpenBao, имеющая доступ к

логинам и паролям (параметр SECRETS_OPENBAO_ROLE_NAME);

- «ИД роли доступа» - идентификатор роли доступа (параметр SECRETS_OPENBAO_ROLE_ID);
- «Путь к логину/паролю СУБД» - путь, настроенный на OpenBao для хранения логина и пароля СУБД (параметр SECRETS_OPENBAO_DB_PATH);
- «Путь к логинам/паролям RabbitMQ» - путь, настроенный на OpenBao для хранения логинов и паролей RabbitMQ (параметр SECRETS_OPENBAO_RABBITMQ_PATH);
- «Путь к другим секретам Termidesk» - путь, настроенный на OpenBao для хранения других логинов и паролей Termidesk VDI (параметр SECRETS_OPENBAO_TERMIDESK_PATH);
- «Время кеширования паролей, с» - время (в секундах) хранения пароля, полученного от OpenBao, во внутренней памяти (параметр SECRETS_OPENBAO_CACHE_LIFETIME);
- «Период проверки токена доступа, с» - интервал (в секундах) проверки актуальности токена (параметр SECRETS_OPENBAO_WATCHDOG_INTERVAL);
- «Обновлять токен до его устар., с» - оставшееся время (в секундах) актуальности токена, по достижении которого он будет обновлен (параметр SECRETS_OPENBAO_TTL_DEADLINE);
- «Время жизни токена, с» - время актуальности (в минутах) одноразового токена (параметр SECRETS_OPENBAO_WRAP_TTL);
- «Пространство имён» - пространство имени, заданного на OpenBao (параметр SECRETS_OPENBAO_NAMESPACE);

- «Задание ключа DJANGO»: позволяет переопределить значение ключа DJANGO (параметр DJANGO_SECRET_KEY), создаваемого на этапе установки. Переопределение ключа может понадобиться при его компрометации;
- «Защита подключения к СУБД»: позволяет выбрать тип подключения к СУБД (параметр DBSSL);
- «Тип установки СУБД»: позволяет выбрать тип СУБД, к которой будет подключаться Termidesk VDI (параметр DB_CLUSTER_MODE);
- «Настройка подключения к СУБД»: позволяет настроить параметры подключения к СУБД:
  - «Адрес» - IP-адрес или FQDN СУБД PostgreSQL (параметр DBHOST);
  - «Адрес (узел 2)»: IP-адрес или FQDN дополнительного узла СУБД (параметр DBHOST2);
  - «Адрес (узел 3)»: IP-адрес или FQDN дополнительного узла СУБД (параметр DBHOST3);
  - «Порт» - порт, который используется для соединения с сервером БД (параметр DBPORT);
  - «Имя базы данных» - имя БД (параметр DBNAME);
  - «Имя» - имя пользователя для подключения к БД (параметр DBUSER);
  - «Пароль» - пароль пользователя в открытом виде (параметр DBPASS);
  - «Время жизни подключения, с»: максимально допустимое время (в секундах) существования одного подключения к БД (параметр DB_CONN_MAX_AGE);
  - «Кол-во задач на подключение»: количество фоновых задач, которое может быть выполнено в рамках одного подключения к БД (параметр CELERY_DB_REUSE_MAX);
  - «Таймаут подключения к СУБД, с»: время ожидания (в секундах) подключения к БД (параметр DB_CONN_TIMEOUT);
- «Защита подключения к RabbitMQ/TermideskMQ»: позволяет выбрать тип подключения к брокеру сообщений (параметр RABBITMQ_SSL);
- «Настройка подключения к RabbitMQ/TermideskMQ»: позволяет настроить параметры подключения к брокеру сообщений (параметр RABBITMQ_URL). При запросе пароль

задается в открытом виде;

- «Настройка параметров клиента TermidesMQ»: позволяет настроить параметры клиентской части TermideskMQ для высокодоступной конфигурации:
  - «Идентификатор клиента»: идентификатор пула очередей сообщений (параметр `TMQ_CLIENT_ID`);
  - «Таймаут ожидания ответа от узла, мс»: время ожидания ответа от узла кластера TermideskMQ (параметр `TMQ_TIMEOUT_AWAIT_SENDING_MESSAGE`);
  - «Количество попыток запросов к узлу»: количество попыток выполнения запроса или отправки сообщение к узлу кластера TermideskMQ (параметр `TMQ_PUT_RETRY_COUNT`);
- «Настройки подключения к Fluentd»: позволяет настроить параметры подключения к узлу «Ретранслятора»:
  - «Время кеширования хоста и порта, с»: время (в секундах) кеширования параметров подключения к узлу «Ретранслятора» (параметр `FLUENTD_CACHE`);
  - «Название таблицы в хранилище»: таблица хранения событий фермы Termidesk VDI (параметр `FLUENTD_TABLE`);
  - «Время ожидания подключения, с»: время (в секундах) ожидания подключения к узлу «Ретранслятора» (параметр `FLUENTD_LOGGER_TIMEOUT`);
- «Настройка журналирования»: позволяет настроить параметры журналирования, такие как:
  - «Адрес логгера» (параметр `LOG_ADDRESS`);
  - «Поток (facility) журнала» (параметр `LOG_FACILITY`);
  - «Место хранения журналов» (параметр `LOG_DIR`);
  - «Владелец файлов журналов» (параметр `LOG_OWNER`);
  - «Группа-владелец файлов журналов» (параметр `LOG_GROUP`);
  - «Права доступа к файлам журналов» (параметр `LOG_PERM`);
  - «Число хранимых файлов журналов» (параметр `LOG_DEEP`);
- «Подробность отладочных сообщений в журналах»: позволяет выбрать уровень подробности отладочных сообщений (параметр `LOG_LEVEL`);
- «Аудит обращений к анонимным эндпоинтам API»: позволяет включить или отключить запись событий аудита с анонимным пользователем в БД (параметр `INTERNAL_AUDIT`);
- «Задание токена проверки состояния служб»: позволяет переопределить значение токена проверки состояния служб (параметр `HEALTH_CHECK_ACCESS_KEY`). Переопределение токена может понадобиться при его компрометации;
- «Задание токена проверки метрик служб»: позволяет переопределить значение токена проверки метрики служб (параметр `METRICS_ACCESS_KEY`). Переопределение токена может понадобиться при его компрометации;
- «Изменение GID встроенных администраторов»: позволяет назначить идентификатор группы, использующегося для встроенного домена. Изменение идентификатора может понадобиться, если встроенная в ОС группа администраторов отличается от `astra-admin (1001)` или если нужно предоставить права администрирования Termidesk VDI группе непривилегированных пользователей;
- «Язык сервера по умолчанию»: язык сервера по умолчанию согласно ISO-639-1 (параметр `LANGUAGE_CODE`);
- «Настройки агрегатора»: позволяет переопределить настройки портала «Агрегатор»:
  - «Путь к файлу с сопоставлением имён узлов и FQDN» - путь к файлу `mapping.yaml`, содержащему сопоставление между именами узлов (`NODE_NAME`) «Агрегатора» и их полным доменным именем (FQDN);

- «Режим mTLS сервера Termidesk»: режим mTLS для взаимодействия между компонентами Termidesk VDI (параметр `MTLS_MODE`);
- «Подключения mTLS»: сценарий взаимодействия между компонентами Termidesk VDI по mTLS (параметр `MTLS_CONNECTIONS`);
- «Настройки Брокера сообщений (экспериментальный)»: позволяет переопределить настройки экспериментального «Брокера сообщений TermideskMQ»:
  - «Адрес для подключений»: IP-адрес прослушивания входящих подключений для «Брокера сообщений TermideskMQ» (параметр `TMQ_BASE_ADDRESS`);
  - «Базовый порт для подключений»: базовый номер порта «Брокера сообщений TermideskMQ» для незащищенного подключения (параметр `TMQ_BASE_PORT`).
- «Перезапуск служб» - позволяет выполнить перезапуск служб Termidesk VDI;
- «Сертификаты» - позволяет выполнить настройку сертификатов и ключей:

> Пункт «Серт. для расшифровки JWT-токена» настраивается только на узле с установленным «Универсальным диспетчером» («Портал администратора» и (или) «Портал пользователя») фермы Termidesk VDI.
>
> Пункт «Прив. ключ для подписи JWT-токена» настраивается только на узле портала «Агрегатор» («Агрегатор администратора» и (или) «Агрегатор пользователя»).
>
> Оставшиеся пункты могут быть настроены на обоих узлах индивидуально.

  - «Сертификат Health Check» - путь к сертификату для защищенного подключения к API проверки состояния (параметр `HEALTH_CHECK_CERT`);
  - «Секр. ключ Health Check» - путь к ключу для защищенного подключения к API проверки состояния (параметр `HEALTH_CHECK_KEY`);
  - «Сертификат Postgres mTLS» - путь к сертификату для защищенного подключения к СУБД (параметр `DBCERT`);
  - «Секр. ключ Postgres mTLS» - путь к ключу для защищенного подключения к СУБД (параметр `DBKEY`);
  - «Серт. промеж. ЦС Postgres mTLS» - путь к корневому и промежуточным сертификатам mTLS для защищенного подключения к СУБД (параметр `DBCHAIN`);
  - «Сертификат OpenBao начального mTLS» - путь к сертификату для начального защищенного подключения к OpenBao (параметр `SECRETS_OPENBAO_CLIENT_CERT`);
  - «Секр. ключ OpenBao начального mTLS» - путь к ключу для начального защищенного подключения к OpenBao (параметр `SECRETS_OPENBAO_CLIENT_KEY`);
  - «Серт. промеж. ЦС OpenBao нач. mTLS» - путь к корневому и промежуточным сертификатам mTLS для начального защищенного подключения к OpenBao (параметр `SECRETS_OPENBAO_SERVER_CERT`);
  - «Путь к серт. для втор. mTLS с OpenBao»: путь к клиентскому сертификату SSL/TLS для вторичного защищенного подключения к OpenBao (параметр `SECRETS_OPENBAO_PKI_CERTS`);
  - «Осн. серт. для расшифровки JWT-токена» - путь к сертификату для получения значения JWT-токена портала «Агрегатор» (параметр `AGGREGATOR_JWT_SSL_CERT`);
  - «Рез. серт. для расшифровки JWT-токена» - путь к резервному сертификату для получения значения JWT-токена портала «Агрегатор» (параметр `AGGREGATOR_JWT_SSL_CERT_SECOND`);
  - «Секр. ключ для подписи JWT-токена» - путь к ключу для подписи JWT-токена портала «Агрегатор» (параметр `AGGREGATOR_JWT_SSL_KEY`);

- «Сертификат ЦС сервера RA» - путь к серверному сертификату SSL/TLS для проверки подключения к «Удаленному помощнику» (REMOTE_ASSISTANT_SERVER_CA);
- «Сертификат RabbitMQ mTLS» - путь к клиентскому сертификату SSL/TLS для защищенного подключения к RabbitMQ (CELERY_BROKER_CERT);
- «Секр.ключ RabbitMQ mTLS» - путь к клиентскому ключу SSL/TLS для защищенного подключения к RabbitMQ (CELERY_BROKER_KEY);
- «Серт. ЦС RabbitMQ mTLS» - путь к корневому сертификату ЦС SSL/TLS для защищенного подключения к RabbitMQ (CELERY_BROKER_CA);
- «Сертификат службы TermideskMQ»: путь к серверному сертификату mTLS для «Брокера сообщений TermideskMQ» (параметр TMQ_SERVER_CERT);
- «Секр. ключ службы TermideskMQ»: путь к ключу для серверного сертификата mTLS для «Брокера сообщений TermideskMQ» (параметр TMQ_SERVER_KEY);
- «Серт. ЦС службы TermideskMQ»: путь к корневому сертификату mTLS для «Брокера сообщений TermideskMQ» (параметр TMQ_SERVER_CA);
- «Публичный ключ ws-proxy»: путь к открытому ключу id_rsa.pub. Явно задавать путь следует только при использовании внешнего хранилища (WSPROXY_PUB_KEY_FILE);
- «Секретный ключ ws-proxy»: путь к озакрытому ключу id_rsa. Явно задавать путь следует только при использовании внешнего хранилища (WSPROXY_PRIV_KEY_FILE);
- «Клиентский сертификат mTLS»: путь к клиентскому сертификату mTLS для защищенного подключения. Используется для взаимной аутентификации сервера Termidesk VDI с другими компонентами (параметр MTLS_CLIENT_CERT);
- «Клиентский секр.ключ mTLS»: путь к клиентскому ключу mTLS для защищенного подключения. Используется для взаимной аутентификации сервера Termidesk VDI с другими компонентами (параметр MTLS_CLIENT_KEY);
- «Клиентский серт. ЦС mTLS»: путь к корневому сертификату ЦС mTLS для защищенного подключения. Используется для взаимной аутентификации сервера Termidesk VDI с другими компонентами (параметр MTLS_CLIENT_CA);
- «Файл с доверенными сертификатами»: путь к файлу с доверенным корневым сертификатом. Задается для настройки работы с сертификатами собственных ЦС (параметр REQESTS_CA_BUNDLE).

Утилита scramble

Утилита scramble предназначена для получения преобразованных значений для параметров конфигурационного файла termidesk.conf.

Вызов утилиты выполняется командой:

```
sudo /opt/termidesk/bin/scramble
```

Вызов справки по утилите выполняется командой:

```
sudo /opt/termidesk/bin/scramble -h
```

Параметры команды приведены в таблице (см. таблицу Параметры команды scramble).

Таблица 178. Параметры команды scramble

Параметр	Значение по умолчанию	Описание

`--value`	`Не задано`	Получение преобразованного значения. По умолчанию используется алгоритм AES-256 с увеличенным числом итераций преобразования, если не задан другой в параметре `--type`.
		
		Пример использования:
		
		• с алгоритмом по умолчанию:
		
		`/opt/termidesk/bin/scramble --value <значение>`
		
		• с указанием алгоритма:
		
		`/opt/termidesk/bin/scramble --value <значение> --type <алгоритм>`
		
		Если значение указывается в формате ключа (значение предваряется символом «-»), то следует изменить его передачу в параметр `--value:`
		
		`/opt/termidesk/bin/scramble --value=<-значение> --type AES256`

Параметр	Значение по умолчанию	Описание

--config	/etc/opt/termidesk-vdi/	Путь к каталогу, в котором расположены конфигурационные файлы termidesk.conf и cookie-файл termidesk.cookie, используемый как вектор преобразования.
		
		При изменении места хранения указанных файлов требуется передавать в утилиту scramble значение нового каталога, если необходимо получить верное преобразованное значение в параметре --value.
		
		Пример использования:
		
		`/opt/termidesk/bin/scramble --config <путь_к_каталогу> --value <значение>`
		
		Пример: предположим, что на узле с «Универсальным диспетчером» появились два каталога, хранящих его конфигурационные файлы termidesk.conf и termidesk.cookie:
		
		• /etc/opt/termidesk-vdi - содержит неактуальные параметры конфигурации;
		• /etc/opt/termidesk-vdi2 - содержит актуальные параметры конфигурации, которые должны использоваться «Универсальным диспетчером».
		
		В этом случае для того, чтобы получить верное преобразованное значение для какого-либо из параметров /etc/opt/termidesk-vdi2/termidesk.conf, может потребоваться указать утилите, какой каталог она должна использовать при работе:
		
		`/opt/termidesk/bin/scramble --config /etc/opt/termidesk-vdi2/ --value <значение>`
		
		Необязательный параметр, поскольку значение каталога передается на этапе установки. Прямое указание параметра может потребоваться в целях тестирования работы Termidesk VDI.

--type	AES256_V2	Указание алгоритма преобразования значения. Возможные значения: • AES256 - преобразование по алгоритму AES-256; • AES256_V2 - преобразование по алгоритму AES-256 с увеличенным числом итераций преобразования

НЕШТАТНЫЕ СИТУАЦИИ

Возможные неисправности при работе с Termidesk VDI и способы их устранения приведены в таблице (см. таблицу Перечень возможных нештатных ситуаций).

Таблица 179. Перечень возможных нештатных ситуаций

Индикация	Описание	Возможное решение
Ошибка: «СБОЙ: оставшиеся слоты подключений зарезервированы для подключений суперпользователя (не для репликации)»	Ошибка возникает при попытке авторизации на Termidesk VDI	Изменить максимальное количество подключений в настройках БД: изменить значение `max_connections` в конфигурационном файле `/etc/postgresql/<версия>/main/postgresql.conf` в бОльшую сторону
Ошибка: «OpenNebula Error 256 User coulnd’t authenticated, abording call»	Ошибка возникает при попытке добавления поставщика ресурсов ПК СВ Брест в «Портале администратора» Termidesk VDI	Необходимо указать правильный путь к файлу `keytab` и внести значения параметра «Токен» непосредственно в интерфейсе ПК СВ Брест
Ошибка: «OpenNebula error 256 User could’t be authericated»	Ошибка возникает при попытке добавления поставщика ресурсов ПК СВ Брест	Необходимо создать новое значение параметра «Токен» для пользователя непосредственно в интерфейсе ПК СВ Брест
Ошибка: «SSL: WRONG_VERSION_NUMBER] wrong version number (_ssl.c:1056)»	Ошибка возникает, если сервер поставщика ресурсов не поддерживает SSL	Необходимо отредактировать поставщика ресурсов, выставив параметру «Использовать SSL» значение «Нет»
Нельзя заполнить поле «Кластер данных», невозможно сохранить шаблон	Ошибка возникает при попытке создания шаблона РМ для поставщика ресурсов VMware поле «Кластер данных» неактивно, невозможно сохранить шаблон	На платформе виртуализации VMware необходимо объявить кластер хранилища данных (Datastore Cluster)
Ошибка: «kinit: Client 'HTTP/termidesk.local@LOCAL' not found in Kerberos database while getting initial credentials»	Ошибка возникает при добавлении или редактировании домена аутентификации FreeIPA	Необходимо создать указанную учетную запись на КД FreeIPA
Ошибка: «'list' object has no attribute 'get'»	Ошибка возникает при разворачивании ВМ из шаблона, в котором указанно больше одного диска	В шаблоне при первоначальном разворачивании ВМ должен быть указан только один диск

Индикация	Описание	Возможное решение

Ошибки при установке пакета «Невозможно найти пакет» или «Неудовлетворенные зависимости»	Ошибка возникает при попытке установить пакет в ОС	Необходимо убедиться, что в файле `/etc/apt/sources.list` заданы и не закомментированы источники получения пакетов (репозитории), затем обновить списки пакетов:
		`sudo apt update`
		После этого нужно вновь выполнить команду установки пакета.
		Для решения проблемы с неудовлетворенными зависимостями, помимо подключения репозиториев в файле `/etc/apt/sources.list`, можно воспользоваться командой:
		`sudo apt -f install`
		Ключ `-f` используется для попытки исправить нарушенные зависимости пакетов

Ошибка:
«Проверка не пройдена. ValueError: Метаданные не получены. Проверьте URL Метаданных и доступность сервера»
	При активации параметра «Проверка SSL» для домена аутентификации SAML тест соединения завершается с ошибкой	Необходимо настроить работу с сертификатами при получении метаданных от домена аутентификации SAML. Для этого:
		• добавить параметр `REQUESTS_CA_BUNDLE` в файле `termidesk.conf`. В параметре нужно указать путь к файлу с доверенным корневым сертификатом. Пример:
		`REQUESTS_CA_BUNDLE='/etc/ssl/certs/ca.crt'`
		• выполнить перезапуск службы `termidesk-vdi`:
		`sudo systemctl restart termidesk-vdi`

Индикация	Описание	Возможное решение
Ошибка: «Для фонда значение политики "Действие при выходе пользователя из ОС" не может быть "Удалять рабочее место"»	Ошибка возникает при создании фонда РМ Метапоставщика через мастерпубликации фонда	Необходимо перейти в настройки политик указанного в ошибке сервисного фонда РМ и для политики «Действие при выходе пользователя из ОС» выбрать значение «Не задано». Затем вновь перейти к созданию фонда РМ Метапоставщика
В записях журнала «Универсального диспетчера» отражен IP-адрес портала «Агрегатор», а не IP-адрес пользователя	При подключении пользователя к ресурсу фермы Termidesk VDI через портал «Агрегатор» в журнале узла «Универсального диспетчера» фиксируется запись с указанием IP-адреса портала «Агрегатор», а не IP-адресом пользователя	Необходимо перейти «Системные параметры - Системные настройки - Безопасность» и включить параметр «Использовать анонсируемый IP клиента»
РМ не вводится в домен MS AD	Учтена запись РМ не создается в домене MS AD, несмотря на то, что используется параметры гостевых ОС с вводом в домен	Необходимо убедиться, что параметр OU в параметрах гостевых ОС задан правильно (см. подразделы **Параметры гостевой ОС Linux** и **Параметры гостевой ОС Microsoft Windows**)
Учетная запись РМ не удаляется из домена MS AD	Учетная запись РМ не удаляется из домена MS AD, несмотря на то, что используется функционал удаления учетной записи при удалении фонда РМ	Необходимо убедиться, что параметр OU в параметрах гостевых ОС задан правильно (см. подразделы **Параметры гостевой ОС Linux** и **Параметры гостевой ОС Microsoft Windows**)
Ошибка: «Информация о доступном месте хранилища не предоставлена поставщиком ресурсов»	Ошибка возникает при публикации связанных клонов через поставщика ресурсов oVirt (или zVirt, «РЕД Виртуализация»), если информация о свободном месте хранилища не приходит на сервер Termidesk VDI	Необходимо убедиться, что на используемой платформе виртуализации хранилище доступно
Ошибка: «Данный шаблон не поддерживается выбранным терминальным сервером» или «The template is not supported by the terminal server»	Ошибка возникает при создании шаблона РМ для терминального сервера	Необходимо убедиться, что выбран верный шаблон РМ терминального сервера: • если используется терминальный сервер STAL, то нужно выбрать шаблон «Рабочий стол STAL» или «Приложение STAL»; • если используется терминальный сервер MS RDS, то нужно выбрать шаблон «Рабочий стол RDS» или «Приложение RDS»
Ошибка: «Достигнуто максимальное количество устаревших шаблонов публикаций» в разделе «Публикации» фонда РМ	При попытке опубликовать фонд РМ отображается подсказка «Достигнуто максимальное количество устаревших шаблонов публикаций»	Достигнуто заданное в политике «Максимальное количество устаревших шаблонов связанных клонов» количество шаблонов для фонда РМ. Необходимо удалить некоторые существующие РМ или задать новое значение политике

Индикация	Описание	Возможное решение

Ошибка:
 	
«Incorrect MTLS based "Device auth" feature setup»
	Ошибка возникает после установки Termidesk VDI и попытке перейти к веб-порталу Termidesk VDI	Необходимо удалить использование экспериментального параметра `experimental.deviceauth.enabled`, если веб-сервер не настроен на использование mTLS:
		
		• перейти в интерфейс командной строки;
		• переключиться на пользователя `termidesk`:
		
		`sudo -u termidesk bash`
		
		• отключить использование параметра `experimental.deviceauth.enabled`:
		
		`/opt/termidesk/sbin/termidesk-vdi-manage tdsk_config set --key experimental.deviceauth.enable --value False`

Для поставщика ресурсов zVirt не тиражируются ВМ	Тиражирование ВМ аварийно завершается на финальной стадии подготовки (в момент создания снимка ВМ)	Необходимо увеличить время ожидания в настройках поставщика ресурсов (см. подраздел **Добавление платформы zVirt**)
Не удается подключиться к автономной машине после смены ее MAC-адреса	Подключение к автономной машине в составе фонда Метапоставщика неуспешно после смены MAC-адреса машины	Необходимо выполнить повторное подключение
При перезагрузке РМ теряются доверительные отношения с доменом MS AD	При перезагрузке РМ (например, по расписанию) и возврату к начальному состоянию теряются доверительное отношения с доменом MS AD	Необходимо убедиться, что для РМ используются параметры гостевых ОС Windows с доменом MS AD (см. подраздел **Параметры гостевой ОС Microsoft Windows**). При утере доверительных отношений «Агент виртуального рабочего места» автоматически отправит ВМ в перезагрузку, после чего доверительные отношения восстановятся
Ошибка: «VM не является шаблоном. Выберите корректный шаблон или преобразуйте VM в шаблон»	Ошибка возникает при публикации фонда РМ для поставщика ресурсов VMware vSphere	Ошибка означает, что выбранный шаблон РМ представляет собой ВМ, а не шаблон. Необходимо выбрать корректный шаблон РМ или преобразовать ВМ в шаблон

Индикация	Описание	Возможное решение
Не удается подключиться к хранилищу паролей	При использовании хранилища паролей через некоторое время пропадает подключение к нему. В журнале сервера Termidesk VDI при этом появляются события вида: «Cannot complete login due to an incorrect user name or password»	Необходимо на узле с установленным хранилищем паролей (например, Hashicorp Vault) увеличить время актуальности токена в параметре `secret_id_ttl`, установив для него значение `999d`

ТЕРМИНЫ

Агрегатор администратора

Веб-интерфейс управления «Агрегатором». Устанавливается из пакета `termidesk-vdi` при выборе пункта «Агрегатор администратора»

Агрегатор пользователя

Веб-интерфейс пользователя для получения ресурсов, предоставляемых «Агрегатором». Устанавливается из пакета `termidesk-vdi` при выборе пункта «Агрегатор пользователя»

Компонент «Агент»

Самостоятельный компонент, отвечающий за контролируемую доставку РМ, взаимодействие с «Универсальным диспетчером» и «Менеджером рабочих мест». Собирательное название для следующих компонентов Termidesk VDI:

- «Агент виртуального рабочего места»;
- «Агент узла виртуализации»;
- «Сессионный агент»;
- «Видеоагент»;
- «Агент виртуальных смарт-карт».

Компонент «Агент виртуальных смарт-карт»

Компонент Termidesk VDI. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление подключенных к пользовательской рабочей станции смарт-карт в ВРМ

Компонент «Агент виртуального рабочего места»

Компонент Termidesk VDI. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет взаимодействие с «Универсальным диспетчером», конфигурирует ВРМ, фиксирует действия пользователя, реализует передачу управляющих сообщений

Компонент «Агент узла виртуализации»

Компонент Termidesk VDI. Устанавливается на узел виртуализации, взаимодействует с гипервизором через модуль `libvirt`

Базовое виртуальное рабочее место

Также: золотой образ, базовый образ. Подразумевает собой образ диска ВМ с предустановленным прикладным ПО и установленным «Агентом виртуального рабочего места». Этот образ далее будет использоваться для создания ВРМ для пользователей

Балансировщик нагрузки

Самостоятельный компонент, отвечающий за распределение нагрузки на множество «Универсальных диспетчеров» и «Шлюзов»

Компонент «Видеоагент»

Компонент Termidesk VDI. Устанавливается в гостевую ОС при подготовке базового ВРМ.

Выполняет перенаправление видеокамеры с пользовательской рабочей станции в ВРМ

Виртуальное рабочее место

Развернутая на ВМ ОС с установленным «Агентом виртуального рабочего места» и необходимым прикладным ПО. Подключение к ВРМ происходит через протоколы удаленного доступа

Рабочее место

Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа. Под РМ подразумеваются как ВРМ, так и терминальный доступ или доступ к опубликованным на терминальном сервере приложениям

Гостевая ОС

ОС, функционирующая на ВМ

Группы рабочих мест

Функциональное объединение множества фондов РМ по определенному признаку

Домен аутентификации

Способ проверки субъектов и их полномочий

Компонент «Менеджер рабочих мест»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за взаимодействие с поставщиком ресурсов и управления жизненным циклом РМ, включая создание, настройку, запуск, отключение и удаление. Является обработчиком фоновых задач. Устанавливается из пакета `termidesk-vdi`. Наименование служб после установки: `termidesk-celery-beat.service` и `termidesk-celery-worker.service`

Компонент «Оркестратор»

Компонент Termidesk VDI. Самостоятельный компонент, отвечающий за согласованную работу всех компонентов программного комплекса при децентрализованном развертывании, для нужд отказоустойчивости и комплексирования с облачными службами

Поставщик ресурсов

ОС, платформа виртуализации или терминальный сервер (MS RDS/STAL), предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов РМ

Протокол доставки

Поддерживаемый в Termidesk VDI протокол удаленного доступа к РМ

Связанный клон

Способ организации ВРМ на основе единого образа, с возможностью экономии дискового пространства, за счет технологии «копирование при записи», и ускорения операций возврата к базовому состоянию, установки дополнительного ПО и обновлений

Компонент «Сессионный агент»

Компонент Termidesk VDI. Устанавливается на терминальный сервер (MS RDS/STAL), активирует возможность множественного доступа пользователей к удаленным рабочим столам и приложениям

Компонент «Универсальный диспетчер»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им РМ и контроля доставки РМ. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки:

`termidesk-vdi.service `

Компонент «Шлюз»

Самостоятельный компонент, отвечающий за туннелирование протоколов доставки, использующих транспортный протокол TCP

Компонент «Сервер терминалов Astra Linux»

Компонент Termidesk VDI. Также: STAL. Обеспечивает подключение пользовательских рабочих станций к РМ с ОС Astra Linux Special Edition через сеанс удаленного терминала

Портал «Агрегатор»

Роль компонента «Универсальный диспетчер», доступная при установке Termidesk VDI. Является единой точкой входа для получения ресурсов пользователями, предоставляет им объединенный список приложений и РМ с ферм Termidesk

Портал администратора

Предоставляет веб-интерфейс для управления Termidesk VDI и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API

Портал пользователя

Предоставляет пользовательский веб-интерфейс Termidesk VDI (без доступа к функциям управления) и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API

Портал универсальный

Предоставляет функции обоих вариантов порталов, как пользовательского, так и административного

Ключ

Последовательность псевдослучайных чисел, сгенерированная особым образом

Сертификат

Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу

Ферма

Логическое объединение узлов, взаимодействующих с одной БД

Фонд рабочих мест

Совокупность подготовленных РМ для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей

Шаблон рабочего места

Параметры конфигурации рабочего места для использования в фонде РМ

СОКРАЩЕНИЯ

БД	База данных
ВМ	Виртуальная машина
ВРМ	Виртуальное рабочее место
ЗПС	Замкнутая программная среда
ИД	Идентификатор
КД	Контроллер домена

ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПК СВ Брест	Программный комплекс «Средства виртуализации «Брест»
ПО	Программное обеспечение
РМ	Рабочее место
СУБД	Система управления базами данных
УЗ	Учетная запись
ЦП	Центральный процессор
ЦПУ	Центральное процессорное устройство
ЦС	Центр сертификации
ЭЦП	Электронная цифровая подпись
ACL	Access Control List (список контроля доступа)
AES	Advanced Encryption Standard (стандарт симметричного шифрования данных)
ALD	Astra Linux Directory (единое пространство пользователей)
ALSA	Advanced Linux Sound Architecture (программная архитектура и набор драйверов для работы со звуком в ОС на базе ядра Linux)
AMQP	Advanced Message Queueing Protocol (открытый протокол для передачи сообщений между компонентами системы)
AMQPS	Расширение протокола AMQP с использованием TLS для шифрования
API	Application Programming Interface (интерфейс прикладного программирования)
CEF	Common Event Format (открытый текстовый формат для стандартизации сообщений о событиях безопасности)
CN	Common Name (общее имя)
CPU	Central Processing Unit (центральный процессор)
CredSSP	Credential Security Service Provider (технология единого входа с помощью услуг безопасности)
CRUD	Create Read Update Delete (акроним основных операций с информацией в БД)
CSR	Certificate Signing Request (зашифрованный запрос на выпуск сертификата)
CUPS	Common Unix Printing System (система печати Unix)
DHCP	Dynamic Host Configuration Protocol (протокол назначения сетевого адреса)

DN	Domain Name (доменное имя)
DNS	Domain Name System (система доменных имен)
Email	Electronic mail (адрес электронной почты)
ETCD	Distributed key-value store (распределенное хранилище типа «ключ-значение»)
FQDN	Fully Qualified Domain Name (полностью определенное имя домена)
FreeIPA	Free Identity, Policy and Audit (открытое решение по безопасности Linux-систем)
GC	Global Catalog (глобальный каталог)
GID	Group Identification Data (идентификатор группы)
GMT	Greenwich Mean Time (среднее время по Гринвичу)
GPU	Graphics Processing Unit (графический процессор)
GSLB	Global Server Load Balancing (технология распределения сетевого трафика между серверами, находящимися в разных географических точках)
GSSAPI	Generic Security Services API (стандартизированный программный интерфейс для доступа к сервисам безопасности)
GUSID	Global Unique Session ID (глобальный уникальный сессионный идентификатор)
HTML	Hypertext Markup Language (язык гипертекстовой разметки)
HTTP	Hypertext Markup Language (язык гипертекстовой разметки)
HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
ID	Identification Data (идентификатор)
IdP	Identity Provider (сервис, управляющий идентификационной информацией)
IP	Internet Protocol (межсетевой протокол)
JSON	JavaScript Object Notation (стандартный текстовый формат для структурированных данных)
JWKS	JSON Web Key Set (набор открытых ключей для проверки веб-токена)
JWT	JSON Web Token (открытый стандартдля создания токенов доступа)
KVM	Kernel Virtual Machine (виртуальная машина на основе ядра, технология аппаратной виртуализации)
LDAP	Lightweight Directory Access Protocol (легковесный протокол доступа к службам каталогов)
LDAPS	Lightweight Directory Access Protocol over SSL/TSL (расширение протокола LDAP)

MAC	Media Access Control (уникальный идентификатор сетевого устройства)
MS AD	Microsoft Active Directory (службы каталогов Microsoft)
MS RDS	Remote Desktop Services (службы удаленного рабочего стола Microsoft)
MS RDSH	Remote Desktop Session Host (хост сеансов удаленных рабочих столов)
mTLS	Multiplexed Transport Layer Security (протокол, основанный на TLS с усиленной безопасностью)
NFS	Network File System (протокол сетевого доступа к файлам)
NLA	Network Level Authentication (аутентификация на сетевом уровне)
NTLM	NT LAN Manager (семейство протоколов безопасности от Microsoft)
OAuth	Open Authorization (открытый стандарт и протокол делегированной авторизации)
OIDC	OpenID Connect (протокол аутентификации, построенный поверх стандарта OAuth 2.0)
OTP	One-Time Password (одноразовый пароль)
OU	Organizational Unit (организационная единица)
PAM	Pluggable Authentication Module (подключаемый модуль аутентификации)
PDF	Portable Document Format (открытый формат электронных документов)
PID	Product ID (идентификатор продукта)
PKCS	Public Key Cryptography Standards (стандарты криптографии с открытым ключом)
PKI	Public Key Infrastructure (система управления цифровыми сертификатами и ключами)
PKINIT	Public Key Cryptography for Initial Authentication (механизм Kerberos, позволяющий использовать сертификаты X.509)
PnP	Plug and Play («подключи и работай»)
PPD	PostScript Printer Description (описание возможностей конкретной модели принтера)
RADIUS	Remote Authentication Dial-In User Service (протокол, предоставляющий функции аутентификации, авторизации и учета)
RDP	Remote Desktop Protocol (протокол удаленного рабочего стола)
RDS	Remote Desktop Services (службы удаленного рабочего стола Microsoft)
REDIS	REmote DIctionary Service (резидентная СУБД)
REST	Representational State Transfer (программная архитектура, определяющая условия работы API)
RFC	Request for Comments (рабочее предложение Интернет)

RPC	Remote Procedure Call (удаленный вызов процедур)
RSA	Rivest, Shamir and Adleman (криптографический алгоритм с открытым ключом)
RTSP	Real-Time Streaming Protocol (протокол для управления потоковой передачей данных)
SAM	Security Account Manager (диспетчер учетных записей безопасности)
SAML	Security Assertion Markup Language (открытый стандарт обмена данными аутентификации)
SASL	Simple Authentication and Security Layer (фреймворк для аутентификации и обеспечения безопасности)
SCSI	Small Computer System Interface (набор стандартов для физического подключения и передачи данных между компьютерами и периферийными устройствами)
SMB	Server Message Block (протокол для удалённого доступа к сетевым ресурсам)
SMTP	Simple Mail Transfer Protocol (сетевой протокол для передачи электронной почты)
SMTPS	Simple Mail Transfer Protocol Secure (защищенная версия протокола SMTP)
SPICE	Simple Protocol for Independent Computing Environments (простой протокол для независимой вычислительной среды)
SRV	Service Record DNS (служебная запись в DNS)
SSL	Secure Sockets Layer (криптографический протокол)
SSO	Single Sign-On (технология единого входа)
SSSD	System Security Services Daemon (системная служба, управляющая доступом к удаленным каталогам и механизмам аутентификации)
STAL	Terminal Server Astra Linux (компонент «Сервер терминалов Astra Linux»)
STUN	Session Traversal Utilities for NAT (сетевой протокол, позволяющий определить внешний IP-адрес и другие параметры)
SUID	Unique Session ID (уникальный сессионный идентификатор, то же самое, что GUSID)
TCP	Transmission Control Protocol (протокол управления передачей)
TERA	Termidesk Remote Access protocol (протокол удаленного доступа разработкиООО «УВЕОН»)
TLS	Transport Layer Security (протокол защиты транспортного уровня)
TOTP	Time-based One Time Password (метод авторизации пользователя)
UDP	User Datagram Protocol (протокол пользовательских датаграмм)

UPN	User Principal Name (уникальное имя пользователя в формате адреса электронной почты)
URI	Uniform Resource Identifier (унифицированный идентификатор ресурса)
URL	Uniform Resource Locator (унифицированный указатель ресурса)
URSI	Unique Resource Start ID (уникальный идентификатор запуска ресурса)
USB	Universal Serial Bus (последовательный интерфейс для подключения периферийных устройств)
UUID	Universally Unique Identifier (уникальный идентификатор)
VDI	Virtual Desktop Infarsticture (инфраструктура виртуальных рабочих столов)
vGPU	Virtual Graphics Processing Unit (виртуальный графический процессор)
VID	Vendor ID (идентификатор производителя)
VLAN	Virtual Local Area Network (виртуальная локальная сеть)
VMSD	Virtual Machine Snapshot Database (БД всех созданных снимков ВМ)
VPN	Virtual Private Network (технология для зашифрованного безопасного соединения)
VRRP	Virtual Redundancy Routing Protocol (сетевой протокол виртуального резервирования маршрутизаторов, предназначенный для увеличения доступности)
VxLAN	Virtual Extensible LAN (технология сетевой виртуализации)
WebDAV	Web Distributed Authoring and Versioning (расширение протокола HTTP, превращающее веб-сервер в сетевое хранилище)
WebRTC	Web Real-Time Communications (открытый проект для организации передачи потоковых данных)
WS	WebSocket (двунаправленный протокол, позволяющий клиенту установить связь с сервером)
WSS	WebSocketSecure (двунаправленный протокол, позволяющий клиенту установить защищенную связь с сервером)
X.509	Стандарт для инфраструктуры открытого ключа
XPS	XML Paper Specification (открытый графический формат фиксированной разметки на базе XML)
2FA	Two-Factor Authentication (двухфакторная аутентификация)

СЛЕТ.10001-01 90 03. РУКОВОДСТВО АДМИНИСТРАТОРА. ГРАФИЧЕСКИЙ ИНТЕРФЕЙС УПРАВЛЕНИЯ ПРОГРАММНЫМ КОМПЛЕКСОМ

ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ

Назначение документа

Настоящий документ является третьей частью руководства администратора на программный комплекс «Диспетчер подключений виртуальных рабочих мест Термидеск» (далее - Termidesk VDI, Termidesk VDI).

Документ описывает общие принципы работы с графическим интерфейсом Termidesk VDI. Для того чтобы получить информацию об установке программного комплекса, необходимо обратиться к первой части руководства администратора - СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса». Для того чтобы получить информацию о настройке программного комплекса, взаимодействии компонентов и настройки отдельного функционала необходимо обратиться ко второй части руководства администратора - СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

Типографские соглашения

Приняты следующие типографские соглашения:

- `моноширинный шрифт` – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk VDI, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

ДОСТУП К ВЕБ-ИНТЕРФЕЙСУ

Доступ веб-интерфейсу осуществляется из веб-браузера по протоколу HTTPS с указанием URL-адреса подключения.

Для подключения должны использоваться веб-браузеры с поддержкой спецификации W3C HTML5: Яндекс.Браузер версии 15.9 и выше, Google Chrome версии 46 и выше, Mozilla Firefox версии 41 и выше.

Минимально необходимое разрешение экрана монитора для работы с веб-интерфейсом - 1366x768 пикселей.

При наличии только домена аутентификации с типом «Встроенный» на странице подключения нужно заполнить экранные поля:

- «Имя пользователя» – идентификатор субъекта с ролью «Администратор»;
- «Пароль» – набор символов, подтверждающий назначение полномочий.

При последующих сеансах входа после добавления нового домена аутентификации потребуется заполнить дополнительное экранное поле:

- «Способ входа» – выбор домена аутентификации для входа в систему.

В Termidesk VDI версии 7.0 основной интерфейс был изменен. Интерфейс, доступный в более ранних версиях, более недоступен.

ТИПЫ ВЕБ-ИНТЕРФЕЙСА TERMIDESK И ИЗМЕНЕНИЕ ФОНА

Типы веб-интерфейса

В Termidesk VDI определены следующие типы веб-интерфейса:

- «Портал администратора»: предоставляет веб-интерфейс для управления Termidesk VDI и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API;
- «Портал пользователя»: предоставляет пользовательский веб-интерфейс Termidesk VDI (без доступа к функциям управления) и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API;
- «Портал универсальный»: предоставляет функции обоих вариантов - и «Портала администратора», и «Портала пользователя». При этом активируется доступ ко всем модулям документации по командам REST API, предоставляемым интерфейсом Swagger.

Доступный тип веб-интерфейса определяется на этапе установки Termidesk VDI.

Нажатие на идентификатор пользователя в правом верхнем углу веб-интерфейса инициирует открытие выпадающего списка, в котором осуществляется выбор для перехода к «Порталу пользователя» («Пользовательский режим») или «Порталу администратора» («Панель управления»).

При установленном типе «Портал администратора» или «Портал универсальный» в левой части веб-интерфейса Termidesk VDI находится панель, содержащая список основных функций:

- «Обзор»;
- «Рабочие места»;
- «Инфраструктура»;
- «Журналы»;
- «Системные параметры»;
- «Лицензия».

Изменение фона веб-интерфейса

Для изменения фона веб-интерфейса Termidesk VDI нужно перейти «Системные параметры - Системные настройки» затем выбрать раздел «Брендирование» (см. подраздел **Брендирование Termidesk VDI** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»).

РАБОТА С ОСНОВНЫМИ ФУНКЦИЯМИ ВЕБ-ИНТЕРФЕЙСА

Функции системной панели

Системная панель представляет собой фиксированную область в верхней части веб-интерфейса, предназначенную для отображения служебной информации и элементов управления (см. рисунок Системная панель в графическом интерфейсе управления Termidesk).

Рисунок 102. Системная панель в графическом интерфейсе управления Termidesk

Системная панель представлена следующими элементами:

- элемент (1): скрывает или отображает список функций в левой части веб-интерфейса;
- элемент (2): отображает сведения о текущей версии компонента «Универсальный диспетчер»;
- элемент (3): отображает заданное наименование компонента «Универсальный диспетчер». Для просмотра сведений о текущем подключении нужно нажать на наименование компонента. При этом в окне «Параметры подключения» будут отображены сведения о текущем подключении (см. рисунок Окно сведений о параметрах текущего подключения):
  - «Имя фермы» - наименование фермы компонента «Универсальный диспетчер»;
  - «Доменное имя сервера» - FQDN фермы компонента «Универсальный диспетчер»;
  - «Имя портала» - идентификатор узла компонента «Универсальный диспетчер»;
  - «IP-адрес» - IP-адрес фермы компонента «Универсальный диспетчер»;
- элемент (4): позволяет выбрать язык отображения веб-интерфейса;
- элемент (5): позволяет выбрать тему оформления графического интерфейса;
- элемент (6): позволяет выбрать тип веб-интерфейса или выполнить выход из веб-интерфейса.

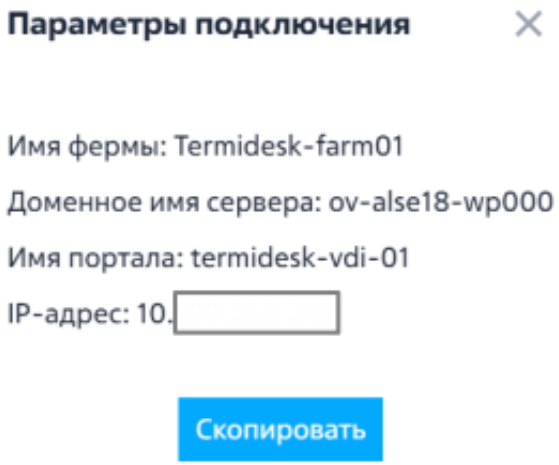


Рисунок 103. Окно сведений о параметрах текущего подключения

Функция «Обзор»

При нажатии в левой части веб-интерфейса на функцию «Обзор», визуализируется краткое представление основных параметров, характеризующих доставку рабочего места (РМ).

В графических блоках функции «Обзор» представлены следующие элементы (см. рисунок Окно функции «Обзор» в графическом интерфейсе управления Termidesk), перенаправляющие на соответствующие процедуры:

- «Рабочие места» – общее число созданных РМ во всех фондах, в том числе назначенные РМ, созданные и размещенные в кеше, и РМ, сигнализирующие об ошибках;
- «Поставщики» – суммарное число поставщиков ресурсов для размещения фондов РМ, в том числе активных поставщиков ресурсов и находящихся в режиме техобслуживания, а также суммарное количество шаблонов РМ, использующих поставщиков ресурсов;
- «Инфраструктура» - диаграмма состояния компонентов Termidesk VDI с распределением по ролям:
  - «Диспетчер подключений» - число и состояние установленных компонентов «Универсальный диспетчер»;
  - «Менеджеры ВРМ» - число и состояние установленных компонентов «Менеджер рабочих мест»;
  - «Порталы» - число и состояние установленных порталов;
  - «Шлюз» - число и состояние установленных компонентов «Шлюз».

Также представлена следующая статистика:

- «Распределение пользователей» – диаграмма общего числа пользователей Termidesk VDI с количественным распределением по доменам аутентификации;
- «Конкурентные соединения» – диаграмма активных подключений относительно максимально допустимых.

В графическом интерфейсе Termidesk VDI термины «рабочее место» и «фонды рабочих мест» относятся к РМ и фондам РМ, соответственно.

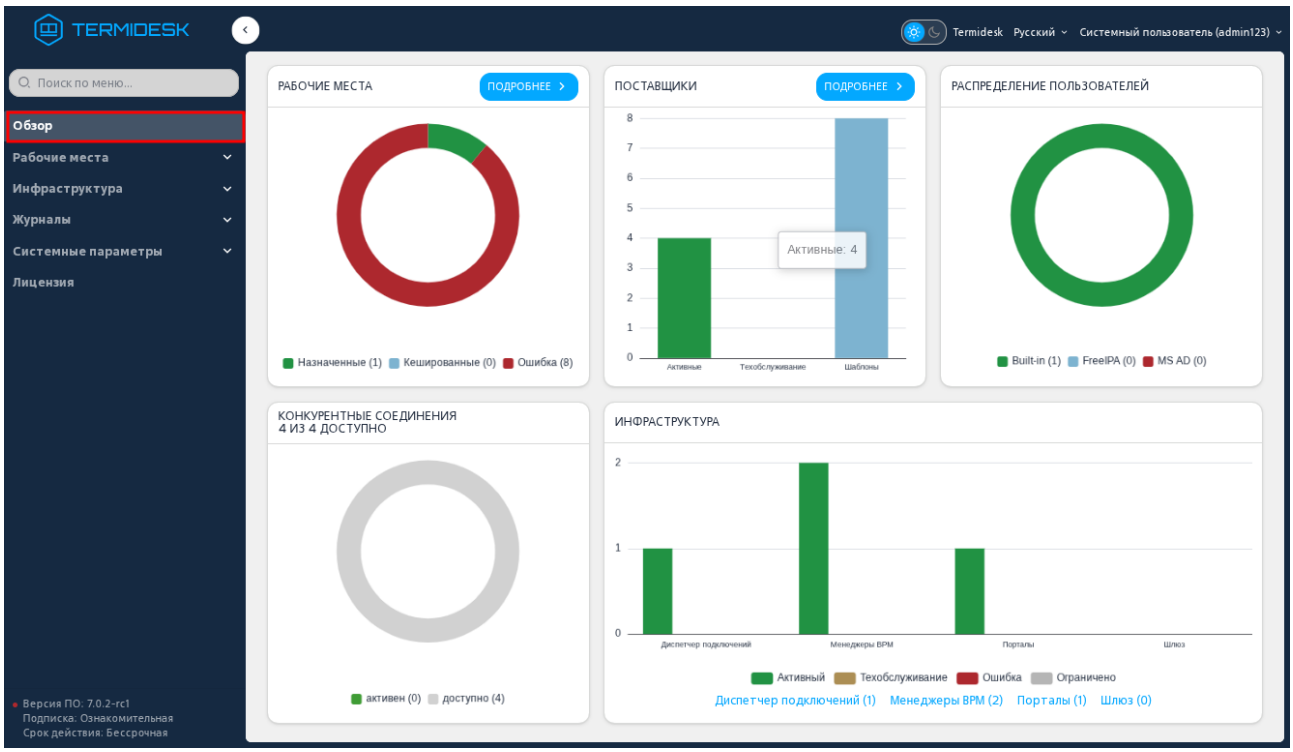


Рисунок 104. Окно функции «Обзор» в графическом интерфейсе управления Termidesk

Функция «Рабочие места»

При нажатии в левой части веб-интерфейса на функцию «Рабочие места» открывается список процедур для управления фондами РМ и просмотра активных пользовательских сессий на выданных РМ.

Функция «Рабочие места» представлена следующими процедурами (см. рисунок Окно функции «Рабочие места» в графическом интерфейсе управления Termidesk):

- «Фонды» – позволяет обеспечить жизненный цикл фондов РМ, от момента создания и до завершения эксплуатации;
- «Библиотека скриптов» - позволяет централизованно управлять скриптами автоматизации развертывания РМ;
- «Галерея» - позволяет загружать и хранить изображения для визуального отображения в фондах РМ в интерфейсе пользователя и интерфейсе управления;
- «Группы рабочих мест» - позволяет объединять фонды РМ в логические группы для отображения в интерфейсе пользователя;
- «Сессии» – позволяет просматривать информацию об активных сессиях пользователей на выданных РМ;
- «Индивидуальные рабочие места» – позволяет просмотреть список РМ из всех фондов РМ;
- «Терминальные серверы» - позволяет просмотреть список сервисных фондов Метапоставщика;
- «Расписания» – позволяет настроить расписания задач, которые должны быть выполнены компонентом «Менеджер рабочих мест»;
- «Параметры гостевых ОС» - позволяет выполнить автоматическую и идентичную настройку одного или нескольких РМ для использования в фонде РМ;
- «Протоколы доставки» - позволяет настраивать протоколы удаленного доступа для подключения к РМ;
- «Профили шлюзов» - позволяет задать параметры шлюзов для использования в

настройках протоколов доставки;

- «Сети» - позволяет настраивать «белые» или «черные» списки доступа на уровне протокола доставки или фонда РМ;
- «Глобальные политики» - позволяет задать глобальные параметры для работы пользователей с РМ, перекрывающие индивидуальные настройки.

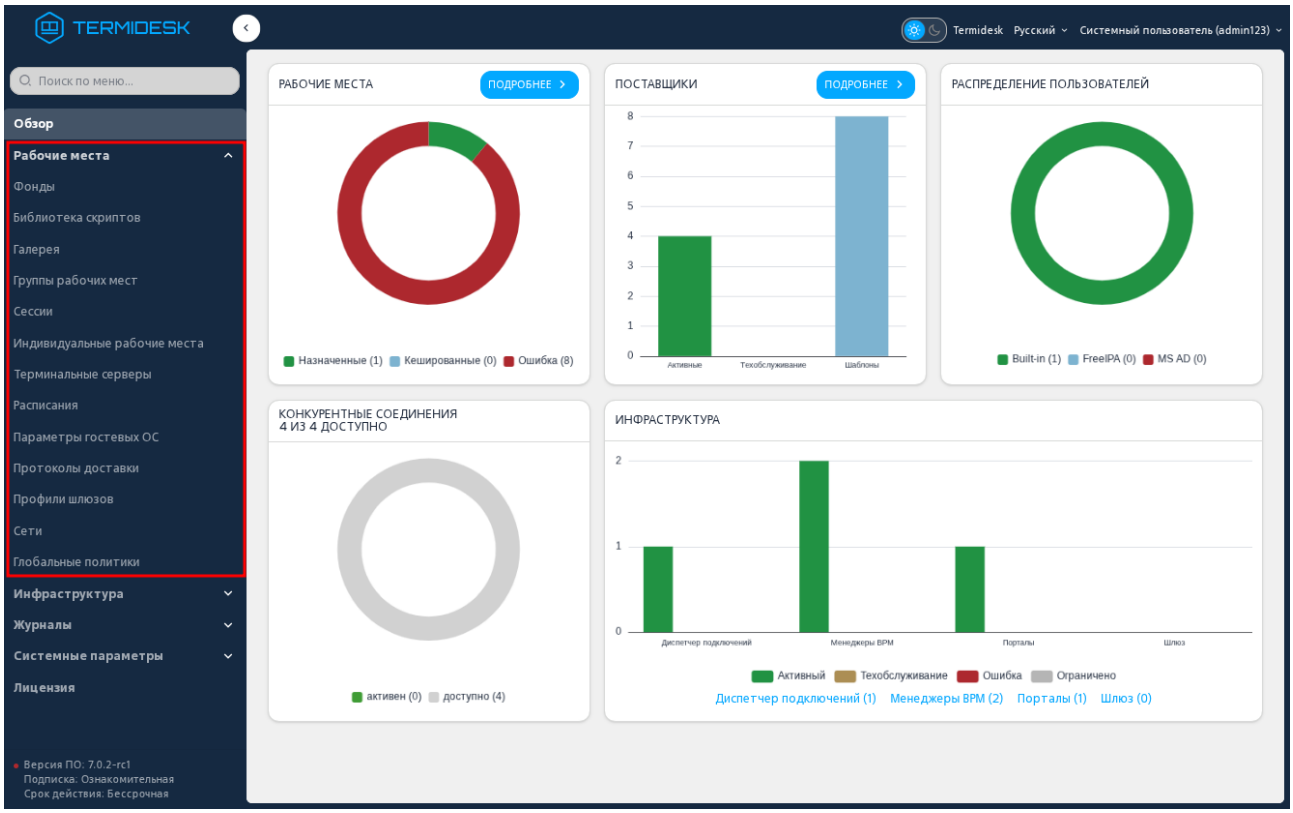


Рисунок 105. Окно функции «Рабочие места» в графическом интерфейсе управления Termidesk

Функция «Инфраструктура»

При нажатии в левой части веб-интерфейса на функцию «Инфраструктура» открывается процедура «Элементы инфраструктуры», позволяющая централизованно управлять компонентами Termidesk VDI и просматривать их статус (см. рисунок Окно функции «Инфраструктура» в графическом интерфейсе управления Termidesk).

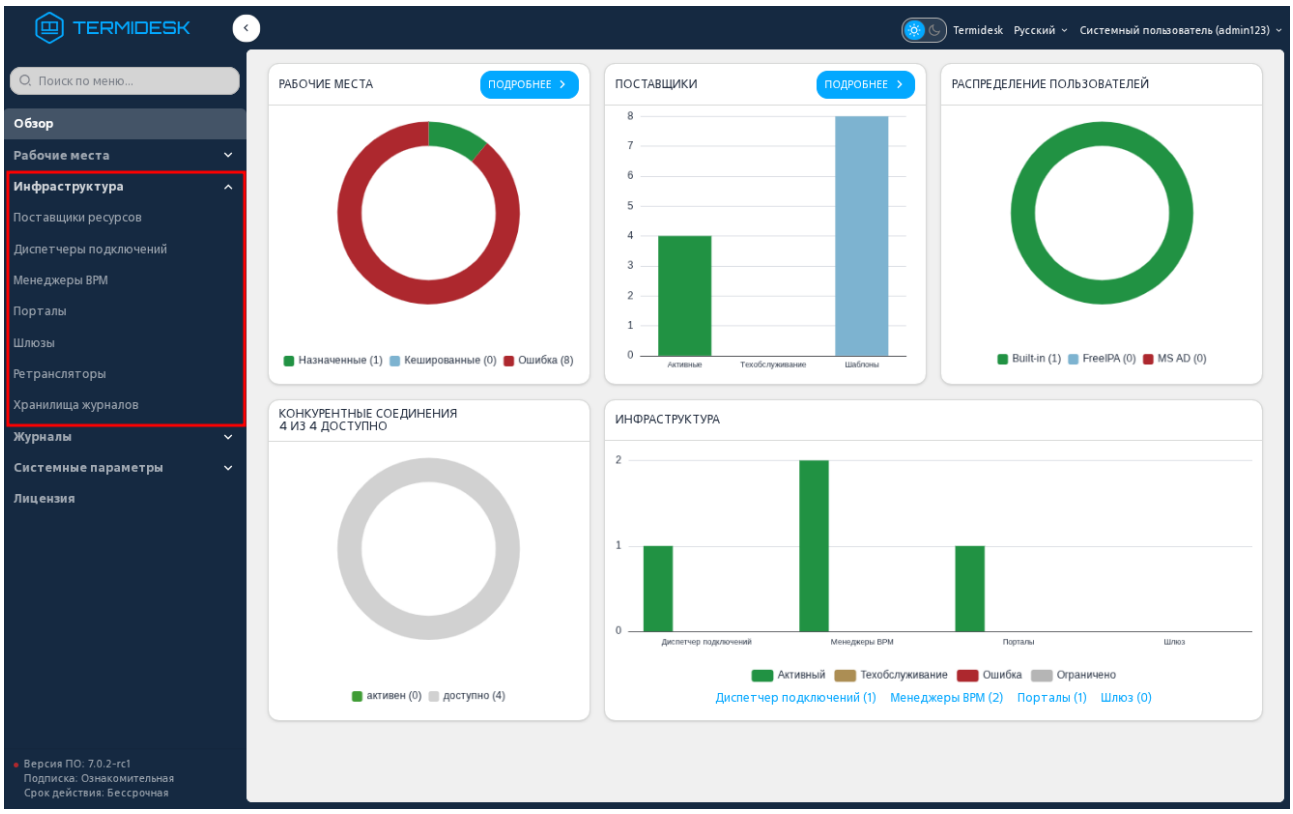


Рисунок 106. Окно функции «Инфраструктура» в графическом интерфейсе управления Termidesk

Функция «Журналы»

При нажатии в левой части веб-интерфейса на функцию «Журналы» открывается список процедур для просмотра и выгрузки в файл событий действий субъектов доступа в интерфейсе управления, а также событий функционирования компонента «Универсальный диспетчер» Termidesk VDI.

Функция «Журналы» представлена следующими процедурами:

- «Системные журналы» – позволяет просматривать и выгружать в csv-файл события функционирования «Универсального диспетчера» Termidesk VDI;
- «Журналы фермы» – позволяет просматривать централизованный журнал событий, связанных с функционированием фермы Termidesk VDI;
- «Аудит» – позволяет просматривать, выгружать в csv-файл и копировать отдельные строки событий действий пользователей и администраторов;
- «Отчёты» – позволяет просматривать и выгружать отчеты по пользовательскому входу, сеансам или подключениям.

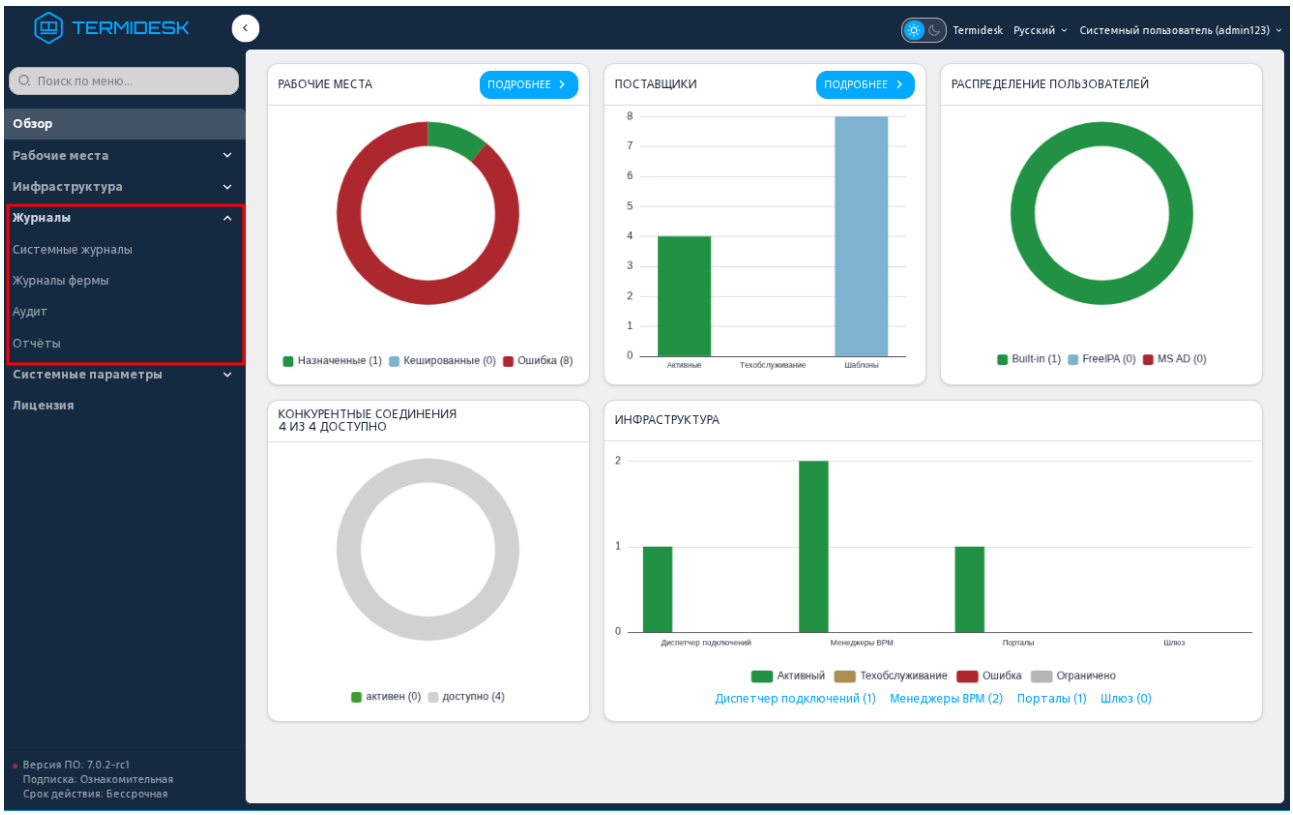


Рисунок 107. Окно функции «Журналы» в графическом интерфейсе управления Termidesk

Функция «Системные параметры»

При нажатии в левой части веб-интерфейса на функцию «Системные параметры» открывается список процедур для формирования эргономичного представления фондов РМ, а также конфигурации системных параметров Termidesk VDI.

Функция «Системные параметры» представлена следующими процедурами (см. рисунок Окно функции «Системные параметры» в графическом интерфейсе управления Termidesk):

- «Домены аутентификации» – определяет порядок действий для настройки взаимодействия с предопределенными источниками сведений о субъектах и их полномочиях;
- «Системные настройки» – определяет системную конфигурацию Termidesk VDI;
- «Управление ACL» - задает параметры доступа к управлению отдельными фондами РМ на основе ролевой модели;
- «Управление ролями» – задает параметры доступа к интерфейсу управления на основе ролевой модели;
- «Управление тегами» - задает параметры тегов, используемых для маркировки и группировки объектов системы.

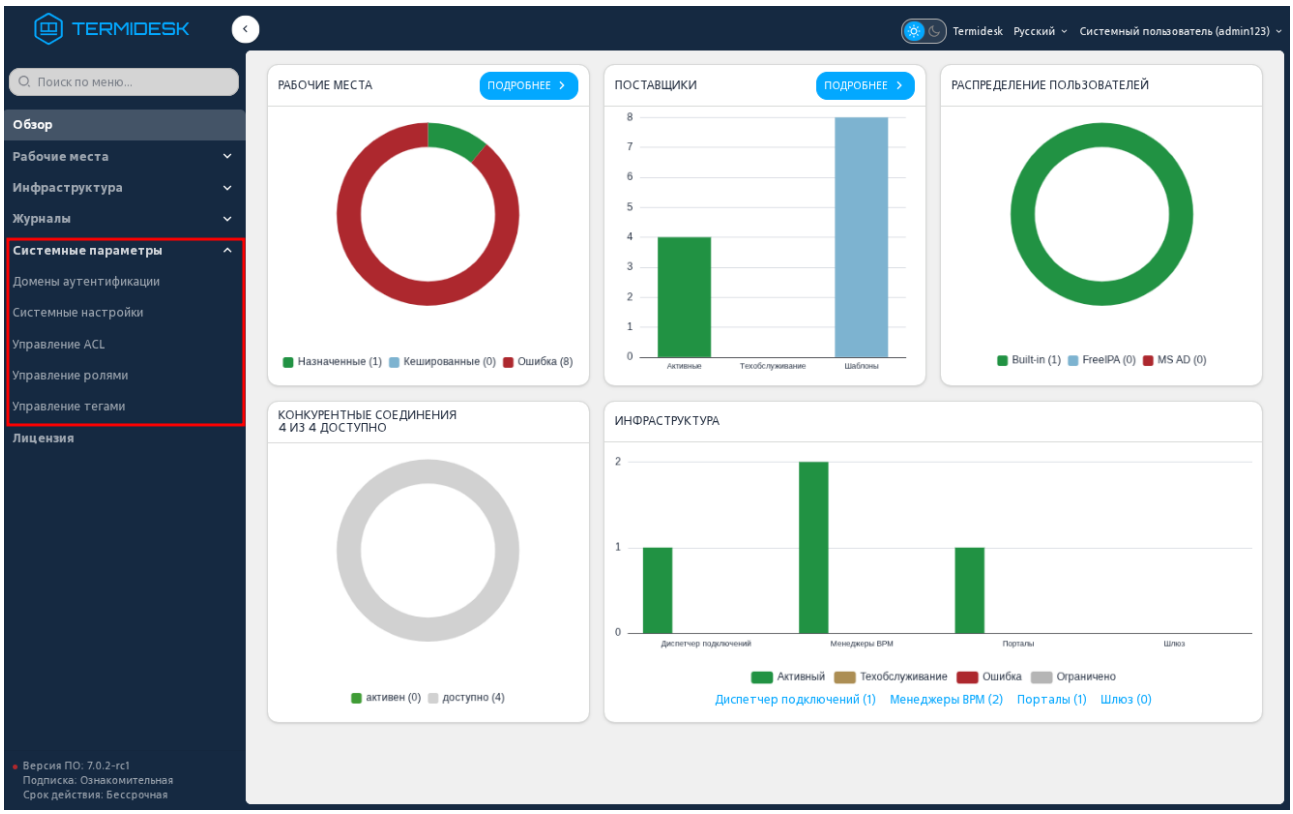


Рисунок 108. Окно функции «Системные параметры» в графическом интерфейсе управления Termidesk

Функция «Лицензия»

Нажатие в левой части веб-интерфейса на функцию «Лицензия» позволяет задать файл лицензии, выполнить просмотр уже установленной лицензии и установленной версии программного комплекса (см. рисунок Окно функции «Лицензия» в графическом интерфейсе управления Termidesk).

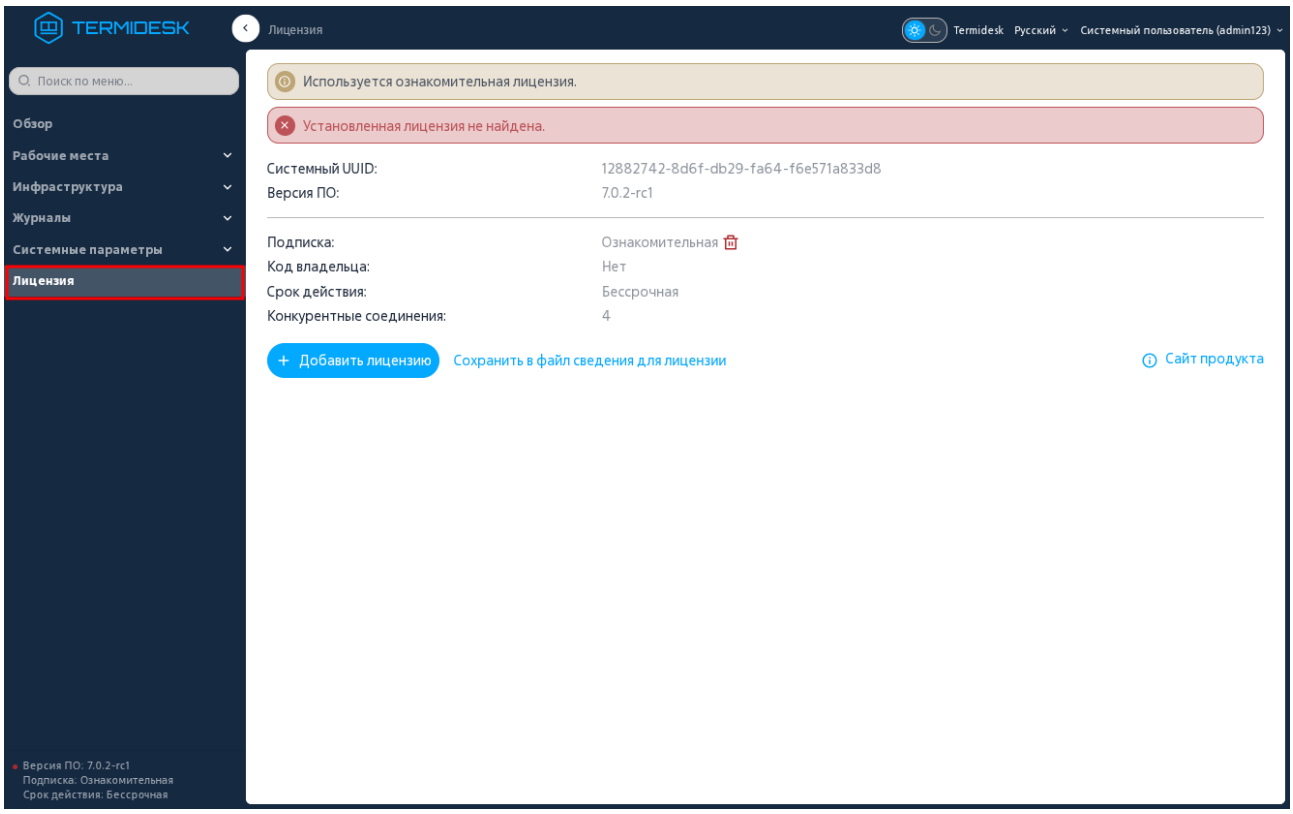


Рисунок 109. Окно функции «Лицензия» в графическом интерфейсе управления Termidesk

ТЕРМИНЫ

Рабочее место

Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа. Под РМ подразумеваются как ВРМ, так и терминальный доступ или доступ к опубликованным на сервере терминалов приложениям

Гостевая ОС

ОС, функционирующая на ВМ

Группы рабочих мест

Функциональное объединение множества фондов РМ по определенному признаку

Домен аутентификации

Способ проверки субъектов и их полномочий

Ключ

Последовательность псевдослучайных чисел, сгенерированная особым образом

Компонент «Менеджер рабочих мест»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за взаимодействие с поставщиком ресурсов и управления жизненным циклом РМ, включая создание, настройку, запуск, отключение и удаление. Является обработчиком фоновых задач. Устанавливается из пакета `termidesk-vdi`. Наименование служб после установки: `termidesk-celery-beat.service` и `termidesk-celery-worker.service`

Компонент «Универсальный диспетчер»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им РМ и контроля доставки РМ. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки:

`termidesk-vdi.service`

Компонент «Шлюз»

Самостоятельный компонент, отвечающий за туннелирование протоколов доставки, использующих транспортный протокол TCP. Устанавливается из пакета `termidesk-gateway`. Наименование службы после установки: `termidesk-gateway.service`

Поставщик ресурсов

ОС, платформа виртуализации или терминальный сервер, предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов РМ

Протокол доставки

Поддерживаемый в Termidesk VDI протокол удаленного доступа к РМ

Портал администратора

Предоставляет веб-интерфейс для управления Termidesk VDI и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API

Портал пользователя

Предоставляет пользовательский веб-интерфейс Termidesk VDI (без доступа к функциям управления) и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API

Портал универсальный

Предоставляет функции обоих вариантов порталов, как пользовательского, так и административного

Сертификат

Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу

Ферма

Логическое объединение узлов, взаимодействующих с одной БД

Фонд рабочих мест

Совокупность подготовленных РМ для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей

Шаблон рабочего места

Параметры конфигурации рабочего места для использования в фонде РМ

СОКРАЩЕНИЯ

ВРМ	Виртуальное рабочее место
ОС	Операционная система
РМ	Рабочее место
ACL	Access Control List (список контроля доступа)
API	Application Programming Interface (интерфейс прикладного программирования)
FQDN	Fully Qualified Domain Name (полностью определенное имя домена)
HTML	Hypertext Markup Language (язык гипертекстовой разметки)

HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
IP	Internet Protocol (межсетевой протокол)
MS RDS	Microsoft Remote Desktop Services (службы удаленного рабочего стола Microsoft)
REST	Representational State Transfer (программная архитектура, определяющая условия работы API)
STAL	Terminal Server Astra Linux (компонент «Сервер терминалов Astra Linux»)
URL	Uniform Resource Locator (унифицированный указатель ресурса)
W3C	World Wide Web Consortium (Консорциум Всемирной паутины)

СЛЕТ.10001-01 90 04. РУКОВОДСТВО АДМИНИСТРАТОРА. НАСТРОЙКА КОМПОНЕНТА «АГЕНТ»

ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ

Назначение документа

Настоящий документ является четвертой частью руководства администратора на программный комплекс «Диспетчер подключений виртуальных рабочих мест Термидеск» (далее - Termidesk VDI, Termidesk VDI). Документ предназначен для администраторов системы и сети.

В этом руководстве приведено назначение, установка и настройка компонента «Агент». Для того, чтобы получить информацию о месте компонента в программном комплексе, необходимо обратиться ко второй части руководства администратора - СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

Типографские соглашения

Приняты следующие типографские соглашения:

- `моноширинный шрифт` – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk VDI, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

АГЕНТ. ОБЩИЕ СВЕДЕНИЯ

Назначение компонента «Агент»

Компонент «Агент» (далее - Агент) входит в состав Termidesk VDI.

К компоненту Агент относятся следующие подкомпоненты, каждый из которых устанавливается отдельно:

- «Агент виртуального рабочего места» (далее - Агент ВРМ) - устанавливается в гостевую операционную систему (ОС) при подготовке базового виртуального рабочего места (ВРМ) или на терминальный сервер. Выполняет взаимодействие с компонентом «Универсальный диспетчер», конфигурирует ВРМ, фиксирует действия пользователя, реализует передачу управляющих сообщений;
- «Агент узла виртуализации» (далее - Агент УВ) - устанавливается на узел виртуализации (УВ). Агент УВ взаимодействует с гипервизором через модуль `libvirt`;
- «Сессионный агент» (далее - сессионный Агент) - устанавливается на терминальный сервер, активирует возможность множественного доступа пользователей к удаленным рабочим столам и приложениям;
- «Видеоагент» (далее - видеоагент) - устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление видеокамеры с пользовательской рабочей

станции в ВРМ;

- «Агент виртуальных смарт-карт» (далее - Агент виртуальных смарт-карт, Агент смарт-карт) - устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление подключенных к пользовательской рабочей станции смарт-карт в ВРМ.

Соответствие перечисленных подкомпонентов установочным файлам приведено в таблице (см. таблицу Соответствие подкомпонентов и наименований установочных файлов).

Таблица 180. Соответствие подкомпонентов и наименований установочных файлов

Наименование подкомпонента	Место установки подкомпонента	Наименование пакета установки
Агент ВРМ	Гостевая ОС, ОС терминального сервера или ОС автономной машины	`termidesk-agent`
Агент УВ	ОС с ПК СВ Брест	`termidesk-vmsd`
Сессионный Агент	ОС терминального сервера	`termidesk-session-agent`
Видеоагент	Гостевая ОС	`termidesk-video-agent`
Агент смарт-карт	Гостевая ОС	`termidesk-pcsc-vscard`

Агент УВ (сервис `termidesk-vmsd`) запускается на узлах программного комплекса «Средства виртуализации «Брест» (далее - ПК СВ Брест) и работает в качестве посредника между `libvirtd` и Агентом ВРМ через `virtio` канал `/dev/virtio-ports/ru.termidesk.tvm.0`.

Полученные от Агента ВРМ команды (`shutdown`, `disconnect`), `termidesk-vmsd` транслирует в `libvirtd`, позволяя тем самым управлять ВМ, на которой запущен Агент ВРМ.

Видеоагент (сервис `termidesk-video-agent`) запускается в ВРМ и предназначен для приема изображения с камеры пользовательской рабочей станции через `virtio` канал `/dev/virtio-ports/ru.termidesk.RealtimeStreaming.0`. Полученный поток перенаправляется на предварительно созданную виртуальную видеокамеру, что позволяет приложениям видеоконференций работать внутри ВРМ.

Требования к аппаратному и программному обеспечению

Для установки подкомпонентов Агента минимальные аппаратные требования узла должны соответствовать следующим:

- процессор архитектуры Intel x86 разрядности 64 бит. Для некоторых ОС поддерживаются другие архитектуры, это указано в списке поддерживаемых ОС;
- оперативная память, не менее 1 ГБ;
- свободное дисковое пространство, не менее 200 МБ;
- сетевое соединение, не менее 100 Мбит/с.

Требования к программному обеспечению для подкомпонентов приведены в таблице (см. таблицу Перечень требований к программному обеспечению).

Таблица 181. Перечень требований к программному обеспечению

Агент ВРМ	Видеоагент и Агент смарт-карт	Агент УВ	Сессионный Агент
ОС: • Astra Linux Special Edition 1.7 (1.7.5, 1.7.6, 1.7.7, 1.7.8, 1.7.9); • Astra Linux Special Edition 1.8 (1.8.3, 1.8.4, 1.8.5, 1.8.6); • РЕД ОС 7.3; • РЕД ОС 8; • Альт Рабочая станция 10; • Альт Рабочая станция 11; • Microsoft Windows 10 1809 LTS • Microsoft Windows 11 LTSC 2024; • Microsoft Windows Server 2022	ОС: • Astra Linux Special Edition 1.7 (1.7.5, 1.7.6, 1.7.7, 1.7.8, 1.7.9); • Astra Linux Special Edition 1.8 (1.8.3, 1.8.4, 1.8.5, 1.8.6); • РЕД ОС 7.3; • РЕД ОС 8; • Альт Рабочая станция 10; • Альт Рабочая станция 11; • Microsoft Windows 10 1809 LTS • Microsoft Windows 11 LTSC 2024; • Microsoft Windows Server 2022	ОС: • Astra Linux Special Edition 1.7 (.7.5, 1.7.6, 1.7.7, 1.7.8, 1.7.9); • Astra Linux Special Edition 1.8 (1.8.3, 1.8.4, 1.8.5, 1.8.6); • РЕД ОС 7.3; • РЕД ОС 8; • CentOS 8	ОС: • Astra Linux Special Edition Server 1.8 (1.8.1, 1.8.2, 1.8.4, 1.8.5, 1.8.6); • Альт Рабочая станция 10; • Microsoft Windows Server 2016; • Microsoft Windows Server 2019; • Microsoft Windows Server 2022 В ОС должны быть установлены: • компонент «Сервер терминалов Astra Linux» для ОС Astra Linux Special Edition (Server); • MS RDS для ОС Microsoft Windows Server

Указанный в таблице компонент «Сервер терминалов Astra Linux» является компонентом Termidesk VDI.

В платформе виртуализации для видеоагента должен быть активирован канал `/dev/virtio-ports/ru.termidesk.RealtimeStreaming.0`.

В платформе виртуализации для Агента УВ должен быть активирован канал `/dev/virtio-ports/ru.termidesk.tvm.0`.

АГЕНТ. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ

Получение пакетов установки через Интернет-репозиторий

Для получения пакетов установки может использоваться Интернет-репозиторий: https://repos.termidesk.ru/.

Для подключения репозитория в ОС Astra Linux Special Edition нужно:

- установить пакеты:

```
sudo apt install -y lsb-release wget apt-transport-https debian-keyring
```

где:

`-y` - ключ для пропуска подтверждения установки;

- добавить Интернет-репозиторий Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list` через командный интерпретатор `sh`:

- выяснить установленную версию ОС:

```
sudo cat /etc/astra_version
```

- определить актуальное имя каталога с пакетами в https://repos.termidesk.ru/astra;
- указать в файле конфигурации APT корректное (фактическое) имя каталога:

```
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra 1.8_x86-64 non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
```

где:

-c - ключ для чтения команд из вводимой строки (стандартный ввод);

echo - команда вывода текста, совместно с символом «>» используется для перенаправления строки в файл;

deb https://repos.termidesk.ru/astra <…> - добавляемый репозиторий;

Приведенный пример команды актуален для установки основных компонентов Termidesk, пакеты которых расположены в каталоге 1.8_x86-64.

- для корректной установки компонентов TERA потребуется корректно подключить дополнительные репозитории и настроить их приоритет:
  - для версий ОС Astra Linux Special Edition меньше или равных 1.7.6, а также для версий 1.8.X:
    - подключить два репозитория:

```
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(cat
/etc/astra_version) non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(lsb_release -cs
2> /dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

    - добавить повышенный приоритет для репозитория с требуемой версией ОС (значение $(cat /etc/astra_version) может подходить не для всех репозиториев, т.к. версия может указываться без точек - в этом случае нужно вручную указать корректную версию):

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000
EOF"
```

  - для версий ОС Astra Linux Special Edition 1.7.7 и 1.7.8:

- подключить три репозитория:

```
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra 1.7.6 non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(cat
/etc/astra_version) non-free" >>
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(lsb_release -cs
2> /dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

- настроить два приоритета:

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=1.7.6
Pin-Priority: 950

Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000

EOF"
```

- получить ключ репозитория Termidesk VDI `GPG-KEY-PUBLIC` и добавить его в ОС:
  - для ОС Astra Linux Special Edition 1.7:

```
wget --no-check-certificate -qO - https://repos.termidesk.ru/astra/GPG-KEY-
PUBLIC | sudo apt-key add -
```

  - для ОС Astra Linux Special Edition 1.8:

```
wget --no-check-certificate -qO - https://repos.termidesk.ru/astra/GPG-KEY-
PUBLIC |  sudo gpg --dearmour -o /etc/apt/trusted.gpg.d/termidesk.gpg
```

- обновить данные пакетного менеджера:

```
sudo apt update
```

- проверить настройку приоритетов репозиториев:

```
apt-cache policy
```

Команду `sudo apt update` необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.

Команды добавления ключа репозитория Termidesk VDI отличаются в зависимости от используемой версии ОС.

Если для ОС Astra Linux Special Edition 1.8 ключ репозитория был добавлен командой, применимой к другой версии ОС, то для исправления нужно:

- узнать идентификатор добавленного ключа репозитория:

```
apt-key list
```

- удалить ключ:

```
apt-key --keyring /etc/apt/trusted.gpg del 4E1632CC
```

где `4E1632CC` - последние 8 символов идентификатора ключа;

- вновь добавить ключ репозитория.

Получение пакетов установки в ОС Astra Linux Special Edition

Дистрибутив представлен бинарным файлом пакета ПО в `deb`-формате. Установка в ОС Astra Linux Special Edition производится из локального репозитория, распространяемого в формате `iso`-образа.

Получить `iso`-образ можно двумя способами:

- заполнив запрос через сайт Termidesk VDI: https://termidesk.ru/support/#request-support;
- через личный кабинет:https://lk.astra.ru/.

Для подключения локального репозитория Termidesk VDI на узле, где предполагается установка, нужно:

- скопировать в домашний каталог пользователя образ диска `termidesk-<версия>.iso`;
- подключить образ диска к файловой системе в каталог `/mnt`:

```
sudo mount -o loop termidesk-<версия>.iso /mnt
```

где:

`-o loop` - параметры для привязки петлевого устройства (`/dev/loop`) к файлу `termidesk-<версия>.iso`, устройство затем монтируется в указанный каталог `/mnt`;

- скопировать содержимое каталога `repos` подключенного образа диска в каталог `/var` локальной файловой системы:

```
sudo cp -Rp /mnt/repos /var
```

где:

-Rp - ключ для рекурсивного копирования подкаталогов и файлов с сохранением исходных свойств;

- отключить подключенный ранее образ диска от узла:

```
sudo umount /mnt
```

- установить пакет lsb-release:

```
sudo apt install -y lsb-release
```

- добавить локальный репозиторий Termidesk VDI в файл /etc/apt/sources.list.d/termidesk_local.list через командный интерпретатор sh:
  - выяснить установленную версию ОС:

    ```
    sudo cat /etc/astra_version
    ```

  - определить актуальное имя каталога с пакетами в /var/repos;
  - указать в файле конфигурации APT корректное (фактическое) имя каталога:

    ```
    sudo sh -c 'echo "deb file:/var/repos/astra 1.8_x86-64 non-free" >
    /etc/apt/sources.list.d/termidesk_local.list'
    ```

    где:

    -c - ключ для чтения команд из вводимой строки (стандартный ввод);

    echo - команда вывода текста, совместно с символом «>» используется для перенаправления строки в файл;

    deb file:/var/repos/astra 1.8_x86-64 non-free - добавляемый репозиторий с вложенной командой получения версии ОС;

    Приведенный пример команды актуален для установки основных компонентов Termidesk, пакеты которых расположены в каталоге 1.8_x86-64.

- для корректной установки компонентов TERA потребуется корректно подключить дополнительные репозитории и настроить их приоритет:
  - для версий ОС Astra Linux Special Edition меньше или равных 1.7.6, а также для версий 1.8.X:
    - подключить два репозитория:

    ```
    sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
    non-free" > /etc/apt/sources.list.d/termidesk_local.list'
    sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
    ```

```
/dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

- добавить повышенный приоритет для репозитория с требуемой версией ОС (значение `$(cat /etc/astra_version)` может подходить не для всех репозиториев, т.к. версия может указываться без точек - в этом случае нужно вручную указать корректную версию):

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000
EOF"
```

- для версий ОС Astra Linux Special Edition 1.7.7 и 1.7.8:
  - подключить три репозитория:

```
sudo sh -c 'echo "deb file:/var/repos/astra 1.7.6 non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
/dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

  - настроить два приоритета:

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=1.7.6
Pin-Priority: 950

Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000

EOF"
```

- выполнить поиск ключа репозитория Termidesk VDI `GPG-KEY-PUBLIC` и добавить его:

```
sudo cat /var/repos/astra/GPG-KEY-PUBLIC | sudo gpg --dearmour -o
/etc/apt/trusted.gpg.d/termidesk.gpg
```

- убедиться, что ключ `release@uveon.ru` был успешно добавлен:

```
apt-key list
```

В случае, если ключ не отображен в выводе команды, необходимо убедиться, что ключ `GPG-KEY-PUBLIC` существует:

```
cat /var/repos/astra/GPG-KEY-PUBLIC
```

Если ключ все же существует, следует проверить правильность выполнения шагов по добавлению репозитория Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list`.

При успешном выполнении всех шагов команда выведет содержимое ключа в формате Base64.

В зависимости от используемой версии ОС команды добавления ключа репозитория Termidesk VDI могут отличаться. Если для ОС Astra Linux Special Edition 1.8 ключ репозитория был добавлен командой, применимой к другой версии ОС, то для исправления нужно:

- узнать идентификатор добавленного ключа репозитория:

```
apt-key list
```

- удалить ключ:

```
apt-key --keyring /etc/apt/trusted.gpg del 4E1632CC
```

где `4E1632CC` - последние 8 символов идентификатора ключа;

- вновь добавить ключ репозитория.

- обновить данные пакетного менеджера:

```
sudo apt update
```

- проверить настройку приоритетов репозиториев:

```
apt-cache policy
```

Команду `sudo apt update` необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.

АГЕНТ. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ

ОС Astra Linux Special Edition

Установка Агента ВРМ в ОС Astra Linux Special Edition

Перед установкой необходимо подключить репозиторий Termidesk VDI, как указано в подразделе **Получение пакетов установки**.

Для установки Агента ВРМ в гостевой ОС:

- выполнить:

```
sudo apt install termidesk-agent
```

- в окне «Расширенные настройки» оставить значения по умолчанию или при необходимости изменить значения:
  - «Каталог журналов»: каталог хранения журналов для службы Агента ВРМ. Значение по умолчанию: `/var/log/termidesk`. По умолчанию после установки права на каталог соответствуют `rwxr-xr-x` (в восьмеричной записи - `755`);
  - «Каталог журналов пользователя»: каталог хранения журналов для непривилегированного пользователя. Значение по умолчанию: `~./config/UVEON/logs`;
  - «Каталог настроек»: каталог хранения конфигурационного файла. Значение по умолчанию: `/etc/termidesk`.

Окно «Расширенные настройки» будет показано единожды, если конфигурационный файл `agent.cfg` отсутствует в системе.

Предпочтительные значения в расширенных настройках будут подставлены автоматически. Если настройки были изменены, то значения подставятся с учетом их приоритета:

- в первую очередь подставляются значения из переменных окружения. Все ранее заданные значения конфигурационного файла игнорируются;
- если переменные окружения не заданы, то подставляются значения из конфигурационного файла;
- если ничего из пунктов выше не задано, то применяются значения по умолчанию.

После установки изменить настройки можно:

- через файл `/etc/default/termidesk-agent` (см. подраздел **Конфигурационные файлы Агента ВРМ**);
- через вызов программы `termidesk-agent-config`:

```
sudo termidesk-agent-config setup --dialog
```

Для «тихой» установки без отображения дополнительных окон следует назначить переменные окружения и передать их в команду установки:

```
sudo TDSK_SETUP_NONINTERACTIVE=1 TDSK_CONFIG_DIR=<путь_к_каталогу>
TDSK_LOG_SRV_DIR=<путь_к_каталогу> TDSK_LOG_USER_DIR=<путь_к_каталогу> apt install
termidesk-agent
```

где:

- `TDSK_SETUP_NONINTERACTIVE=1` - переменная, указывающая запуск в режиме «тихой» установки;

- TDSK_CONFIG_DIR=<путь_к_каталогу> - переменная, указывающая путь к каталогу с конфигурационным файлом agent.cfg. Например, TDSK_CONFIG_DIR=/etc/termidesk-test;
- TDSK_LOG_SRV_DIR=<путь_к_каталогу> - переменная, указывающая путь к каталогу хранения журналов службы Агента ВРМ;
- TDSK_LOG_USER_DIR=<путь_к_каталогу> - переменная, указывающая путь к каталогу хранения журналов для непривилегированного пользователя.

В состав пакета termidesk-agent входят:

- termidesk-agent-config - программа, осуществляющая настройку Агента ВРМ;
- termidesk-agent-user - программа, отслеживающая состояние пользовательской сессии и отображающая иконку Агента ВРМ в системном трее;
- termidesk-agent-daemon - служба, регистрирующая ВМ в компоненте «Универсальный диспетчер», принимающая и обрабатывающая команды;
- termidesk-cupsd - служба, динамически обновляющая список принтеров.

После установки Агент ВРМ обязательно должен быть настроен согласно подразделу **Настройка для ОС Astra Linux Special Edition**.

Проверка состояния службы Агента ВРМ выполняется командой:

```
sudo systemctl status termidesk-agent
```

Проверка состояния службы termidesk-cupsd выполняется командой:

```
sudo systemctl status termidesk-cupsd
```

Установка видеоагента в ОС Astra Linux Special Edition

Перед установкой необходимо подключить репозиторий Termidesk VDI, как указано в подразделе **Получение пакетов установки**.

Перед установкой видеоагента (служба termidesk-video-agent) необходимо:

- установить пакет linux-headers, соответствующий ядру, загруженному в работающей ОС:

```
sudo apt install linux-headers-`uname -r`
```

Если видеоагент устанавливается не в ОС Astra Linux Special Edition следует учесть, что наименование пакета заголовочных файлов ядра может отличаться от linux-headers.

- если видеоагент должен быть установлен в ОС с включенным режимом замкнутой программной среды (ЗПС) нужно:
  - удостовериться, что используемая версия ОС - 1.7.5 и выше;
  - затем установить пакет v4l2loopback-kmod, соответствующий ядру, загруженному в работающей ОС:

```
sudo apt install v4l2loopback-kmod-`uname -r`
```

Установка видеоагента выполняется в гостевой ОС командой:

```
sudo apt install termidesk-video-agent
```

После установки нужно добавить в автоматическую загрузку и запустить службу `termidesk-video-agent`:

```
sudo systemctl enable termidesk-video-agent.service
sudo systemctl start termidesk-video-agent.service
```

Проверить состояние службы:

```
sudo systemctl status termidesk-video-agent.service
```

Установка Агента смарт-карт в ОС Astra Linux Special Edition

Перед установкой необходимо подключить репозиторий Termidesk VDI, как указано в подразделе **Получение пакетов установки**.

Установка Агента смарт-карт выполняется в гостевой ОС командой:

```
sudo apt install termidesk-pcsc-vscard
```

После установки Агент смарт-карт должен быть настроен согласно подразделу **Настройка Агента виртуальных смарт-карт**.

Установка Агента УВ в ОС Astra Linux Special Edition

Агент УВ (сервис `termidesk-vmsd`) запускается на узлах виртуализации ПК СВ Брест и работает в качестве посредника между `libvirtd` и Агентом ВРМ через `virtio`-канал `/dev/virtio-ports/ru.termidesk.tvm.0`.

Полученные от Агента ВРМ команды (`shutdown`, `disconnect`), `termidesk-vmsd` транслирует в `libvirtd`, позволяя тем самым управлять ВМ, на которой запущен Агент ВРМ.

Агент УВ устанавливается из `deb`-пакета `termidesk-vmsd`.

Перед установкой необходимо обязательно удалить предыдущую версию!

Для установки Агента УВ нужно:

- подключить репозиторий Termidesk VDI, как указано в подразделе как указано в подразделе **Получение пакетов установки**;
- выполнить:

```
sudo apt install termidesk-vmsd
```

- убедиться, что пользователь, от имени которого запущена служба `termidesk-vmsd`, добавлен в группы `libvirt`, `libvirt-admin`, `libvirt-qemu` и `kvm`.

После установки рекомендуется выполнить перезагрузку узла виртуализации.

Установка сессионного Агента в ОС Astra Linux Special Edition

Сессионный Агент устанавливается на терминальном сервере ОС Astra Linux Special Edition (Server) из `deb`-пакета `termidesk-session-agent`.

Для установки сессионного Агента:

- подключить репозиторий Termidesk VDI, как указано в подразделе **Получение пакетов установки**;
- выполнить:

```
sudo apt install termidesk-session-agent
```

- в окне «Лицензионное соглашение» ознакомиться с соглашением и нажать экранную кнопку **[Выход]**;
- на запрос «Принимаете ли вы условия лицензионного соглашения?» подтвердить принятие соглашения, нажав экранную кнопку **[Принимаю]**;
- в окне «Расширенные настройки»:
  - указать путь к каталогу хранения файлов конфигурации. Значение по умолчанию: `/etc/opt/termidesk-session-agent`;
  - указать путь к каталогу хранения журналов. Значение по умолчанию: `/var/log/termidesk`;
  - нажать экранную кнопку **[Далее]**;
- дождаться завершения установки.

Для «тихой» установки без отображения дополнительных окон следует назначить переменные окружения `DEBIAN_FRONTEND=noninteractive`, `SSA_CONFIG_DIR` и `SSA_LOG_DIR` и передать их в команду установки:

```
sudo DEBIAN_FRONTEND=noninteractive SSA_CONFIG_DIR=<путь_к_каталогу>
SSA_LOG_DIR=/<путь_к_каталогу> apt install termidesk-session-agent
```

Где:

- `DEBIAN_FRONTEND=noninteractive` - переменная, указывающая запуск в режиме «тихой» установки;
- `SSA_CONFIG_DIR=<путь_к_каталогу>` - переменная, указывающая путь к каталогу хранения файлов конфигурации. Заменяет значение по умолчанию, если передается непустое значение;
- `SSA_LOG_DIR=<путь_к_каталогу>` - переменная, указывающая путь к каталогу хранения журналов. Заменяет значение по умолчанию, если передается непустое значение.

После установки изменить настройки можно через файл /etc/default/termidesk-session-agent.

После установки служба termidesk-session-agent автоматически запустится, также создастся конфигурационный файл session_agent.ini.

После установки сессионный Агент может быть настроен согласно подразделу **Первичная настройка**.

После установки сессионного Агента будет создан файл БД SQLite /opt/termidesk/share/termidesk-session-agent/termidesk_ssa.db, предназначенный для сбора и хранения метрик узла. БД инициализируется при запуске сессионного Агента.

Установка в режиме ЗПС

Замкнутая программная среда (ЗПС) является средством повышения безопасности ОС путем контроля целостности (неизменности) файлов.

Механизм контроля реализован в виде невыгружаемого модуля ядра ОС Astra Linux Special Edition (модуль digsig_verif), выполняющего проверку электронной цифровой подписи файлов (ЭЦП).

Перед установкой компонентов Termidesk VDI необходимо установить пакет termidesk-digsig-keys, для этого:

- подключить репозиторий Termidesk VDI или получить отдельный пакет termidesk-digsig-keys из репозитория;
- выполнить установку с использованием репозитория:

```
sudo apt -y install termidesk-digsig-keys
```

- либо выполнить установку из deb-пакета:

```
sudo apt install -y /home/user/termidesk-digsig-keys-XXXXXX_amd64.deb
```

где:

-y - ключ для пропуска подтверждения установки;

/home/user/termidesk-digsig-keys-XXXXXX_amd64.deb - расположение пакета termidesk-digsig-keys-XXXXXX_amd64.deb.

- перезагрузить ОС:

```
sudo reboot
```

- выполнить установку компонента Termidesk VDI.

Для ЗПС может быть активирован режим проверки встроенной ЭЦП в расширенных атрибутах (DIGSIG_XATTR_MODE). В этом случае потребуется подписать файлы, которые будут проходить проверку, имеющимися в организации ключами. Информация о процессе

подписи и активации механизма проверки встроенной ЭЦП в расширенных атрибутах приведена в справочном центре Astra Linux: https://wiki.astralinux.ru/pages/viewpage.action?pageId=41190634.

Постановка Агента на контроль целостности

После установки и настройки Агентов необходимо поставить их на контроль целостности.

В подразделе приведена процедура только для Агентов, установленных в ОС Astra Linux Special Edition.

Для контроля целостности используются встроенные в ОС Astra Linux Special Edition программные средства на основе `Another File Integrity Checker`, представленного пакетом `afick`.

Настройка регламентного контроля целостности выполняется в конфигурационном файле `/etc/afick.conf`.

Настройку следует производить только после окончательного внедрения компонента, поскольку с файлов конфигурации и исполняемых файлов будут сняты эталонные контрольные суммы.

Для постановки на контроль целостности Агента ВРМ, Агента смарт-карт,видеоагента необходимо добавить в конфигурационный файл `/etc/afick.conf` следующие строки:

```
/etc/termidesk PARSEC
/etc/systemd/system/multi-user.target.wants/termidesk-agent.service PARSEC
/etc/systemd/system/multi-user.target.wants/termidesk-cupsd.service PARSEC
/usr/bin/termidesk-agent-user PARSEC
/usr/lib/python3/dist-packages/termidesk_agent PARSEC
/usr/lib/systemd/system/termidesk-video-agent.service PARSEC
/usr/sbin/termidesk-agent-config PARSEC
/usr/sbin/termidesk-agent-daemon PARSEC
/usr/sbin/termidesk-cups-daemon PARSEC
/usr/share/doc/termidesk-agent PARSEC
/usr/share/doc/termidesk-pcsc-vscard PARSEC
/usr/share/doc/termidesk-video-agent PARSEC
/usr/share/polkit-1/actions/org.termidesk.pkexec.TermideskAgentConfig.policy PARSEC
/usr/share/termidesk-agent PARSEC
/var/lib/systemd/deb-systemd-helper-enabled/multi-user.target.wants/termidesk-
cupsd.service  PARSEC
/var/lib/systemd/deb-systemd-helper-enabled/termidesk-cupsd.service.dsh-also PARSEC
/var/lib/systemd/deb-systemd-helper-enabled/termidesk-video-agent.service.dsh-also
PARSEC
/var/lib/systemd/deb-systemd-helper-enabled/termidesk-agent.service.dsh-also PARSEC

#Репозиторий Termidesk VDI (если используется)
/var/repos/ PARSEC
```

Для постановки на контроль целостности Агента УВ необходимо добавить в конфигурационный файл `/etc/afick.conf` следующие строки:

```
/etc/systemd/system/multi-user.target.wants/termidesk-vmsd.service PARSEC
/usr/lib/python3/dist-packages/termidesk_agent PARSEC
/usr/lib/systemd/system/termidesk-vmsd.service PARSEC
/usr/sbin/termidesk-vmsd PARSEC
/usr/share/doc/termidesk-vmsd PARSEC
/var/lib/systemd/deb-systemd-helper-enabled/multi-user.target.wants/termidesk-
vmsd.service PARSEC
/var/lib/systemd/deb-systemd-helper-enabled/termidesk-vmsd.service.dsh-also PARSEC

#Репозиторий Termidesk VDI (если используется)
/var/repos/ PARSEC
```

Для постановки на контроль целостности сессионного Агента необходимо добавить в конфигурационный файл `/etc/afick.conf` следующие строки:

```
/etc/systemd/system/multi-user.target.wants/termidesk-stal.service PARSEC
/etc/systemd/system/termidesk-stal.service PARSEC
/etc/X11/Xresources/x11-stal PARSEC
/etc/X11/stal.conf PARSEC
/etc/dbus-1/system.d/ru.uveon.stal.conf PARSEC
/etc/logrotate.d/stal PARSEC
/etc/pam.d/stal PARSEC
/etc/pam.d/stal-rdp PARSEC
/etc/stal PARSEC
/etc/syslog-ng/conf.d/stal-proxy.conf PARSEC
/etc/syslog-ng/conf.d/stal-service.conf PARSEC
/etc/syslog-ng/conf.d/stal-watchdog.conf PARSEC
/etc/systemd/system/multi-user.target.wants/stal-proxy.service PARSEC
/etc/systemd/system/multi-user.target.wants/stal-watchdog.service PARSEC
/etc/systemd/system/multi-user.target.wants/termidesk-stal.service PARSEC
/etc/systemd/system/stal-proxy.service PARSEC
/etc/systemd/system/stal-watchdog.service PARSEC
/etc/systemd/system/termidesk-stal.service PARSEC
/etc/ufw/applications.d/stal-proxy PARSEC
/usr/libexec/stal PARSEC
/usr/sbin/stal_proxy PARSEC
/usr/sbin/stal_service PARSEC
/usr/sbin/stal_watchdog PARSEC
/usr/share/doc/stal PARSEC

#Репозиторий Termidesk VDI (если используется)
/var/repos/ PARSEC
```

Для снятия эталонных значений контрольных сумм используется команда:

```
afick -i
```

Для проверки соответствия контрольных сумм эталонным значениям автоматически создаются задания в системном планировщике заданий `cron`.

Для ручной проверки соответствия контрольных сумм используется команда:

```
afick -k
```

В случае отсутствия по какой-либо причине исполняемых фалов `*.pyc`, они будут повторно сгенерированы при перезапуске сервера Python. В этом случае нужно повторно проинициализировать средство регламентного контроля целостности `afick`.

Обновление Агентов в ОС Astra Linux Special Edition

Обновление Агентов выполняется установкой новой версии поверх предыдущей, кроме Агента ВРМ и Агента УВ.

Для обновления Агента ВРМ нужно:

- удалить предыдущую версию (рекомендуется, чтобы корректно обновились права на каталоги для новой версии):

```
sudo aptitude purge -y termidesk-agent
```

- установить новую версию:

```
sudo apt install -y termidesk-agent
```

Для обновления Агента УВ нужно:

- удалить предыдущую версию (рекомендуется, чтобы корректно обновились права на каталоги для новой версии):

```
sudo aptitude purge -y termidesk-vmsd
```

- установить новую версию:

```
sudo apt install -y termidesk-vmsd
```

В случае, если обновление компонента «Универсальный диспетчер» произошло раньше обновления сессионного Агента, то на узле с «Универсальным диспетчером» (роль «Портал администратора») нужно:

- в интерфейсе командной строки переключиться на пользователя `termidesk`:

```
sudo -u termidesk bash
```

- выполнить регистрацию сессионного Агента:

```
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_refresh_ssa
```

Удаление Агентов в ОС Astra Linux Special Edition

Удаление Агентов из среды ОС Astra Linux Special Edition выполняется командой:

```
sudo aptitude purge -y <наименование_пакета>
```

Наименования пакетов:

- `termidesk-agent` - Агент ВРМ;
- `termidesk-session-agent` - сессионный Агент;
- `termidesk-video-agent` - видеоагент;
- `termidesk-pcsc-vscard` - Агент смарт-карт;
- `termidesk-vmsd` - Агент УВ.

Если установка пакета производилась не из локального репозитория, удаление выполняется командой:

```
sudo dpkg -P <наименование_пакета>
```

Вместе с удалением сессионного Агента будет удален файл БД SQLite `termidesk_ssa.db`.

ОС Альт Рабочая станция

Установка Агента ВРМ в ОС Альт Рабочая станция

Агент ВРМ устанавливается в ОС Альт Рабочая станция из `rpm`-пакета `termidesk-agent`.

Для установки Агента ВРМ:

- (опционально) подключить Интернет-репозиторий Termidesk VDI (см. пример в подразделе **Получение пакетов установки**);
- переключиться в окружение суперпользователя:

```
su -
```

- выполнить установку `termidesk-agent`:
  - если установка выполняется с подключенным Интернет-репозиторием:

    ```
    apt-get install termidesk-agent
    ```

- если установка выполняется без подключенного Интернет-репозитория:

```
apt-get install <путь_к_пакету>
```

- в окне «Расширенные настройки» оставить значения по умолчанию или при необходимости изменить значения:
  - «Каталог журналов»: каталог хранения журналов для службы Агента ВРМ. Значение по умолчанию: `/var/log/termidesk`. По умолчанию после установки права на каталог соответствуют `rwxr-xr-x` (в восьмеричной записи - `755`);
  - «Каталог журналов пользователя»: каталог хранения журналов для непривилегированного пользователя. Значение по умолчанию: `~./config/UVEON/logs`;
  - «Каталог настроек»: каталог хранения конфигурационного файла. Значение по умолчанию: `/etc/termidesk`.

Окно «Расширенные настройки» будет показано единожды, если конфигурационный файл `agent.cfg` отсутствует в системе.

Предпочтительные значения в расширенных настройках будут подставлены автоматически. Если настройки были изменены, то значения подставятся с учетом их приоритета:

- в первую очередь подставляются значения из переменных окружения. Все ранее заданные значения конфигурационного файла игнорируются;
- если переменные окружения не заданы, то подставляются значения из конфигурационного файла;
- если ничего из пунктов выше не задано, то применяются значения по умолчанию.

После установки изменить настройки можно:

- через файл `/etc/default/termidesk-agent` (см. подраздел **Конфигурационные файлы Агента ВРМ**);
- через вызов программы `termidesk-agent-config`:

```
termidesk-agent-config setup --dialog
```

Для «тихой» установки без отображения дополнительных окон следует назначить переменные окружения и передать их в команду установки:

```
TDSK_SETUP_NONINTERACTIVE=1 TDSK_CONFIG_DIR=<путь_к_каталогу>
TDSK_LOG_SRV_DIR=<путь_к_каталогу> TDSK_LOG_USER_DIR=<путь_к_каталогу> apt install
<путь_к_пакету>
```

где:

- `TDSK_SETUP_NONINTERACTIVE=1` - переменная, указывающая запуск в режиме «тихой» установки;
- `TDSK_CONFIG_DIR=<путь_к_каталогу>` - переменная, указывающая путь к каталогу с конфигурационным файлом `agent.cfg`. Например, `TDSK_CONFIG_DIR=/etc/termidesk-test`;

- TDSK_LOG_SRV_DIR=<путь_к_каталогу> - переменная, указывающая путь к каталогу хранения журналов службы Агента ВРМ;
- TDSK_LOG_USER_DIR=<путь_к_каталогу> - переменная, указывающая путь к каталогу хранения журналов для непривилегированного пользователя.

После установки нужно добавить в автоматическую загрузку и запустить службу termidesk-agent:

```
systemctl enable termidesk-agent.service
systemctl start termidesk-agent.service
```

Проверить состояние службы:

```
systemctl status termidesk-agent.service
```

После установки Агент ВРМ обязательно должен быть настроен.

Установка видеоагента в ОС Альт Рабочая станция

Видеоагент устанавливается в ОС Альт Рабочая станция из rpm-пакета termidesk-video-agent.

Перед установкой видеоагента необходимо:

- установить пакет kernel-headers-modules, соответствующий ядру, загруженному в работающей ОС, пример:

```
apt-get install kernel-headers-modules-std-def
```

Для установки видеоагента:

- переключиться в окружение суперпользователя:

```
su -
```

- выполнить установку termidesk-video-agent:

```
apt-get install <путь_к_пакету>
```

После установки нужно добавить в автоматическую загрузку и запустить службу termidesk-video-agent:

```
systemctl enable termidesk-video-agent.service
systemctl start termidesk-video-agent.service
```

Проверить состояние службы:

```
systemctl status termidesk-video-agent.service
```

Установка Агента смарт-карт в ОС Альт Рабочая станция

Агент смарт-карт устанавливается в ОС Альт Рабочая станция из `rpm`-пакета `termidesk-pcsc-vscard`.

Для установки сессионного Агента:

- переключиться в окружение суперпользователя:

```
su -
```

- выполнить установку `termidesk-pcsc-vscard`:

```
apt-get install <путь_к_пакету>
```

После установки Агент смарт-карт должен быть настроен согласно подразделу **Настройка Агента виртуальных смарт-карт**.

Установка сессионного Агента в ОС Альт Рабочая станция

Сессионный Агент устанавливается в ОС Альт Рабочая станция из `rpm`-пакета `termidesk-session-agent`.

Для установки сессионного Агента:

- переключиться в окружение суперпользователя:

```
su -
```

- выполнить установку `termidesk-session-agent`:

```
apt-get install <путь_к_пакету>
```

- в окне «Лицензионное соглашение» ознакомиться с соглашением и нажать экранную кнопку **[Выход]**;
- на запрос «Принимаете ли вы условия лицензионного соглашения?» подтвердить принятие соглашения, нажав экранную кнопку **[Принимаю]**;
- в окне «Расширенные настройки»:
  - указать путь к каталогу хранения файлов конфигурации. Значение по умолчанию: `/etc/opt/termidesk-session-agent`;
  - указать путь к каталогу хранения журналов. Значение по умолчанию: `/var/log/termidesk`;
  - нажать экранную кнопку **[Далее]**;
- дождаться завершения установки.

Для «тихой» установки без отображения дополнительных окон следует назначить переменные окружения DEBIAN_FRONTEND=noninteractive, SSA_CONFIG_DIR и SSA_LOG_DIR и передать их в команду установки:

```
TDSK_FRONTEND=noninteractive SSA_CONFIG_DIR=<путь_к_каталогу>
SSA_LOG_DIR=<путь_к_каталогу> apt-get install <путь_к_пакету>
```

Где:

- TDSK_FRONTEND=noninteractive - переменная, указывающая запуск в режиме «тихой» установки;
- SSA_CONFIG_DIR=<путь_к_каталогу> - переменная, указывающая путь к каталогу хранения файлов конфигурации. Заменяет значение по умолчанию, если передается непустое значение;
- SSA_LOG_DIR=<путь_к_каталогу> - переменная, указывающая путь к каталогу хранения журналов. Заменяет значение по умолчанию, если передается непустое значение.

После установки изменить настройки можно через файл /etc/default/termidesk-session-agent.

После установки нужно добавить в автоматическую загрузку и запустить службу termidesk-session-agent:

```
systemctl enable termidesk-session-agent.service
systemctl start termidesk-session-agent.service
```

Проверить состояние службы:

```
systemctl status termidesk-session-agent.service
```

После установки сессионный Агент может быть настроен согласно подразделу **Первичная настройка**.

После установки сессионного Агента создастся конфигурационный файл session_agent.ini, а также файл БД SQLite /opt/termidesk/share/termidesk-session-agent/termidesk_ssa.db, предназначенный для сбора и хранения метрик узла. БД инициализируется при запуске сессионного Агента.

Обновление Агентов в ОС Альт Рабочая станция

Обновление Агентов выполняется установкой новой версии поверх предыдущей, кроме Агента ВРМ.

Для обновления Агента ВРМ нужно:

- переключиться в окружение суперпользователя:

```
su -
```

- удалить предыдущую версию (рекомендуется, чтобы корректно обновились права на каталоги для новой версии):

```
apt-get remove -y termidesk-agent
```

- установить новую версию:

```
apt-get install -y termidesk-agent
```

В случае, если обновление компонента «Универсальный диспетчер» произошло раньше обновления сессионного Агента, то на узле с «Универсальным диспетчером» (роль «Портал администратора») нужно:

- в интерфейсе командной строки переключиться на пользователя `termidesk`:

```
sudo -u termidesk bash
```

- выполнить регистрацию сессионного Агента:

```
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_refresh_ssa
```

Удаление Агентов в ОС Альт Рабочая станция

Удаление Агентов выполняется командой:

```
sudo apt-get remove -y <наименование_пакета>
```

Наименования пакетов:

- `termidesk-agent` - Агент ВРМ;
- `termidesk-session-agent` - сессионный Агент.

Вместе с удалением сессионного Агента будет удален файл БД SQLite `termidesk_ssa.db`.

Другие ОС Linux

Установка Агентов в других ОС Linux

Для установки Агентов в гостевой ОС выполнить:

```
sudo yum install <путь_к_пакету>
```

Для установки Агента ВРМ в гостевой ОС:

- выполнить:

```
sudo yum install termidesk-agent
```

В зависимости от дистрибутива ОС Linux, а именно пакетного менеджера, команда установки может отличаться от приведенной.

Для ввода гостевой ОС Debian 12/13 в домен MS AD нужно установить пакеты, которые не являются зависимостями агента: `sssd-tools`, `adcli`, `sssd`, `libnss-sss`, `libpam-sss`.

После установки Агент ВРМ обязательно должен быть настроен.

- в окне «Расширенные настройки» оставить значения по умолчанию или при необходимости изменить значения:
  - «Каталог журналов»: каталог хранения журналов для службы Агента ВРМ. Значение по умолчанию: `/var/log/termidesk`. По умолчанию после установки права на каталог соответствуют `rwxr-xr-x` (в восьмеричной записи - `755`);
  - «Каталог журналов пользователя»: каталог хранения журналов для непривилегированного пользователя. Значение по умолчанию: `~./config/UVEON/logs`;
  - «Каталог настроек»: каталог хранения конфигурационного файла. Значение по умолчанию: `/etc/termidesk`.

Окно «Расширенные настройки» будет показано единожды, если конфигурационный файл `agent.cfg` отсутствует в системе.

Предпочтительные значения в расширенных настройках будут подставлены автоматически. Если настройки были изменены, то значения подставятся с учетом их приоритета:

- в первую очередь подставляются значения из переменных окружения. Все ранее заданные значения конфигурационного файла игнорируются;
- если переменные окружения не заданы, то подставляются значения из конфигурационного файла;
- если ничего из пунктов выше не задано, то применяются значения по умолчанию.

После установки изменить настройки можно:

- через файл `/etc/default/termidesk-agent` (см. подраздел **Конфигурационные файлы Агента ВРМ**);
- через вызов программы `termidesk-agent-config`:

```
sudo termidesk-agent-config setup --dialog
```

Для «тихой» установки без отображения дополнительных окон следует назначить переменные окружения и передать их в команду установки:

```
sudo TDSK_SETUP_NONINTERACTIVE=1 TDSK_CONFIG_DIR=<путь_к_каталогу>
TDSK_LOG_SRV_DIR=<путь_к_каталогу> TDSK_LOG_USER_DIR=<путь_к_каталогу> apt install
termidesk-agent
```

где:

- TDSK_SETUP_NONINTERACTIVE=1 - переменная, указывающая запуск в режиме «тихой» установки;
- TDSK_CONFIG_DIR=<путь_к_каталогу> - переменная, указывающая путь к каталогу с конфигурационным файлом agent.cfg. Например, TDSK_CONFIG_DIR=/etc/termidesk-test;
- TDSK_LOG_SRV_DIR=<путь_к_каталогу> - переменная, указывающая путь к каталогу хранения журналов службы Агента ВРМ;
- TDSK_LOG_USER_DIR=<путь_к_каталогу> - переменная, указывающая путь к каталогу хранения журналов для непривилегированного пользователя.

После установки нужно добавить в автоматическую загрузку и запустить службу termidesk-agent:

```
sudo systemctl enable termidesk-agent.service
sudo systemctl start termidesk-agent.service
```

Проверить состояние службы:

```
sudo systemctl status termidesk-agent.service
```

Обновление Агентов в других ОС Linux

Обновление Агентов выполняется установкой новой версии поверх предыдущей, кроме Агента ВРМ и Агента УВ.

Для обновления Агента ВРМ на ОС Linux нужно:

- удалить предыдущую версию (рекомендуется, чтобы корректно обновились права на каталоги для новой версии):

```
sudo aptitude purge -y termidesk-agent
```

- установить новую версию:

```
sudo apt install -y termidesk-agent
```

Для обновления Агента УВ нужно:

- удалить предыдущую версию (рекомендуется, чтобы корректно обновились права на каталоги для новой версии):

```
sudo aptitude purge -y termidesk-vmsd
```

- установить новую версию:

```
sudo apt install -y termidesk-vmsd
```

Удаление Агентов в других ОС Linux

Удаление Агентов выполняется командой:

```
sudo aptitude purge -y <наименование_пакета>
```

Наименования пакетов:

- `termidesk-agent` - Агент ВРМ;
- `termidesk-session-agent` - сессионный Агент;
- `termidesk-video-agent` - видеоагент;
- `termidesk-pcsc-vscard` - Агент смарт-карт;
- `termidesk-vmsd` - Агент УВ.

Если установка пакета производилась не из локального репозитория, удаление выполняется командой:

```
sudo dpkg -P <наименование_пакета>
```

Вместе с удалением сессионного Агента будет удален файл БД SQLite `termidesk_ssa.db`.

ОС Microsoft Windows

Установка Агента ВРМ в ОС Microsoft Windows

Для установки Агента ВРМ необходимо предварительно подготовить базовое ВРМ с гостевой ОС (см. подраздел **Обязательные настройки гостевой ОС РМ** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»).

Агент ВРМ устанавливается из `msi`-пакета `termidesk-agent`, доступного из поставляемого `iso`-образа. В состав поставляемого пакета по умолчанию включена возможность установки подкомпонентов:

- «Temidesk PCSC Driver» - Агент смарт-карт для перенаправления подключенных к пользовательской рабочей станции смарт-карт в ВРМ;
- «Temidesk Video Agent» - видеоагент для перенаправления видеокамеры с пользовательской рабочей станции в ВРМ.

После запуска пакета необходимо:

- принять лицензионное соглашение;
- в окне «Выборочная установка» убедиться, что отмечены все компоненты, затем нажать экранную кнопку **[Далее]** (см. рисунок Окно установки компонентов Агента ВРМ).

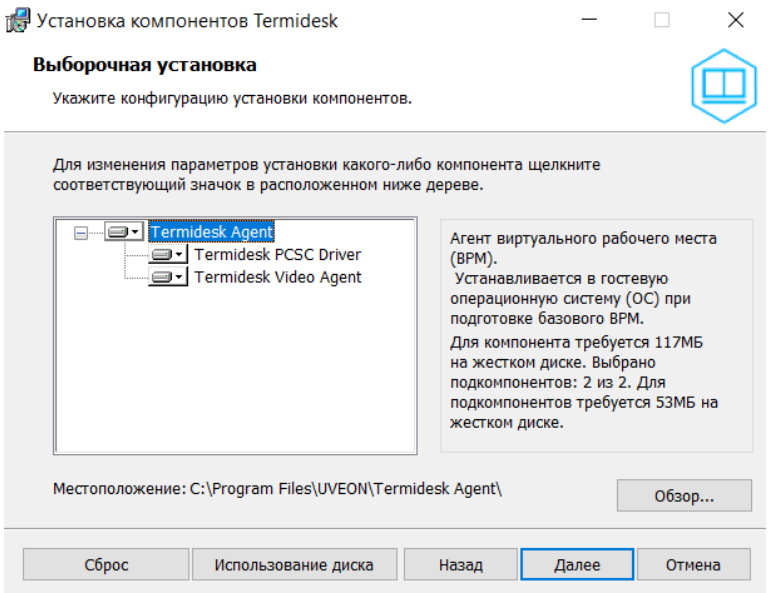


Рисунок 110. Окно установки компонентов Агента ВРМ

- в окне «Настройка редиректора WebDAV» определить максимальный размер файла для передачи через WebDAV и нажать экранную кнопку **[Далее]** (см. рисунок Окно «Настройка редиректора WebDAV»):
  - при активации пункта «Изменить ограничения по умолчанию» Агент ВРМ присваивает значение `4294967295` (4 ГБ, тип `REG_DWORD`) параметру `FileSizeLimitInBytes` в ветке реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters`;
  - при отключении пункта «Изменить ограничения по умолчанию» значение параметра определяется настройками ОС Microsoft Windows (по умолчанию 50 МБ);

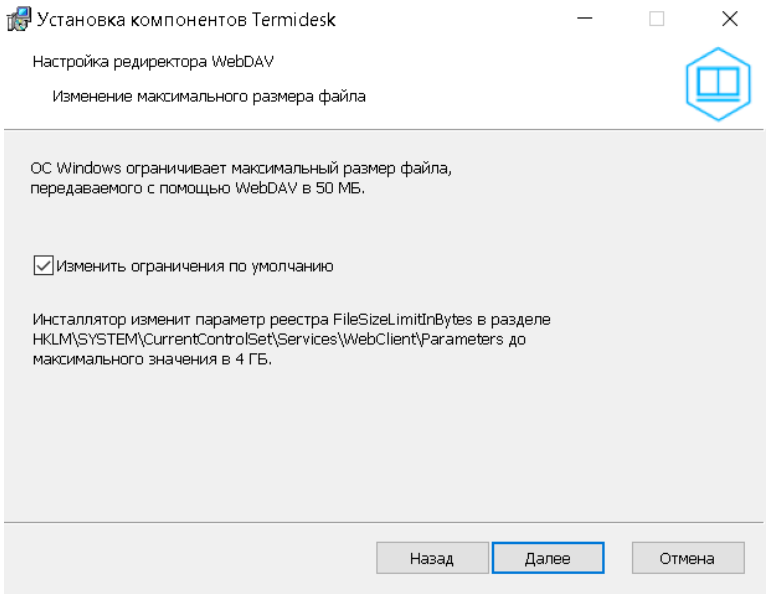


Рисунок 111. Окно «Настройка редиректора WebDAV»

- после выполнения конфигурации следует дождаться завершения установки. Установка произойдет для всех пользователей ОС;
- в окне завершения установки по умолчанию активирован параметр «Запустить мастер настройки приложения» (см. рисунок Завершение установки Агента ВРМ). Для перехода к настройке Агента ВРМ нужно нажать экранную кнопку **[Готово]** и выполнить настройку согласно подразделу **Настройка для ОС Microsoft Windows**. Для выхода из мастера установки без настройки Агента ВРМ нужно снять галочку в параметре «Запустить мастер настройки приложения».

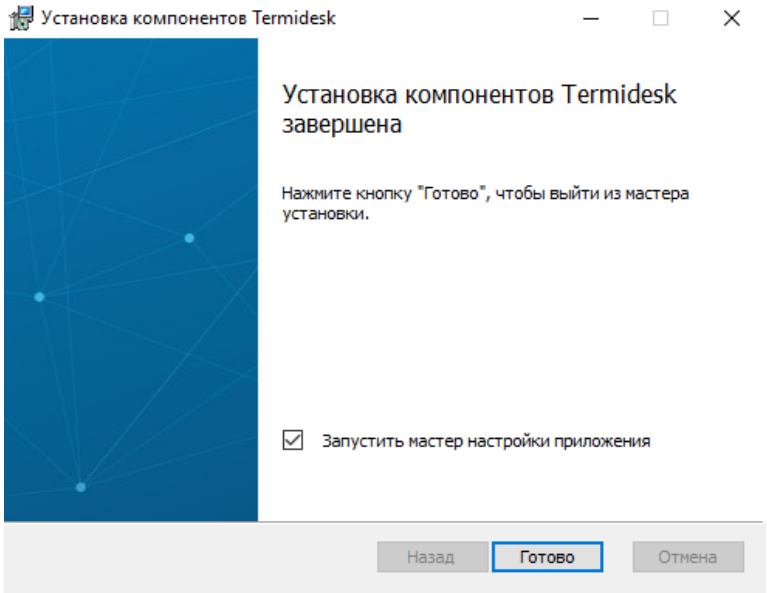


Рисунок 112. Завершение установки Агента ВРМ

После установки:

- будут доступны следующие службы:
  - `Termidesk Agent Daemon` - основная служба Агента ВРМ. Вызывается исполняемым файлом `TermideskAgentDaemon.exe`. По-умолчанию службе назначен тип запуска «Автоматически (отложенный запуск)», при котором ее запуск происходит спустя некоторое время после после запуска всех необходимых для работы служб. При ручном изменении типа запуска Агент ВРМ не будет его менять в значение по-умолчанию при следующем запуске;
  - `Termidesk Pcsc Rights Service` - служба, отвечающая за перенаправление подключенных к пользовательской рабочей станции смарт-карт в ВРМ. Вызывается исполняемым файлом `PcscRights.exe`;
  - `Termidesk Video Agent` - служба, отвечающая за перенаправление видеокамеры с пользовательской рабочей станции в ВРМ. Вызывается исполняемым файлом `video_agent.exe`;
- будет доступно ПО tera-webdav, предоставляющее возможность перенаправления каталога из пользовательской рабочей станции в ВРМ. Запуск ПО tera-webdav выполняется для каждого пользователя после его авторизации в ВРМ с параметрами: `--no-service --rdp-enable`.

Установка Видеоагента в ОС Microsoft Windows

Видеоагент («Termidesk Video Agent») устанавливается в гостевую ОС для корректного перенаправления подключенных к пользовательской рабочей станции веб-камер и входит в состав установочного файла Агента ВРМ.

Установка видеоагента выполняется при установке Агента ВРМ (установочный файл `termidesk-agent_<версия>.msi`).

Установка Агента виртуальных смарт-карт в ОС Microsoft Windows

Агент смарт-карт («Temidesk PCSC Driver») устанавливается в гостевую ОС для корректного перенаправления подключенных к пользовательской рабочей станции смарт-карт в ВРМ и входит в состав установочного файла Агента ВРМ.

Установка Агента смарт-карт выполняется при установке Агента ВРМ (установочный файл termidesk-agent_<версия>.msi).

Установка сессионного Агента в ОС Microsoft Windows

Сессионный Агент устанавливается на сервер терминалов Microsoft Windows Server из msi -пакета termidesk-session-agent.

Для установки сессионного Агента нужно:

- выполнить запуск установочного файла termidesk-session-agent_XXX.msi;
- в окне приветствия нажать кнопку **[Далее]** (см. рисунок Окно приветствия установки сессионного Агента);

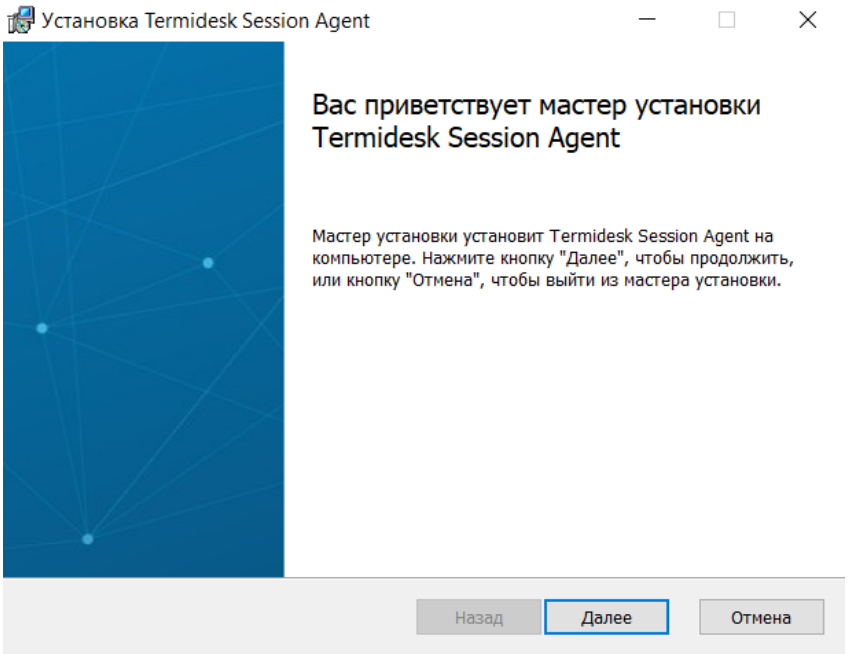


Рисунок 113. Окно приветствия установки сессионного Агента

- принять условия лицензионного соглашения и нажать кнопку **[Далее]** (см. рисунок Окно с условиями лицензионного соглашения);

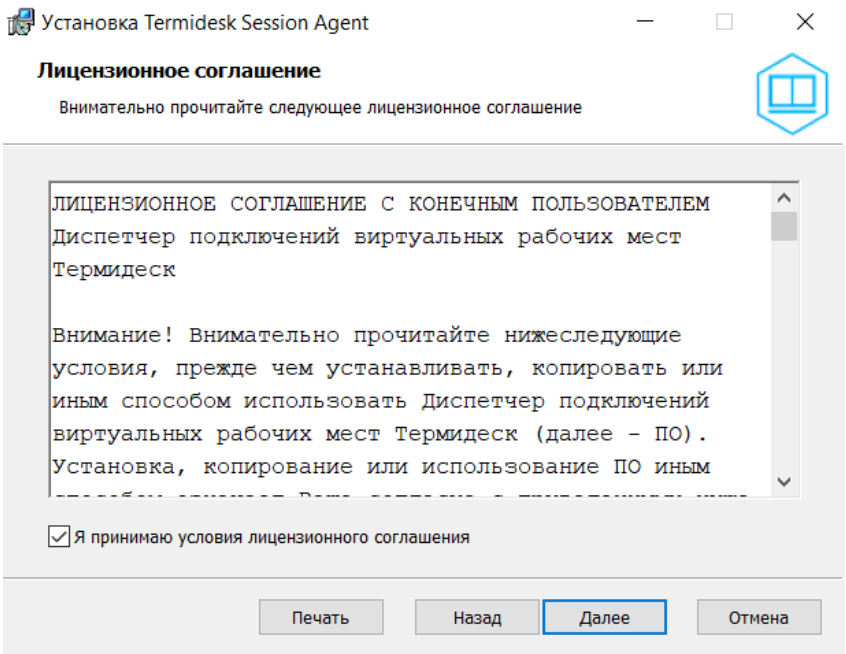


Рисунок 114. Окно с условиями лицензионного соглашения

- выбрать путь установки или оставить его по умолчанию и нажать кнопку **[Далее]** (см. рисунок Окно выбора каталога установки);

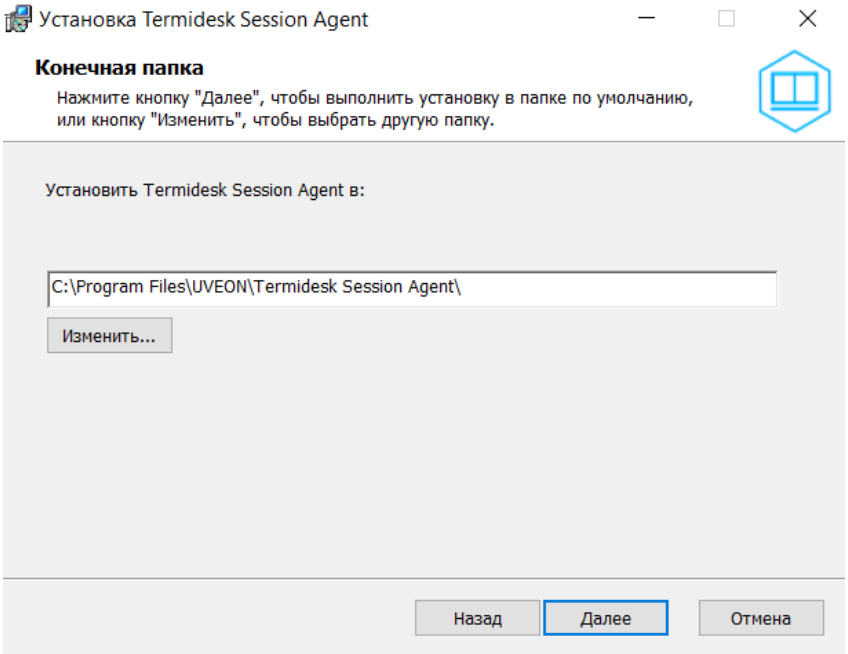


Рисунок 115. Окно выбора каталога установки

- нажать кнопку **[Установить]** для начала процесса установки (см. рисунок Окно подтверждения установки);

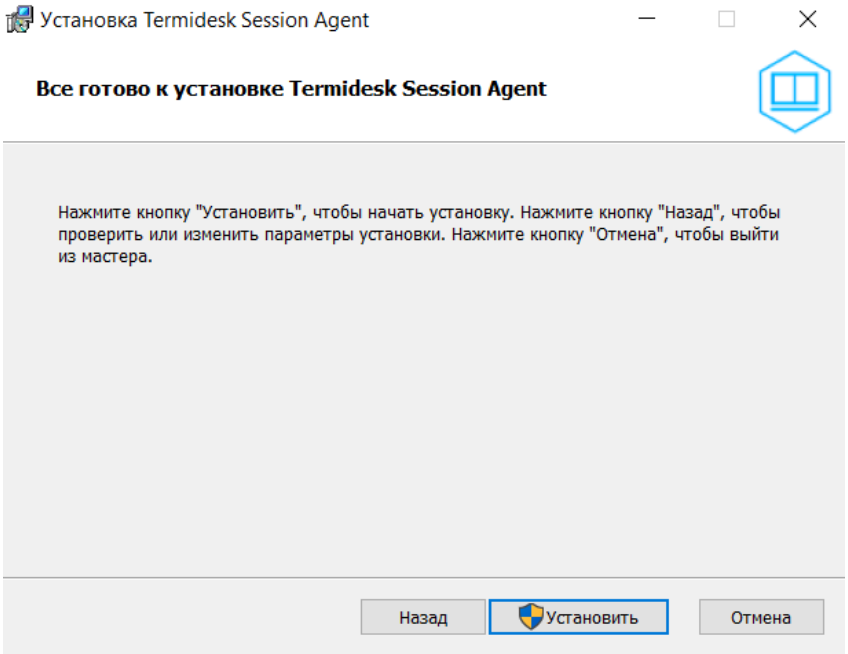


Рисунок 116. Окно подтверждения установки

- завершить работу мастера после установки сессионного Агента, нажав кнопку **[Готово]** (см. рисунок Окно подтверждения перезагрузки системы после установки);
- при появлении сообщения о необходимости перезагрузки нужно согласиться с перезагрузкой системы, нажав кнопку **[OK]** (см. рисунок Окно подтверждения перезагрузки системы после установки). В противном случае установка будет прервана.

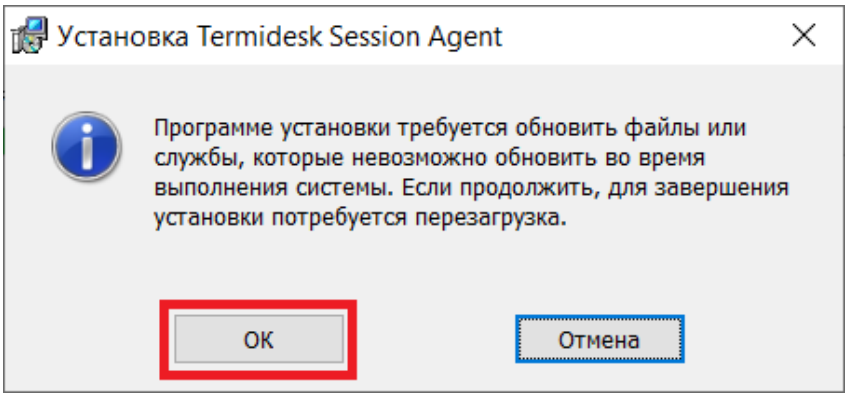


Рисунок 117. Окно подтверждения перезагрузки системы после установки

После установки создастся конфигурационный файл `C:\ProgramData\UVEON\Termidesk Session Agent\session_agent.ini`.

После установки сессионного Агента:

- необходимо создать правило для брандмауэра на открытие порта `31000`;
- при необходимости может быть выполнена настройка согласно подразделу **Первичная настройка**;
- будет создан файл базы данных (БД) SQLite `C:\ProgramData\UVEON\Termidesk Session Agent\log\termidesk_ssa.db`, который предназначен для сбора и хранения метрик узла. БД инициализируется при запуске сессионного Агента.

Установка Агента ВРМ через интерфейс командной строки

Для выполнения тихой установки (silent install) Агента ВРМ через командную строку `cmd.exe` нужно:

- открыть интерфейс командной строки от имени администратора;
- выполнить команду `msiexec`:

```
msiexec /i "<путь_к_пакету_termidesk-agent>.msi" /qn
```

Где:

`/qn` - обеспечивает тихую установку, без отображения окон и сообщений.

По умолчанию вместе с Агентом ВРМ будут установлены Агент смарт-карт («Temidesk PCSC Driver») и видеоагент («Temidesk Video Agent»). Для управления установкой компонентов нужно воспользоваться свойством ADDLOCAL:

- команда установки только Агента ВРМ (при этом другие компоненты установлены не будут):

```
msiexec /i "<путь_к_пакету_termidesk-agent>.msi" ADDLOCAL="Termidesk_Agent" /qn
```

- команда установки только Агента смарт-карт (при этом Агент ВРМ все равно будет установлен):

```
msiexec /i "<путь_к_пакету_termidesk-agent>.msi" ADDLOCAL="Termidesk_PCSC_Driver"
/qn
```

- команда установки только видеоагента (при этом Агент ВРМ все равно будет установлен):

```
msiexec /i "<путь_к_пакету_termidesk-agent>.msi" ADDLOCAL="Termidesk_Video_Agent"
/qn
```

При установке Агента ВРМ может быть задан максимальный размер файла, передаваемого через WebDAV. Для управления конфигурацией следует воспользоваться свойством `WEBDAVFILESIZELIMITINBYTES` с нужным значением:

- `1` - присваивает значение `4294967295` (4 ГБ, тип `REG_DWORD`) параметру `FileSizeLimitInBytes` в ветке реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters`;
- `0` - устанавливает параметр `FileSizeLimitInBytes` в исходное значение ОС Microsoft Windows - `52428800` (50 МБ).

Сценарии установки:

- первая установка в тихом режиме. При первой установке Агента ВРМ без свойства `WEBDAVFILESIZELIMITINBYTES` будет применено значение по умолчанию - `0` (максимальный размер файла определяется ОС Microsoft Windows - 50 МБ);
- установка поверх предыдущей версии:

- если ранее Агент ВРМ был установлен со свойством `WEBDAVFILESIZELIMITINBYTES=0` или без него и необходимо изменить конфигурацию, то выполнить, используя ту же версию пакета:

```
msiexec /i "<путь_к_пакету_termidesk-agent>.msi" WEBDAVFILESIZELIMITINBYTES=1
/qn
```

- если ранее Агент ВРМ был установлен со свойством `WEBDAVFILESIZELIMITINBYTES=1` и необходимо изменить конфигурацию, то выполнить, используя ту же версию пакета:

```
msiexec /i "<путь_к_пакету_termidesk-agent>.msi" WEBDAVFILESIZELIMITINBYTES=0
/qn
```

Обновление Агентов в ОС Microsoft Windows

Обновление Агентов выполняется установкой новой версии поверх предыдущей.

В случае, если обновление компонента «Универсального диспетчера» произошло раньше обновления сессионного Агента, то на узле с «Универсальным диспетчером» (роль «Портал администратора») нужно:

- в интерфейсе командной строки переключиться на пользователя `termidesk`:

```
sudo -u termidesk bash
```

- выполнить регистрацию сессионного Агента:

```
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_refresh_ssa
```

Удаление Агентов в ОС Microsoft Windows

Удаление Агентов из среды ОС Microsoft Windows выполняется через «Пуск - Панель управления - Удаление программы». Необходимо выбрать из списка установленных программ компонент и нажать экранную кнопку **[Удалить]**.

При удалении Агента восстанавливается исходное значение параметра `FileSizeLimitInBytes` в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters`.

Вместе с удалением сессионного Агента будет удален файл БД SQLite `termidesk_ssa.db`.

АГЕНТ. НАСТРОЙКИ

Переменные окружения и аргументы командной строки

Переменные окружения и другие параметры конфигурирования

В Termidesk VDI используются переменные окружения для указания параметров настройки компонентов программного комплекса.

Для включения переопределения значений параметров Агента ВРМ через переменные окружения используются два способа:

- активация параметра «Разрешить переопределение значений через переменные окружения» в графическом интерфейсе Агента ВРМ. Для ОС Linux должен быть задан файл с перечислением переменных окружения и их значениями `/etc/default/termidesk-agent`;
- или назначение параметру `env` значения `True` в конфигурационном файле `/etc/termidesk/agent.cfg`. Для ОС Linux должен быть задан файл с перечислением переменных окружения и их значениями `/etc/default/termidesk-agent`.

Для других Агентов дополнительные действия не требуются.

В ОС Microsoft Windows задание настроек Агента ВРМ может быть выполнено из командной строки. Для этого:

- открыть командную строку от имени администратора;
- вызывать Агент ВРМ из каталога `C:\Program Files\UVEON\Termidesk Agent\TermideskAgentConfig.exe`;
- выполнить:

```
"C:\Program Files\UVEON\Termidesk Agent\TermideskAgentConfig.exe" update --host
192.0.2.30 --key 0123456789 --loglevel 20000 --httpd-port=43900
```

где:

`--host 192.0.2.30` - IP-адрес компонента «Универсальный диспетчер» («Портала администратора»);

`--key 0123456789` - значение мастер-ключа для подключения к компоненту «Универсальный диспетчер» («Порталу администратора»);

`--loglevel 20000` - категория сообщений;

`--httpd-port=43900` - порт Агента ВРМ.

Пример получения полной информации по доступным аргументам командной строки с выводом в файл `C:\agent_help_all.txt`:

```
"C:\Program Files\UVEON\Termidesk Agent\TermideskAgentConfig.exe" -h >
C:\agent_help_all.txt
```

Агент ВРМ также предусматривает возможность конфигурирования переносимых профилей и настройки аутентификации пользователей ВРМ через файл с помощью модуля `pam_tdsk`. Для подробной информации следует обратиться к подразделам **Перемещаемые профили**, **Технология единого входа**, **Настройка аутентификации пользователей ВРМ через файл**документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

Перечень переменных окружения и аргументов CLI, используемых Агентами, приведены далее в таблицах:

- переменные окружения Агента ВРМ (см. таблицу Переменные окружения и аргументы CLI Агента ВРМ);
- переменные окружения Агента УВ (см. таблицу Переменные окружения Агента УВ);
- переменные окружения видеоагента (см. таблицу Переменные окружения и аргументы CLI видеоагента);
- переменные окружения Агента смарт-карт (см. таблицу Переменные окружения Агента смарт-карт);
- переменные окружения сессионного Агента (см. таблицу Переменные окружения сессионного Агента).

Таблица 182. Переменные окружения и аргументы CLI Агента ВРМ

Переменная окружения	Значение по умолчанию	Описание	Аргумент командной строки
`TDSK_AD_JOIN_METHOD`	`Не задано`	Управляет способом ввода ВРМ в домен MS AD. Переменная окружения используется только в ОС Linux. Возможные значения: • `adcli` - ввод ВРМ в домен MS AD с использованием утилиты `adcli`; • `samba` - ввод ВРМ в домен MS AD с использованием средств пакета `samba`	`Не задано`
`TDSK_VDI_URL`	`Не задано`	Задает URL-адрес компонента «Универсальный диспетчер» («Портала администратора») для подключения к нему	`--host`
`TDSK_VDI_KEY`	`Не задано`	Задает значение мастер-ключа для подключения к компоненту «Универсальный диспетчер» («Порталу администратора»). Для получения значения мастер-ключа в «Портале администратора» нужно перейти «Системные параметры - Системные настройки - Безопасность»	`--key`

Переменная окружения	Значение по умолчанию	Описание	Аргумент командной строки
TDSK_VDI_LOGLEVEL	20000	Задает категорию сообщений, которые будут записываться в журнал Агента BPM. Возможные значения (может указываться как цифровое значение, так и буквенное): • 20000 - соответствует уровню DEBUG; • 30000 - соответствует уровню INFO; • 40000 - соответствует уровню WARN; • 30000 - соответствует уровню ERROR; • 40000 - соответствует уровню FATAL. Пример для ОС Linux: ``` sudo termidesk-agent-config update --loglevel 20000 sudo termidesk-agent-config update --loglevel INFO ``` Пример для ОС Microsoft Windows: ``` "C:\Program Files\UVEON\Termidesk Agent\TermideskAgentConfig.exe" update --loglevel 20000 "C:\Program Files\UVEON\Termidesk Agent\TermideskAgentConfig.exe" update --loglevel INFO ```	--loglevel

Переменная окружения	Значение по умолчанию	Описание	Аргумент командной строки

Не задано	Не задано	Управление режимом подстановки значений параметров из переменных окружения.
		
		Возможные значения:
		
		• True - использовать подстановку значений параметров из переменных окружения;
		• False - не использовать подстановку значений параметров из переменных окружения.
		
		Если не задать значение, то будет использоваться True.
		
		Пример для ОС Linux:
		
		`sudo termidesk-agent-config update --env=True`
		`sudo termidesk-agent-config update --env`
		
		Пример для ОС Microsoft Windows:
		
		`"C:\Program Files\UVEON\Termidesk Agent\TermideskAgentConfig.exe" update --env=True`
		`"C:\Program Files\UVEON\Termidesk Agent\TermideskAgentConfig.exe" update --env`
			--env

TDSK_METRIC_INTERVAL	3	Интервал (в секундах) получения и обновления метрик узла Агентом ВРМ. Переменная окружения доступна с версии 5.1. По умолчанию интервал 3 секунды, однако через REST API получить метрики можно в любой момент	Не задано
SSSD_DEFAULT_CONF	/etc/sssd/sssd.conf	Задает путь к конфигурационному файлу, в котором задано значение параметра use_fully_qualified_names. В зависимости от значения параметра use_fully_qualified_names будут применены действия: • суффикс домена не будет подставлен, если use_fully_qualified_names = False или отсутствует; • суффикс домена будет подставлен, если use_fully_qualified_names = True	Не задано
TDSK_LOG_ROTATE_COUNT	5	Задает максимальное количество файлов журналов. Переменная окружения доступна с версии 6.0	Не задано

Переменная окружения	Значение по умолчанию	Описание	Аргумент командной строки
TDSK_LOG_ROTATE_MAX_SIZE	10	Задает максимальный размер (МБ) файла журнала. Переменная окружения доступна с версии 6.0	Не задано
LOUDPLAY_LISTEN_IPV4	127.0.0.1	Задает IP-адрес сервера Loudplay для взаимодействия с ним	Не задано
LOUDPLAY_LISTEN_PORT	10061	Задает порт сервера Loudplay для взаимодействия с ним	Не задано
LOUDPLAY_CONNECT_DELAY	30	Задает время ожидания (в секундах), по истечении которого Агент ВРМ отключит неактивную сессию пользователя на сервере Loudplay	Не задано

TDSK_CONFIG_DIR	Не задано	Задает место хранения файлов конфигурации Агента ВРМ.
		
		Пример: администратор хочет изменить место хранения файла конфигурирования Агента ВРМ.
		
		Для этого ему нужно:
		
		• создать файл agent.cfg с настройками или скопировать его из /etc/termidesk;
		• поместить agent.cfg в нужный каталог. Каталог должен обладать свойствами:
		  ▫ права доступа: rw-r—r-- (в восьмеричной записи - 644);
		  ▫ владелец и группа: root:root;
		• создать файл /etc/default/termidesk-agent. Указать в нем каталог, откуда будет считан конфигурационный файл:
		
		`TDSK_CONFIG_DIR=/etc/opt/termidesk`
		
		• перезапустить службу termidesk-agent:
		
		`sudo systemctl restart termidesk-agent`
			Не задано

TDSK_HTTP_PORT	43900	Сетевой порт HTTP-сервера Агента ВРМ. ⚠ Начиная с Termidesk VDI версии 6.1 для работы Агента ВРМ более не выбираются случайные RPC-порты из диапазона 43900-44000. Теперь порт задаются вручную через конфигурационный файл или через переменную окружения. Если порт не задан, то используется значение по умолчанию. Возможные значения: от 1 до 65535	--httpd-port

Переменная окружения	Значение по умолчанию	Описание	Аргумент командной строки
TDSK_HTTP_INTERFACE	Не задано	Сетевой интерфейс, используемый для подключения к компоненту «Универсальный диспетчер». Переменная окружения доступна с версии 7.0. В качестве значения используется наименование сетевого интерфейса. Пример для ОС Linux: `Если значение не задано, либо указанный интерфейс отсутствует, то выбор сетевого интерфейса выполняется автоматически`	Не задано
TDSK_LOG_SRV_DIR	Не задано	Каталог хранения журналов службы Агента ВРМ	Не задано
TDSK_LOG_USER_DIR	Не задано	Каталог хранения журналов для непривилегированного пользователя	Не задано
TDSK_SETUP_NONINTERACTIVE	Не задано	«Тихий» режим установки. Возможные значения: • 1 - активировать режим. Используется при необходимости установки Агента ВРМ без отображения дополнительных окон	Не задано
TERA_QXL_CONFIG_FILE	Не задано	Путь к конфигурационному файлу TERA для ВМ. Используется для считывания параметров, заданных в настройках TERA. Если значение не задано, то используется путь /etc/X11/xorg.conf.d/30-teraqxl.xorg.conf	Не задано
TDSK_SSO_WAITING_TIMEOUT	60	Время (в секундах) задержки подключения ПО Termidesk Viewer к РМ при использовании технологии единого входа (SSO). Переменная ограничивает время, по истечении которого Агент ВРМ уведомит компонент «Клиент» о неудачной процедуре SSO. Значение менять не рекомендуется: при штатном сценарии вход в систему выполняется быстрее установленного лимита. Изменение значения может потребоваться только в случаях отладки и при возникновении проблем с подключением	Не задано

Таблица 183. Переменные окружения Агента УВ

Переменная окружения	Значение по умолчанию	Описание

TVMD_ILEVEL_SOCKET	63	Задает значение метки целостности на создаваемый TVMD -сокет. Параметр задается в конфигурационном файле /etc/termidesk/termidesk-vmsd.conf.
		
		По умолчанию после установки конфигурационный файл может не существовать. В этом случае нужно:
		
		• создать каталог /etc/termidesk/:
		
		`sudo mkdir /etc/termidesk`
		
		• изменить права на каталог:
		
		`sudo chmod 755 /etc/termidesk`
		
		• создать конфигурационный файл:
		
		`sudo touch /etc/termidesk/termidesk-vmsd.conf`
		
		• изменить права на файл:
		
		`sudo chmod 644 /etc/termidesk/termidesk-vmsd.conf`
		
		Изменение значения метки целостности может понадобиться, если ОС имеет уровень целостности, отличный от 16. При возникновении ситуации, когда уровень целостности ОС отличается от 16, следует:
		
		• узнать текущий уровень целостности, выставляемый ОС для ВМ, командой:
		
		`cat /etc/libvirt/libvirtd.conf | grep ilev_vm`
		
		• если полученный уровень отличается, то добавить параметр TVMD_ILEVEL_SOCKET с нужным значением уровня (например,TVMD_ILEVEL_SOCKET=16) в конфигурационный файл /etc/termidesk/termidesk-vmsd.conf

LIBVIRT_PASSWORD_SCRIPT	Не задано	Задает путь для исполняемого файла, реализующего альтернативный механизм сброса сессий (см. подраздел **Использование альтернативного механизма сброса сессий**)

Таблица 184. Переменные окружения и аргументы CLI видеоагента

Переменная окружения	Значение по умолчанию	Описание	Аргумент командной строки
TDSK_DEBUG	Не задано	Включение режима отладки. Возможные значения: yes	Не задано

Переменная окружения	Значение по умолчанию	Описание	Аргумент командной строки
Не задано	Не задано	Вывод справки по использованию аргументов командной строки. Для вызова справки нужно выполнить: `sudo /usr/local/sbin/video_agent -h`	-h
Не задано	/dev/video0	Устройство вывода видео	-o
Не задано	Не задано	Вывод версии приложения. Для вывода версии нужно выполнить: `sudo /usr/local/sbin/video_agent -v`	-v
TDSK_VIDEO_CODEC	libtheora	Кодек видеокамеры. Возможные значения: • libtheora - нативный метод кодирования Theora; • theora - кодирование через конвейер Gstreamer	-c

Таблица 185. Переменные окружения Агента смарт-карт

Переменная окружения	Значение по умолчанию	Описание
TDSK_DEBUG	Не задано	Включение режима отладки. Может также использоваться файл /etc/reader.conf.d/exconf/vscard (см. подраздел **Настройка Агента виртуальных смарт-карт**). Возможные значения: yes

Таблица 186. Переменные окружения сессионного Агента

Переменная окружения	Значение по умолчанию	Описание

CONFIG_DIR	/etc/opt/termidesk-session-agent	Задает каталог хранения конфигурационных файлов сессионного Агента.
		
		Пример: администратор хочет изменить место хранения файла конфигурирования сессионного Агента.
		
		Для этого нужно:
		
		• создать файл session_agent.ini с настройками или скопировать его из существующего каталога;
		• поместить session_agent.ini в нужный каталог. Каталог должен обладать свойствами:
		  права доступа: rwxr-xr-x (в восьмеричной записи - 755);
		  владелец и группа: termidesk:termidesk;
		• создать файл /etc/default/termidesk-session-agent (если он не существует). Указать в нем каталог в переменной CONFIG_DIR, откуда будет считан конфигурационный файл. Пример:
		
		`CONFIG_DIR=/etc/opt/termidesk/session-agent`
		
		• перезапустить службу termidesk-session-agent.service:
		
		`sudo systemctl restart termidesk-session-agent.service`

Агент ВРМ

Конфигурационные файлы Агента ВРМ

Конфигурационный файл Агента ВРМ

Для настройки Агента ВРМ используется конфигурационный файл:

- в ОС Linux - /etc/termidesk/agent.cfg;

> Администратор может изменить каталог хранения файла в ОС Linux на этапе установки или через переменную окружения TDSK_CONFIG_DIR, указанную в файле /etc/default/termidesk-agent.

- в ОС Microsoft Windows - конфигурационный файл упакован и размещен в реестре по пути HKEY_LOCAL_MACHINE\Software\Termidesk\Agent.

Параметры, доступные в конфигурационном файле для ОС Linux, приведены в таблице (см. таблицу Параметры конфигурирования Агента ВРМ в ОС Linux).

Таблица 187. Параметры конфигурирования Агента ВРМ в ОС Linux

Параметр	Значение по умолчанию	Описание
Секция [agent]		
adJoinMethod	Не задано	Управление способом ввода ВРМ в домен MS AD. Возможные значения: • adcli - ввод ВРМ в домен MS AD с использованием утилиты adcli; • samba - ввод ВРМ в домен MS AD с использованием средств пакета samba
env	False	Управление режимом переопределения параметров через переменные окружения (см. подраздел **Переменные окружения и аргументы командной строки**). Для ОС Linux должен быть задан файл /etc/default/termidesk-agent с перечислением переменных окружения и их значениями (см. подраздел **Конфигурационные файлы Агента ВРМ**). Возможные значения: • True - режим включен. Значения параметров переопределяются через переменные окружения; • False - режим отключен
host	Не задано	IP-адрес или FQDN компонента «Универсальный диспетчер» («Портала администратора»). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-kv://secret#agent/host
hostSSL	ssl_host	SSL-профиль (настройки SSL) для HTTP-клиента. Профиль задается ниже в секции [ssl_host]. Может быть задано несколько SSL-профилей
httpSSL	ssl_http	SSL-профиль для HTTP-сервера. Профиль задается ниже в секции [ssl_http]. Может быть задано несколько SSL-профилей
httpSSLasHost	False	Управление режимом использования SSL-профиля HTTP-сервера для запросов к компоненту «Универсальный диспетчер». Возможные значения: • True - использовать SSL-профиль HTTP-сервера для запросов к компоненту «Универсальный диспетчер»; • False - не использовать SSL-профиль HTTP-сервера для запросов к компоненту «Универсальный диспетчер»

Параметр	Значение по умолчанию	Описание
`httpPort`	`43900`	Сетевой порт HTTP-сервера Агента BPM. Начиная с Termidesk VDI версии 6.1 для работы Агента BPM более не выбираются случайные RPC-порты из диапазона 43900-44000. Теперь порт задается вручную через конфигурационный файл или через переменную окружения. Если порт не задан, то используется значение по умолчанию. Возможные значения: от 1 до 65535
`httpInterface`	`Не задано`	Сетевой интерфейс, используемый для подключения к компоненту «Универсальный диспетчер». IP-адреса выбранного интерфейса должны находиться в маршрутизируемой сети и быть доступны компоненту «Универсальный диспетчер» после публикации фонда РМ. В качестве значения используется наименование сетевого интерфейса. Пример использования: `httpInterface = enp6s0` Если значение не задано, либо указанный интерфейс отсутствует, то выбор сетевого интерфейса выполняется автоматически
`vault`	`vault_host`	Профиль защищенного хранилища секретов. Параметры профиля задаются в секции `[vault_host]`. Может быть задано несколько профилей защищенного хранилища секретов
`metrics`	`metrics_host`	Профиль хранения метрик. Параметры профиля задаются в секции `[metrics_host]`
`masterKey`	`Не задано`	Значение мастер-ключа для подключения к компоненту «Универсальный диспетчер». Для получения значения мастер-ключа нужно перейти в «Портале администратора»: «Системные параметры - Системные настройки - Безопасность». Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/masterKey`
`logLevel`	`20000`	Степень детализации служебных сообщений. Возможные значения: • `20000` - соответствует уровню DEBUG; • `30000` - соответствует уровню INFO; • `40000` - соответствует уровню WARN; • `50000` - соответствует уровню ERROR; • `60000` - соответствует уровню FATAL

Параметр	Значение по умолчанию	Описание
logoffSignal	0	Управление сигналом завершения сессии через утилиту loginctl. WARNING: Значение параметра применяется только к новым сессиям и не влияет на активные сессии. При значении 0 по умолчанию используется сигнал SIGTERM (15). Возможные значения: от 0 до 33
logSrvDir	/var/log/termidesk	Каталог хранения журналов службы Агента ВРМ. По умолчанию после установки права на каталог соответствуют rwxr-xr-x (в восьмеричной записи - 755)
logUserDir	~/config/UVEON/logs	Каталог хранения журналов для непривилегированного пользователя
mtls	DISABLED	Режим mTLS для защищенного подключения и взаимной аутентификации. Возможные значения: • DISABLED (по умолчанию) - сертификаты игнорируются, их проверка не производится. Агент ВРМ использует самоподписанный сертификат, если является «Сервером». В этом режиме mTLS не используется; • PERMISSIVE - нестрогий режим проверки сертификата. Проверка выполняется, но если сертификат не предоставлен или он недействительный, то он не проверяется. Соединение при этом продолжает работать; • STRICT - строгий режим проверки сертификата. Предоставление действительных сертификатов обязательно. Соединение сбрасывается, если сертификат не прошел проверку
certSource	Не задано	Тип хранилища сертификатов. Возможные значения: • FILESYSTEM - сертификаты располагаются локально, в файловой системе; • VAULT - сертификаты располагаются во внешнем защищенном хранилище сертификатов
ssl	True	Управление режимом подключения к компоненту «Универсальный диспетчер». Начиная с Termidesk 6.1 подключение всегда выполняется по протоколу HTTPS. Менять значение не рекомендуется
rebootAfterOperation	True	Необходимость перезагрузки ОС, если узел переименуется. Параметр действует только в ОС Linux. Возможные значения: • True - ОС будет перезагружена, если узел переименуется; • False - ОС не будет перезагружена
Секция [ssl_host]		

Параметр	Значение по умолчанию	Описание
ca	Не задано	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент ВРМ автоматически заменяет значение {{fqdn}} на FQDN РМ. Также допускается ручное указание FQDN РМ
certificate	Не задано	Путь к клиентскому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}#example-dot-com/certificate В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент ВРМ автоматически заменяет значение {{fqdn}} на FQDN РМ. Также допускается ручное указание FQDN РМ
certificateKey	Не задано	Путь к клиентскому закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент ВРМ автоматически заменяет значение {{fqdn}} на FQDN РМ. Также допускается ручное указание FQDN РМ
passphrase	Не задано	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-kv://secret#agent/passphrase
Секция [ssl_http]		
ca	Не задано	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент ВРМ автоматически заменяет значение {{fqdn}} на FQDN РМ. Также допускается ручное указание FQDN РМ

Параметр	Значение по умолчанию	Описание
certificate	Не задано	Путь к серверному сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}#example-dot-com/certificate В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент ВРМ автоматически заменяет значение {{fqdn}} на FQDN РМ. Также допускается ручное указание FQDN РМ
certificateKey	Не задано	Путь к серверному закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент ВРМ автоматически заменяет значение {{fqdn}} на FQDN РМ. Также допускается ручное указание FQDN РМ
passphrase	Не задано	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-kv://secret#agent/passphrase
Секция [vault_host]		
role_id	Не задано	Идентификатор роли, используемый для взаимодействия с защищенным хранилищем секретов
ttl	3600	Время (в секундах) жизни токена, использующегося для аутентификации при подключении к защищенному хранилищу секретов
ttl_deadline	30	Оставшееся время (в секундах) актуальности токена, по достижении которого он будет обновлен
timeout	1	Время ожидания (в секундах) подключения к защищенному хранилищу секретов
token	Не задано	Путь к файлу с токеном подключения к защищенному хранилищу секретов
url	Не задано	URL-адрес подключения к защищенному хранилищу секретов
Секция [metrics_host]		
interval	3	Периодичность (в секундах) опроса и сохранения метрик сессий
filepath	Не задано	Путь к файлу хранения сведений о метриках сессий. Если значение не задано, то используется /var/lib/termidesk/agent/metrics.json

Параметры, доступные для ОС Microsoft Windows, приведены в таблице (см. таблицу Параметры конфигурирования Агента ВРМ в ОС Microsoft Windows).

Таблица 188. Параметры конфигурирования Агента ВРМ в ОС Microsoft Windows

Параметр	Тип	Описание
Каталог реестра HKEY_LOCAL_MACHINE\SOFTWARE\Termidesk\Agent\Policies		

Параметр	Тип	Описание
HKLMReboot	dword	Параметр определяет необходимость перезагрузки ОС после изменения реестра ОС. Возможные значения: • 00000000 - если политики реестра изменились, ОС не будет перезагружена; • 00000001 - если политики реестра изменились, ОС будет перезагружена. Если параметр отсутствует, то: • для Агента ВРМ версии ниже 6.1 ОС будет перезагружаться после обновления реестра; • для Агента ВРМ версии 6.1 и выше ОС не будет перезагружаться после обновления реестра

PrinterRedirectPolicy	dword	Параметр определяет работу функционала перенаправления принтеров на стороне Агента ВРМ.
		
		Возможные значения:
		
		• 00000000 - перенаправление принтеров запрещено;
		• 00000001 - перенаправление принтеров разрешено.
		
		Значение по умолчанию: 00000001.
		
		Особенности работы:
		
		• Агент ВРМ при создании РМ вне зависимости от политики Termidesk VDI записывает значение в реестр:
		  - 00000000 (разрешить перенаправление) в HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\fDisableCpm;
		  - 00000001 (разрешить перенаправление) в HKEY_LOCAL_MACHINE\SOFTWARE\Termidesk\Agent\Policies;
		• после применения значения Агент ВРМ перегружает РМ;
		• Агент ВРМ отслеживает значение параметра реестра fDisableCpm. Если оно изменилось, то Агент ВРМ фиксирует событие изменения в журнале РМ, не пытаясь обновить реестр

Каталог реестра HKEY_LOCAL_MACHINE\SOFTWARE\Termidesk\Agent\Store		
env	dword	Управление режимом переопределения параметров через переменные окружения (см. подраздел **Переменные окружения и аргументы командной строки**). Возможные значения: • 1 - режим включен. Значения параметров переопределяются через переменные окружения; • 0 (по умолчанию) - режим отключен
host	sz	IP-адрес или FQDN компонента «Универсальный диспетчер» («Портала администратора»). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-kv://secret#agent/host

Параметр	Тип	Описание
`httpInterface`	`sz`	Сетевой интерфейс, используемый для подключения к компоненту «Универсальный диспетчер». IP-адреса выбранного интерфейса должны находиться в маршрутизируемой сети и быть доступны компоненту «Универсальный диспетчер» после публикации фонда РМ. В качестве значения используется наименование сетевого интерфейса. Если значение не задано, либо указанный интерфейс отсутствует, то выбор сетевого интерфейса выполняется автоматически
`httpPort`	`dword`	Сетевой порт HTTP-сервера Агента ВРМ. Начиная с Termidesk версии 6.1 для работы Агента ВРМ более не выбираются случайные RPC-порты из диапазона 43900-44000. Теперь порт задается вручную через конфигурационный файл или через переменную окружения. Если порт не задан, то используется значение по умолчанию. Возможные значения: от 1 до 65535 Значение по умолчанию: 43900
`logLevel`	`sz`	Степень детализации служебных сообщений. Возможные значения: • `DEBUG`; • `INFO`; • `WARN`; • `ERROR`; • `FATAL`
`masterKey`	`sz`	Значение мастер-ключа для подключения к компоненту «Универсальный диспетчер». Для получения значения мастер-ключа нужно перейти в «Портале администратора»: «Системные параметры - Системные настройки - Безопасность». Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/masterKey`
`modifyTimeStamp`	`dword`	Время Unix последнего изменения конфигурации Агента ВРМ

Параметр	Тип	Описание
mtls	sz	Режим mTLS для защищенного подключения и взаимной аутентификации. Возможные значения: • DISABLED (по умолчанию) - сертификаты игнорируются, их проверка не производится. Агент ВРМ использует самоподписанный сертификат, если является «Сервером». В этом режиме mTLS не используется; • PERMISSIVE - нестрогий режим проверки сертификата. Проверка выполняется, но если сертификат не предоставлен или он недействительный, то он не проверяется. Соединение при этом продолжает работать; • STRICT - строгий режим проверки сертификата. Предоставление действительных сертификатов обязательно. Соединение сбрасывается, если сертификат не прошел проверку
Каталог реестра HKEY_LOCAL_MACHINE\SOFTWARE\Termidesk\Agent\Store\ssl_host		
ca	sz	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент ВРМ автоматически заменяет значение {{fqdn}} на FQDN РМ. Также допускается ручное указание FQDN РМ
certificate	sz	Путь к клиентскому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}#example-dot-com/certificate В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент ВРМ автоматически заменяет значение {{fqdn}} на FQDN РМ. Также допускается ручное указание FQDN РМ
certificateKey	sz	Путь к клиентскому закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент ВРМ автоматически заменяет значение {{fqdn}} на FQDN РМ. Также допускается ручное указание FQDN РМ
MSx509Location	sz	Область хранилища сертификатов ОС Microsoft Windows. Возможные значения: • MACHINE - хранилище сертификатов, доступных всем пользователям ОС. Находится в системном реестре в HKEY_LOCAL_MACHINE; • USER - хранилище сертификатов, доступных текущему пользователю ОС. Находится в системном реестре в HKEY_CURRENT_USER
MSx509Use	sz	Отпечаток сертификата, выбранного в хранилище сертификатов ОС Microsoft Windows

Параметр	Тип	Описание
passphrase	sz	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-kv://secret#agent/passphrase
Каталог реестра HKEY_LOCAL_MACHINE\SOFTWARE\Termidesk\Agent\Store\ssl_http		
ca	sz	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент ВРМ автоматически заменяет значение {{fqdn}} на FQDN РМ. Также допускается ручное указание FQDN РМ
certificate	sz	Путь к серверному сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}.com#example-dot-com/certificate В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент ВРМ автоматически заменяет значение {{fqdn}} на FQDN РМ. Также допускается ручное указание FQDN РМ
certificateKey	sz	Путь к серверному закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент ВРМ автоматически заменяет значение {{fqdn}} на FQDN РМ. Также допускается ручное указание FQDN РМ
MSx509Location	sz	Область хранилища сертификатов ОС Microsoft Windows. Возможные значения: • MACHINE - хранилище сертификатов, доступных всем пользователям ОС. Находится в системном реестре в HKEY_LOCAL_MACHINE; • USER - хранилище сертификатов, доступных текущему пользователю ОС. Находится в системном реестре в HKEY_CURRENT_USER
MSx509Use	sz	Отпечаток сертификата, выбранного в хранилище сертификатов ОС Microsoft Windows
passphrase	sz	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-kv://secret#agent/passphrase
Каталог реестра HKEY_LOCAL_MACHINE\SOFTWARE\Termidesk\Agent\Store\vault_host		
role_id	sz	Идентификатор роли, используемый для взаимодействия с защищенным хранилищем секретов

Параметр	Тип	Описание
timeout	dword	Время ожидания (в секундах) подключения к защищенному хранилищу секретов
token	sz	Путь к файлу с токеном подключения к защищенному хранилищу секретов
ttl	dword	Время (в секундах) жизни токена, использующегося для аутентификации при подключении к защищенному хранилищу секретов
url	sz	URL-адрес подключения к защищенному хранилищу секретов
ttl_deadline	dword	Оставшееся время (в секундах) актуальности токена, по достижении которого он будет обновлен

Файл `/etc/default/termidesk-agent`

Одним из параметров службы `termidesk-agent` является аргумент `EnvironmentFile`, задающий путь к дополнительным аргументам запуска, перечисленным в файле `/etc/default/termidesk-agent`.

Файл `/etc/default/termidesk-agent`:

- является необязательным и может отсутствовать в ОС;
- если он существует, то происходит его построчное чтение в формате `<ключ>=<значение>` и в запускаемый процесс Агента ВРМ добавляются переменные окружения (см. подраздел **Переменные окружения и аргументы командной строки**).

Настройка для ОС Astra Linux Special Edition

Настройка Агента ВРМ для ОС Astra Linux Special Edition 1.7

Для настройки Агента ВРМ нужно:

- перейти в графическом интерфейсе ОС в «Звезда - Панель управления - Система» и выбрать ярлык «VDI Agent Configuration» (см. рисунок Расположение ярлыка Агента ВРМ в ОС);

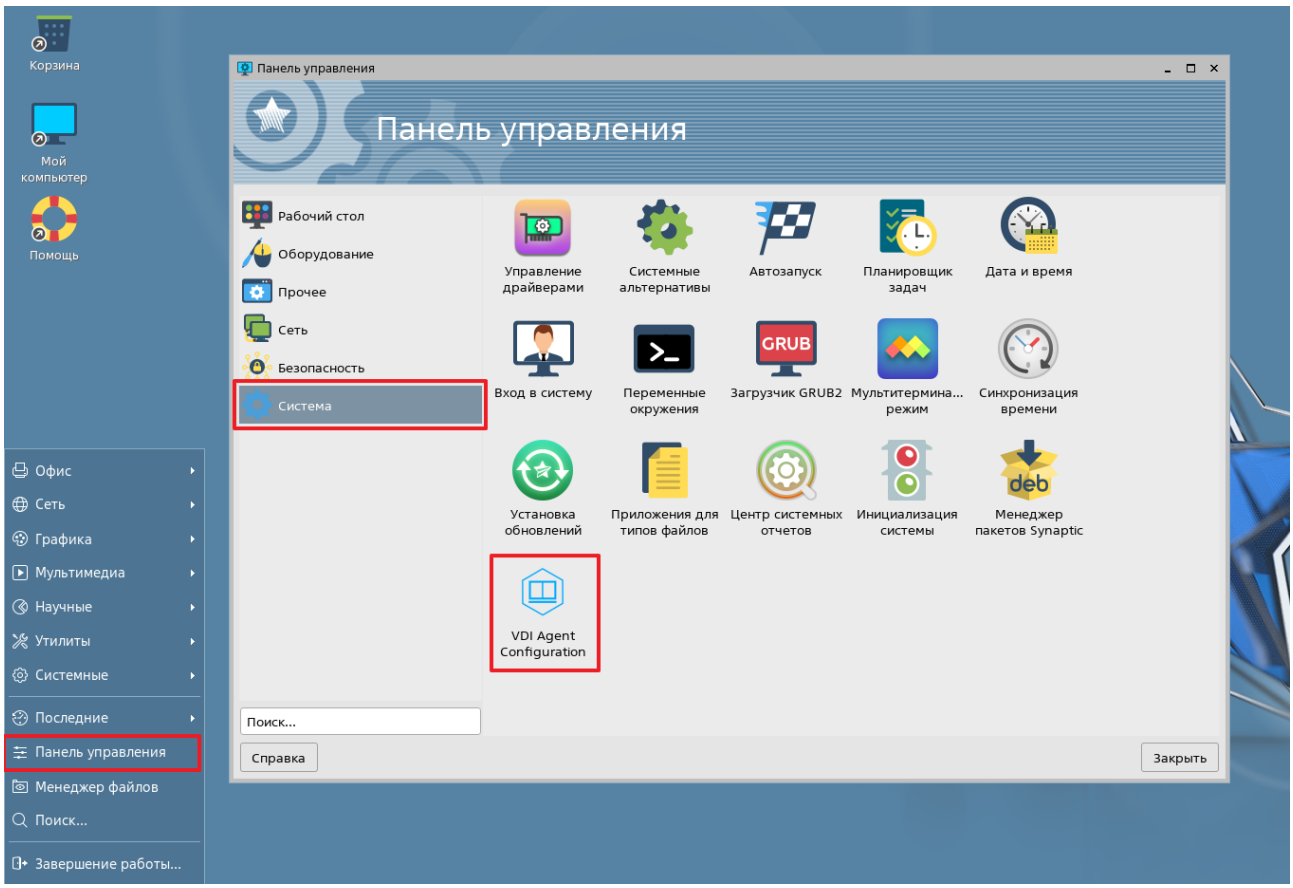


Рисунок 118. Расположение ярлыка Агента ВРМ в ОС

- ввести пароль суперпользователя ОС;
- указать основные параметры конфигурирования (см. таблицу Основные параметры конфигурирования Агента ВРМ в ОС Astra Linux Special Edition 1.7);
- при использовании защищенного хранилища секретов нужно задать параметры подключения к нему в конфигурационном файле `/etc/termidesk/agent.cfg` (см. подраздел **Конфигурационный файл Агента ВРМ**).

Таблица 189. Основные параметры конфигурирования Агента ВРМ в ОС Astra Linux Special Edition 1.7

Параметр	Описание
«Адрес сервера»	IP-адрес или FQDN компонента «Универсальный диспетчер» («Портал администратора»). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/host`

Параметр	Описание
«Мастер-ключ»	Используется для взаимодействия с компонентом «Универсальный диспетчер». Значение мастер-ключа можно получить в «Портале администратора», перейдя в «Системные параметры - Системные настройки - Безопасность» и скопировав значение параметра «Мастер-ключ». Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/masterKey`
«Уровень отладки»	Степень детализации служебных сообщений. Возможные значения: • «DEBUG»; • «INFO» (по умолчанию); • «WARN»; • «ERROR»; • «FATAL»
«Порт агента»	Порт, на котором Агент BPM будет принимать подключения от компонента «Универсальный диспетчер». Если номер порта не задан, то при проверке корректности параметров будет восстановлено значение по умолчанию («43900»)
«Сетевой интерфейс»	Сетевой интерфейс, используемый для подключения к компоненту «Универсальный диспетчер». IP-адреса выбранного интерфейса должны находиться в маршрутизируемой сети и быть доступны компоненту «Универсальный диспетчер» после публикации фонда BPM. Начиная с Termidesk VDI версии 6.1 Агент BPM подключается к «Универсальному диспетчеру» («Порталу администратора») только по защищенному соединению (протоколу HTTPS). Если значение не задано, либо указанный интерфейс отсутствует, то будет восстановлено значение по умолчанию («Автоматически»)
«Разрешить переопределение значений через переменные окружения»	Управление переопределением значений параметров Агента BPM через переменные окружения (см. подраздел **Переменные окружения и другие параметры конфигурирования**)

Параметр	Описание
«mTLS»	Выбор режима mTLS для защищенного подключения и взаимной аутентификации. Пример настройки mTLS между компонентами «Универсальный диспетчер» и «Агент виртуального рабочего места» приведен в подразделе **Пример конфигурирования mTLS между компонентами «Универсальный диспетчер» и «Агент виртуального рабочего места»** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Настройка программного комплекса». Возможные значения: • «Выключено» (по умолчанию) - сертификаты игнорируются, их проверка не производится. Агент ВРМ использует самоподписанный сертификат, если является «Сервером». В этом режиме mTLS не используется, заполнять пункты «Сервер» и «Клиент» не требуется; • «Разрешительный режим» - нестрогий режим проверки сертификата. Проверка выполняется, но если сертификат не предоставлен или он недействительный, то он не проверяется. Соединение при этом продолжает работать; • «Строгий режим» - строгий режим проверки сертификата. Предоставление действительных сертификатов обязательно. Соединение сбрасывается, если сертификат не прошел проверку
«Источник сертификатов»	Тип хранилища сертификатов. Возможные значения: • «Файловая система» - сертификаты располагаются локально, в файловой системе; • «Openbao, SecMan (Platform V)» - сертификаты располагаются во внешнем защищенном хранилище сертификатов
Вкладка «Сервер»	
«Цепочка ЦС»	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ

Параметр	Описание
«Сертификат»	Путь к серверному сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/certificate` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ
«Закрытый ключ»	Путь к серверному закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ
«Пароль»	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/passphrase`
«Использовать как клиентский сертификат»	Серверный сертификат будет использоваться как клиентский. При активации параметра заполнять вкладку «Клиент» не требуется
Вкладка «Клиент»	
«Цепочка ЦС»	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ

Параметр	Описание
«Сертификат»	Путь к клиентскому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/certificate` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ
«Закрытый ключ»	Путь к клиентскому закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ
«Пароль»	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/passphrase`

Существующие ограничения:

- не поддерживается работа с отозванными сертификатами и цепочкой сертификатов промежуточных УЦ;
- срок действия сертификатов проверяется только при установлении соединения.

Сертификаты, использующиеся для mTLS должны содержать расширения «authClient» и (или) «authServer». В противном случае их нельзя будет добавить.

При использовании mTLS конфигурационный файл веб-сервера Apache компонента «Универсальный диспетчер» должен быть скорректирован (см. подраздел **Конфигурирование веб-сервера Apache для mTLS** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Настройка программного комплекса»).

После задания значений следует:

- проверить корректность введенных значений, нажав экранную кнопку **[Проверить]**. Результатом проверки должно являться сообщение «Проверка успешно завершена»;
- сохранить значения, нажав на экранную кнопку **[Сохранить]**, а затем закрыть окно при помощи экранной кнопки **[Закрыть]**.

Настройка Агента ВРМ для ОС Astra Linux Special Edition 1.8

Для настройки Агента ВРМ нужно:

- перейти в графическом интерфейсе ОС в «Звезда - Программы - Инструменты» и выбрать ярлык «VDI Agent Configuration» (см. рисунок Расположение ярлыка Агента ВРМ в ОС);

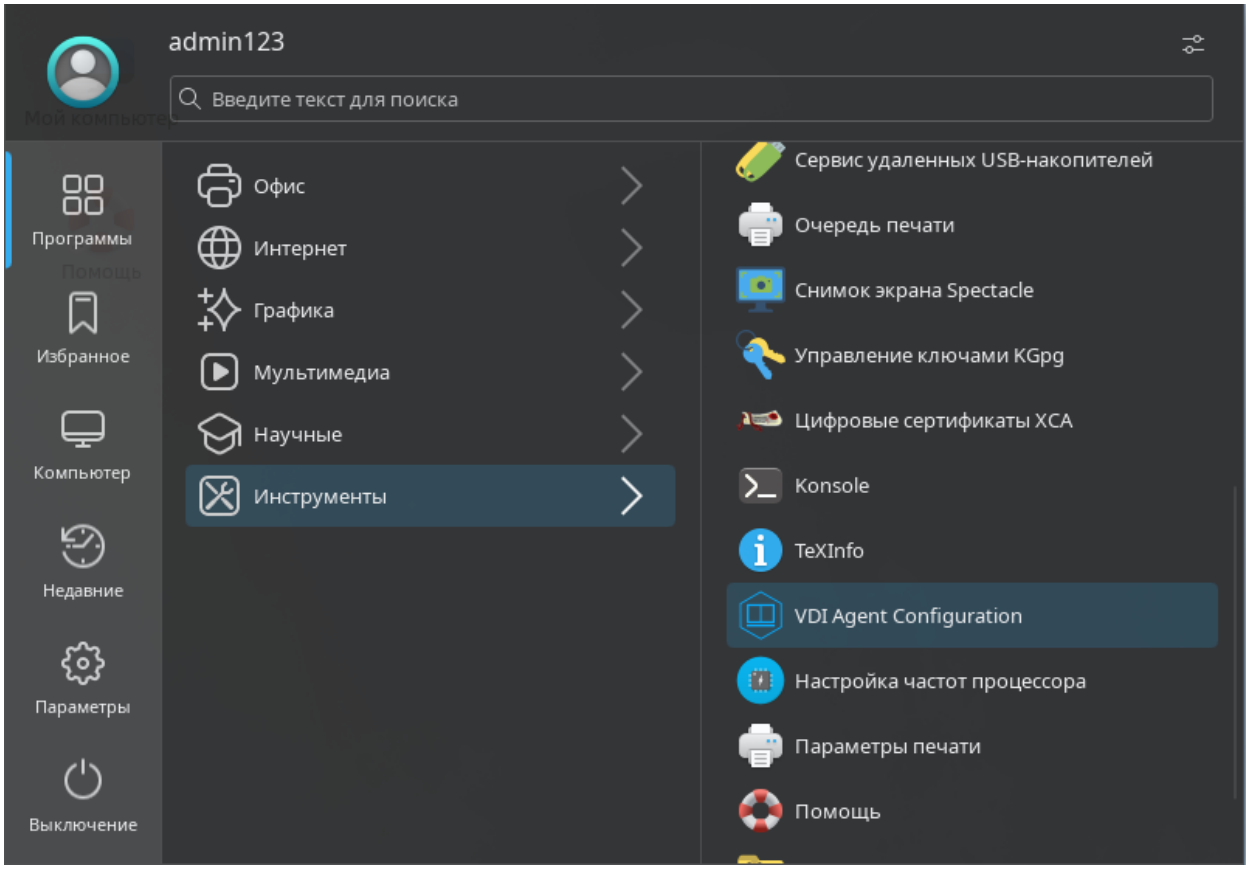


Рисунок 119. Расположение ярлыка Агента ВРМ в ОС

- ввести пароль суперпользователя ОС;
- указать основные параметры конфигурирования (см. таблицу Основные параметры конфигурирования Агента ВРМ в ОС Astra Linux Special Edition 1.8);
- при использовании защищенного хранилища секретов нужно задать параметры подключения к нему в конфигурационном файле `/etc/termidesk/agent.cfg` (см. подраздел **Конфигурационный файл Агента ВРМ**).

Таблица 190. Основные параметры конфигурирования Агента ВРМ в ОС Astra Linux Special Edition 1.8

Параметр	Описание
«Адрес сервера»	IP-адрес или FQDN компонента «Универсальный диспетчер» («Портал администратора»). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/host`

Параметр	Описание
«Мастер-ключ»	Используется для взаимодействия с компонентом «Универсальный диспетчер». Значение мастер-ключа можно получить в «Портале администратора», перейдя в «Системные параметры - Системные настройки - Безопасность» и скопировав значение параметра «Мастер-ключ». Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/masterKey`
«Уровень отладки»	Степень детализации служебных сообщений. Возможные значения: • «DEBUG»; • «INFO» (по умолчанию); • «WARN»; • «ERROR»; • «FATAL»
«Порт агента»	Порт, на котором Агент BPM будет принимать подключения от компонента «Универсальный диспетчер». Если номер порта не задан, то при проверке корректности параметров будет восстановлено значение по умолчанию («43900»)
«Сетевой интерфейс»	Сетевой интерфейс, используемый для подключения к компоненту «Универсальный диспетчер». IP-адреса выбранного интерфейса должны находиться в маршрутизируемой сети и быть доступны компоненту «Универсальный диспетчер» после публикации фонда BPM. Начиная с Termidesk VDI версии 6.1 Агент BPM подключается к «Универсальному диспетчеру» («Порталу администратора») только по защищенному соединению (протоколу HTTPS). Если значение не задано, либо указанный интерфейс отсутствует, то будет восстановлено значение по умолчанию («Автоматически»)
«Разрешить переопределение значений через переменные окружения»	Управление переопределением значений параметров Агента BPM через переменные окружения (см. подраздел **Переменные окружения и другие параметры конфигурирования**)

Параметр	Описание
«mTLS»	Выбор режима mTLS для защищенного подключения и взаимной аутентификации. Пример настройки mTLS между компонентами «Универсальный диспетчер» и «Агент виртуального рабочего места» приведен в подразделе **Пример конфигурирования mTLS между компонентами «Универсальный диспетчер» и «Агент виртуального рабочего места»** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Настройка программного комплекса». Возможные значения: • «Выключено» (по умолчанию) - сертификаты игнорируются, их проверка не производится. Агент ВРМ использует самоподписанный сертификат, если является «Сервером». В этом режиме mTLS не используется, заполнять пункты «Сервер» и «Клиент» не требуется; • «Разрешительный режим» - нестрогий режим проверки сертификата. Проверка выполняется, но если сертификат не предоставлен или он недействительный, то он не проверяется. Соединение при этом продолжает работать; • «Строгий режим» - строгий режим проверки сертификата. Предоставление действительных сертификатов обязательно. Соединение сбрасывается, если сертификат не прошел проверку
«Источник сертификатов»	Тип хранилища сертификатов. Возможные значения: • «Файловая система» - сертификаты располагаются локально, в файловой системе; • «Openbao, SecMan (Platform V)» - сертификаты располагаются во внешнем защищенном хранилище сертификатов
Вкладка «Сервер»	
«Цепочка ЦС»	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ

Параметр	Описание
«Сертификат»	Путь к серверному сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/certificate` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ
«Закрытый ключ»	Путь к серверному закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ
«Пароль»	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/passphrase`
«Использовать как клиентский сертификат»	Серверный сертификат будет использоваться как клиентский. При активации параметра заполнять вкладку «Клиент» не требуется
Вкладка «Клиент»	
«Цепочка ЦС»	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ

Параметр	Описание
«Сертификат»	Путь к клиентскому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/certificate` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ
«Закрытый ключ»	Путь к клиентскому закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ
«Пароль»	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/passphrase`

Существующие ограничения:

- не поддерживается работа с отозванными сертификатами и цепочкой сертификатов промежуточных УЦ;
- срок действия сертификатов проверяется только при установлении соединения.

Сертификаты, использующиеся для mTLS должны содержать расширения «authClient» и (или) «authServer». В противном случае их нельзя будет добавить.

При использовании mTLS конфигурационный файл веб-сервера Apache компонента «Универсальный диспетчер» должен быть скорректирован (см. подраздел **Конфигурирование веб-сервера Apache для mTLS** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Настройка программного комплекса»).

После задания значений следует:

- проверить корректность введенных значений, нажав экранную кнопку **[Проверить]**. Результатом проверки должно являться сообщение «Проверка успешно завершена»;
- сохранить значения, нажав на экранную кнопку **[Сохранить]**, а затем закрыть окно при помощи экранной кнопки **[Закрыть]**.

Настройка для ОС Microsoft Windows

Настройка Агента ВРМ для ОС Microsoft Windows

После установки Агента ВРМ следует выполнить его настройку для взаимодействия с компонентом «Универсальный диспетчер».

Для настройки Агента ВРМ нужно:

- перейти «Пуск - Все программы» выбрать каталог «Termidesk» и нажать левой клавишей мыши на ярлык Агента «Termidesk VDI Agent»;
- указать основные параметры конфигурирования (см. таблицу Основные параметры конфигурирования Агента ВРМ в ОС Microsoft Windows);
- при использовании защищенного хранилища секретов задать параметры подключения к нему в каталоге реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Termidesk\Agent\Store\vault_host` (см. подраздел **Конфигурационный файл Агента ВРМ**).

Начиная с Termidesk VDI версии 5.0 запускать ярлык Агента «Termidesk Agent» от имени администратора вручную не требуется, если в ОС включен контроль учетных записей пользователя (User Account Control, UAC). В случае, если контроль учетных записей выключен, то для пользователя, не являющегося администратором, появится сообщение «Эта программа должна запускаться от привилегированного пользователя», а не окно ввода данных привилегированного пользователя.

Таблица 191. Основные параметры конфигурирования Агента ВРМ в ОС Microsoft Windows

Параметр	Описание
«Адрес сервера»	IP-адрес или FQDN компонента «Универсальный диспетчер» («Портал администратора»). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/host`
«Мастер-ключ»	Используется для взаимодействия с компонентом «Универсальный диспетчер». Значение мастер-ключа можно получить в «Портале администратора», перейдя в «Системные параметры - Системные настройки - Безопасность» и скопировав значение параметра «Мастер-ключ». Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/masterKey`
«Уровень отладки»	Степень детализации служебных сообщений. Возможные значения: • «DEBUG»; • «INFO» (по умолчанию); • «WARN»; • «ERROR»; • «FATAL»

Параметр	Описание
«Порт агента»	Порт, на котором Агент ВРМ будет принимать подключения от компонента «Универсальный диспетчер». Если номер порта не задан, то при проверке корректности параметров будет восстановлено значение по умолчанию («43900»)
«Сетевой интерфейс»	Сетевой интерфейс, используемый для подключения к компоненту «Универсальный диспетчер». IP-адреса выбранного интерфейса должны находиться в маршрутизируемой сети и быть доступны компоненту «Универсальный диспетчер» после публикации фонда ВРМ. Начиная с Termidesk VDI версии 6.1 Агент ВРМ подключается к «Универсальному диспетчеру» («Порталу администратора») только по защищенному соединению (протоколу HTTPS). Если значение не задано, либо указанный интерфейс отсутствует, то будет восстановлено значение по умолчанию («Автоматически»)
«Разрешить переопределение значений через переменные окружения»	Управление переопределением значений параметров Агента ВРМ через переменные окружения (см. подраздел **Переменные окружения и другие параметры конфигурирования**)
«mTLS»	Выбор режима mTLS для защищенного подключения и взаимной аутентификации. Пример настройки mTLS между компонентами «Универсальный диспетчер» и «Агент виртуального рабочего места» приведен в подразделе **Пример конфигурирования mTLS между компонентами «Универсальный диспетчер» и «Агент виртуального рабочего места»** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Настройка программного комплекса». Возможные значения: • «Выключено» (по умолчанию) - сертификаты игнорируются, их проверка не производится. Агент ВРМ использует самоподписанный сертификат, если является «Сервером». В этом режиме mTLS не используется, заполнять пункты «Сервер» и «Клиент» не требуется; • «Разрешительный режим» - нестрогий режим проверки сертификата. Проверка выполняется, но если сертификат не предоставлен или он недействительный, то он не проверяется. Соединение при этом продолжает работать; • «Строгий режим» - строгий режим проверки сертификата. Предоставление действительных сертификатов обязательно. Соединение сбрасывается, если сертификат не прошел проверку

Параметр	Описание
«Источник сертификатов»	Тип хранилища сертификатов. Возможные значения: • «Файловая система» - сертификаты располагаются локально, в файловой системе; • «Openbao, SecMan (Platform V)» - сертификаты располагаются во внешнем защищенном хранилище сертификатов; • «Хранилище сертификатов Windows» - сертификаты располагаются локально, в хранилище сертификатов ОС Microsoft Windows
Вкладка «Сервер»	
«Цепочка ЦС»	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ
«Сертификат»	Путь к серверному сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/certificate` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ
«Закрытый ключ»	Путь к серверному закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ
«Пароль»	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/passphrase`

Параметр	Описание
«Тип сертификата»	Область хранилища сертификатов ОС Microsoft Windows. Параметр доступен при выборе значения «Хранилище сертификатов Windows» в параметре «Источник сертификатов». Возможные значения: • «Машина» - хранилище сертификатов, доступных всем пользователям ОС. Находится в системном реестре в `HKEY_LOCAL_MACHINE`; • «Пользователь» - хранилище сертификатов, доступных текущему пользователю ОС. Находится в системном реестре в `HKEY_CURRENT_USER`
«Сертификат»	Выбор серверного сертификата mTLS. Параметр доступен при выборе значения «Хранилище сертификатов Windows» в параметре «Источник сертификатов». Для выбора сертификата следует нажать экранную кнопку **[Выберите]**, выбрать нужный сертификат в списке и нажать экранную кнопку **[OK]**. Для просмотра свойств выбранного сертификата следует нажать экранную кнопку **[Просмотр]**
«Использовать как клиентский сертификат»	Серверный сертификат будет использоваться как клиентский. При активации параметра заполнять вкладку «Клиент» не требуется
Вкладка «Клиент»	
«Цепочка ЦС»	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ
«Сертификат»	Путь к клиентскому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/certificate` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ

Параметр	Описание
«Закрытый ключ»	Путь к клиентскому закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ
«Пароль»	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/passphrase`
«Тип сертификата»	Область хранилища сертификатов ОС Microsoft Windows. Параметр доступен при выборе значения «Хранилище сертификатов Windows» в параметре «Источник сертификатов». Возможные значения: • «Машина» - хранилище сертификатов, доступных всем пользователям ОС. Находится в системном реестре в `HKEY_LOCAL_MACHINE`; • «Пользователь» - хранилище сертификатов, доступных текущему пользователю ОС. Находится в системном реестре в `HKEY_CURRENT_USER`
«Сертификат»	Выбор клиентского сертификата mTLS. Параметр доступен при выборе значения «Хранилище сертификатов Windows» в параметре «Источник сертификатов». Для выбора сертификата следует нажать экранную кнопку **[Выберите]**, выбрать нужный сертификат в списке и нажать экранную кнопку **[OK]**. Для просмотра свойств выбранного сертификата следует нажать экранную кнопку **[Просмотр]**

Существующие ограничения:

- не поддерживается работа с отозванными сертификатами и цепочкой сертификатов промежуточных УЦ;
- срок действия сертификатов проверяется только при установлении соединения.

Сертификаты, использующиеся для mTLS должны содержать расширения «authClient» и (или) «authServer». В противном случае их нельзя будет добавить.

При использовании mTLS конфигурационный файл веб-сервера Apache компонента «Универсальный диспетчер» должен быть скорректирован

(см. подраздел **Конфигурирование веб-сервера Apache для mTLS** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Настройка программного комплекса»).

После задания значений следует:

- проверить корректность введенных значений, нажав экранную кнопку **[Проверить]**. Результатом проверки должно являться сообщение «Проверка успешно завершена»;
- сохранить значения, нажав на экранную кнопку **[Сохранить]**, а затем закрыть окно при помощи экранной кнопки **[Закрыть]**.

Агент ВРМ автоматически запускается при загрузке ОС Microsoft Windows и создает правило подключения к ВРМ для межсетевого экрана. Для ручной настройки правил подключений межсетевого экрана с помощью Агента ВРМ следует обратиться к подразделу **Настройка для ОС Microsoft Windows**.

Пользователь, подключающийся по протоколу RDP к ВРМ, автоматически будет добавлен в группу «Пользователи удаленного рабочего стола» Агентом ВРМ.

Управление правилами межсетевого экрана ОС Microsoft Windows

Агент ВРМ предоставляет возможность управления правилами межсетевого экрана гостевой ОС Microsoft Windows, используя интерфейс командной строки (CLI).

Управление правилами межсетевого экрана ОС Microsoft Windows выполняется при помощи команды:

```
> TermideskAgentConfig advfirewall
```

Перечень параметров и аргументов CLI, используемых Агентом ВРМ, указан в таблице (см. таблицу Параметры управления правилами межсетевого экрана Агента ВРМ).

Для просмотра созданных или удаленных правил межсетевого экрана можно воспользоваться утилитой «Монитор брандмауэра Защитника Windows».

Таблица 192. Параметры управления правилами межсетевого экрана Агента ВРМ

Параметр командной строки	Аргумент командной строки	Описание
`--help`	`Не задан`	Вывод справки по использованию параметров командной строки. Для вызова справки нужно выполнить: `TermideskAgentConfig advfirewall --help`

Параметр командной строки	Аргумент командной строки	Описание
list	Не задан	Вывод списка правил, заданных для межсетевого экрана. Пример: TermideskAgentConfig advfirewall list По умолчанию отображаются поля «name», «port», «status»
	--fields	Указание полей, отображаемых при формировании списка правил, заданных для межсетевого экрана. Пример: TermideskAgentConfig advfirewall list --fields name,status где: name - название правила; status - статус правила
	--to-csv	Вывод списка правил в формате CSV. Пример: TermideskAgentConfig advfirewall list --to-csv
create	--port --name --remote-address	Создание правила для межсетевого экрана. Пример: TermideskAgentConfig advfirewall create --name RULE --remote-address 198.51.100.15 где: name - название правила; remote-address - IP-адрес, для которого применяется разрешение
delete	--port --name	Удаление правила для межсетевого экрана. При наличии нескольких правил с одинаковым названием, будет удалено только первое правило в списке. Пример: TermideskAgentConfig advfirewall delete --name RULE --port 4005 где: name - название правила; port - порт, для которого применяется разрешение

Параметр командной строки	Аргумент командной строки	Описание
status	--port --name	Просмотр статуса правила для межсетевого экрана. Пример: TermideskAgentConfig advfirewall status --name RULE где: name - название правила
enable	--port --name	Активация правила для межсетевого экрана. Пример: TermideskAgentConfig advfirewall enable --name RULE где: name - название правила
disable	--port --name	Деактивация правила для межсетевого экрана. Пример: TermideskAgentConfig advfirewall disable --name RULE где: name - название правила

Хранение сертификатов в хранилище Microsoft Windows

Для добавления сертификатов в хранилище Microsoft Windows нужно:

- выбрать нужный файл в формате .pfx, нажать правой кнопкой мыши и в контекстном меню выбрать действие «Установить PFX» (см. рисунок Добавление сертификата);

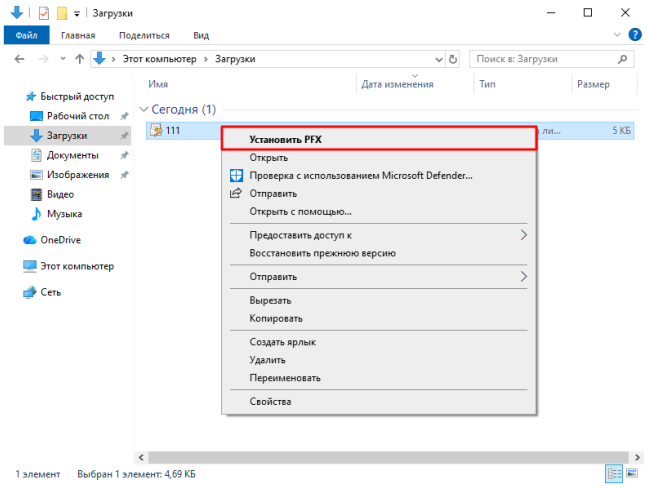


Рисунок 120. Добавление сертификата

- в окне «Мастер импорта сертификатов» указать область хранилища сертификатов и нажать экранную кнопку **[Далее]** (см. рисунок Выбор области хранения сертификатов);

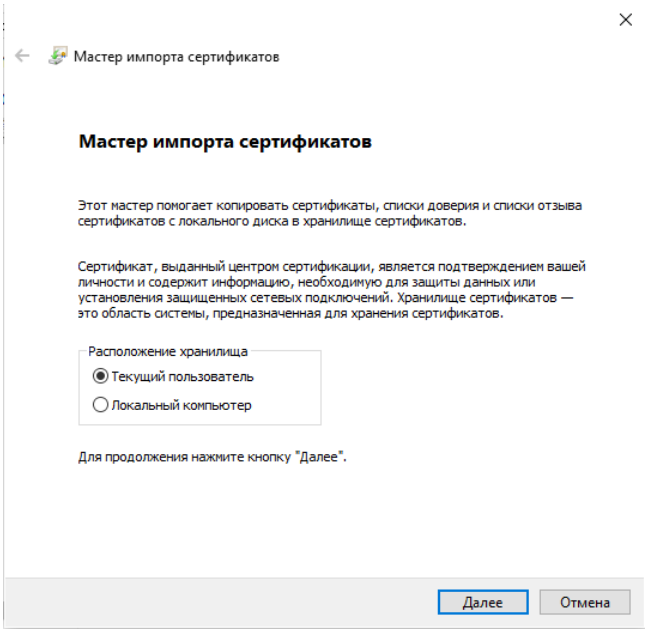


Рисунок 121. Выбор области хранения сертификатов

- в форме «Импортируемый файл» указать путь к файлу в формате `.pfx` (при необходимости) и нажать экранную кнопку **[Далее]** (см. рисунок Указание пути к сертификату);

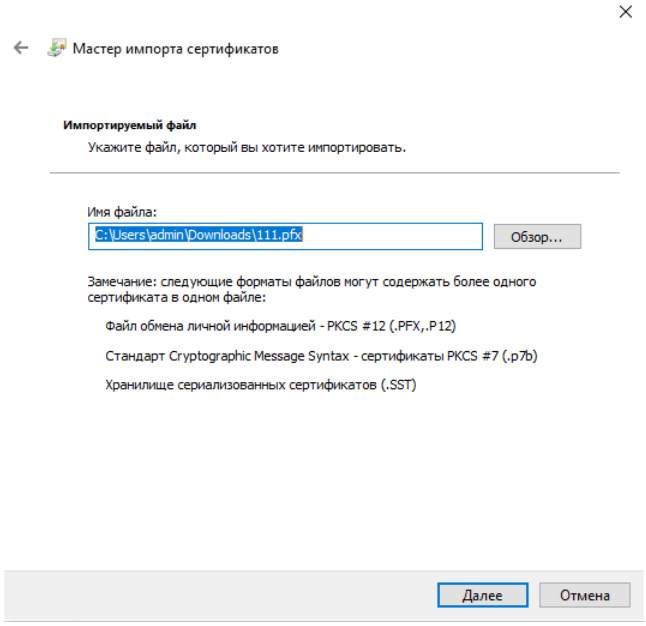


Рисунок 122. Указание пути к сертификату

- в форме «Защита с помощью закрытого ключа» указать пароль, активировать параметр «Пометить этот ключ как экспортируемый, что позволит сохранять резервную копию ключа и перемещать его» и нажать экранную кнопку **[Далее]** (см. рисунок Параметры добавления сертификата);

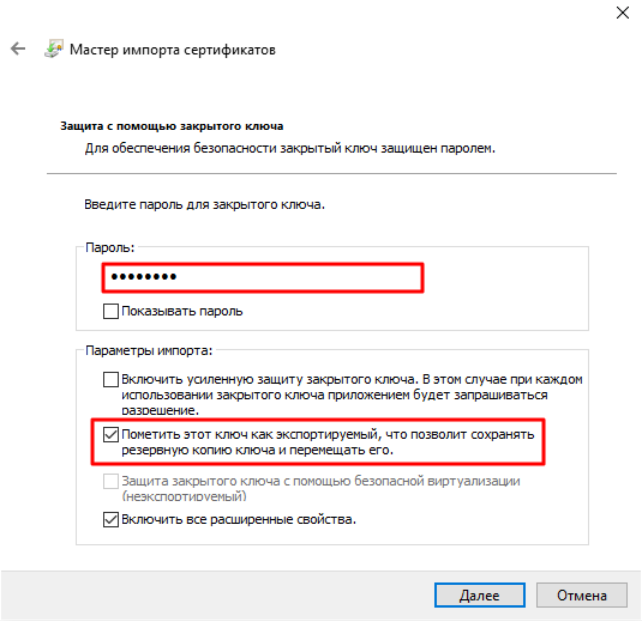


Рисунок 123. Параметры добавления сертификата

- в форме «Хранилище сертификатов» указать хранилище для размещения сертификата, нажать экранную кнопку **[Далее]** (см. рисунок Выбор хранилища сертификатов);

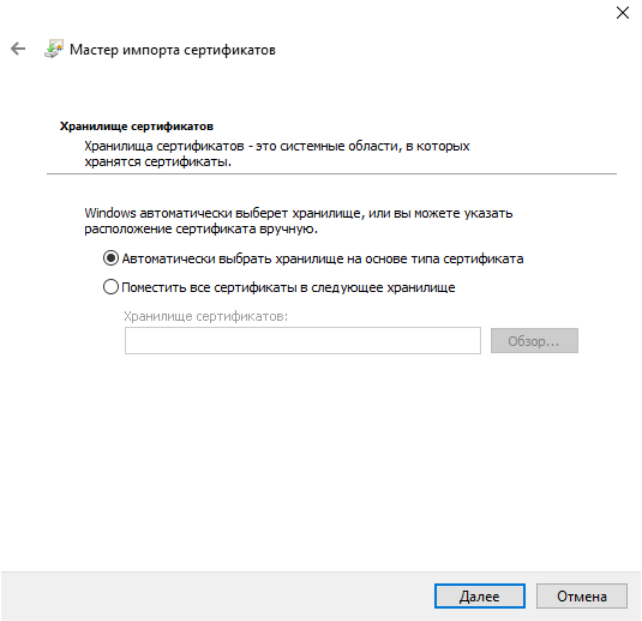


Рисунок 124. Выбор хранилища сертификатов

- ознакомиться с параметрами добавления сертификатов и нажать экранную кнопку **[Готово]**.

Требования к сертификатам:

Параметр «Улучшенный ключ» сертификата должен содержать значения:

- «Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)» - для использования сертификата в качестве серверного;
- «Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)» - для использования сертификата в качестве клиентского.

Допускается наличие обоих значений.

При отсутствии требуемого значения сертификат не отображается в списке доступных сертификатов.

При использовании службы сертификации Active Directory Certificate Services (AD CS) возможность экспорта закрытого ключа должна быть разрешена в свойствах шаблона сертификата и при создании сертификата.

Хранение информации о сессии пользователя

Агент ВРМ поддерживает хранение информации о сессии пользователя, подключившегося к ОС. Этот функционал работает следующим образом:

- пользователь через компонент «Клиент» подключается к серверу Termidesk VDI;
- компонент «Клиент» отправляет серверу (компоненту «Универсальный диспетчер») сведения о пользовательской рабочей станции;
- компонент «Универсальный диспетчер» («Портал пользователя» или «Агрегатор пользователя») получает информацию от компонента «Клиент» и дополняет эти сведения информацией о пользователе и информацией о фонде,и отправляет Агенту ВРМ эти сведения;
- Агент ВРМ сохраняет полученные сведения:
  - для ОС Microsoft Windows: в параметре реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Termidesk\Session\<идентификатор_сессии>`;
  - для ОС Linux: в файле `/var/lib/termidesk/agent/metrics.json`. Файл можно изменить через конфигурационный файл `agent.cfg` в параметре `filepath` (см. подраздел **Конфигурационный файл Агента ВРМ**);
- по API-запросу `/health/metrics` Агент ВРМ вернет полную информацию о сессии пользователя (сведения о пользовательской рабочей станции и метрики сессии).

Сведения о сессии пользователя:

- хранятся для всех сессий, существующих в текущий момент времени;
- создаются при создании сессии и удаляются при ее завершении (logoff);
- доступны для чтения пользователям, но не доступны для изменения.

Перечень параметров, хранимых Агентом ВРМ, приведен в таблице (см. рисунок Перечень параметров, хранимых Агентом ВРМ).

Не все указанные в таблице параметры будут записаны значениями.

Запись актуальных значений производится для параметров:

- `AgentVersion`;
- `ClientAddress`;
- `ClientName`;
- `ClientPlatform`;
- `ClientVersion`;
- `DomainName`;
- `GUSI`;
- `Id`;
- `IdleTime`;
- `LastReconnectReason`;

- LastReconnectTimestamp;
- LogonTimestamp;
- PoolName;
- PublishedName;
- ReconnectionsNumber;
- SessionStatus;
- SessionCreateTimestamp;
- SessionDuration;
- StatusChangedTimestamp;
- Uptime;
- URSI;
- UserName;
- UserSid;
- ViewerVersion.

Если для параметра записано значение, но параметр не отображен в перечне, то в текущей версии Termidesk VDI запись актуального значения для него не производится.

Таблица 193. Перечень параметров, хранимых Агентом ВРМ

Параметр	Описание
AgentVersion	Версия Агента ВРМ
AppliedPolicies	Значения политик, полученные от компонента «Универсальный диспетчер» и примененные Агентом ВРМ
ClientAddress	Локальный IP-адрес пользовательской рабочей станции, через который выполнено подключение к ферме Termidesk VDI. Параметр подчиняется настройке «Использовать анонсируемый IP клиента», заданной в «Портале администратора» Termidesk Если у пользовательской рабочей станции существует более одного IP-адреса, то будет записан IP-адрес Агента ВРМ.
ClientName	Полное доменное имя пользовательской рабочей станции
ClientPlatform	Сведения об ОС пользовательской рабочей станции, на которой установлен компонент «Клиент»
ClientVersion	Версия компонента «Клиент»
ColorDepth	Глубина цвета в сессии пользователя
ConnectionMode	Режим подключения (прямой или через шлюз)
DeliveryProtocol	Тип протокола доставки и его название в ферме Termidesk
DisplaysNumber	Количество мониторов в сессии пользователя
DomainName	Имя домена, в котором аутентифицировался пользователь. В случае, если имя домена отсутствует, то записывается имя домена аутентификации Termidesk
GUSI	Текущий глобальный уникальный сессионный идентификатор
Id	Локальный идентификатор сессии пользователя на РМ

Параметр	Описание
IdleTime	Время бездействия пользователя
LastReconnectReason	Причина последнего отключения
LastReconnectTimestamp	Отметка времени последнего переподключения
LogonTimestamp	Отметка времени входа пользователя в РМ
MachineModifiedDate	Дата и время изменения РМ
PoolName	Имя фонда РМ
PublishedName	Имя публикации
ReconnectionsNumber	Количество переподключений в сессию пользователя
ScreenResolution	Разрешение сессии пользователя (экранное)
SessionType	Тип сессии пользователя (рабочий стол или приложение)
SessionStatus	Состояние сессии (active, idle, disconnected)
SessionCreateTimestamp	Отметка времени создания сессии пользователя
SessionDuration	Длительность сессии пользователя
StatusChangedTimestamp	Отметка времени, когда изменилось состояние сессии пользователя
Uptime	Время с момента загрузки
UserName	Имя пользователя, аутентифицировавшегося в Termidesk
UserSid	Security IDentifier (SID) доменного пользователя (записывается для домена MS AD)
URSI	Текущий уникальный идентификатор запуска ресурса в сессии пользователя
ViewerVersion	Версия ПО Termidesk Viewer

Агент виртуальных смарт-карт

Настройка Агента виртуальных смарт-карт

Дополнительная настройка непосредственно Агента смарт-карт обычно не требуется, однако для разрешения нештатных ситуаций может потребоваться включение более подробного уровня журналирования событий драйвера виртуальной смарт-карты:

- уровень журналирования определяется конфигурационным файлом /etc/reader.conf.d/exconf/vscard. Этого файла может не быть, в таком случае необходимо создать каталог, перейти в него и создать пустой файл:

```
sudo mkdir -p /etc/reader.conf.d/exconf
cd /etc/reader.conf.d/exconf
sudo touch vscard
```

- для включения отладочного журналирования конфигурационный файл должен содержать единственное значение - LOGLEVEL со значением DEBUG:

```
LOGLEVEL DEBUG
```

Параметр LOGLEVEL определяет уровень журналирования и может принимать значения: DEBUG, INFO, ERROR. При отсутствии файла /etc/reader.conf.d/exconf/vscard значение параметра LOGLEVEL по умолчанию INFO. Это значение может быть переопределено переменной окружения TDSK_DEBUG, в таком случае уровень журналирования будет иметь значение DEBUG.

Для перенаправления смарт-карт по протоколу TERA нужно выполнить дополнительную настройку:

- удалить файл /etc/reader.conf.d/type/vscard.spice:

```
sudo rm /etc/reader.conf.d/type/vscard.spice
```

- скопировать существующий файл на замену удаленного:

```
sudo cp /etc/reader.conf.d/type/vscard.tera /etc/reader.conf.d/type/vscard.spice
```

- перезагрузить службу:

```
sudo systemctl restart pcscd
```

Видеоагент

Настройка видеоагента

Для настройки видеоагента нужно:

- разрешить автоматический запуск после перезагрузки ОС:

```
sudo systemctl enable termidesk-video-agent.servoce
```

- осуществить запуск видеоагента:

```
sudo systemctl start termidesk-video-agent.service
```

Для проверки состояния службы видеоагента ввести команду:

```
sudo systemctl status termidesk-video-agent.service
```

Строка Active отображает состояние сервиса, где статус active (running) или active (exited) свидетельствует об успешном запуске видеоагента и его готовности к работе.

Агент узла виртуализации

Использование альтернативного механизма сброса сессий

Для корректной работы функционала сброса сессий при подключении пользователя по протоколу SPICE к ВРМ, опубликованным на платформе ПК СВ Брест, нужно выполнить настройку:

- на узлах платформы виртуализации добавить пользователя `root` в группы `libvirt` и `libvirt-admin`, и перезапустить службу `opennebula`:

```
sudo usermod -a -G libvirt root
sudo usermod -a -G libvirt-admin root
sudo systemctl restart opennebula
```

- активировать использование альтернативного механизма сброса сессий для Агента УВ, как приведено ниже.

Для использования альтернативного механизма сброса сессий:

- создать исполняемый файл, который должен реализовать механизм сброса сессий, например, `/etc/termidesk/script.sh`. Содержимое исполняемого файла приведено ниже для примера;
- создать каталог `/etc/termidesk/`:

```
sudo mkdir /etc/termidesk
```

- создать файл `script.sh`:

```
sudo nano /etc/termidesk/script.sh
```

- задать исполняемому файлу флаг выполнения:

```
sudo chmod +x /etc/termidesk/script.sh
```

- изменить права на каталог:

```
sudo chmod 755 /etc/termidesk
```

- создать конфигурационный файл `/etc/termidesk/termidesk-vmsd.conf`:

```
sudo nano /etc/termidesk/termidesk-vmsd.conf
```

- изменить права на файл:

```
sudo chmod 644 /etc/termidesk/termidesk-vmsd.conf
```

- установить переменную LIBVIRT_PASSWORD_SCRIPT, определив ее в конфигурационном файле /etc/termidesk/termidesk-vmsd.conf. Переменная должна содержать путь к исполняемому файлу:

```
LIBVIRT_PASSWORD_SCRIPT=/etc/termidesk/script.sh
```

Пример содержимого исполняемого файла для сброса сессий:

```
#!/bin/sh
#linux-cli$ /path/to/script --protocol=spice --password=no_password
--connected=disconnect sun-123
# где
#--protocol возможные варианты протокола [spice|vnc]
#--password пароль подключения
#--connected действия [ keep | disconnect | fail ]
VM_PROTOCOL=""
VM_PASSWORD=""
VM_CONNECTED=""
VM_ID=""
if [ -z "${1}" ]; then
    echo "Не заданы параметры"
fi

while [ -n "${1}" ]; do
    case "$(echo "${1}" | cut -d'=' -f1)" in
        --protocol)
            VM_PROTOCOL="$(echo "${1}" | cut -d'=' -f2)"
            ;;
        --connected)
            VM_CONNECTED="$(echo "${1}" | cut -d'=' -f2)"
            ;;
        --password)
            VM_PASSWORD="$(echo "${1}" | cut -d'=' -f2)"
            ;;
        *)
            [ "$(echo "${1}" | grep -i "one-")" ] && VM_ID="${1}"
            ;;
    esac
    shift
done

if [ -n "$(echo "$VM_CONNECTED" | grep -i "disconnect")" ]; then
    IP_PORT=$(ps ax| grep -i "guest=${VM_ID}[^0-9]" | grep -v grep | sed -E -e
"s/.*[[:space:]]+\-${VM_PROTOCOL}[[:space:]]+//" | cut -d' ' -f1 | sed "s/port=//"
| cut -d',' -f1)
    echo "VM SPICE port: $IP_PORT"
    if [ "$IP_PORT" ]; then
        ss --kill -t src :${IP_PORT}
```

```
    fi
fi
```

Сессионный Агент

Конфигурационные файлы сессионного Агента

Конфигурационный файл session_agent.ini

Для настройки сессионного Агента используется конфигурационный файл:

- для ОС Astra Linux Special Edition (Server) - /etc/opt/termidesk-session-agent/session_agent.ini;
- для ОС Microsoft Windows Server - C:\ProgramData\UVEON\Termidesk Session Agent\session_agent.ini.

Администратор может изменить каталог хранения на этапе установки или (в ОС Linux) после установки через переменную окружения CONFIG_DIR, указанную в файле /etc/default/termidesk-session-agent.

Доступные в конфигурационном файле параметры приведены в таблице (см. таблицу Параметры конфигурирования сессионного Агента).

Таблица 194. Параметры конфигурирования сессионного Агента

Параметр	Значение по умолчанию	Описание
		Сетевые настройки
LISTEN_IP	0.0.0.0	IP-адрес или FQDN сессионного Агента
LISTEN_PORT	31000	Порт сессионного Агента
URL_BALANCER	Не задано	Параметр необходимо задать для работы аутентификации по билету Kerberos на терминальных серверах MS RDS. URL-адрес «Универсального диспетчера» с любой из ролей: «Портал администратора», «Портал пользователя», «Портал универсальный». Для распределенной установки Termidesk VDI указывается узел балансировщика, который будет перенаправлять подключение на нужный узел «Универсального диспетчера». Если значение в параметре не задано, то для отправки сообщений будет использоваться IP-адрес «Универсального диспетчера» из БД сессионного Агента, который записывается при автоматической регистрации со стороны «Универсального диспетчера». Для распределенной установки Termidesk VDI следует указывать значение этого параметра в конфигурационном файле. Необходимо учесть, что узел «Универсального диспетчера» должен уметь разрешать FQDN узла сессионного Агента в IP-адрес. Для этого необходимо, чтобы на DNS-сервере были добавлены записи типа «A» и «PTR». Примеры: URL_BALANCER = https://192.168.0.2 URL_BALANCER = https://disp.termidesk.ru URL_BALANCER = http://192.168.0.2
		Настройки мониторинга

Параметр	Значение по умолчанию	Описание
METRICS_ACCESS_KEY	None	Ключ доступа для аутентификации запросов к API /health/metrics. Значение по умолчанию: None (ключ не задан, проверка запроса на аутентификацию не осуществляется). При задании значения ключа следует руководствоваться правилом, что: • размер ключа должен составлять от 0 до 64 символа; • должны использоваться символы в шестнадцатеричной системе (0-9, a-f)
Настройки взаимодействия с сервером терминалов MS RDS		
INSTALL_RDS_ROLE_ON_NEXT_BOOT	False	Управление ролью сервера терминалов в ОС Microsoft Windows Server. Применяется только при использовании поставщика ресурсов Метапоставщик в Termidesk VDI. Возможные значения: • True - активировать роль сервера терминалов. После активации будет добавлено правило для сессионного Агента в межсетевом экране (брандмауэре) Windows; • False - выключить роль сервера терминалов. После запуска сессионного Агента значение параметра вновь изменится на False, поскольку операция активации выполняется единожды
MASTER_KEY	None	Параметр необходимо задать для работы аутентификации по билету Kerberos на терминальных серверах MS RDS. Значение мастер-ключа «Портала администратора», с которым обменивается данными сессионный Агент
Настройки взаимодействия со STAL		
OTP_TOKEN_TTL	30	Время жизни (в секундах) одноразового токена, использующегося для аутентификации компонента «Клиент» в рамках инициализации сессии пользователя на компоненте «Сервер терминалов Astra Linux»
STAL_TOKEN_TTL	30	Время жизни (в секундах) одноразового токена, использующегося для аутентификации пользователя при подключении к компоненту «Сервер терминалов Astra Linux» с использованием смарт-карт

Параметр	Значение по умолчанию	Описание
STAL_CONNECT_RDP_TTL	10	Если версия компонента «Сервер терминалов Astra Linux»: • соответствует версии 3.0, то требуется изменить значение на 600; • ниже 3.0, то значение по умолчанию (10) можно не менять. Время ожидания (в секундах) подключения к компоненту «Сервер терминалов Astra Linux»

Параметр	Значение по умолчанию	Описание

USE_USER_PRINCIPAL_NAME	Auto	Если версия компонента «Сервер терминалов Astra Linux»:
		• соответствует или выше 4.0, то параметр не используется;
		• соответствует 3.0, то поддерживается значение Auto;
		• ниже 3.0, то поддерживаются только значения True или False.
		
		Параметр управляет подстановкой суффикса домена.
		
		Возможные значения:
		
		• True - к имени пользователя будет добавлен суффикс домена. Для этого рекомендуется настроить SSSD-сервисы ОС, задав параметру use_fully_qualified_names значение True. Параметр может быть сконфигурирован:
		  - в файле /etc/sssd/sssd.conf. Если параметр переопределен в файлах каталога /etc/sssd/conf.d/, то их обработка будет приоритетной;
		  - в файлах, размещенных в /etc/sssd/conf.d/. Любой файл из каталога, заканчивающийся на .conf и не начинающийся с точки, будет использоваться вместе с /etc/sssd/sssd.conf. Файлы могут иметь приоритет обработки;
		• False - имя пользователя не будет модифицироваться;
		• Auto - автоматическое применение действий:
		  - для локальных пользователей суффикс домена не будет подставлен;
		  - для доменных пользователей выполнится запрос к «Серверу терминалов Astra Linux» для проверки свойства use_fully_qualified_names:
		  - если возвращен ответ True (ожидается имя в формате userPrincipalName), то:
		  - при наличии доменной части имя пользователя остается без изменений;
		  - при отсутствии доменной части имя пользователя модифицируется с добавлением суффикса домена;
		  - если возвращен ответ False (ожидается имя в формате sAMAccountName) то:
		  - при наличии доменной части вызывается исключение;
		  - при отсутствии доменной части имя пользователя остается без изменений.
		
		Значение по умолчанию: Auto

Параметр	Значение по умолчанию	Описание
DBUS_TIMEOUT	25	Время ожидания (в секундах) выполнения запросов создания сессии в шине DBUS
REMOVE_INACTIVE_SESSION_FREQUENCY	30	Периодичность (в секундах) запуска задачи удаления неактивных сессий
APPS_SHARING_SESSIONS	None	Параметр используется для запуска приложений, использующих профили пользователя. Список многопрофильных приложений, которые должны быть открыты в том же окне ПО Termidesk Viewer. По умолчанию список не задан и приложения открываются в новых окнах ПО Termidesk Viewer. Если приложение из списка повторно запускается пользователем, то новая сессия будет запущена в рамках уже существующей, а уникальный идентификатор запуска ресурса новой сессии перестанет существовать, будет использоваться ранее назначенный. Для перечисления нескольких приложений следует использовать разделитель - запятую. Пример: APPS_SHARING_SESSIONS = chromium,yandexbrowser
Настройки взаимодействия с сервером терминалов Метапоставщика		

Параметр	Значение по умолчанию	Описание
MAX_SESSIONS	181 или 250	Параметр действует на терминальный сервер, если он используется в поставщике ресурсов Метапоставщик. Если в поставщике ресурсов параметр «Применить "Сессий всего"» не используется, то предел количества подключений будет зависеть от значения параметра MAX_SESSIONS. При этом количество сессий на узле может быть больше указанного в MAX_SESSIONS значения, если в поставщике ресурсов используются параметры «Соиспользование сессий» и «Предпочитать соиспользование сессий вместо балансировки». Максимально допустимое количество сессий на терминальном сервере. Значение параметра отправляется совместно с метриками узла терминального сервера. Возможные значения: • 181 - для терминального сервера компонента «Сервер терминалов Astra Linux»; • 250 - для терминального сервера MS RDS. Значение по умолчанию определяется автоматически, в зависимости от терминального сервера, на который установлен сессионный Агент
Настройки подключения по протоколу HTTPS		
USE_HTTPS	False	Управление запуском сессионного Агента в режиме использования протокола HTTPS. Возможные значения: • True - используется протокол HTTPS, запросы по протоколу HTTP не обрабатываются; • False - используется протокол HTTP. Необходимо настроить «Портал администратора» на использование протокола HTTP, скорректировав файл /etc/apache2/sites-available/termidesk.conf (см. подраздел **Перенаправление на HTTPS** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»)

Параметр	Значение по умолчанию	Описание
VERIFY_CERT	False	Управление проверкой SSL-сертификата в режиме использования протокола HTTPS. При использовании режима mTLS параметр VERIFY_CERT игнорируется. Возможные значения: • True - проверка SSL-сертификата включена. Режим работы: HTTPS с проверкой сертификата; • False - проверка SSL-сертификата отключена. Режим работы: HTTPS без проверки сертификата, или HTTP (если параметр USE_HTTPS=False). Если используется значение True, то на узел должен быть загружен корневой сертификат: • если путь указан в параметре CA_CERTIFICATE_PATH, то будет использоваться сертификат, указанный в значении этого параметра; • если путь не указан в параметре CA_CERTIFICATE_PATH, то будет использоваться сертификат из системного хранилища сертификатов
CERTIFICATE_PATH	/etc/opt/termidesk-session-agent/certs/cert.pem или C:\ProgramData\UVEON\Termidesk Session Agent\certs\cert.pem	Путь до SSL-сертификата. Для ОС Astra Linux Special Edition: /etc/opt/termidesk-session-agent/certs/cert.pem. Для ОС Microsoft Windows Server: C:\ProgramData\UVEON\Termidesk Session Agent\certs\cert.pem
PRIVATE_KEY_PATH	/etc/opt/termidesk-session-agent/certs/key.pem или C:\ProgramData\UVEON\Termidesk Session Agent\certs/key.pem	Путь до закрытого ключа. Для ОС Astra Linux Special Edition: /etc/opt/termidesk-session-agent/certs/key.pem. Для ОС Microsoft Windows Server: C:\ProgramData\UVEON\Termidesk Session Agent\certs/key.pem
Настройки взаимной аутентификации mTLS		

Параметр	Значение по умолчанию	Описание
MTLS_MODE	0	Режим mTLS для защищенного подключения и взаимной аутентификации. Возможные значения: • 0 - сертификаты игнорируются, их проверка не производится. В этом режиме mTLS не используется; • 1 - нестрогий режим проверки сертификата. Проверка выполняется, но если сертификат не предоставлен, или он недействительный, или возникли ошибки при его проверке, то это не приведет к разрыву соединения; • 2 - строгий режим проверки сертификата. Предоставление действительных сертификатов обязательно. Соединение сбрасывается, если сертификат не прошел проверку
CIPHERS	TLSv1.2	Протокол подключения для mTLS. Возможные значения: • TLSv1.2; • TLSv1.3
CA_CERTIFICATE_PATH	Не задано	Путь к корневому сертификату mTLS
CLIENT_CERTIFICATE_PATH	Не задано	Путь к клиентскому сертификату mTLS
CLIENT_PRIVATE_KEY_PATH	Не задано	Путь к клиентскому закрытому ключу mTLS. Ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению: openssl rsa -in <путь_к_файлу_ключа.key> -out <путь_сохранения_преобразованного_ключа.key>
Настройки журналирования		
LEVEL	INFO	Уровень журналирования. Допустимые значения: NOTSET, DEBUG, INFO, WARNING, ERROR, CRITICAL
ROTATION_LIMIT	5	Максимальное количество файлов журналов. После достижения предела, происходит сжатие журналов в архив
MAX_FILE_SIZE	2097152	Максимальный размер файла журнала (в байтах)

Параметр	Значение по умолчанию	Описание

LOG_DIR	/var/log/termidesk	Задает каталог хранения журналов сессионного Агента.
		
		Пример: администратор хочет изменить место хранения журналов сессионного Агента.
		
		Для этого администратору нужно:
		
		• создать нужный каталог. Каталог должен обладать свойствами:
		  права доступа: rwxr-xr-x (в восьмеричной записи - 755);
		  владелец и группа: termidesk:termidesk;
		• задать параметру новое значение;
		• перезапустить службу termidesk-session-agent:
		
		`sudo systemctl restart termidesk-session-agent`

SEND_LOGS_TO_REPEATER	False	Управление отправкой журналов событий на компонент «Ретранслятор». Возможные значения: • True - события отправляются на компонент «Ретранслятор»; • False - события не отправляются на компонент «Ретранслятор»

Файл `/etc/default/termidesk-session-agent`

Одним из параметров службы `termidesk-session-agent` является аргумент `EnvironmentFile`, задающий путь к дополнительным аргументам запуска, перечисленным в файле `/etc/default/termidesk-session-agent`.

Файл `/etc/default/termidesk-session-agent`:

- автоматически создается в ОС при установке сессионного Агента;
- если файл существует, то происходит его построчное чтение в формате `<ключ>=<значение>` и в запускаемый процесс сессионного Агента добавляются переменные окружения (см. подраздел **Переменные окружения и аргументы командной строки**).

Есть ряд переменных окружения, которые требуются для нормального функционирования сессионного Агента. Такими переменные окружения являются:

> Эти переменные окружения запрещено удалять или модифицировать. Переменные, доступные для модификации, перечислены в подразделе **Переменные окружения и аргументы командной строки**.

- `SHELL`;
- `USER_TERMIDESK`;
- `GROUP_TERMIDESK`;
- `HOME_DIR`;
- `VIRTUAL_ENV`.

Первичная настройка

В обычной конфигурации настройка сессионного Агента не требуется.

Сертификаты открытого ключа (`cert.pem`) и закрытый ключ (`key.pem`), используемые сессионным Агентом для формирования токенов и взаимодействия с другими компонентами Termidesk VDI, генерируются автоматически.

Сертификаты и ключ расположены в каталоге:

- для ОС Astra Linux Special Edition (Server) и ОС Альт Рабочая станция - `/etc/opt/termidesk-session-agent/certs/`;
- для ОС Microsoft Windows Server - `C:\ProgramData\UVEON\Termidesk Session Agent\certs\`.

Настройка сессионного Агента на использование протокола HTTPS

По умолчанию после установки сессионный Агент использует протокол HTTP для обработки запросов. Для того чтобы сессионный Агент обрабатывал запросы по протоколу HTTPS нужно:

- выполнить импорт сертификата и ключей на узел с сессионным Агентом;
- указать пути к сертификату и ключу в параметрах конфигурации сессионного Агента `session_agent.ini`;
- присвоить параметру `USE_HTTPS` значение `True` в параметрах конфигурации сессионного Агента `session_agent.ini`;
- выполнить перезапуск службы «TermideskSessionAgentService» через оснастку «Службы» в ОС Microsoft Windows Server или командой в ОС Astra Linux Special Edition (Server):

```
sudo systemctl restart termidesk-session-agent
```

После выполненных действий необходимо включить параметр «Использовать HTTPS» в настройках поставщика «Сервер терминалов» в веб-интерфейсе Termidesk VDI.

Активация роли терминального сервера в ОС Microsoft Windows Server

Этот подраздел настроек используется только при использовании поставщика ресурсов Метапоставщик в Termidesk VDI.

Для тиражирования приложений ОС Microsoft Windows Server необходимо после установки роли «Remote Desktop Session Host» из состава «Remote Desktop Services» выполнить активацию через сессионный Агент. Для этого нужно присвоить параметру `INSTALL_RDS_ROLE_ON_NEXT_BOOT` значение `True` в параметрах конфигурации сессионного Агента `session_agent.ini`.

АГЕНТ. ЖУРНАЛИРОВАНИЕ

Журналы работы Агентов

Журналы работы Агента ВРМ расположены в следующих файлах:

- ОС Linux:
  - журналы непосредственно Агента ВРМ: для непривилегированного пользователя `~/.config/UVEON/logs/termidesk_agent.log`, для службы `/var/log/termidesk/agent.log`;
  - журнал драйвера печати CUPS: `/var/log/termidesk/cups_daemon.log`;
- ОС Microsoft Windows:
  - для непривилегированного пользователя `%APPDATA%\UVEON\logs\termidesk_agent.log`;
  - для службы `%PROGRAMDATA%\UVEON\logs\termidesk_agent.log`.

Каталог хранения журналов Агента ВРМ в ОС Linux может быть переопределен через конфигурационный файл `/etc/termidesk/agent.cfg` или переменные окружения `TDSK_LOG_SRV_DIR` и `TDSK_LOG_USER_DIR`.

Агент ВРМ поддерживает ротацию журналов работы `agent.log` и `termidesk_agent.log`. Настройка ротации выполняется через переменные окружения `TDSK_LOG_ROTATE_MAX_SIZE` и `TDSK_LOG_ROTATE_MAX_SIZE`.

Журнал Агента ВРМ можно также просмотреть в системном журнале ОС Microsoft Windows. Для этого (см. рисунок Расположение событий Агента в системном журнале ОС Microsoft Windows):

- перейти «Пуск - Средства администрирования Windows - Просмотр событий»;
- в открывшемся окне перейти по дереву «Журналы Windows - Приложение»;
- затем в доступных действиях выбрать «Фильтр текущего журнала» и задать в поле «Источники событий» значение «Termidesk Agent»;
- нажать экранную кнопку **[OK]**.

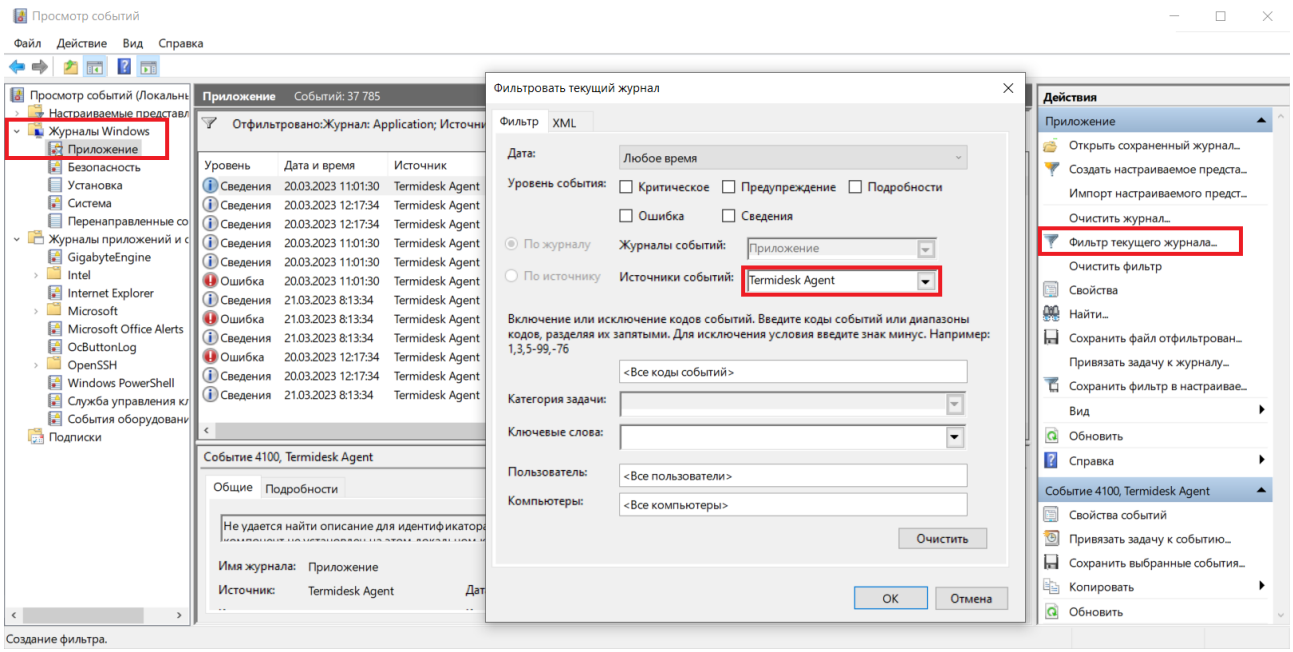


Рисунок 125. Расположение событий Агента в системном журнале ОС Microsoft Windows

Журналы работы сессионного Агента расположены в следующих файлах:

- ОС Astra Linux Special Edition: `/var/log/termidesk/session-agent.log`;
- ОС Microsoft Windows: `%PROGRAMDATA%\UVEON\Termidesk Session Agent\log\session-agent.log`.

Администратор может изменить каталог хранения на этапе установки или (в ОС Linux) после установки через параметр `LOG_DIR`, указанный в конфигурационном файле `/etc/opt/termidesk-session-agent/session_agent.ini`.

События создания файла БД, очистки БД и записи метрик в нее регистрируются в журнале сессионного Агента.

Журналы работы Агента виртуальных смарт-карт расположены в следующих файлах:

- ОС Astra Linux Special Edition: `/var/log/termidesk/pcscd.log`.

События, связанные с видеоагентом, регистрируются в журнале `syslog` (сообщения о статусе запуска службы), а также файлах:

- ОС Astra Linux Special Edition: `/var/log/termidesk/video_agent.log`;
- ОС Microsoft Windows: `%PROGRAMDATA%\UVEON\logs\termidesk_video_agent.log`.

Для просмотра событий, регистрируемых в журнале `syslog`, можно воспользоваться инструментом `journalctl` и отсортировать вывод событий по тексту «video» утилитой `grep`. Пример:

```
sudo journalctl | grep 'video'
```

Журнал работы Агента УВ расположен в файле `/var/log/termidesk/agent.log`.

В журналах регистрируются следующие события:

- информация о запуске Агента;

- информация о настройке Агента;
- сообщения, передаваемые между Агентом и компонентом «Универсальный диспетчер»;
- сообщения, передаваемые от администратора к пользователю ВРМ;
- время простоя ВРМ;
- подключение и отключение пользователя к ВРМ по протоколу RDP;
- подключение переносимых профилей (при включении соответствующего функционала);
- в журналах сессионного Агента и Агента ВРМ регистрируется информация о глобальном уникальном идентификаторе сессии, позволяющим однозначно сопоставить пользователя и производимые им действия;
- в журналах сессионного Агента и Агента ВРМ также регистрируется информация об уникальном идентификаторе запуска ресурса, позволяющим однозначно сопоставить пользователя и доступные ему ресурсы: ВРМ и приложения.

Сбор и передача событий аутентификации, блокировки и разблокировки сессии

Агент ВРМ поддерживает мониторинг и запись событий аутентификации, блокировки и разблокировки пользовательской сессии в гостевой ОС, и их передачу в журнал РМ «Портала администратора».

Функционал сбора событий для разных ОС отличается:

- ОС Microsoft Windows: производится подписка на события. То есть, ОС Microsoft Windows присылает события в сторону Агента ВРМ, который их разбирает и отправляет в журнал РМ;
- ОС Linux: производится мониторинг событий журнала аудита ОС Linux Агентом ВРМ.

Для событий фиксируются:

- `elapsed` - время (в секундах) с момента отправки запроса параметров подключения от ПО Termidesk Viewer и до авторизации в гостевой ОС (API-запрос `/preConnect`);
- `user` - имя пользователя РМ;
- результат действия, например: `UNLOCK SUCCESS` (успешная разблокировка), `Auth SUCCESS` (успешная аутентификация);
- `logon_id` - (для ОС Microsoft Windows) уникальный идентификатор пользовательской сессии в ОС (создается непосредственно ОС). Используется для сопоставления пользовательской сессии и отслеживания ее жизненного цикла;
- `logon_type` - (для ОС Microsoft Windows) тип авторизации пользователя. Возможные коды и их описания приведены в таблице (см. таблицу Возможные коды для параметра `logon_type`). Описание от производителя ОС Microsoft Windows приведено по ссылке: https://learn.microsoft.com/ru-ru/windows-server/identity/securing-privileged-access/reference-tools-logon-types;
- `auth_type` - тип аутентификации пользователя. Возможные значения и их описания приведены в таблице (см. таблицу Возможные значения для параметра `auth_type`);
- `reason` - (для ОС Microsoft Windows) причина ошибки. Возможные коды и их описания приведены в таблице (см. таблицу Возможные коды для параметра `reason`);
- `session_id` - (для ОС Linux) уникальный идентификатор пользовательской сессии в ОС.

Примеры записи событий:

- ОС Microsoft Windows, первая авторизация (RDP):

```
Security events monitoring. Auth SUCCESS | session_id=0x690183 user=cld@test-
win1000000 logon_type=10 auth_type=negotiate total=1
Security events monitoring. Auth SUCCESS | session_id=0x685f78 user=cld@test-
win1000000 logon_type=3 auth_type=plain total=1 elapsed=5.703s
```

- ОС Microsoft Windows, разблокировка сессии (RDP):

```
Security events monitoring. Workstation UNLOCK SUCCESS | logon_id=0x77ef2d
user=cld@test-win1000000 auth_type=negotiate total=1
Security events monitoring. Workstation UNLOCK FAILURE | logon_id=0x3e7
user=cld@test-win1000000 auth_type=negotiate reason=%%2313 total=2
```

- ОС Linux, первая авторизация:

```
Security events monitoring. Auth SUCCESS | user=admin123 auth_type=plain
total_success=1 elapsed=11.169s
```

- ОС Linux, блокировка и разблокировка сессии:

```
Security events monitoring. Workstation UNLOCK | user=admin123
Security events monitoring. Auth FAILURE | user=admin123 auth_type=plain
total_failure=1
Security events monitoring. Workstation LOCK | user=admin123 cause=user
```

Таблица 195. Возможные коды для параметра `logon_type`

Код	Название	Описание
0	System	Системный вход
2	Interactive	Локальный вход
3	Network	Сетевой доступ
4	Batch	Планировщик задач
5	Service	Сервис
7	Unlock	Разблокировка
8	NetworkCleartext	Пароль в явном виде
9	NewCredentials	Сетевой доступ, но с сохранением локальной сессии
10	RemoteInteractive	Удаленный вход по RDP
11	CachedInteractive	Кешированный вход
12	CachedRemoteInteractive	Удаленный вход по RDP с кешированием
13	CachedUnlock	Разблокировка с кешированием

Таблица 196. Возможные значения для параметра `auth_type`

Значение	Описание
`plain`	Простая парольная аутентификация
`kerberos`	Kerberos-аутентификация
`smartcard`	Kerberos-аутентификация по сертификату, размещенному на смарт-карте
`negotiate`	Автоматический выбор наиболее безопасного типа аутентификации: Kerberos или NTLM. Предпочтительно выбирается Kerberos-аутентификация, при необходимости происходит переключение на NTLM. Только для ОС Microsoft Windows
`digest`	Deigest-аутентификация. Только для ОС Microsoft Windows
`schannel`	Аутентификация с использованием протокола SSL/TLS для шифрования сообщений между аутентифицированными сторонами. Только для ОС Microsoft Windows
`cloudap`	Аутентификация Azure AD. Только для ОС Microsoft Windows

Таблица 197. Возможные коды для параметра `reason`

Код	Нормализованное имя	Описание
`%%2304`	account_locked	Учетная запись заблокирована
`%%2305`	account_disabled	Учетная запись отключена
`%%2307`	account_expired	У учетной записи истек срок действия
`%%2309`	invalid_logon_hours	Вход запрещен по времени
`%%2310`	invalid_workstation	Вход запрещен с данного узла
`%%2311`	password_expired	У пароля истек срок действия
`%%2312`	account_restriction	Учетная запись ограничена
`%%2313`	bad_credentials	Неверное имя пользователя или пароль

АГЕНТ. НЕШТАТНЫЕ СИТУАЦИИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

Возможные неисправности при работе с Удаленным помощником и способы их устранения приведены в таблице (см. таблицу Перечень возможных нештатных ситуация и способов их устранения).

Таблица 198. Перечень возможных нештатных ситуация и способов их устранения

Индикация	Описание	Возможное решение

Ошибки авторизации пользователя при подключении к гостевой ОС РМ	Пользователь не может авторизоваться в гостевой ОС при подключении к РМ	Чаще всего ситуация возникает при неправильной настройке модуля pam_tdsk. Для отладки и поиска ошибок в модуле pam_tdsk нужно:
		• создать пользователя с UID < 1000 и GID < 1000 и авторизоваться им в ОС;
		• изменить файл /etc/pam.d/common-session в строке с pam_exec.so:
		`session required pam_exec.so log=/var/log/termidesk/pam_tdsk.log /usr/bin/pam_tdsk.sh`
		• создать дополнительный отладочный файл журнала:
		`touch /var/log/termidesk/pam_tdsk.log`
		• создать исполняемый файл /usr/bin/pam_tdsk.sh, вызывающий pam_tdsk:
		`#!/bin/sh -x`
		`env`
		`SELF_BIN=$(realpath ${0})`
		`SELF_DIR=$(dirname ${SELF_BIN})`
		`args="$@"`
		`pam_tdsk $@`
		`exit_code=$?`
		`exit ${exit_code}`
		• одновременно открыть созданный отладочный файл журнала (/var/log/termidesk/pam_tdsk.log) и стандартный журнал (/var/log/termidesk/agent.log):
		`tail -f /var/log/termidesk/pam_tdsk.log /var/log/termidesk/agent.log`
		• повторить попытку подключения пользователем (допускается как подключение из компонента «Клиент», так и через удаленное подключение по протоколу SSH). Проанализировать сообщения, начинающиеся с pam_tdsk. При необходимости обратиться в техническую поддержку с предоставлением файлов журналов

ТЕРМИНЫ

Компонент «Агент»

Самостоятельный компонент, отвечающий за контролируемую доставку РМ, взаимодействие с «Универсальным диспетчером» и «Менеджером рабочих мест». Собирательное название для следующих компонентов Termidesk VDI:

- «Агент виртуального рабочего места»;

- «Агент узла виртуализации»;
- «Сессионный агент»;
- «Видеоагент»;
- «Агент виртуальных смарт-карт»

Компонент «Агент виртуальных смарт-карт»

Компонент Termidesk VDI. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление подключенных к пользовательской рабочей станции смарт-карт в ВРМ

Компонент «Агент виртуального рабочего места»

Компонент Termidesk VDI. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет взаимодействие с «Универсальным диспетчером», конфигурирует ВРМ, фиксирует действия пользователя, реализует передачу управляющих сообщений

Компонент «Агент узла виртуализации»

Компонент Termidesk VDI. Устанавливается на узел виртуализации, взаимодействует с гипервизором через модуль `libvirt`

Базовое виртуальное рабочее место

Также: золотой образ, базовый образ. Подразумевает собой образ диска ВМ с предустановленным прикладным ПО и установленным «Агентом виртуального рабочего места». Этот образ далее будет использоваться для создания ВРМ для пользователей

Компонент «Видеоагент»

Компонент Termidesk VDI. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление видеокамеры с пользовательской рабочей станции в ВРМ

Виртуальное рабочее место

Развернутая на ВМ ОС с установленным «Агентом виртуального рабочего места» и необходимым прикладным ПО. Подключение к ВРМ происходит через протоколы удаленного доступа

Рабочее место

Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа. Под РМ подразумеваются как ВРМ, так и терминальный доступ или доступ к опубликованным на терминальном сервере приложениям

Гостевая ОС

ОС, функционирующая на ВМ

Компонент «Менеджер рабочих мест»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за взаимодействие с поставщиком ресурсов и управления жизненным циклом РМ, включая создание, настройку, запуск, отключение и удаление. Является обработчиком фоновых задач. Устанавливается из пакета `termidesk-vdi`. Наименование служб после установки: `termidesk-celery-beat.service` и `termidesk-celery-worker.service`

Поставщик ресурсов

ОС, платформа виртуализации или терминальный сервер (MS RDS/STAL), предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов РМ

Протокол доставки

Поддерживаемый в Termidesk VDI протокол удаленного доступа к РМ

Компонент «Сессионный агент»

Компонент Termidesk VDI. Устанавливается на терминальный сервер (MS RDS/STAL), активирует возможность множественного доступа пользователей к удаленным рабочим столам и приложениям

Компонент «Универсальный диспетчер»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им РМ и контроля доставки РМ. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-vdi.service `

Фонд рабочих мест

Совокупность подготовленных РМ для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей

Шаблон рабочего места

Параметры конфигурации рабочего места для использования в фонде РМ

Компонент «Сервер терминалов Astra Linux»

Компонент Termidesk VDI. Также: STAL. Обеспечивает подключение пользовательских рабочих станций к РМ с ОС Astra Linux Special Edition через сеанс удаленного терминала

Ключ

Применяется в контексте файла, не опции в команде. Последовательность псевдослучайных чисел, сгенерированная особым образом

Сертификат

Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу

СОКРАЩЕНИЯ

БД	База данных
ВМ	Виртуальная машина
ВРМ	Виртуальное рабочее место
ЗПС	Замкнутая программная среда
ОС	Операционная система
ПК СВ Брест	Программный комплекс «Средства виртуализации «Брест»
ПО	Программное обеспечение
РМ	Рабочее место
УВ	Узел виртуализации
ЦС	Центр сертификации
ЭЦП	Электронная цифровая подпись
API	Application Programming Interface (интерфейс прикладного программирования)
CLI	Command Line Interface (интерфейс командной строки)

CUPS	Common UNIX Printing System (система печати Unix)
DBus	Desktop Bus (система межпроцессного взаимодействия)
DNS	Domain Name System (система доменных имен)
EULA	End-User License Agreement (лицензионное соглашение с конечным пользователем)
FQDN	Fully Qualified Domain Name (полностью определенное имя домена)
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста)
HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
IP	Internet Protocol (межсетевой протокол)
MS AD	Microsoft Active Directory Domain Service (службы каталогов Microsoft)
mTLS	Multiplexed Transport Layer Security (протокол, основанный на TLS с усиленной безопасностью)
PCSC	Personal Computer Smart Card (стандарт для взаимодействия между персональными компьютерами и смарт-картами)
RDP	Remote Desktop Protocol (протокол удаленного рабочего стола)
RDS	Remote Desktop Services (службы удаленного рабочего стола)
REST	Representational State Transfer (программная архитектура, определяющая условия работы API)
RFC	Request for Comments (рабочее предложение Интернет)
RPC	Remote Procedure Call (удаленный вызов процедур)
SID	Security IDentifier (уникальный идентификатор безопасности)
SPICE	Simple Protocol for Independent Computing Environments (открытый протокол для удаленного доступа к рабочим столам ВМ)
SSL	Secure Sockets Layer (криптографический протокол)
SSSD	System Security Services Daemon (системная служба, управляющая доступом к удаленным каталогам и механизмам аутентификации)
STAL	Terminal Server Astra Linux (компонент «Сервер терминалов Astra Linux»)
TERA	Termidesk Remote Access protocol (протокол удаленного доступа разработкиООО «УВЕОН»)
UAC	User Account Control User (контроль учетных записей пользователей)
URL	Uniform Resource Locator (унифицированный указатель ресурса)
USB	Universal Serial Bus (последовательный интерфейс для подключения периферийных устройств)

СЛЕТ.10001-01 90 06. РУКОВОДСТВО АДМИНИСТРАТОРА. НАСТРОЙКА КОМПОНЕНТА «ОРКЕСТРАТОР»

ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ

Назначение документа

Настоящий документ является шестой частью руководства администратора на программный комплекс «Диспетчер подключений виртуальных рабочих мест Термидеск» (далее - Termidesk VDI, Termidesk VDI). Документ предназначен для администраторов системы и сети.

В этом руководстве приведено назначение, установка и настройка компонента «Оркестратор». Для того чтобы получить информацию о месте компонента в программном комплексе, необходимо обратиться ко второй части руководства администратора - СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

Типографские соглашения

Приняты следующие типографские соглашения:

- `моноширинный шрифт` – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk VDI, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

ОРКЕСТРАТОР. ОБЩИЕ СВЕДЕНИЯ

Назначение компонента «Оркестратор»

Компонент «Оркестратор» (далее - Оркестратор) входит в состав Termidesk VDI.

Оркестратор отвечает за согласованную работу всех компонентов Termidesk VDI при децентрализованном развертывании в целях отказоустойчивости и комплексирования с облачными службами.

Оркестратор построен по архитектуре «Клиент - Сервер», выступая по отношению к облачным службам как в роли клиента, так и в роли сервера.

Оркестратор также является API-шлюзом: управляющие запросы, пришедшие из облачной инфраструктуры, транслируются (транзитом) в запросы к Termidesk VDI, а ответы (включая ошибки) возвращаются в облачную инфраструктуру.

Требования к программному и аппаратному обеспечению

Для установки Оркестратора минимальные аппаратные требования узла должны соответствовать следующим:

- процессор архитектуры Intel x86 с разрядностью 64 бит;
- оперативная память, не менее 4 ГБ ;
- свободное дисковое пространство, не менее 1 ГБ;
- сетевое соединение, не менее 100 Мбит/с.

Среда функционирования Оркестратора должна соответствовать следующим требованиям:

- должна быть установлена операционная система (ОС) Astra Linux Special Edition версии 1.7 и выше;
- должен быть установлен Python 3.7.3 из состава ОС;
- должен быть доступен API компонента Keystone из состава OpenStack для проверки токена приложения;
- должен быть доступен API компонента «Универсальный диспетчер».

ОРКЕСТРАТОР. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ

Получение пакетов установки в ОС Astra Linux Special Edition

Дистрибутив представлен бинарным файлом пакета ПО в `deb`-формате. Установка в ОС Astra Linux Special Edition производится из локального репозитория, распространяемого в формате `iso`-образа.

Получить `iso`-образ можно двумя способами:

- заполнив запрос через сайт Termidesk VDI: https://termidesk.ru/support/#request-support;
- через личный кабинет:https://lk.astra.ru/.

Для подключения локального репозитория Termidesk VDI на узле, где предполагается установка, нужно:

- скопировать в домашний каталог пользователя образ диска `termidesk-<версия>.iso`;
- подключить образ диска к файловой системе в каталог `/mnt`:

```
sudo mount -o loop termidesk-<версия>.iso /mnt
```

где:

`-o loop` - параметры для привязки петлевого устройства (`/dev/loop`) к файлу `termidesk-<версия>.iso`, устройство затем монтируется в указанный каталог `/mnt`;

- скопировать содержимое каталога `repos` подключенного образа диска в каталог `/var` локальной файловой системы:

```
sudo cp -Rp /mnt/repos /var
```

где:

`-Rp` - ключ для рекурсивного копирования подкаталогов и файлов с сохранением исходных свойств;

- отключить подключенный ранее образ диска от узла:

```
sudo umount /mnt
```

- установить пакет `lsb-release`:

```
sudo apt install -y lsb-release
```

- добавить локальный репозиторий Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list` через командный интерпретатор `sh`:
  - выяснить установленную версию ОС:

    ```
    sudo cat /etc/astra_version
    ```

  - определить актуальное имя каталога с пакетами в `/var/repos`;
  - указать в файле конфигурации APT корректное (фактическое) имя каталога:

    ```
    sudo sh -c 'echo "deb file:/var/repos/astra 1.8_x86-64 non-free" >
    /etc/apt/sources.list.d/termidesk_local.list'
    ```

    где:

    `-c` - ключ для чтения команд из вводимой строки (стандартный ввод);

    `echo` - команда вывода текста, совместно с символом «>» используется для перенаправления строки в файл;

    `deb file:/var/repos/astra 1.8_x86-64 non-free` - добавляемый репозиторий с вложенной командой получения версии ОС;

    Приведенный пример команды актуален для установки основных компонентов Termidesk, пакеты которых расположены в каталоге `1.8_x86-64`.

- для корректной установки компонентов TERA потребуется корректно подключить дополнительные репозитории и настроить их приоритет:
  - для версий ОС Astra Linux Special Edition меньше или равных 1.7.6, а также для версий 1.8.X:
    - подключить два репозитория:

      ```
      sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
      non-free" > /etc/apt/sources.list.d/termidesk_local.list'
      sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
      /dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
      ```

    - добавить повышенный приоритет для репозитория с требуемой версией ОС

(значение `$(cat /etc/astra_version)` может подходить не для всех репозиториев, т.к. версия может указываться без точек - в этом случае нужно вручную указать корректную версию):

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000
EOF"
```

- для версий ОС Astra Linux Special Edition 1.7.7 и 1.7.8:
  - подключить три репозитория:

```
sudo sh -c 'echo "deb file:/var/repos/astra 1.7.6 non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
/dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

  - настроить два приоритета:

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=1.7.6
Pin-Priority: 950

Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000

EOF"
```

- выполнить поиск ключа репозитория Termidesk VDI `GPG-KEY-PUBLIC` и добавить его:

```
sudo cat /var/repos/astra/GPG-KEY-PUBLIC | sudo gpg --dearmour -o
/etc/apt/trusted.gpg.d/termidesk.gpg
```

- убедиться, что ключ `release@uveon.ru` был успешно добавлен:

```
apt-key list
```

В случае, если ключ не отображен в выводе команды, необходимо убедиться, что ключ `GPG-KEY-PUBLIC` существует:

```
cat /var/repos/astra/GPG-KEY-PUBLIC
```

Если ключ все же существует, следует проверить правильность выполнения шагов по добавлению репозитория Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list`.

При успешном выполнении всех шагов команда выведет содержимое ключа в формате Base64.

В зависимости от используемой версии ОС команды добавления ключа репозитория Termidesk VDI могут отличаться. Если для ОС Astra Linux Special Edition 1.8 ключ репозитория был добавлен командой, применимой к другой версии ОС, то для исправления нужно:

- узнать идентификатор добавленного ключа репозитория:

```
apt-key list
```

- удалить ключ:

```
apt-key --keyring /etc/apt/trusted.gpg del 4E1632CC
```

где `4E1632CC` - последние 8 символов идентификатора ключа;

- вновь добавить ключ репозитория.

- обновить данные пакетного менеджера:

```
sudo apt update
```

- проверить настройку приоритетов репозиториев:

```
apt-cache policy
```

Команду `sudo apt update` необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.

ОРКЕСТРАТОР. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ

Настройки среды функционирования

Узлу, на который будет установлен Оркестратор, необходимо присвоить имя (`hostname`) командой:

```
sudo hostname orchestrator.test.lan
```

Где `orchestrator.test.lan` - назначаемое узлу имя.

Для того, чтобы после перезагрузки ОС назначенное имя сохранилось, необходимо внести его в файл /etc/hosts.

Пример файла /etc/hosts с указанием полного и короткого имени узла:

```
127.0.0.1       localhost
192.0.2.35   orchestrator.test.lan orchestrator
```

Где 192.0.2.35 - IP-адрес сервера с установленным Оркестратором. Пример IP-адреса приведен в соответствии с RFC 5737, он должен быть заменен на актуальный, используемый согласно схеме адресации, принятой в инфраструктуре организации.

ОС Astra Linux Special Edition

Установка Оркестратора

Для установки Оркестратора:

- подключить локальный репозиторий Termidesk VDI;
- выполнить:

```
sudo apt install termidesk-orchestrator
```

Установку можно также выполнить из deb-пакета, не подключая локальный репозиторий:

```
sudo apt install /home/user/termidesk-orchestrator_XXX-astra17_amd64.deb
```

где /home/user/termidesk-orchestrator_XXX-astra17_amd64.deb - путь к deb пакету.

В процессе установки необходимо принять лицензионное соглашение, доступное в псевдографическом интерфейсе. Для виспользования псевдографического интерфейса должен быть установлен пакет dialog.

Дополнительно установятся следующие пакеты (зависимости):

- apache2;
- ssl-cert;
- memcached;
- openssl;
- libcurl3-nss;
- libcairo2;
- gettext;
- python3-click;
- python3-distutils.

Постановка Оркестратора на контроль целостности

После установки и настройки Оркестратора необходимо поставить его на контроль целостности.

Для контроля целостности используются встроенные в ОС Astra Linux Special Edition программные средства на основе `Another File Integrity Checker`, представленного пакетом `afick`.

Настройка регламентного контроля целостности выполняется в конфигурационном файле `/etc/afick.conf`.

> Настройку следует производить только после окончательного внедрения компонента, поскольку с файлов конфигурации и исполняемых файлов будут сняты эталонные контрольные суммы.

Для постановки на контроль целостности Оркестратора необходимо добавить в конфигурационный файл `/etc/afick.conf` следующие строки:

```
/etc/default/termidesk-orchestrator PARSEC
/etc/opt/termidesk-orchestrator  PARSEC
/opt/termidesk  PARSEC
/usr/lib/systemd/system/termidesk-orchestrator.service  PARSEC
/usr/share/doc/termidesk-orchestrator  PARSEC
/var/opt/termidesk-ochestrator  PARSEC

#Репозиторий Termidesk
/var/repos/ PARSEC
```

Для снятия эталонных значений контрольных сумм используется команда:

```
afick -i
```

Для проверки соответствия контрольных сумм эталонным значениям автоматически создаются задания в системном планировщике заданий `cron`.

Для ручной проверки соответствия контрольных сумм используется команда:

```
afick -k
```

> В случае отсутствия по какой-либо причине исполняемых фалов `*.pyc`, они будут повторно сгенерированы при перезапуске сервера Python. В этом случае нужно повторно проинициализировать средство регламентного контроля целостности `afick`.

Обновление Оркестратора

Обновление Оркестратора выполняется установкой новой версии поверх предыдущей.

Удаление Оркестратора

Удаление Оркестратора из среды ОС Astra Linux Special Edition 1.7 выполняется командой:

```
sudo aptitude purge -y termidesk-orchestrator
```

где:

`-y` - ключ для пропуска подтверждения удаления.

После удаления необходимо очистить оставшиеся зависимости и конфигурации:

```
sudo aptitude purge ~c -y
```

Команда полностью удалит оставшиеся настройки и зависимости уже удаленных пакетов.

Проверка работоспособности Оркестратора

Для проверки работоспособности нужно:

- получить самоподписанный сертификат для обращения по протоколу HTTPS (опционально);
- получить токен приложения (обязательно).

Для получения самоподписанного сертификата, используемого для обращений по протоколу HTTPS, необходимо воспользоваться командой:

```
echo quit | openssl s_client -showcerts -servername orchestrator.test.lan -connect
orchestrator.test.lan:443 > /home/user/orchestrator.test.lan.pem
```

Где:

`orchestrator.test.lan` - имя узла, на котором установлен Оркестратор;

`/home/user/orchestrator.test.lan.pem` - путь к файлу, формата `.pem`, в который будет сохранен сертификат.

Токен приложения используется для авторизации запросов пользователя и запрашивается на сервере OpenStack через функционал API.

Для выполнения API-запросов следует установить утилиту `curl`:

```
sudo apt install curl
```

Для запроса токена нужно выполнить команду:

```
:~$ curl -i \
  -H "Content-Type: application/json" \
  -d '
```

```
{ "auth": {
    "identity": {
      "methods": ["application_credential"],
      "application_credential": {
        "name": "orchestrator",
        "secret": "orchestrator_secret_key",
        "user": {
          "name": "admin",
          "domain": { "name": "Default" }
        }
      }
    }
  }
}' "http://IP-address/identity/v3/auth/tokens" | grep "X-Subject-Token" | sed -e
's/\r//' -e 's/\n//'
```

Где:

`IP-address` - IP-адрес сервера OpenStack.

Вывод команды будет содержать необходимый токен:

```
X-Subject-Token: gAAAAABjdlObymw<...cuted out...>-pJ2JcKNDI_s_FleOLuZOuyt-r
```

Полученный токен необходимо разместить в переменную окружения `APP_TOKEN` и подставлять в заголовок «X-ORC-TOKEN-APP» при каждом запросе к Оркестратору.

Для задания переменной окружения следует воспользоваться командой:

```
export APP_TOKEN="gAAAAABjdlObymw<...cuted out...>-pJ2JcKNDI_s_FleOLuZOuyt-r"
```

Проверка состояния Оркестратора (`healthcheck`) выполняется запросом через утилиту `curl`:

```
curl -s -H "X-ORC-TOKEN-APP: $APP_TOKEN" --cacert orchestrator.test.lan.pem
https://orchestrator.test.lan/api/draft/orc/health/ | python -m json.tool
```

Где:

`orchestrator.test.lan.pem` - ранее сохраненный самоподписанный сертификат;

`orchestrator.test.lan` - имя узла, на котором установлен Оркестратор.

Проверка состояния компонента «Универсальный диспетчер» через Оркестратор выполняется запросом через утилиту `curl`:

```
curl -s -H "X-ORC-TOKEN-APP: $APP_TOKEN" --cacert orchestrator.test.lan.pem
https://orchestrator.test.lan/api/draft/health/ | python -m json.tool
```

При правильном функционировании запрашиваемого компонента ответ должен содержать:

```
{
    "data": "ok"
}
```

ОРКЕСТРАТОР. НАСТРОЙКИ

Настройка сервера apache2 для Оркестратора

Вместе с Оркестратором будет установлен сервер apache2, если он не был установлен ранее.

После установки Оркестратора необходимо скорректировать файл конфигурации веб-сервера `/etc/apache2/apache2.conf`. Для этого следует найти и раскомментировать строку с параметром `AstraMode`, далее присвоить данному параметру значение `off`, точно соблюдая отступы и пробелы в файле.

Пример:

```
# Astra security mode.
#
AstraMode off
```

После перезапустить веб-сервер:

```
sudo systemctl restart apache2
```

Настройка Оркестратора

Для настройки Оркестратора нужно отредактировать разделы `Termidesk VDI params` и `OpenStack params` в файле `/opt/termidesk/share/termidesk-orchestrator/src/config/orc_config.py`.

При первой установке этот конфигурационный файл отсутствует. Его можно скопировать из шаблона `/opt/termidesk/share/termidesk-orchestrator/src/config/orc_config.py.dist`, для этого:

- перейти в каталог с конфигурационными файлами:

```
cd /opt/termidesk/share/termidesk-orchestrator/src/config
```

- переключиться на пользователя `termidesk`:

```
sudo -u termidesk bash
```

- скопировать шаблон в новый файл:

```
cp orc_config.py.dist orc_config.py
```

- выйти из окружения пользователя `termidesk` :

```
exit
```

Проверка заданных настроек Оркестратора

Для проверки корректности заданных настроек применяется исполняемый файл `/opt/termidesk/share/termidesk-orchestrator/src/self_check.py`.

Для его использования нужно выполнить команды:

```
cd /opt/termidesk/share/termidesk-orchestrator/src/
python3 self_check.py
```

Если во время проверки возникает ошибка, подробную информацию о ней можно найти в файле `/tmp/termidesk_self_check_crash.log`. Файл журнала перезаписывается при каждом запуске проверок.

Конфигурационные файлы Оркестратора

Конфигурационный файл `orc_config.py`

Для настройки Оркестратора используется конфигурационный файл `/opt/termidesk/share/termidesk-orchestrator/src/config/orc_config.py`.

Параметры имеют следующую структуру:

```
ВНУТРЕННЯЯ_ПЕРЕМЕННАЯ = os.getenv("ПЕРЕМЕННАЯ_ОКРУЖЕНИЯ",
"ЗНАЧЕНИЕ_ВВОДИМОЕ_ВРУЧНУЮ")
```

Где:

`ПЕРЕМЕННАЯ_ОКРУЖЕНИЯ` - наименование переменной окружения, назначенной через команду `export`. Если переменная в окружении не задана, она добавится с указанным значением;

`ЗНАЧЕНИЕ_ВВОДИМОЕ_ВРУЧНУЮ` - новое значение переменной.

Пример файла `/opt/termidesk/share/termidesk-orchestrator/src/config/orc_config.py`:

```
# Termidesk VDI params
TERMIDESK_HOST = os.getenv("TSRV_HOST", '')
TERMIDESK_PORT = os.getenv("TERMIDESK_PORT", "")
TERMIDESK_USERNAME = os.getenv("TSRV_USERNAME", '')
TERMIDESK_PASSWORD = os.getenv("TSRV_PASSWORD", '')
#Termidesk VDI auth domain ID: authSmallName
 TERMIDESK_AUTH = os.getenv("TSRV_AUTH", '')
```

```
TERMIDESK_AUTH_URL = os.getenv('TSRV_AUTH_URI', '/api/auth/draft/legacy/login')

# OpenStack params
# The name of application credentials
APP_CREDENTIALS_NAME = os.getenv("APP_CREDENTIALS_NAME", "")
# The secret for application credentials
APP_CREDENTIALS_SECRET = os.getenv("APP_CREDENTIALS_SECRET", "")
# The user name for application credentials
APP_CREDENTIALS_USER_NAME = os.getenv("APP_CREDENTIALS_USER_NAME", "")
# The name of user domain for application credentials
APP_CREDENTIALS_USER_DOMAIN = os.getenv("APP_CREDENTIALS_USER_DOMAIN", "")
# The url of application credentials authentication. Example:
http://0.0.0.0/identity/v3/auth/tokens
OPENSTACK_AUTH_URL = os.getenv("OPENSTACK_AUTH_URL", "")
```

Список доступных параметров конфигурационного файла приведен в таблице (см. таблицу Описание параметров конфигурационного файла Оркестратора).

Таблица 199. Описание параметров конфигурационного файла Оркестратора

Параметр	Назначение	Значение по умолчанию
Параметры компонента «Универсальный диспетчер» (секция `Termidesk VDI params`)		
`TERMIDESK_HOST`	FQDN или IP-адрес компонента «Универсальный диспетчер»	`Не задано`
`TERMIDESK_PORT`	Номер порта компонента «Универсальный диспетчер» (как правило, 80 или 443)	`Не задано`
`TERMIDESK_USERNAME`	Имя пользователя с правами администратора в компоненте «Универсальный диспетчер»	`Не задано`
`TERMIDESK_PASSWORD`	Пароль пользователя с правами администратора в компоненте «Универсальный диспетчер»	`Не задано`
`TERMIDESK_AUTH`	Идентификатор домена аутентификации (authSmallName, метка) в компоненте «Универсальный диспетчер», в который входит пользователь `TERMIDESK_USERNAME`	`Не задано`
`TERMIDESK_AUTH_URL`	URL для проверки состояния (`healthcheck`) компонента «Универсальный диспетчер». Если страница доступна (получен ответ: `HTTP_200_OK`), то считается, что компонент «Универсальный диспетчер» функционирует правильно	`/api/auth/draft/legacy/login`
Параметры для проверки пароля приложений OpenStack (секция `OpenStack params`)		
`APP_CREDENTIALS_NAME`	Имя приложения для подключения к OpenStack	`Не задано`
`APP_CREDENTIALS_SECRET`	Ключ-пароль для подключения к OpenStack. Может быть задан или автоматически сгенерирован при создании доступа для приложения. Отображается в интерфейсе OpenStack только один раз, и, в случае утери, требует перегенерации	`Не задано`
`APP_CREDENTIALS_USER_NAME`	Имя пользователя, предоставляющего доступ приложению. Уровень пользователя должен быть не ниже «member». Возможные варианты уровня: «member», «admin»,«owner»	`Не задано`
`APP_CREDENTIALS_USER_DOMAIN`	Имя (не идентификатор) домена OpenStack, в который входит пользователь `APP_CREDENTIALS_USER_NAME`	`Не задано`

Параметр	Назначение	Значение по умолчанию
`OPENSTACK_AUTH_URL`	URL компонента Identity, располагается в OpenStack по пути «Проект - Доступ к API - Identity»	`Не задано`

Запуск служб Оркестратора

Запуск служб осуществляется после задания настроек и проверки их корректности.

Для добавления в автоматический запуск службы Оркестратора:

- выполнить:

```
sudo systemctl enable termidesk-orchestrator.service
```

- затем запустить службу:

```
sudo systemctl start termidesk-orchestrator.service
```

ОРКЕСТРАТОР. ЖУРНАЛИРОВАНИЕ

Журнал работы Оркестратора расположен в файле /`var/log/termidesk/orchestrator.log`.

ТЕРМИНЫ

Балансировщик нагрузки

Самостоятельный компонент, отвечающий за распределение нагрузки на множество «Универсальных диспетчеров» и «Шлюзов»

Домен аутентификации

Способ проверки субъектов и их полномочий

Компонент «Оркестратор»

Компонент Termidesk VDI. Самостоятельный компонент, отвечающий за согласованную работу всех компонентов программного комплекса при децентрализованном развертывании, для нужд отказоустойчивости и комплексирования с облачными службами

Компонент «Универсальный диспетчер»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение и контроль доставки им рабочих мест. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-vdi.service`

Ключ

Последовательность псевдослучайных чисел, сгенерированная особым образом

Сертификат

Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу

СОКРАЩЕНИЯ

ОС	Операционная система
ПО	Программное обеспечение
API	Application Programming Interface (интерфейс прикладного программирования)
FQDN	Fully Qualified Domain Name (полностью определенное имя домена)
HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
IP	Internet Protocol (межсетевой протокол)
RFC	Request for Comments (рабочее предложение Интернет)
URL	Uniform Resource Locator (унифицированный указатель ресурса)

СЛЕТ.10001-01 90 07. РУКОВОДСТВО АДМИНИСТРАТОРА. НАСТРОЙКА КОМПОНЕНТА «СЕРВЕР ТЕРМИНАЛОВ ASTRA LINUX»

ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ

Назначение документа

Настоящий документ является седьмой частью руководства администратора на программный комплекс «Диспетчер подключений виртуальных рабочих мест Термидеск» (далее - Termidesk VDI, Termidesk VDI). Документ предназначен для администраторов системы и сети.

В этом руководстве приведено назначение, установка и настройка компонента «Сервер терминалов Astra Linux». Для того, чтобы получить информацию о месте компонента в программном комплексе, необходимо обратиться ко второй части руководства администратора - СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

Типографские соглашения

Приняты следующие типографские соглашения:

- `моноширинный шрифт` – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk VDI, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

STAL. ОБЩИЕ СВЕДЕНИЯ

Назначение компонента «Сервер терминалов Astra Linux»

Компонент «Сервер терминалов Astra Linux» (англ. «Terminal Server Astra Linux», далее - STAL, сервер терминалов Astra Linux) входит в состав Termidesk VDI.

STAL обеспечивает подключение пользовательских рабочих станций к рабочим местам (РМ) с операционной системой (ОС) Astra Linux Special Edition через сеанс удаленного терминала.

STAL позволяет выполнять доставку как рабочего стола РМ с ОС Astra Linux Special Edition, так и опубликованных приложений.

STAL устанавливается на узел, выбранный в качестве терминального сервера, совместно с компонентом «Сессионный агент» из состава Termidesk VDI.

Для работы со STAL в политиках фонда РМ параметру «Аутентификация на уровне сети (RDP)» должно быть задано значение «TLS» или «RDP».

Требования к программному и аппаратному обеспечению

Для установки STAL минимальные аппаратные требования узла должны соответствовать следующим:

- процессор архитектуры Intel x86 разрядности 64 бит;
- оперативная память, не менее 2 ГБ;
- свободное дисковое пространство, не менее 200 МБ;
- сетевое соединение, не менее 100 Мбит/с.

STAL устанавливается на ОС:

- Astra Linux Special Edition (Server) 1.8 (1.8.1, 1.8.2, 1.8.3, 1.8.4 - максимальная поддерживаемая версия 1.8.4.X). ОС должна быть установлена с графическим интерфейсом;
- Альт Рабочая станция 10. ОС должна быть установлена с графическим интерфейсом, поддерживаются MATE и KDE Plasma.

Для корректной установки всех зависимостей в ОС Astra Linux Special Edition в файле `/etc/apt/sources.list` должны быть указаны репозитории, соответствующие используемой и поддерживаемой версии ОС или версии 1.8.4. Например: при использовании ОС Astra Linux Special Edition версии 1.8.4 файл `/etc/apt/sources.list` приводится к виду:

```
deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.4/main-repository/
1.8_x86-64 main contrib non-free non-free-firmware
deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.4/extended-repository/
1.8_x86-64 main contrib non-free non-free-firmware
```

STAL. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ

Получение пакетов установки в ОС Astra Linux Special Edition

Дистрибутив представлен бинарным файлом пакета ПО в `deb`-формате. Установка в ОС Astra Linux Special Edition производится из локального репозитория, распространяемого в формате `iso`-образа.

Получить `iso`-образ можно двумя способами:

- заполнив запрос через сайт Termidesk VDI: https://termidesk.ru/support/#request-support;
- через личный кабинет:https://lk.astra.ru/.

Для подключения локального репозитория Termidesk VDI на узле, где предполагается установка, нужно:

- скопировать в домашний каталог пользователя образ диска `termidesk-<версия>.iso`;
- подключить образ диска к файловой системе в каталог `/mnt`:

```
sudo mount -o loop termidesk-<версия>.iso /mnt
```

где:

`-o loop` - параметры для привязки петлевого устройства (`/dev/loop`) к файлу `termidesk-<версия>.iso`, устройство затем монтируется в указанный каталог `/mnt`;

- скопировать содержимое каталога `repos` подключенного образа диска в каталог `/var` локальной файловой системы:

```
sudo cp -Rp /mnt/repos /var
```

где:

`-Rp` - ключ для рекурсивного копирования подкаталогов и файлов с сохранением исходных свойств;

- отключить подключенный ранее образ диска от узла:

```
sudo umount /mnt
```

- установить пакет `lsb-release`:

```
sudo apt install -y lsb-release
```

- добавить локальный репозиторий Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list` через командный интерпретатор `sh`:
  - выяснить установленную версию ОС:

    ```
    sudo cat /etc/astra_version
    ```

  - определить актуальное имя каталога с пакетами в `/var/repos`;
  - указать в файле конфигурации APT корректное (фактическое) имя каталога:

    ```
    sudo sh -c 'echo "deb file:/var/repos/astra 1.8_x86-64 non-free" >
    /etc/apt/sources.list.d/termidesk_local.list'
    ```

    где:

    `-c` - ключ для чтения команд из вводимой строки (стандартный ввод);

    `echo` - команда вывода текста, совместно с символом «>» используется для перенаправления строки в файл;

    `deb file:/var/repos/astra 1.8_x86-64 non-free` - добавляемый репозиторий с вложенной командой получения версии ОС;

    Приведенный пример команды актуален для установки основных компонентов Termidesk, пакеты которых расположены в каталоге `1.8_x86-64`.

- для корректной установки компонентов TERA потребуется корректно подключить

дополнительные репозитории и настроить их приоритет:

- для версий ОС Astra Linux Special Edition меньше или равных 1.7.6, а также для версий 1.8.X:
  - подключить два репозитория:

```
sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
non-free" > /etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
/dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

  - добавить повышенный приоритет для репозитория с требуемой версией ОС (значение `$(cat /etc/astra_version)` может подходить не для всех репозиториев, т.к. версия может указываться без точек - в этом случае нужно вручную указать корректную версию):

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000
EOF"
```

- для версий ОС Astra Linux Special Edition 1.7.7 и 1.7.8:
  - подключить три репозитория:

```
sudo sh -c 'echo "deb file:/var/repos/astra 1.7.6 non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
/dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

  - настроить два приоритета:

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=1.7.6
Pin-Priority: 950

Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000

EOF"
```

- выполнить поиск ключа репозитория Termidesk VDI `GPG-KEY-PUBLIC` и добавить его:

```
sudo cat /var/repos/astra/GPG-KEY-PUBLIC | sudo gpg --dearmour -o
/etc/apt/trusted.gpg.d/termidesk.gpg
```

- убедиться, что ключ `release@uveon.ru` был успешно добавлен:

```
apt-key list
```

В случае, если ключ не отображен в выводе команды, необходимо убедиться, что ключ `GPG-KEY-PUBLIC` существует:

```
cat /var/repos/astra/GPG-KEY-PUBLIC
```

Если ключ все же существует, следует проверить правильность выполнения шагов по добавлению репозитория Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list`.

При успешном выполнении всех шагов команда выведет содержимое ключа в формате Base64.

В зависимости от используемой версии ОС команды добавления ключа репозитория Termidesk VDI могут отличаться. Если для ОС Astra Linux Special Edition 1.8 ключ репозитория был добавлен командой, применимой к другой версии ОС, то для исправления нужно:

- узнать идентификатор добавленного ключа репозитория:

```
apt-key list
```

- удалить ключ:

```
apt-key --keyring /etc/apt/trusted.gpg del 4E1632CC
```

где `4E1632CC` - последние 8 символов идентификатора ключа;

- вновь добавить ключ репозитория.

- обновить данные пакетного менеджера:

```
sudo apt update
```

- проверить настройку приоритетов репозиториев:

```
apt-cache policy
```

Команду `sudo apt update` необходимо выполнять при каждом изменении списка источников

пакетов или при изменении содержимого этих источников.

STAL. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ

ОС Astra Linux Special Edition

Установка STAL в ОС Astra Linux Special Edition

Настройка среды функционирования перед установкой

Перед установкой необходимо подключить локальный репозиторий Termidesk. ОС, на которую устанавливается STAL, должна быть установлена с графическим интерфейсом.

Для подключения к опубликованным приложениям и к терминальным сессиям можно использовать отдельные установки STAL для удобства разделения по функционалу: на одном сервере - только приложения, на другом - только терминальные сессии.

Перед началом использования STAL доменными пользователями нужно убедиться в корректной настройке доменного сервера: в имени домена и поддоменов допустимо использовать латиницу, использование кириллицы запрещено. Для проверки следует авторизоваться доменным пользователем в ОС по протоколу SSH или войти через интерфейс GNOME.

При наличии в файле `/etc/apt/sources.list` репозитория `astra-ce` нужно закомментировать его, чтобы избежать установки несовместимых версий пакетов.

Для корректной установки всех зависимостей в ОС Astra Linux Special Edition в файле `/etc/apt/sources.list` должны быть указаны репозитории, соответствующие используемой и поддерживаемой Termidesk VDI версии ОС.

Подробную информацию о сетевых репозиториях ОС Astra Linux Special Edition можно получить в справочном центре Astra Linux:

- для ОС Astra Linux Special Edition 1.8: https://wiki.astralinux.ru/pages/viewpage.action?pageId=302043111.

Например, для ОС Astra Linux Special Edition 1.8.4 файл будет следующим:

```
deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.4/main-repository/
1.8_x86-64 main contrib non-free non-free-firmware
deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.4/extended-repository/
1.8_x86-64 main contrib non-free non-free-firmware
```

Установка STAL в ОС

Для установки STAL нужно:

- выполнить установку основного пакета `termidesk-stal`:

```
sudo apt install termidesk-stal
```

- установить компонент «Сессионный агент» (termidesk-session-agent) из состава Termidesk VDI. После установки компонента «Сессионный агент» рекомендуется выполнить его настройку в конфигурационном файле session_agent.ini: изменить параметр USE_USER_PRINCIPAL_NAME в соответствии с установленной версией STAL;
- (опционально) если STAL устанавливается на отдельный узел и будет подключаться в «Портале администратора» Termidesk VDI через поставщик ресурсов «Автономная машина», то потребуется также установить компонент «Агент виртуального рабочего места» (см. подраздел **ОС Astra Linux Special Edition**).

Если STAL используется в режиме доставки приложений, то нужно убедиться, что политике «Многомониторный режим (RDP, SPICE, TERA)» задано значение «Запрещен».

После установки службы STAL автоматически добавляются в автозагрузку и запускаются. Вручную выполнить перезапуск служб можно командой:

```
sudo systemctl restart termidesk-stal.service termidesk-stal-sesman.service
```

Проверка состояния STAL производится командами:

```
sudo systemctl status termidesk-stal.service
sudo systemctl status termidesk-stal-sesman.service
```

Строка Active отображает состояние сервиса, где статус active (running) означает успешный запуск.

Установка в режиме ЗПС

Замкнутая программная среда (ЗПС) является средством повышения безопасности ОС путем контроля целостности (неизменности) файлов.

Механизм контроля реализован в виде невыгружаемого модуля ядра ОС Astra Linux Special Edition (модуль digsig_verif), выполняющего проверку электронной цифровой подписи файлов (ЭЦП).

Перед установкой компонентов Termidesk VDI необходимо установить пакет termidesk-digsig-keys, для этого:

- подключить репозиторий Termidesk VDI или получить отдельный пакет termidesk-digsig-keys из репозитория;
- выполнить установку с использованием репозитория:

```
sudo apt -y install termidesk-digsig-keys
```

- либо выполнить установку из deb-пакета:

```
sudo apt install -y /home/user/termidesk-digsig-keys-XXXXXX_amd64.deb
```

где:

`-y` - ключ для пропуска подтверждения установки;

`/home/user/termidesk-digsig-keys-XXXXXX_amd64.deb` - расположение пакета `termidesk-digsig-keys-XXXXXX_amd64.deb`.

- перезагрузить ОС:

```
sudo reboot
```

- выполнить установку компонента Termidesk VDI.

Для ЗПС может быть активирован режим проверки встроенной ЭЦП в расширенных атрибутах (`DIGSIG_XATTR_MODE`). В этом случае потребуется подписать файлы, которые будут проходить проверку, имеющимися в организации ключами. Информация о процессе подписи и активации механизма проверки встроенной ЭЦП в расширенных атрибутах приведена в справочном центре Astra Linux: https://wiki.astralinux.ru/pages/viewpage.action?pageId=41190634.

Постановка STAL на контроль целостности

После установки и настройки STAL необходимо поставить его на контроль целостности.

Для контроля целостности используются встроенные в ОС Astra Linux Special Edition программные средства на основе `Another File Integrity Checker`, представленного пакетом `afick`.

Настройка регламентного контроля целостности выполняется в конфигурационном файле `/etc/afick.conf`.

Настройку следует производить только после окончательного внедрения компонента, поскольку с файлов конфигурации и исполняемых файлов будут сняты эталонные контрольные суммы.

Для постановки на контроль целостности STAL необходимо добавить в конфигурационный файл `/etc/afick.conf` следующие строки:

Перечень содержит список строк для компонента «Сессионный агент», поскольку он ставится совместно со STAL.

```
/opt/termidesk/stal/lib/libwinpr3.so.3 PARSEC
/opt/termidesk/stal/lib/libfreerdp3.so.3.16.0 PARSEC
/opt/termidesk/stal/lib/libfreerdp-server3.so.3 PARSEC
/opt/termidesk/stal/lib/libfreerdp-server3.so.3.16.0 PARSEC
/opt/termidesk/stal/lib/libfreerdp-shadow3.so.3 PARSEC
/opt/termidesk/stal/lib/libfreerdp-shadow3.so.3.16.0 PARSEC
/opt/termidesk/stal/lib/libfreerdp-shadow-subsystem3.so.3 PARSEC
/opt/termidesk/stal/lib/libfreerdp-shadow-subsystem3.so.3.16.0 PARSEC
/opt/termidesk/stal/lib/librdtk0.so.0 PARSEC
/opt/termidesk/stal/lib/librdtk0.so.0.2.0 PARSEC
/opt/termidesk/stal/lib/libwinpr3.so.3 PARSEC
/opt/termidesk/stal/lib/libwinpr3.so.3.16.0 PARSEC
/opt/termidesk/stal/lib/libwinpr-tools3.so.3 PARSEC
/opt/termidesk/stal/lib/libwinpr-tools3.so.3.16.0 PARSEC
```

```
/opt/termidesk/stal/plugins/cliprdr-plugin.so PARSEC
/opt/termidesk/stal/plugins/rdpaudin-plugin.so PARSEC
/opt/termidesk/stal/plugins/rdpdisp-plugin.so PARSEC
/opt/termidesk/stal/plugins/rdpdr-plugin.so PARSEC
/opt/termidesk/stal/plugins/rdpvcam-plugin.so PARSEC
/opt/termidesk/stal/plugins/vtmdrv-plugin.so PARSEC

/opt/termidesk/stal/scripts/clear-logs.sh PARSEC
/opt/termidesk/stal/scripts/stal-create-report.sh PARSEC
/opt/termidesk/stal/scripts/stal-mk-keytab.sh PARSEC

/opt/termidesk/stal/stal-kiosk PARSEC
/opt/termidesk/stal/stal-migration PARSEC
/opt/termidesk/stal/stal-service PARSEC
/opt/termidesk/stal/stal-session PARSEC
/opt/termidesk/stal/stal-session-manager PARSEC
/opt/termidesk/stal/stal-shadow-server PARSEC
/opt/termidesk/stal/stal-vprint PARSEC
/opt/termidesk/stal/stal-waitx PARSEC
/opt/termidesk/stal/xsession.sh PARSEC

#Репозиторий Termidesk
/var/repos/ PARSEC
```

Для снятия эталонных значений контрольных сумм используется команда:

```
afick -i
```

Для проверки соответствия контрольных сумм эталонным значениям автоматически создаются задания в системном планировщике заданий `cron`.

Для ручной проверки соответствия контрольных сумм используется команда:

```
afick -k
```

В случае отсутствия по какой-либо причине исполняемых фалов `*.pyc`, они будут повторно сгенерированы при перезапуске сервера Python. В этом случае нужно повторно проинициализировать средство регламентного контроля целостности `afick`.

Обновление STAL в ОС Astra Linux Special Edition

Для обновления STAL с версии 3.0.X до версии 4.0.X нужно:

- удалить STAL версии 3.0.X с сохранением конфигурации и настроек:

```
sudo apt remove -y stal stal-multimedia stal-rdp-transport stal-redirect-api stal-
```

```
redirect-drive stal-redirect-print stal-redirect-clip stal-redirect-scard
```

- полностью удалить предыдущую установленную версию компонента «Сессионный агент»:

```
sudo apt purge -y termidesk-session-agent
```

- выполнить установку STAL версии 4.0.X (см. подраздел **Установка STAL**). В процессе установки будет выполнена миграция конфигурации STAL, предыдущая конфигурация сохранится в резервных копиях;
- выполнить установку компонента «Сессионный агент» актуальной версии из состава релиза Termidesk VDI;

> **!** Использование компонента «Сессионный агент» предыдущих версий (например, из состава Termidesk VDI версии 6.1 или 6.1.1) запрещено.

- выполнить полное удаление STAL версии 3.0.X:

```
sudo apt purge -y stal stal-multimedia stal-rdp-transport stal-redirect-api stal-
redirect-drive stal-redirect-print stal-redirect-clip stal-redirect-scard
```

Удаление STAL в ОС Astra Linux Special Edition

Удаление STAL выполняется командой:

```
sudo aptitude purge -y termidesk-stal
```

Где:

`-y` - ключ для пропуска подтверждения удаления.

После удаления необходимо очистить оставшиеся зависимости и конфигурации:

```
sudo aptitude purge ~c -y
```

Команда полностью удалит оставшиеся настройки и зависимости уже удаленных пакетов.

ОС Альт Рабочая станция

Установка STAL в ОС Альт Рабочая станция

STAL устанавливается в ОС Альт Рабочая станция из `rpm`-пакета `termidesk-stal`.

Для установки STAL:

- переключиться в окружение суперпользователя:

```
su -
```

- выполнить установку `xorg-drv-dummy` версии не ниже 0.4.1:

Пакет `xorg-drv-dummy` размещен в Интернет-репозитории Termidesk VDI.

```
apt-get install <путь_к_пакету>
```

- выполнить установку `termidesk-stal`:

```
apt-get install <путь_к_пакету>
```

Проверить состояние служб после установки:

```
systemctl status termidesk-stal.service termidesk-stal-sesman.service
```

Обновление STAL в ОС Альт Рабочая станция

Обновление STAL выполняется установкой новой версии поверх предыдущей.

Удаление STAL в ОС Альт Рабочая станция

Удаление STAL выполняется командой:

```
sudo apt-get remove -y termidesk-stal
```

STAL. НАСТРОЙКИ

Конфигурационные файлы STAL

Общие сведения о конфигурационных файлах, исполняемых файлах и службах STAL

Для настройки и функционирования STAL используются конфигурационные и исполняемые файлы, перечисленные в таблице (см. таблицу Список конфигурационных и исполняемых файлов STAL).

Перечень и описание служб STAL приведено в таблице (см. таблицу Список и описание служб, процессов и утилит STAL).

В большинстве случаев STAL не требует изменения конфигурационных файлов после установки.

Параметры внутри конфигурационных `JSON`-файлах имеют следующую структуру:

```
{
```

```
    "параметр": "значение",
    "параметр": [ "значение 1", ..., "значение N" ],
    "параметр": [ "значение 1", "%{значение 2}", ..., "значение N" ],
    "параметр": [ "аргумент:%\{значение}" ]
}
```

Поля формата `%{параметр}` используются для подстановки служебных значений.

Целочисленные значения не заключаются в кавычки.

Таблица 200. Список конфигурационных и исполняемых файлов STAL

Файл	Описание
Исполняемые файлы STAL	
`/opt/termidesk/stal/scripts/clear-logs.sh`	Скрипт для очистки всех журналов системы systemd а также утилиты `dmesg`
`/opt/termidesk/stal/scripts/stal-create-report.sh`	Скрипт для сбора всех журналов работы STAL (см. подраздел **Сбор журналов STAL для передачи в техническую поддержку**)
`/opt/termidesk/stal/scripts/stal-mk-keytab.sh`	Скрипт для формирования `keytab`-файла для Kerberos-аутентификации (см. подраздел **Kerberos-аутентификация в STAL**)
`/opt/termidesk/stal/stal-kiosk`	Исполняемый файл процесса `stal-kiosk`
`/opt/termidesk/stal/stal-migration`	Исполняемый файл службы `stal-migration`
`/opt/termidesk/stal/stal-service`	Исполняемый файл службы `stal-service`
`/opt/termidesk/stal/stal-session`	Исполняемый файл процесса `stal-session`
`/opt/termidesk/stal/stal-session-manager`	Исполняемый файл службы `stal-session-manager`
`/opt/termidesk/stal/stal-shadow-server`	Исполняемый файл процесса `stal-shadow-server`
`/opt/termidesk/stal/stal-vprint`	Исполняемый файл процесса `stal-vprint`
`/opt/termidesk/stal/stal-waitx`	Исполняемый файл процесса `stal-waitx`
`/opt/termidesk/stal/xsession.sh`	Скрипт для предварительной настройки и запуска графической оболочки, оконного менеджера. Запускается лидером сеанса `stal-session` после запуска процесса Xorg
Конфигурационные файлы STAL	
`/etc/stal/stal-applications.json`	Конфигурационный файл настройки списка разрешенных программ
`/etc/stal/stal-config.json`	Конфигурационный файл настройки основных служб STAL
`/etc/stal/stal-constrains.json`	Конфигурационный файл настройки ограничения используемых ресурсов пользователя
`/etc/stal/stal-kiosk.json`	Конфигурационный файл настройки определения свойств окон приложений, запускаемых в режиме доставки приложений (киоск)
Конфигурационные файлы системы systemd	
`/usr/lib/systemd/system/termidesk-stal.service`	Конфигурационный файл настройки запуска службы `stal-service`. Запуск службы выполняется автоматически после установки пакета и при перезапуске системы
`/usr/lib/systemd/system/termidesk-stal-sesman.service`	Конфигурационный файл настройки запуска службы `stal-session-manager`. Запуск службы выполняется автоматически после установки пакета и при перезапуске системы

Файл	Описание
Конфигурационные файлы системы PAM	
/etc/pam.d/stal-auth	Конфигурационный файл настройки PAM при создании сеанса с обязательным требованием аутентификации пользователя перед созданием сеанса STAL интегрирован с инструментом мониторинга событий и журналирования auditd ОС Astra Linux Special Edition, а также с системой PAM. Применение настроенных параметров мониторинга событий осуществляется модулем pam_parsec_aud. По умолчанию регистрация событий включена в PAM-сценариях /etc/pam.d/stal-auth, /etc/pam.d/stal-trust.
/etc/pam.d/stal-trust	Конфигурационный файл настройки PAM при создании сеанса для пользователя, который не может пройти аутентификацию перед созданием сеанса, например для схемы аутентификации с использованием Kerberos, OIDC или смарт-карт
Конфигурационные файлы системы D-BUS	
/usr/share/dbus-1/system.d/ru.uveon.stal.conf	Конфигурационный файл для регистрации интерфейса ru.uveon.stal на системной шине D-BUS. Доступ к интерфейсу для управления возможен только для пользователей или процессов, включенных в группу stal-dbus. Интерфейс ru.uveon.stal предоставляет минимальный набор методов и сигналов необходимый для обеспечения управления функциями STAL Изменять файл запрещено!
/usr/share/dbus-1/system.d/ru.uveon.stal.SessionManager.conf	Конфигурационный файл регистрации интерфейса ru.uveon.stal.SessionManager на системной шине D-BUS. Доступ к интерфейсу для управления возможен только для системной учетной записи stal-proxy Изменять файл запрещено!
Конфигурационные файлы утилиты logrotate	
/etc/logrotate.d/stal	Конфигурационный файл настройки ротации журналов STAL
Конфигурационные файлы сервера Xorg	
/etc/X11/stal-xorg.conf	Файл конфигурации драйвера для видео подсистемы сервера Xorg. WARNING: Изменять файл не рекомендуется.
/etc/X11/Xresources/x11-stal	Файл конфигурации графического сервера Xorg
Конфигурационные файлы службы ведения журналов syslog-ng	
/etc/syslog-ng/conf.d/stal-kiosk.conf	Конфигурационный файл настройки перенаправления журналирования для процесса stal-kiosk Конфигурационные файлы из каталога /etc/syslog-ng/conf.d/ используются службой systemd-ng для перенаправления сообщений, зарегистрированных службой systemd-journald, в тот или иной каталог.
/etc/syslog-ng/conf.d/stal-service.conf	Конфигурационный файл настройки журналирования для службы stal-service

Файл	Описание
`/etc/syslog-ng/conf.d/stal-session.conf`	Конфигурационный файл настройки журналирования для процесса `stal-session`
`/etc/syslog-ng/conf.d/stal-session-manager.conf`	Конфигурационный файл настройки журналирования для службы `stal-session-manager`
`/etc/syslog-ng/conf.d/stal-shadow-server.conf`	Конфигурационный файл настройки журналирования для процесса `stal-shadow-server`
`/etc/syslog-ng/conf.d/stal-vprint.conf`	Конфигурационный файл настройки журналирования для процесса `stal-vprint`
`/etc/syslog-ng/conf.d/stal-waitx.conf`	Конфигурационный файл настройки журналирования для процесса `stal-waitx`

Таблица 201. Список и описание служб, процессов и утилит STAL

Служба	Описание
`stal-service`	Служба, являющаяся адаптером для всех взаимодействий с внешним окружением (компонентом «Сессионный агент», подключающимися к сеансу RDP-клиентами). Служба работает с уровнем привилегии системной учетной записи `stal-proxy`. Функции службы: • изоляция менеджера сеансов `stal-session-manager` от внешних воздействий; • обслуживание подключений в процессе с низким уровнем привилегий; • обработка RDP-подключений через диспетчер входящих подключений, реализованный непосредственно в `stal-service`; • взаимодействие с компонентом «Сессионный агент». Обеспечивается регистрацией на системной шине D-BUS интерфейса ru.uveon.stal. Последовательность обработки RDP-подключения: • диспетчер входящих подключений идентифицирует входящий запрос на подключение (на уровне обработки пакета `CR-PDU`); • при успешном определении цели подключения служба `stal-service` обращается с запросом к менеджеру сеансов `stal-session-manager` для организации канала транспорта; • в случае успешной проверки и доступности необходимого сеанса диспетчер входящих подключений передает дескриптор (сокет) входящего подключения в процесс транспорта `stal-shadow-server`; • `stal-shadow-server` запускается в контексте процесса лидера необходимого сеанса и далее работает с привилегией учетной записи пользователя, для которого организован сеанс

Служба	Описание
`stal-session`	Процесс, организующий работу сеанса пользователя и являющийся лидером сеанса. Порождается службой `stal-session-manager`. Процесс регистрирует все события в системном журнале с идентификатором `stal-session`. Функции процесса: • создание группы процессов, необходимых для функционирования графического окружения сеанса пользователя: запуск сервера X11, оконного менеджера и процесса транспорта `stal-shadow-server`, а также запрос к системе PAM для аутентификации пользователя и открытия или закрытия сеанса; • отслеживание состояния порожденных процессов; • взаимодействие с менеджером сеансов `stal-session-manager` для полного контроля над текущим состоянием сеанса и возможности оперативного изменения его настроек; • запуск транспорта для входящего RDP-подключения по запросу службы `stal-service` через `stal-session-manager`
`stal-session-manager`	Служба, управляющая сеансами пользователей, является менеджером сеансов и работает с высоким уровнем привилегий для обеспечения возможности создания и управления лидерами сеансов `stal-session`. Функции службы: • управление сеансами пользователей: создание, удаление, подключение протокола и т.д. Обеспечивается регистрацией на системной шине D-BUS интерфейса ru.uveon.stal.SessionManager; • ограничение ресурсов для процессов лидеров сеансов; • ограничение ресурсов пользовательских сеансов, заданных в файле `stal-constrains.json`
`stal-shadow-server`	Процесс, реализующий доставку графического окружения пользователя, перенаправление каталогов, буфера обмена, аудио, видео, микрофона, принтера, смарт-карт, считывателей и др. Процесс использует реализацию протокола RDP в виде доработанных библиотек FreeRDP, поставляемых вместе с остальными компонентами STAL. Библиотеки FreeRDP, поставляемые в составе дистрибутива ОС, не используются. Выполняется в контексте процесса с уровнем привилегии пользователя. Функции процесса: • перенаправление ресурсов и доставка графического окружения; • загрузка необходимых плагинов (`/opt/termidesk/stal/plugins/`) в зависимости от настроек и политик
`stal-kiosk`	Процесс для работы с окнами приложений в режиме киоска
`stal-migration`	Процесс для работы с миграциями конфигураций при обновлении со STAL версии 3.0.X
`stal-vprint`	Процесс для подсистемы печати
`stal-waitx`	Процесс для проверки корректности запуска и работы графического сервера Xorg

Лидер сеанса (session leader) - это процесс, идентификатор сеанса (SID) которого равен его собственному идентификатору (PID). Отвечает за создание сеанса и группировку связанных процессов.

Файл stal-config.json

Файл /etc/stal/stal-config.json определяет параметры работы основных служб STAL, обеспечивающих запуск и останов графических сессий пользователя и реализующих основной функционал компонента.

Пример файла /etc/stal/stal-config.json:

```
{
    "logger": {
        "type": "systemd",
        "level": "debug"
    },

    "runtime": {
        "dir": "/run/stal",
        "env": []
    },

    "xserver": {
        "path": "/usr/bin/Xorg",
        "args": [ "-config", "stal-xorg.conf", "-nolisten", "tcp" ],
        "sock": "/tmp/.X11-unix/X%{display}"
    },

    "xsession": {
        "path": "/usr/bin/fly-wm",
        "args": []
    },

    "applications": {
        "systems": true,
        "config": "/etc/stal/stal-applications.json",
        "ignores": [
            "1cestart.desktop"
        ]
    },

    "pam": {
        "auth": "stal-auth",
        "noauth": "stal-trust"
    },

    "limits": {
        "users": 200,
        "sessions": 1000,
        "clipboard": 0
    },

    "groups": {
```

```
        "allow": [],
        "xauth": "stal-xauth",
        "sdbus": "stal-dbus"
    },

    "timeouts": {
        "start": 15,
        "seamless": 60,
        "notconnected": 60,
        "inactivity": 0,
        "duration": 0,
        "disconnect": 0,
        "autoconnect": 10
    },

    "transport": {

        "logger": {
            "type": "default",
            "level": "info"
        },

        "kerberos": {
            "realm": "UVEON",
            "keytab": "/etc/krb5.keytab"
        },

        "tcp": {

            "listener": {
                "port": 3389,
                "host": "0.0.0.0",
                "backlog": 5
            },

            "keepalive": {
                "enable": true,
                "delay": 5,
                "retries": 3,
                "interval": 2
            }
        },

        "rdp": {
            "shm": true,
            "fps": 5,
            "codecs": [
                "+gfx-progressive",
                "-gfx-rfx",
```

```
                "-gfx-planar",
                "-gfx-avc420",
                "-gfx-avc444"
            ]
        },

        "redirects": {
            "drive": true,
            "print": true,
            "smartcard": true,
            "audio": false,
            "microphone": false,
            "videocam": false,
            "vitamin": false,
            "clipboard:server": true,
            "clipboard:client": true,
            "clipboard:file": true
        },

        "printers": [
            {
                "name": "Brother HL-1200 series",
                "ppd": "brother-HL1200-cups-en.ppd"
            },
            {
                "name": "Brother HL-1500 series",
                "ppd": "brother-HL1500-cups-en.ppd"
            }
        ]
    },

    "policies": {
        "connection": "PrevReplace",
        "notification": false
    },

    "options": {
        "session:disconnected:freeze": false,
        "desktop:scaling": false,
        "device:scaling": false
    }
}
```

Список доступных параметров конфигурационного файла `/etc/stal/stal-config.json` приведен в таблице (см. таблицу Описание параметров файла конфигурации `stal-config.json`).

Для упрощения записи параметров дочерних узлов дерева конфигурации в таблице используется синтаксис с разделителем `::`. Таким образом,

например, запись `logger::type` соответствует фрагменту конфигурации:

```
{
    ...
    "logger": {
        "type": "systemd",
   },
    ...
}
```

Таблица 202. Описание параметров файла конфигурации `stal-config.json`

Параметр	Значение по умолчанию	Назначение
`logger::type`	`systemd`	Тип системы для журналирования сообщений Менять значение по умолчанию не рекомендуется.
`logger::level`	`debug`	Уровень отладочных сообщений для служб `termidesk-stal`, `termidesk-stal-sesman`, а также процессов лидеров сеансов `stal-session`. Возможные значения: `debug`, `info`, `none`
`runtime::dir`	`/run/stal`	Рабочий каталог сервиса STAL
`runtime::env`	Не задано	Пользовательские переменные окружения, которые будут доступны в сеансе. Допустимо применять шаблон `%{uid}`, в который подставляется реальный UID пользователя. Возможные переменные: • `RDPSND_BUFFER_THRESHOLD` - настройка механизма адаптации размера отправляемых аудиоблоков. Позволяет принудительно отключить адаптивный режим и зафиксировать размер блоков (по умолчанию STAL настраивает размер буфера для аудиоданных длительностью 200 мс). Диапазон значений (в процентах): от 20 до 100. Пример задания значения: `RDPSND_BUFFER_THRESHOLD=70`; • `XDG_RUNTIME_STAL_REDIRECT_DIR` - настройка корня для перенаправляемых каталогов. Если определена переменная окружения `XDG_RUNTIME_STAL_REDIRECT_DIR` (важен сам факт ее определения, например, `XDG_RUNTIME_STAL_REDIRECT_DIR=1`), то корнем для всех перенаправляемых каталогов становится `${XDG_RUNTIME_DIR}/stal`
`xserver::path`	`/usr/lib/xorg/Xorg`	Путь запуска X11-сервера

Параметр	Значение по умолчанию	Назначение
xserver::args	"-config", "stal-xorg.conf", "-nolisten", "tcp"	Список аргументов для X11-сервера Менять значение по умолчанию не рекомендуется.
xserver::sock	/tmp/.X11-unix/X%{display}	Шаблон формата для размещения сокета X11-сервера
xsession::path	/usr/bin/fly-wm	Путь для запуска оконного менеджера сеанса. Значение зависит от целевого дистрибутива. Значение по умолчанию приведено для ОС Astra Linux Special Edition
xsession::args	Не задано	Список аргументов для запуска оконного менеджера сеанса. Значение зависит от целевого дистрибутива. Значение по умолчанию приведено для ОС Astra Linux Special Edition
applications::system	true	Флаг для управления функцией выдачи списка опубликованных приложений. Значение true применяется для выдачи списка всех приложений, описанных в desktop-файлах каталога /usr/share/applications
applications::config	/etc/stal/stal-applications.json	Путь к файлу с конфигурацией опубликованных приложений, не описанных в desktop-файлах каталога /usr/share/applications или для определения полного списка приложений при применении параметра applications::system со значением false
applications::ignores	1cestart.desktop	Список имен приложений, игнорируемых для публикации. В значении параметра должен указываться desktop-файл программы: <имя программы>.desktop
pam::auth	stal-auth	Путь к файлу с описанием правил системы PAM, используемых при создании сеанса с обязательным требованием аутентификации пользователя перед этим
pam::noauth	stal-trust	Путь к файлу с описанием правил системы PAM, используемых при создании сеанса пользователя, который не может пройти аутентификацию перед этим. Например, для схемы аутентификации с использованием Kerberos, OIDC или смарт-карт
limits::users	200	Максимальное количество сеансов в режиме доставки приложений для одного пользователя
limits::sessions	1000	Общее максимальное количество всех сеансов
limits::clipboard	0	Размер буфера обмена в байтах. Значение 0 - буфер обмена не ограничен
timeouts::start	15	Время ожидания (в секундах) запуска сеанса. По истечении указанного времени произойдет отказ создания сеанса

Параметр	Значение по умолчанию	Назначение
`timeouts::seamless`	`60`	Время жизни (в секундах) сеанса приложения после отключения транспорта. В течение этого времени: • можно повторно подключиться сеансу; • приложение сохраняет свое состояние
`groups::allow`	Не задано	Список групп пользователей, которым разрешена аутентификация на сервере STAL. Если список не задан, то аутентификация разрешена всем пользователям
`groups::xauth`	`stal-xauth`	
`groups::sdbus`	`stal-dbus`	
`timeouts::notconnected`	`60`	Время ожидания (в секундах) первого подключения к сеансу после его создания. По истечении указанного времени сеанс завершится
`timeouts::inactivity`	`0`	Время жизни (в секундах) сеанса при бездействии. Значение `0` - время не ограничено
`timeouts::duration`	`0`	Время (в секундах) продолжительности работы сеанса. Значение `0` - время не ограничено
`timeouts::disconnect`	`0`	Время жизни (в секундах) сеанса доставки рабочего стола после отключения транспорта. Значение `0` - время не ограничено
`timeouts::autoconnect`	`10`	Время ожидания (в секундах) подключения транспорта. Применяется для совместимости с клиентами подключений, не идентифицировавшими запрос соединения в пакете `CR-PDU` с применением серверного идентификатора (cookie) для созданного сеанса
`policies::connection`	`PrevReplace`	Политика для нового подключения транспорта к сеансу с активным подключением. Возможные значения: • `NextDeny` - если сеанс занят, то следующее соединение в него отменяется; • `PrevReplace` - если сеанс занят, то предыдущее соединение в него отменяется
`policies::notification`	`false`	Включение или отключение политики для информирования пользователя в его сеансе через механизм всплывающих сообщений
`options::session:disconnected:freeze`	`false`	Системный параметр, менять значение не рекомендуется
`options::desktop:scaling`	`false`	Включение или отключение поддержки масштабирования экрана в сеансе доставки рабочего стола
`options::device:scaling`	`false`	Системный параметр, менять значение не рекомендуется

Параметр	Значение по умолчанию	Назначение
Конфигурация секции `transport`		
`logger::level`	`info`	Уровень отладочных сообщений для процесса `stal-shadow-server`. Возможные значения: `debug`, `info`
`logger::type`	`default`	Тип системы для журналирования сообщений Менять значение по умолчанию не рекомендуется.
`kerberos::realm`	`UVEON`	Область домена аутентификации Kerberos
`kerberos::keytab`	`/etc/krb5.keytab`	Путь к файлу ключей Kerberos для STAL. Для файла должно быть выдано разрешение на чтение для группы `stal-proxy`
`tcp::listener::port`	`3389`	TCP-порт для подключения транспорта RDP
`tcp::listener::host`	`0.0.0.0`	IP-адрес (IPv4) интерфейса для сокета пролушивания входящих подключений. Значение `0.0.0.0` - сокет привязывается ко всем интерфейсам узла
`tcp::listener::backlog`	`5`	Размер очереди (на уровне ядра ОС) для сокета пролушивания входящих подключений. При переполнении очереди соединение сбрасывается. STAL способен распределить обработку входящих соединений между 4 потоками, а также ставить обработку соединений в свою очередь для пула обрабатывающих потоков. Увеличивать значение не имеет практического смысла, поскольку очередь будет накапливаться только в случае высокой загрузки системы, но в этом случае функция очередей не исправит ситуацию
`keepalive::enable`	`true`	Включение или отключение использования механизма `keepalive`
`keepalive::delay`	`5`	Время простоя (в секундах) соединения, по истечении которого начнется передача проверочных TCP-пакетов (keepalive probes)
`keepalive::retries`	`3`	Максимальное количество проверочных TCP-пакетов, отправляемых перед сбросом соединения
`keepalive::interval`	`2`	Время (в секундах) между отправками отдельных проверочных TCP-пакетов
`rdp::shm`	`true`	Включение или отключение поддержки расширения `MIT-SHM` для X11-сервера

Параметр	Значение по умолчанию	Назначение
`rdp::fps`	`5`	Максимальное количество кадров в секунду (FPS) для захвата, кодирования и доставки изображения рабочего стола или приложения. Реальное значение FPS в процессе работы зависит от пропускной способности канала и адаптируется в диапазоне значений от 1 до максимального: • если значение параметра меньше 10, то адаптация возможна до значения, на половину большее указанного (<значение> + 0.5 * <значение>); • если значение параметра больше или равно 10, то адаптация возможна только до указанного значения. Параметр непосредственно связан с ресурсами узла и его текущей загруженности. Менять значение по умолчанию не рекомендуется. В большинстве случаев указанное значение является оптимальным для работы с офисными приложениями в условиях многопользовательского режим использования ресурсов узла. Возможные значения: от 5 до 25
`rdp::codecs`	`"+gfx-progressive", "-gfx-rfx", "-gfx-planar", "-gfx-avc420", "-gfx-avc444"`	Список кодеков для декодирования изображения. Используется для процесса `stal-shadow-server` (транспорта RDP) WARNING: Менять значения по умолчанию не рекомендуется. Изменение должно согласовываться с возможностями клиента подключений, системным окружением и самого STAL.
`redirects::drive`	`true`	Включение или отключение политики перенаправления каталогов
`redirects::print`	`true`	Включение или отключение политики перенаправления принтеров
`redirects::smartcard`	`true`	Включение или отключение политики перенаправления смарт-карт
`redirects::audio`	`false`	Включение или отключение политики перенаправления аудио-вывода
`redirects::microphone`	`false`	Включение или отключение политики перенаправления микрофона
`redirects::videocam`	`false`	Включение или отключение политики перенаправления веб-камеры
`redirects::vitamin`	`false`	Включение или отключение политики перенаправления считывателя TouchMemory производства ООО «Фирма ИнфоКрипт»

Параметр	Значение по умолчанию	Назначение
redirects::clipboard:server	true	Включение или отключение политики разрешения перенаправления буфера обмена на сервер
redirects::clipboard:client	true	Включение или отключение политики разрешения перенаправления буфера обмена на клиент подключений
redirects::clipboard:file	true	Включение или отключение политики разрешения перенаправления файлов через буфер обмена на сервер
printers::name	Brother HL-1200 series, Brother HL-1500 series	Имя драйвера принтера, используемого пользователем
printers::ppd	brother-HL1200-cups-en.ppd, brother-HL1500-cups-en.ppd	Имя файла драйвера принтера, используемого пользователем

Файл stal-kiosk.json

Файл /etc/stal/stal-kiosk.json предназначен для определения свойств окон приложений (см. рисунок Влияние stal-kiosk на поведение окна), запускаемых в режиме доставки приложений (киоск).

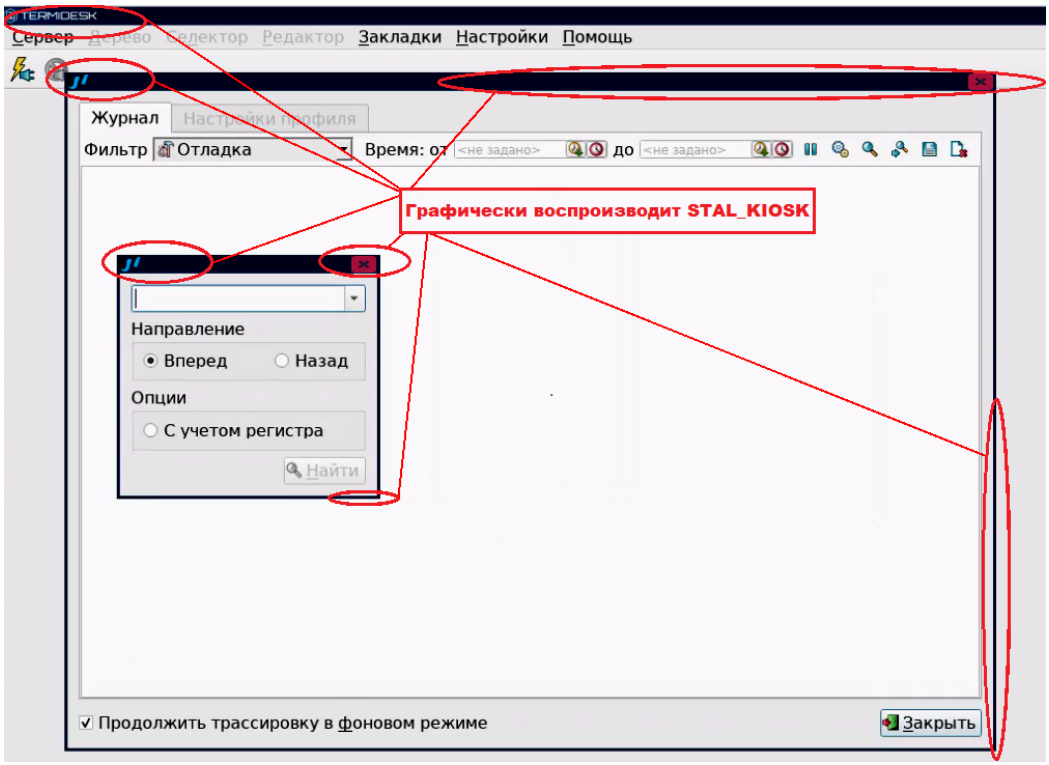


Рисунок 126. Влияние stal-kiosk на поведение окна

Пример файла /etc/stal/stal-kiosk.json:

```
[
    {
        "wm:window:type": "dialog",
        "wm:class": "1cv8*",
        "wm:window:role": "GtkFileChooserDialog",
        "frame": false,
```

```
        "fullscreen": true
    },
    {
        "wm:window:type": "dialog",
        "wm:class": "1cv8*",
        "frame": false,
        "fullscreen": false
    },
    {
        "wm:class": "xterm",
        "frame": false,
        "fullscreen": true
    },
    {
        "wm:window:type": "normal",
        "wm:class": "*",
        "frame": false,
        "fullscreen": true
    },
    {
        "wm:window:type": "dialog",
        "wm:class": "*",
        "frame": true,
        "fullscreen": false
    }
]
```

Поведение окон, описанное в файле конфигурации `/etc/stal/stal-kiosk.json`, реализуется по тегам системной утилиты `xprop`. Список доступных параметров приведен в таблице (см. таблицу Описание параметров файла конфигурации stal_kiosk).

Для получения значения тега для определенного окна нужно:

- запустить окно нужного приложения;
- запустить утилиту `xprop` из интерфейса командной строки:

```
xprop
```

- выбрать левой кнопкой мыши открытое окно, теги которого необходимо получить;
- информация по тегам утилиты `xprop`, назначенных для этого окна, отобразится в интерфейсе командной строки, пример:

```
WM_NAME(COMPOUND_TEXT) = "Домашняя - Менеджер файлов"
_NET_WM_NAME(UTF8_STRING) = "Домашняя - Менеджер файлов"
_MOTIF_WM_HINTS(_MOTIF_WM_HINTS) = 0x3, 0x3e, 0x7e, 0x0, 0x0
_NET_WM_WINDOW_TYPE(ATOM) = _NET_WM_WINDOW_TYPE_NORMAL
_XEMBED_INFO(_XEMBED_INFO) = 0x0, 0x1
WM_CLIENT_LEADER(WINDOW): window id # 0x3200008
```

```
WM_HINTS(WM_HINTS):
                Client accepts input or input focus: True
                window id # of group leader: 0x3200008
WM_CLIENT_MACHINE(STRING) = "cl-00000"
_NET_WM_PID(CARDINAL) = 1721
_NET_WM_SYNC_REQUEST_COUNTER(CARDINAL) = 52429217
WM_CLASS(STRING) = "fly-fm-service", "fly-fm-service"
WM_PROTOCOLS(ATOM): protocols  WM_DELETE_WINDOW, WM_TAKE_FOCUS, _NET_WM_PING,
_NET_WM_SYNC_REQUEST
WM_NORMAL_HINTS(WM_SIZE_HINTS):
                user specified size: 1333 by 913
                program specified minimum size: 182 by 219
                window gravity: Static
```

Таблица 203. Описание параметров файла конфигурации stal_kiosk

Параметр	Назначение
`wm:window:type`	Соответствует тегу `_NET_WM_WINDOW_TYPE` утилиты `xprop`. Допустимые значения: «dialog», «utility», «splash», «menu», «popup_menu», «tooltip», «notification», «normal»
`wm:class`	Соответствует тегу `WM_CLASS` утилиты `xprop`
`wm:window:role`	Соответствует тегу `WM_WINDOW_ROLE` утилиты `xprop`
`frame`	Определяет реализуемое действие: использовать (`true`) или запретить (`false`) дополнительное оформление окна
`fullscreen`	Определяет реализуемое действие: использовать (`true`) или запретить (`false`) полноэкранный режим для окна

Главное окно приложения всегда запускается в полноэкранном режиме!

Файл `stal-constrains.json`

Конфигурационный файл `/etc/stal/stal-constrains.json` предназначен для определения ограничений на используемые ресурсы сессий пользователя: памяти, процессора, количества процессов и задач, сети.

Для просмотра информации о конфигурационном файле используется команда:

```
man stal-constrains
```

Конфигурационный файл содержит секции:

- `"default"`: задает ограничения по умолчанию;
- `"groups"`: задает ограничения пользователя, если он состоит в указанной группе;
- `"users"`: задает ограничения пользователя.

Пример конфигурационного файла после установки STAL:

```
{
    "default": {
        "cpu:weight": 0,
        "cpu:quota": 0,
        "memory:high": "",
        "memory:max": "",
        "tasks:max": 0,
        "network:deny": "",
        "network:allow": ""
    },
    "groups": [
        {
            "name": "test-admins",
            "limits": {
                "cpu:weight": 0,
                "cpu:quota": 0,
                "memory:high": "",
                "memory:max": "",
                "tasks:max": 1024
            }
        },
        {
            "name": "test-users",
            "limits": {
                "cpu:weight": 0,
                "cpu:quota": 20,
                "memory:high": "2G",
                "memory:max": "3G",
                "tasks:max": 256
            }
        }
    ],
    "users": [
        {
            "name": "vasyan",
            "limits": {
                "cpu:weight": 0,
                "cpu:quota": 3,
                "memory:high": "1G",
                "memory:max": "2G",
                "tasks:max": 128,
                "network:deny": "any",
                "network:allow": "localhost"
            }
        }
    ]
}
```

Список доступных параметров конфигурационного файла приведен в таблице (см. таблицу Описание параметров конфигурационного файла `stal-constrains.json`).

Для упрощения записи параметров дочерних узлов дерева конфигурации в таблице используется синтаксис с разделителем `::`. Таким образом, например, запись `limits::cpu:weight` соответствует фрагменту конфигурации:

```
{
    ...
    "limits": {
        "cpu:weight": 0,
   },
    ...
}
```

Подробную информацию по используемым значениям параметров системы управления службами `systemd` можно получить по ссылке: https://www.freedesktop.org/software/systemd/man/latest/systemd.resource-control.html.

Таблица 204. Описание параметров конфигурационного файла `stal-constrains.json`

Параметр	Назначение
Секция `"default"`	
`cpu:weight`	Соответствует параметру «CPUWeight» в системе управления службами systemd. Значение по умолчанию: `100`. Разрешенные значения: от 1 до 10000. Значение `0`: функциональность не используется
`cpu:quota`	Соответствует параметру «CPUQuota» в системе управления службами systemd. Значение указывается в процентах на одно ядро процессора. Значение `0`: функциональность не используется
`memory:high`	Ограничение использования памяти выполняемыми процессами. Соответствует параметру «MemoryHigh» в системе управления службами systemd. Значение задается в байтах. Также могут быть использованы суффиксы: • K - килобайт, например: 1K; • M - мегабайт, например: 1M; • G - гигабайт, например: 1G; • T - терабайт, например: 1T. Значение не задано: параметр и функциональность не используются
`memory:max`	Абсолютное ограничение использования памяти выполняемыми процессами. Соответствует параметру «MemoryMax» в системе управления службами systemd. Значения задаются аналогично параметру `memory:high`. Значение не задано: функциональность не используется

Параметр	Назначение
`tasks:max`	Максимальное количество задач, которые можно создать для сессии. Соответствует параметру «TasksMax» в системе управления службами systemd. Значение `0`: функциональность не используется
`network:deny`	Соответствует параметру «IPAddressDeny» в системе управления службами `systemd`. В качестве значений можно указывать: • разделенный пробелами список IP-адресов, каждый из которых может иметь значение маски после символа «/», например: 192.0.2.1/24; • символическое имя `any`: любой узел; • символическое имя `localhost`: локальный узел; • символическое имя `link-local`: все локальные IP-адреса; • символическое имя `multicast`: все IP-адреса многоадресной рассылки. Значение не задано: функциональность не используется
`network:allow`	Соответствует параметру «IPAddressAllow» в системе управления службами systemd. Значения задаются аналогично параметру `network:deny`. Значение не задано: функциональность не используется
Секции `"groups"` и `"users"`	
`name`	Имя группы или пользователя, к которому будут применены ограничения
`limits::cpu:weight`	Аналогично параметру `cpu:weight`
`limits::cpu:quota`	Аналогично параметру `cpu:quota`
`limits::memory:high`	Аналогично параметру `memory:high`
`limits::memory:max`	Аналогично параметру `memory:max`
`limits::tasks:max`	Аналогично параметру `tasks:max`
`limits::network:deny`	Аналогично параметру `network:deny`
`limits::network:allow`	Аналогично параметру `network:allow`

Файл `stal-applications.json`

Конфигурационный файл `/etc/stal/stal-applications.json` предназначен для задания списка разрешенных приложений, не имеющих файлов `.desktop` в каталоге `/usr/share/applications`.

Для просмотра информации о конфигурационном файле используется команда:

```
man stal-applications
```

Параметры внутри файла `/etc/stal/stal-applications.json` имеют следующую структуру:

```
[
    {
        "name": "наименование приложения",
        "path": "путь для запуска приложения" ,
```

```
        "args": [ "аргумент запуска 1", ..., "аргумент запуска N" ],
    }
]
```

Пример файла:

```
[
    {
        "name": "Midnight Commander",
        "path": "/usr/bin/xterm",
        "args": [ "-e", "/usr/bin/mc" ]
    },
    {
        "name": "Firefox (Secondary Profile)",
        "path": "/usr/bin/firefox",
        "args": [ "--ProfileManager" ]
    },
    {
        "name": "Chromium (Secondary Profile)",
        "path": "/usr/bin/chromium",
        "args": [ "--temp-profile" ]
    }
]
```

Настройка динамического разрешения экрана и поддержки высокого разрешения

STAL поддерживает динамическое разрешение экрана при подключении пользователя через компонент «Клиент» к терминальной сессии или опубликованному в STAL приложению.

В случае, если пользователь подключается к терминальной сессии STAL или получает опубликованное приложение с ОС Microsoft Windows 11 функциональность динамического разрешения экрана не работает.

Рекомендуется включить сглаживание шрифтов перед первым входом пользователя в терминальную сессию, для этого:

- на сервере STAL перейти «Звезда - Панель управления - Рабочий стол - Шрифты»;
- задать параметру «Сглаживание» значение «Включить» и нажать кнопку **[Применить]** (см. рисунок Включение сглаживания шрифтов).

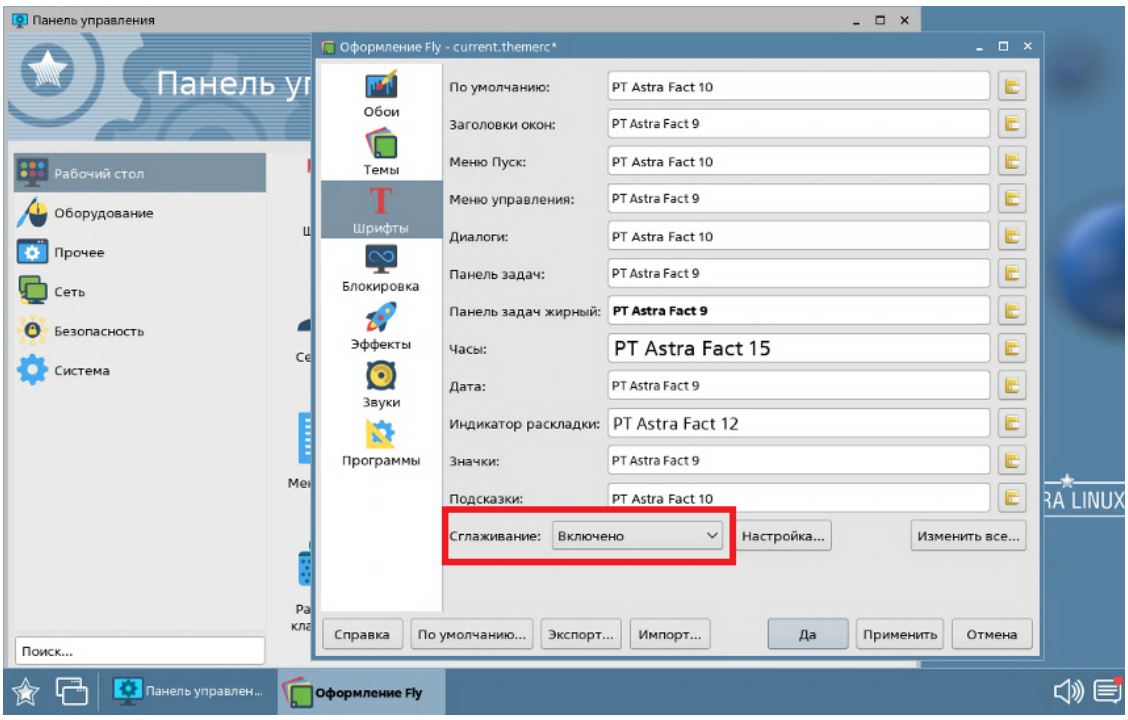


Рисунок 127. Включение сглаживания шрифтов

Задание списка разрешенных программ в STAL

Список разрешенных программ создается двумя механизмами, дополняющими друг друга:

- автоматически, через сканирование каталога `/usr/share/applications` файлов `.desktop`;
- вручную, дополнительно файлом `/etc/stal/stal-applications.json` (см. подраздел **Файл stal-applications.json**).

Консольные программы необходимо запускать через графический терминал, пример для `Midnight Commander`:

```
[
    {
        "name": "Midnight Commander",
        "path": "/usr/bin/xterm",
        "args": [ "-e", "/usr/bin/mc" ]
    }
]
```

Несистемные программы, требующие дополнительных настроек переменных среды, например `LD_LIBRARY_PATH`, следует запускать отдельным скриптом, в котором все эти переменные должны быть определены.

Пример файла сценария для определения переменных среды и запуска программы `RuBackup Manager`:

```
#!/bin/bash
export PATH=$PATH:/opt/rubackup/bin
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/rubackup/lib
```

```
/opt/rubackup/bin/rbm

exit 0
```

Задание списка запрещенных программ в STAL

В некоторых случаях может потребоваться задать список запрещенных программ, которые не должны быть опубликованы сервером STAL.

Такая необходимость может возникнуть в случае, если программа может выполняться в фоновом режиме. Например, в списке программ после установки 1С есть три исполняемых экземпляра:

- `1C:Enterprise x64`;
- `1C:Enterprise - Thin client x64`;
- `1C:Enterprise x64` - этот экземпляр запускает подпрограмму `1cestart`, которая выполняется только в фоновом режиме.

Список запрещенных программ задается через параметр `applications:ignores` конфигурационного файла `/etc/stal/stal-config.json` (см. подраздел **Файл `stal-config.json`**). По умолчанию в нем уже хранится значение для запрета программы 1С - `1cestart.desktop`.

Ограничение ресурсов сессий пользователя

В STAL поддерживается определение ограничений на используемые ресурсы сессий пользователя: памяти, процессора, количества процессов и задач, сети.

Ограничения задаются в конфигурационном файле `/etc/stal/stal-constrains.json` (см. подраздел **Файл `stal-constrains.json`**).

Для контроля значений ресурсов нужно воспользоваться командами:

```
sudo loginctl list-sessions
sudo systemctl show session-SID.scope
sudo systemctl show user-UID.slice
```

Где:

`SID` - идентификатор сессии пользователя;

`UID` - идентификатор пользователя.

Оптимизация работы FreeRDP3

В параметрах конфигурирования STAL доступен выбор видеокодека для улучшения производительности при передаче графически насыщенного контента (видео, 3D-графики и анимации).

Для оптимизации передачи графических данных по протоколу FreeRDP3 используются параметры `rdp:shm`, `rdp:fps` и `rdp:codecs` файла `/etc/stal/stal-config.json` (см. подраздел **Файл `stal-config.json`**).

STAL распределяет ресурсы системы для обеспечения возможности работы множества

сеансов пользователей и значение FPS ограничивается, поскольку он непосредственно связан с ресурсами сервера STAL. Каждая единица параметра FPS - это операция захвата, кодирования и доставки изображения размером, равным разрешению пользовательского монитора.

Реальное значение FPS в процессе работы адаптируется в диапазоне значений от 1 до максимального (`FPS max`):

- если значение параметра `rdp:fps` меньше 10, то адаптация возможна до значения `FPS max` = `rdp:fps` + `rdp:fps` / 2, т.е. возможно автоматическое увеличение на 50%;
- если значение параметра `rdp:fps` больше или равно 10, то адаптация возможна до значения `FPS max` = `rdp:fps`, т.е. без увеличения на 50%.

Алгоритм расчета реального значения FPS основан на анализе очереди кадров, находящихся в процессе обработки, и непосредственно связан с пропускной способностью канала связи:

- при плохом качестве канала связи выполнять захват и кодирование изображения не имеет практического значения, поскольку есть очередь кадров, находящихся в обработке и не подтвержденных клиентской стороной. Поэтому значение FPS постепенно уменьшается (минимум до 1), пока не будет достигнут баланс;
- при хорошем качестве канала связи, когда кадры могут передаваться быстро, значение FPS может адаптироваться в сторону увеличения до значения `FPS max`, в зависимости от текущей загрузки сервера. Поэтому не рекомендуется изменять предустановленное значение 5 FPS, поскольку в большинстве случаев это оптимальное значение для работы с офисными приложениями в условиях многопользовательского режима использования ресурсов сервера.

Аутентификация OIDC в STAL

Настройка аутентификации OIDC

Для настройки аутентификации OIDC в STAL нужно задать дополнительные параметры в конфигурационном файле `/etc/sssd/sssd.conf`.

Для этого после ввода ОС Astra Linux Special Edition в домен выполнить:

- отредактировать файл `/etc/sssd/sssd.conf`, присвоив параметру `use_fully_qualified_names` значение `True`;
- перезапустить службу `sssd`:

```
sudo systemctl restart sssd
```

Kerberos-аутентификация в STAL

Общие сведения

STAL поддерживает Kerberos-аутентификацию в домене MS AD при доступе пользователя к РМ.

Kerberos-аутентификация возможна, если:

- для доступа к STAL используется домен аутентификации Termidesk VDI, поддерживающий функционал Kerberos и настроенный на его использование;
- узел STAL был введен в домен с использованием утилиты `sssd` (при использовании

службы каталогов MS AD утилита winbind не должна использоваться);

- в компоненте «Сессионный агент» используется параметр USE_USER_PRINCIPAL_NAME со значениями Auto или True;
- в «Портале администратора» Termidesk VDI заданы политики:
  - «Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)» в значение «Включен»;
  - «Аутентификация на уровне сети (RDP)» в значение «NLA» или «Автосогласование»;
- в «Портале администратора» Termidesk VDI поставщик ресурсов «Сервер терминалов» добавлен по FQDN;
- выполнена настройка узла STAL, как приведено ниже.

Настройка узла STAL состоит из:

- подготовки узла с настройкой службы SSSD;
- получении keytab;
- настройки конфигурации stal-config.json.

Подготовка узла

Требования к имени узла (hostname):

- имя узла не должно превышать 15 символов;
- имя узла должно совпадать с ComputerName в службе каталогов Active Directory с точностью до регистра символов.

Пример: если ComputerName = OS-STAL, то и hostname должен быть OS-STAL (регистр не учитывается разрешением имен, но для keytab это критично).

Требования к DNS-записям:

- в DNS-зоне домена должны присутствовать корректные A (или AAAA) и PTR-записи для данного узла.

Если узел не прописан в DNS, при создании keytab не будут сгенерированы записи для FQDN, что приведет к ошибкам аутентификации.

Для настройки службы SSSD нужно:

- отредактировать файл /etc/sssd/sssd.conf, присвоив параметру use_fully_qualified_names значение True;
- перезапустить службу sssd:

```
sudo systemctl restart sssd
```

Получение keytab

Для получения keytab нужно:

- получить билет администратора домена. Имя администратора домена и имя домена необходимо уточнить у администраторов инфраструктуры:

```
sudo kinit <Администратор_домена>@<ИМЯ_ДОМЕНА>
```

Пример:

```
sudo kinit administrator@LAN.LOC
```

- установить утилиту msktutil, доступную в репозитории Termidesk VDI:

```
sudo apt install msktutil
```

- создать учетную запись узла и создать keytab:
  - выполнить предварительное создание:

```
msktutil --server <КОНТРОЛЛЕР_ДОМЕНА> \
         --precreate \
         --host <ИМЯ_УЗЛА> \
         --computer-name <ИМЯ_КОМПЬЮТЕРА_В_ВЕРХНЕМ_РЕГИСТРЕ> \
         -b cn=computers \
         --service TERMSRV \
         --enctypes 24 \
         -N
```

  - выполнить обновление и выгрузку keytab. В результате выполнения команды будет создан файл temp.keytab:

```
msktutil --server <КОНТРОЛЛЕР_ДОМЕНА> \
         --auto-update \
         --computer-name <ИМЯ_КОМПЬЮТЕРА_В_ВЕРХНЕМ_РЕГИСТРЕ> \
         --keytab temp.keytab \
         --host <ИМЯ_УЗЛА> \
         -N
```

- заменить существующий файл /etc/krb5.keytab новым и установить корректные права доступа:

```
mv temp.keytab /etc/krb5.keytab
chown root:stal-proxy /etc/krb5.keytab
chmod 640 /etc/krb5.keytab
```

Для проверки корректности keytab нужно:

- просмотреть содержимое keytab:

```
sudo klist -kt /etc/krb5.keytab
```

- убедиться, что в выводе команды присутствуют следующие обязательные типы записей:
  - запись имени узла с символом `$` (в верхнем регистре). Пример: `OS-STAL$@LAN.LOC`;
  - запись службы `TERMSRV`. Примеры: `TERMSRV/os-stal@LAN.LOC`, `TERMSRV/os-stal.lan.loc@LAN.LOC`;
  - записи `host` и `RestrictedKrbHost` для обоих вариантов имени (короткого и FQDN);
- убедиться, что в выводе команды отсутствует запись имени узла в нижнем регистре с символом `$` в конце:
  - неправильно: `os-stal$@LAN.LOC`;
  - правильно: `OS-STAL$@LAN.LOC`.

Настройка конфигурации `stal-config.json`

В конфигурационном файле `/etc/stal/stal-config.json` необходимо добавить (или раскомментировать) следующие параметры, отвечающие за Kerberos-аутентификацию:

```
// ...
        "kerberos": {
            "realm": "TST.LOC",
            "keytab": "/etc/krb5.keytab",
            "check:domain": true
        },
// ...
```

Где `LAN.LOC` - имя домена.

Аутентификация по смарт-картам в STAL

STAL поддерживает сквозную аутентификацию по смарт-картам при доступе пользователя к РМ.

Сквозная аутентификация по смарт-картам возможна, если:

- для доступа к STAL используется домен аутентификации Termidesk VDI, поддерживающий функционал PKINIT и настроенный на его использование;
- узел STAL введен в домен с использованием инструмента `sssd` (при использовании службы каталогов MS AD инструмент `winbind` не должен использоваться);
- выполнена настройка службы `SSSD`, как приведено ниже.

Для настройки службы `SSSD` нужно:

- отредактировать файл `/etc/sssd/sssd.conf`, присвоив параметру `use_fully_qualified_names` значение `True`;
- перезапустить службу `sssd`:

```
sudo systemctl restart sssd
```

STAL. ПЕРЕНАПРАВЛЕНИЕ РЕСУРСОВ

Общие сведения по перенаправлению ресурсов в STAL

Правила перенаправления ресурсов для терминальных сессий задаются политиками фонда в «Портале администратора» Termidesk VDI, а также в конфигурационном файле `/etc/stal/stal-config.json` (см. подраздел **Файл `stal-config.json`**).

STAL поддерживает:

- перенаправление дисков и каталогов;
- перенаправление принтеров;
- перенаправление буфера обмена (файлы, текст, картинки);
- перенаправление смарт-карт;
- перенаправление звука (требуется включить принудительно через конфигурационный файл `/etc/stal/stal-config.json`);
- перенаправление микрофона (требуется включить принудительно через конфигурационный файл `/etc/stal/stal-config.json`);
- перенаправление веб-камеры (требуется включить принудительно через конфигурационный файл `/etc/stal/stal-config.json`);
- перенаправление считывателя TouchMemory (требуется включить принудительно через конфигурационный файл `/etc/stal/stal-config.json`)/

Не гарантируется копирование файлов через буфер обмена с сервера STAL в пользовательскую ОС Astra Linux Special Edition, если в ОС установлен режим «Смоленск».

Перенаправление ресурсов не работает:

- при подключении высокоуровневым пользователем - это блокируется защитными механизмами ОС Astra Linux Special Edition («Смоленск», «Воронеж»);
- при использовании в ОС Astra Linux Special Edition 1.8 («Смоленск», «Воронеж») механизма ЗПС$
- при подключении к сеансу пользователем с высоким уровнем целостности.

Перенаправление принтеров в STAL

Перенаправление принтеров для ОС Astra Linux Special Edition 1.8 доступно как при включении механизма мандатного контроля целостности в ОС, так и при его отключении.

По умолчанию для принтеров используется драйвер `raw`, который отправляет на печать задание без дополнительного конвертирования (как есть).

Если принтер поддерживает Postscript (PS) или Page Description Language (PCL), или другой язык, то достаточно получить информацию об используемом драйвере, добавить ее в файл `/etc/stal/stal-config.json` и перезапустить сервис `termidesk-stal.service`, как приведено ниже.

Настройка перенаправления принтеров в STAL будет отличаться в зависимости от ОС

пользовательской рабочей станции:

- пользовательская ОС на базе Linux: задание `raw`-формата отправится без изменения и будет распечатано клиентской программой через систему печати CUPS, настроенной на пользовательской рабочей станции в соответствии с документацией на ОС. Дополнительные настройки на STAL в этом случае выполнять не нужно;
- пользовательская ОС Microsoft Windows: может потребоваться конвертирование задания печати, потому что не все принтеры способны распечатать файл без дополнительного преобразования в поддерживаемый ими формат. В этом случае:
  - если для принтера не существует драйвер под ОС на базе Linux, то достаточно добавить программный виртуальный принтер PDF/XPS на пользовательской рабочей станции и не выполнять дополнительную настройку STAL;
  - если для принтера существует драйвер под ОС на базе Linux, то администратору нужно выполнить настройку STAL, описание которой приведено ниже. Настройка заключается в изменении конфигурации, ассоциирующей драйвер принтера с драйвером системы CUPS.

Для настройки печати на сервере STAL нужно выполнить:

- установить драйвер для системы печати CUPS (x86_64) в соответствии с инструкцией драйвера;
- получить информацию об используемом пользователем драйвере:
  - получить имя принтера (в сессии пользователя):

```
lpstat -a
```

  - проверить, что принтер ассоциирован с виртуальным:

```
lpoptions -p <имя_принтера_из_команды_выше> | grep -oP 'printer-info=STAL
virtual printer`
```

  - получить имя файла CUPS-драйвера:

```
sudo lpinfo -m | grep -i <имя_производителя>
```

```
Пример вывода:

brother-HL1200-cups-en.ppd Brother HL1200 for CUPS
lsb/usr/brother/brother-HL1200-cups-en.ppd Brother HL1200 for CUPS
```

- добавить полученную информацию в файл `/etc/stal/stal-config.json`. Пример файла:

```
"printers": [
    {
        "name": "Brother HL-1200 series",
        "ppd": "brother-HL1200-cups-en.ppd"
    },
```

```
    {
        "name": "Brother HL-1500 series",
        "ppd": "brother-HL1500-cups-en.ppd"
    }
]
```

- перезапустить сервис `termidesk-stal.service`:

```
sudo systemctl restart termidesk-stal.service
```

После выполненной настройки при использовании пользователем принтера (в примере «Brother-1200») для печати будет использоваться ассоциация на нативный Linux-драйвер.

Перенаправление дисков в STAL

Диски, отмеченные для перенаправления в сессию пользователя при подключении к STAL, монтируются в файловую систему ОС по пути:

- `${HOME}/Public` по умолчанию;
- `$XDG_RUNTIME_DIR/stal/$MOUNTPOINT`, если переменная окружения `XDG_RUNTIME_STAL_REDIRECT_DIR` определена в конфигурационном файле `stal-config.json` в параметре `runtime::env`.

Путь `$XDG_RUNTIME_DIR/stal/$MOUNTPOINT` обычно соответствует `/run/user/<идентификатор_пользователя>/stal/<наименование_диска>`.

Перенаправление смарт-карт в STAL

Для работы со смарт-картами в STAL нужно установить:

- драйверы и библиотеки, определенные производителем смарт-карт;
- ПО для работы со смарт-картами.

Перенаправление веб-камер в STAL

В STAL перенаправление веб-камеры реализовано с использованием мультимедийного сервера PipeWire. Видеопоток с камеры на клиентском устройстве передаётся на сервер терминалов и предоставляется в пользовательскую сессию как источник видео PipeWire. Для работы с перенаправленной камерой приложение должно поддерживать получение видео через PipeWire.

Перенаправление и работа с веб-камерами поддерживается в STAL, однако в некоторых случаях, перечисленных ниже, потребуется дополнительная настройка:

- если STAL установлен в ОС Альт Рабочая станция с графической средой KDE Plasma: потребуется замена стандартного звукового сервера PulseAudio на PipeWire. Для этого:
  - отключить PulseAudio:

    ```
    systemctl --user disable --now pulseaudio{,.socket,-x11}
    ```

  - полностью заблокировать запуск PulseAudio:

```
systemctl --user mask pulseaudio{,.socket,-x11}
```

- запустить PipeWire и WirePlumber:

```
systemctl --user enable --now pipewire{,-pulse}.socket wireplumber
```

STAL. ЖУРНАЛИРОВАНИЕ

Журналирование в STAL

Журналы работы STAL расположены в файлах `/var/log/termidesk/stal-*.log`, например:

- `stal-kiosk.log` - события работы процесса `stal-kiosk`;
- `stal-service.log` - события работы службы `stal-service`;
- `stal-session.log` - события работы процесса `stal-session`;
- `stal-session-manager.log` - события работы службы `stal-session-manager`;
- `stal-shadow-server.log` - события работы процесса `stal-shadow-server`;
- `stal-vprint.log` - события работы процесса `stal-vprint`;
- `stal-waitx.log` - события работы процесса `stal-waitx`.

Требуется установленная служба ведения журналов `syslog-ng`.

Параметры ротации журналов STAL определены конфигурационным файлом `/etc/logrotate.d/stal`.

В случае, если в ОС не установлена служба ведения журналов `syslog-ng`, просмотр журналов выполняется командой:

```
sudo journalctl -t <служба_или_процесс>
```

Пример:

```
sudo journalctl -t stal-service
sudo journalctl -t stal-session
sudo journalctl -t stal-session-manager
sudo journalctl -t stal-waitx
```

Сбор журналов STAL для передачи в техническую поддержку

При возникновении нештатных ситуаций может понадобиться сбор всех журналов работы STAL и их отправка в техническую поддержку. Для удобства может использоваться скрипт `/opt/termidesk/stal/scripts/stal-create-report.sh`.

Для формирования файла архива с журналами нужно выполнить:

```
sudo /opt/termidesk/stal/scripts/stal-create-report.sh
```

Для формирования файла архива с журналами за определенный период времени нужно выполнить:

```
sudo /opt/termidesk/stal/scripts/stal-create-report.sh <timestamp>
```

Где параметр `<timestamp>` может принимать значения:

- `10 minutes ago` - журналы за последние 10 минут;
- `1 hour ago` - журналы за последний час;
- `2026-05-01` - журналы, начиная с указанной даты;
- `2026-05-18 09:00:00` - журналы, начиная с указанной даты и времени.

В результате выполнения команды создастся файл `/var/tmp/stal_report_YYYYMMDD_HHMI.tgz`, где `YYYY` - год, `MM` - месяц, `DD` - день, `HH` - часы, `MI` - минуты формирования файла. При обращении в техническую поддержку необходимо приложить этот архив в запрос.

В случае, если какие-то из собираемых файлов журналов пусты, после выполнения команды может отобразиться ошибка «Нет такого файла или каталога», которая не влияет на формирование итогового файла архива.

STAL. НЕШТАТНЫЕ СИТУАЦИИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

Возможные неисправности при работе со STAL и способы их устранения приведены в таблице (см. таблицу Перечень возможных нештатных ситуаций).

Таблица 205. Перечень возможных нештатных ситуаций

Индикация	Описание	Возможное решение
Ошибка: «Ошибка сервера»	Ошибка появляется при попытке соединения к STAL	Ошибка появляется при установленном пакете `xserver-xorg-legacy` и связана со значением параметра `allowed_users` в файле `/etc/X11/Xwrapper.config`. Параметру необходимо присвоить значение `anybody`. Рекомендуемое решение: установить новейшую версию STAL
При добавлении поставщика ресурсов STAL или приложения в веб-интерфейсе Termidesk VDI появляются ошибки «TypeError: 'NoneType' object is not iterable» и «Неверное имя пользователя и пароль»	Подключение к опубликованным приложениям перестало работать. Присутствует ошибка «The name ru.uveon.stal was not provided by any .service files» при запросе статуса службы `termidesk-session-agent`	Необходимо проверить журнал событий `/var/log/termidesk/stal_service.log` на наличие записей «Error from reader» и «Missing in array declaration». Наличие ошибок свидетельствует, что в файле `/etc/stal/programs.json` допущена синтаксическая ошибка. Рекомендуется также установить новейшую версию STAL

Индикация	Описание	Возможное решение
Отображается черное окно при подключении к терминальной сессии	Подключение к терминальной сессии не происходит, открывается черное окно и через секунду закрывается. Если пользователь еще не входил в ОС в графическом режиме, то в этом окне появляется надпись «Инициализация...», в домашнем каталоге пользователя создаются каталоги, но как только инициализация завершается, окно закрывается	Ошибка устранена в версии ОС Astra Linux Special Edition 1.7.5. Рекомендуется обновить ОС на версию 1.7.5 или новее и установить новейшую версию STAL
Не запускается опубликованное приложение	При подключении через STAL не происходит запуск опубликованных приложений. У подключившегося к STAL пользователя при этом может быть доступен рабочий стол и другие (неопубликованные) приложения	Необходимо проверить, установлен ли пакет `xrdp` на сервере STAL. Если он установлен, его необходимо удалить, поскольку `xrdp` занимает порт 3389, на котором работает STAL. Также возможна ситуация, когда некоторые программы не позволяют запускать другие свои копии. Поэтому необходимо проверить, было ли опубликованное приложение открыто в общей сессии того же пользователя, которая активна в данный момент. Если приложение было открыто, то нужно его закрыть и выйти (logout) из общей сессии. Для публикации некоторых из таких приложений можно использовать запуск с ключами, например, `firefox --ProfileManager` или `chromium --temp-profile`
Нет подключения при попытке получить опубликованное приложение	При попытке получить опубликованное приложение возникает черный экран, подключения нет. STAL находится в домене MS AD	Необходимо проверить журнал событий `/var/log/termidesk/stal_service.log` на наличие записи «Permission denied». Наличие записи свидетельствует, что при вводе аутентификационных данных для подключения не был соблюден регистр букв в логине пользователя. Логин пользователя должен быть указан в точности такой, какой используется на доменном сервере
При попытке соединения к терминальному серверу или опубликованному на нем приложению соединение не устанавливается	При подключении к STAL соединение не устанавливается. При подключении к опубликованному приложению STAL вместо приложения отображается черный фон	Для устранения проблемы необходимо в «Портале администратора» Termidesk VDI перейти «Рабочие места - Фонды», выбрать фонд STAL и задать ему значение политики «Аутентификация на уровне сети (RDP)»: «TLS» или «RDP»

Индикация	Описание	Возможное решение
При попытке подключения возникает ошибка «Этот сеанс будет прекращен из-за ошибки протокола. Попробуйте подключиться заново к удаленному компьютеру»	Ошибка появляется при попытке соединения к STAL через стандартную утилиту Windows `mstsc`	Необходимо проверить значение политики «Глубина цвета (RDP)» в «Портале администратора» компонента «Универсальный диспетчер»: значение политики должно быть «32 бит»
При запуске сессии воспроизводится звук, который к данной сессии не привязан	При подключении к STAL пользователю воспроизводится звук, который не был им запущен для проигрывания	Необходимо проверить наличие других активных сессий для данного пользователя (соединения могут быть закрыты), восстановить соединение и закрыть программы проигрывания звука, или завершить ненужные сессии (выполнить logout)

Невозможно подключиться доменным пользователем к терминальному серверу STAL	При попытке подключиться доменным пользователем к STAL соединение не устанавливается	Необходимо проверить значение параметра `use_fully_qualified_names` в конфигурационном файле `SSSD`-сервисов ОС `/etc/sssd/sssd.conf`. Если параметру задано значение `True`, то в конфигурационном файле «Сессионного агента» нужно присвоить значение `True` параметру `USE_USER_PRINCIPAL_NAME`.
		
		Если требуется изменение конфигурации службы `SSSD`, то после изменения необходимо:
		
		• перезапустить службу `sssd`:
		
		`sudo systemctl restart sssd`
		
		• перезапустить службу `stal-proxy`:
		
		`sudo systemctl restart stal-proxy`

Индикация	Описание	Возможное решение

Ошибка:
 	
«PAM _pam_init_handlers: no default config other»
	В журнале STAL отображается ошибка взаимодействия с модулем PAM: «PAM _pam_init_handlers: no default config other». При этом у пользователя при авторизации на STAL в «Клиенте» появляется ошибка «Невозможно пройти авторизацию на сессионном агенте»	Необходимо увеличить лимит на количество открываемых файлов (в целом на систему), для этого:
		
		• изменить файл `/etc/sysctl.conf`, добавив в конце строку:
		
		`fs.file-max = 50000000`
		
		• сохранить изменения в файле;
		• применить конфигурацию командой:
		
		`sudo sysctl -p`
		
		• изменить файл `/etc/pam.d/common-session`, добавив строку:
		
		`session required pam_limits.so`
		
		• сохранить изменения в файле;
		• перезагрузить сервер STAL

При подключении к сессии отображается черный экран вместо окна ввода логина и пароля пользователя	При попытке подключения к терминальной сессии не отображается окно ввода логина и пароля пользователя	Необходимо изменить значение политики «Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)» в «Портале администратора» компонента «Универсальный диспетчер»: значение политики должно быть «Включен». После этого выполнить перезапуск служб STAL: `sudo systemctl restart stal-proxy termidesk-stal`
При длительном вводе логина и пароля на экране ввода пользовательских данных STAL сессия закрывается	Поведение проявляется, если политика «Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)» в фонде отключена. При попытке подключения к терминальному серверу и длительном вводе логина и пароля на экране ввода пользовательских данных STAL сессия закрывается	Необходимо в конфигурационном файле «Сессионного агента» увеличить время ожидания в параметре `STAL_CONNECT_RDP_TTL`

ТЕРМИНЫ

Виртуальное рабочее место

Развернутая на ВМ ОС с установленным «Агентом виртуального рабочего места» и необходимым прикладным ПО. Подключение происходит через протоколы удаленного доступа

Рабочее место

Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа. Под РМ подразумеваются как виртуальное рабочее место, так и терминальный доступ или доступ к опубликованным на терминальном сервере приложениям

Гостевая ОС

ОС, функционирующая на ВМ

Поставщик ресурсов

ОС, платформа виртуализации или терминальный сервер (MS RDS/STAL), предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов РМ

Протокол доставки

Поддерживаемый в Termidesk VDI протокол удаленного доступа к РМ

Компонент «Сессионный агент»

Компонент Termidesk VDI. Устанавливается на терминальный сервер (MS RDS/STAL), активирует возможность множественного доступа пользователей к удаленным рабочим столам и приложениям

Компонент «Универсальный диспетчер»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им РМ и контроля доставки РМ. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-vdi.service`

Лидер сеанса (session leader)

Процесс, идентификатор сеанса (SID) которого равен его собственному идентификатору (PID). Отвечает за создание сеанса и группировку связанных процессов

Фонд рабочих мест

Совокупность подготовленных РМ для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей

Компонент «Сервер терминалов Astra Linux»

Компонент Termidesk VDI. Также: STAL. Обеспечивает подключение пользовательских рабочих станций к РМ с ОС Astra Linux Special Edition через сеанс удаленного терминала

СОКРАЩЕНИЯ

ВМ	Виртуальная машина
БД	База данных
ЗПС	Замкнутая программная среда
ОС	Операционная система
ПО	Программное обеспечение

РМ	Рабочее место
ЭЦП	Электронная цифровая подпись
API	Application Programming Interface (интерфейс прикладного программирования)
CUPS	Common Unix Printing System (система печати Unix)
IP	Internet Protocol (межсетевой протокол)
JSON	JavaScript Object Notation (стандартный текстовый формат для структурированных данных)
MS AD	Microsoft Active Directory (службы каталогов Microsoft)
MS RDS	Microsoft Remote Desktop Services (службы удаленного рабочего стола Microsoft)
OIDC	OpenID Connect (протокол аутентификации, построенный поверх стандарта OAuth 2.0)
PAM	Pluggable Authentication Module (подключаемый модуль аутентификации)
PCL	Page Description Language (язык описания страниц)
PDF	Portable Document Format (открытый формат электронных документов)
PKINIT	Public Key Cryptography for Initial Authentication (механизм Kerberos, позволяющий использовать сертификаты X.509)
PS	PostScript (язык программирования и описания графических документов)
RDP	Remote Desktop Protocol (протокол удаленного рабочего стола)
SID	Session ID (сессионный идентификатор)
SPICE	Simple Protocol for Independent Computing Environments (простой протокол для независимой вычислительной среды)
SSH	Secure Shell Protocol (протокол защищенной передачи информации)
SSSD	System Security Services Daemon (системная служба, управляющая доступом к удаленным каталогам и механизмам аутентификации)
STAL	Terminal Server Astra Linux (компонент «Сервер терминалов Astra Linux»)
TCP	Transmission Control Protocol (протокол управления передачей)
TERA	Termidesk Remote Access protocol (протокол удаленного доступа разработкиООО «УВЕОН»)
TLS	Transport Layer Security (протокол защиты транспортного уровня)
UID	Unique Identifier (уникальный идентификатор)
X11	Базовый протокол и подсистема для создания графического интерфейса пользователя
XDG	Cross-Desktop Group (проект и набор спецификаций для графических приложений в Linux и Unix)

XPS XML Paper Specification (открытый графический формат фиксированной разметки на базе XML)

СЛЕТ.10001-01 90 08. РУКОВОДСТВО АДМИНИСТРАТОРА. УСТАНОВКА И НАСТРОЙКА «АГРЕГАТОРА»

ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ

Назначение документа

Настоящий документ является восьмой частью руководства администратора на программный комплекс «Диспетчер подключений виртуальных рабочих мест Termidesk» (далее - Termidesk VDI, Termidesk VDI). Документ определяет назначение, установку и настройку «Агрегатора» и предназначен для администраторов системы и сети.

Типографские соглашения

Приняты следующие типографские соглашения:

- `моноширинный шрифт` – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk VDI, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

АГРЕГАТОР. ОБЩИЕ СВЕДЕНИЯ

Назначение «Агрегатора»

«Агрегатор» - это тип роли, доступный при установке Termidesk VDI. «Агрегатор» является единой точкой входа для получения ресурсов пользователями Termidesk VDI и предоставляет им объединенный список приложений с нескольких установок Termidesk VDI, с возможностью объединения одинаковых приложений или виртуальных рабочих мест (ВРМ).

«Агрегатор» должен быть установлен отдельно от узлов с ролями «Портал администратора», «Портал пользователя».

«Агрегатор» может быть установлен со следующими типами веб-интерфейса:

- «Агрегатор администратора» - веб-интерфейс управления «Агрегатором»;
- «Агрегатор пользователя» - веб-интерфейс пользователя для получения ресурсов, предоставляемых Агрегатором;
- «Агрегатор универсальный» - веб-интерфейс, предоставляющий функции обоих вариантов.

Функции «Агрегатора»:

- объединение установки основных узлов Termidesk VDI в виде ферм поставщиков ресурсов;
- дедупликация (объединение, устранение дубликатов) приложений или ВРМ на фермах

поставщиков ресурсов;

- создание единого списка ресурсов (приложений, BPM) для пользователя с нескольких ферм поставщиков ресурсов.

Требования к аппаратному и программному обеспечению

Минимальные аппаратные требования к узлу приведены в таблице Минимальные аппаратные требования.

Комплексная установка рекомендуется для использования в тестовой среде при количестве не более 50 одновременных подключений. Рекомендуемые аппаратные требования для данного варианта установки не приводятся.

Таблица 206. Минимальные аппаратные требования

CPU, шт	RAM, ГБ	HDD, ГБ	Сеть, Мбит/с
Узел «Агрегатора» в комплексном варианте установки			
4	4	80	100
Узел «Агрегатора» с ролью «Агрегатор универсальный»			
4	4	80	100
Узел «Агрегатора» с ролью «Агрегатор администратора»			
4	4	60	100
Узел «Агрегатора» с ролью «Агрегатор пользователя»			
4	4	80	100
Узел «Агрегатора» с ролью «Менеджер рабочих мест»			
4	4	60	100
Узел СУБД PostgreSQL			
4	4	60	100
Узел брокера сообщений RabbitMQ			
2	4	60	100
Узел «Шлюза» (Termidesk Connect с лицензией Termidesk Connect Basic)			
2	12	50	100
Узел балансировщика нагрузки (Termidesk Connect с лицензией Termidesk Connect)			
2	12	50	100

Рекомендуемые аппаратные требования к узлу приведены в таблице Рекомендуемые аппаратные требования.

В производственной среде следует использовать конфигурацию, соответствующую рекомендуемым аппаратным требованиям, исходя из расчета:

- один узел «Универсального диспетчера» на каждые 1000 одновременных подключений;
- один узел «Шлюза» или балансировщика нагрузки Termidesk Connect на каждые 2000 одновременных подключений. Подробные сведения об аппаратных требованиях Termidesk Connect доступны по ссылке: Требования к аппаратному и программному обеспечению

Для узлов СУБД PostgreSQL и брокера сообщений RabbitMQ приведены рекомендуемые аппаратные требования для указанного количества одновременных подключений. При выборе аппаратной конфигурации данных узлов также необходимо учитывать требования, приведенные в документации соответствующих компонентов.

Таблица 207. Рекомендуемые аппаратные требования

CPU, шт	RAM, ГБ	HDD, ГБ	Сеть, Мбит/с
Узел «Агрегатора» с ролью «Агрегатор универсальный»			
8	8	80	100
Узел «Агрегатора» с ролью «Агрегатор администратора»			
4	4	60	100
Узел «Агрегатора» с ролью «Агрегатор пользователя»			
8	8	80	100
Узел «Агрегатора» с ролью «Менеджер рабочих мест»			
4	4	60	100
Узел СУБД PostgreSQL			
8	8	100	100
Узел брокера сообщений RabbitMQ			
4	4	60	100
Узел «Шлюза» (Termidesk Connect с лицензией Termidesk Connect Basic)			
2	12	50	20 000
Узел балансировщика нагрузки (Termidesk Connect с лицензией Termidesk Connect)			
2	12	50	20 000

В среде функционирования должны быть предварительно установлены:

- ОС Astra Linux Special Edition версии 1.8 (1.8.1, 1.8.2, 1.8.3, 1.8.4, 1.8.5, 1.8.6);
- СУБД PostgreSQL версии 15 из состава репозитория ОС Astra Linux Special Edition версии 1.8. Из внешних по отношению к ОС Astra Linux Special Edition версии 1.8 СУБД поддерживается СУБД PostgreSQL версии 14 и выше;
- брокер сообщений RabbitMQ из состава репозитория ОС Astra Linux Special Edition.

ОС Astra Linux Special Edition версии 1.8 должна быть установлена из `iso`-образа, доступного в личном кабинете на портале Astra Linux: https://lk.astra.ru/. Работа Termidesk VDI на преднастроенных образах ОС не гарантируется.

Требования к настройкам инфраструктуры

Требования к синхронизации времени

В сетевой инфраструктуре должен быть настроен NTP-сервер, обеспечивающий синхронизацию времени для компонентов Termidesk VDI.

Требования к службам DNS и DHCP

В сетевой инфраструктуре должны быть развернуты и исправно функционировать службы доменных имен (DNS) и автоматического назначения сетевых параметров (DHCP) в необходимых сегментах сети.

Требования к серверам каталогов

Серверы каталогов должны удовлетворять следующим требованиям:

- сервер каталогов должен размещаться в том же сегменте локальной сети, где развернут «Агрегатор». Если выполнение требования невозможно и сервер каталогов находится в другом сегменте, то необходимо обеспечить маршрутизацию между этими сегментами;
- при использовании Microsoft Active Directory Domain Service (MS AD) необходимо создать сервисную учетную запись для взаимодействия Termidesk VDI с контроллером домена (КД). Допускается использование учетной записи администратора домена;
- при использовании MS AD рекомендуется создавать отдельные организационные подразделения (OU) для пользователей рабочих мест (РМ) и для учетных записей типа «Компьютер» для самих РМ. Права на OU для компьютеров должны быть либо у созданной сервисной учетной записи, либо у отдельной созданной учетной записи, допускается также использовать учетную запись администратора домена.

АГРЕГАТОР. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ

Получение пакетов установки в ОС Astra Linux Special Edition

Дистрибутив представлен бинарным файлом пакета ПО в `deb`-формате. Установка в ОС Astra Linux Special Edition производится из локального репозитория, распространяемого в формате `iso`-образа.

Получить `iso`-образ можно двумя способами:

- заполнив запрос через сайт Termidesk VDI: https://termidesk.ru/support/#request-support;
- через личный кабинет:https://lk.astra.ru/.

Для подключения локального репозитория Termidesk VDI на узле, где предполагается установка, нужно:

- скопировать в домашний каталог пользователя образ диска `termidesk-<версия>.iso`;
- подключить образ диска к файловой системе в каталог `/mnt`:

```
sudo mount -o loop termidesk-<версия>.iso /mnt
```

где:

`-o loop` - параметры для привязки петлевого устройства (`/dev/loop`) к файлу `termidesk-<версия>.iso`, устройство затем монтируется в указанный каталог `/mnt`;

- скопировать содержимое каталога `repos` подключенного образа диска в каталог `/var` локальной файловой системы:

```
sudo cp -Rp /mnt/repos /var
```

где:

`-Rp` - ключ для рекурсивного копирования подкаталогов и файлов с сохранением исходных свойств;

- отключить подключенный ранее образ диска от узла:

```
sudo umount /mnt
```

- установить пакет `lsb-release`:

```
sudo apt install -y lsb-release
```

- добавить локальный репозиторий Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list` через командный интерпретатор `sh`:
  - выяснить установленную версию ОС:

    ```
    sudo cat /etc/astra_version
    ```

  - определить актуальное имя каталога с пакетами в `/var/repos`;
  - указать в файле конфигурации APT корректное (фактическое) имя каталога:

    ```
    sudo sh -c 'echo "deb file:/var/repos/astra 1.8_x86-64 non-free" >
    /etc/apt/sources.list.d/termidesk_local.list'
    ```

    где:

    `-c` - ключ для чтения команд из вводимой строки (стандартный ввод);

    `echo` - команда вывода текста, совместно с символом «>» используется для перенаправления строки в файл;

    `deb file:/var/repos/astra 1.8_x86-64 non-free` - добавляемый репозиторий с вложенной командой получения версии ОС;

    Приведенный пример команды актуален для установки основных компонентов Termidesk, пакеты которых расположены в каталоге `1.8_x86-64`.

- для корректной установки компонентов TERA потребуется корректно подключить дополнительные репозитории и настроить их приоритет:
  - для версий ОС Astra Linux Special Edition меньше или равных 1.7.6, а также для версий 1.8.X:
    - подключить два репозитория:

      ```
      sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
      non-free" > /etc/apt/sources.list.d/termidesk_local.list'
      sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
      /dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
      ```

    - добавить повышенный приоритет для репозитория с требуемой версией ОС

(значение `$(cat /etc/astra_version)` может подходить не для всех репозиториев, т.к. версия может указываться без точек - в этом случае нужно вручную указать корректную версию):

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000
EOF"
```

- для версий ОС Astra Linux Special Edition 1.7.7 и 1.7.8:
  - подключить три репозитория:

```
sudo sh -c 'echo "deb file:/var/repos/astra 1.7.6 non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
/dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

  - настроить два приоритета:

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=1.7.6
Pin-Priority: 950

Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000

EOF"
```

- выполнить поиск ключа репозитория Termidesk VDI `GPG-KEY-PUBLIC` и добавить его:

```
sudo cat /var/repos/astra/GPG-KEY-PUBLIC | sudo gpg --dearmour -o
/etc/apt/trusted.gpg.d/termidesk.gpg
```

- убедиться, что ключ `release@uveon.ru` был успешно добавлен:

```
apt-key list
```

В случае, если ключ не отображен в выводе команды, необходимо убедиться, что ключ `GPG-KEY-PUBLIC` существует:

```
cat /var/repos/astra/GPG-KEY-PUBLIC
```

Если ключ все же существует, следует проверить правильность выполнения шагов по добавлению репозитория Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list`.

При успешном выполнении всех шагов команда выведет содержимое ключа в формате Base64.

В зависимости от используемой версии ОС команды добавления ключа репозитория Termidesk VDI могут отличаться. Если для ОС Astra Linux Special Edition 1.8 ключ репозитория был добавлен командой, применимой к другой версии ОС, то для исправления нужно:

- узнать идентификатор добавленного ключа репозитория:

```
apt-key list
```

- удалить ключ:

```
apt-key --keyring /etc/apt/trusted.gpg del 4E1632CC
```

где `4E1632CC` - последние 8 символов идентификатора ключа;

- вновь добавить ключ репозитория.

- обновить данные пакетного менеджера:

```
sudo apt update
```

- проверить настройку приоритетов репозиториев:

```
apt-cache policy
```

Команду `sudo apt update` необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.

АГРЕГАТОР. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ

Подготовка среды функционирования для «Агрегатора»

Перед установкой «Агрегатора» должна быть предварительно подготовлена среда функционирования узла:

- установлена и настроена система управления базами данных (СУБД) PostgreSQL;
- установлен и настроен брокер сообщений RabbitMQ.

В Termidesk VDI версии 6.1 в экспериментальном режиме поддерживается

установка «Брокера сообщений TermideskMQ»:

- выбор «Брокера сообщений TermideskMQ» производится при установке пакета `termidesk-vdi`;
- одновременное использование RabbitMQ и «Брокера сообщений TermideskMQ» в рамках одной фермы не поддерживается. Рекомендуется удалить RabbitMQ или отключить службу `rabbitmq-server`, если будет использоваться «Брокер сообщений TermideskMQ».

Подготовка среды функционирования осуществляется аналогично разделу **Подготовка среды функционирования** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса».

Узел «Агрегатора» не должен использовать экземпляры базы данных (БД) и брокера сообщений, предназначенные для других компонентов Termidesk VDI. БД и брокер сообщений RabbitMQ могут быть установлены локально на узел «Агрегатора».

Для корректной регистрации событий подключения пользователя к ресурсу фермы Termidesk VDI необходимо на всех узлах «Универсального диспетчера», ферма которого подключается к порталу «Агрегатор», перейти «Системные параметры - Системные настройки - Безопасность» и включить параметр «Использовать анонсируемый IP клиента». В противном случае при подключении пользователей к ресурсам ферм Termidesk VDI в журналах «Универсального диспетчера» будет отображен IP-адрес портала «Агрегатор», а не IP-адреса подключившихся пользователей.

ОС Astra Linux Special Edition

Автоматизированная установка «Агрегатора»

Перед установкой «Агрегатора» должна быть подготовлена среда функционирования (см. подраздел **Подготовка среды функционирования**).

Перед установкой следует убедиться, что в БД отсутствуют записи (необходимо использовать чистую БД).

Для автоматизированной установки нужно:

- создать файл `/etc/default/termidesk-vdi.local`:

```
sudo touch /etc/default/termidesk-vdi.local
```

- указать в созданном файле каталоги расположения конфигурационного файла и шаблонов настройки регистрации событий и журналирования:

```
ETC='/etc/opt/termidesk-vdi'
TEMPLATES_DIR='/etc/opt/termidesk-vdi/templates'
```

- создать каталог `/etc/opt/termidesk-vdi`:

```
sudo mkdir /etc/opt/termidesk-vdi
```

- создать файл `/etc/opt/termidesk-vdi/termidesk.conf`:

```
sudo touch /etc/opt/termidesk-vdi/termidesk.conf
```

- отредактировать созданный файл по примеру ниже;
- выполнить:

> Переменная `NON_INTERACTIVE_INSTALLATION` используется для «тихой» установки без отображения дополнительных диалоговых окон. Переменная может быть передана другим способом, но после завершения установки должна быть отключена.
>
> При использовании этой переменной со значением `yes` убедитесь, что в конфигурационном файле `termidesk.conf` присутствуют **все** параметры, которые имеются в файле конфигурации дистрибутива (`termidesk.conf.dist`). В противном случае установка пакета завершится ошибкой. Подробности о недостающих параметрах можно найти в файле `/var/log/syslog`.

```
sudo NON_INTERACTIVE_INSTALLATION='yes' apt install -y termidesk-vdi
```

> Описание параметров файла приведено в подразделе **Конфигурационный файл `termidesk.conf`**.

Пример файла `/etc/opt/termidesk-vdi/termidesk.conf`:

- используются значения по умолчанию для имени пользователи и пароля;
- пароли и имена хранятся в конфигурационном файле (хранилище не используется);
- используется незащищенное подключение к БД и RabbitMQ .

```
TERMIDESK_FARM_MODE='AGGREGATOR'
NODE_ROLES='ADMIN,USER,CELERYMAN'
NODE_NAME=aggregator-portal-celery_0050568fef1a
SECRETS_STORAGE_METHOD='config'
DB_CLUSTER_MODE='single'
DBHOST='localhost'
DBPORT='5432'
DBSSL='Disable'
DBNAME='termidesk'
DBUSER='termideskdb'
DBPASS='ksedimret'
DB_CONN_MAX_AGE=600
CELERY_DB_REUSE_MAX=1000
DB_CONN_TIMEOUT=10
RABBITMQ_URL1='amqp://termidesk:ksedimret@localhost:5672/termidesk'
```

```
RABBITMQ_URL2=
RABBITMQ_URL3=
RABBITMQ_SSL='Disable'
DJANGO_SECRET_KEY='t6ajnMB3KMyfMEffz8SYlZMzCsGP0dENc2wFXYPAfgc='
LOG_LEVEL='INFO'
LOG_ADDRESS='/dev/log'
LOG_FACILITY='local3'
LOG_DIR='/var/log/termidesk'
LOG_OWNER='termidesk'
LOG_GROUP='adm'
LOG_PERM='0440'
LOG_DEEP='14'
FLUENTD_CACHE=15
FLUENTD_TABLE='logs'
FLUENTD_LOGGER_TIMEOUT=5
HEALTH_CHECK_ACCESS_KEY='7e3a48572334c022ce774668047b4b00d44a7129e7857ae0a068f00832
aee499'
METRICS_ACCESS_KEY='0f77b6a57b491e0aa4cd7a78d3d068386a5a0b6832c25b6b0c2bdcfbc079e92
a'
EULA_ACCEPTED='YES'
AGGREGATOR_IMAGE_CACHE_LIFETIME_HOURS=672
AGGREGATOR_HTTP_TIMEOUT=10
```

После установки указанные в открытом виде пароли можно привести к преобразованным значениям через утилиту `/opt/termidesk/bin/scramble`.

После установки необходимо убедиться, что переменная `NON_INTERACTIVE_INSTALLATION` отключена (не задана в окружении или имеет значение, отличное от `yes`).

После установки нужно:

- скорректировать файл конфигурации веб-сервера `/etc/apache2/apache2.conf`. Для этого нужно найти и раскомментировать строку с параметром `AstraMode`, далее присвоить данному параметру значение `off`, точно соблюдая отступы и пробелы в файле:

```
# Astra security mode
#
AstraMode off
```

- затем перезапустить веб-сервер:

```
sudo systemctl restart apache2
```

- задать ключ для подписи JWT-токена для взаимодействия с узлами фермы Termidesk VDI. Ключ может быть задан через файл `termidesk.conf` (параметр `AGGREGATOR_JWT_SSL_KEY`) или через утилиту `termidesk-config`;
- заполнить файл сопоставления `mapping.yaml` и указать его в `termidesk.conf` (параметр `AGGREGATOR_YAML_FILE`).

После установки параметры «Агрегатора» могут быть изменены:

- через файл `termidesk.conf`;
- или через утилиту `termidesk-config`.

Неавтоматизированная установка «Агрегатора»

Перед установкой «Агрегатора» должна быть подготовлена среда функционирования (см. подраздел **Подготовка среды функционирования**).

Перед установкой следует убедиться, что в БД отсутствуют записи (необходимо использовать чистую БД).

Установка производится аналогично подразделу **Неавтоматизированная комплексная установка Termidesk VDI** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса».

Возможность установки веб-порталов «Агрегатор администратора» и «Агрегатор пользователя» зависит от типа редакции Termidesk VDI.

Установка веб-порталов «Агрегатор администратора» и/или «Агрегатор пользователя» должна производиться на узле, отличном от «Портала администратора» и/или «Портала пользователя» фермы Termidesk VDI.

Начиная с Termidesk VDI версии 6.1 компонент «Шлюз» (пакет `termidesk-gateway`) более не входит в поставку. Для использования «Шлюза» следует установить программу для электронной вычислительной машины «Балансировщик нагрузки Термидеск Коннект» (Termidesk Connect).

В процессе установки необходимо отметить следующие пункты:

Описание относится к комплексной установке: все указанные роли устанавливаются на одном узле.

- при выборе режима работы ПО: «Агрегатор»;
- при выборе ролей:
  - «Портал администратора». После установки будет запущена служба `termidesk-vdi`;
  - и (или) «Портал пользователя». После установки будет запущена служба `termidesk-vdi`;
- «Менеджер рабочих мест». После установки будут запущены службы `termidesk-celery-beat`, `termidesk-celery-worker`.

После установки нужно:

- скорректировать файл конфигурации веб-сервера `/etc/apache2/apache2.conf`. Для этого нужно найти и раскомментировать строку с параметром `AstraMode`, далее присвоить данному параметру значение `off`, точно соблюдая отступы и пробелы в файле:

```
# Astra security mode
#
AstraMode off
```

- затем перезапустить веб-сервер:

```
sudo systemctl restart apache2
```

- задать ключ для подписи JWT-токена для взаимодействия с узлами фермы Termidesk VDI. Ключ может быть задан через файл `termidesk.conf` (параметр `AGGREGATOR_JWT_SSL_KEY`) или через утилиту `termidesk-config`;
- заполнить файл сопоставления `mapping.yaml` и указать его в `termidesk.conf` (параметр `AGGREGATOR_YAML_FILE`).

После установки параметры «Агрегатора» могут быть изменены:

- через файл `termidesk.conf`;
- или через утилиту `termidesk-config`.

Минимальная распределенная установка «Агрегатора»

Основные принципы минимальной распределенной установки

В Termidesk VDI предусмотрена распределенная установка компонентов на отдельные серверы или ВМ.

Описание применимо к ферме «Агрегатора».

Реализация отказоустойчивости инфраструктурных сервисов выполняется организацией в соответствии с требованиями к инфраструктуре.

При использовании внешней по отношению к Termidesk VDI СУБД, следует установить брокер сообщений RabbitMQ на узел «Менеджера рабочих мест» или на отдельный узел.

Начиная с Termidesk VDI версии 6.1 компонент «Шлюз» (пакет `termidesk-gateway`) не входит в основную поставку. Для замены «Шлюза» следует использовать программу для электронной вычислительной машины «Балансировщик нагрузки Термидеск Коннект» (Termidesk Connect).

Инструкции по установке и настройке доступны по ссылкам: Инструкция по настройке Шлюза для Termidesk VDI (первый способ), Инструкция по настройке Шлюза для Termidesk VDI (второй способ, единая точка входа Termidesk VDI).

В минимальном распределенном варианте устанавливаются:

- «Агрегатор» (служба `termidesk-vdi`);
- «Менеджер рабочих мест» (службы `termidesk-celery-beat`, `termidesk-celery-worker`).

Перечень условий для минимальной распределенной установки:

- брокер сообщений RabbitMQ устанавливается на одном узле с СУБД (в общем случае этот компонент может устанавливаться на отдельный узел, но в рамках настоящей процедуры данный вариант не рассматривается);
- на всех узлах, предназначенных для установки компонентов, настроены статические IP-адреса;
- на всех узлах настроена синхронизация времени от единого источника.

Упрощенная общая схема при минимальной распределенной установке Termidesk VDI приведена на рисунке (см. рисунок Схема минимальной распределенной установки).

Схема минимальной распределенной установки с Termidesk Connect приведена на рисунке (см. рисунок Схема минимальной распределенной установки при наличии лицензии Termidesk Connect).

Особенности:

- для реализации функционала «Шлюза» используется лицензия Termidesk Connect Basic;
- для реализации функционала балансировщика используется лицензия Termidesk Connect. При отсутствии лицензии допускается использование сторонних балансировщиков нагрузки.

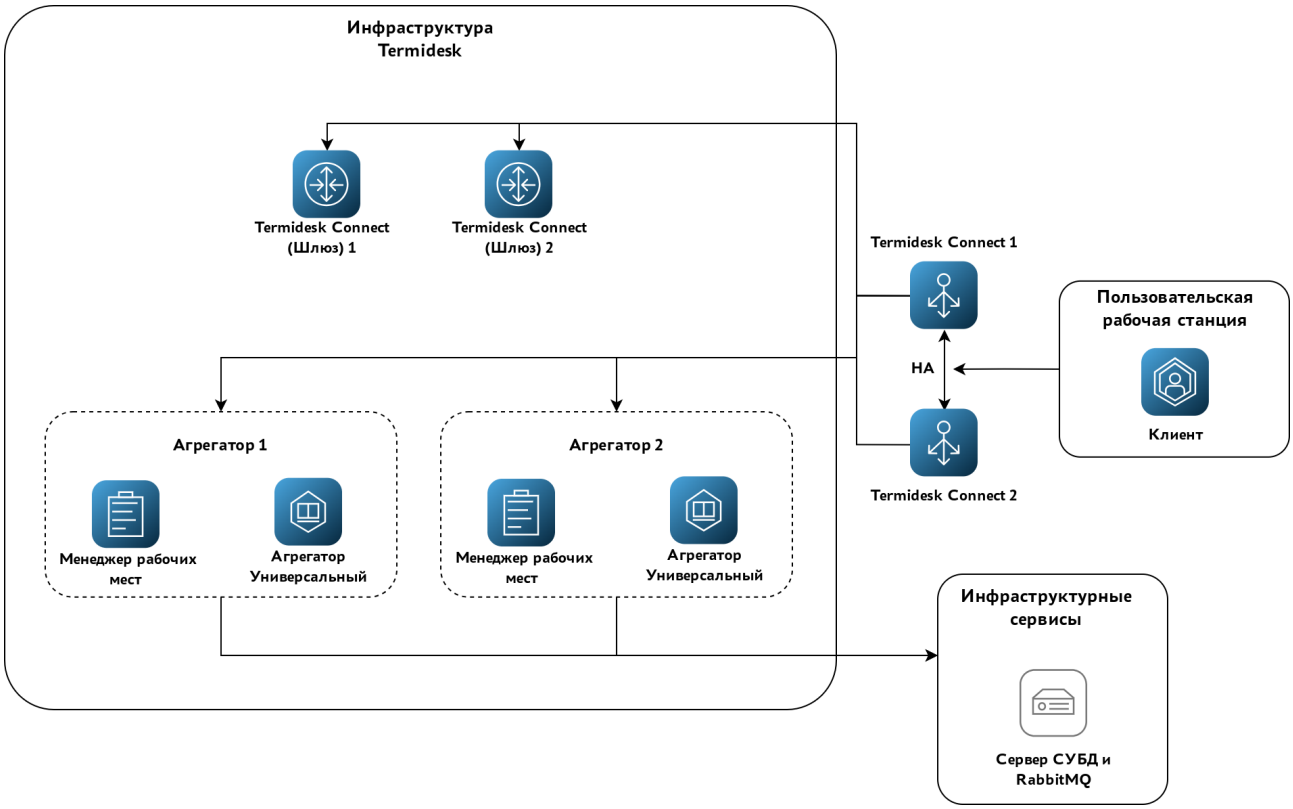


Рисунок 128. Схема минимальной распределенной установки

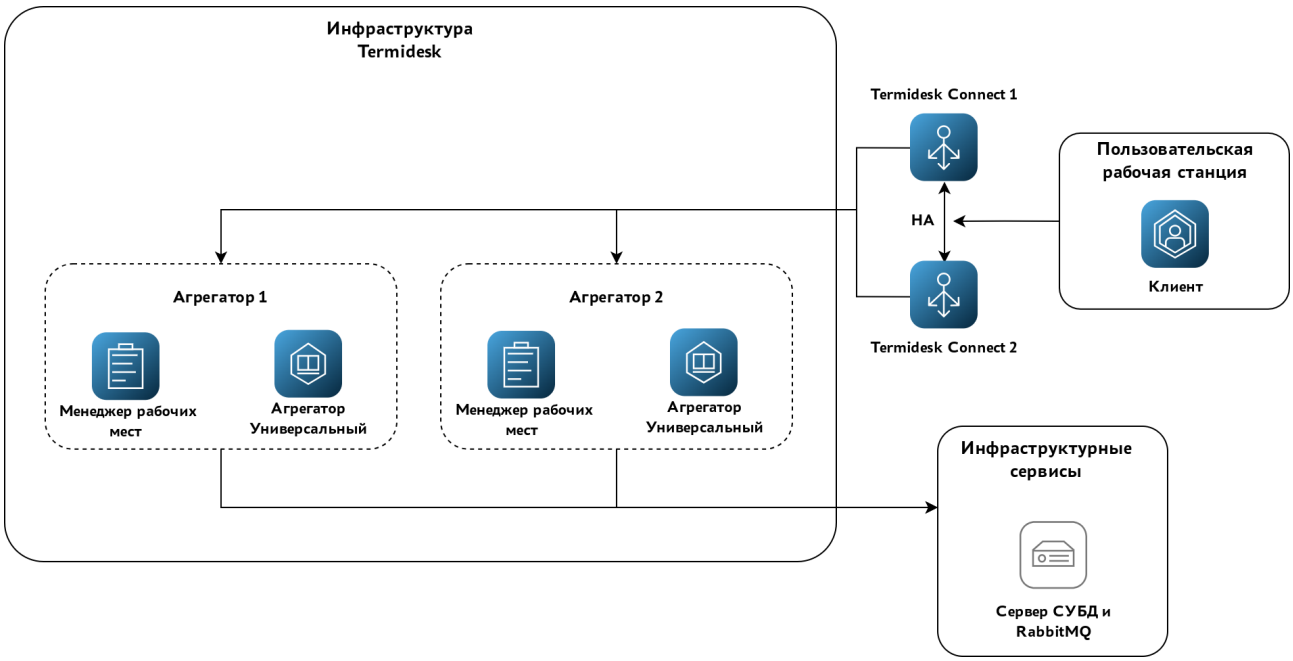


Рисунок 129. Схема минимальной распределенной установки при наличии лицензии Termidesk Connect

Перечень обозначенных на схеме компонентов приведен в таблице (см. таблицу Перечень компонентов схемы минимальной распределенной установки).

Таблица 208. Перечень компонентов схемы минимальной распределенной установки

Компонент	FQDN	Подпись на схеме
«Агрегатор» №1 с ролью «Агрегатор универсальный»	`aggr1termidesk.local`	«Агрегатор 1»
«Агрегатор» №2 с ролью «Агрегатор универсальный»	`aggr2.termidesk.local`	«Агрегатор 2»
Termidesk Connect (лицензия «Termidesk Connect Basic») №1	`tdc-gw1.termidesk.local`	«Termidesk Connect (Шлюз) 1»
Termidesk Connect (лицензия «Termidesk Connect Basic») №2	`tdc-gw2.termidesk.local`	«Termidesk Connect (Шлюз) 2»
«Менеджер рабочих мест» №1	`tsk1.termidesk.local`	«Менеджер рабочих мест 1»
«Менеджер рабочих мест» №2	`tsk2.termidesk.local`	«Менеджер рабочих мест 2»
Termidesk Connect №1	`tdc-lb1.termidesk.local`	«Termidesk Connect 1»
Termidesk Connect №2	`tdc-lb2.termidesk.local`	«Termidesk Connect 2»
База данных с брокером сообщений RabbitMQ	`db.termidesk.local`	«Сервер СУБД и RabbitMQ»

Минимальная распределенная установка проводится в следующей последовательности:

- на одном узле устанавливаются СУБД и RabbitMQ. При установке следует учесть, что в БД должны отсутствовать записи (необходимо использовать чистую БД);
- устанавливается первый (эталонный) узел с «Агрегатором». При установке необходимо выбрать роль «Агрегатор универсальный» (роль активируется при одновременном выборе ролей «Агрегатор администратора» и «Агрегатор пользователя» в диалоговом окне псевдографического интерфейса инсталлятора) и «Менеджер рабочих мест»;

Настройки первого узла с «Агрегатором» будут использоваться как эталонные для других узлов.

Нужно скопировать каталог `/etc/opt/termidesk-vdi` вместе с его содержимым на другие узлы «Агрегатора» и «Менеджера рабочих мест».

- устанавливаются остальные «Агрегаторы» с копированием файлов, указанных выше, с эталонного узла;
- устанавливаются шлюзы.

Заключительным этапом устанавливаются и настраиваются «Балансировщики нагрузки».

Установка и настройка СУБД PostgreSQL

Процесс установки брокера сообщений RabbitMQ не отличается от процесса, описанного в разделе **Подготовка среды функционирования**. Установка и настройка СУБД PostgreSQL осуществляется согласно выбранной версии.

Для завершения настройки нужно:

- отредактировать файл `/etc/rabbitmq/rabbitmq-env.conf`, приведя его к виду:

```
# Defaults to rabbit. This can be useful if you want to run more than one node
# per machine - RABBITMQ_NODENAME should be unique per erlang-node-and-machine
# combination. See the clustering on a single machine guide for details:
# http://www.rabbitmq.com/clustering.html#single-machine
#NODENAME=rabbit

# By default RabbitMQ will bind to all interfaces, on IPv4 and IPv6 if
# available. Set this if you only want to bind to one network interface or#
# address family.
NODE_IP_ADDRESS=0.0.0.0
# Defaults to 5672.
NODE_PORT=5672
```

- сохранить файл и перезапустить службу `rabbitmq-server`:

```
sudo systemctl restart rabbitmq-server
```

Установка первого узла с «Агрегатором»

Процесс установки первого узла с «Агрегатором» аналогичен комплексной установке. В процессе установки следует выбрать роли: «Агрегатор администратора (AGGR_ADM)», «Агрегатор пользователя (AGGR_USR)» и «Менеджер рабочих мест (CELERYMAN)».

После установки передать каталог `/etc/opt/termidesk-vdi` на остальные узлы «Агрегатора»:

```
sudo scp -r /etc/opt/termidesk-vdi localuser@ipaddr_or_fqdn_host:/home/user/
```

где:

`-r` - ключ для рекурсивной (со вложенными каталогами) передачи;

`localuser` - имя пользователя целевого узла;

`ipaddr_or_fqdn_host` - IP-адрес или FQDN целевого узла;

`/home/user` - путь, куда будет скопирован каталог.

Перед началом установки остальных узлов «Агрегатора» необходимо переместить скопированный ранее каталог `termidesk-vdi` в каталог `/etc/opt/`:

```
sudo mv /home/user/termidesk-vdi /etc/opt/
```

Установить второй узел с «Агрегатором» по аналогии с первым, не меняя параметры в диалогах подключения к СУБД и заполнения информации о подключении к RabbitMQ.

Установка шлюзов

Начиная с Termidesk VDI версии 6.1 функционал «Шлюза» реализуется через продукт Termidesk Connect. Подробные сведения приведены в документации Termidesk Connect (доступ по ссылке: https://termidesk.ru/docs/).

Установка «Балансировщиков нагрузки»

Подробные сведения по установке «Балансировщика нагрузки» приведены в документации Termidesk Connect (доступ по ссылке: https://termidesk.ru/docs/).

При отсутствии полной лицензии на Termidesk Connect допускается использование сторонних балансировщиков нагрузки.

Действия после минимальной распределенной установки

Настройка «Балансировщика нагрузки» приведена в документации Termidesk Connect (доступ по ссылке: https://termidesk.ru/docs/).

После установки нужно задать ключ для подписи JWT-токена для взаимодействия с узлами фермы Termidesk VDI. Ключ может быть задан через файл `termidesk.conf` (параметр `AGGREGATOR_JWT_SSL_KEY`) или через утилиту `termidesk-config`.

После установки параметры «Агрегатора» могут быть изменены:

- через файл `termidesk.conf`;
- или через утилиту `termidesk-config`.

Стандартная распределенная установка «Агрегатора»

Основные принципы стандартной распределенной установки

В Termidesk VDI предусмотрена распределенная установка компонентов на отдельные серверы или ВМ.

Описание применимо к ферме «Агрегатора».

Реализация отказоустойчивости инфраструктурных сервисов выполняется организацией в соответствии с требованиями к инфраструктуре.

> При использовании внешней по отношению к Termidesk VDI СУБД, следует установить брокер сообщений RabbitMQ на узел «Менеджера рабочих мест» или на отдельный узел.
>
> Начиная с Termidesk VDI версии 6.1, компонент «Шлюз» (пакет `termidesk-gateway`) не входит в основную поставку. Для замены «Шлюза» следует использовать программу для электронной вычислительной машины «Балансировщик нагрузки Термидеск Коннект» (Termidesk Connect).
>
> Инструкции по установке и настройке доступны по ссылкам: Инструкция по настройке Шлюза для Termidesk VDI (первый способ), Инструкция по настройке Шлюза для Termidesk VDI (второй способ, единая точка входа Termidesk VDI).

В стандартном распределенном варианте устанавливаются:

- «Агрегатор» (служба `termidesk-vdi`);
- «Менеджер рабочих мест» (службы `termidesk-celery-beat`, `termidesk-celery-worker`).

Перечень условий для стандартной распределенной установки:

- брокер сообщений RabbitMQ устанавливается на одном узле с СУБД (в общем случае этот компонент может устанавливаться на отдельный узел, но в рамках настоящей процедуры данный вариант не рассматривается);
- на всех узлах, предназначенных для установки компонентов, настроены статические IP-адреса;
- на всех узлах настроена синхронизация времени от единого источника.

Упрощенная общая схема при стандартной распределенной установке Termidesk VDI приведена на рисунке (см. рисунок Схема стандартной распределенной установки).

Схема стандартной распределенной установки с Termidesk Connect приведена на рисунке (см. рисунок Схема стандартной распределенной установки при наличии лицензии). Особенности:

- для реализации функционала «Шлюза» используется лицензия Termidesk Connect Basic;
- для реализации функционала балансировщика используется лицензия Termidesk Connect. При отсутствии лицензии допускается использование сторонних балансировщиков нагрузки.

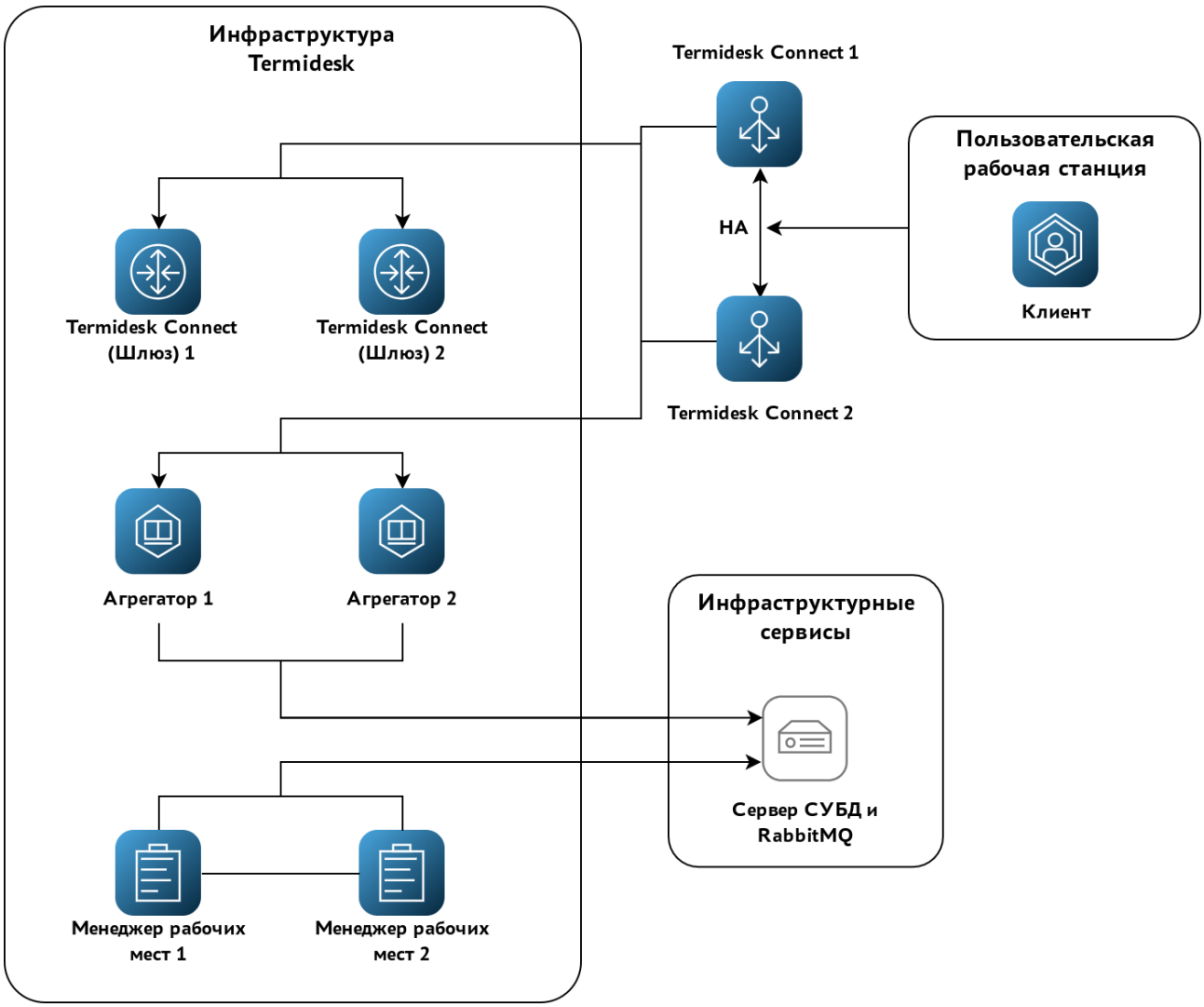


Рисунок 130. Схема стандартной распределенной установки

Схема стандартной распределенной установки при наличии лицензии

Termidesk Connect image::screenshots/407896716/407896837.png[image,align=center,width=752]

Перечень обозначенных на схеме компонентов приведен в таблице (см. таблицу Перечень компонентов схемы стандартной распределенной установки).

Таблица 209. Перечень компонентов схемы стандартной распределенной установки

Компонент	FQDN	Подпись на схеме
«Агрегатор» №1 с ролью «Агрегатор универсальный»	`aggr1.termidesk.local`	«Агрегатор 1»
«Агрегатор» №2 с ролью «Агрегатор универсальный»	`aggr2.termidesk.local`	«Агрегатор 2»
Termidesk Connect (лицензия «Termidesk Connect Basic») №1	`tdc-gw1.termidesk.local`	«Termidesk Connect (Шлюз) 1»
Termidesk Connect (лицензия «Termidesk Connect Basic») №2	`tdc-gw2.termidesk.local`	«Termidesk Connect (Шлюз) 2»
«Менеджер рабочих мест» №1	`tsk1.termidesk.local`	«Менеджер рабочих мест 1»
«Менеджер рабочих мест» №2	`tsk2.termidesk.local`	«Менеджер рабочих мест 2»

Компонент	FQDN	Подпись на схеме
Termidesk Connect №1	`tdc-lb1.termidesk.local`	«Termidesk Connect 1»
Termidesk Connect №2	`tdc-lb2.termidesk.local`	«Termidesk Connect 2»
База данных с брокером сообщений RabbitMQ	`db.termidesk.local`	«Сервер СУБД и RabbitMQ»

Стандартная распределенная установка проводится в следующей последовательности:

- на одном узле устанавливаются СУБД и RabbitMQ. При установке следует учесть, что в БД должны отсутствовать записи (необходимо использовать чистую БД);
- устанавливается первый (эталонный) узел с «Агрегатором». При установке необходимо выбрать роль «Агрегатор универсальный». Роль активируется при одновременном выборе ролей «Агрегатор администратора» и «Агрегатор пользователя» в диалоговом окне псевдографического интерфейса инсталлятора;

Настройки первого узла с «Агрегатором» будут использоваться как эталонные для других узлов.

Нужно скопировать каталог `/etc/opt/termidesk-vdi` вместе с его содержимым на другие узлы «Агрегатора» и «Менеджера рабочих мест».

- устанавливаются остальные «Агрегаторы» с копированием файлов, указанных выше, с эталонного узла;
- устанавливаются шлюзы;
- устанавливаются «Менеджеры рабочих мест» с копированием файлов, указанных выше, с эталонного узла.

Заключительным этапом устанавливаются и настраиваются «Балансировщики нагрузки».

Установка и настройка СУБД PostgreSQL

Процесс установки брокера сообщений RabbitMQ не отличается от процесса, описанного в разделе **Подготовка среды функционирования**. Установка и настройка СУБД PostgreSQL осуществляется согласно выбранной версии.

Для завершения настройки нужно:

- отредактировать файл `/etc/rabbitmq/rabbitmq-env.conf`, приведя его к виду:

```
# Defaults to rabbit. This can be useful if you want to run more than one node
# per machine - RABBITMQ_NODENAME should be unique per erlang-node-and-machine
# combination. See the clustering on a single machine guide for details:
# http://www.rabbitmq.com/clustering.html#single-machine
#NODENAME=rabbit

# By default RabbitMQ will bind to all interfaces, on IPv4 and IPv6 if
# available. Set this if you only want to bind to one network interface or#
# address family.
NODE_IP_ADDRESS=0.0.0.0
# Defaults to 5672.
```

```
NODE_PORT=5672
```

- сохранить файл и перезапустить службу `rabbitmq-server`:

```
sudo systemctl restart rabbitmq-server
```

Установка первого узла с «Агрегатором»

Процесс установки первого узла с «Агрегатором» аналогичен комплексной установке. В процессе установки следует выбрать роли: «Агрегатор администратора (AGGR_ADM)», «Агрегатор пользователя (AGGR_USR)».

После установки передать каталог `/etc/opt/termidesk-vdi` на остальные узлы «Агрегатора» и «Менеджера рабочих мест»:

```
sudo scp -r /etc/opt/termidesk-vdi localuser@ipaddr_or_fqdn_host:/home/user/
```

где:

`-r` - ключ для рекурсивной (со вложенными каталогами) передачи;

`localuser` - имя пользователя целевого узла;

`ipaddr_or_fqdn_host` - IP-адрес или FQDN целевого узла;

`/home/user` - путь, куда будет скопирован каталог.

Перед началом установки остальных узлов «Агрегатора» необходимо переместить скопированный ранее каталог `termidesk-vdi` в каталог `/etc/opt/`:

```
sudo mv /home/user/termidesk-vdi /etc/opt/
```

При копировании конфигурации с эталонного узла на другие узлы параметр `NODE_NAME` в файле `/etc/opt/termidesk-vdi/termidesk.conf` также копируется. Этот параметр должен быть уникальным для каждого узла в ферме. На каждом узле необходимо изменить значение `NODE_NAME` на уникальное, либо удалить его, чтобы при следующем запуске инсталлятор сгенерировал новое значение автоматически. Изменить параметр можно вручную в файле или с помощью утилиты `termidesk-config`.

Установить второй узел с «Агрегатором» по аналогии с первым, не меняя параметры в диалогах подключения к СУБД и заполнения информации о подключении к RabbitMQ.

Установка шлюзов

Начиная с Termidesk VDI версии 6.1, функционал «Шлюза» реализуется через продукт Termidesk Connect. Подробные сведения приведены в документации Termidesk Connect (доступ по ссылке: https://termidesk.ru/docs/).

Установка «Менеджеров рабочих мест»

Установка «Менеджеров рабочих мест» производится на два узла, работающих в режиме отказоустойчивой конфигурации, при которой оба узла активно обрабатывают трафик (конфигурация «Active - Active»), а отказ одного из них не нарушает работоспособность фермы Termidesk VDI.

Установка компонента на первый узел проводится в следующей последовательности:

- перемещается скопированный ранее каталог `termidesk-vdi` в каталог `/etc/opt/`:

```
sudo mv /home/user/termidesk-vdi /etc/opt/
```

При копировании конфигурации с эталонного узла на другие узлы параметр `NODE_NAME` в файле `/etc/opt/termidesk-vdi/termidesk.conf` также копируется. Этот параметр должен быть уникальным для каждого узла в ферме. На каждом узле необходимо изменить значение `NODE_NAME` на уникальное, либо удалить его, чтобы при следующем запуске инсталлятор сгенерировал новое значение автоматически. Изменить параметр можно вручную в файле или с помощью утилиты `termidesk-config`.

- создается файл `/etc/default/termidesk-vdi.local`:

```
sudo touch /etc/default/termidesk-vdi.local
```

- в созданном файле указываются каталоги расположения конфигурационного файла и шаблонов настройки регистрации событий и журналирования:

```
ETC='/etc/opt/termidesk-vdi'

TEMPLATES_DIR='/etc/opt/termidesk-vdi/templates'
```

- редактируется файл `/etc/opt/termidesk-vdi/termidesk.conf`, параметру `NODE_ROLES` присваивается значение `CELERYMAN`;
- устанавливается пакет `termidesk-vdi`:

```
sudo apt -y install termidesk-vdi
```

где:

`-y` - ключ для пропуска подтверждения установки.

В результате установки пакета `termidesk-vdi` на узле будут запущены службы `termidesk-celery-beat`, `termidesk-celery-worker`.

Установка второго узла с «Менеджером рабочих мест» выполняется по аналогии с первым.

Установка «Балансировщиков нагрузки»

Подробные сведения по установке «Балансировщика нагрузки» приведены в документации Termidesk Connect (доступ по ссылке: https://termidesk.ru/docs/).

При отсутствии полной лицензии на Termidesk Connect допускается использование сторонних балансировщиков нагрузки.

Действия после стандартной распределенной установки

Настройка «Балансировщика нагрузки» приведена в документации Termidesk Connect (доступ по ссылке: https://termidesk.ru/docs/).

После установки нужно задать ключ для подписи JWT-токена для взаимодействия с узлами фермы Termidesk VDI. Ключ может быть задан через файл `termidesk.conf` (параметр `AGGREGATOR_JWT_SSL_KEY`) или через утилиту `termidesk-config`.

После установки параметры «Агрегатора» могут быть изменены:

- через файл `termidesk.conf`;
- или через утилиту `termidesk-config`.

Комплексное обновление «Агрегатора»

Обновление должно осуществляться с соблюдением условий:

- обновление выполняется последовательно, с установкой промежуточных версий релизов. Например: 6.0 - 6.0.1 - 6.0.2 - 6.1;
- обновление выполняется операцией установки поверх предыдущей версии. В противном случае, если ранее «Агрегатор» был удален без удаления БД, при повторной установке может возникнуть ряд ошибок;
- после начала процедуры обновления запрещается производить любые операции с объектами с предыдущими версиями «Агрегатора».

Если в файлы запуска вручную были внесены какие-либо изменения, то эти изменения при обновлении не сохраняются.

Начиная с Termidesk VDI версии 6.1 компонент «Шлюз» (пакет `termidesk-gateway`) не входит в основную поставку. Для замены «Шлюза» следует использовать программу для электронной вычислительной машины «Балансировщик нагрузки Термидеск Коннект» (Termidesk Connect).

Инструкции по установке и настройке доступны по ссылкам: Инструкция по настройке Шлюза для Termidesk VDI (первый способ), Инструкция по настройке Шлюза для Termidesk VDI (второй способ, единая точка входа Termidesk VDI).

Особенности:

- для реализации функционала «Шлюза» используется лицензия Termidesk Connect Basic;
- для реализации функционала балансировщика используется лицензия Termidesk Connect. При отсутствии лицензии допускается использование сторонних балансировщиков нагрузки.

Перед любым обновлением рекомендуется выполнить резервное копирование БД:

```
pg_dump -d <наименование БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь> -W >
<имя_файла_для_сохранения_БД.sql>
```

где:

`-d <наименование БД>` - имя БД. При стандартных настройках используется имя `termidesk`;

`-h <IP-адрес_хоста>` - IP-адрес узла, где расположена БД. Если БД устанавливалась локально, нужно указать `localhost`;

`-p <порт>` - порт для подключения к БД. При стандартных настройках используется `5432`;

`-U <пользователь>` - имя пользователя для подключения. При стандартных настройках используется имя `termideskdb`;

`-W` - запрос пароля для подключения к БД. При стандартных настройках при появлении запроса нужно указать `ksedimret`;

`<имя_файла_для_сохранения_БД.sql>` - имя и формат файла (`sql`) для сохранения БД.

Для обновления «Агрегатора» нужно:

- остановить службы:

```
sudo systemctl stop termidesk-vdi termidesk-celery-beat termidesk-celery-worker
```

- подключить репозиторий Termidesk VDI;
- при использовании ОС Astra Linux Special Edition в более защищенном режиме, например, «Смоленск», потребуется выполнить дополнительную настройку:
  - для пользователя БД назначить классификационную метку (в примере используется `termideskdb`, в более ранних версиях использовалось имя пользователя `termidesk`):

    ```
    sudo pdpl-user -i 0 termideskdb
    ```

  - предоставить пользователю `postgres` права на чтение файла, содержащего классификационную метку пользователя `termideskdb`, подключающегося к БД:

    ```
    sudo setfacl -m u:postgres:r /etc/parsec/macdb/$(id -u termideskdb)
    ```

  - создать системного пользователя `termideskdb` (имя должно совпадать с именем пользователя в БД):

    ```
    sudo useradd -M termideskdb -s /usr/sbin/nologin -d /home/termideskdb
    ```

- выполнить обновление:

```
sudo apt install -y termidesk-vdi
```

где:

`-y` - ключ для пропуска подтверждения установки;

- в диалогах ввода параметров подключения к СУБД и RabbitMQ нажать экранную кнопку **[OK]**;
- в диалоге выбора ролей нужно нажать экранную кнопку **[OK]**;

Диалоги настройки параметров отображаются в том случае, если ранее они не были заданы.

После обновления нужно заполнить файл сопоставления `mapping.yaml` и указать его в `termidesk.conf` (параметр `AGGREGATOR_YAML_FILE`).

Обновление для распределенной конфигурации установки «Агрегатора»

Общая концепция обновления

Описание применимо к ферме «Агрегатора», установленной в распределенной конфигурации. Общая последовательность действий приведена на рисунке Последовательность обновления распределенной конфигурации.

Обновление должно осуществляться с соблюдением условий:

- если используется «Агрегатор», то ферма «Агрегатора» обновляется первой, и только потом обновляется ферма поставщиков ресурсов (ферма Termidesk VDI);
- обновление выполняется последовательно, с установкой промежуточных версий релизов. Например: 6.0 - 6.0.1 - 6.0.2 - 6.1;
- обновление выполняется операцией установки поверх предыдущей версии. В противном случае, если ранее «Агрегатор» был удален без удаления БД, при повторной установке может возникнуть ряд ошибок;
- после начала процедуры обновления запрещается производить любые операции с объектами с предыдущими версиями «Агрегатора».

Начиная с Termidesk VDI версии 6.1 компонент «Шлюз» (пакет `termidesk-gateway`) не входит в основную поставку. Для замены «Шлюза» следует использовать программу для электронной вычислительной машины «Балансировщик нагрузки Термидеск Коннект» (Termidesk Connect).

Инструкции по установке и настройке доступны по ссылкам: Инструкция по настройке Шлюза для Termidesk VDI (первый способ), Инструкция по настройке Шлюза для Termidesk VDI (второй способ, единая точка входа Termidesk VDI).

Особенности:

- для реализации функционала «Шлюза» используется лицензия Termidesk Connect Basic;
- для реализации функционала балансировщика используется лицензия Termidesk Connect. При отсутствии лицензии допускается использование сторонних балансировщиков нагрузки.

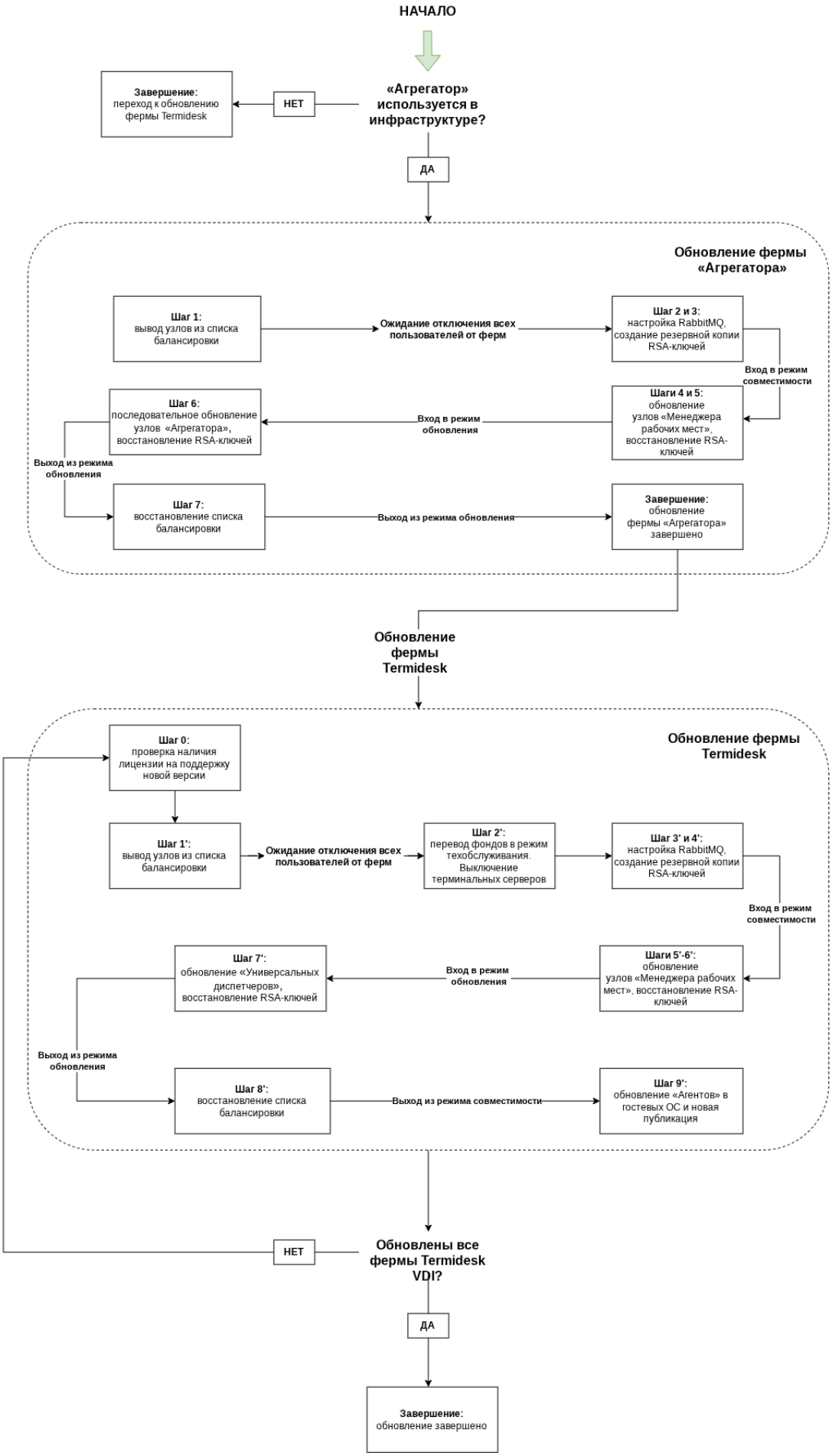


Рисунок 131. Последовательность обновления распределенной конфигурации

На схеме:

- режим совместимости - режим, характеризующийся отличием в версиях между любыми компонентами фермы «Агрегатора»;
- режим обновления - режим, характеризующийся наличием не обновленных «Агрегаторов» при уже обновленных записях БД.

Последовательность обновления фермы «Агрегатора», установленной в распределенной отказоустойчивой конфигурации:

Шаг 1. На всех балансировщиках нагрузки, отвечающих за распределение подключений к «Агрегаторам», из списка балансировки исключаются все узлы, кроме одного резервного, чтобы сохранить работоспособность балансировщика. Это позволит избежать ошибки при перезапуске nginx из-за пустого `upstream`.

Шаг 2. На сервер с СУБД, либо на отдельно выделенный сервер, устанавливается и настраивается компонент RabbitMQ в случае, если ранее RabbitMQ не был установлен.

Шаг 3. Создается резервная копия RSA-ключей, расположенных в каталоге `/etc/opt/termidesk-vdi/wsproxy/`.

Шаг 4. Обновляется первый «Менеджер рабочих мест». Запуск служб выполняется автоматически. На обновленном «Менеджере рабочих мест» восстанавливаются RSA-ключи из резервной копии, созданной на **Шаге 3**. В этом процессе автоматически будут обновлены записи в БД.

Шаг 5. Обновляются последующие «Менеджеры рабочих мест». Запуск служб выполняется автоматически. На обновленном «Менеджере рабочих мест» восстанавливаются RSA-ключи из резервной копии, созданной на **Шаге 3**.

Шаг 6. Последовательно обновляются все узлы «Агрегатора» («Агрегатор администратора», «Агрегатор пользователя», «Агрегатор универсальный»). Запуск служб выполняется автоматически. На обновленных «Агрегаторах» восстанавливаются RSA-ключи из резервных копий, созданных на **Шаге 3**. Узлы перезагружаются.

Шаг 7. На всех балансировщиках нагрузки список балансировки восстанавливается до исходного (все ранее исключенные узлы возвращаются в списки `upstream`).

После обновления фермы «Агрегатора» выполняется обновление фермы Termidesk VDI.

Описание обновления фермы Termidesk VDI приведено в подразделе **Обновление для распределенной конфигурации установки** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса».

Шаг 1. Редактирование конфигурации балансировщика нагрузки

На балансировщике нагрузки открыть и отредактировать файл `/etc/nginx/sites-available/sampledomain.ru.conf`.

В данном конфигурационном файле следует найти директиву `daas-upstream-nodes` с перечислением списка «Агрегаторов» и закомментировать все узлы, кроме одного резервного, чтобы сохранить работоспособность балансировщика.

Здесь и далее примеры IP-адресов приведены в соответствии с RFC 5737. Указанные IP-адреса должны быть заменены на актуальные, используемые согласно схеме адресации, принятой в инфраструктуре организации.

```
upstream daas-upstream-nodes {
 least_conn;
     server 192.0.2.33;
     server 192.0.2.34;
     server 192.0.2.35;
 }
```

Для исключения всех узлов, кроме одного, файл приводится к виду (оставлен активным узел 192.0.2.33):

```
upstream daas-upstream-nodes {
 least_conn;
     server 192.0.2.33;
     #server 192.0.2.34;
     #server 192.0.2.35;
 }
```

После изменения файла перезапустить веб-сервер:

```
sudo systemctl restart nginx
```

Убедиться, что перезапуск прошел успешно и ошибок нет. При необходимости проверить логи nginx.

Шаг 2. Установка и настройка RabbitMQ

При отсутствии ранее установленного RabbitMQ выполняется его установка в соответствии с подразделом **Подготовка среды функционирования** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса».

Ферма «Агрегатора» не должна использовать экземпляры БД и брокера сообщений RabbitMQ, предназначенные для фермы Termidesk VDI.

Предполагается, что СУБД установлена на узле RabbitMQ. При использовании ОС Astra Linux Special Edition в более защищенном режиме, например, «Смоленск», потребуется выполнить дополнительную настройку:

- для пользователя БД назначить классификационную метку (в примере используется `termideskdb`, в более ранних версиях использовалось имя пользователя `termidesk`):

```
sudo pdpl-user -i 0 termideskdb
```

- предоставить пользователю `postgres` права на чтение файла, содержащего классификационную метку пользователя `termideskdb`, подключающегося к БД:

```
sudo setfacl -m u:postgres:r /etc/parsec/macdb/$(id -u termideskdb)
```

- создать системного пользователя termideskdb (имя должно совпадать с именем пользователя в БД):

```
sudo useradd -M termideskdb -s /usr/sbin/nologin -d /home/termideskdb
```

Шаг 3. Резервное копирование RSA-ключей

Выполнить резервное копирование RSA-ключей с одного из узлов «Агрегатора». Резервные копии ключей можно скопировать, например, на другой сетевой узел командой:

```
sudo scp -r /etc/opt/termidesk-vdi/wsproxy
localuser@ipaddr_or_fqdn_host:/home/localuser/
```

где:

-r - ключ для рекурсивной (со вложенными каталогами) передачи;

localuser - имя пользователя целевого узла;

ipaddr_or_fqdn_host - IP-адрес или FQDN целевого узла;

/home/user - путь, куда будет скопирован каталог.

Шаг 4. Обновление первого «Менеджера рабочих мест»

Перед запуском процедуры обновления нужно:

- отредактировать файл /etc/opt/termidesk-vdi/termidesk.conf и задать значение для параметра METRICS_ACCESS_KEY, если оно не задано;

> При редактировании файла /etc/opt/termidesk-vdi/termidesk.conf рекомендуется использовать одинаковое значение параметра METRICS_ACCESS_KEY для всех «Менеджеров рабочих мест».

- остановить службы Termidesk VDI:

```
sudo systemctl stop termidesk-celery-beat termidesk-celery-worker
```

- удалить кеш файла ответов debconf командами:

```
sudo rm -f /var/cache/debconf/config.dat
sudo rm -f /var/cache/debconf/config.dat-old
```

Для обновления «Менеджера рабочих мест»:

- обновить список пакетов и выполнить запуск файла установщика:

```
sudo apt update
```

```
sudo apt install termidesk-vdi
```

- в диалоговом окне псевдографического интерфейса инсталлятора выбрать режим работы ПО «Агрегатор».

После обновления выполнить копирование сохраненных на **Шаге 3** RSA-ключей на узел с обновленным «Менеджером рабочих мест».

Шаг 5. Обновление остальных «Менеджеров рабочих мест»

Обновление производится аналогично **Шагу 4**.

Шаг 6. Обновление узлов «Агрегаторов»

Перед запуском процедуры обновления нужно:

- отредактировать файл `/etc/opt/termidesk-vdi/termidesk.conf` и задать значение для параметра `METRICS_ACCESS_KEY`, если оно не задано;

> Корректировка файла `/etc/apache2/apache2.conf` при обновлении не производится.
>
> При редактировании файла `/etc/opt/termidesk-vdi/termidesk.conf` рекомендуется задать одинаковое значение параметра `METRICS_ACCESS_KEY` для всех узлов «Агрегатора».

- остановить службу Termidesk VDI:

```
sudo systemctl stop termidesk-vdi
```

- удалить кеш файла ответов `debconf` командами:

```
sudo rm -f /var/cache/debconf/config.dat
sudo rm -f /var/cache/debconf/config.dat-old
```

где:

`-f` - ключ игнорирования несуществующих файлов.

Для обновления «Агрегатора»:

- обновить список пакетов и выполнить запуск файла установщика:

```
sudo apt update
sudo apt install termidesk-vdi
```

- в диалоговом окне псевдографического интерфейса инсталлятора выбирается режим работы «Агрегатор», роль «Портал администратора» и/или «Портал пользователя» в зависимости от ранее установленной роли.

После обновления:

- выполнить копирование сохраненных на **Шаге 3** RSA-ключей на узлы с обновленными «Агрегаторами»;
- заполнить файл сопоставления `mapping.yaml` и указать его в `termidesk.conf` (параметр `AGGREGATOR_YAML_FILE`);
- перезагрузить узлы:

```
sudo reboot
```

После загрузки узла проверить состояние служб:

```
sudo systemctl -a | grep termidesk
```

где:

`-a` - ключ для вывода списка служб;

`grep` - утилита для поиска текста в выводе предыдущей команды.

Проверить доступность веб-порталов «Агрегатора» через веб-браузер.

Шаг 7. Восстановление конфигурации балансировщика нагрузки

По завершении обновления **ВСЕХ** узлов «Агрегатора» список балансировки на **ВСЕХ** балансировщиках восстанавливается до исходного (все ранее исключенные узлы возвращаются в списки `upstream`).

Пример для балансировщика nginx:

- ранее закомментированные строки нужно раскомментировать;
- затем выполнить перезагрузку службы `nginx` на каждом балансировщике:

```
sudo systemctl restart nginx
```

Выполнить проверку доступности веб-портала «Агрегатора» через веб-браузер сначала обращением на IP-адрес каждого из «Агрегаторов», затем обращением на IP-адрес балансировщика нагрузки.

Удаление Termidesk

Для удаления нужно:

- выполнить:

```
sudo apt purge termidesk-vdi
```

- удалить файлы, задающие переменные окружения:

```
sudo rm /etc/default/termidesk-vdi.local
```

```
sudo rm /etc/default/termidesk-vdi
```

Для удаления БД и роли пользователя следует выполнить следующие действия, строго соблюдая их последовательность:

- переключиться на пользователя `postgres` (через пользователя `root`):

```
sudo su postgres
```

- запустить терминальный клиент СУБД:

```
psql
```

- используя интерактивный интерфейс терминального клиента СУБД, удалить БД:

```
postgres=# DROP DATABASE termidesk;
```

- удалить роль пользователя БД:

```
postgres=# DROP ROLE termidesk;
```

- выйти из интерактивного интерфейса терминального клиента СУБД:

```
postgres=# \q
```

- выйти из сеанса пользователя `postgres`:

```
exit
```

- удалить оставшийся каталог с файлами, содержащими переменные для подключения к БД, сертификат и ключ:

Если для хранения конфигурационных файлов, журналов и шаблонов использовались каталоги, отличные от стандартных, нужно удалить их.

```
sudo rm -R /etc/opt/termidesk-vdi
```

где:

`-R` - ключ для рекурсивного действия. Будут удалены все вложенные подкаталоги.

Проверка работоспособности после установки «Агрегатора»

«Агрегатор» является работоспособным, если в результате перехода в веб-браузере по адресу https://localhost/ или https://127.0.0.1/ отобразилась страница входа в веб-портал. Если страница сразу не отобразилась, следует подождать 10-15 секунд и обновить ее.

После установки по умолчанию для доступа к порталу включено перенаправление на протокол HTTPS. При необходимости использования незащищенного протокола HTTP администратор должен изменить файл `/etc/apache2/sites-available/termidesk.conf`.

Указанные адреса используются в случае локальной установки. Если «Агрегатор» установлен на узле, отличном от того, на котором происходит проверка, необходимо вместо localhost или 127.0.0.1 использовать IP-адрес узла «Агрегатора».

По умолчанию после установки вход в веб-портал доступен только авторизованному пользователю ОС с ролью «Администратор»:

- пользователь ОС должен быть членом группы с GID `1001`;
- для входа в полях «Логин» и «Пароль» необходимо указать идентификатор пользователя ОС и его пароль соответственно, а затем нажать экранную кнопку **[Войти]**.

В некоторых версиях ОС Astra Linux Special Edition указанной группе по умолчанию может быть назначен GID `1000` вместо `1001`.

Группу можно поменять после установки через утилиту `termidesk-config` или командой:

```
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_config set --key
security.adminPamGroup --value ${ADMIN_GID}
```

Проверка добавления ключа от репозитория производителя в ОС выполняется командой:

```
apt-key list
```

Проверка состояния компонентов выполняется командами:

```
systemctl status termidesk-vdi.service
systemctl status termidesk-celery-beat.service
systemctl status termidesk-celery-worker.service
```

Строка `Active` отображает состояние сервиса, где статус `active (running)` свидетельствует об успешном запуске.

АГРЕГАТОР. НАСТРОЙКА АГРЕГАЦИИ РЕСУРСОВ

Общая последовательность шагов по настройке агрегации ресурсов выглядит следующим образом:

- подготовка сетевой инфраструктуры в соответствии с требованиями;

- подготовка среды функционирования в соответствии с подразделом **Подготовка среды функционирования**;
- установка «Агрегатора»;
- переход в веб-портал «Агрегатор администратора»;
- добавление домена аутентификации;
- добавление групп домена аутентификации;
- добавление ферм поставщиков ресурсов;
- добавление узлов;
- создание сайта;
- создание объединенного набора ресурсов.

После этого пользователю станет доступно подключение к «Агрегатору» через компонент «Клиент» для получения объединенного набора ресурсов.

АГРЕГАТОР. ДОМЕНЫ АУТЕНТИФИКАЦИИ

Добавление доменов аутентификации в «Агрегаторе»

Общие сведения о доменах аутентификации

Домен аутентификации - источник сведений о субъектах и их полномочиях.

Следует предусмотреть, что в целях безопасности учетная запись для биндинга (подключения) к домену не должна иметь прав на удаление или изменение объекта типа «пользователь».

Для отображения списка доменов аутентификации следует перейти «Системные параметры - Домены аутентификации». Основные параметры списка приведены в таблице (см. таблицу Параметры списка доменов аутентификации).

Доступ к разделу «Системные параметры» определяется разрешениями «Просмотр системных параметров» и «Изменение системных параметров» (см. подраздел **Назначение служебных функций администраторам**).

Таблица 210. Параметры списка доменов аутентификации

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Приоритет»	Приоритет отображения в списке доменов аутентификации
«Название в системе»	Тип домена аутентификации
«Пользователи»	Количество пользователей домена аутентификации
«Комментарии»	Информационное сообщение, используемое для описания назначения домена аутентификации
«Теги»	Список тегов, назначенных домену аутентификации. При выборе тега выполняется переход к разделу «Системные параметры – Теги» со списком объектов, которым назначен данный тег

Поддерживается:

- поиск записей по таблице;

- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Доступны следующие действия над доменом аутентификации:

- редактирование. Для этого нужно пометить домен аутентификации и нажать на экранную кнопку **[Изменить]**;
- удаление. Для этого нужно пометить домен аутентификации и нажать на экранную кнопку **[Удалить]**;
- назначение тегов домену аутентификации. Для этого нужно пометить домен аутентификации и нажать экранную кнопку **[Теги]**. Общее описание по применению тегов приведено в подразделе **Общие сведения о тегах**.

Добавление домена аутентификации LDAP

Перечень параметров для добавления домена аутентификации MS AD (LDAP)

Для добавления домена аутентификации следует перейти «Системные параметры - Домены аутентификации», а затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «Microsoft AD DS/LDAP».

Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления аутентификации MS AD).

Для проверки и сохранения параметров конфигурации нужно нажать экранную кнопку **[Тест]**, затем **[Создать]**.

Таблица 211. Данные для добавления аутентификации MS AD

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения домена аутентификации
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий. Порядок отображения доменов зависит от приоритета домена и его наименования: • чем ниже приоритет, тем выше домен в списке; • при наличии доменов с одинаковым приоритетом действует сортировка по алфавиту

Параметр	Описание
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных. Параметр используется для поиска аналогичного домена «Универсального диспетчера», поэтому должен быть одинаковым как на портале «Агрегатор администратора» (при его использовании), так и на «Портале администратора». Поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)
«Субъекты»	Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: • «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на порталах «Агрегетор администратора», «Агрегатор пользователя», «Агрегатор универсальный», и при подключении из компонента «Клиент»; • «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Агрегаторе администратора» или «Агрегаторе универсальном»; • «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Агрегаторе пользователя», «Агрегаторе универсальном» или при подключении пользователя из компонента «Клиент»; • «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала

Параметр	Описание
«Порталы»	Выбор порталов «Агрегатора», для которых будет доступен домен аутентификации. Если портал не выбран, то домен аутентификации не будет доступен для него. В списке доступных значений отображаются все доступные узлы порталов с их полным доменным именем. Администратору нужно выбирать узел в соответствии со значением, указанным в параметре «Субъекты». Примеры: • если в параметре «Субъекты» указано «Пользователи», то в параметре «Порталы» должен быть выбран узел, соответствующий либо «Агрегатору пользователя», либо «Агрегатору универсальному»; • если в параметре «Субъекты» указано «Администраторы и персонал», в параметре «Порталы» должен быть выбран узел, соответствующий либо «Агрегатору администратора», либо «Агрегатору универсальному»; • если в параметре «Субъекты» указано «Все», то в параметре «Порталы» может быть выбран узел, соответствующий либо «Агрегатору пользователя», либо «Агрегатору администратора», либо «Агрегатору универсальному». Значение выбирается исходя из потребностей в разделении доменов аутентификации для того или иного субъекта. При изменении списка узлов: • если узел удален, то он автоматически удалится из списка доступных значений для этого параметра. Уже назначенное значение удалится из свойств домена аутентификации; • если узел добавлен, то он автоматически добавится в список доступных значений для этого параметра, но не будет автоматически выбран для использования. ! В случае, если в параметре «Порталы» был указан единственный узел, который затем был удален, то этот домен аутентификации не будет доступен ни в каком из порталов. Для выбора всех порталов используется значение «Все»
«Сервер LDAP»	IP-адрес или доменное имя сервера службы каталогов, являющегося источником сведений о субъектах и их полномочиях
«Порт»	TCP-порт, на котором запущена служба каталогов. Возможные стандартные значения: • «389» (по умолчанию). Используется, если доступ к службе каталогов осуществляется по протоколу LDAP; • «636». Используется, если доступ к службе каталогов осуществляется по протоколу LDAPS; • «3268». Альтернативный порт. Используется, если доступ к службе каталогов осуществляется по протоколу LDAP; • «3269». Альтернативный порт. Используется, если доступ к службе каталогов осуществляется по протоколу LDAPS. Для ускорения поиска пользователей в службе каталогов рекомендуется указывать альтернативный порт
«Использовать SSL»	Использовать защищенное соединение при взаимодействии со службой каталогов

Параметр	Описание

«Проверять SSL»	Выполнять проверку цепочки сертификатов и имени (hostname) сервера службы каталогов.
	
	Возможные значения:
	
	• «Да» (по умолчанию для создаваемых доменов) - использовать механизм проверки. Если при этом выключен параметр «Использовать SSL», то значение «Проверять SSL» не применяется (то есть, проверка сертификатов отключена). Если используется защищенное соединение и включен механизм проверки, то TLS-соединение будет установлено только при отсутствии ошибок проверки сертификатов и имя сервера службы каталогов;
	• «Нет» (по умолчанию для уже созданных ранее доменов) - не использовать механизм проверки. Если при этом включен параметр «Использовать SSL», то ошибки при проверке сертификатов не влияют на подключение (TLS-соединение все равно будет установлено)
	
	Корневой сертификат УЦ должен быть добавлен на узел «Агрегатора администратора» (см. подраздел **Установка корневого сертификата центра сертификации** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»). При этом:
	
	• сертификат должен быть задан в формате `Base64`, пример:
	
	`-----BEGIN CERTIFICATE-----`
	`MIIDVzCCAj+gAwIBAgIQPvc7pjfSf5VLzNdgExZPxzANBgkqhkiG9w0`
	`BAQsFADA+`
	`MRMwEQYKCZImiZPyLGQBGRYDbGFuMRIwEAYKCZImiZPyLGQBGRYCc2Q`
	`xEzARBgNV`
	`....`
	`-----END CERTIFICATE-----`
	
	• использование параметра `REQUESTS_CA_BUNDLE` конфигурационного файла `termidesk.conf` опционально: достаточно добавить корневой сертификат в системное хранилище ОС, но работа с параметром также поддерживается.

«Путь к секретам»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «hvac». Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**. Пример: «hvac-kv://secret#termidesk-admin/msad/»

Параметр	Описание

«Механизм подключения»	Механизм подключения к службе каталогов.
	
	Возможные значения:
	
	• «SASL Bind» - безопасный механизм подключения с использованием протокола SASL. При выборе этого значения потребуется:
	  заполнить параметр «Путь до Keytab», при этом вводить сервер Termidesk VDI в домен не требуется (необходимо только задание и наличие `keytab`-файла);
	  убедиться, что на узле существует файл `/etc/krb5.conf`, в котором заданы настройки доменов для подключений к ним. Пример файла `/etc/krb5.conf` приведен после таблицы;
	• «Simple Bind» - небезопасный механизм подключения, передающий данные для подключения в открытом виде.
	
	Значение по умолчанию: «SASL Bind»

«Учётная запись»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Учетная запись в формате Distinguished Name (DN) в домене MS AD (LDAP), используемая для подключения к службе каталогов. Пример: «CN=admin,OU=user,DC=test,DC=desk»
«Пароль учётной записи»	Параметр доступен, если на этапе установки Termidesk VDI был выбран способ хранения паролей «config». Набор символов, подтверждающий полномочия объекта для подключения к службе каталогов
«Таймаут, с»	Время ожидания (в секундах) ответа от службы каталогов. Значение по умолчанию: «10»
«Base DN»	Корень поиска в службе каталогов в формате DN. Параметру следует задавать значение, соответствующее записи верхнего уровня в иерархии службы каталогов (без указания OU). Вводимое значение не должно содержать пробелов: • в начале и конце строки; • рядом с разделителями (запятыми); • в элементах пути (например, «DC=company name,DC=de»). Пример: «DC=test,DC=desk»
«Имя класса пользователя»	Атрибут класса пользователя в службе каталогов. Для корректного заполнения данного поля необходимо указать значение «person»

Параметр	Описание
«Атрибут идентификатора пользователя»	Атрибут уникального имени или идентификатора пользователя в службе каталогов. Атрибут идентификатора пользователя задается с учетом того, какой шаблон использовался при выдаче сертификата пользователя. Например, значение «name» для механизма аутентификации Kerberos PKINIT указывается в том случае, если сертификат для подключения выдан на имя пользователя. Для корректного заполнения данного поля необходимо указать: • значение «name», если активирован параметр «Использовать PKINIT»; • значение «userPrincipalName», если в параметре «Формат имени пользователя для аутентификации» используется «userPrincipalName»; • значение «SamAccountName» в остальных случаях
«Список атрибутов пользователя»	Список атрибутов, содержащий уникальные данные пользователя, разделенные запятыми. Для корректного заполнения данного поля необходимо указать значение: • «userPrincipalName», если в параметре «Формат имени пользователя для аутентификации» используется «userPrincipalName»; • «name», если в параметре «Формат имени пользователя для аутентификации» используется «sAMAccountName»
«Формат имени пользователя для аутентификации»	Формат имени пользователя, заданный в службе каталогов. Если на пользовательской рабочей станции установлен компонент «Клиент» версии, младше 6.0, то он будет поддерживать только формат «sAMAccountName». Возможные значения: • «sAMAccountName» (по умолчанию) - имя пользователя без доменной части; • «userPrincipalName» - имя пользователя с доменной частью
«Имя атрибута группы»	Атрибут принадлежности к группе в службе каталогов. Для корректного заполнения данного поля необходимо указать значение «group»

Параметр	Описание
«Атрибут имени группы»	Атрибут идентификатора группы, к которой относится субъект в службе каталогов. Атрибут имени группы задается с учетом того, какой шаблон использовался при выдаче сертификата пользователя. Например, значение «name» для механизма аутентификации Kerberos PKINIT указывается в том случае, если сертификат для подключения выдан на имя пользователя. Для корректного заполнения данного поля необходимо указать: • значение «distinguishedname», если включены параметры «Использовать рекурсивный поиск групп» или «Использовать обратный порядок проверки членства пользователей»; • значение «name», если активирован параметр «Использовать PKINIT» или «Использовать Kerberos»; • значение «cn» в остальных случаях. Если используется значение «distinguishedname», то при добавлении группы в домен аутентификации по пути «Системные параметры - Домены аутентификации - Наименование домена - Группы» нужно указывать длинные имена групп, например: «CN=RootGroup,CN=Users,DC=test,DC=desk». Если используется значение «cn», то нужно указывать короткие имена групп. Если параметр «Атрибут имени группы» был изменен, то необходимо заново добавить группы, используя соответствующие имена групп: для «cn» - короткие имена, для «distinguishedname» - длинные имена
«Атрибут членства в группе»	Идентификатор группы для назначения полномочий субъекту. Для корректного заполнения данного поля необходимо указать значение «member»
«Атрибут групп для LDAP-запросов»	Атрибут, определяющий группы пользователя при запросах к службе каталогов. Возможные значения: «objectClass», «objectCategory»
«Время хранения дополнительных атрибутов учетной записи пользователей, сут»	Срок хранения (в сутках) дополнительных атрибутов учетной записи пользователей в БД. При наступлении срока данные будут очищены. Возможные значения: • «0» (по умолчанию) - не хранить дополнительные атрибуты; • числовое значение - хранить дополнительные атрибуты на протяжении заданного срока
«Использовать рекурсивный поиск групп»	При запросе групп пользователя будут учтены его родительские группы, в которых он состоит неявно. При этом проверяется вхождение пользователя только в те группы, которые добавлены в домен аутентификации в Termidesk VDI. Если дополнительно включен параметр «Использовать обратный порядок проверки членства пользователей», то параметр «Использовать рекурсивный поиск групп» можно не включать. Возможные значения: • «Да» - использовать рекурсивный поиск; • «Нет» (по умолчанию) - не использовать рекурсивный поиск

Параметр	Описание
«Использовать обратный порядок проверки членства пользователей»	Проверка соответствия членства пользователя в группах службы каталогов членству в группах домена аутентификации. Для работы функционала необходимо, чтобы был задан параметр «Атрибут имени группы». Этот параметр нужно включить при большом количестве групп непосредственно на службе каталогов MS AD. В этом случае сначала будет проверяться вхождение пользователя в группы домена аутентификации (в том числе рекурсивно), затем будет происходить проверка найденных групп в службе каталогов MS AD. При выключении этого параметра применяется настройка выбора «Атрибут групп для LDAP-запросов»: «objectClass» или «objectCategory». При включении этого параметра всегда применяется настройка выбора «Атрибут групп для LDAP-запросов»: «objectClass». Возможные значения: • «Да» - использовать обратный порядок; • «Нет» (по умолчанию) - не использовать обратный порядок

Параметр	Описание

«Динамическая проверка членства пользователя в группах»	Управление динамической проверкой вхождения пользователя в группу службы каталогов.
	
	Параметр определяет, как будет происходить проверка нахождения пользователя в группе службы каталогов при аутентификации в Termidesk VDI и получении ресурсов.
	
	Особенности функционирования:
	
	• если пользователю уже назначено РМ, то проверяется вхождение пользователя в группу, указанную в свойствах фонда РМ. Проверка выполняется каждый раз при доступе к ресурсу. При этом если у пользователя отозваны права на доступ, то он:
	  - либо не увидит скрытый ресурс в зависимости от настройки «Скрывать недоступные ресурсы»;
	  - либо увидит, но не сможет получить доступ к нему;
	  - либо получит доступ к назначенному РМ, если права доступа были назначены на другую группу, в которую входит пользователь и которая указана в свойствах фонда РМ;
	  - либо получит доступ к назначенному РМ, если оно назначено на учетную запись пользователя напрямую.
	
	Возможные значения:
	
	• «Режим совместимости 6.0» (по умолчанию) - при аутентификации пользователя происходит запрос к службе каталогов для проверки его вхождения в группы. После этого группы пользователя актуализируются в БД. При попытке получить ресурс из фонда доступ определяется на основе информации из БД (БД не обновляется);
	• «Периодическое обновление» - если пользователя нет в БД и он впервые аутентифицируется, то происходит запрос к службе каталогов для получения актуальной информации о нем. Если пользователь есть в БД, то информация берется из нее. Актуализация пользователей и групп для всех доменов аутентификации с этим значением выполняется периодической фоновой задачей раз в 24 часа;
	• «Динамическая проверка» - при аутентификации пользователя или получении ресурсов происходит запрос к службе каталогов для получения актуальной информации о нем. При обращении к службе каталогов информация о полученных группах кешируется во внутренней памяти. Время кеширования определяется системным параметром «Таймаут кеша хранения групп домена, с»

Параметр	Описание
«Использовать PKINIT»	Использовать механизм аутентификации Kerberos PKINIT при аутентификации пользователя. PKINIT - механизм, позволяющий использовать сертификаты X.509 в качестве метода аутентификации. Предполагается, что механизм аутентификации Kerberos PKINIT настроен в инфраструктуре организации и пользователю выданы соответствующие сертификаты и ключи для подключения (персональный сертификат, закрытый ключ к нему и корневой сертификат ЦС, на котором выпущен персональный сертификат). При активации механизма аутентификации Kerberos PKINIT нужно указать актуальный порт в параметре «Порт PKINIT», а также указать нужные значения параметров «Атрибут имени группы» и «Атрибут идентификатора пользователя». Настройки параметров «Атрибут имени группы» и «Атрибут идентификатора пользователя», и связанных с ними «Формат имени пользователя для аутентификации» и «Список атрибутов пользователя» задаются с учетом того, какой шаблон использовался при выдаче сертификата пользователя. Поскольку служба каталогов MS AD использует шаблон с форматом «userPrincipalName», то рекомендуется использовать в настройках параметров этот формат (там, где он применим). Возможные значения: • «Да» - использовать механизм; • «Нет» (по умолчанию) - не использовать механизм
«Порт PKINIT»	TCP/UDP порт, на котором запущена служба Kerberos. Значение по умолчанию: «88»

Параметр	Описание
«Использовать Kerberos»	Использовать механизм аутентификации по билету Kerberos. Доступность функционала зависит от типа редакции Termidesk VDI. Предполагается, что механизм аутентификации по билету Kerberos настроен в инфраструктуре организации (см. подразделы Получение и добавление `keytab`-файла для Kerberos-аутентификации и Настройка пользовательской рабочей станции для Kerberos-аутентификации). Для работы аутентификации по билету Kerberos на терминальных серверах MS RDS, необходимо выполнить дополнительную настройку «Сессионного агента», задав значения параметрам `MASTER_KEY` и `URL_BALANCER` в его конфигурационном файле. Если используется аутентификация Kerberos, то нужно заполнить параметр «Путь до Keytab». Потребуется правильная настройка параметров «Атрибут имени группы», «Атрибут идентификатора пользователя», «Формат имени пользователя для аутентификации», «Список атрибутов пользователя». Поскольку служба каталогов MS AD использует шаблон с форматом «userPrincipalName», то рекомендуется использовать в настройках параметров этот формат (там, где он применим). Возможные значения: • «Да» - использовать механизм; • «Нет» (по умолчанию) - не использовать механизм
«Путь до Keytab»	Путь к файлу с ключами для сервисного аккаунта. В зависимости от места хранения файла следует указать путь в формате: • в случае стандартного хранения файла: «/etc/opt/termidesk-vdi/termidesk.keytab»; • в случае хранения файла в хранилище hvac: «hvac-kv://secret#termidesk-admin/keytabs/kerberos». Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»** Если используется хранилище, то сгенерированный на контроллере домена `keytab`-файл должен быть преобразован к формату BASE64.

Для подключения к службе каталогов учетная запись должна иметь как минимум следующие привилегии:

- право на чтение объектов пользователей;
- право на чтение Base DN;
- право на чтение атрибутов групп.

Пример файла `/etc/krb5.conf` при выборе значения «SASL Bind» в параметре «Механизм подключения»:

Приведен только пример, требуется изменить файл при внедрении в соответствии с инфраструктурой организации.

```
[libdefaults]
  default_realm = TEST.LOC
  dns_lookup_realm = true
  rdns = false
  dns_canonicalize_hostname = false
  dns_lookup_kdc = true
  ticket_lifetime = 24h
  forwardable = true
  udp_preference_limit = 0
  default_ccache_name = KEYRING:persistent:%{uid}
#canonicalize = true
[realms]
  TEST.LOC = {
    pkinit_anchors = FILE:/var/lib/ipa-client/pki/kdc-ca-bundle.pem
    pkinit_pool = FILE:/var/lib/ipa-client/pki/ca-bundle.pem  }
    TST.LOC = {
        kdc = tst.loc
        kdc = msad.tst.loc
        admin_server = tst.loc
        default_domain = tst.loc
[domain_realm]
  .test.loc = TEST.LOC
  test.loc = TEST.LOC
  tdsk.test.loc = TEST.LOC
    tst.loc = TST.LOC
    .tst.loc = TST.LOC
```

Получение и добавление `keytab`-файла для Kerberos-аутентификации

Для получения `keytab`-файла на контроллере домена MS AD нужно:

- заранее создать учетную запись (сервисный аккаунт), от имени которой будет работать служба. Для создания учетной записи нужно на КД перейти в стандартную утилиту «Active Directory - пользователи и компьютеры»;
- в свойствах учетной записи во вкладке «Account» активировать параметр «This account supports Kerberos AES 256 bit encryption» (см. рисунок Активация параметра «This account supports Kerberos AES 256 bit encryption»);

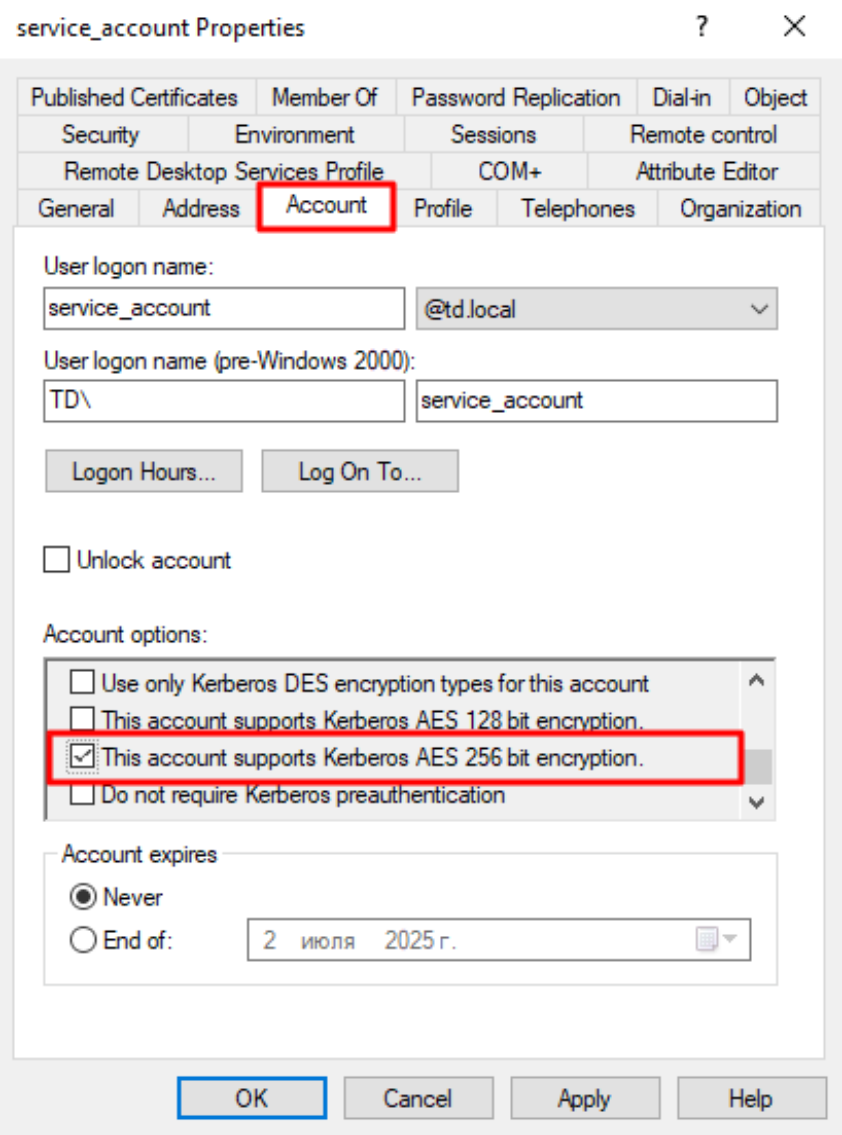


Рисунок 132. Активация параметра «This account supports Kerberos AES 256 bit encryption»

- открыть интерфейс командной строки PowerShell и выполнить команду добавления службы для сервисного аккаунта:

```
setspn -A HTTP/disp.termidesk.local service_account
```

где:

`service_account` - наименование сервисного аккаунта;

- для просмотра списка служб сервисного аккаунта можно воспользоваться командой:

```
setspn -L service_account
```

- создать файл `termidesk-msad.keytab` для сервисного аккаунта:

```
ktpass -princ HTTP/disp.termidesk.local@TERMIDESK.LOCAL -mapuser
service_account@TERMIDESK.LOCAL -pass <пароль_сервисного_аккаунта> -ptype
```

```
KRB5_NT_PRINCIPAL -out termidesk-msad.keytab -crypto AES256-SHA1
```

где:

`HTTP/disp.termidesk.local` - указание ранее созданного субъекта-службы;

`service_account@TERMIDESK.LOCAL` - наименование сервисного аккаунта;

`-out termidesk-msad.keytab` - сохранение в файл `termidesk-msad.keytab`;

`-crypto AES256-SHA1` - алгоритм для преобразования `keytab`-файла.

Алгоритм преобразования `keytab`-файла следует выбирать согласно установленным политикам безопасности MS AD.

Полученный файл `termidesk-msad.keytab` следует передать на целевой узел для хранения. Файл может быть сохранен в файловой системе узла Termidesk VDI или в хранилище OpenBao.

Для передачи файла на целевой узел нужно выполнить команду:

```
scp C:\Windows\System32\termidesk-msad.keytab localuser@192.0.2.30:termidesk-
msad.keytab
```

где:

`C:\Windows\System32\termidesk-msad.keytab` - путь к `keytab`-файлу;

`localuser` - имя пользователя целевого узла;

`192.0.2.30` - IP-адрес целевого узла.

После передачи файла необходимо выполнить ряд действий в зависимости от выбранного хранилища.

При хранении файла в файловой системе узла Termidesk VDI:

- переместить файл `termidesk-msad.keytab` в каталог `/etc/opt/termidesk-vdi`:

```
sudo mv /home/user/termidesk-msad.keytab /etc/opt/termidesk-vdi/
```

- сделать владельцем этого файла пользователя `termidesk`:

```
sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/termidesk-msad.keytab
```

- перезапустить службу `termidesk-vdi`:

```
sudo systemctl restart termidesk-vdi
```

При хранении файла в хранилище OpenBao:

- запустить интерпретатор Python:

```
sudo python3
```

- перевести файл в формат base64:

```
import base64 with open('/home/user/termidesk-msad.keytab', 'rb') as file:
keytab_bytes = file.read() keytab_base64 =
base64.b64encode(keytab_bytes).decode('utf-8') keytab_base64
```

где:

`/home/user/termidesk-msad.keytab` - путь к `keytab`-файлу;

- сохранить результат выполнения команды в хранилище OpenBao:

```
bao kv put secret/termidesk/ldap
keytab='BQIAAABGAAIAC1VTVVA0MDcuTEFOAARIVFRQABJ0ZXJtaWRlc2subXlkb21h
aW4AAAABAAAAAAUAFwAQhKQHwhUvWGEJk92QgI/tNA=='
```

где:

`termidesk` - значение переменной `SECRETS_OPENBAO_TERMIDESK_PATH`, заданной в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf`;

`ldap` - путь к хранилищу OpenBao, где следует сохранить результат выполнения команды.

Настройка пользовательской рабочей станции для Kerberos-аутентификации

Для корректной аутентификации пользовательская рабочая станция должна быть введена в соответствующий домен аутентификации Kerberos, используемый в ферме и указанный в портале.

Пользователь не может быть локальным администратором при доступе через Kerberos-аутентификацию.

По умолчанию билет Kerberos выдается автоматически при аутентификации пользователя в системе. Однако, если билет не был выдан автоматически, нужно:

- просмотреть список билетов:

```
klist
```

- получить билет Kerberos:

```
kinit -f termidesk@TERMIDESK.LOCAL
```

где:

`termidesk@TERMIDESK.LOCAL` - учетная запись, для которой запрашивается билет.

Kerberos-аутентификация через веб-браузер требует настройки параметров безопасности в зависимости от используемой ОС и типа браузера.

На пользовательской рабочей станции с ОС Microsoft Windows:

- при использовании веб-браузера, основанного на Chromium, нужно настроить его параметры безопасности для зоны, в которой находится сервер Termidesk VDI. Для этого:
  - перейти «Панель управления - Свойства браузера - Безопасность»;
  - в разделе «Выберите зону для параметры ее параметров безопасности» выбрать зону «Местная интрасеть», нажать экранную кнопку **[Сайты]**;
  - в окне «Местная интрасеть» нажать экранную кнопку **[Дополнительно]**;
  - в поле «Добавить в зону следующий узел» ввести FQDN сервера Termidesk VDI, нажать экранную кнопку **[Добавить]** (см. рисунок Добавление FQDN компонента «Универсальный диспетчер» в зону «Местная интрасеть»);

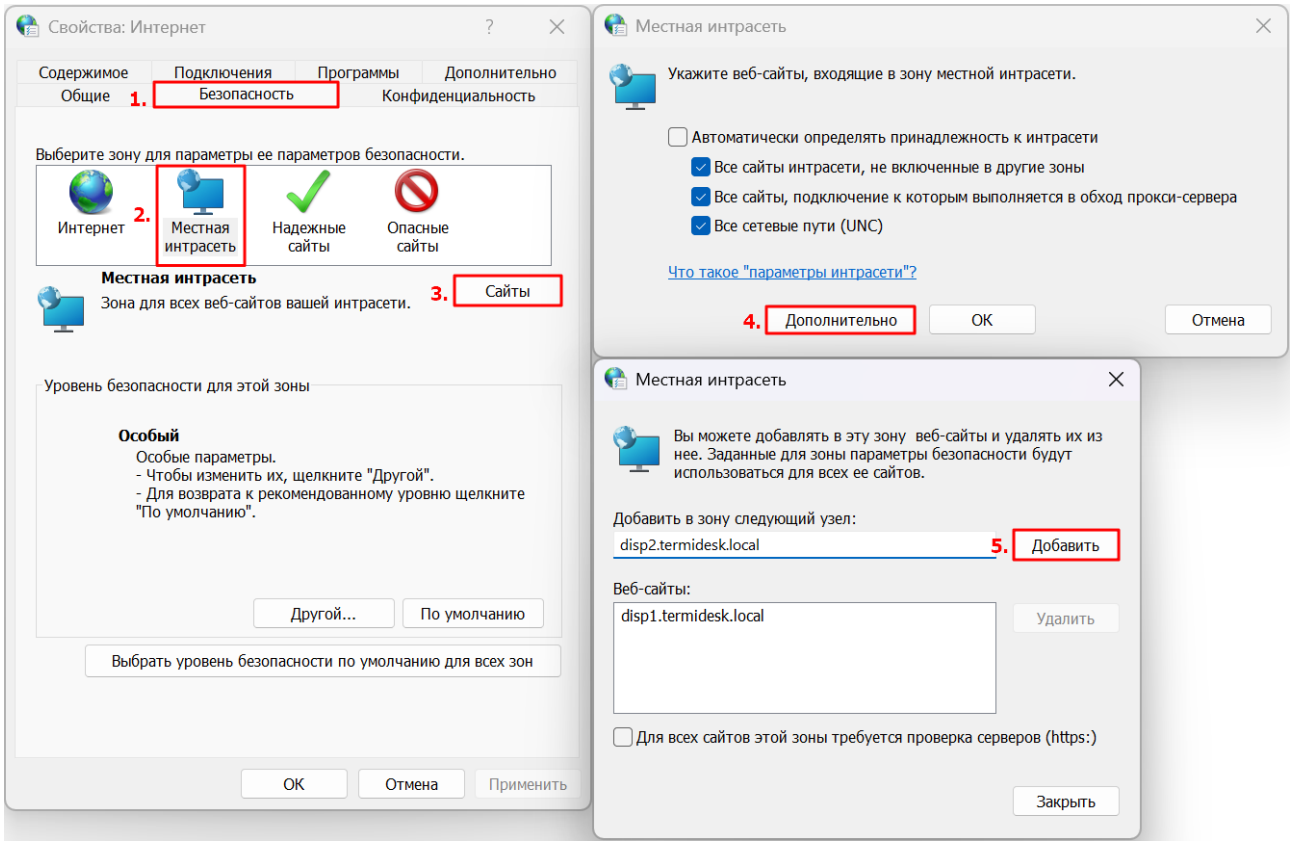


Рисунок 133. Добавление FQDN компонента «Универсальный диспетчер» в зону «Местная интрасеть»

- при использовании в ОС Microsoft Windows веб-браузера Mozilla Firefox нужно:
  - в адресной строке ввести `about:config`;
  - присвоить соответствующие значения параметрам, перечисленным в таблице (см. таблицу Данные для настройки Kerberos-аутентификации через веб-браузер Mozilla Firefox в ОС Microsoft Windows).

Таблица 212. Данные для настройки Kerberos-аутентификации через веб-браузер Mozilla Firefox в ОС Microsoft Windows

Параметр	Значение
network.negotiate-auth.allow-proxies	True
network.negotiate-auth.delegation-uris	.termidesk.local
network.negotiate-auth.trusted-uris	.termidesk.local

На пользовательской рабочей станции с ОС Astra Linux Special Edition:

- для работы технологии единого входа с Kerberos-аутентификацией изменить файл /etc/krb5.conf, добавив в раздел libdefaults параметр forwardable = true:

```
[libdefaults]
forwardable = true
...
```

- для настройки веб-браузера Chromium нужно:
  - в файл /etc/chromium/policies/managed/policies.json добавить строки:

```
{
    "AuthServerAllowlist": "*.termidesk.local" ,
    "AuthNegotiateDelegateAllowlist": "*.termidesk.local"
}
```

    где:

    *.termidesk.local - имя домена, для которого применяется Kerberos-аутентификация;

- для настройки веб-браузера Яндекс.Браузер нужно:
  - создать каталог /etc/opt/yandex/browser/policies/managed:

```
mkdir -p /etc/opt/yandex/browser/policies/managed
```

  - создать файл /etc/opt/yandex/browser/policies/managed/policies.json следующего содержания:

```
{
    "AuthServerAllowlist": "*.termidesk.local",
    "AuthNegotiateDelegateAllowlist": "*.termidesk.local"
}
```

- для настройки веб-браузера Mozilla Firefox нужно:
  - в адресной строке ввести about:config;
  - присвоить соответствующие значения параметрам, перечисленным в таблице (см. таблицу Данные для настройки Kerberos-аутентификации через веб-браузер Mozilla Firefox в ОС Astra Linux Special Edition).

Таблица 213. Данные для настройки Kerberos-аутентификации через веб-браузер Mozilla Firefox в ОС Astra Linux Special Edition

Параметр	Значение
`network.negotiate-auth.allow-proxies`	`True`
`network.negotiate-auth.delegation-uris`	`.termidesk.local`
`network.negotiate-auth.trusted-uris`	`.termidesk.local`

Добавление домена аутентификации OIDC

OpenID Connect (OIDC) - это механизм, позволяющий приложению связаться со службой идентификации (Identity provider, IdP), получить данные о пользователе и вернуть их обратно в приложение. Таким образом, OIDC обеспечивает аутентификацию администраторов и пользователей без необходимости ввода логина и пароля.

Служба идентификации IdP (например, keycloak) должна быть предварительно настроена в инфраструктуре организации для возможности использования OIDC как домена аутентификации.

Поддерживаются следующие типы аутентификации:

- по идентификатору и секрету. В этом случае используются параметры «Client ID» и «Client Secret», заданные в службе идентификации IdP;
- по подписанному JWT-токену. В этом случае используются параметры «Client ID» и «Signed Jwt», заданные в службе идентификации IdP. Закрытый ключ, использующийся для подписи JWT-токена, должен быть загружен на узлы Агрегатора («Агрегатор администратора», «Агрегатор пользователя»).

Для добавления домена аутентификации следует перейти «Системные параметры - Домены аутентификации», а затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «OIDC».

Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления аутентификации через OIDC).

Для сохранения параметров конфигурации нужно использовать экранную кнопку **[Создать]**.

Таблица 214. Данные для добавления аутентификации через OIDC

Параметр	Описание
«Название»	Параметр обязателен для заполнения. Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Параметр обязателен для заполнения. Приоритет использования домена аутентификации при проверке субъекта и его полномочий

Параметр	Описание
«Метка»	Параметр обязателен для заполнения. Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk VDI. Начиная с Termidesk VDI версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)
«Субъекты»	Параметр обязателен для заполнения. Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: • «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на порталах «Агрегатор администратора», «Агрегатор пользователя», «Агрегатор универсальный», и при подключении из компонента «Клиент»; • «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Агрегаторе администратора» или «Агрегаторе универсальном»; • «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Агрегаторе пользователя», «Агрегаторе универсальном» или при подключении пользователя из компонента «Клиент»; • «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала

Параметр	Описание
«Порталы»	Выбор порталов «Агрегатора», для которых будет доступен домен аутентификации. Если портал не выбран, то домен аутентификации не будет доступен для него. В списке доступных значений отображаются все доступные узлы порталов с их полным доменным именем. Администратору нужно выбирать узел в соответствии со значением, указанным в параметре «Субъекты». Примеры: • если в параметре «Субъекты» указано «Пользователи», то в параметре «Порталы» должен быть выбран узел, соответствующий либо «Агрегатору пользователя», либо «Агрегатору универсальному»; • если в параметре «Субъекты» указано «Администраторы и персонал», в параметре «Порталы» должен быть выбран узел, соответствующий либо «Агрегатору администратора», либо «Агрегатору универсальному»; • если в параметре «Субъекты» указано «Все», то в параметре «Порталы» может быть выбран узел, соответствующий либо «Агрегатору пользователя», либо «Агрегатору администратора», либо «Агрегатору универсальному». Значение выбирается исходя из потребностей в разделении доменов аутентификации для того или иного субъекта. При изменении списка узлов: • если узел удален, то он автоматически удалится из списка доступных значений для этого параметра. Уже назначенное значение удалится из свойств домена аутентификации; • если узел добавлен, то он автоматически добавится в список доступных значений для этого параметра, но не будет автоматически выбран для использования. В случае, если в параметре «Порталы» был указан единственный узел, который затем был удален, то этот домен аутентификации не будет доступен ни в каком из порталов. Для выбора всех порталов используется значение «Все»
«Client ID»	Уникальный идентификатор приложения, полученный от службы идентификации IdP. Пример: «openid-test-cl»

Параметр	Описание
«Client secret»	Ключ приложения, полученный от службы идентификации IdP. Параметр должен быть пустым, если задан параметр «Приватный Ключ»
«Приватный ключ»	Путь к закрытому ключу, использующемуся для подписи JWT-токена. Закрытый ключ, используемый в службе идентификации IdP, должен быть добавлен на сервер Termidesk VDI. Для этого: • скопировать его в каталог `/etc/opt/termidesk-vdi/`; • назначить владельцем файла пользователя `termidesk`: `sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.key` Пример: «/etc/opt/termidesk-vdi/client.key»
«Authorization endpoint»	Параметр обязателен для заполнения. URL-адрес авторизации службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/auth»
«Logout endpoint»	Параметр обязателен для заполнения. URL-адрес получения информации о завершении сессии пользователя от службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/logout»
«Token endpoint»	Параметр обязателен для заполнения. URL-адрес получения токена службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/token»
«Userinfo endpoint»	Параметр обязателен для заполнения. URL-адрес получения информации о пользователе от службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/userinfo»
«JWKS URI»	URL-адрес получения сертификатов службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/certs»

Параметр	Описание
«Scope»	Параметр обязателен для заполнения. Набор областей действия, поддерживаемый в службе идентификации IdP. Области действия определяются спецификацией протокола OAuth 2.0. Неполный список возможных значений (указываются через пробел): • «openid» (обязательное значение для OIDC) - запуск аутентификации с использованием OIDC; • «profile» - доступ к профилю пользователя; • «email» - доступ к адресу электронной почты пользователя; • «offline_access» - обновление токена доступа без необходимости повторной аутентификации; • «groups» - доступ к списку ролей пользователя. Значение по умолчанию: «openid email profile groups». Если нужно указать другой набор значений, следует убедиться, что он поддерживается используемой службой идентификации IdP
«Атрибут имени пользователя»	Параметр обязателен для заполнения. Имя атрибута, в котором хранится имя пользователя (логин) в службе идентификации IdP. Значение по умолчанию: «email»
«Проверка SSL»	Проверка использования SSL

Параметр	Описание

«Динамическая проверка членства пользователя в группах»	Управление динамической проверкой вхождения пользователя в группу службы каталогов.
	
	Параметр определяет, как будет происходить проверка нахождения пользователя в группе службы каталогов при аутентификации в Termidesk VDI и получении ресурсов.
	
	Особенности функционирования:
	
	• если пользователю уже назначено РМ, то проверяется вхождение пользователя в группу, указанную в свойствах фонда РМ. Проверка выполняется каждый раз при доступе к ресурсу. При этом если у пользователя отозваны права на доступ, то он:
	  - либо не увидит скрытый ресурс в зависимости от настройки «Скрывать недоступные ресурсы»;
	  - либо увидит, но не сможет получить доступ к нему;
	  - либо получит доступ к назначенному РМ, если права доступа были назначены на другую группу, в которую входит пользователь и которая указана в свойствах фонда РМ;
	  - либо получит доступ к назначенному РМ, если оно назначено на учетную запись пользователя напрямую.
	
	Возможные значения:
	
	• «Режим совместимости 6.0» (по умолчанию) - при аутентификации пользователя происходит запрос к службе каталогов для проверки его вхождения в группы. После этого группы пользователя актуализируются в БД. При попытке получить ресурс из фонда доступ определяется на основе информации из БД (БД не обновляется);
	• «Периодическое обновление» - если пользователя нет в БД и он впервые аутентифицируется, то происходит запрос к службе каталогов для получения актуальной информации о нем. Если пользователь есть в БД, то информация берется из нее. Актуализация пользователей и групп для всех доменов аутентификации с этим значением выполняется периодической фоновой задачей раз в 24 часа;
	• «Динамическая проверка» - при аутентификации пользователя или получении ресурсов происходит запрос к службе каталогов для получения актуальной информации о нем. При обращении к службе каталогов информация о полученных группах кешируется во внутренней памяти. Время кеширования определяется системным параметром «Таймаут кеша хранения групп домена, с»

Добавление домена аутентификации RADIUS

Для добавления домена аутентификации RADIUS администратору Termidesk VDI следует перейти «Системные параметры - Домены аутентификации», затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «RADIUS».

Затем необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления аутентификации Radius).

Таблица 215. Данные для добавления аутентификации Radius

Параметр	Описание
«Название»	Текстовое наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях
«Приоритет»	Преимущество использования домена аутентификации при проверке субъекта и его полномочий. Порядок отображения доменов зависит от приоритета домена и его наименования: • чем ниже приоритет, тем выше домен в списке; • при наличии доменов с одинаковым приоритетом действует сортировка по алфавиту
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk VDI. Начиная с Termidesk VDI версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)
«Субъекты»	Выбор субъектов, для которых будет доступен домен аутентификации. Возможные значения: • «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»; • «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»; • «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»; • «Системные» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала

Параметр	Описание
«Порталы»	Выбор порталов фермы Termidesk VDI, для которых будет доступен домен аутентификации. Если портал не выбран, то домен аутентификации не будет доступен для него. В списке доступных значений отображаются все узлы инфраструктуры с их полным доменным именем. Администратору нужно выбирать узел в соответствии со значением, указанным в параметре «Субъекты». Примеры: • если в параметре «Субъекты» указано «Пользователи», то в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Администраторы и персонал», в параметре «Порталы» должен быть выбран узел, соответствующий либо «Порталу администратора», либо «Порталу универсальному»; • если в параметре «Субъекты» указано «Все», то в параметре «Порталы» может быть выбран узел, соответствующий либо «Порталу пользователя», либо «Порталу администратора», либо «Порталу универсальному». Значение выбирается исходя из потребностей в разделении доменов аутентификации для того или иного субъекта. При изменении списка узлов инфраструктуры: • если узел удален, то он автоматически удалится из списка доступных значений для этого параметра. Уже назначенное значение удалится из свойств домена аутентификации; • если узел добавлен, то он автоматически добавится в список доступных значений для этого параметра, но не будет автоматически выбран для использования. В случае, если в параметре «Порталы» был указан единственный узел, который затем был удален из инфраструктуры, то этот домен аутентификации не будет доступен ни в каком из порталов. Для выбора всех порталов используется значение «Все»

Параметр	Описание
«RADIUS сервер»	IP-адрес или доменное имя ресурса, являющегося источником сведений о субъектах и их полномочиях (сервер RADIUS) Если осуществляется подключение к серверу NPS (Network Policy Server), то доменное имя ресурса нужно указывать заглавными символами.
«Аутентификационный порт»	Порт для обработки запросов на аутентификацию
«Секрет»	Набор символов (пароль), подтверждающий подключение к серверу RADIUS
«NAS-Identifier»	Идентификатор фермы «Агрегатора», используемый при отправке запросов на сервер RADIUS. Значение по умолчанию: «termidesk-server»
«Время ожидания соединения, с»	Максимальное время ожидания (в секундах) для установки соединения
«Регистрозависимость»	Учитывать регистр символов в имени пользователя при аутентификации. Активация параметра позволяет обрабатывать имена пользователей с отличающимся регистром как разные учетные записи. При этом выполняется создание новых учетных записей в интерфейсе Termidesk VDI, а каждому пользователю может быть назначено отдельное РМ. Отключение параметра позволяет обрабатывать имена пользователей с отличающимся регистром как одну учетную запись. При этом создание новых учетных записей в интерфейсе Termidesk VDI не выполняется, а пользователь подключается к одному и тому же РМ. Возможные значения: • «Да» - регистр символов учитывается; • «Нет» (по умолчанию) - регистр символов не учитывается
«Использовать OTP»	Использовать при аутентификации пользователя OTP - механизм, позволяющий применять одноразовые пароли для дополнительной аутентификации. Сервер RADIUS должен быть настроен на аутентификацию пользователей с использованием OTP. Возможные значения: • «Да» - использовать механизм; • «Нет» (по умолчанию) - не использовать механизм

Параметр	Описание
«Режим аутентификации»	Выбор режима, который будет использован при аутентификации пользователя. Для работы функционала нужно активировать параметр «Использовать OTP». На сервере RADIUS должен быть настроен соответствующий режим аутентификации (примеры настроек приведены в подразделе интеграции с системами сайта документации Termidesk VDI: **Примеры параметров конфигурации сервера RADIUS для работы в различных режимах аутентификации**). Возможные значения: • «Одноэтапный (только Access-Request)» (по умолчанию) - пароль и OTP пользователя передаются для проверки одновременно. Проверка учетных данных выполняется за один этап аутентификации; • «Многоэтапный (Access-Request + Access-Challenge)» - пароль и OTP пользователя передаются для проверки последовательно. Проверка учетных данных выполняется за несколько этапов аутентификации

Параметр	Описание

«Динамическая проверка членства пользователя в группах»	Управление динамической проверкой вхождения пользователя в группу службы каталогов.
	
	Параметр определяет, как будет происходить проверка нахождения пользователя в группе службы каталогов при аутентификации в Termidesk VDI и получении ресурсов.
	
	Особенности функционирования:
	
	• если пользователю уже назначено РМ, то проверяется вхождение пользователя в группу, указанную в свойствах фонда РМ. Проверка выполняется каждый раз при доступе к ресурсу. При этом если у пользователя отозваны права на доступ, то он:
	  - либо не увидит скрытый ресурс в зависимости от настройки «Скрывать недоступные ресурсы»;
	  - либо увидит, но не сможет получить доступ к нему;
	  - либо получит доступ к назначенному РМ, если права доступа были назначены на другую группу, в которую входит пользователь и которая указана в свойствах фонда РМ;
	  - либо получит доступ к назначенному РМ, если оно назначено на учетную запись пользователя напрямую.
	
	Возможные значения:
	
	• «Режим совместимости 6.0» (по умолчанию) - при аутентификации пользователя происходит запрос к службе каталогов для проверки его вхождения в группы. После этого группы пользователя актуализируются в БД. При попытке получить ресурс из фонда доступ определяется на основе информации из БД (БД не обновляется);
	• «Периодическое обновление» - если пользователя нет в БД и он впервые аутентифицируется, то происходит запрос к службе каталогов для получения актуальной информации о нем. Если пользователь есть в БД, то информация берется из нее. Актуализация пользователей и групп для всех доменов аутентификации с этим значением выполняется периодической фоновой задачей раз в 24 часа;
	• «Динамическая проверка» - при аутентификации пользователя или получении ресурсов происходит запрос к службе каталогов для получения актуальной информации о нем. При обращении к службе каталогов информация о полученных группах кешируется во внутренней памяти. Время кеширования определяется системным параметром «Таймаут кеша хранения групп домена,с»

Валидация заданных параметров экранной кнопкой **[Тест]** проверяет корректность заданного имени сервера (возможность получить IP-адрес, используя DNS), доступность сервера (корректный порт, работоспособность сервера RADIUS).

После добавления домена аутентификации RADIUS необходимо перейти в созданный объект и указать актуальный список групп, пользователи которых могут производить вход в Termidesk VDI.

При дальнейшей эксплуатации сервер Termidesk VDI, обрабатывая запрос на аутентификацию, получает актуальный список групп пользователя и сравнивает со своей

конфигурацией. Если ни одного совпадения не обнаружено, то пользователю будет отказано в доступе.

Конфигурация сервера RADIUS должна учитывать передачу списка групп пользователя в атрибуте с ключом 25 (Class) в ответе со статусом авторизации.

Для корректного получения списка групп на Termidesk VDI сервер RADIUS может быть настроен следующим образом:

Пример настройки приведен для сервера freeRADIUS.

- файл `/etc/freeradius/3.0/mods-enabled/ldap` должен содержать конструкцию вида:

```
ldap {
...
  update {
     ...
     reply:memberOf                  += 'memberOf'
  }
...
}
```

- в файл `/etc/freeradius/3.0/dictionary` необходимо добавить строку:

```
ATTRIBUTE       memberOf                3001    string
```

- в файле `/etc/freeradius/3.0/sites-enabled/default` необходимо найти секцию `post-auth` и добавить регулярное выражение, фильтрующее название группы из получаемых от сервера атрибутов:

```
foreach &reply:memberOf {
       if ("%{Foreach-Variable-0}" =~ /cn=([^,=]+)/i)
           }
```

- в файле `/etc/freeradius/3.0/mods-enabled/exec` указать для параметра `wait` значение `yes`:

```
wait = yes
```

Для корректной работы автоматического входа пользователя (SSO) нужно настроить конфигурацию сервера RADIUS:

- скорректировать файл `/etc/freeradius/3.0/mods-available/ldap`, добавив фильтр в секции `user`:

```
user {
                base_dn = "${..base_dn}"
```

```
...
                # Фильтр: поиск по sAMAccountName ИЛИ по userPrincipalName (UPN)
                filter = "(|(sAMAccountName=%{%{Stripped-User-Name}:-%{User-
Name}})(userPrincipalName=%{User-Name}))"
...
}
```

- остальные параметры настроить аналогично примеру выше.

Действия над группами в домене аутентификации в «Агрегаторе»

Группы - перечень объектов домена аутентификации, определяющих разрешения пользователей на доступ к фондам РМ. Перечень групп, доступных для добавления, запрашивается «Агрегатором» у домена аутентификации.

Доступны следующие действия над группами домена аутентификации:

- добавление существующей в службе каталогов группы;
- редактирование;
- удаление;
- просмотр сведений таблицы «Группы».

Редактирование и удаление групп в домене аутентификации в веб-портале «Агрегатор администратора» не приводит к каким-либо изменениям объекта в службе каталогов.

Для просмотра списка групп следует перейти «Системные параметры - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне перейти во вкладку «Группы».

Основные параметры списка приведены в таблице.

Таблица 216. Параметры списка групп доменов аутентификации

Параметр	Описание
«Название»	Текстовое наименование группы домена аутентификации
«Тип учетной записи»	Характеристика функции субъекта
«Комментарий»	Информационное сообщение, используемое для описания группы
«Статус»	Характеристика состояния группы

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;

- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Для добавления группы следует перейти «Системные параметры - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне во вкладке «Группы» нажать экранную кнопку **[Добавить]**.

Для добавления группы необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления группы домена аутентификации).

Таблица 217. Данные для добавления группы домена аутентификации

Параметр	Описание

«Название»	Наименование группы.
	
	Для службы каталогов MS AD (LDAP) поддерживаются следующие способы задания группы:
	
	• автоматический поиск через службу каталогов. Для выбора группы из списка доступных нужно начать ввод ее наименования;
	• ввод названия группы вручную:
	  если указывается несуществующая в службе каталогов группа или группа, уже добавленная в «Агрегатор», то будет выведена ошибка;
	  если указывается существующая в службе каталогов группа, то она будет успешно добавлена

«Комментарий»	Информационное сообщение, используемое для описания группы
«Статус»	Характеристика состояния субъектов группы при доступе к «Агрегатору». Доступные значения: • «Активный» - субъекты группы могут аутентифицироваться в портале «Агрегатор администратора» и/или «Агрегатор пользователя»; • «Неактивный» - субъекты группы не могут аутентифицироваться в портале «Агрегатор администратора» и/или «Агрегатор пользователя»
«Тип учетной записи»	Служебные функции субъектов группы при доступе к «Агрегатору». Доступные значения параметра: • «Пользователь» - субъекты группы не будут иметь доступ к порталу «Агрегатор администратора»; • «Администратор» - субъекты группы будут иметь полный доступ к порталу «Агрегатор администратора»
«Роли»	Назначение служебных функций пользователям группы. Доступность выбора значений зависит от параметра «Тип учетной записи» и того, созданы ли роли на странице «Системные параметры - Управление ролями»
«Метагруппа»	Характеристика использования метагруппы. Метагруппа - группа, объединяющая несколько стандартных групп в «Агрегаторе». Рекомендуется не использовать параметр

Параметр	Описание
«Отображать метагруппу»	Характеристика использования метагруппы. Рекомендуется не использовать параметр

Действия над пользователями в домене аутентификации в «Агрегаторе»

Пользователи – перечень объектов, имеющих в рамках домена аутентификации служебные функции на использование объединенных ресурсов. Пользователи будут автоматически добавлены в домен аутентификации после авторизации на сайте «Агрегатора».

Доступны следующие действия над пользователями внутри домена аутентификации:

- редактирование;
- удаление;
- просмотр сведений.

В «Агрегаторе» предусмотрена возможность автоматической регистрации пользователей при запросе опубликованных ресурсов на «Универсальном диспетчере».

Для этого нужно добавить идентичные группы в соответствующих доменах аутентификации «Агрегатора» и «Универсального диспетчера». После входа пользователя на «Агрегатор» и запроса ресурсов с «Универсального диспетчера» его учетная запись будет автоматически зарегистрирована, если он состоит в группах, существующих на «Универсальном диспетчере».

Редактирование и удаление пользователя в домене аутентификации в веб-портале не приводит к каким-либо изменениям объекта в службе каталогов.

«Агрегатор» хранит информацию о назначении прав пользователя в БД, поэтому в случае, если пользователь должен быть исключен из группы администрирования, то необходимо удалить пользователя из группы непосредственно в доменной службе каталогов и на стороне «Агрегатора» одновременно.

Для просмотра списка групп следует перейти «Системные параметры - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне перейти во вкладку «Пользователи».

Основные параметры списка приведены в таблице (см. таблицу Параметры списка пользователей доменов аутентификации).

Таблица 218. Параметры списка пользователей доменов аутентификации

Параметр	Описание
«Имя»	Отображаемое имя пользователя в «Агрегаторе»
«Полное имя»	Имя пользователя, полученное от службы каталогов
«Тип пользователя»	Служебные функции субъекта при доступе к «Агрегатору»
«Комментарий»	Информационное сообщение, используемое для описания пользователя
«Статус»	Характеристика состояния пользователя

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Для редактирования информации о пользователе следует перейти «Системные параметры - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне в таблице «Пользователи» выделить строку с именем пользователя и нажать экранную кнопку **[Изменить]**.

В окне редактирования пользователя доступны данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для редактирования пользователя домена аутентификации).

Таблица 219. Данные для редактирования пользователя домена аутентификации

Параметр	Описание
«Имя»	Отображаемое имя пользователя в «Агрегаторе». Параметр получен автоматически от службы каталогов, его нельзя изменить
«Реальное имя»	Имя пользователя в службе каталогов
«Комментарий»	Информационное сообщение, используемое для описания назначения пользователя
«Статус»	Характеристика состояния пользователя при доступе к «Агрегатору». Возможные значения: • «Активен» - пользователь может аутентифицироваться; • «Неактивен» - пользователь не может аутентифицироваться

Параметр	Описание
«Тип пользователя»	Служебные функции субъекта при доступе к «Агрегатору». Значение наследуется от группы, в которую входит пользователь. При этом по умолчанию тип учетной записи устанавливается в значение с более высоким уровнем прав. Пример: если пользователь одновременно состоит в группе с типом учетной записи «Администратор» и группе с типом «Пользователь», то по умолчанию для пользователя будет установлен тип учетной записи «Администратор». Доступные значения параметра: • «Пользователь» - субъект не будет иметь доступ к «Агрегатору администратора». При выборе этого значения параметр «Роли» будет недоступен; • «Персонал» - субъект будет иметь доступ к странице «Обзор» и будет обладать набором разрешений, определенных служебными функциями. При выборе этого значения в параметре «Роль» можно выбрать одно или несколько значений классов администратора, созданных на странице «Системные параметры - Управление ролями» (см.подраздел **Назначение служебных функций администраторам**); • «Администратор» - субъект будет иметь полный доступ к «Порталу администратора». При выборе этого значения параметр «Роли» будет недоступен
«Группы»	Наименования групп, используемых для определения разрешений по доступу к фондам РМ. Назначение параметра «Группы» будет доступно, если «Тип учетной записи» соответствует «Персонал». Список групп пользователя будет получен автоматически от службы каталогов
«Роли»	Назначение служебной функции указанному пользователю. Доступность выбора значений зависит от параметра «Тип пользователя» и того, созданы ли роли на странице «Системные параметры - Управление ролями». Назначение параметра «Роли» будет доступно, если «Тип пользователя» соответствует «Персонал»

Просмотр данных о пользователе домена аутентификации в «Агрегаторе»

Для просмотра данных о пользователе домена аутентификации следует перейти «Системные параметры - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации.

В открывшемся окне перейти во вкладку «Пользователи» и нажать по ссылке с именем пользователя.

Для просмотра будут доступны таблицы:

- «Группы» - отображает информацию о вхождении пользователя в группы домена аутентификации;
- «Рабочие места» - отображает информацию о списке РМ пользователя;
- «Ассоциированные машины» - отображает информацию о назначенных пользователю машинах;
- «Журнал» - отображает события аудита, связанные с действиями пользователя;
- «Атрибуты» - отображает атрибуты, назначенные для пользователя.

Действия над атрибутами в домене аутентификации в «Агрегаторе»

Для домена аутентификации «Microsoft AD DS/LDAP» поддерживается указание дополнительных атрибутов учетной записи пользователя, заданных в службе каталогов. Функционал предоставляет возможность сопоставлять учетные записи пользователей с различными объектами, например, подразделениями, в которые он входит.

Доступны следующие действия над атрибутами внутри домена аутентификации:

- создание;
- удаление.

Для просмотра списка атрибутов следует перейти «Системные параметры - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне перейти во вкладку «Атрибуты».

Основные параметры списка приведены в таблице (см. таблицу Параметры списка атрибутов домена аутентификации).

Таблица 220. Параметры списка атрибутов домена аутентификации

Параметр	Описание
«Атрибут»	Атрибут учетной записи пользователя из службы каталогов
«Название»	Отображаемое имя атрибута

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Для создания атрибута следует перейти Системные параметры - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне перейти во вкладку «Атрибуты» и нажать экранную кнопку **[Создать]**.

Для добавления атрибута администратору Termidesk VDI необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления атрибута домена аутентификации).

Особенности функционирования:

- получение и сохранение атрибутов пользователя выполняется при первой авторизации;

- срок хранения атрибутов задается параметром «Время хранения дополнительных атрибутов учетной записи пользователей, сут»;
- очистка устаревших атрибутов пользователя производится периодической задачей каждые 24 часа.

Таблица 221. Данные для добавления атрибута домена аутентификации

Параметр	Описание
«Название»	Наименование добавляемого атрибута
«Атрибут»	Атрибут учетной записи пользователя из службы каталогов

АГРЕГАТОР. ФЕРМЫ ПОСТАВЩИКОВ РЕСУРСОВ

Общие сведения о фермах поставщиков ресурсов

Ферма - логическое объединение узлов, взаимодействующих с одной БД.

Ферма поставщиков ресурсов - ферма, объединяющая установку узлов Termidesk VDI. Например, узел «Портал администратора» и узел «Портал пользователя» могут быть объединены в одну ферму поставщиков ресурсов.

Для отображения списка ферм поставщиков ресурсов следует перейти «Инфраструктура - Фермы поставщиков ресурсов». Основные параметры списка приведены в таблице (см. таблицу Параметры списка ферм поставщиков ресурсов).

Таблица 222. Параметры списка ферм поставщиков ресурсов

Параметр	Описание
«Название»	Текстовое наименование фермы
«Комментарий»	Информационное сообщение, используемое для описания фермы
«Шлюз»	Шлюз, используемый в ферме
«Узлы»	Узлы, используемые в ферме
«Транспорт»	Протокол, используемый для подключения к узлу фермы
«Порт»	Порт, используемый для протокола
«Время обхода»	Периодичность (в минутах) опроса фермы
«Группы приоритетов»	Группы пользователей, которым предоставлен приоритетный доступ к ферме
«Статус»	Характеристика состояния фермы. Может быть: • «Активен» - ферма активна и доступна для пользователей; • «Не активен» - ферма неактивна и недоступна для пользователей (не участвует в выдаче ресурсов); • «Техобслуживание» - ферма находится в режиме техобслуживания и недоступная для пользователей Балансировка подключений пользователей происходит только для активных ферм.
«Дата создания»	Временная метка создания фермы
«Дата обновления»	Временная метка обновления фермы

Параметр	Описание
«Теги»	Список тегов, назначенных ферме. При выборе тега выполняется переход к разделу «Системные параметры – Теги» со списком объектов, которым назначен данный тег

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Доступны следующие действия над фермой поставщиков ресурсов:

- редактирование. Для этого нужно пометить ферму и нажать экранную кнопку **[Изменить]**;
- удаление. Для этого нужно пометить ферму и нажать экранную кнопку **[Удалить]**;
- назначение тегов ферме поставщиков ресурсов. Для этого нужно пометить ферму и нажать экранную кнопку **[Теги]**. Общее описание по применению тегов приведено в подразделе **Общие сведения о тегах**.

Добавление фермы поставщиков ресурсов

Для добавления фермы поставщиков ресурсов следует перейти «Инфраструктура - Фермы поставщиков ресурсов», а затем нажать экранную кнопку **[Создать]**.

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления фермы поставщиков ресурсов).

Для сохранения параметров конфигурации нужно нажать экранную кнопку **[Создать]**.

Перед тем, как ферма поставщиков ресурсов будет выдана пользователю, производится проверка наличия в ней свободных ВМ в кеше 1-го и 2-го уровней, а также назначенных пользователю ВМ. Если свободных или назначенных ВМ нет, ферма не отобразится пользователю.

В случае неудачи при аутентификации между «Агрегатором» и «Универсальным диспетчером» фермы, она будет игнорироваться для выдачи пользователю до восстановления работоспособности. Для восстановления работоспособности следует перейти «Системные параметры - Системные настройки», выбрать раздел «Общие» и проверить значение параметра «Заголовок access token».

Для корректного добавления фермы поставщиков ресурсов требуется:

- на узле «Агрегатора» задать ключ подписи JWT-токена для взаимодействия с узлами фермы Termidesk. Ключ может быть задан через файл `termidesk.conf` (параметр `AGGREGATOR_JWT_SSL_KEY`) или через утилиту `termidesk-config`;
- на узлах «Универсального диспетчера» добавляемой фермы задать сертификат для проверки JWT-токена. Сертификат быть задан через файл `termidesk.conf` (параметр `AGGREGATOR_JWT_SSL_CERT`) или через утилиту `termidesk-config`.

Таблица 223. Данные для добавления фермы поставщиков ресурсов

Параметр	Описание
«Название»	Текстовое наименование для добавляемой фермы
«Комментарий»	Информационное сообщение, используемое для описания назначения фермы
«Приоритет»	Приоритет фермы при балансировке подключений. Параметр используется, если при добавлении объединенного набора ресурсов параметру «Балансировка подключений» задано значение «Нет» (см. подраздел **Добавление объединенного набора ресурсов**). По умолчанию «0»
«Длительность обхода (мин)»	Периодичность опроса фермы (в минутах) для подтверждения ее активности. По умолчанию «60» (каждые 60 минут). Пример: пусть параметру «Длительность обхода» задано значение «60», а параметру «Длительность обхода при всех ошибках» задано значение «5». В таком случае, если ферма не пришлет свое состояние в момент опроса (через 60 минут), то через 5 минут, если ферма так и не отправит свое состояние, она будет отмечена неактивной
«Длительность обхода при всех ошибках (мин)»	Продолжительность времени (в минутах), по истечении которого ферма считается неактивной, если она не подтверждает свое активное состояние. По умолчанию «0»
«Максимум неудачных серверов на запрос»	Количество узлов в неактивном состоянии, при превышении которого ферма будет отмечена неактивной. По умолчанию «0»
«Приоритетные группы»	Выбор группы пользователей, которой будет предоставлен приоритетный доступ к данной ферме. Алгоритм работы приоритизации приведен после таблицы. Приоритетных групп может быть несколько, при этом одна группа может быть приоритетной для двух и более ферм. Для восстановления стандартной балансировки подключений необходимо исключить группу из списка приоритетных для фермы

Параметр	Описание
«Транспорт»	Протокол, по которому будет происходить подключение к узлу. Возможные значения: • «HTTP» - незащищенное подключение; • «HTTPS» (по умолчанию) - защищенное подключение
«Порт»	Порт, который будет использоваться при подключении по указанному в параметре «Транспорт» протоколу. При стандартных настройках для протокола HTTP используется порт 80, для протокола HTTPS - 443. По умолчанию «443»
«Шлюз»	Выбор шлюза, через который пользователь будет получать ресурсы. Можно выбрать только одно значение. Шлюз должен быть добавлен через «Управление - Шлюзы» для возможности его выбора в этом параметре
«Балансировать узлы»	Управление режимом балансировки подключений к узлам фермы поставщика ресурсов: • если параметр включен, то балансировка подключений выполняется по алгоритму round-robin; • если параметр выключен, то подключение выполняется последовательно по алгоритму failover: при недоступности выбранного узла выполняется попытка подключения к следующему узлу. По умолчанию параметр включен. Балансировка подключений выполняется только между узлами фермы поставщика ресурсов соответствующей роли: • подключения к «Порталу пользователя» балансируются только между узлами фермы поставщика ресурсов с ролью «Портал пользователя»; • подключения к «Порталу администратора» балансируются только между узлами фермы поставщика ресурсов с ролью «Портал администратора»
«Техобслуживание»	Управление режимом техобслуживания фермы. При активации параметра ферма не участвует в выдаче ресурсов, становятся неактивными все узлы, входящие в нее (такие узлы не участвуют в механизме балансировки). Балансировка подключений пользователей происходит только для активных узлов фермы. Режим техобслуживания - это запрет пользователям подключаться к ферме. Этот режим предназначен для проведения плановых регламентных или аварийных работ

Параметр	Описание
«Проверять SSL»	Управление проверкой валидности SSL-сертификата. Параметр необходимо выключить в случае, если проверку валидности пройти не удается: • на узлах фермы используются самоподписанные сертификаты; • или на узлах фермы используются сертификаты, выпущенные центром сертификации, корневой сертификат которого не добавлен в список доверенных на узле «Агрегатора». По умолчанию проверка валидности сертификатов выключена
«Использовать mTLS»	Управление использованием mTLS для взаимной аутентификации с фермой. Для корректной работы потребуется задать клиентские сертификаты и ключ в параметрах `MTLS_CLIENT_CERT`, `MTLS_CLIENT_KEY`, `MTLS_CLIENT_CA` конфигурационного файла `termidesk.conf`. Дополнительная настройка веб-сервера Apache на узле «Агрегатора» не требуется

При запросе ресурса пользователем подходящая ферма будет выбрана по следующему алгоритму:

- если есть приоритетные группы для ферм, то пользователь получит ресурс от одной из них, исходя из правил:
  - сначала будут выданы те фермы, в которых имеется активная сессия пользователя (статус «in_use»);
  - затем будут выданы те фермы, в которых имеется назначенная пользователю сессия (статус «has_assigned»);
  - если пункты выше не выполнены, то действует общий приоритет, исходя из правил объединения набора ресурсов;
- если приоритетных групп для ферм нет, то пользователь получит ресурс, исходя из правил:
  - сначала будут выданы те фермы, в которых имеется активная сессия пользователя (статус «in_use»);
  - затем будут выданы те фермы, в которых имеется назначенная пользователю сессия (статус «has_assigned»);
  - если пункты выше не выполнены, то действует общий приоритет, исходя из правил объединения набора ресурсов;
- если пользователь ранее уже работал с приоритетной фермой, то он получит ресурс от нее. Поведение настраивается при создании «Сайта» (параметр «Приоритет ресурса»).

Пример для третьего сценария:

- пользователь подключился к приоритетной ферме и получил ресурс от нее, ресурсу назначены статусы «in_use» или «has_assigned»;
- доступ к приоритетной ферме прекратился, например, из-за выхода из строя всей фермы;
- пользователь получил ресурс из неприоритетной фермы, ресурсу назначены статусы «in_use» или «has_assigned»;
- в какой-то момент приоритетная ферма вновь заработала и стала

доступна.

В этом случае после переподключения пользователя к «Агрегатору» он вновь получит доступ к приоритетной ферме и ресурс из нее, если параметру «Приоритет ресурса» задано значение «Приоритетные фермы».

АГРЕГАТОР. УЗЛЫ ФЕРМ ПОСТАВЩИКОВ РЕСУРСОВ

Общие сведения об узлах

Узел - аппаратный или виртуальный сервер компонента «Универсальный диспетчер».

Несколько узлов, взаимодействующих с единой БД, объединяются в одну ферму поставщиков ресурсов.

Для отображения списка узлов следует перейти «Инфраструктура - Узлы». Основные параметры списка приведены в таблице (см. таблицу Параметры списка узлов).

Таблица 224. Параметры списка узлов

Параметр	Описание
«Название»	Текстовое наименование узла
«Хост»	IP-адрес или FQDN узла
«Токен»	Токен доступа к API узла
«Статус»	Характеристика состояния узла. Может быть: • «Активен» - узел активен и доступен для пользователей; • «Не активен» - узел неактивен и недоступен для пользователей (не участвует в выдаче ресурсов); • «Техобслуживание» - узел находится в режиме техобслуживания и недоступен для пользователей Балансировка подключений пользователей происходит только для активных узлов.
«Дата создания»	Временная метка создания узла
«Дата обновления»	Временная метка обновления узла
«Теги»	Список тегов, назначенных узлу. При выборе тега выполняется переход к разделу «Системные параметры – Теги» со списком объектов, которым назначен данный тег

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует

воспользоваться экранной кнопкой **[Сбросить]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;

- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Отредактировать информацию об узле можно двумя способами:

- перейти «Инфраструктура - Фермы поставщиков ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование фермы. В открывшемся окне «Узлы фермы» нажать экранную кнопку **[Изменить]**;
- перейти «Инфраструктура - Узлы», затем выбрать необходимый узел и нажать на экранную кнопку **[Изменить]**.

Удалить узел можно двумя способами:

- перейти «Инфраструктура - Фермы поставщиков ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование фермы. В открывшемся окне «Узлы фермы» нажать экранную кнопку **[Удалить]**;
- перейти «Инфраструктура - Узлы», затем выбрать необходимый узел и нажать на экранную кнопку **[Удалить]**.

Для назначения тега узлу следует перейти «Инфраструктура - Узлы», затем выбрать необходимый узел и нажать на экранную кнопку **[Теги]**. Общее описание по применению тегов приведено в подразделе **Общие сведения о тегах**.

Добавление узла Termidesk

Для добавления узла Termidesk VDI следует перейти «Инфраструктура - Фермы поставщиков ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование фермы. В открывшемся окне «Узлы фермы» нажать экранную кнопку **[Добавить узел]**.

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления узла Termidesk VDI).

Для сохранения параметров конфигурации нужно использовать экранную кнопку **[Добавить]**. При сохранении будет запрошена проверка состояния `healthcheck` и узел будет сохранен, если он существует и ответил на запрос.

Для просмотра всех добавленных узлов с привязкой к ферме поставщиков ресурсов следует перейти «Инфраструктура - Узлы».

> Узлы, которые по каким-то причинам вышли из строя и перестали отвечать на запрос проверки состояния `healthcheck`, автоматически будут помечены как неактивные и не будут участвовать в балансировке подключений и выдаче ресурсов пользователю.
>
> Если узел вновь ответил на запрос проверки состояния `healthcheck`, его состояние изменится на активное.

Таблица 225. Данные для добавления узла Termidesk VDI

Параметр	Описание
«Название»	Текстовое наименование добавляемого узла

Параметр	Описание
«Хост»	IP-адрес или FQDN сервер с установленным компонентом «Универсальный диспетчер»
«Токен авторизации»	Токен для доступа к API добавляемого узла. Значение параметра может быть получено из переменной `HEALTH_CHECK_ACCESS_KEY`, определенной в конфигурационном файле `termidesk.conf` узла «Универсального диспетчера»
«Тип портала»	Роль компонента «Универсальный диспетчер», установленная на добавляемом узле. Параметр влияет на то, с какими API-запросами сможет работать «Агрегатор». Возможные значения: • «Администратора» - узел с ролью «Портал администратора». Доступны только API-запросы для администрирования; • «Пользователя» - узел с ролью «Портал пользователя». Доступны только API-запросы для получения ресурсов; • «Универсальный» - узел с ролью «Портал универсальный». Доступен весь пул API-запросов. Механизм определения типа портала отличается в зависимости от версии добавляемого узла: • если добавляется компонент «Универсальный диспетчер» Termidesk VDI версии 6.0 и выше, то тип автоматически меняется в зависимости от настроек на добавляемом узле. Изменение происходит также при периодическом опросе состояния узлов: если узел изменил свою роль, то тип также автоматически изменится; • если добавляется компонент «Универсальный диспетчер» Termidesk VDI версии 5.1, то администратор должен вручную добавить тип. Это требует осторожности! Консоль управления фермами может работать только с узлами роли «Портал администратора», а получение ресурсов через «Агрегатор» возможно только от узлов с ролью «Портал пользователя». Пример: добавлен узел с ролью «Портал администратора», для него выбран соответствующий тип - портал «Администратора». В этом случае при подключении через «Клиент» пользователю не будут отображены ресурсы с этого узла.

Параметр	Описание
«Техобслуживание»	Управление режимом техобслуживания узла. Балансировка подключений пользователей происходит только для активных узлов фермы. Режим техобслуживания - это запрет пользователям подключаться к узлу. Этот режим предназначен для проведения плановых регламентных или аварийных работ
«Путь к публичному ключу ws-proxy узла»	Путь к публичному ключу для взаимодействия со шлюзом. Параметр требуется указывать, если в ферме «Агрегатора» используется шлюз. Ключ должен быть получен из узла фермы Termidesk VDI (узла «Универсального диспетчера», файл `id_rsa.pub` по умолчанию расположен в `/etc/opt/termidesk-vdi/wsproxy`) и добавлен: • либо в файловую систему узла «Агрегатора»; • либо в хранилище чувствительной информации

АГРЕГАТОР. САЙТЫ

Общие сведения о сайтах

Сайт - физическая площадка, на которой может быть развернута одна или несколько ферм. Сайт объединяет одну или несколько добавленных ферм и является единой точкой входа для получения ресурсов пользователями.

Обязательным условием для использования сайта является создание объединенного набора ресурсов, представляющего собой правила, при которых сайт функционирует. Если не будет создан объединенный набор ресурсов или он будет неактивен, сайт будет недоступен для пользователей.

Для отображения списка сайтов следует перейти «Управление - Сайты».

Основные параметры списка приведены в таблице (см. таблицу Параметры списка сайтов).

Таблица 226. Параметры списка сайтов

Параметр	Описание
«Название»	Текстовое наименование сайта
«Комментарий»	Информационное сообщение, используемое для описания фермы
«URI»	Адрес начальной страницы для входа на сайт
«Группы пользователей»	Количество групп пользователей домена аутентификации, которые могут аутентифицироваться на сайте
«Фермы»	Перечень ферм, используемых для сайта
«Активен»	Статус сайта. Статус будет активен (зеленая галочка), если у сайта активен хотя бы один объединенный набор ресурсов

Параметр	Описание
«Техобслуживание»	Характеристика состояния техобслуживания сайта
«Шаблоны техобслуживания»	Наименование шаблона техобслуживания, используемого для сайта
«Теги»	Список тегов, назначенных сайту. При выборе тега выполняется переход к разделу «Системные параметры – Теги» со списком объектов, которым назначен данный тег

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Доступны следующие действия над сайтом:

- редактирование. Для этого нужно пометить сайт и нажать на экранную кнопку **[Изменить]**;
- удаление. Для этого нужно пометить сайт и нажать на экранную кнопку **[Удалить]**;
- назначение тегов сайту. Для этого нужно пометить сайт и нажать экранную кнопку **[Теги]**. Общее описание по применению тегов приведено в подразделе **Общие сведения о тегах**.

Добавление сайта

Для добавления сайта следует перейти «Управление - Сайты», а затем нажать экранную кнопку **[Создать]**.

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления сайта).

Для сохранения параметров конфигурации нужно использовать экранную кнопку **[Создать]**.

Таблица 227. Данные для добавления сайта

Параметр	Описание
«Название»	Параметр обязателен для заполнения. Текстовое наименование добавляемого сайта. Наименование может содержать только буквы латинского алфавита, цифры, знаки «-» (дефис)
«Комментарий»	Информационное сообщение, используемое для описания назначения сайта
«URI»	Параметр обязателен для заполнения. Адрес начальной страницы для входа на сайт
«Домены аутентификации»	Параметр обязателен для заполнения. Выбор домена или доменов аутентификации, пользователи которого смогут аутентифицироваться на сайте. Домен аутентификации должен быть добавлен через «Системные параметры - Домены аутентификации» для возможности его выбора в этом параметре. Для удобства нахождения домена аутентификации можно воспользоваться формой поиска, расположенной в верхней части выпадающего блока параметра «Домены аутентификации»
«Группы пользователей»	Выбор группы или групп пользователей домена аутентификации, которые могут аутентифицироваться на сайте. Группы пользователей должны быть добавлены в домене аутентификации («Системные параметры - Домены аутентификации») для возможности их выбора в этом параметре. Список групп пользователей будет отображен после выбора домена в параметре «Домен аутентификации»
«Пользователи»	Выбор пользователей, которые могут аутентифицироваться на сайте. Пользователи должны быть добавлены в домене аутентификации («Системные параметры - Домены аутентификации») для возможности их выбора в этом параметре. Список пользователей будет отображен после выбора домена в параметре «Домен аутентификации». Для удобства нахождения пользователя можно воспользоваться формой поиска, расположенной в верхней части выпадающего блока параметра «Пользователи»

Параметр	Описание
«Фермы поставщиков ресурсов»	Параметр обязателен для заполнения. Выбор фермы или ферм, для которых будет создан сайт. Фермы поставщиков ресурсов должны быть добавлены через «Инфраструктура - Фермы поставщиков ресурсов» для возможности их выбора в этом параметре
«Техобслуживание»	Управление режимом техобслуживания сайта. Режим техобслуживания - это запрет пользователям подключаться к сайту. Этот режим предназначен для проведения плановых регламентных или аварийных работ
«Шаблон техобслуживания»	Выбор ранее созданного шаблона, текст из которого будет выведен пользователю при попытке подключиться к сайту, находящемуся в режиме техобслуживания. Создание шаблона приведено в подразделе **Шаблоны техобслуживания**
«Переподключаться при обрыве связи»	Параметр обязателен для заполнения. Управление режимом восстановления подключения. Возможные значения: • «Не переподключаться» (по умолчанию) - попытки восстановления связи выполняться не будут. При потере соединения подключение к РМ останавливается и не возобновляется; • «5» - при потере соединения выполняются 5 попыток для восстановления подключения; • «10» - при потере соединения выполняются 10 попыток для восстановления подключения; • «30» - при потере соединения выполняются 30 попыток для восстановления подключения; • «Не задано» - выбор режима будет задан пользователем в интерфейсе «Клиента»
«Разрешить сохранение имени пользователя в клиенте»	Управление параметром сохранения имени пользователя в компоненте «Клиент» при подключении к «Агрегатору». По умолчанию параметр не активирован

Параметр	Описание
«Сохранять пароль пользователя»	Сохранение пароля пользователя в компоненте «Клиент» при подключении к «Агрегатору». Если параметр: • активирован, то пароль, ранее введенный пользователем при подключении к «Агрегатору», будет сохранен в конфигурационном файле компонента «Клиент»; • не активирован, то пароль, ранее введенный пользователем при подключении к «Агрегатору», не будет храниться в конфигурационном файле компонента «Клиент». Влияние параметров сохранения пароля в различных сценариях приведено в таблице ниже (см. таблицу Влияние параметров, управляющих сохранением пароля или PIN-кода). По умолчанию параметр не активирован
«Использовать введённый пароль для подключения к РМ»	Сохранение пароля, введенного пользователем при подключении к «Агрегатору», в оперативной памяти для дальнейшего подключения к РМ. Если параметр: • активирован, то пароль, ранее введенный пользователем при подключении к «Агрегатору», будет использован для дальнейшего подключения к РМ; • не активирован, то пароль, ранее введенный пользователем при подключении к «Агрегатору», не будет храниться и при подключении к РМ потребуется его ввести. Влияние параметров сохранения пароля в различных сценариях приведено в таблице ниже (см. таблицу Влияние параметров, управляющих сохранением пароля или PIN-кода). По умолчанию параметр активирован

Параметр	Описание
«Использовать введённый PIN для подключения к РМ»	Сохранение PIN-кода смарт-карты, введенного пользователем при подключении к «Агрегатору», в оперативной памяти для дальнейшего подключения к РМ. Если параметр: • активирован, то PIN-код, ранее введенный пользователем при подключении к «Агрегатору», будет использован для дальнейшего подключения к РМ; • не активирован, то PIN-код, ранее введенный пользователем при подключении к «Агрегатору», не будет храниться и при подключении к РМ потребуется его ввести. Влияние параметров сохранения PIN-кода в различных сценариях приведено в таблице ниже (см. таблицу Влияние параметров, управляющих сохранением пароля или PIN-кода). По умолчанию параметр активирован
«Скрывать недоступные ресурсы»	Управление сокрытием недоступных ресурсов при подключении пользователя к «Агрегатору». Недоступность ресурса определяется его статусом, при этом пользователю в интерфейсе «Клиента» отображается причина недоступности. Если параметр: • активирован, то недоступные ресурсы не будут отображаться пользователю; • не активирован, то недоступные ресурсы будут отображены пользователю, но он не сможет к ним подключиться. По умолчанию параметр активирован
«Активировать управление перемещением сеансов»	Форсировать управление режимом повторного подключения пользователя. При активации параметра пользователь не сможет самостоятельно изменить настройку повторного подключения в интерфейсе «Клиента». Значение параметра применяется ко всем фермам поставщиков ресурсов и имеет приоритет над их настройками. Возможные значения: • «Да» (по умолчанию)- переподключение пользователя будет форсировано со стороны «Агрегатора»; • «Нет» - переподключение пользователя будет управляться в интерфейсе «Клиента». При выборе этого значения в параметре «Использовать перемещение сеансов» будет всегда использоваться «Не назначено»

Параметр	Описание
«Использовать перемещение сеансов»	Использование возможно при активации параметра «Активировать управление перемещением сеансов». Значение параметра применяется ко всем фермам поставщиков ресурсов и имеет приоритет над их настройками. Управление повторным подключением пользователя к отключенным и активным сеансам. Функционал позволяет восстанавливать подключение после разрыва соединения или смены устройства (пользовательской рабочей станции). Таким образом пользователь сможет получить тот же сеанс, с которым работал ранее, не теряя прогресс работы. Возможные значения: • «Не назначено» - выбор режима будет задан пользователем в интерфейсе «Клиента»; • «Запрещено» - повторное переподключение не используется; • «Повторно подключаться к активным и отключенным сеансам» (по умолчанию). В этом случае при переподключении сначала будет произведена процедура отключения активного сеанса пользователя, после которой он будет повторно подключен к отключенному сеансу; • «Повторно подключаться только к отключенным сеансам». В этом случае переподключение пользователя будет происходить только к отключенным сеансам
«Повторно подключаться к сеансам при аутентификации»	Использование возможно при активации параметра «Активировать управление перемещением сеансов». Значение параметра применяется ко всем фермам поставщиков ресурсов и имеет приоритет над их настройками. Параметр определяет режим повторного подключения к ресурсам при активации параметра «Активировать управление перемещением сеансов». Возможные значения: • «Да» (по умолчанию) - переподключение будет происходить при аутентификации пользователя через «Клиент»; • «Нет» - переподключение не будет происходить при аутентификации пользователя

Параметр	Описание
«Повторно подключаться к сеансам при обновлении списка приложений»	Использование возможно при активации параметра «Активировать управление перемещением сеансов». Значение параметра применяется ко всем фермам поставщиков ресурсов и имеет приоритет над их настройками. Параметр определяет режим повторного подключения к ресурсам при активации параметра «Активировать управление перемещением сеансов». Возможные значения: • «Да» - переподключение будет происходить при обновлении списка ресурсов; • «Нет» (по умолчанию) - переподключение не будет происходить при обновлении списка ресурсов
«Разрешать изменение адреса подключения в клиенте»	Управление возможностью изменения адреса подключения к «Агрегатору» в интерфейсе «Клиента». Значение параметра применяется ко всем фермам поставщиков ресурсов и имеет приоритет над их настройками. Если параметр: • активирован, то пользователь может изменять адрес подключения к «Агрегатору»; • не активирован, то пользователь не может изменять адрес подключения к «Агрегатору». По умолчанию параметр активирован
«Автоматическое обновление пользовательских ресурсов»	Управление возможностью автоматического обновления списка ферм поставщиков ресурсов. Если параметр: • активирован, то обновление списка ферм поставщиков ресурсов выполняется автоматически; • не активирован, то обновление списка ферм поставщиков ресурсов не выполняется. По умолчанию параметр не активирован
«Периодичность фонового обновления списка приложений, с»	Параметр определяет периодичность (в секундах), с которой будет происходить обновление списка ресурсов в интерфейсе «Клиента». Возможные значения: от 60 до 28800. Значение по умолчанию: «300»

Параметр	Описание
«Обновлять список ресурсов при каждом запуске ресурса»	Управление режимом обновления списка ресурсов. Возможные значения: • «Не задано» - выбор режима будет задан пользователем в интерфейсе «Клиента»; • «Включено» - обновление списка ресурсов будет происходить при запуске какого-либо ресурса пользователем; • «Выключено» (по умолчанию) - обновление списка ресурсов не будет происходить при запуске какого-либо ресурса пользователем
«Приоритет ресурса»	Управление режимом выдачи ресурса. Параметр определяет, ресурс из какой фермы будет предоставлен пользователю, если он считается используемым на нескольких фермах сразу. Пример: • пользователь подключился к приоритетной ферме и получил ресурс от нее, ресурсу назначены статусы «in_use» или «has_assigned»; • доступ к приоритетной ферме прекратился, например, из-за выхода из строя всей фермы; • пользователь получил ресурс из неприоритетной фермы, ресурсу назначены статусы «in_use» или «has_assigned»; • в какой-то момент приоритетная ферма вновь заработала и стала доступна. В этом случае, если параметру «Приоритет ресурса» задано значение «Приоритетные фермы», то после переподключения пользователя к «Агрегатору» он вновь получит доступ к приоритетной ферме и ресурс из нее. Возможные значения: • «Используемые ресурсы» (по умолчанию) - ресурс будет выдан из любой фермы, в которой он уже используется (статус «in_use»); • «Приоритетные фермы» - ресурс будет получен у приоритетной фермы, в которой пользователь ранее его получил
«Интервал обновления (минуты)»	Периодичность (в минутах), с которой будет происходить автоматическое обновление списка ферм поставщиков ресурсов при активации параметра «Автоматическое обновление пользовательских ресурсов». Возможные значения: от 1 до 2147483647. Значение по умолчанию: «15»

Параметр	Описание
«Соединение по RDP через Termidesk Viewer»	Управление режимом использования ПО Termidesk Viewer при подключении к РМ по протоколу RDP. Возможные значения: • «Не задано» - выбор режима будет задан пользователем в интерфейсе «Клиента». При подключении пользователя из веб-браузера используется встроенный веб-клиент Termidesk Web Viewer, использование сторонних программ настраивается через конфигурационный файл «Клиента» (`Termidesk Client.ini`); • «Включено» (по умолчанию) - при подключении к РМ по протоколу RDP будет использоваться ПО Termidesk Viewer; • «Выключено» - при подключении к РМ по протоколу RDP будут использоваться системные программы доставки РМ (`mstsc.exe`, `xfreerdp`)

В таблице приняты обозначения:

- параметр 1 - «Использовать введённый пароль для подключения к РМ»;
- параметр 2 - «Использовать введённый PIN для подключения к РМ»;
- параметр 3 - «Сохранять пароль пользователя»;
- политика SSO - политика «Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)».

Таблица 228. Влияние параметров, управляющих сохранением пароля или PIN-кода

Параметр 1	Параметр 2	Параметр 3	Политика SSO	Результат подключения к РМ
Активирован	Активирован	Активирован	«Включен»	Выполняется SSO. Используется пароль, введенный пользователем при подключении
Активирован	Активирован	Активирован	«Выключен»	По требованию политики запрашивается пароль
Активирован	Активирован	Не активирован	«Включен»	Выполняется SSO. Используется пароль, введенный пользователем при подключении
Активирован	Активирован	Не активирован	«Выключен»	По требованию политики запрашивается пароль
Не активирован	Не активирован	Активирован	«Включен»	В отдельном окне запрашивается пароль, на этапе входа в ОС выполняется SSO
Не активирован	Не активирован	Активирован	«Выключен»	В отдельном окне запрашивается пароль, на этапе входа в ОС по требованию политики снова запрашивается пароль
Не активирован	Не активирован	Не активирован	«Включен»	В отдельном окне запрашивается пароль, на этапе входа в ОС выполняется SSO
Не активирован	Не активирован	Не активирован	«Выключен»	По требованию политики запрашивается пароль на этапе входа в ОС

Добавление объединенного набора ресурсов

Для добавления объединенного набора ресурсов следует перейти «Управление - Сайты», затем в столбце «Название» сводной таблицы нажать на наименование сайта. На открывшейся странице нажать экранную кнопку **[Добавить]**.

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления объединенного набора ресурсов).

Для сохранения параметров конфигурации нужно использовать экранную кнопку **[Добавить]**.

Таблица 229. Данные для добавления объединенного набора ресурсов

Параметр	Описание
«Название»	Текстовое наименование добавляемого объединенного набора ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения объединенного набора ресурсов
«Приоритет»	Приоритет набора для формирования ресурсов. Параметр влияет на выбор правила, которое будет применено для формирования ресурсов
«Фермы»	Выбор фермы или ферм, для которых будут действовать правила объединенного набора ресурсов
«Публикуются идентичные ресурсы»	Характеристика публикуемых ресурсов: • «Да» - все наборы ресурсов, опубликованные на фермах, идентичны; • «Нет» - наборы ресурсов, опубликованные на фермах, неидентичны. Параметр определяет, будет ли «Агрегатор» опрашивать каждую ферму для получения всех ресурсов: • если отмечено, что все ресурсы идентичны на указанных фермах, ресурсы будут получены только от одной фермы; • если ресурсы неидентичны на фермах, они будут получены от каждой из ферм. «Агрегатор» не проверяет, действительно ли все ресурсы на указанных фермах идентичны - это подтверждает администратор через указанный параметр Особенности работы: • если для пользователя в ферме доступны все ресурсы, то они будут выданы именно с этой фермы; • если в ферме есть недоступные пользователю ресурсы, то «Агрегатор» обратится к следующей ферме и попытается получить недостающие ресурсы. Как только список доступных ресурсов будет сформирован, он будет выдан пользователю
«Балансировка подключений»	Характеристика активации балансировки подключений: • «Да» - подключения балансируются по схеме least-connection; • «Нет» - подключения балансируются на первую доступную ферму по схеме first-host. Приоритет фермы в списке балансировки задается при добавлении фермы поставщиков ресурсов (см. подраздел **Добавление фермы поставщиков ресурсов**)

Параметр	Описание
«Активен»	Характеристика состояния объединенного набора ресурсов: • «Да» - объединенный набор ресурсов активен и доступен для пользователей; • «Нет» - объединенный набор ресурсов неактивен и недоступен для пользователей

АГРЕГАТОР. ШАБЛОНЫ ТЕХОБСЛУЖИВАНИЯ

Общие сведения о шаблонах техобслуживания

Шаблон техобслуживания определяет текст сообщения, отправляемого пользователю при попытке подключиться к сайту, находящемуся в режиме техобслуживания.

Для отображения списка шаблонов техобслуживания следует перейти «Управление - Шаблоны техобслуживания». Основные параметры списка приведены в таблице (см. таблицу Параметры списка шаблонов техобслуживания).

Таблица 230. Параметры списка шаблонов техобслуживания

Параметр	Описание
«Название»	Текстовое наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания шаблона
«Сообщение»	Сообщение, используемое в шаблоне
«Дата создания»	Временная метка создания шаблона

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Созданный шаблон техобслуживания можно:

- редактировать, для этого нужно пометить шаблон и нажать на экранную кнопку **[Изменить]**;
- удалить, для этого нужно пометить шаблон и нажать на экранную кнопку **[Удалить]**.

Добавление шаблона техобслуживания

Для добавления шаблона следует перейти «Управление - Шаблоны техобслуживания», затем нажать экранную кнопку **[Создать]**.

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шаблона техобслуживания).

Для сохранения параметров конфигурации нужно нажать экранную кнопку **[Создать]**.

Таблица 231. Данные для добавления шаблона техобслуживания

Параметр	Описание
«Название»	Параметр обязателен для заполнения. Текстовое наименование добавляемого шаблона
«Комментарий»	Информационное сообщение, используемое для описания назначения шаблона
«Сообщение»	Параметр обязателен для заполнения. Текст сообщения, которое будет отображено пользователю

АГРЕГАТОР. ШЛЮЗЫ

Общие сведения по использованию шлюза

Шлюз - аппаратный или виртуальный сервер, отвечающий за туннелирование трафика и обеспечивающий отделение внутренней локальной сети организации от внешних локальных или глобальных сетей. Шлюз в «Агрегаторе» - это абстракция, позволяющая добавить существующий шлюз в качестве объекта для взаимодействия с ним.

Использование шлюза делает доступным сценарий, при котором пользователь запрашивает ресурсы, доступ к которым не осуществляется напрямую.

Типовой сценарий для использования шлюза:

- в сетевой инфраструктуре организации существует сегмент, скрытый от внешних подключений;
- в указанном сегменте развернута ферма поставщиков ресурсов, в которой используется сервер с компонентом «Шлюз» для туннелирования протоколов доставки;
- в другом сегменте сетевой инфраструктуры организации развернут «Агрегатор».

В таком сценарии целесообразно в одном сегменте с «Агрегатором» установить еще один сервер со шлюзом (шлюз «Агрегатора»), адрес которого будет подставлен в параметрах подключения к ресурсу, отдаваемых пользователю, вместо адреса шлюза фермы поставщиков ресурсов.

Для отображения списка шлюзов следует перейти «Управление - Шлюзы». Основные параметры списка приведены в таблице (см. таблицу Параметры списка шлюзов).

Таблица 232. Параметры списка шлюзов

Параметр	Описание
«Название»	Текстовое наименование шлюза
«URL»	Адрес шлюза, обеспечивающего формирование и поддержание соединения

Параметр	Описание
«Теги»	Список тегов, назначенных шлюзу. При выборе тега выполняется переход к разделу «Системные параметры – Теги» со списком объектов, которым назначен данный тег

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Доступны следующие действия над шлюзом:

- редактирование. Для этого нужно пометить шлюз и нажать на экранную кнопку **[Изменить]**;
- удаление. Для этого нужно пометить шлюз и нажать на экранную кнопку **[Удалить]**;
- назначение тегов шлюзу. Для этого нужно пометить шлюз и нажать экранную кнопку **[Теги]**. Общее описание по применению тегов приведено в подразделе **Общие сведения о тегах**.

Добавление шлюза

Для добавления шлюза следует перейти «Управление - Шлюзы», а затем нажать экранную кнопку **[Создать]**.

Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления шлюза).

Для сохранения параметров конфигурации нужно нажать экранную кнопку **[Создать]**.

Таблица 233. Данные для добавления шлюза

Параметр	Описание
«Название»	Текстовое наименование добавляемого шлюза

Параметр	Описание
«URL»	Адрес узла шлюза, обеспечивающего формирование и поддержание соединения, заданный в формате: • ws(s)://<IP-адрес_или_доменное_имя>:<порт>; • или ws(s)://<IP-адрес_или_доменное_имя>/<путь>. Протокол WS (WebSocket) используется, если шлюз не настроен на защищенное соединение. Протокол WSS используется, если выполняется защищенное подключение к шлюзу. Пример: «wss://termidesk.loc/websockify»

АГРЕГАТОР. ТЕГИ

Общие сведения о тегах

Теги предназначены для классификации объектов «Агрегатора» и упрощения их поиска и управления.

Созданный тег может быть назначен следующим объектам:

- фермам поставщиков ресурсов;
- узлам фермы поставщиков ресурсов;
- сайтам;
- шлюзам;
- доменам аутентификации;
- фондам РМ;
- индивидуальным РМ.

Существующие ограничения:

- в наименовании тегов допускается указывать прописные и строчные буквы, цифры, а также символы «.», «-» и «_». Использование пробелов не допускается;
- теги являются регистронезависимыми;
- просмотр страницы управления тегами будет доступен оператору, если у него есть пользовательское разрешение «Просмотр тегов»;
- управление тегами будет доступно оператору, если у него есть пользовательское разрешение «Управление тегами»;
- на страницах «Консоль управления фермами – Фонды» и «Консоль управления фермами – Индивидуальные рабочие места» поддерживается просмотр и назначение тегов, созданных на ферме поставщиков ресурсов. При этом:
  - оператор должен иметь права на управление объектом как на ферме Termidesk VDI, так и на «Агрегаторе»;
  - оператор должен иметь права на просмотр и управление тегами на ферме Termidesk VDI;
  - разрешения на просмотр и управление тегами, заданные на ферме «Агрегатора», не оказывают влияния на разрешения, заданные на ферме Termidesk VDI.

Для отображения списка тегов следует перейти «Системные параметры – Теги». Основные параметры списка приведены в таблице (см. таблицу Параметры списка тегов).

Таблица 234. Параметры списка тегов

Параметр	Описание
«Название»	Наименование тега
«Кол-во использований»	Количество объектов, которым назначен тег

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Для добавления тега в «Агрегатор» используется экранная кнопка **[Создать]**.

Доступны следующие действия над тегами:

- редактирование. Для этого нужно пометить тег и нажать экранную кнопку **[Изменить]**;
- удаление. Для этого нужно пометить тег и нажать экранную кнопку **[Удалить]**.

Удаление тега приводит к его удалению у всех связанных объектов.

После добавления тега можно перейти к просмотру связанных с ним объектов. Для этого в сводной таблице страницы «Теги» в столбце «Название» следует нажать на наименование тега. Подробные сведения о работе с тегами приведены в подразделе **Работа с тегами**.

Добавление тегов

Для добавления тега нужно перейти «Системные параметры - Теги», затем нажать экранную кнопку **[Создать]**.

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления тега). Для сохранения параметров конфигурации нужно нажать экранную кнопку **[Создать]**.

Таблица 235. Данные для добавления тега

Параметр	Описание
«Название»	Наименование тега

Работа с тегами

Для просмотра списка объектов, связанных с тегом нужно перейти «Системные параметры - Теги», затем в столбце «Название» сводной таблицы нажать на наименование тега.

На открывшейся странице будет представлен список объектов, связанных с выбранным тегом. Основные параметры списка приведены в таблице (см. таблицу Параметры списка тегированных объектов).

Таблица 236. Параметры списка тегированных объектов

Параметр	Описание
«Название»	Наименование объекта, которому назначен тег
«Тип сущности»	Тип объекта
«Теги»	Список тегов, назначенных объекту

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Объект, связанный с тегом можно отредактировать. Для этого нужно пометить объект и нажать экранную кнопку **[Изменить]**. В зависимости от типа объекта откроется соответствующая форма редактирования:

- «Редактирование фермы» для объектов с типом «Ферма поставщиков ресурсов»;
- «Редактирование сайта» для объектов с типом «Сайт»;
- «Редактирование домена аутентификации» для объектов с типом «Домен аутентификации»;
- «Редактирование шлюза» для объектов с типом «Шлюз»;
- «Редактирование узла» для объектов с типом «Узел».

АГРЕГАТОР. КОНСОЛЬ УПРАВЛЕНИЯ ФЕРМАМИ

Общие сведения по управлению из консоли

Консоль управления фермами предназначена для централизованного администрирования фондов РМ, сессий и индивидуальных РМ.

Доступ к разделу «Консоль управления фермами» определяется разрешением «Доступ к консоли управления фермой» (см. подраздел **Назначение служебных функций администраторам**).

Раздел предоставляет доступ к следующим функциональным возможностям:

- «Фонды» - отображает сведения о фондах РМ, размещенных в фермах поставщиков

ресурсов; позволяет управлять политиками и режимом техобслуживания фондов РМ;

- «Сессии» - отображает сведения о сессиях; позволяет управлять их состоянием, выполнять подключение к активным сессиям пользователей через компонент «Удаленный помощник»;
- «Индивидуальные рабочие места» - отображает сведения о РМ из всех фондов; позволяет управлять состоянием и режимом техобслуживания РМ.

Управление фондами РМ

Для отображения списка фондов РМ следует перейти «Консоль управления фермами - Фонды». Основные параметры списка приведены в таблице (см. таблицу Параметры списка фондов РМ).

Доступ к разделу «Фонды» определяется разрешениями «Доступ к консоли управления фермой» и «Доступ к пулам в консоли управления фермой» (см. подраздел **Назначение служебных функций администраторам**).

Таблица 237. Параметры списка фондов РМ

Параметр	Описание
«Фонд рабочих мест»	Наименование фонда РМ
«Ферма»	Наименование фермы, в составе которой находится фонд РМ
«Статус»	Состояние готовности фонда РМ
«Места»	Общее количество РМ в фонде
«Готовятся»	Количество подготавливаемых РМ
«Выбор протокола»	Флаг возможности выбора пользователем протокола доставки при работе с фондом РМ. Значение определяется политикой фонда РМ «Выбор пользователем протокола доставки»
«Группа рабочих мест»	Принадлежность фонда группе РМ
«Шаблон»	Шаблон РМ, примененный в фонде
«Комментарий»	Информационное сообщение, используемое для описания назначения фонда РМ
«Теги»	Список тегов, назначенных фонду РМ. Доступ к тегам фонда РМ определяется пользовательскими разрешениями, заданными на самой ферме Termidesk VDI (разрешения, заданные на ферме «Агрегатора», не оказывают влияния). При выборе тега выполняется переход к разделу «Системные параметры – Теги» со списком объектов, которым назначен данный тег

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Над фондом РМ можно выполнять следующие действия:

- просматривать политики фонда РМ;
- редактировать фонд РМ;
- управлять режимом техобслуживания фонда РМ;
- назначать теги фонду РМ.

Управление сессиями

Для отображения списка сессий следует перейти «Консоль управления фермами - Сессии». Основные параметры списка приведены в таблице (см. таблицу Параметры списка сессий).

Доступ к разделу «Сессии» определяется разрешениями «Доступ к консоли управления фермой» и «Доступ к сессиям в консоли управления фермой» (см. подраздел **Назначение служебных функций администраторам**).

Таблица 238. Параметры списка сессий

Параметр	Описание
«Дата и время»	Дата и время входа пользователя на РМ
«Пользователь»	Имя пользователя, которому было выдано РМ
«IP-адрес»	IP-адрес инициатора сессии
«Хост»	Наименование инициатора сессии
«Место»	Наименование РМ, выданного пользователю
«IP места»	IP-адрес РМ, выданного пользователю
«ИД места»	Идентификатор РМ, выданного пользователю
«Фонд»	Наименование фонда, в составе которого находится выданное РМ
«Ферма»	Наименование фермы, в составе которой находится выданное РМ

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Подробные сведения о доступных действиях над сессиями содержатся в подразделе **Управление сессиями подключенных к фондам пользователей** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

Управление индивидуальными рабочими местами

Для отображения списка РМ из всех фондов следует перейти «Консоль управления фермами - Индивидуальные рабочие места». Основные параметры списка приведены в таблице (см. таблицу Параметры списка индивидуальных рабочих мест).

Доступ к разделу «Индивидуальные рабочие места» определяется разрешениями «Доступ к консоли управления фермой» и «Доступ к отдельным рабочим местам в консоли управления фермой» (см. подраздел **Назначение служебных функций администраторам**).

Таблица 239. Параметры списка индивидуальных рабочих мест

Параметр	Описание
«Дата и время создания»	Временная метка выполнения публикации РМ
«Уникальный ИД»	Уникальный идентификатор РМ: MAC-адрес или номер сессии
«Редакция»	Порядковый номер версии публикации
«IP-адрес»	IP-адрес, назначенный РМ
«Название»	Наименование РМ
«Уровень кеша»	Уровень кеша, на котором находится РМ
«Дата и время последнего логина»	Временная метка последней успешной аутентификации пользователя
«Фонд»	Наименование фонда РМ и ссылка на него
«Ферма»	Наименование фермы, в составе которой находится РМ
«Статус»	Флаг использования публикации РМ из фонда РМ
«Статус обновлен»	Временная метка обновления статуса
«Используется»	Флаг назначения РМ пользователю при наличии активной сессии. Значение «Нет» свидетельствует о том, что РМ не используется пользователем в данный момент. Значение «Да» может сохраниться на некоторое время даже при закрытии пользователем ПО Termidesk Viewer и обновится на «Нет» периодической задачей, выполняемой каждые 90 секунд
«Хост источника»	Наименование инициатора выдачи РМ
«IP источника»	IP-адрес инициатора выдачи РМ
«Владелец»	Субъект, запросивший выдачу РМ
«Версия агента»	Версия компонента «Агент», установленного в гостевой ОС РМ

Параметр	Описание
«Теги»	Список тегов, назначенных РМ. Доступ к тегам РМ определяется пользовательскими разрешениями, заданными на самой ферме Termidesk VDI (разрешения, заданные на ферме «Агрегатора», не оказывают влияния). При выборе тега выполняется переход к разделу «Системные параметры – Теги» со списком объектов, которым назначен данный тег

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Подробные сведения о доступных действиях над РМ содержатся в подразделе **Управление состоянием ВМ в назначенном фонде РМ** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

АГРЕГАТОР. НАЗНАЧЕНИЕ СЛУЖЕБНЫХ ФУНКЦИЙ АДМИНИСТРАТОРАМ

Для администраторов «Агрегатора» реализовано разделение доступных служебных функций.

Для назначения доступных служебных функций следует перейти «Системные параметры - Управление ролями» и нажать экранную кнопку **[Создать роль]** (см. рисунок Окно назначения пользовательских разрешений).

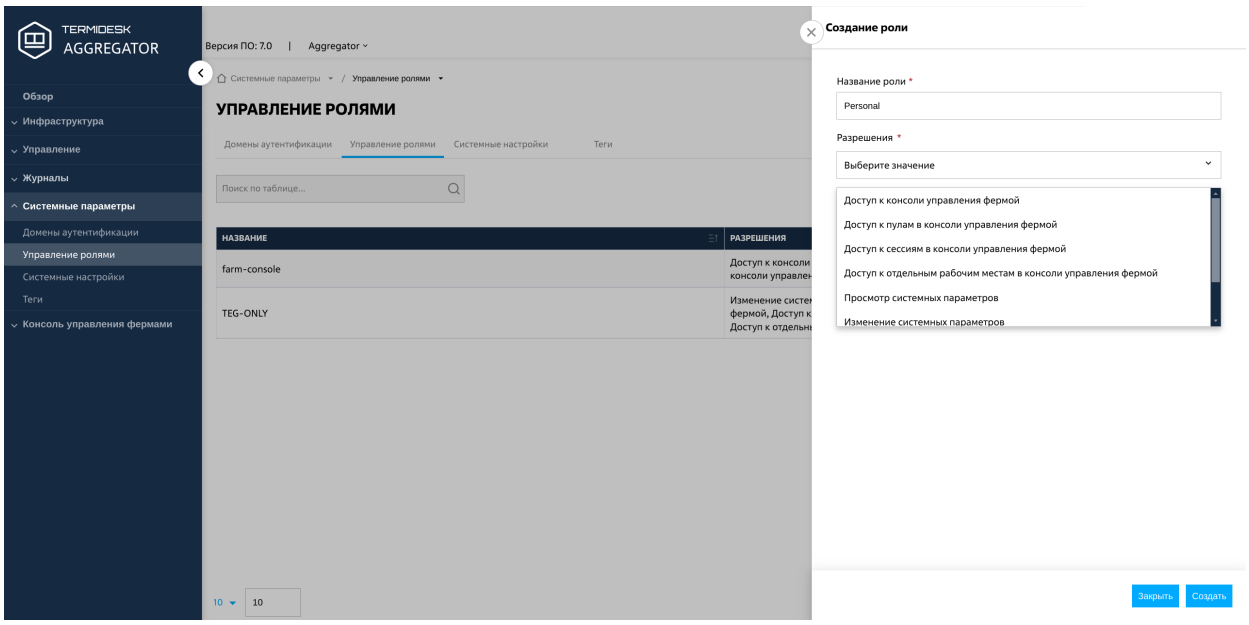


Рисунок 134. Окно назначения пользовательских разрешений

При добавлении функции необходимо ввести текстовое наименование создаваемого класса администратора, а также выбрать список назначаемых разрешений.

Список разрешений для назначения служебных функций администраторам перечислен в следующей таблице (см. таблицу Список доступных для выбора разрешений).

Таблица 240. Список доступных для выбора разрешений

Разрешение	Описание
«Доступ к консоли управления фермой»	Предоставляет доступ на чтение страницы «Консоль управления фермами». Разрешение позволяет выполнять просмотр: • раздела «Фонды»; • раздела «Сессии»; • раздела «Индивидуальные рабочие места»

«Доступ к пулам в консоли управления фермой»	Предоставляет доступ на чтение страницы «Консоль управления фермами - Фонды». Разрешение позволяет:
	• просматривать раздел «Фонды» и выполнять действия в разделе:
	  - просматривать список фондов РМ;
	  - управлять политиками фонда РМ;
	  - редактировать фонды РМ;
	  - управлять режимом техобслуживания фонда РМ

Разрешение	Описание

«Доступ к сессиям в консоли управления фермой»	Предоставляет доступ на чтение страницы «Консоль управления фермами - Сессии». Разрешение позволяет:
	• просматривать раздел «Сессии» и выполнять действия в разделе:
	  просматривать список сессий;
	  отключать сессию;
	  завершать сессию;
	  выполнять подключение к сессии через компонент «Удаленный помощник»

«Доступ к отдельным рабочим местам в консоли управления фермой»	Предоставляет доступ на чтение страницы «Консоль управления фермами - Индивидуальные рабочие места». Разрешение позволяет:
	• просматривать раздел «Индивидуальные рабочие места» и выполнять действия в разделе:
	  просматривать список РМ;
	  управлять состоянием РМ;
	  назначать владельца РМ;
	  управлять режимом техобслуживания РМ

«Просмотр системных параметров»	Предоставляет доступ на просмотр страниц внутри раздела «Системные параметры»
«Изменение системных параметров»	Предоставляет доступ на изменение страниц внутри раздела «Системные параметры»
«Просмотр тегов»	Предоставляет доступ на чтение страницы «Системные параметры - Теги»
«Управление тегами»	Предоставляет доступ на чтение страницы «Системные параметры - Теги». Разрешение позволяет: • создавать теги; • редактировать теги; • удалять теги

Класс администратора может быть назначен определенному пользователю. Для назначения созданного класса следует перейти «Системные параметры - Домены аутентификации» и затем в столбце «Название» сводной таблицы выбрать домен аутентификации, в который входит пользователь.

Служебные функции пользователей «Агрегатора» и фермы Termidesk VDI должны быть одинаковыми для корректного получения данных в «Агрегаторе».

Пример: пользователю user1 с типом «Персонал» назначена роль с разрешениями «Доступ к консоли управления фермой», «Доступ к пулам в консоли управления фермой», «Доступ к сессиям в консоли управления фермой».

В этом случае требуется, чтобы:

- либо пользователю user1 в ферме Termidesk VDI была назначена роль с разрешением «Просмотр фондов рабочих мест»;
- либо пользователь user1 в ферме Termidesk VDI был администратором.

На открывшейся странице в таблице «Пользователи» нужно выбрать пользователя и нажать экранную кнопку **[Изменить]**. В открывшейся форме редактирования пользователя в поле «Роли» выбрать класс (см. рисунок Окно назначения пользовательских ролей).

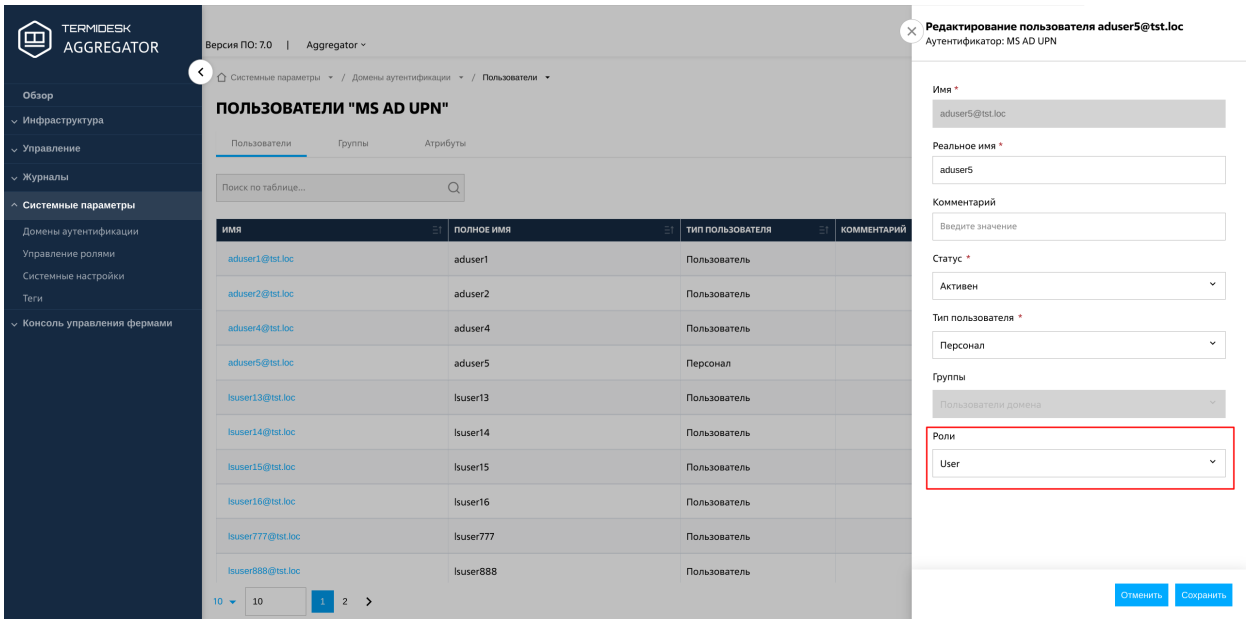


Рисунок 135. Окно назначения пользовательских ролей

Параметр «Персонал» указывает, что пользователь является оператором «Агрегатора» (класс администратора с ограниченными полномочиями).

АГРЕГАТОР. НАСТРОЙКИ

Конфигурационные файлы «Агрегатора»

Конфигурационный файл `termidesk.conf`

Для настройки сервера Termidesk VDI («Универсальный диспетчер», «Агрегатор», «Менеджер рабочих мест», «Брокер сообщений TermideskMQ») используется конфигурационный файл `/etc/opt/termidesk-vdi/termidesk.conf`.

> Каталог хранения конфигурационного файла `termidesk.conf` и указанные ниже параметры можно изменить через утилиту `termidesk-config`.
>
> При установке пакета `termidesk-vdi` возможно активировать режим отладки инсталлятора через переменную окружения `TDSK_DEBUG=1`.

Полный перечень параметров, задающихся через файл, приведен в таблице (см. таблицу Параметры файла `termidesk.conf`).

Таблица 241. Параметры файла `termidesk.conf`

Параметр	Значение по умолчанию	Описание
Настройка режима работы ПО		

Параметр	Значение по умолчанию	Описание
TERMIDESK_FARM_MODE	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора», «Брокера сообщений TermideskMQ». Определяет режим работы Termidesk VDI. Возможные значения: • BROKER - установка фермы «Универсального диспетчера»; • AGGREGATOR - установка фермы «Агрегатора». При обновлении Termidesk VDI пытается автоматически определить предыдущий режим установки и использовать нужное значение на узлах с «Порталами» «Универсального диспетчера». В случаях с другими узлами требуется указать значение вручную
Настройки установленных ролей Termidesk		
NODE_ROLES	Не задано	Параметр обязателен и задается на этапе установки на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора», «Брокера сообщений TermideskMQ». Определяет тип роли, с которой будет установлен Termidesk VDI. Возможные значения: • ADMIN - роль «Портал администратора» (ферма «Универсального диспетчера») или «Агрегатор администратора» (ферма «Агрегатора»); • USER - роль «Портал пользователя» (ферма «Универсального диспетчера») или «Агрегатор пользователя» (ферма «Агрегатора»); • CELERYMAN - роль «Менеджер рабочих мест»; • TERMQ - роль «Брокер сообщений». При переустановке значение параметра в конфигурационном файле будет перезаписано
Настройка языка сервера Termidesk		
LANGUAGE_CODE	en	Параметр обязателен и задается на этапе установки. Определяет язык сервера Termidesk VDI, использующийся по умолчанию. Значение соответствует коду языка согласно ISO-639-1
Настройка уникального имени узла		

Параметр	Значение по умолчанию	Описание
NODE_NAME	Не задано	Параметр обязателен и задается на этапе установки. Определяет уникальное имя узла для его идентификации в различных структурах Termidesk VDI. В частности: * для идентификации узлов «Агрегатора» во время балансировки подключений к ним; * для отображения узла в разделе «Инфраструктура» «Портала администратора» Следует задавать уникальное имя узла понятным и отражающим его роль, например «AdminPortal-01», «UserPortal-01». По умолчанию для заполнения параметра используется заданный в системе hostname и буквенно-числовой идентификатор
Настройка проверки данных при взаимодействии компонентов Termidesk		
DJANGO_SECRET_KEY	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Используется для проверки данных, пересылаемых между компонентами Termidesk VDI. Значение генерируется при установке Termidesk VDI и должно быть одинаковым для всех узлов при распределенной установке. Параметр может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: DJANGO_SECRET_KEY='hvac-kv://secret#termidesk-admin/django/key' Если параметр располагается в хранилище паролей, то все параметры, ранее заданные с преобразованными через утилиту scramble значениями, должны быть указаны с открытыми значениями (RABBITMQ_URL, DBPASS и др.). Это ограничение связано с тем, что при выборе на этапе установки хранилища для параметров подразумевается, что защита чувствительных данных реализуется только через хранилище
Настройки токена доступа к API для проверок состояния служб Termidesk		

Параметр	Значение по умолчанию	Описание
HEALTH_CHECK_ACCESS_KEY	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет токен доступа к API проверки состояния сервера. Начальное значение генерируется на этапе установки. При задании значения параметра следует руководствоваться правилом, что: • размер должен составлять от 0 до 64 символа; • должны использоваться символы в шестнадцатеричной системе (0-9, a-f). Значение также может быть сгенерировано через openssl: openssl rand -hex 32. Параметр может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: HEALTH_CHECK_ACCESS_KEY='hvac-kv://secret#termidesk-admin/tokens/healthcheck'
Настройки токена доступа к API получения метрик узла		
METRICS_ACCESS_KEY	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет токен доступа к API получения метрик узла. Начальное значение генерируется на этапе установки. При задании значения параметра следует руководствоваться правилом, что: • размер должен составлять от 0 до 64 символа; • должны использоваться символы в шестнадцатеричной системе (0-9, a-f). Значение также может быть сгенерировано через openssl: openssl rand -hex 32. Параметр может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: METRICS_ACCESS_KEY='hvac-kv://secret#termidesk-admin/tokens/metrics'
Настройки подключения к СУБД		
DB_CLUSTER_MODE	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет тип установки СУБД, к которой осуществляется подключение. Возможные значения: • single - подключение производится к отдельному серверу СУБД; • cluster - подключение производится к кластеру СУБД, адреса нод которого заданы в DBHOST, DBHOST2, DBHOST3. Termidesk VDI будет последовательно обращаться к заданным адресам нод, пока не подключится к мастер-ноде

Параметр	Значение по умолчанию	Описание
DBHOST	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет IP-адрес или FQDN СУБД PostgreSQL. Начальное значение задается на этапе подготовке среды функционирования и установки Termidesk
DBHOST2	Не задано	Параметр необязательный, может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет IP-адрес или FQDN дополнительного узла СУБД PostgreSQL, если используется подключение к кластеру СУБД (см. параметр DB_CLUSTER_MODE). Начальное значение задается на этапе установки Termidesk
DBHOST3	Не задано	Параметр необязательный, может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет IP-адрес или FQDN дополнительного узла СУБД PostgreSQL, если используется подключение к кластеру СУБД (см. параметр DB_CLUSTER_MODE). Начальное значение задается на этапе установки Termidesk
DBPORT	5432	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет порт соединения с сервером БД
DBSSL	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет протокол подключения к БД. Возможные значения: • Disable; • TLSv1.2; • TLSv1.3. Начальное значение задается на этапе установки Termidesk
DBNAME	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет имя БД. Начальное значение задается на этапе подготовки среды функционирования перед установкой Termidesk
DBUSER	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет имя пользователя, имеющего доступ к БД. Начальное значение задается на этапе подготовки среды функционирования перед установкой Termidesk

Параметр	Значение по умолчанию	Описание
DBPASS	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет пароль пользователя, имеющего доступ к БД. Начальное значение задается на этапе подготовки среды функционирования во время установки Termidesk VDI и хранится в конфигурационном файле termidesk.conf в преобразованном виде. В стандартных установках значение менять не следует. Чтобы получить преобразованное значение пароля, следует воспользоваться утилитой scramble: • для получения значения по стандартному алгоритму (не рекомендуется): /opt/termidesk/bin/scramble --value <пароль> --type AES256; • для получения значения с увеличенным числом итераций преобразования (рекомендуется): /opt/termidesk/bin/scramble --value <пароль> --type AES256_V2 Если значение пароля указывается в формате ключа (значение предваряется символом «-»), то следует изменить его передачу в параметр --value: /opt/termidesk/bin/scramble --value=←пароль> --type AES256_V2 Если конфигурационный файл termidesk.conf хранится в каталоге, отличном от /etc/opt/termidesk-vdi/, может потребоваться указание дополнительного параметра --config в утилите scramble.
DBCERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к клиентскому сертификату mTLS для защищенного подключения к БД. mTLS - метод обеспечения защищенного соединения с БД через двустороннюю аутентификацию с использованием сертификатов. Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt • установить корневой сертификат ЦС. Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: DBCERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'

Параметр	Значение по умолчанию	Описание
DBKEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к ключу mTLS для защищенного подключения к БД. Ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению: openssl rsa -in <путь_к_файлу_ключа.key> -out <путь_сохранения_преобразованного_ключа.key> Для использования ключа нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key • установить корневой сертификат ЦС, если ранее он не был установлен. Ключ может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: DBKEY='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/key'
DBCHAIN	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к промежуточному сертификату mTLS для защищенного подключения к БД. Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem • установить корневой сертификат ЦС, если ранее он не был установлен. Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему. Пример задания сертификата из хранилища: DBCHAIN='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/ca'

Параметр	Значение по умолчанию	Описание
DB_CONN_MAX_AGE	0	Максимально допустимое время (в секундах) существования одного подключения к БД. Параметр управляет жизненным циклом подключения к БД для Django. Для корректной работы это значение должно быть меньше аналогичной настройки на БД, которая может закрывать простаивающие подключения по истечении времени. Значение 0: • обеспечивает совместимость с предыдущими версиями Termidesk VDI; • определяет, что подключения к БД будут закрыты после обработки HTTP-запроса
CELERY_DB_REUSE_MAX	1000	Количество фоновых задач, которое может быть выполнено в рамках одного подключения к БД. По достижении этого количества подключение к БД пересоздастся. Параметр управляет жизненным циклом подключения к БД для служб celery «Менеджера рабочих мест»
DB_CONN_TIMEOUT	10	Время ожидания (в секундах) подключения к БД
Настройки «Менеджера рабочих мест» для распределенной установки		

CELERY_BEAT_PRIMARY_CHECK_INTERVAL	30	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».
		
		Определяет интервал (в секундах) проверки доступности главного процесса среди всех экземпляров «Менеджера рабочих мест» (службы termidesk-celery-beat).
		
		Параметры CELERY_BEAT_PRIMARY_CHECK_INTERVAL и CELERY_BEAT_PRIMARY_LOCK_TIMEOUT реализуют механизм корректной работы termidesk-celery-beat при распределенной установке:
		
		• при запуске нескольких экземпляров termidesk-celery-beat каждый из них пытается сделать запись в кеше БД. БД используется одна на все экземпляры;
		• если экземпляр termidesk-celery-beat:
		  - делает запись в БД, то он отправляет сообщения в очередь брокера сообщений;
		  - не делает запись в БД, то он ожидает своей очереди на добавление записи

CELERY_BEAT_PRIMARY_LOCK_TIMEOUT	45	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет время (в секундах) действия блокировки главного процесса среди всех экземпляров «Менеджера рабочих мест» (службы termidesk-celery-beat). Значение параметра CELERY_BEAT_PRIMARY_LOCK_TIMEOUT должно превышать значение CELERY_BEAT_PRIMARY_CHECK_INTERVAL. Это необходимо для возможности продления интервала проверки главным процессом termidesk-celery-beat
Настройка таймаутов задач «Менеджера рабочих мест»		

Параметр	Значение по умолчанию	Описание
REGISTRATIONS_PROVIDERS_TASK_RESOLVE_TIMEOUT	5	Параметр необязательный, может быть задан на узлах «Менеджера рабочих мест». Через утилиту termidesk-config не задается. Определяет время (в секундах) ожидания разрешения имени узла в IP-адрес в задаче синхронизации регистрации компонента «Сессионный агент» в Метапоставщиках
REGISTRATIONS_PROVIDERS_TASK_TIMEOUT	54	Параметр необязательный, может быть задан на узлах «Менеджера рабочих мест». Через утилиту termidesk-config не задается. Определяет время (в секундах) выполнения задачи синхронизации регистрации компонента «Сессионный агент» в Метапоставщиках. Если задача не завершится за отведенное время, то произойдет ожидание завершения последней блокирующей операции и остановка службы termidesk-celery-worker. Значение 0 отключает таймаут. При установке отрицательного значения задачи не будут выполнены.
CELERY_TASK_TIME_LIMIT	0	Параметр необязательный, может быть задан на узлах «Менеджера рабочих мест». Через утилиту termidesk-config не задается. Определяет глобальное время (в секундах) выполнения задач службы termidesk-celery-worker. Значение 0 отключает ограничение времени выполнения. Если задано ненулевое значение и в журнале службы появляются ошибки «TimeoutError: The read operation timed out», значение следует увеличить.
Настройка подключения к брокеру сообщений (RabbitMQ или TermideskMQ)		

Параметр	Значение по умолчанию	Описание
RABBITMQ_URL	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет URL-адрес подключения к серверам брокера сообщений. Параметр используется как для RabbitMQ, так и для TermideskMQ. Можно подключить до трех (включительно) серверов. Пароль подключения к брокеру сообщений, указанный в RABBITMQ_URL, хранится в конфигурационном файле termidesk.conf в преобразованном виде. Чтобы получить преобразованное значение пароля, следует воспользоваться утилитой scramble: • для получения значения по стандартному алгоритму (не рекомендуется): /opt/termidesk/bin/scramble --value <пароль> --type AES256; • для получения значения с увеличенным числом итераций преобразования (рекомендуется): /opt/termidesk/bin/scramble --value <пароль> --type AES256_V2. Если значение пароля указывается в формате ключа (значение предваряется символом «-»), то следует изменить его передачу в параметр --value: /opt/termidesk/bin/scramble --value=←пароль> --type AES256_V2 Если конфигурационный файл termidesk.conf хранится в каталоге, отличном от /etc/opt/termidesk-vdi/, может потребоваться указание дополнительного параметра --config. Для использования преобразованного значения следует указать его в RABBITMQ_URL и выполнить перезапуск служб. Начальное значение RABBITMQ_URL задается на этапе установки
RABBITMQ_SSL	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет протокол подключения к брокеру сообщений. Параметр используется как для RabbitMQ, так и для TermideskMQ. Возможные значения: Disable, TLSv1.2. Начальное значение задается на этапе установки
Настройки защищенного подключения к брокеру сообщений (RabbitMQ или TermideskMQ)		

Параметр	Значение по умолчанию	Описание
CELERY_BROKER_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к клиентскому сертификату mTLS для защищенного подключения к брокеру сообщений (RabbitMQ или TermideskMQ). Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt; • установить корневой сертификат ЦС, если ранее он не был установлен. Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: CELERY_BROKER_CERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'
CELERY_BROKER_KEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к закрытому ключу mTLS для защищенного подключения к брокеру сообщений (RabbitMQ или TermideskMQ). Ключ может иметь парольную защиту. Для использования в Termidesk VDI нужно преобразовать его к начальному значению: openssl rsa -in <путь_к_файлу_ключа.key> -out <путь_сохранения_преобразованного_ключа.key>. Для использования ключа нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key; • установить корневой сертификат ЦС, если ранее он не был установлен. Ключ может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: CCELERY_BROKER_KEY='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/key'

Параметр	Значение по умолчанию	Описание
CELERY_BROKER_CA	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к корневому сертификату ЦС mTLS для защищенного подключения к брокеру сообщений (RabbitMQ или TermideskMQ). Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt; • установить корневой сертификат ЦС. Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: CELERY_BROKER_CA='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/ca'
Настройки журналирования		
LOG_LEVEL	INFO	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет уровень журналирования сообщений. Возможные значения: DEBUG, INFO, WARNING, ERROR, CRITICAL. Включение уровня DEBUG может привести к повышенной нагрузке системы, поэтому после сбора подробных журналов следует вернуть значение к уровню INFO
LOG_ADDRESS	/dev/log	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет адрес отправки записей в системный журнал. Обычно это /dev/log для Linux-систем. Возможно указать IP-адрес и порт
LOG_FACILITY	local3	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет категорию сообщений syslog. Категория должна совпадать с настройками в конфигурационном файле /etc/syslog-ng/conffirst.d/termidesk.conf. При редактирование параметра через утилиту termidesk-config нужные значения в настройку syslog-ng будут подставлены автоматически
Настройки шаблонов для регистрации событий и журналирования (syslog-ng и logrotate)		

Параметр	Значение по умолчанию	Описание
LOG_DIR	/var/log/termidesk	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к каталогу с журналами, используется в настройках шаблонов logrotate и syslog-ng. Путь к шаблонам определен в файле /etc/default/termidesk-vdi.local. Каталог должен обладать следующими свойствами: • права доступа: rwxr-x--- (в восьмеричной записи - 750); • владелец и группа: root:termidesk. Рекомендуется выполнять изменение параметра через утилиту termidesk-config. Если изменение параметра выполнено вручную, то требуется выполнить команду: sudo /opt/termidesk/sbin/termidesk-config update_logger_config
LOG_OWNER	termidesk	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет владельца файлов журналов, используется в настройках шаблонов logrotate и syslog-ng. Путь к шаблонам определен в файле /etc/default/termidesk-vdi.local. Рекомендуется выполнять изменение параметра через утилиту termidesk-config. Если изменение параметра выполнено вручную, то требуется выполнить команду: sudo /opt/termidesk/sbin/termidesk-config update_logger_config
LOG_GROUP	adm	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет группу-владельца файлов журналов, используется в настройках шаблонов logrotate и syslog-ng. Путь к шаблонам определен в файле /etc/default/termidesk-vdi.local. Рекомендуется выполнять изменение параметра через утилиту termidesk-config. Если изменение параметра выполнено вручную, то требуется выполнить команду: sudo /opt/termidesk/sbin/termidesk-config update_logger_config
LOG_PERM	0440	Параметр может быть задан на узлах «Универсального диспетчера»,«Менеджера рабочих мест», «Агрегатора». Определяет права доступа к файлам журналов, используется в настройках шаблонов logrotate и syslog-ng. Путь к шаблонам определен в файле /etc/default/termidesk-vdi.local. Рекомендуется выполнять изменение параметра через утилиту termidesk-config. Если изменение параметра выполнено вручную, то требуется выполнить команду: sudo /opt/termidesk/sbin/termidesk-config update_logger_config

Параметр	Значение по умолчанию	Описание
LOG_DEEP	14	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет количество устаревеших файлов журналов, которое нужно хранить. Используется в настройках шаблонов logrotate и syslog-ng. Путь к шаблонам определен в файле /etc/default/termidesk-vdi.local. Рекомендуется выполнять изменение параметра через утилиту termidesk-config. Если изменение параметра выполнено вручную, то требуется выполнить команду: sudo /opt/termidesk/sbin/termidesk-config update_logger_config
INTERNAL_AUDIT	Disabled	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет включение или отключение записи событий аудита с анонимным пользователем в БД. Анонимный пользователь AnonymousUser(AnonymousAuth) указывается для запросов, выполняемых без аутентификации. Возможные значения: • Enabled - запись событий аудита с анонимным пользователем включена; • Disabled - запись событий аудита с анонимным пользователем отключена
Настройки защищенного подключения для проверок состояния служб «Менеджера рабочих мест»		
HEALTH_CHECK_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора» (в зависимости от варианта установки). Определяет путь к сертификату SSL/TLS для защищенного подключения к API проверки состояния служб «Менеджера рабочих мест». Для использования сертификата нужно: * скопировать его в каталог /etc/opt/termidesk-vdi/; * назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt; * изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt; * установить корневой сертификат ЦС, если ранее он не был установлен. Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: HEALTH_CHECK_CERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'

Параметр	Значение по умолчанию	Описание
HEALTH_CHECK_KEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера»,«Менеджера рабочих мест», «Агрегатора» (в зависимости от варианта установки). Определяет путь к ключу SSL/TLS для защищенного подключения к API проверки состояния служб «Менеджера рабочих мест». Ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению: openssl rsa -in <путь_к_файлу_ключа.key> -out <путь_сохранения_преобразованного_ключа.key> Для использования ключа нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key; • установить корневой сертификат ЦС, если ранее он не был установлен. Ключ может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: HEALTH_CHECK_KEY='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/key'
Настройки проверок состояния (health check)		
CELERY_BEAT_HEALTH_CHECK_PORT	8103	Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест». Определяет порт, на котором работает веб-сервер для обслуживания API проверки состояния компонента «Менеджер рабочих мест» (службы termidesk-celery-beat). Изначально параметр закомментирован (используется значение по умолчанию)
CELERY_BEAT_HEALTH_CHECK_IP	0.0.0.0	Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест». Определяет IP-адрес, с которым служба termidesk-celery-beat регистрируется в подсистеме проверки состояния на странице «Инфраструктура» Termidesk VDI. Опрос состояния службы будет проводиться по этому адресу. Если IP-адрес не задан, то будет использоваться имя (hostname) или FQDN узла. Изначально параметр закомментирован (используется значение по умолчанию)
CELERY_WORKER_HEALTH_CHECK_PORT	8104	Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест». Определяет порт, на котором работает веб-сервер для обслуживания API проверки состояния компонента «Менеджер рабочих мест» (службы termidesk-celery-worker). Изначально параметр закомментирован (используется значение по умолчанию)

Параметр	Значение по умолчанию	Описание
CELERY_WORKER_HEALTH_CHECK_IP	0.0.0.0	Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест». Определяет IP-адрес, с которым служба termidesk-celery-worker регистрируется в подсистеме проверки состояния на странице «Инфраструктура». Опрос состояния службы будет проводиться по этому адресу. Если IP-адрес не задан, то будет использоваться имя (hostname) или FQDN узла. Изначально параметр закомментирован (используется значение по умолчанию)
HEALTH_CHECK_TIMEOUT	10	Таймаут (в секундах) обработки запроса проверки состояния. По истечении указанного времени: • возвращается стандартная для health check структура ответа; • проверки, которые не успели завершиться, приобретают статус «fail» с причиной «timeout»
CELERY_HEALTH_CHECK_CHECKS	Не задано	Определяет список проверок состояния, выполняемые узлом «Менеджер рабочих мест» (службами termidesk-celery-beat и termidesk-celery-worker). Таймаут обработки запроса проверки состояния определяется параметром HEALTH_CHECK_TIMEOUT. Возможные значения: • db - проверка БД (проверяется подключение); • rabbit - проверка брокера сообщений (проверяется состояние); • fluentd - проверка компонента «Ретранслятор» (проверяется состояние и отправляется тестовое сообщение). Если значение не задано, то выполняются все проверки
TERMIDESK_HEALTH_CHECK_CHECKS	Не задано	Определяет список проверок состояния, выполняемые узлом «Универсальный диспетчер». Таймаут обработки запроса проверки состояния определяется параметром HEALTH_CHECK_TIMEOUT. Возможные значения: • celery - проверка компонента «Менеджер рабочих мест» (проверяется состояние обработчика); • db - проверка БД (проверяется подключение); • rabbit - проверка брокера сообщений (проверяется состояние); • fluentd - проверка компонента «Ретранлятор» (проверяется состояние и отправляется тестовое сообщение). Если значение не задано, то выполняются все проверки

Параметр	Значение по умолчанию	Описание
AGGREGATOR_HEALTH_CHECK_CHECKS	Не задано	Определяет список проверок состояния, выполняемые узлом «Агрегатор». Таймаут обработки запроса проверки состояния определяется параметром HEALTH_CHECK_TIMEOUT. Возможные значения: • celery - проверка компонента «Менеджер рабочих мест» (проверяется состояние обработчика); • db - проверка БД (проверяется подключение); • rabbit - проверка брокера сообщений (проверяется состояние); • fluentd - проверка компонента «Ретранлятор» (проверяется состояние и отправляется тестовое сообщение); • sites - проверка сайтов «Агрегатора» (проверяется состояние сайтов, в случае неактивности выполняется перевод в статус «warning»). Если значение не задано, то выполняются все проверки
Настройки подключения к серверу «Удаленного помощника»		
REMOTE_ASSISTANT_SERVER_CA	Не задано	Параметр может быть задан на узлах «Универсального диспетчера» («Портал администратора», «Портал пользователя»). Определяет путь к корневому сертификату SSL/TLS и используется для проверки подключения к «Удаленному помощнику» (проверка того, что подключение происходит к нужному серверу «Удаленного помощника»). Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem; • установить корневой сертификат ЦС, если ранее он не был установлен. Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: REMOTE_ASSISTANT_SERVER_CA='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'
Настройки доверенных корневых сертификатов		

Параметр	Значение по умолчанию	Описание
REQUESTS_CA_BUNDLE	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к файлу с доверенным корневым сертификатом, задается для настройки работы с сертификатами собственных ЦС. По умолчанию параметр не используется (закомментирован). Параметр является переменной окружения. Рекомендуется задать его в файле termidesk.conf и в /etc/default/termidesk-vdi.local, иначе его обработка не гарантируется
Настройка веб-сервера Apache		
HTTP_SERVER_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет путь к файлу с серверным сертификатом для веб-сервера Apache. Если для хранения чувствительной информации используется хранилище паролей OpenBao или Hashicorp Vault и заданы пути к сертификатам и ключам из хранилища, то они будут скопированы в каталог /dev/shm/: • /dev/shm/http.crt; • /dev/shm/http.key; • /dev/shm/http_ca.crt. При этом обновление сертификата, если такое предусмотрено, будет выполняться на веб-сервере автоматически через службу termidesk-watchdog.service и файл /lib/systemd/system/termidesk-watchdog.path. Если сертификаты и ключи не заданы в параметрах, то будут использоваться сертификаты и ключи по умолчанию (из ОС)
HTTP_SERVER_KEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет путь к файлу с закрытым ключом для веб-сервера Apache. Условия использования аналогичны параметру HTTP_SERVER_CERT
HTTP_SERVER_CA	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет путь к файлу с цепочкой сертификатов корневого и промежуточного УЦ для веб-сервера Apache. Условия использования аналогичны параметру HTTP_SERVER_CERT

Параметр	Значение по умолчанию	Описание
DJANGO_ALLOWED_HOSTS	*	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет список имен или IP-адресов узла, разделенных запятыми, на которые будет отвечать веб-сервер Apache. Рекомендуется использование параметра для повышения безопасности и снижения риска атак через HTTP-заголовки. По умолчанию разрешены любые узлы
DJANGO_SECURE_SSL_REDIRECT	True	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет режим обработки запросов: перенаправлять HTTP-запросы на HTTPS или нет. Возможные значения: • True - все HTTP-запросы перенаправятся на HTTPS; • False - перенаправление на HTTPS не осуществляется. Использование значения имеет практический смысл в случае, если в настройках веб-сервера Apache включена обработка HTTP-запросов
DJANGO_SECURE_HSTS_SECONDS	0	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет установку HTTP-заголовка Strict Transport Security. Если параметр задан ненулевым значением, то заголовок будет установлен во всех ответах, не содержащих его Настройка всех HSTS-параметров должна выполняться только после того, как узлу будет назначено корректное имя, а в настройках веб-сервера Apache будут заданы действующие сертификаты. В противном случае можно потерять доступ к веб-интерфейсу на время, указанное в DJANGO_SECURE_HSTS_SECONDS. Рекомендуется проверить корректность работы механизма на небольшом временном интервале и только после проверки устанавливать в параметре более длительное время.

Параметр	Значение по умолчанию	Описание
DJANGO_SECURE_HSTS_INCLUDE_SUBDOMAINS	False	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет установку директивы includeSubDomains в HTTP-заголовок Strict Transport Security. Возможные значения: • True - директива подставится в HTTP-заголовок; • False - директива не подставится в HTTP-заголовок Настройка всех HSTS-параметров должна выполняться только после того, как узлу будет назначено корректное имя, а в настройках веб-сервера Apache будут заданы действующие сертификаты. В противном случае можно потерять доступ к веб-интерфейсу на время, указанное в DJANGO_SECURE_HSTS_SECONDS.
DJANGO_SECURE_HSTS_PRELOAD	False	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет установку директивы preload в HTTP-заголовок Strict Transport Security. Возможные значения: • True - директива подставится в HTTP-заголовок; • False - директива не подставится в HTTP-заголовок Настройка всех HSTS-параметров должна выполняться только после того, как узлу будет назначено корректное имя, а в настройках веб-сервера Apache будут заданы действующие сертификаты. В противном случае можно потерять доступ к веб-интерфейсу на время, указанное в DJANGO_SECURE_HSTS_SECONDS.
Настройки, связанные с лицензированием		
EULA_ACCEPTED	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет принятие лицензионного соглашения при установке. В случае автоматизированной установки наличие параметра обязательно

Параметр	Значение по умолчанию	Описание
LICENSE_CACHE_TIME	0	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест». Определяет время (в секундах) кеширования данных о лицензии для внутренних процессов Termidesk VDI. Если срок кеширования истек, то следующее обращение к лицензии вызовет: • ее считывание из БД; • обновление времени кеширования. Возможные значения: • 0 - кеширование данных о лицензии отключено; • значение, большее 0 - кеширование данных о лицензии включено. Если была добавлена новая лицензия, то данные о ней не будут отображаться до истечения времени кеширования
Настройки узла «Агрегатора» и его взаимодействия с «Универсальным диспетчером»		
AGGREGATOR_JWT_SSL_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», использующихся в фермах, подключаемых к «Агрегатору». Обязателен для заполнения в случае, если в инфраструктуре используется «Агрегатор». Определяет путь к сертификату для получения значения JWT-токена «Агрегатора». Для использования сертификата нужно: * скопировать его в каталог /etc/opt/termidesk-vdi/; * назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem; * изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem; * установить корневой сертификат ЦС, если ранее он не был установлен. Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: AGGREGATOR_JWT_SSL_CERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'

Параметр	Значение по умолчанию	Описание
AGGREGATOR_JWT_SSL_CERT_SECOND	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», использующихся в фермах, подключаемых к «Агрегатору». Обязателен для заполнения в случае, если в инфраструктуре используется «Агрегатор». Определяет путь к резервному сертификату для получения значения JWT-токена «Агрегатора». Если сертификат, заданный в AGGREGATOR_JWT_SSL_CERT, станет невалидным, то будет использоваться сертификат, указанный в AGGREGATOR_JWT_SSL_CERT_SECOND. Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem; • установить корневой сертификат ЦС, если ранее он не был установлен. Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: AGGREGATOR_JWT_SSL_CERT_SECOND='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pemsecond'
AGGREGATOR_JWT_SSL_KEY	Не задано	Параметр обязателен и задается на узлах «Агрегатора» (портал «Агрегатор пользователя» и портал «Агрегатор администратора»), «Менеджера рабочих мест». Определяет путь к ключу для подписи JWT-токена «Агрегатора». Для использования ключа нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key; • установить корневой сертификат ЦС, если ранее он не был установлен. Ключ может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему: AGGREGATOR_JWT_SSL_KEY='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/key'

Параметр	Значение по умолчанию	Описание
AGGREGATOR_YAML_FILE	Не задано	Параметр задается на узлах с установленным «Агрегатором». Параметр определяет путь к файлу mapping.yaml, содержащему сопоставление между именами узлов (NODE_NAME) «Агрегатора» и их полным доменным именем (FQDN) или IP-адресом. При работе с географической балансировкой (GSLB) файл должен быть одинаков на всех узлах распределенной установки «Агрегатора» для корректной обработки переключений между узлами и фермами «Агрегатора». Файл может располагаться в файловой системе узла или в хранилище чувствительной информации: AGGREGATOR_YAML_FILE='/etc/opt/termidesk-vdi/mapping.yaml'
Настройки подключения к хранилищу паролей OpenBao		
SECRETS_STORAGE_METHOD	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет способ хранения паролей подключения к СУБД и RabbitMQ: • config - пароли будут храниться в преобразованном виде в файле termidesk.conf; • hvac - для хранения паролей будет использоваться хранилище паролей OpenBao или Hashicorp Vault (хранилище должно быть заранее создано и настроено); • openbao - для хранения паролей будет использоваться хранилище паролей OpenBao (хранилище должно быть заранее создано и настроено). При этом пароли располагаются внутри хранилища, имена контейнеров хранения генерируются автоматически. Если для хранения чувствительной информации используется хранилище паролей OpenBao или Hashicorp Vault и в параметрах HTTP_SERVER_CERT, HTTP_SERVER_KEY, HTTP_SERVER_CA заданы пути к сертификатам и ключам из хранилища, то они будут скопированы для веб-сервера Apache (см. описание параметров). Хранилище паролей OpenBao должно быть реализовано в отказоустойчивом варианте, иначе Termidesk VDI не будет работать в период простоя узлов OpenBao. Начальное значение задается на этапе установки

Параметр	Значение по умолчанию	Описание
SECRETS_OPENBAO_URL	http://openbao:8200	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет IP-адреса или FQDN узла и порта с установленным хранилищем OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Формат: http://<IP-адрес или FQDN>:8200. Подключение может выполняться по протоколу HTTPS, если OpenBao настроен соответствующим образом. Начальное значение задается на этапе установки. Пример задания параметра: SECRETS_OPENBAO_URL='http://127.0.0.1:8200'
SECRETS_OPENBAO_KV_VERSION	1	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Используется для указания версии API OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Возможные значения: • 1 (по умолчанию); • 2. Начальное значение задается на этапе установки. Пример задания параметра: SECRETS_OPENBAO_KV_VERSION=1

Параметр	Значение по умолчанию	Описание
SECRETS_OPENBAO_CLIENT_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к сертификату mTLS для начального защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы. Особенности функционирования: • если параметры SECRETS_OPENBAO_CLIENT_CERT и SECRETS_OPENBAO_CLIENT_KEY заданы, то выполняется защищенное соединение по протоколу TLS; • если параметры SECRETS_OPENBAO_CLIENT_CERT и SECRETS_OPENBAO_CLIENT_KEY не заданы, то выполняется незащищенное соединение; • если помимо параметров SECRETS_OPENBAO_CLIENT_CERT, SECRETS_OPENBAO_CLIENT_KEY задан SECRETS_OPENBAO_SERVER_CERT, то выполняется защищенное соединение по протоколу mTLS; • сертификат должен размещаться в файловой системе узла (внешнее хранилище не используется). Начальное защищенное соединение настраивается в случаях, если сертификаты имеют продолжительный срок действия или их обновление производится средствами, отличными от OpenBao. В случае, если у сертифкатов непродолжительный срок действия или их обновление производится через OpenBao, следует выполнить настройку параметр SECRETS_OPENBAO_PKI_CERTS. Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt; • установить корневой сертификат ЦС, если ранее он не был установлен. Пример задания параметра: SECRETS_OPENBAO_CLIENT_CERT='/etc/opt/termidesk-vdi/openbao-client.crt'

Параметр	Значение по умолчанию	Описание
SECRETS_OPENBAO_CLIENT_KEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к ключу mTLS для начального защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы. Особенности функционирования: • если параметры SECRETS_OPENBAO_CLIENT_CERT и SECRETS_OPENBAO_CLIENT_KEY заданы, то выполняется защищенное соединение по протоколу TLS; • если параметры SECRETS_OPENBAO_CLIENT_CERT и SECRETS_OPENBAO_CLIENT_KEY не заданы, то выполняется незащищенное соединение; • если помимо параметров SECRETS_OPENBAO_CLIENT_CERT, SECRETS_OPENBAO_CLIENT_KEY задан SECRETS_OPENBAO_SERVER_CERT, то выполняется защищенное соединение по протоколу mTLS; • ключ должен размещаться в файловой системе узла (внешнее хранилище не используется). Начальное защищенное соединение настраивается в случаях, если сертификаты имеют продолжительный срок действия или их обновление производится средствами, отличными от OpenBao. В случае, если у сертифкатов непродолжительный срок действия или их обновление производится через OpenBao, следует выполнить настройку параметра SECRETS_OPENBAO_PKI_CERTS. Ключ может иметь парольную защиту. Для использования ключа в Termidesk VDI нужно преобразовать его к начальному значению: openssl rsa -in <путь_к_файлу_ключа.key> -out <преобразованный_ключ.key>. Для использования ключа нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key; • установить корневой сертификат ЦС, если ранее он не был установлен. Пример задания параметра: SECRETS_OPENBAO_CLIENT_KEY='/etc/opt/termidesk-vdi/openbao-client.key'

Параметр	Значение по умолчанию	Описание
SECRETS_OPENBAO_SERVER_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к промежуточному сертификату ЦС mTLS для начального защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы. Для работы защищенного соединения по протоколу mTLS требуется задать параметры SECRETS_OPENBAO_CLIENT_CERT, SECRETS_OPENBAO_CLIENT_KEY. Сертификат должен размещаться в файловой системе узла (внешнее хранилище не используется). Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem; • установить корневой сертификат ЦС, если ранее он не был установлен. Пример задания параметра: SECRETS_OPENBAO_SERVER_CERT='/etc/opt/termidesk-vdi/openbao-ca.pem'
SECRETS_OPENBAO_PKI_CERTS	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к клиентскому сертфикату и ключу, размещенному в OpenBao, для вторичной проверки подключения к OpenBao. В случае, если у сертифкатов непродолжительный срок действия или их обновление производится через OpenBao, следует использовать этот параметр. Пример задания параметра: SECRETS_OPENBAO_PKI_CERTS = 'hvac-pki://pki?common_name=www.my-website.com#example-dot-com/issuing_ca'
SECRETS_OPENBAO_TOKEN	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к файлу, содержащему одноразовый токен доступа к OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Пример задания параметра: SECRETS_OPENBAO_TOKEN='/etc/opt/termidesk-vdi/openbao.token'

Параметр	Значение по умолчанию	Описание
SECRETS_OPENBAO_DB_PATH	hvac-kv://secret#postgresql/	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь, настроенный на OpenBao и используемый для хранения данных подключения к СУБД. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Начальное значение задается на этапе установки. Данные могут быть расположены в специальном хранилище паролей, в этом случае указывается путь к ним: SECRETS_OPENBAO_DB_PATH='hvac-kv://secret#/postgresql/'
SECRETS_OPENBAO_ROLE_NAME	termidesk-role	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет роль (имя приложения), настроенную на OpenBao и имеющую доступ к логинам и паролям. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Начальное значение задается на этапе установки. Пример задания параметра: SECRETS_OPENBAO_ROLE_NAME='vdi-role'
SECRETS_OPENBAO_ROLE_ID	a877a491-71a4-bfe8-e24c-d5beff3dddd2	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет идентификатор роли, заданной в параметре SECRETS_OPENBAO_ROLE_NAME. Идентификатор должен быть получен на OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Пример задания параметра: SECRETS_OPENBAO_ROLE_ID='a877a491-71a4-bfe8-e24c-d5beff3dddd2'
SECRETS_OPENBAO_WATCHDOG_INTERVAL	10	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет интервал (в секундах) проверки актуальности одноразового токена (параметр SECRETS_OPENBAO_TOKEN). Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac
SECRETS_OPENBAO_TTL_DEADLINE	30	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет оставшееся время (в секундах) актуальности одноразового токена, по достижении которого он будет обновлен. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac

Параметр	Значение по умолчанию	Описание
SECRETS_OPENBAO_WRAP_TTL	10m	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет время актуальности (в минутах) одноразового токена. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac
SECRETS_OPENBAO_NAMESPACE	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет пространство имени, заданного на OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac
SECRETS_OPENBAO_RABBITMQ_PATH	hvac-kv://secret#rabbitmq/	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь, настроенный на OpenBao и используемый для хранения данных подключения к RabbitMQ. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Начальное значение задается на этапе установки. Данные могут быть расположены в специальном хранилище паролей, в этом случае указывается путь к ним: SECRETS_OPENBAO_RABBITMQ_PATH='hvac-kv://secret#/rabbitmq/'
SECRETS_OPENBAO_TERMIDESK_PATH	/termidesk	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь, настроенный на OpenBao для хранения паролей Termidesk VDI. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Начальное значение задается на этапе установки. Пример задания параметра: SECRETS_OPENBAO_TERMIDESK_PATH='hvac-kv://secret#/termidesk'
SECRETS_OPENBAO_CACHE_LIFETIME	5	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет время (в секундах) хранения пароля, полученного от OpenBao, во внутренней памяти. Позволяет сохранить полученный от OpenBao пароль на некоторое время в кеше для сокращения количества обращений к OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac. Начальное значение задается на этапе установки
Настройки взаимодействия с узлом «Ретранслятора»		

Параметр	Значение по умолчанию	Описание
FLUENTD_CACHE	15	Параметр может быть задан на узлах «Универсального диспетчера». Определяет время (в секундах) кеширования параметров подключения к узлу «Ретранслятора». По умолчанию после установки время кеширования составляет 15 секунд. В случае, если нужно изменить значение, следует раскомментировать параметр и задать ему новое значение
FLUENTD_TABLE	logs	Параметр может быть задан на узлах «Универсального диспетчера». Определяет таблицу хранения событий фермы. По умолчанию после установки «Универсальный диспетчер» обращается к таблице «logs» БД «Ретранслятора». В случае, если в БД «Ретранслятора» для хранения событий используется другая таблица, следует раскомментировать параметр и указать новое имя таблицы
FLUENTD_LOGGER_TIMEOUT	5	Параметр может быть задан на узлах «Универсального диспетчера». Определяет время (в секундах) ожидания подключения к узлу «Ретранслятора»
Настройки «Шлюза»		
WSPROXY_PUB_KEY_FILE	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет путь к открытому ключу id_rsa.pub. Используется для подписи токенов при взаимной аутентификации «Шлюза» и «Универсального диспетчера», «Агрегатора». По умолчанию создается при первой установке и хранится в каталоге /etc/opt/termidesk-vdi/wsproxy. Явно задавать путь следует только при использовани внешнего хранилища. Пример: WSPROXY_PUB_KEY_FILE='hvac-kv://secret#termidesk-admin/wsproxy/pub'
WSPROXY_PRIV_KEY_FILE	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора». Определяет путь к закрытому ключу id_rsa. Используется для подписи токенов при взаимной аутентификации «Шлюза» и «Универсального диспетчера», «Агрегатора». По умолчанию создается при первой установке и хранится в каталоге /etc/opt/termidesk-vdi/wsproxy. Явно задавать путь следует только при использовани внешнего хранилища. Пример: WSPROXY_PRIV_KEY_FILE='hvac-kv://secret#termidesk-admin/wsproxy/priv'
Настройка защищенного взаимодействия сервера Termidesk VDI с другими компонентами по mTLS		

Параметр	Значение по умолчанию	Описание
MTLS_MODE	disabled	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет режим mTLS для взаимодействия между компонентами Termidesk VDI. В этом сценарии сервер Termidesk VDI выступает в роли клиента процесса взаимной аутентификации. Возможные значения: • disabled - результат проверки сертификата игнорируется. В этом режиме mTLS не используется; • permissive - нестрогий режим проверки сертификата. Проверка выполняется, но если сертификат не предоставлен или он недействительный, то в журнал записывается предупреждение. Запрос при этом выполняется; • strict - строгий режим проверки сертификата. Предоставление действительных сертификатов обязательно. Запрос отклоняется, когда сертификат не прошел проверку Если включен строгий режим проверки, то работа со всеми API (значение all_api параметра MTLS_CONNECTIONS) и «Агрегатором пользователя» (значение client_aggr_portal параметра MTLS_CONNECTIONS) будет запрещена.

Параметр	Значение по умолчанию	Описание
MTLS_CONNECTIONS	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет сценарий взаимодействия между компонентами Termidesk VDI по mTLS. Узлы должны быть настроены на использование mTLS: • должны быть загружены и использоваться валидные клиентские и серверные сертификаты; • должен быть активирован режим использования mTLS. Изменение параметра потребует перезапуска службы termidesk-vdi. Возможные значения: • va_agent - взаимодействие по mTLS осуществляется с «Агентом виртуального рабочего места»; • session_agent - взаимодействие по mTLS осуществляется с «Сессионным агентом»; • client_aggr_portal - взаимодействие по mTLS осуществляется со всеми видами порталов («Агрегатором пользователя», «Агрегатором администратора», «Порталом администратора», «Порталом пользователя»). Значение не должно использоваться, если включен строгий режим mTLS; • gateway - взаимодействие по mTLS осуществляется со шлюзом, обеспечивающим формирование и поддержание соединения; • all_api - взаимодействие по mTLS осуществляется для всех API-запросов «Универсального диспетчера». Значение не должно использоваться, если включен строгий режим mTLS; • health_check - взаимодействие по mTLS осуществляется для API-запроса /api/health/check «Универсального диспетчера»; • metrics - взаимодействие по mTLS осуществляется для API-запроса /api/health/metrics «Универсального диспетчера»
MTLS_CLIENT_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к клиентскому сертификату mTLS для защищенного подключения и взаимной аутентификации с другими компонентами (например, службами каталогов или платформами виртуализации). Для работы mTLS необходимо выбрать режим проверки и сценарии в параметрах MTLS_MODE и MTLS_CONNECTIONS. Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem

Параметр	Значение по умолчанию	Описание
MTLS_CLIENT_KEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к клиентскому ключу mTLS для защищенного подключения и взаимной аутентификации с другими компонентами (например, службами каталогов или платформами виртуализации). Для работы mTLS необходимо выбрать режим проверки и сценарии в параметрах MTLS_MODE и MTLS_CONNECTIONS. Для использования ключа нужно: * скопировать его в каталог /etc/opt/termidesk-vdi/; * назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key; * изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key
MTLS_CLIENT_CA	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к клиентскому корневому сертификату mTLS для защищенного подключения и взаимной аутентификации с другими компонентами (например, службами каталогов или платформами виртуализации). Для работы mTLS необходимо выбрать режим проверки и сценарии в параметрах MTLS_MODE и MTLS_CONNECTIONS. Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem
Настройка «Брокера сообщений TermideskMQ»		
TMQ_BASE_ADDRESS	0.0.0.0	IP-адрес прослушивания входящих подключений для «Брокера сообщений TermideskMQ»

Параметр	Значение по умолчанию	Описание

TMQ_BASE_PORT	5555	Номер базового порта «Брокера сообщений TermideskMQ».
		
		Если режим mTLS не используется, то:
		
		• действует правило выделения портов: <базовый_порт> + один последующий для IP-адреса, указанного в TMQ_BASE_ADDRESS;
		• базовый порт используется для приема сообщений, дополнительный порт - для отправки сообщений.
		
		Если режим mTLS используется, то:
		
		• в зависимости от базового порта будут определены внутренние TCP-порты для запуска «Брокера сообщений TermideskMQ» на localhost;
		• порты mTLS, использующиеся для IP-адреса, указанного в TMQ_BASE_ADDRESS:
		  - базовый порт (например, 5555);
		  - базовый порт +1 (например, 5556);
		• внутренние TCP-порты для запуска на localhost:
		  - базовый порт + 3 (например, 5558), используется для приема сообщений;
		  - базовый порт + 3 + 1 (например, 5559), используется для приема подключения и отправки сообщений

Настройка «Брокера сообщений TermideskMQ» для работы с mTLS		
TMQ_SERVER_CERT	Не задано	Определяет путь к серверному сертификату mTLS для «Брокера сообщений TermideskMQ». Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem
TMQ_SERVER_KEY	Не задано	Определяет путь к ключу для серверного сертификата mTLS для «Брокера сообщений TermideskMQ». Для использования ключа нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key

Параметр	Значение по умолчанию	Описание
TMQ_SERVER_CA	Не задано	Определяет путь к корневому сертификату mTLS для «Брокера сообщений TermideskMQ». Для использования сертификата нужно: • скопировать его в каталог /etc/opt/termidesk-vdi/; • назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem; • изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem
Настройка высокодоступной конфигурации «Брокера сообщений TermideskMQ»		
TMQ_CLIENT_ID	default	Определяет идентификатор клиента «Брокере сообщений TermideskMQ». Для работы нескольких ферм Termidesk VDI (или ферм «Агрегатора») с одним кластером «Брокера сообщений TermideskMQ» нужно указать уникальный идентификатор для каждой фермы, в этом случае все клиенты в рамках нее полчат один идентификатор. Тип значения идентификатора - строка
TMQ_TIMEOUT_AWAIT_SENDING_MESSAGEL	10000	Определяет время ожидания ответа от узла кластера «Брокера сообщений TermideskMQ». При использования высокодоступной конфигурации требуется настройка «Брокера сообщений TermideskMQ» для работы с mTLS
TMQ_PUT_RETRY_COUNT	3	Определяет количество попыток выполнения запроса или отправки сообщения к узлу кластера «Брокера сообщений TermideskMQ». При использования высокодоступной конфигурации требуется настройка «Брокера сообщений TermideskMQ» для работы с mTLS
Настройки использования веб-интерфейса		
TERMIDESK_OLD_INTERFACE_ENABLED	True	Параметр может быть задан на узлах «Универсального диспетчера» («Портал администратора», «Портал пользователя»). Определяет использование старого веб-интерфейса. Возможные значения: • True - доступны старый и новый веб-интерфейсы; • False - доступен только новый веб-интерфейс. При этом будет окно авторизации для старого веб-интерфейса будет доступно, но не будет работать
Настройка взаимодействия со службой каталогов MS AD		

Параметр	Значение по умолчанию	Описание
AUTH_MSAD_META_USE_UPN	True	Параметр может быть задан на узлах «Универсального диспетчера». Определяет формат передачи имени метапользователя в службу каталогов MS AD. Возможные значения: • True - для имени метапользователя используется формат UPN; • False - для имени метапользователя не используется формат UPN
Настройка подключения пользователя к BPM		
CONNECTION_TICKET_VALIDITY	60	Параметр может быть задан на узлах «Универсального диспетчера». Определяет время валидности (в секундах) тикета для подключения пользователя к BPM. Значение следует менять только при возникновении ошибок подключения, связанных с долгой обработкой подключения

Пример файла конфигурации сервера OpenBao, который активирует строгую проверку клиентского SSL-сертификата:

```
listener "tcp" {
tls_min_version = "tls12"
tls_disable = "false"
address = "0.0.0.0:8200"
tls_cert_file = "/etc/bao/openbao.stand8.local.crt"
tls_key_file = "/etc/bao/openbao.stand8.local.key"
# Если включён, то будет проверять сертификат клиента на корректность
tls_require_and_verify_client_cert = "true"
# Если выключён, то будет требовать наличие сертификата клиента
tls_disable_client_certs = "false"
}
```

Файл /etc/default/termidesk-vdi.local

Для настройки путей хранения файлов конфигурации и некоторых других параметров, влияющих на установщик Termidesk и запуск службы termidesk-vdi, используется файл /etc/default/termidesk-vdi.local.

Перечень параметров, задающихся через файл, приведен в таблице (см. таблицу Параметры файла /etc/default/termidesk-vdi.local).

Если во время обновления Termidesk VDI было выбрано новое место хранения конфигурации, то:

- создастся (если не существовал) новый каталог для хранения конфигурации;
- в новый каталог будут скопированы (если не существовали) файлы из старого каталога (termidesk.conf, termidesk.cookie, CRYPTO_RSA_KEY,

/wsproxy/id_rsa, /wsproxy/id_rsa.pub).

Рекомендуется выполнять изменение путей к каталогам через утилиту termidesk-config.

Если изменение было сделано вручную, то потребуется:

- при изменении места хранения шаблонов выполнить:

```
sudo /opt/termidesk/sbin/termidesk-config update_logger_config
```

- при любых изменениях перезапустить службы Termidesk VDI (в зависимости от установленной роли узла список служб может отличаться).

Таблица 242. Параметры файла /etc/default/termidesk-vdi.local

Параметр	Значение по умолчанию	Описание
ETC	/etc/opt/termidesk-vdi	Параметр может быть задан на узлах «Универсального диспетчера»,«Менеджера рабочих мест», «Агрегатора». Определяет путь к каталогу с конфигурационными файлами (termidesk.conf, termidesk.cookie, CRYPTO_RSA_KEY, /wsproxy/id_rsa, /wsproxy/id_rsa.pub). Каталог должен обладать следующими свойствами: • права доступа: rwxr-x--- (в восьмеричной записи - 750); • владелец и группа: root:termidesk. Пример: ETC='/etc/opt/termidesk-vdi'
TEMPLATES_DIR	/etc/opt/termidesk-vdi/templates	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора». Определяет путь к каталогу с шаблонами для настройки регистрации событий и журналирования. Каталог должен обладать следующими свойствами: • права доступа: rwxr-x--- (в восьмеричной записи - 750); • владелец и группа: root:termidesk. Пример: TEMPLATES_DIR='/etc/opt/termidesk-vdi/templates'

Параметр	Значение по умолчанию	Описание
NON_INTERACTIVE_INSTALLATION	Не задано	Параметр определяет режим работы установщика при его запуске. Возможные значения: • yes - при запуске установщика (пакета termidesk-vdi) диалоги настройки параметров не отображаются. Значение рекомендуется использовать, если требуется выполнить установку без отображения псевдографического интерфейса установщика; • любое другое значение или пустое - при запуске установщика диалоги настройки параметров отображаются
GUNICORN_VDI_WORKERS	Не задано	Параметр определяет количество обработчиков запросов, используемых службой termidesk-vdi. По умолчанию параметр отсутствует и добавляется вручную. Значение параметра выбирается с учетом производительности сервера Termidesk VDI. Если переменная отсутствует или имеет значение меньше 1, то количество обработчиков автоматически рассчитывается по формуле: количество ядер CPU, умноженное на 3.

Файл mapping.yaml

Файл mapping.yaml используется для сопоставления имен узлов «Агрегатора» (параметр NODE_NAME конфигурационного файла termidesk.conf) с их полным доменным именем (FQDN) или IP-адресом:

- NODE_NAME является логическим идентификатором экземпляра «Агрегатора» и при использовании mapping.yaml служит ключом для привязки узла к параметрам redirect_url (перенаправление) и healthcheck_url (проверка состояния). Также имя узла используется для идентификации «Агрегатора» при работе за GSLB;
- в GSLB файл mapping.yaml нужен для выбора адресов и URL для обращения конкретных логических узлов «Агрегатора» при перенаправлении и контроле доступности. Отдельные установки узлов при этом остаются независимы;
- в mapping.yaml должны быть описаны участвующие в GSLB экземпляры «Агрегатора», для которых требуются индивидуальные redirect_url и healthcheck_url. Файл должен быть одинаковым на всех этих «Агрегаторах». Узлы других ролей («Портал администратора», «Портал пользователя» фермы Termidesk VDI и «Менеджер рабочих мест») в mapping.yaml не добавляются;
- при GSLB NODE_NAME используется как идентификатор конкретного узла «Агрегатора». Если запрос попадает на другой «Агрегатор», mapping.yaml позволяет по NODE_NAME определить адреса redirect_url и healthcheck_url ранее использованного узла, проверить его доступность и перенаправить пользователя обратно на него.

При работе с географической балансировкой (GSLB) файл должен быть одинаков на всех узлах распределенной установки «Агрегатора» для корректной обработки переключений между узлами и фермами «Агрегатора».

Имя файла может быть любым, требуется только указать его в конфигурационном файле termidesk.conf (параметр AGGREGATOR_YAML_FILE).

Пример файла:

```
Kaliningrad-01:
     redirect_url: https://aggr-kgd-01.domain.ru:999
     healthcheck_url: https://aggr-kgd-01.internal.domain.ru:999
Kaliningrad-02:
     redirect_url: https://aggr-kgd-02.domain.ru
     healthcheck_url: https://aggr-kgd-02.internal.domain.ru
Vladivostok-01:
     redirect_url: https://aggr-vvo-01.domain.ru
     healthcheck_url: https://aggr-vvo-01.internal.domain.ru
Vladivostok-02:
     redirect_url: https://aggr-vvo-02.domain.ru
     healthcheck_url: https://aggr-vvo-02.internal.domain.ru
```

Перечень параметров, задающихся через файл, приведен в таблице (см. таблицу Параметры файла mapping.yaml).

Таблица 243. Параметры файла mapping.yaml

Параметр	Описание
redirect_url	Параметр задает доменное имя и порт узла, доступного для подключения пользователей из внешней сети
healthcheck_url	Параметр задает доменное имя узла, на котором доступен сервис проверки состояния узла (healthcheck) из внутренней сети. Параметр необязателен: если он не задан, то используется значение из параметра redirect_url

Общие системные настройки «Агрегатора»

Общие системные настройки позволяют задать основные значения, необходимые для успешного функционирования «Агрегатора».

Для конфигурации общих системных настроек следует перейти «Системные параметры - Системные настройки», выбрать раздел «Общие».

Доступные для редактирования параметры перечислены в столбце «Параметр» следующей таблицы (см. таблицу Общие системные настройки).

Доступ к разделу «Системные параметры» определяется разрешениями «Просмотр системных параметров» и «Изменение системных параметров» (см. подраздел **Назначение служебных функций администраторам**).

Изменение системных настроек вступит в силу после перезагрузки службы termidesk-vdi.

Таблица 244. Общие системные настройки

Параметр	Описание
«Название фермы»	Наименование фермы, отображаемое в «Агрегаторе пользователя», «Агрегаторе администратора» и компоненте «Клиент»
«Время блокировки входа, с»	Задает время (в секундах) после истечения которого будет возможен повторный вход субъекта «Администратор», «Персонал» в случае превышения лимита неудачных попыток входа. По истечении этого времени пользователь продолжит визуально быть заблокированным (статус «Временно заблокирован») в списке пользователей в домене аутентификации. Статус сменится на «Активный» только после авторизации пользователя с правильным паролем или после смены статуса администратором. Значение по умолчанию: «300»
«Срок хранения статистики, сут»	Время (в сутках) хранения файлов журналов, по истечению которого журналы будут перезаписаны. Значение по умолчанию: «365»
«Время жизни access token, с»	Определяет времени жизни (в секундах) JWT-токена, подписанного «Агрегатором». Значение по умолчанию: «600»
«Заголовок access token»	Задает заголовок JWT-токена, предназначенный для настройки взаимодействия между «Агрегатором» и «Универсальным диспетчером». Значение по умолчанию: «Access»
«Частота опроса версий узлов ферм, с»	Частота опроса версии «Универсального диспетчера» фермы Termidesk VDI. Значение по умолчанию: «30» (раз в 30 секунд)
«Время кеширования редиректа сайта, с»	Определяет максимальное время ожидания (в секундах) HTTP-запросов «Агрегатора» и позволяет предотвратить бесконечное ожидание со стороны «Агрегатора», если «Универсальный диспетчер» фермы Termidesk VDI не вернул ответ на запрос. Рекомендации по изменению значения: • значение следует увеличить, если при получении списка РМ наблюдаются ошибки, связанные с тем, что «Агрегатор» завершает запрос раньше, чем «Универсальный диспетчер» фермы Termidesk VDI успевает вернуть ответ; • значение следует уменьшить, если требуется быстрее завершать неудачные подключения или сократить общее время ожидания при недоступности «Универсального диспетчера» фермы Termidesk VDI. Значение по умолчанию: «600»
«Время жизни токена шлюза»	Определяет время жизни (в секундах) токена, используемого для взаимодействия «Агрегатора» и шлюза. Значение по умолчанию: «20»

Параметр	Описание
«Таймаут кеша хранения групп домена, с»	Определяет время хранения (в секундах) информации о группах пользователя, полученной от службы каталогов. Работает совместно с параметром «Динамическая проверка членства пользователя в группах», заданным в свойствах домена. Значение по умолчанию: «30»
«Время кеширования JWT сертификатов агрегатора, с»	Определяет время кеширования (в секундах) сертификатов для получения значения JWT-токена во внутренней памяти. Позволяет сохранить сертификат на некоторое время в кеше для сокращения количества обращений к источнику хранения сертификатов. Значение по умолчанию: «30»
«Таймаут аутентификации RADIUS, с»	Определяет время ожидания (в секундах) завершения всех этапов аутентификации пользователя на сервере RADIUS. Если появляются ошибки аутентификации пользователя на сервере RADIUS (например, после ввода OTP), то рекомендуется увеличить значение параметра. Значение по умолчанию: «60»
«Таймаут HTTP-запросов агрегатора, с»	Определяет максимальное время ожидания (в секундах) HTTP-запросов «Агрегатора» и позволяет предотвратить бесконечное ожидание со стороны «Агрегатора», если «Универсальный диспетчер» фермы Termidesk VDI не вернул ответ на запрос. Если при выполнении HTTP-запросов появляются ошибки связанные с тем, что «Агрегатор» завершает запрос раньше, чем «Универсальный диспетчер» фермы Termidesk VDI успевает вернуть ответ, то рекомендуется увеличить значение параметра. Если требуется быстрее завершать неудачные подключения или сократить общее время ожидания при недоступности «Универсального диспетчера» фермы, то значение следует уменьшить. Значение по умолчанию: «10»
«Время кеширования консоли управления фермами, с»	Определяет время кеширования (в секундах) данных страницы «Консоль управления фермами» во внутренней памяти. Позволяет сохранить данные страницы «Консоль управления фермами» на некоторое время в кеше для сокращения количества обращений к «Универсальному диспетчеру» фермы Termidesk VDI. Значение по умолчанию: «30»
«Время жизни кеша узлов агрегатора, с»	Определяет время кеширования (в секундах) списка узлов «Агрегатора» во внутренней памяти. Позволяет сохранить списки узлов «Агрегатора» на некоторое время в кеше для сокращения количества обращений к ним. Список узлов задается в конфигурационном файле `mapping.yaml`. Значение по умолчанию: «300»

Параметр	Описание
«Время жизни кеша изображений на агрегаторе, ч»	Определяет время кеширования (в часах) изображений «Универсального диспетчера» фермы Termidesk VDI во внутренней памяти. Позволяет сохранить изображения, полученные от «Универсального диспетчера» фермы Termidesk VDI, на некоторое время в кеше для сокращения количества обращений к нему. Значение по умолчанию: «672»
«Интервал очистки истекших JWT токенов агрегатора, ч»	Периодичность очистки (в часах) JWT-токенов «Агрегатора» с истекшим сроком действия. Значение по умолчанию: «24»

Системные настройки безопасности «Агрегатора»

Для конфигурации системных настроек безопасности следует перейти «Системные параметры - Системные настройки», выбрать раздел «Безопасность».

Доступ к разделу «Системные параметры» определяется разрешениями «Просмотр системных параметров» и «Изменение системных параметров» (см. подраздел **Назначение служебных функций администраторам**).

Доступные для редактирования параметры перечислены в столбце «Параметр» следующей таблицы (см. таблицу Системные настройки безопасности).

Таблица 245. Системные настройки безопасности

Параметр	Описание
«Длительность сессии администратора, с»	Временной интервал сессии (в секундах), инициированной на «Агрегаторе администратора». Значение по умолчанию: «14400»
«Доступ к веб-части системным пользователем»	Возможность системному администратору подключаться к «Агрегатору администратора»
«GID системной группы администратора»	Идентификатор группы администратора. Значение по умолчанию: «1001»
«Длительность сессии пользователя, с»	Временной интервал (в секундах) сессии пользователя. Параметр влияет на длительность сессии пользователя в «Агрегаторе пользователя». Вне зависимости от того, активен пользователь или нет, каждую секунду происходит уменьшение значения параметра на 1, при достижении значения 0 подключение пользователя завершится, при этом в системном трее на пользовательской рабочей станции отобразится уведомление от приложения «Клиент»: «Ваш сеанс завершился». В журнале «Клиента» отражаются события как получения параметра («userSessionLength»), так и завершения сессии по таймауту

Параметр	Описание
«Максимум попыток входа Администраторов»	Пороговое положительное значение числа неудачных попыток входа администратора. Параметр может быть изменен только администратором. Значение «0» эквивалентно «без ограничений». Значение по умолчанию: «0»
«Максимум попыток входа Персонала»	Пороговое положительное значение числа неудачных попыток входа субъектов, не относящихся к администратору. Значение «0» эквивалентно «без ограничений» Значение по умолчанию: «3»
«Максимум попыток входа Пользователей»	Пороговое положительное значение числа неудачных попыток входа пользователей. Значение «0» эквивалентно «без ограничений» Значение по умолчанию: «3»
«Список доверенных прокси»	Настройка списка доверенных прокси-серверов в сети для определения клиентского IP-адреса. Позволяет определить оригинальный клиентский IP-адрес в случае использования прокси-серверов и балансировщиков нагрузки. Поиск в списке клиентских IP-адресов производится с самого правого, пропуская все адреса из списка доверенных прокси-серверов. Первый несовпадающий IP-адрес будет целевым. Значение задается в виде списка IP-адресов, указанных через запятую. По умолчанию параметр пуст

АГРЕГАТОР. СИСТЕМА АУДИТА

Системные настройки аудита «Агрегатора»

Для конфигурации системных настроек аудита следует перейти «Системные параметры - Системные настройки», выбрать раздел «Аудит».

Доступ к разделу «Системные параметры» определяется разрешениями «Просмотр системных параметров» и «Изменение системных параметров» (см. подраздел **Назначение служебных функций администраторам**).

Доступные для редактирования администратору Termidesk VDI параметры перечислены в столбце «Параметр» следующей таблицы (см. таблицу Системные настройки аудита).

События аудита, регистрируемые Агрегатором, приведены в подразделе **Описание шаблонов событий аудита**.

Таблица 246. Системные настройки аудита

Параметр	Описание
«Использовать "строгий" режим аудита»	Управление использованием «строгого» режима аудита. Этот режим аудита запрещает внесение изменений в часть настроек при недоступности БД (таблицы `termidesk_audit_event_log_v2`). Значение по умолчанию: «Нет»
«Использовать формат CEF»	Управление использованием формата CEF для записи событий аудита. События аудита в этом формате: • записываются в таблицу БД AuditEventV2, если параметр «Сохранение в БД» активирован; • записываются в локальный файл журнала, если параметр «Сохранение в файл журнала» активирован. Потребуется выполнить дополнительную настройку (см. подраздел **Использование формата CEF**); • отправляются на отдельный syslog-сервер, если параметр «Отправка в Syslog» активирован и заданы параметры syslog-сервера. Значение по умолчанию: «Нет»
«Сохранение в БД»	Выбор сохранения событий аудита в БД
«Время хранения записи в БД, сут»	Время хранения (в сутках) записей событий аудита в БД. Удаление устаревших записей аудита выполняется периодической задачей каждые 24 часа. Значение по умолчанию: «7»
«Максимум удаляемых событий»	Максимальное количество удаляемых событий в журнале аудита. Значение по умолчанию: «1000»
«Сохранение в файл журнала»	Выбор сохранения событий аудита в отдельный файл журнала `/var/log/termidesk/audit.log`. Значение по умолчанию: «Нет»
«Отправка в Syslog»	Направление логирования на отдельный syslog-сервер. Значение по умолчанию: «Нет»
«Хост»	IP-адрес или имя узла, на котором развёрнута служба syslog-сервера. Значение по умолчанию: «localhost»
«Протокол»	Выбор протокола работы для службы syslog-сервера. Доступные значения: «UDP», «TCP», «TLS». При использовании протокола «TLS» необходимо установить на «Агрегатор» корневой сертификат ЦС, использующийся в syslog-сервере, согласно подразделу **Установка корневого сертификата центра сертификации** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса». Значение по умолчанию: «UDP»
«Порт»	Порт, на котором находится служба syslog-сервера. Значение по умолчанию: «514»

Параметр	Описание
«Категория сообщения»	Выбор категории сообщений syslog, которые будут записываться в журнал аудита. Параметр не влияет на состав регистрируемых событий и не учитывается при записи в файл журнала. Значение по умолчанию: «local7»
«Интервал удаления устаревших записей аудита, с»	Периодичность (в секундах) удаления устаревших записей событий аудита в БД. Удаление записей выполняется после истечения срока хранения, заданного в параметре «Время хранения записи в БД, сут». Значение по умолчанию: «86400»

Описание шаблонов событий аудита «Агрегатора»

Типы данных регистрируемой информации событий аудита

При фиксации событий аудита используется ряд типов данных регистрируемой информации, состав которых может отличаться для разных событий (см. таблицу Типы данных регистрируемой информации).

Таблица 247. Типы данных регистрируемой информации

Тип данных	Описание
Дата/время	Дата и время указываются в формате: `DD.MM.YYYY, hh:mm:ss`, где: `DD.MM.YYYY` обозначает «день» - «месяц» - «год»; `hh:mm:ss` обозначает элементы времени «час» - «минута» - «секунда»; «`.`» и «`:`» используются как разделители в обозначениях даты и времени дня соответственно
Имя/логин	Идентификационные данные субъекта, совершающего доступ к объекту
Наименование параметра/секции/политики	Указывает объект, над которым производится действие
Значение	Указывается значение, которое принимал или принял объект после выполнения над ним операции
Тип объекта/сущности	Указывает тип объекта, над которым производится действие
Действие	Название операции, которую совершил субъект над объектом
Результат	Результат выполнения действия
Уровень важности	Показатель критичности события
Идентификатор	Указывают уникальную (для соответствующего объекта) последовательность чисел для его однозначной идентификации
IP-адрес	32-битовое число. Формой записи IP-адреса является запись в виде четырех десятичных чисел значением от 0 до 255, разделенных точками (например, 192.0.2.1)

Типы и шаблоны регистрируемых событий аудита

Список регистрируемых событий аудита и шаблоны к ним приведены в таблице (см. таблицу Список типов и шаблонов регистрируемых событий аудита).

Для запросов, выполняемых без аутентификации, указывается пользователь AnonymousUser(AnonymousAuth). Включение записи таких событий управляется параметром INTERNAL_AUDIT в конфигурационном файле /etc/opt/termidesk-vdi/termidesk.conf.

Таблица 248. Список типов и шаблонов регистрируемых событий аудита

Событие	Состав регистрируемой информации	Шаблон регистрации события
Базовый класс событий		
Изменение объектов пользователями base.InformationEvent	Регистрируется: • наименование домена аутентификации (user_auth); • имя пользователя (user_name); • тип учетной записи пользователя (user_type); • выполненное действие (action); • имя объекта, над которым произошло действие (obj_name); • тип объекта, над которым произошло действие (obj_type); • внутреннее наименование причины изменения (reason); • результат выполнения действия (result); • измененные данные (updated_data)	«[user_type] [user_name] из домена [user_auth] выполнил операцию [action] над объектом [obj_name] ([obj_type]) с помощью [reason]. Результат - [result]. Измененные данные: [updated_data]»
События, связанные с объектом «Узлы»		
Добавление узла aggregator.audit.events.provider.create	Регистрируется: • название узла (provider_name); • имя пользователя (username); • название домена аутентификации (authenticator_name); • название фермы поставщиков ресурсов (farm_name)	«Пользователь [username] ([authenticator_name]) создал узел [provider_name] в ферме [farm_name]»
Изменение узла aggregator.audit.events.provider.update	Регистрируется: • название узла (provider_name); • имя пользователя (username); • название домена аутентификации (authenticator_name); • название фермы поставщиков ресурсов (farm_name)	«Пользователь [username] ([authenticator_name]) обновил узел [provider_name] в ферме [farm_name]»

Событие	Состав регистрируемой информации	Шаблон регистрации события
Удаление узла aggregator.audit.events.provider.delete	Регистрируется: • название узла (provider_name); • имя пользователя (username); • название домена аутентификации (authenticator_name); • название фермы поставщиков ресурсов (farm_name)	«Пользователь [username] ([authenticator_name]) удалил узел [provider_name] из фермы [farm_name]»
Включение технического обслуживания узла aggregator.audit.events.server.maintenance.on	Регистрируется: • название узла (provider_name); • имя пользователя (username)	«Пользователь [username] включил техобслуживание Узла [provider_name]»
Отключение технического обслуживания узла aggregator.audit.events.server.maintenance.off	Регистрируется: • название узла (provider_name); • имя пользователя (username)	«Пользователь [username] отключил техобслуживание Узла [provider_name]»
События, связанные с объектом «Ферма поставщик ресурсов»		
Добавление фермы поставщиков ресурсов aggregator.audit.events.farms.create	Регистрируется: • название фермы поставщиков ресурсов (farm_name); • название домена аутентификации (authenticator_name); • имя пользователя (username)	«Пользователь [username] ([authenticator_name]) создал ферму [farm_name]»
Изменение фермы поставщиков ресурсов aggregator.audit.events.farms.update	Регистрируется: • название фермы поставщиков ресурсов (farm_name); • название домена аутентификации (authenticator_name); • имя пользователя (username)	«Пользователь [username] ([authenticator_name]) обновил ферму [farm_name]»
Удаление фермы поставщиков ресурсов aggregator.audit.events.farms.delete	Регистрируется: • название фермы поставщиков ресурсов (farm_name); • название домена аутентификации (authenticator_name); • имя пользователя (username)	«Пользователь [username] ([authenticator_name]) удалил ферму [farm_name]»

Событие	Состав регистрируемой информации	Шаблон регистрации события
Включение технического обслуживания фермы поставщиков ресурсов aggregator.audit.events.server.maintenance.on	Регистрируется: • название фермы поставщиков ресурсов (farm_name); • имя пользователя (username)	«Пользователь [username] включил техобслуживание Фермы [farm_name]»
Отключение технического обслуживания фермы поставщиков ресурсов aggregator.audit.events.server.maintenance.off	Регистрируется: • название фермы поставщиков ресурсов (farm_name); • имя пользователя (username)	«Пользователь [username] отключил техобслуживание Фермы [farm_name]»
События, связанные с объектом «Сайт»		
Добавление сайта aggregator.audit.events.site.create	Регистрируется: • название сайта (site_name); • название домена аутентификации (authenticator_name); • имя пользователя (username)	«Пользователь [username] ([authenticator_name]) создал сайт [site_name]»
Изменение сайта aggregator.audit.events.site.update	Регистрируется: • название сайта (site_name); • название домена аутентификации (authenticator_name); • имя пользователя (username)	«Пользователь [username] ([authenticator_name]) обновил сайт [site_name]»
Удаление сайта aggregator.audit.events.site.delete	Регистрируется: • название сайта (site_name); • название домена аутентификации (authenticator_name); • имя пользователя (username)	«Пользователь [username] ([authenticator_name]) удалил сайт [site_name]»
Добавление правила aggregator.audit.events.rule.create	Регистрируется: • имя пользователя (username); • название домена аутентификации (authenticator_name); • название правила для сайта (rule_name); • название сайта (site_name)	«Пользователь [username] ([authenticator_name]) создал правило [rule_name] в сайте [site_name]»

Событие	Состав регистрируемой информации	Шаблон регистрации события
Изменение правила aggregator.audit.events.rule.update	Регистрируется: • имя пользователя (username); • название домена аутентификации (authenticator_name); • название правила для сайта (rule_name); • название сайта (site_name)	«Пользователь [username] ([authenticator_name]) обновил правило [rule_name] в сайте [site_name]»
Удаление правила aggregator.audit.events.rule.delete	Регистрируется: • имя пользователя (username); • название домена аутентификации (authenticator_name); • название правила для сайта (rule_name); • название сайта (site_name)	«Пользователь [username] ([authenticator_name]) удалил правило [rule_name] в сайте [site_name]»
Включение технического обслуживания сайта aggregator.audit.events.site.maintenance.on	Регистрируется: • название сайта (site_name); • имя пользователя (username)	«Пользователь [username] включил техобслуживание Сайта [site_name]»
Отключение технического обслуживания сайта aggregator.audit.events.site.maintenance.off	Регистрируется: • название сайта (site_name); • имя пользователя (username)	«Пользователь [username] отключил техобслуживание Сайта [site_name]»
События, связанные с объектом «Шлюз»		
Добавление шлюза aggregator.api.webui.gateway.create	Регистрируется: • название шлюза (gateway_name); • имя пользователя (username); • название домена аутентификации (authenticator_name)	«Пользователь [username] ([authenticator_name]) создал шлюз [gateway_name]»
Изменение шлюза aggregator.api.webui.gateway.update	Регистрируется: • название шлюза (gateway_name); • имя пользователя (username); • название домена аутентификации (authenticator_name)	«Пользователь [username] ([authenticator_name]) обновил шлюз [gateway_name]»
Удаление шлюза aggregator.api.webui.gateway.delete	Регистрируется: • название шлюза (gateway_name); • имя пользователя (username); • название домена аутентификации (authenticator_name)	«Пользователь [username] ([authenticator_name]) удалил шлюз [gateway_name]»

Событие	Состав регистрируемой информации	Шаблон регистрации события
События, связанные с объектом «Домен аутентификации»		
Создание домена аутентификации aggregator.audit.events.authenticators.create	Регистрируется: • название домена аутентификации (authenticator_name); • имя пользователя (username)	«Пользователь [username] ([authenticator_name]) создал аутентификатор [authenticator_name]»
Изменение домена аутентификации aggregator.audit.events.authenticators.update	Регистрируется: • название домена аутентификации (authenticator_name); • имя пользователя (username)	«Пользователь [username] ([authenticator_name]) обновил аутентификатор [authenticator_name]»
Удаление домена аутентификации aggregator.audit.events.authenticators.delete	Регистрируется: • название домена аутентификации (authenticator_name); • имя пользователя (username)	«Пользователь [username] ([authenticator_name]) удалил аутентификатор [authenticator_name]»
Добавление группы пользователей aggregator.audit.events.authenticators.group.create	Регистрируется: • название домена аутентификации (authenticator_name); • имя пользователя (username); • название группы домена аутентификации (group_name)	«Пользователь [username] ([authenticator_name]) создал группу [group_name] в домене [authenticator_name]»
Изменение группы пользователей aggregator.audit.events.authenticators.group.update	Регистрируется: • название домена аутентификации (authenticator_name); • имя пользователя (username); • название группы домена аутентификации (group_name)	«Пользователь [username] ([authenticator_name]) обновил группу [group_name] в домене [authenticator_name]»
Удаление группы пользователей aggregator.audit.events.authenticators.group.delete	Регистрируется: • название домена аутентификации (authenticator_name); • имя пользователя (username); • название группы домена аутентификации (group_name)	«Пользователь [username] ([authenticator_name]) удалил группу [group_name] у домена [authenticator_name]»
Изменение пользователя в домене aggregator.audit.events.authenticators.user.update	Регистрируется: • имя пользователя, который производит действие (username); • идентификатор пользователя, над которым производится действие (updated_user)	«Пользователь [username] ([authenticator_name]) обновил пользователя [updated_user]»

Событие	Состав регистрируемой информации	Шаблон регистрации события
Удаление пользователя из домена aggregator.audit.events.authenticators.user.delete	Регистрируется: • имя пользователя, который производит действие (username); • идентификатор пользователя, над которым производится действие (deleted_user)	«Пользователь [username] ([authenticator_name]) удалил пользователя [deleted_user]»
Создание пользователя при входе aggregator.audit.events.authenticators.user.create	Регистрируется: • название домена аутентификации (authenticator_name); • имя пользователя (username)	«При логине был создан пользователь [username] ([authenticator_name])»
События, связанные с объектом «Шаблоны техобслуживания»		
Создание шаблона техобслуживания aggregator.audit.events.maintenance.template.create	Регистрируется: • название шаблона техобслуживания (template_name); • название домена аутентификации (authenticator_name); • имя пользователя (username)	«Пользователь [username] ([authenticator_name]) создал шаблон техобслуживания [template_name]»
Изменение шаблона техобслуживания aggregator.audit.events.maintenance.template.update	Регистрируется: • название шаблона техобслуживания (template_name); • название домена аутентификации (authenticator_name); • имя пользователя (username)	«Пользователь [username] ([authenticator_name]) обновил шаблон техобслуживания [template_name]»
Удаление шаблона техобслуживания aggregator.audit.events.maintenance.template.delete	Регистрируется: • название шаблона техобслуживания (template_name); • название домена аутентификации (authenticator_name); • имя пользователя (username)	«Пользователь [username] ([authenticator_name]) удалил шаблон техобслуживания [template_name]»
События, связанные с пользователем		
Получение пользователем списка доступных ресурсов aggregator.audit.events.client.views.services_list	Регистрируется: • название домена аутентификации (authenticator_name); • имя пользователя (username)	«Пользователь [username] ([authenticator_name]) получил список доступных ресурсов»

Событие	Состав регистрируемой информации	Шаблон регистрации события
Вход пользователя в систему через веб-интерфейс aggregator.audit.events.web.UserLogin	Регистрируется: • название домена аутентификации (authenticator_name); • имя пользователя (username); • тип учетной записи пользователя (user_type); • IP-адрес, с которого был сделан запрос (ip); • тип портала (portal)	«[user_type] [username] ([authenticator_name]) вошел в систему с ip-адреса [ip] через [portal]»
Неудачная попытка регистрации пользователя aggregator.audit.events.web.UserLoginForbidden	Регистрируется: • IP-адрес, с которого был сделан запрос (ip); • ошибка аутентификации (error); • запрос авторизации (handler_path)	«Выполнена неудачная попытка регистрации пользователя api - [handler_path] ошибка - [error] ip - [ip]»
Выход пользователя из веб-интерфейса aggregator.audit.events.web.UserLogout	Регистрируется: • название домена аутентификации (authenticator_name); • имя пользователя (username); • тип учетной записи пользователя (user_type); • IP-адрес, с которого был сделан запрос (ip); • тип портала (portal)	«[user_type] [username] ([authenticator_name]) вышел из системы (ip-адрес [ip]) через [portal]»
Предоставление пользователю параметров подключения к ресурсу aggregator.audit.events.client.views.resource_connect	Регистрируется: • название домена аутентификации (authenticator_name); • имя пользователя (username); • IP-адрес, с которого был сделан запрос (ip)	«Пользователь [username] ([authenticator_name]) подключился к ресурсу с IP [ip]»
Запрос пользователем ресурсов aggregator.audit.events.client.views.user_requested_resource	Регистрируется: • название домена аутентификации (authenticator_name); • имя пользователя (username); • IP-адрес, с которого был сделан запрос (ip)	«Пользователь [username] ([authenticator_name]) запросил ресурс с IP [ip]»

Событие	Состав регистрируемой информации	Шаблон регистрации события
Аутентификация пользователя на «Универсальном диспетчере» aggregator.audit.events.user.authentication_on_dispatcher	Регистрируется: • название домена аутентификации (authenticator_name); • имя пользователя (username); • имя узла фермы (dispatcher_name)	«Пользователь [username] ([authenticator_name]) аутентифицировался на диспетчере подключений [dispatcher_name]»
Аутентификация пользователя на «Агрегаторе» aggregator.audit.events.user.authentication_on_aggregator_from_arm	Регистрируется: • название домена аутентификации (authenticator_name); • имя пользователя (username); • имя пользовательской рабочей станции (name)	«Пользователь [username] ([authenticator_name]) аутентифицировался на Агрегаторе с АРМ [name]»
Подключение пользователя к ВРМ aggregator.audit.events.user.connection_to_warm	Регистрируется: • название домена аутентификации (authenticator_name); • имя пользователя (username); • IP-адрес ВРМ (warm_ip); • имя ВРМ (warm_name)	«Пользователь [username] ([authenticator_name]) подключился к ВАРМ [warm_name] по ip-адресу [warm_ip]»
Подключение пользователя через «Шлюз» aggregator.audit.events.user.connection_through_gateway	Регистрируется: • название домена аутентификации (authenticator_name); • имя пользователя (username); • IP-адрес (gateway_ip); • имя «Шлюза» (gateway_name)	«Пользователь [username] ([authenticator_name]) подключился через шлюз [gateway_name] с ip-адреса [gateway_ip]»
Аутентификация пользователя на «Агрегаторе» aggregator.audit.events.web.aggregator.UserLogin	Регистрируется: • название домена аутентификации (authenticator_name); • имя пользователя (username); • IP-адрес, с которого был сделан запрос (ip); • имя ВМ (aggregator_hostname); • IP-адрес ВМ (aggregator_ip); • информация о «Клиенте» Termidesk VDI (user_agent)	«Пользователь [username] ([authenticator_name]) подключился через [user_agent] с АРМ [ip] к агрегатору [aggregator_hostname] ([aggregator_ip])»

Событие	Состав регистрируемой информации	Шаблон регистрации события
Подключение пользователя к РМ или терминальному приложению aggregator.audit.events.web.aggregator.UserConnectToVW	Регистрируется: • название домена аутентификации (authenticator_name); • имя пользователя (username); • имя «Универсального диспетчера» (dispatcher_hostname); • IP-адрес «Универсального диспетчера» (dispatcher_ip); • имя РМ (vw_hostname); • IP-адрес РМ (vw_ip); • имя шлюза (gateway_hostname); • IP-адрес шлюза (gateway_ip)	«Пользователь [username] ([authenticator_name]) подключился к ВРМ [vw_hostname] ([vw_ip]) через диспетчер [dispatcher_hostname] ([dispatcher_ip]) и шлюз [gateway_hostname] ([gateway_ip])»
События, связанные с командной строкой		
Изменение системных параметров через командную строку aggregator.audit.events.cli.SystemConfigChanged	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • IP-адрес, с которого был сделан запрос (ip); • старое значение параметра (old_value); • новое значение параметра (new_value); • имя параметра (name); • ключ параметра (key)	«[user_type] [username] ([authenticator]) изменил системный параметр [name] ([key]), старое значение - [old_value], новое значение - [new_value] (IP-адрес [ip])»
CRUD-операции с объектами через командную строку aggregator.audit.events.cli.EntityAction	Регистрируется: • имя системного пользователя, запустившего команду (username); • тип сущности (entity); • уникальный идентификатор (uuid); • тип объекта (subtype); • название объекта (name); • действие над объектом (action)	«Пользователь [username] выполнил операцию [action] для объекта [entity] ([uuid]) [subtype] [name]»
События, связанные с веб-интерфейсом		

Событие	Состав регистрируемой информации	Шаблон регистрации события
Изменение системных параметров «Универсального диспетчера» aggregator.audit.events.web.SystemConfigChanged	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • IP-адрес, с которого был сделан запрос (ip); • старое значение параметра (old_value); • новое значение параметра (new_value); • имя параметра (name); • ключ параметра (key)	«[user_type] [username] ([authenticator]) изменил системный параметр [name] ([key]), старое значение - [old_value], новое значение - [new_value] (IP-адрес [ip])»
CRUD операции с объектами через REST API web.EntityAction	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • тип учетной записи пользователя (user_type); • IP-адрес, с которого был сделан запрос (ip); • тип сущности (entity); • идентификатор (uuid); • тип объекта (subtype); • название объекта (name); • действие над объектом (action)	«[user_type] [username] ([authenticator]) выполнил операцию [action] для объекта [entity] ([uuid]) [subtype] [name] (ip-адрес [ip])»
Изменение связей тегов web.TagRelationChanged	Регистрируется: • название домена аутентификации пользователя (authenticator); • имя пользователя (username); • имя связанной сущности (name_relation_entity); • тип связанной сущности (type_relation_entity); • старые значения (old_value); • новые значения (new_value)	«[user_type] [username] ([authenticator]) изменил теги у сущности [name_relation_entity] ([type_relation_entity]), старое значение - [old_value], новое значение - [new_value]»

Форматы регистрируемых событий аудита и их примеры

Каждая запись аудита в веб-интерфейсе отображается в формате: [Дата и время][Наименование события][Текст события согласно шаблону] [Уровень важности]

Пример отображения записи аудита «Создание домена аутентификации» в веб-интерфейсе на странице «Журналы - Аудит»:

Дата и время	Уровень	Событие	Описание
06.06.2025, 12:35:24	Высокий	aggregator.audit.events.aggregator.authenticators.create	«Пользователь "admin123(Встроенный)" создал аутентификатор "1"»

Поддерживается запись каждого события аудита в формате CEF:

`[Дата и время]|[Узел]|[CEF:версия]|[Uveon]|[Aggregator]|[Версия Termidesk VDI]|[Идентификатор объекта]|[Наименование события]|[Объекты события]|[Уровень важности]`

Пример события «Вход пользователя в систему через веб-интерфейс» в формате CEF:

```
2025-05-16T16:06:10.334400 ash-ast181-or CEF:0|Uveon|Aggregator|6.0-rc1|api/auth/v7.0/login:POST|Вход пользователя в систему через веб-интерфейс|3|suser=AnonymousUser msg={'username': 'admin123(Встроенный)', 'ip': '10.10.100.11'}
```

Для активации хранения аудита в формате CEF нужно обратиться к подразделу **Использование формата CEF**.

Формат CEF в «Агрегаторе»

Termidesk VDI поддерживает запись каждого события аудита в формате Common Event Format (CEF).

Формат CEF описывается следующим набором обязательных полей:

- Version - версия формата CEF;
- Device Vendor, Device Product и Device Version - однозначная идентификация источника события;
- Signature ID - уникальный идентификатор типа события;
- Name - понятное описание события;
- Severity - важность события (от 0 до 10);
- Extension - набор пар «ключ - значение».

Для использования формата CEF нужно включить использование CEF в системных параметрах аудита «Портала администратора» (перейти «Системные параметры - Системные настройки», выбрать раздел «Аудит»).

Для того, чтобы события в формате CEF корректно сохранялись в локальный файл журнала, нужно:

- включить сохранение событий в файл в системных параметрах аудита «Портала администратора» (перейти «Системные параметры - Системные настройки», выбрать раздел «Аудит»);
- отредактировать шаблон отправки сообщений в каталоге `/etc/opt/termidesk-vdi/templates`:
  - закомментировать:

```
template t_termidesk_audit { template("[$ISODATE] $MESSAGE\n"); };
```

- раскомментировать:

```
template t_termidesk_audit { template("$MESSAGE\n"); };
```

- выполнить:

```
sudo /opt/termidesk/sbin/termidesk-config update_logger_config
```

- включить использование CEF в системных параметрах аудита «Портала администратора» (перейти «Системные параметры - Системные настройки», выбрать раздел «Аудит»).

АГРЕГАТОР. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

Утилита `termidesk-vdi-manage` в «Агрегаторе»

Утилита `termidesk-vdi-manage` используется для настройки «Универсального диспетчера» из интерфейса командной строки.

Для вызова утилиты следует:

- в интерфейсе командной строки переключиться на пользователя `termidesk`:

```
sudo -u termidesk bash
```

- вывести список команд утилиты:

```
/opt/termidesk/sbin/termidesk-vdi-manage help
```

Каждая подкоманда в приведенных ниже командах поддерживает вывод справки через ключ `-h`. В командах поддерживаются аргументы вывода:

- `--version` - вывод версии программы;
- `-v {0,1,2,3}`, `--verbosity {0,1,2,3}` - уровень детализации сообщений;
- `--settings <настройки>` - путь к модулю настроек Python;
- `--pythonpath <каталог Python>` - каталог, который нужно добавить в путь Python, например `/home/djangoprojects/myproject`;
- `--traceback` - вызов исключений;
- `--no-color` - вывод команды без подсвечивания;
- `--force-color` - вывод команды с принудительным подсвечиванием;
- `--skip-checks` - пропуск проверки системы.

Для управления параметрами поставщиков ресурсов, доменов аутентификации, протоколов доставки и других компонентов, настраиваемых через «Агрегатор администратора» Termidesk VDI, следует обратиться к командам секции `[termidesk]`.

Большая часть команд из вывода `/opt/termidesk/sbin/termidesk-vdi-manage help` предназначена для работы с БД и фреймворком Django и не приведена здесь.

Команды секции `[termidesk]` приведены в таблице (см. таблицу Команды секции `[termidesk]`).

Таблица 249. Команды секции `[termidesk]`

Параметр	Описание
`aggr_clear_resources`	Удаляет из БД информацию о РМ пользователей. Для просмотра списка ключей следует воспользоваться аргументом `-h`: `/opt/termidesk/sbin/termidesk-vdi-manage aggr_clear_resources -h`
`tdsk_auth`	Управление доменами аутентификации. Для просмотра списка ключей следует воспользоваться аргументом `-h`: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_auth -h` Поддерживаются подкоманды: • `create` - создание домена аутентификации; • `list` - вывод списка доменов аутентификации; • `remove` - удаление домена аутентификации; • `login` - аутентификация в указанный домен; • `logout` - завершение сессии.
`tdsk_auth create`	Создание домена аутентификации. Подкоманда `create` принимает аргументы: • `--type` - задание типа домена аутентификации. Доступны: `SimpleLdapAuthenticator` («Microsoft AD DS/LDAP»), `OIDCAuth` («OIDC»), BuiltinAuthenticator («Встроенный»); • `--params` - задание параметров домена аутентификации. Формат: `имя1=значение1 имя2=значение2` и т.д. Доступные параметры для указанного типа домена аутентификации можно получить через команду `--list` , например: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_auth create --type OIDCAuth --name test --small_name test` • `--list` - вывод параметров домена аутентификации; • `--test` - проверка параметров без создания домена аутентификации; • `--quiet` - вывод только сообщений об ошибках; • `--name <ИМЯ>` - имя домена аутентификации; • `--small_name <короткое имя>` - короткое имя домена аутентификации. Допустимые символы: a-z, A-Z, 0-9. Максимальная длина 32 символа; • `--priority <приоритет>` - числовое значение приоритета домена аутентификации, по умолчанию «1»; • `--comments <комментарий>` - комментарий к создаваемому домену

Параметр	Описание
`tdsk_auth list`	Вывод списка доменов аутентификации. Подкоманда `list` принимает аргумент `--output json` для вывода списка в формате JSON
`tdsk_auth remove`	Удаление домена аутентификации. Подкоманда `remove` принимает аргументы: • `--output json` - вывод параметров в формате JSON; • `--silent` - «тихое» удаление для выполнения команды из исполняемого файла; • `--uuid <идентификатор>` - идентификатор объекта для удаления.
`tdsk_auth login`	Аутентификация в указанный домен. Подкоманда `login` принимает аргументы: • `--uuid <идентификатор>` - идентификатор объекта для аутентификации; • `--small_name <короткое имя>` - короткое имя домена аутентификации; • `--output json` - вывод параметров в формате JSON.
`tdsk_auth logout`	Завершение сессии в указанном домене. Подкоманда `logout` принимает аргументы: • `--token <токен>` - токен сессии пользователя; • `--output json` - вывод параметров в формате JSON
`tdsk_clear_cache`	Удаляет ненужные кешированные данные. Для просмотра списка ключей следует воспользоваться аргументом `-h`: `/opt/termidesk/sbin/termidesk-vdi-manage tdsk_clear_cache -h`
`tdsk_clearsessions`	Порционная очистка сессий. Поддерживаются аргументы: • `-chunk <количество>` - количество сессий для удаления, по умолчанию 1000
`tdsk_config`	Управление системными настройками. Поддерживаются подкоманды: • `list` - вывод конфигурационных параметров и их значений; • `set` - установка значения конфигурационному параметру
`tdsk_config set`	Установка значения конфигурационному параметру. Подкоманда `set` принимает аргументы: • `--key <ключ>` - ключ параметра; • `--value <значение>` - значение параметра

Параметр	Описание
tdsk_graph_models	Создание файла GraphViz с описанием моделей БД для указанных имен приложений. Можно передать несколько имен приложений, и все они будут объединены в одну модель. Поддерживаются аргументы: • app_label - наименование приложения; • --pygraphviz - использование PyGraphViz для создания изображения; • --pydot - использование PyDot(Plus) для создания изображения; • --disable-fields, -d - не показывать поля; • --group-models, -g - сгруппировать модели в соответствии с их применением; • --all-applications, -a - включить все приложения для вывода модели; • --output <путь к файлу>, -o <путь к файлу> - запись вывода в файл; • --layout <макет>, -l <макет> - использование макета GraphViz для визуализации. Поддерживаются: circo, dot, fdpneato, nop, nop1, nop2, twopi; • --verbose-names, -n - использование подробных имен для моделей и полей; • --language <локализация>, -L <локализация> - указания языка, который будет использоваться для подробных имен; • --exclude-columns <столбцы>, -x <столбцы> - исключение определенных столбцов; • --exclude-models <модели>, -X <модели> - исключение определенных моделей; • --include-models <модели>, -I <модели> - ограничение только указанными моделями; • --inheritance, -e - включение наследования (используется по умолчанию); • --no-inheritance, -E - выключение наследования
tdsk_setup	Настройка Termidesk VDI после установки. Выполняет миграцию данных, создание таблицы кеша данных, сбор статических файлов, компиляцию файлов
tdsk_version	Получение версии «Агрегатора»

Утилита termidesk-config в «Агрегаторе»

Утилита termidesk-config используется для переопределения настроек, заданных на этапе установки, и вносит изменения в конфигурационный файл termidesk.conf и /etc/default/termidesk-vdi.local.

Для вызова утилиты следует:

- в интерфейсе командной строки перейти в каталог /opt/termidesk/sbin/:

```
cd /opt/termidesk/sbin/
```

- выполнить запуск:

```
sudo ./termidesk-config
```

- откроется интерфейс утилиты (см. рисунок Интерфейс утилиты termidesk-config).

```
+---------------Настройка сервера Термидеск-----------------+
| Выберите раздел для настройки:                            |
| +-------------------------------------------------------+ |
| | Настройка путей к журналам и конфигурации             | |
| | Режим работы узла [BROKER]                            | |
| | Роли узла (сервера) [TERMQ]                           | |
| | Задание имени службам узла                            | |
| | Способ хранения паролей [config]                      | |
| | Настройка хранилища OpenBao                           | |
| | Задание ключа DJANGO                                  | |
| | Защита подключения к СУБД [Disable]                   | |
| | Тип установки СУБД [single]                           | |
| | Настройка подключения к СУБД                          | |
| | Защита подключения к RabbitMQ/TermideskMQ [Disable]   | |
| | Настройка подключения к RabbitMQ/TermideskMQ          | |
| | Настройка параметров клиента TermideskMQ              | |
| | Настройки подключения к Fluentd                       | |
| +----↓(+)-----------------------------------------60%-----+ |
+-----------------------------------------------------------+
|              <Выбрать>          < Выход >                 |
+-----------------------------------------------------------+
```

Рисунок 136. Интерфейс утилиты termidesk-config

Доступны следующие функции утилиты:

После выполнения изменений в любом из разделов рекомендуется воспользоваться пунктом «Перезапуск служб» для применения изменений.

- «Настройка путей к журналам и конфигурации: позволяет настроить каталоги для хранения конфигурации Termidesk VDI:
  - «Расположения конфигурации»: каталог, в котором будет расположен файл `termidesk.conf` (параметр `ETC` файла `/etc/default/termidesk-vdi.local`);
  - «Хранения журналов»: каталог, в котором будут расположены файлы журналов (параметр `LOG_DIR`);

Параметр `LOG_DIR` доступен для изменения как в пункте «Место хранения журналов», так и в пункте «Настройка журналирования» - «Место хранения журналов». В обоих случаях фактически меняется значение только в параметре `LOG_DIR` конфигурационного файла `termidesk.conf`.

  - «Шаблонов syslog/logrotate»: каталог, в котором будут расположены шаблоны для настройки регистрации событий и журналирования (параметр `TEMPLATES_DIR` файла `/etc/default/termidesk-vdi.local`);
- «Режим работы узла»: позволяет задать режим работы (параметр `TERMIDESK_FARM_MODE`):
  - «Диспетчер»: режим работы для фермы «Универсального диспетчера»;
  - «Агрегатор»: режим работы для фермы «Агрегатора»;

Установка «Агрегатора» должна производиться на узле, отличном от «Диспетчера».

Ранее установленный «Диспетчер» нельзя перенастроить на использование «Агрегатора».

- «Роли узла (сервера)»: позволяет изменить роли, которые запускаются на узле (параметр NODE_ROLES). Доступные роли:
  - «Портал администратора»;
  - «Портал пользователя»;
  - «Менеджер рабочих мест»;
  - «Брокер сообщений»;
- «Задание имени службам узла»: позволяет задать уникальное имя узла для его идентификации (параметр NODE_NAME);
- «Способ хранения паролей»: позволяет настроить способ хранения паролей подключения к СУБД и RabbitMQ (параметр SECRETS_STORAGE_METHOD):
  - «config» - пароли будут храниться в преобразованном виде в файле /etc/opt/termidesk-vdi/termidesk.conf;
  - «hvac» (рекомендуемый способ для безопасного хранения) - для хранения паролей будет использоваться хранилище паролей OpenBao или Hashicorp Vault (хранилище должно быть заранее создано и настроено);
  - «openbao» - для хранения паролей будет использоваться хранилище паролей OpenBao (хранилище должно быть заранее создано и настроено). В случае выбора «openbao» необходимо выполнить настройку подключения к хранилищу через функцию «Настройка хранилища OpenBao»;
- «Настройка хранилища OpenBao»: позволяет настроить параметры подключения к хранилищу и задать параметры, настроенные непосредственно на хранилище:
  - «URL хранилища» - IP-адрес или FQDN узла и порт с установленным хранилищем OpenBao (параметр SECRETS_OPENBAO_URL). Формат: http://<IP-адрес>:8200 или http://<FQDN>:8200. Подключение может выполняться по протоколу HTTPS, если OpenBao настроен соответствующим образом;
  - «Версия API OpenBao» - установленная версия API на OpenBao (параметр SECRETS_OPENBAO_KV_VERSION). Может принимать значения: 1 или 2;
  - «Путь к токену доступа к хранилищу» - путь к файлу с токеном доступа к хранилищу (параметр SECRETS_OPENBAO_TOKEN);
  - «Роль доступа Termidesk» - роль, настроенная на OpenBao, имеющая доступ к логинам и паролям (параметр SECRETS_OPENBAO_ROLE_NAME);
  - «ИД роли доступа» - идентификатор роли доступа (параметр SECRETS_OPENBAO_ROLE_ID);
  - «Путь к логину/паролю СУБД» - путь, настроенный на OpenBao для хранения логина и пароля СУБД (параметр SECRETS_OPENBAO_DB_PATH);
  - «Путь к логинам/паролям RabbitMQ» - путь, настроенный на OpenBao для хранения логинов и паролей RabbitMQ (параметр SECRETS_OPENBAO_RABBITMQ_PATH);
  - «Путь к другим секретам Termidesk» - путь, настроенный на OpenBao для хранения других логинов и паролей Termidesk VDI (параметр SECRETS_OPENBAO_TERMIDESK_PATH);
  - «Время кеширования паролей, с» - время (в секундах) хранения пароля, полученного от OpenBao, во внутренней памяти (параметр SECRETS_OPENBAO_CACHE_LIFETIME);
  - «Период проверки токена доступа, с» - интервал (в секундах) проверки актуальности токена (параметр SECRETS_OPENBAO_WATCHDOG_INTERVAL);
  - «Обновлять токен до его устар., с» - оставшееся время (в секундах) актуальности токена, по достижении которого он будет обновлен (параметр SECRETS_OPENBAO_TTL_DEADLINE);
  - «Время жизни токена, с» - время актуальности (в минутах) одноразового токена (параметр SECRETS_OPENBAO_WRAP_TTL);

  - «Пространство имён» - пространство имени, заданного на OpenBao (параметр SECRETS_OPENBAO_NAMESPACE);
- «Задание ключа DJANGO»: позволяет переопределить значение ключа DJANGO (параметр DJANGO_SECRET_KEY), создаваемого на этапе установки. Переопределение ключа может понадобиться при его компрометации;
- «Защита подключения к СУБД»: позволяет выбрать тип подключения к СУБД (параметр DBSSL);
- «Тип установки СУБД»: позволяет выбрать тип СУБД, к которой будет подключаться Termidesk VDI (параметр DB_CLUSTER_MODE);
- «Настройка подключения к СУБД»: позволяет настроить параметры подключения к СУБД:
  - «Адрес» - IP-адрес или FQDN СУБД PostgreSQL (параметр DBHOST);
  - «Адрес (узел 2)»: IP-адрес или FQDN дополнительного узла СУБД (параметр DBHOST2);
  - «Адрес (узел 3)»: IP-адрес или FQDN дополнительного узла СУБД (параметр DBHOST3);
  - «Порт» - порт, который используется для соединения с сервером БД (параметр DBPORT);
  - «Имя базы данных» - имя БД (параметр DBNAME);
  - «Имя» - имя пользователя для подключения к БД (параметр DBUSER);
  - «Пароль» - пароль пользователя в открытом виде (параметр DBPASS);
  - «Время жизни подключения, с»: максимально допустимое время (в секундах) существования одного подключения к БД (параметр DB_CONN_MAX_AGE);
  - «Кол-во задач на подключение»: количество фоновых задач, которое может быть выполнено в рамках одного подключения к БД (параметр CELERY_DB_REUSE_MAX);
  - «Таймаут подключения к СУБД, с»: время ожидания (в секундах) подключения к БД (параметр DB_CONN_TIMEOUT);
- «Защита подключения к RabbitMQ/TermideskMQ»: позволяет выбрать тип подключения к брокеру сообщений (параметр RABBITMQ_SSL);
- «Настройка подключения к RabbitMQ/TermideskMQ»: позволяет настроить параметры подключения к брокеру сообщений (параметр RABBITMQ_URL). При запросе пароль задается в открытом виде;
- «Настройка параметров клиента TermidesMQ»: позволяет настроить параметры клиентской части TermideskMQ для высокодоступной конфигурации:
  - «Идентификатор клиента»: идентификатор пула очередей сообщений (параметр TMQ_CLIENT_ID);
  - «Таймаут ожидания ответа от узла, мс»: время ожидания ответа от узла кластера TermideskMQ (параметр TMQ_TIMEOUT_AWAIT_SENDING_MESSAGE);
  - «Количество попыток запросов к узлу»: количество попыток выполнения запроса или отправки сообщение к узлу кластера TermideskMQ (параметр TMQ_PUT_RETRY_COUNT);
- «Настройки подключения к Fluentd»: позволяет настроить параметры подключения к узлу «Ретранслятора»:
  - «Время кеширования хоста и порта, с»: время (в секундах) кеширования параметров подключения к узлу «Ретранслятора» (параметр FLUENTD_CACHE);
  - «Название таблицы в хранилище»: таблица хранения событий фермы Termidesk VDI (параметр FLUENTD_TABLE);
  - «Время ожидания подключения, с»: время (в секундах) ожидания подключения к узлу «Ретранслятора» (параметр FLUENTD_LOGGER_TIMEOUT);
- «Настройка журналирования»: позволяет настроить параметры журналирования,

такие как:

- «Адрес логгера» (параметр LOG_ADDRESS);
- «Поток (facility) журнала» (параметр LOG_FACILITY);
- «Место хранения журналов» (параметр LOG_DIR);
- «Владелец файлов журналов» (параметр LOG_OWNER);
- «Группа-владелец файлов журналов» (параметр LOG_GROUP);
- «Права доступа к файлам журналов» (параметр LOG_PERM);
- «Число хранимых файлов журналов» (параметр LOG_DEEP);

- «Подробность отладочных сообщений в журналах»: позволяет выбрать уровень подробности отладочных сообщений (параметр LOG_LEVEL);
- «Аудит обращений к анонимным эндпоинтам API»: позволяет включить или отключить запись событий аудита с анонимным пользователем в БД (параметр INTERNAL_AUDIT);
- «Задание токена проверки состояния служб»: позволяет переопределить значение токена проверки состояния служб (параметр HEALTH_CHECK_ACCESS_KEY). Переопределение токена может понадобиться при его компрометации;
- «Задание токена проверки метрик служб»: позволяет переопределить значение токена проверки метрики служб (параметр METRICS_ACCESS_KEY). Переопределение токена может понадобиться при его компрометации;
- «Изменение GID встроенных администраторов»: позволяет назначить идентификатор группы, использующегося для встроенного домена. Изменение идентификатора может понадобиться, если встроенная в ОС группа администраторов отличается от astra-admin (1001) или если нужно предоставить права администрирования Termidesk VDI группе непривилегированных пользователей;
- «Язык сервера по умолчанию»: язык сервера по умолчанию согласно ISO-639-1 (параметр LANGUAGE_CODE);
- «Настройки агрегатора»: позволяет переопределить настройки портала «Агрегатор»:
  - «Путь к файлу с сопоставлением имён узлов и FQDN» - путь к файлу mapping.yaml, содержащему сопоставление между именами узлов (NODE_NAME) «Агрегатора» и их полным доменным именем (FQDN);
- «Режим mTLS сервера Termidesk»: режим mTLS для взаимодействия между компонентами Termidesk VDI (параметр MTLS_MODE);
- «Подключения mTLS»: сценарий взаимодействия между компонентами Termidesk VDI по mTLS (параметр MTLS_CONNECTIONS);
- «Настройки Брокера сообщений (экспериментальный)»: позволяет переопределить настройки экспериментального «Брокера сообщений TermideskMQ»:
  - «Адрес для подключений»: IP-адрес прослушивания входящих подключений для «Брокера сообщений TermideskMQ» (параметр TMQ_BASE_ADDRESS);
  - «Базовый порт для подключений»: базовый номер порта «Брокера сообщений TermideskMQ» для незащищенного подключения (параметр TMQ_BASE_PORT).
- «Перезапуск служб» - позволяет выполнить перезапуск служб Termidesk VDI;
- «Сертификаты» - позволяет выполнить настройку сертификатов и ключей:

Пункт «Серт. для расшифровки JWT-токена» настраивается только на узле с установленным «Универсальным диспетчером» («Портал администратора» и (или) «Портал пользователя») фермы Termidesk VDI.

Пункт «Прив. ключ для подписи JWT-токена» настраивается только на узле портала «Агрегатор» («Агрегатор администратора» и (или)

«Агрегатор пользователя»).

Оставшиеся пункты могут быть настроены на обоих узлах индивидуально.

- «Сертификат Health Check» - путь к сертификату для защищенного подключения к API проверки состояния (параметр HEALTH_CHECK_CERT);
- «Секр. ключ Health Check» - путь к ключу для защищенного подключения к API проверки состояния (параметр HEALTH_CHECK_KEY);
- «Сертификат Postgres mTLS» - путь к сертификату для защищенного подключения к СУБД (параметр DBCERT);
- «Секр. ключ Postgres mTLS» - путь к ключу для защищенного подключения к СУБД (параметр DBKEY);
- «Серт. промеж. ЦС Postgres mTLS» - путь к корневому и промежуточным сертификатам mTLS для защищенного подключения к СУБД (параметр DBCHAIN);
- «Сертификат OpenBao начального mTLS» - путь к сертификату для начального защищенного подключения к OpenBao (параметр SECRETS_OPENBAO_CLIENT_CERT);
- «Секр. ключ OpenBao начального mTLS» - путь к ключу для начального защищенного подключения к OpenBao (параметр SECRETS_OPENBAO_CLIENT_KEY);
- «Серт. промеж. ЦС OpenBao нач. mTLS» - путь к корневому и промежуточным сертификатам mTLS для начального защищенного подключения к OpenBao (параметр SECRETS_OPENBAO_SERVER_CERT);
- «Путь к серт. для втор. mTLS с OpenBao»: путь к клиентскому сертификату SSL/TLS для вторичного защищенного подключения к OpenBao (параметр SECRETS_OPENBAO_PKI_CERTS);
- «Осн. серт. для расшифровки JWT-токена» - путь к сертификату для получения значения JWT-токена портала «Агрегатор» (параметр AGGREGATOR_JWT_SSL_CERT);
- «Рез. серт. для расшифровки JWT-токена» - путь к резервному сертификату для получения значения JWT-токена портала «Агрегатор» (параметр AGGREGATOR_JWT_SSL_CERT_SECOND);
- «Секр. ключ для подписи JWT-токена» - путь к ключу для подписи JWT-токена портала «Агрегатор» (параметр AGGREGATOR_JWT_SSL_KEY);
- «Сертификат ЦС сервера RA» - путь к серверному сертификату SSL/TLS для проверки подключения к «Удаленному помощнику» (REMOTE_ASSISTANT_SERVER_CA);
- «Сертификат RabbitMQ mTLS» - путь к клиентскому сертификату SSL/TLS для защищенного подключения к RabbitMQ (CELERY_BROKER_CERT);
- «Секр.ключ RabbitMQ mTLS» - путь к клиентскому ключу SSL/TLS для защищенного подключения к RabbitMQ (CELERY_BROKER_KEY);
- «Серт. ЦС RabbitMQ mTLS» - путь к корневому сертификату ЦС SSL/TLS для защищенного подключения к RabbitMQ (CELERY_BROKER_CA);
- «Сертификат службы TermideskMQ»: путь к серверному сертификату mTLS для «Брокера сообщений TermideskMQ» (параметр TMQ_SERVER_CERT);
- «Секр. ключ службы TermideskMQ»: путь к ключу для серверного сертификата mTLS для «Брокера сообщений TermideskMQ» (параметр TMQ_SERVER_KEY);
- «Серт. ЦС службы TermideskMQ»: путь к корневому сертификату mTLS для «Брокера сообщений TermideskMQ» (параметр TMQ_SERVER_CA);
- «Публичный ключ ws-proxy»: путь к открытому ключу id_rsa.pub. Явно задавать путь следует только при использовании внешнего хранилища (WSPROXY_PUB_KEY_FILE);
- «Секретный ключ ws-proxy»: путь к озакрытому ключу id_rsa. Явно задавать путь следует только при использовании внешнего хранилища (WSPROXY_PRIV_KEY_FILE);

- «Клиентский сертификат mTLS»: путь к клиентскому сертификату mTLS для защищенного подключения. Используется для взаимной аутентификации сервера Termidesk VDI с другими компонентами (параметр `MTLS_CLIENT_CERT`);
- «Клиентский секр.ключ mTLS»: путь к клиентскому ключу mTLS для защищенного подключения. Используется для взаимной аутентификации сервера Termidesk VDI с другими компонентами (параметр `MTLS_CLIENT_KEY`);
- «Клиентский серт. ЦС mTLS»: путь к корневому сертификату ЦС mTLS для защищенного подключения. Используется для взаимной аутентификации сервера Termidesk VDI с другими компонентами (параметр `MTLS_CLIENT_CA`);
- «Файл с доверенными сертификатами»: путь к файлу с доверенным корневым сертификатом. Задается для настройки работы с сертификатами собственных ЦС (параметр `REQESTS_CA_BUNDLE`).

Утилита `scramble` в «Агрегаторе»

Утилита `scramble` предназначена для получения преобразованных значений для параметров конфигурационного файла `termidesk.conf`.

Вызов утилиты выполняется командой:

```
sudo /opt/termidesk/bin/scramble
```

Вызов справки по утилите выполняется командой:

```
sudo /opt/termidesk/bin/scramble -h
```

Параметры команды приведены в таблице (см. таблицу Параметры команды scramble).

Таблица 250. Параметры команды scramble

Параметр	Значение по умолчанию	Описание

`--value`	`Не задано`	Получение преобразованного значения. По умолчанию используется алгоритм AES-256 с увеличенным числом итераций преобразования, если не задан другой в параметре `--type`.
		
		Пример использования:
		
		• с алгоритмом по умолчанию:
		
		`/opt/termidesk/bin/scramble --value <значение>`
		
		• с указанием алгоритма:
		
		`/opt/termidesk/bin/scramble --value <значение> --type <алгоритм>`
		
		Если значение указывается в формате ключа (значение предваряется символом «-»), то следует изменить его передачу в параметр `--value:`
		
		`/opt/termidesk/bin/scramble --value=<-значение> --type AES256`

Параметр	Значение по умолчанию	Описание

--config	/etc/opt/termidesk-vdi/	Путь к каталогу, в котором расположены конфигурационные файлы termidesk.conf и cookie-файл termidesk.cookie, используемый как вектор преобразования.
		
		При изменении места хранения указанных файлов требуется передавать в утилиту scramble значение нового каталога, если необходимо получить верное преобразованное значение в параметре --value.
		
		Пример использования:
		
		`/opt/termidesk/bin/scramble --config <путь_к_каталогу> --value <значение>`
		
		Пример: предположим, что на узле с «Универсальным диспетчером» появились два каталога, хранящих его конфигурационные файлы termidesk.conf и termidesk.cookie:
		
		• /etc/opt/termidesk-vdi - содержит неактуальные параметры конфигурации;
		• /etc/opt/termidesk-vdi2 - содержит актуальные параметры конфигурации, которые должны использоваться «Универсальным диспетчером».
		
		В этом случае для того, чтобы получить верное преобразованное значение для какого-либо из параметров /etc/opt/termidesk-vdi2/termidesk.conf, может потребоваться указать утилите, какой каталог она должна использовать при работе:
		
		`/opt/termidesk/bin/scramble --config /etc/opt/termidesk-vdi2/ --value <значение>`
		
		Необязательный параметр, поскольку значение каталога передается на этапе установки. Прямое указание параметра может потребоваться в целях тестирования работы Termidesk VDI.

--type	AES256_V2	Указание алгоритма преобразования значения. Возможные значения: • AES256 - преобразование по алгоритму AES-256; • AES256_V2 - преобразование по алгоритму AES-256 с увеличенным числом итераций преобразования

АГРЕГАТОР. ГРАФИЧЕСКИЙ ИНТЕРФЕЙС

Доступ к веб-интерфейсу «Агрегатора»

Доступ веб-интерфейсу осуществляется из веб-браузера по протоколу HTTPS с указанием URL-адреса подключения.

Для подключения должны использоваться веб-браузеры с поддержкой спецификации W3C HTML5: Яндекс.Браузер версии 15.9 и выше, Google Chrome версии 46 и выше, Mozilla Firefox версии 41 и выше.

Минимально необходимое разрешение экрана монитора для работы с веб-интерфейсом - 1366x768 пикселей.

При наличии только домена аутентификации с типом «Встроенный» на странице подключения нужно заполнить экранные поля:

- «Логин пользователя» – идентификатор субъекта с ролью «Администратор»;
- «Пароль пользователя» – набор символов, подтверждающий назначение полномочий.

При последующих сеансах входа после добавления нового домена аутентификации потребуется выбрать домен аутентификации в раскрывающемся списке «Способ входа».

Для входа в систему без повторного ввода учетных данных следует установить флажок в поле «Запомнить меня».

Типы веб-интерфейса «Агрегатора»

В «Агрегаторе» определены следующие типы веб-интерфейса:

- «Агрегатор администратора» - предоставляет интерфейс для управления объединенными ресурсами (фермами) Termidesk VDI;
- «Агрегатор пользователя» - предоставляет пользовательский интерфейс «Агрегатора» без функций управления;
- «Агрегатор универсальный» - предоставляет функции обоих вариантов - «Агрегатор администратора» и «Агрегатор пользователя».

Доступный тип веб-интерфейса определяется на этапе установки.

Работа с основными функциями веб-интерфейса «Агрегатора»

Функции системной панели

Системная панель представляет собой фиксированную область в верхней части веб-интерфейса, предназначенную для отображения служебной информации и элементов управления (см. рисунок Системная панель в графическом интерфейсе управления Termidesk).

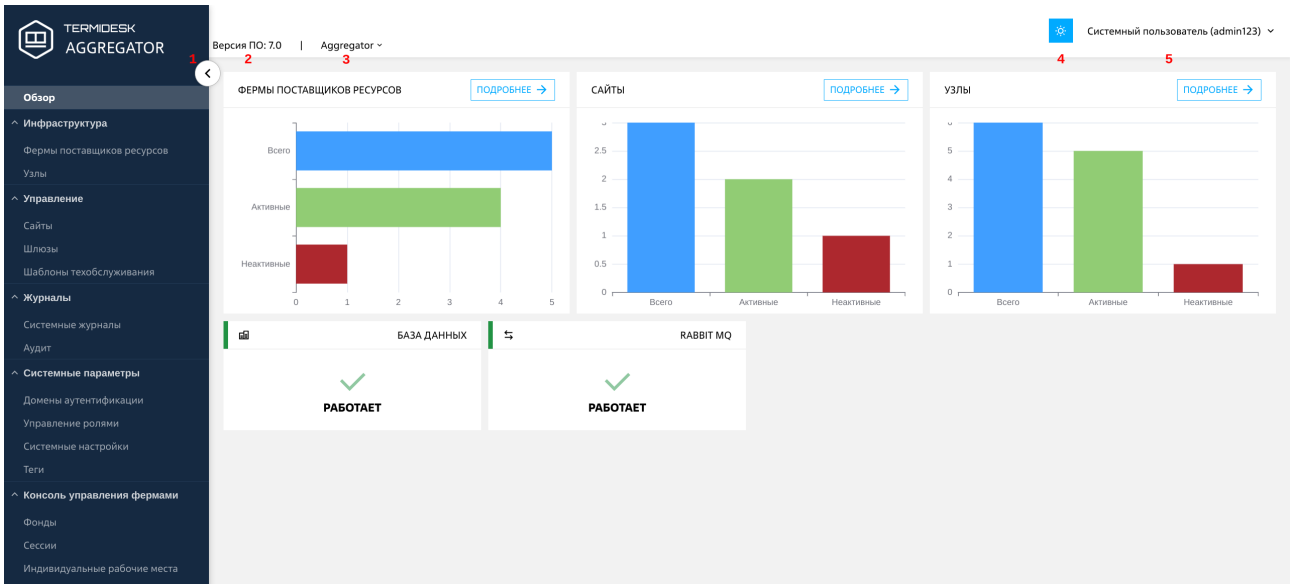


Рисунок 137. Системная панель в графическом интерфейсе управления Termidesk

Системная панель представлена следующими элементами:

- элемент (1): скрывает или отображает список функций в левой части веб-интерфейса;
- элемент (2): отображает сведения о текущей версии «Агрегатора»;
- элемент (3): отображает заданное наименование «Агрегатора». Для просмотра сведений о текущем подключении нужно нажать на наименование компонента. При этом в окне «Параметры подключения» будут отображены сведения о текущем подключении (см. рисунок Окно сведений о параметрах текущего подключения):
  - «Имя фермы» - наименование фермы «Агрегатора»;
  - «Доменное имя сервера» - FQDN фермы «Агрегатора»;
  - «Имя портала» - идентификатор узла «Агрегатора»;
  - «IP-адрес» - IP-адрес фермы «Агрегатора»;
- элемент (4): позволяет выбрать тему оформления графического интерфейса;
- элемент (5): позволяет выбрать тип веб-интерфейса или выполнить выход из веб-интерфейса.

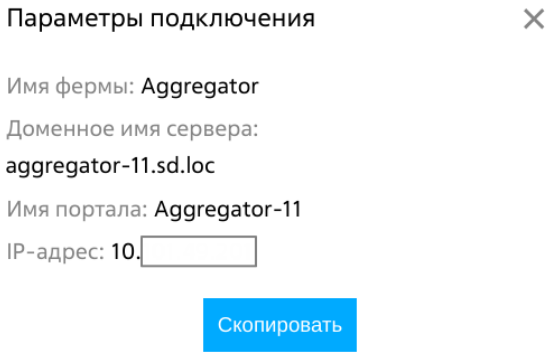


Рисунок 138. Окно сведений о параметрах текущего подключения

Функция «Обзор»

При нажатии в левой части веб-интерфейса на функцию «Обзор» визуализируется краткое представление состояния основных параметров.

В графических блоках функции «Обзор» представлены следующие элементы (см. рисунок Окно функции «Обзор» в графическом интерфейсе управления «Агрегатора»):

- «Фермы поставщиков ресурсов» - суммарное число и состояние ферм поставщиков ресурсов, добавленных на «Агрегатор»;
- «Сайты» - суммарное число и состояние сайтов, созданных на «Агрегаторе»;
- «Узлы» - суммарное число и состояние узлов ферм поставщиков ресурсов, добавленных на «Агрегатор»;
- «База данных» - состояние БД, к которой подключен «Агрегатор»;
- «Rabbit MQ» - состояние брокера сообщений, к которому подключен «Агрегатор».

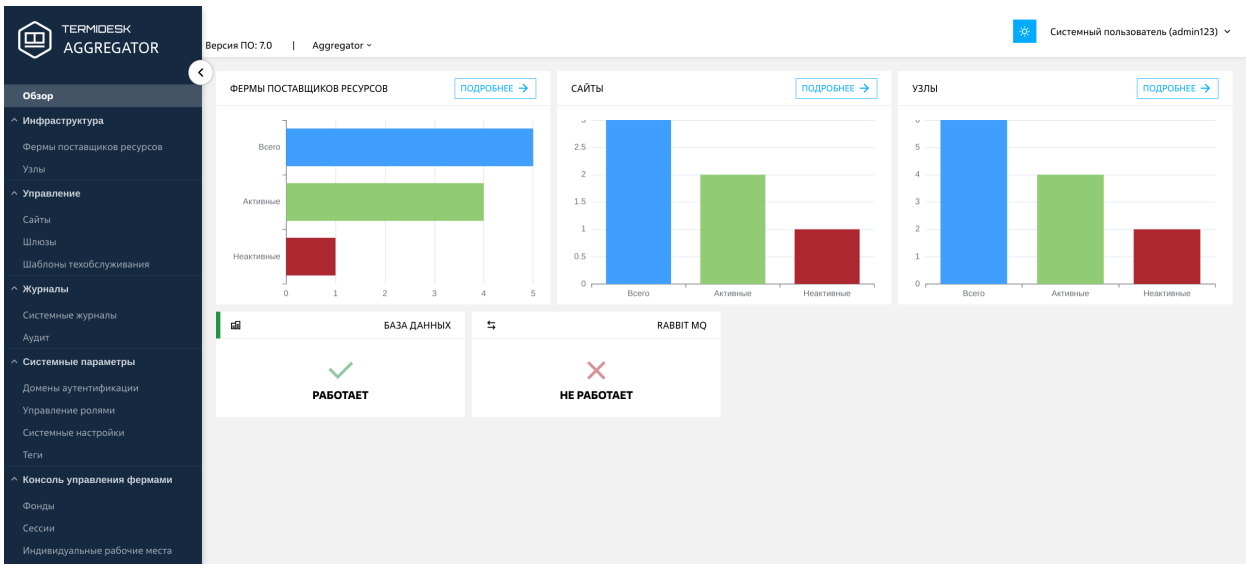


Рисунок 139. Окно функции «Обзор» в графическом интерфейсе управления «Агрегатора»

Функция «Инфраструктура»

При нажатии в левой части веб-интерфейса на функцию «Инфраструктура» открывается список, содержащий процедуры для настройки взаимодействия «Агрегатора» с фермами поставщиков ресурсов.

Функция «Инфраструктура» представлена следующими процедурами:

- «Фермы поставщиков ресурсов» - определяет настройку взаимодействия с фермами поставщиков ресурсов;
- «Узлы» - предоставляет список добавленных в ферму поставщиков ресурсов объектов типа «Узел».

Функция «Управление»

При нажатии в левой части веб-интерфейса на функцию «Управление» открывается список, содержащий процедуры для формирования эргономичного представления списка ресурсов и дополнительной настройки взаимодействия «Агрегатора» с фермами поставщиков ресурсов.

Функция «Управление» представлена следующими процедурами:

- «Сайты» - определяет настройку размещения объединенных ресурсов для пользователей;
- «Шлюзы» - определяет настройку шлюзов;
- «Шаблоны техобслуживания» - определяет настройку текстов сообщений, отправляемых пользователю при попытке подключиться к сайту, находящемуся в режиме техобслуживания.

Функция «Журналы»

При нажатии в левой части веб-интерфейса на функцию «Журналы» открывается список процедур для просмотра событий субъектов доступа, а также событий функционирования «Агрегатора».

Функция «Журналы» представлена следующими процедурами:

- «Системные журналы» - позволяет просматривать события функционирования «Агрегатора»;

- «Аудит» - позволяет просматривать события аудита из веб-интерфейса «Агрегатора».

Функция «Системные параметры»

При нажатии в левой части веб-интерфейса на функцию «Системные параметры» открывается список процедур для настройки «Агрегатора».

Функция «Системные параметры» представлена следующими процедурами:

- «Домены аутентификации» - определяет настройку взаимодействия с источниками сведений о субъектах и их полномочиях;
- «Управление ролями» - определяет назначение служебных функций администраторам «Агрегатора»;
- «Системные настройки» - определяет настройку системных параметров «Агрегатора»;
- «Теги» - определяет параметры тегов, используемых для маркировки и группировки объектов системы «Агрегатора».

Функция «Консоль управления фермами»

При нажатии в левой части веб-интерфейса на функцию «Консоль управления фермами» открывается список процедур для управления фондами, сессиями пользователей и рабочими местами, размещенными в фермах поставщиков ресурсов.

Функция «Консоль управления фермами» представлена следующими процедурами:

- «Фонды» - позволяет управлять фондами, размещенными в фермах поставщиков ресурсов;
- «Сессии» - позволяет управлять сессиями подключенных к фондам пользователей;
- «Индивидуальные рабочие места» - позволяет управлять рабочими местами фондов.

АГРЕГАТОР. ЖУРНАЛИРОВАНИЕ

Системные настройки журналирования «Агрегатора»

Для конфигурации системных настроек журналирования следует перейти «Системные параметры - Системные настройки», выбрать раздел «Логирование».

Доступ к разделу «Системные параметры» определяется разрешениями «Просмотр системных параметров» и «Изменение системных параметров» (см. подраздел **Назначение служебных функций администраторам**).

Доступные для редактирования администратору Termidesk VDI параметры перечислены в столбце «Параметр» следующей таблицы (см. таблицу Системные настройки журналирования).

Локальные файлы журналов, регистрируемые «Агрегатором», приведены в подразделе **Журналы**. Для изменения уровня журналирования в локальных файлах журналов следует обратиться к подразделу **Настройка журналирования**.

Таблица 251. Системные настройки журналирования

Параметр	Описание
«Логирование Syslog»	Перенаправление потока событий мониторинга на отдельный syslog-сервер

Параметр	Описание
«Хост 1»—«Хост 3»	IP-адреса или имена узлов, на которых развернута служба syslog-сервера
«Протокол»	Выбор протокола работы для службы syslog-сервера. Доступные значения: «UDP», «TCP», «TLS». При использовании протокола «TLS» необходимо установить на узел с «Универсальным диспетчером» Termidesk VDI корневой сертификат ЦС, использующийся в syslog-сервере, согласно подразделу **Установка корневого сертификата центра сертификации** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса». Значение по умолчанию: «UDP»
«Категория сообщения»	Выбор категории сообщений, которые будут записываться в журнал мониторинга
«Уровень логирования»	Выбор уровня логирования событий («INFO», «WARNING», «ERROR», «CRITICAL», «DEBUG»)
«Тег ретранслятора»	Тег записи, обрабатываемый «Ретранслятором». Должен соответствовать параметру `Match`, указанному в конфигурационном файле «Ретранслятора»
«Суффикс тега ретранслятора»	Суффикс тега записи, обрабатываемый «Ретранслятором». Должен соответствовать параметру `Match`, указанному в конфигурационном файле «Ретранслятора»

Настройка уровня журналирования «Агрегатора»

Уровень журналирования задается параметром `LOG_LEVEL` в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf`.

Для изменения уровня журналирования нужно:

- изменить параметр `LOG_LEVEL`;
- перезапустить службы:

```
sudo systemctl restart termidesk-vdi.service termidesk-celery-beat.service
termidesk-celery-worker.service
```

Журналы «Агрегатора»

Журналы «Агрегатора» хранятся в каталоге `/var/log/termidesk`.

Администратор может изменить каталог хранения через утилиту `termidesk-config` (см. подраздел **Утилита `termidesk-config`**).

Настройки ротации журналов определены в конфигурационном файле `/etc/logrotate.d/termidesk.conf` и формируются по шаблонам, указанным в каталоге `/etc/opt/termidesk-vdi/templates`. Каталог хранения шаблонов может быть изменен через утилиту `termidesk-config`.

Установлены следующие журналы «Агрегатора», разделенные по типам записываемых в них событий:

- broker.log - записываются события «Брокера сообщений TermideskMQ». Поддерживается автоматическая ротация журнала для исключения возможности переполнения пространства диска;
- celery-beat.log - записываются события периодической проверки состояния обработчика заданий через брокера сообщений. Поддерживается автоматическая ротация журнала для исключения возможности переполнения пространства диска;
- celery-worker.log - записываются события обработчика заданий через брокера сообщений. Поддерживается автоматическая ротация журнала для исключения возможности переполнения пространства диска;
- other.log - записываются события, не попавшие в другие журналы;
- termidesk.log - записываются события работы «Агрегатора»;
- workers.log - записываются события обработчика фоновых задач;
- gunicorn-access.log - записываются события доступов к внутреннему серверу Gunicorn;
- gunicorn-error.log - записываются события функционирования внутреннего сервера Gunicorn.

Устаревшие журналы (aggregator.log, auth.log) допускается удалить вручную.

Просмотр журналов в «Агрегаторе»

Просмотр системного журнала

Для просмотра общего журнала событий, связанного с функционированием «Агрегатора» и действиями субъектов доступа, следует перейти «Журналы - Системные журналы» (см. рисунок Отображение общего журнала событий).

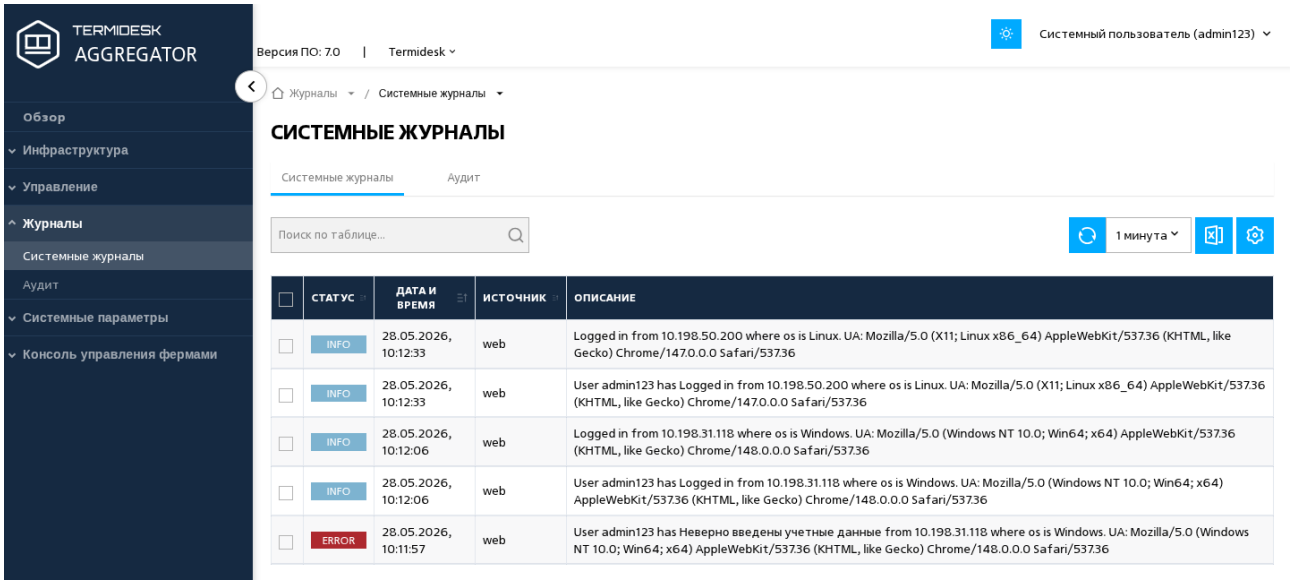


Рисунок 140. Отображение общего журнала событий

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- поиск записей по таблице;
- изменение внешнего вида таблицы;
- экспорт записей таблицы в `csv`-файл. Можно выгрузить:
  - все записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Всё]**;
  - выбранные записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Выбранные]**.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Просмотр журнала аудита

Для просмотра журнала событий, связанного с действиями субъектов доступа, следует перейти «Журналы - Аудит» (см. рисунок Отображение журнала аудита).

Если события аудита не отображаются, то необходимо убедиться, что на странице «Системные параметры - Системные настройки» во вкладке «Аудит» активирован параметр «Сохранение в БД».

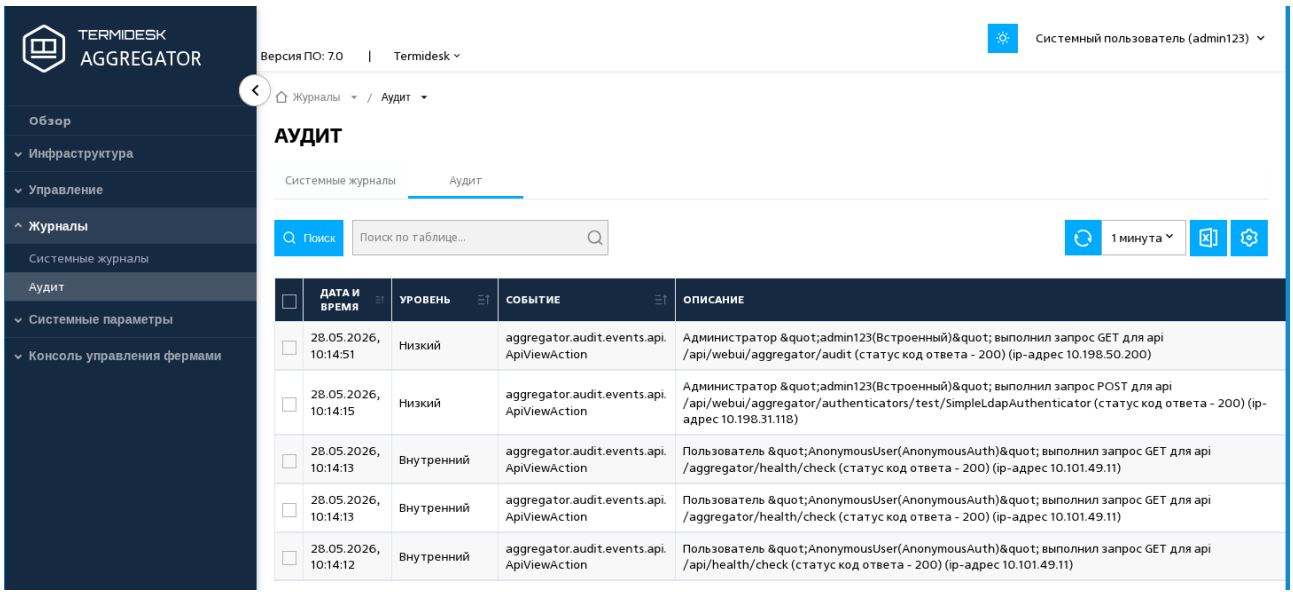


Рисунок 141. Отображение журнала аудита

Доступна возможность множественного выбора записей таблицы, для этого:

- либо отметить нужные строки через графический элемент множественного выбора;
- либо зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам.

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- поиск записей по таблице;
- изменение внешнего вида таблицы;
- экспорт записей таблицы в `csv`-файл. Можно выгрузить:
  - все записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Всё]**;
  - выбранные записи таблицы, для этого нажать графический элемент , затем нажать экранную кнопку **[Выбранные]**.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца;
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом

для соответствующего столбца.

ТЕРМИНЫ

Агрегатор администратора

Веб-интерфейс управления «Агрегатором». Устанавливается из пакета `termidesk-vdi` при выборе пункта «Агрегатор администратора»

Агрегатор пользователя

Веб-интерфейс пользователя для получения ресурсов, предоставляемых «Агрегатором». Устанавливается из пакета `termidesk-vdi` при выборе пункта «Агрегатор пользователя»

Домен аутентификации

Способ проверки субъектов и их полномочий

Компонент «Универсальный диспетчер»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им РМ и контроля доставки РМ. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-vdi.service`

Компонент «Шлюз»

Самостоятельный компонент, отвечающий за туннелирование протоколов доставки, использующих транспортный протокол TCP

Портал администратора

Предоставляет веб-интерфейс для управления фермой Termidesk VDI и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API

Портал пользователя

Предоставляет пользовательский веб-интерфейс фермы Termidesk VDI (без доступа к функциям управления) и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API

Рабочее место

Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа. Под РМ подразумеваются как виртуальные РМ, так и терминальные рабочие столы или приложения

Сайт

Физическая площадка, на которой может быть развернута одна или несколько ферм

Узел

Аппаратный или виртуальный сервер компонента «Универсальный диспетчер»

Ферма поставщиков ресурсов

Также: ферма Termidesk VDI. Ферма, объединяющая установку основных узлов Termidesk VDI, взаимодействующих с поставщиками ресурсов

СОКРАЩЕНИЯ

БД	База данных
ВМ	Виртуальная машина

ВРМ	Виртуальное рабочее место
КД	Контроллер домена
ИД	Идентификатор
ОС	Операционная система
ПО	Программное обеспечение
РМ	Рабочее место
СУБД	Система управления базами данных
ЦС	Центр сертификации
AES	Advanced Encryption Standard (стандарт симметричного шифрования данных)
API	Application Programming Interface (интерфейс прикладного программирования)
CEF	Common Event Format (открытый текстовый формат для стандартизации сообщений о событиях безопасности)
CRUD	Create Read Update Delete (акроним основных операций с информацией в БД)
DHCP	Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста)
DN	Domain Name (доменное имя)
DNS	Domain Name System (система доменных имен)
FQDN	Fully Qualified Domain Name (полностью определенное имя домена)
GID	Group Identification Data (идентификатор группы)
GSLB	Global Server Load Balancing (технология распределения сетевого трафика между серверами, находящимися в разных географических точках)
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста)
HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
ID	Identification Data (идентификатор)
IdP	Identity Provider (сервис, управляющий идентификационной информацией)
IP	Internet Protocol (межсетевой протокол)
JSON	JavaScript Object Notation (стандартный текстовый формат для структурированных данных)
JWT	JSON Web Token (открытый стандарт для создания токенов доступа)
LDAP	Lightweight Directory Access Protocol (легковесный протокол доступа к службам каталогов)

LDAPS	Lightweight Directory Access Protocol over SSL/TSL (расширение протокола LDAP)
MAC	Media Access Control (уникальный идентификатор сетевого устройства)
MS AD	Microsoft Active Directory Domain Service (службы каталогов Microsoft)
mTLS	Multiplexed Transport Layer Security (протокол, основанный на TLS с усиленной безопасностью)
NTP	Network Time Protocol (протокол сетевого времени)
OIDC	OpenID Connect (протокол аутентификации, построенный поверх стандарта OAuth 2.0.)
OU	Organizational Unit (организационная единица)
PKINIT	Public Key Cryptography for Initial Authentication (механизм Kerberos, позволяющий использовать сертификаты X.509)
RSA	Rivest, Shamir and Adleman (криптографический алгоритм с открытым ключом)
REST	Representational State Transfer (программная архитектура, определяющая условия работы API)
RFC	Request for Comments (рабочее предложение Интернет)
SSL	Secure Sockets Layer (криптографический протокол)
TCP	Transmission Control Protocol (протокол управления передачей)
TLS	Transport Layer Security (протокол защиты транспортного уровня)
UDP	User Datagram Protocol (протокол пользовательских датаграмм)
URI	Uniform Resource Identifier (унифицированный идентификатор ресурса)
URL	Uniform Resource Locator (унифицированный указатель ресурса)
W3C	World Wide Web Consortium (Консорциум Всемирной паутины)
WS	WebSocket (двунаправленный протокол, позволяющий клиенту установитьсвязь с сервером)
WSS	WebSocketSecure (двунаправленный протокол, позволяющий клиенту установить защищенную связь с сервером)
X.509	Стандарт для инфраструктуры открытого ключа

СЛЕТ.10001-01 90 09. РУКОВОДСТВО АДМИНИСТРАТОРА. НАСТРОЙКА КОМПОНЕНТА TERA

ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ

Назначение документа

Настоящий документ является девятой частью руководства администратора на программный комплекс «Диспетчер подключений виртуальных рабочих мест Termidesk» (далее - Termidesk VDI, Termidesk VDI). Документ определяет назначение, установку и настройку компонента TERA и предназначен для администраторов системы и сети.

Типографские соглашения

Приняты следующие типографские соглашения:

- `моноширинный шрифт` – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk VDI, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

TERA. ОБЩИЕ СВЕДЕНИЯ

Назначение TERA

Протокол удаленного доступа TERA (англ. Termidesk Remote Access protocol) входит в состав Termidesk VDI.

TERA обеспечивает:

- прямое подключение к гостевой операционной системе (ОС) рабочего места (РМ) независимо от используемой платформы виртуализации;
- безопасную аутентификацию пользователя по логину и паролю, передаваемого в преобразованном виде. Для безопасной аутентификации по умолчанию после установки используются самоподписанные сертификаты.

TERA устанавливается в ОС базового РМ. РМ при этом может быть реализовано:

- виртуальной машиной (ВМ);
- физической машиной. В этом случае к РМ может подключиться только пользователь, имеющий локальную учетную запись в ОС физической машины.

Требования к программному и аппаратному обеспечению

Для установки TERA минимальные аппаратные требования узла должны соответствовать следующим:

- процессор архитектуры Intel x86 разрядности 64 бит;
- оперативная память, не менее 1 ГБ;
- свободное дисковое пространство, не менее 200 МБ;
- сетевое соединение, не менее 100 Мбит/с.

Поддерживаемые ОС для установки TERA:

- (для вариантов ВМ и физической машины) Astra Linux Special Edition 1.7 (1.7.5, 1.7.6, 1.7.7, 1.7.8, 1.7.9). TERA использует разные драйверы для этих ОС, поэтому при обновлении ОС на другую версию нужно переустановить TERA;
- (для вариантов ВМ и физической машины) Astra Linux Special Edition 1.8 (1.8.1, 1.8.2, 1.8.3, 1.8.4, 1.8.5, 1.8.6);
- (для варианта ВМ) Microsoft Windows 10 1809 LTS. Редакции Professional (Профессиональная), Enterprise (Корпоративная);
- (для варианта ВМ) Microsoft Windows 10 2021 LTS. Редакции Professional (Профессиональная), Enterprise (Корпоративная);
- (для варианта ВМ) Microsoft Windows 11 LTSC 2024. Редакции Professional (Профессиональная), Enterprise (Корпоративная).

ОС Microsoft Windows редакций Home и Educational не поддерживается. При попытке установки будет выведено окно с ошибкой.

Работа TERA в ОС Astra Linux Special Edition гарантирована при установке в ОС уровня защищенности «Орел», «Воронеж» или «Смоленск».

Для подключения пользователя по TERA к РМ на пользовательской рабочей станции должен быть установлен компонент «Клиент» совместно с программным обеспечением (ПО) Termidesk Viewer.

Требования к пропускной способности канала

Фиксированных требований к пропускной способности канала при использовании TERA нет, поскольку объем данных напрямую зависит от сценария использования и активности пользователя в рамках удаленного сеанса.

Например, при работе с офисными приложениями или статичным графическим интерфейсом пользователь может потреблять минимальный трафик, однако при переключении на задачи с высокой динамикой изменений экрана потребление пропускной способности может возрастать кратно. Для разных типов рабочих нагрузок и разрешений дисплея требуются различные параметры сети, с оценкой которых можно ознакомиться в подразделе методических материалов сайта документации Termidesk VDI: **Полоса пропускания протоколов RDP, SPICE и TERA для разных нагрузок**.

Требования к настройке IPv6

При использовании IPv6-адресов в настройках протокола TERA (как для TCP, так и для UDP) необходимо указывать `scope_id` - идентификатор сетевого интерфейса (например, `%eth0` или `%wlan0`). Без корректного `scope_id` ОС не может определить, через какой интерфейс направлять соединение, что приведет к ошибке `Invalid argument` (код `22`).

Для получения `scope_id` нужно:

- получить список сетевых интерфейсов:

```
ip a
```

- определить полный адрес с помощью команды `ping` для каждого интересующего IPv6-адреса (в ответе ОС автоматически подставит `scope_id`), например:

```
ping fe80::9afc:84ff:fee0:dab4
```

Пример ответа:

```
PING fe80::9afc:84ff:fee0:dab4(fe80::9afc:84ff:fee0:dab4%eth0) ...
```

Правильная настройка для указанного примера будет: `fe80::9afc:84ff:fee0:dab4%eth0`.

Таким образом в настройках TERA при использовании IPv6 требуется указывать адрес вместе со `scope_id` в тех случаях, когда указывается конкретный адрес, а не общий (`0.0.0.0` или `0:0:0:0:0:0:0:0`).

TERA. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ

Получение пакетов установки в ОС Astra Linux Special Edition

Дистрибутив представлен бинарным файлом пакета ПО в `deb`-формате. Установка в ОС Astra Linux Special Edition производится из локального репозитория, распространяемого в формате `iso`-образа.

Получить `iso`-образ можно двумя способами:

- заполнив запрос через сайт Termidesk VDI: https://termidesk.ru/support/#request-support;
- через личный кабинет:https://lk.astra.ru/.

Для подключения локального репозитория Termidesk VDI на узле, где предполагается установка, нужно:

- скопировать в домашний каталог пользователя образ диска `termidesk-<версия>.iso`;
- подключить образ диска к файловой системе в каталог `/mnt`:

```
sudo mount -o loop termidesk-<версия>.iso /mnt
```

где:

`-o loop` - параметры для привязки петлевого устройства (`/dev/loop`) к файлу `termidesk-<версия>.iso`, устройство затем монтируется в указанный каталог `/mnt`;

- скопировать содержимое каталога `repos` подключенного образа диска в каталог `/var` локальной файловой системы:

```
sudo cp -Rp /mnt/repos /var
```

где:

`-Rp` - ключ для рекурсивного копирования подкаталогов и файлов с сохранением исходных свойств;

- отключить подключенный ранее образ диска от узла:

```
sudo umount /mnt
```

- установить пакет `lsb-release`:

```
sudo apt install -y lsb-release
```

- добавить локальный репозиторий Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list` через командный интерпретатор `sh`:
  - выяснить установленную версию ОС:

    ```
    sudo cat /etc/astra_version
    ```

  - определить актуальное имя каталога с пакетами в `/var/repos`;
  - указать в файле конфигурации APT корректное (фактическое) имя каталога:

    ```
    sudo sh -c 'echo "deb file:/var/repos/astra 1.8_x86-64 non-free" >
    /etc/apt/sources.list.d/termidesk_local.list'
    ```

    где:

    `-c` - ключ для чтения команд из вводимой строки (стандартный ввод);

    `echo` - команда вывода текста, совместно с символом «>» используется для перенаправления строки в файл;

    `deb file:/var/repos/astra 1.8_x86-64 non-free` - добавляемый репозиторий с вложенной командой получения версии ОС;

    Приведенный пример команды актуален для установки основных компонентов Termidesk, пакеты которых расположены в каталоге `1.8_x86-64`.

- для корректной установки компонентов TERA потребуется корректно подключить дополнительные репозитории и настроить их приоритет:
  - для версий ОС Astra Linux Special Edition меньше или равных 1.7.6, а также для версий 1.8.X:
    - подключить два репозитория:

```
sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
non-free" > /etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
/dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

- добавить повышенный приоритет для репозитория с требуемой версией ОС (значение `$(cat /etc/astra_version)` может подходить не для всех репозиториев, т.к. версия может указываться без точек - в этом случае нужно вручную указать корректную версию):

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000
EOF"
```

- для версий ОС Astra Linux Special Edition 1.7.7 и 1.7.8:
  - подключить три репозитория:

```
sudo sh -c 'echo "deb file:/var/repos/astra 1.7.6 non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
/dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

  - настроить два приоритета:

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=1.7.6
Pin-Priority: 950

Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000

EOF"
```

- выполнить поиск ключа репозитория Termidesk VDI `GPG-KEY-PUBLIC` и добавить его:

```
sudo cat /var/repos/astra/GPG-KEY-PUBLIC | sudo gpg --dearmour -o
/etc/apt/trusted.gpg.d/termidesk.gpg
```

- убедиться, что ключ `release@uveon.ru` был успешно добавлен:

```
apt-key list
```

В случае, если ключ не отображен в выводе команды, необходимо убедиться, что ключ `GPG-KEY-PUBLIC` существует:

```
cat /var/repos/astra/GPG-KEY-PUBLIC
```

Если ключ все же существует, следует проверить правильность выполнения шагов по добавлению репозитория Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list`.

При успешном выполнении всех шагов команда выведет содержимое ключа в формате Base64.

В зависимости от используемой версии ОС команды добавления ключа репозитория Termidesk VDI могут отличаться. Если для ОС Astra Linux Special Edition 1.8 ключ репозитория был добавлен командой, применимой к другой версии ОС, то для исправления нужно:

- узнать идентификатор добавленного ключа репозитория:

```
apt-key list
```

- удалить ключ:

```
apt-key --keyring /etc/apt/trusted.gpg del 4E1632CC
```

где `4E1632CC` - последние 8 символов идентификатора ключа;

- вновь добавить ключ репозитория.

- обновить данные пакетного менеджера:

```
sudo apt update
```

- проверить настройку приоритетов репозиториев:

```
apt-cache policy
```

Команду `sudo apt update` необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.

Получение пакетов установки через Интернет-репозиторий

Для получения пакетов установки может использоваться Интернет-репозиторий:

https://repos.termidesk.ru/.

Для подключения репозитория в ОС Astra Linux Special Edition нужно:

- установить пакеты:

```
sudo apt install -y lsb-release wget apt-transport-https debian-keyring
```

где:

-y - ключ для пропуска подтверждения установки;

- добавить Интернет-репозиторий Termidesk VDI в файл /etc/apt/sources.list.d/termidesk_local.list через командный интерпретатор sh:
  - выяснить установленную версию ОС:

    ```
    sudo cat /etc/astra_version
    ```

  - определить актуальное имя каталога с пакетами в https://repos.termidesk.ru/astra;
  - указать в файле конфигурации APT корректное (фактическое) имя каталога:

    ```
    sudo sh -c 'echo "deb https://repos.termidesk.ru/astra 1.8_x86-64 non-free" >
    /etc/apt/sources.list.d/termidesk_local.list'
    ```

    где:

    -c - ключ для чтения команд из вводимой строки (стандартный ввод);

    echo - команда вывода текста, совместно с символом «>» используется для перенаправления строки в файл;

    deb https://repos.termidesk.ru/astra <…> - добавляемый репозиторий;

    Приведенный пример команды актуален для установки основных компонентов Termidesk, пакеты которых расположены в каталоге 1.8_x86-64.

- для корректной установки компонентов TERA потребуется корректно подключить дополнительные репозитории и настроить их приоритет:
  - для версий ОС Astra Linux Special Edition меньше или равных 1.7.6, а также для версий 1.8.X:
    - подключить два репозитория:

      ```
      sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(cat
      /etc/astra_version) non-free" >
      /etc/apt/sources.list.d/termidesk_local.list'
      sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(lsb_release -cs
      2> /dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
      ```

- добавить повышенный приоритет для репозитория с требуемой версией ОС (значение `$(cat /etc/astra_version)` может подходить не для всех репозиториев, т.к. версия может указываться без точек - в этом случае нужно вручную указать корректную версию):

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000
EOF"
```

- для версий ОС Astra Linux Special Edition 1.7.7 и 1.7.8:
  - подключить три репозитория:

```
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra 1.7.6 non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(cat
/etc/astra_version) non-free" >>
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(lsb_release -cs
2> /dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

  - настроить два приоритета:

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=1.7.6
Pin-Priority: 950

Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000

EOF"
```

- получить ключ репозитория Termidesk VDI `GPG-KEY-PUBLIC` и добавить его в ОС:
  - для ОС Astra Linux Special Edition 1.7:

```
wget --no-check-certificate -qO - https://repos.termidesk.ru/astra/GPG-KEY-
PUBLIC | sudo apt-key add -
```

  - для ОС Astra Linux Special Edition 1.8:

```
wget --no-check-certificate -qO - https://repos.termidesk.ru/astra/GPG-KEY-
```

```
PUBLIC |  sudo gpg --dearmour -o /etc/apt/trusted.gpg.d/termidesk.gpg
```

- обновить данные пакетного менеджера:

```
sudo apt update
```

- проверить настройку приоритетов репозиториев:

```
apt-cache policy
```

Команду `sudo apt update` необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.

Команды добавления ключа репозитория Termidesk VDI отличаются в зависимости от используемой версии ОС.

Если для ОС Astra Linux Special Edition 1.8 ключ репозитория был добавлен командой, применимой к другой версии ОС, то для исправления нужно:

- узнать идентификатор добавленного ключа репозитория:

```
apt-key list
```

- удалить ключ:

```
apt-key --keyring /etc/apt/trusted.gpg del 4E1632CC
```

где `4E1632CC` - последние 8 символов идентификатора ключа;

- вновь добавить ключ репозитория.

TERA. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ

ОС Astra Linux Special Edition

Установка в ОС Astra Linux Special Edition для ВМ

После установки TERA графический интерфейс гостевой ОС ВМ будет недоступен при подключении к ней напрямую через платформу виртуализации. Управление будет доступно только по протоколу SSH.

Нужно проверить доступность SSH сервера заблаговременно (сервис должен быть в состояниях `enabled` и `active`):

```
systemctl status ssh.service
```

Для установки TERA в среде ВМ с ОС Astra Linux Special Edition нужно:

- предварительно установить компоненты «Агент виртуального рабочего места», «Видеоагент», «Агент виртуальных смарт-карт»;
- удалить пакеты `spice-vdagent` и `xserver-xorg-video-qxl`, если они были установлены:

```
sudo apt purge spice-vdagent xserver-xorg-video-qxl
```

- установить программу для обмена информацией между ВМ и хост-системой (для KVM-виртуализации это пакет `qemu-guest-agent`, для VMware это пакет `open-vm-tools`):

```
sudo apt install qemu-guest-agent
```

- убедиться, что имя хоста (`hostname`) и информация в `/etc/hosts` совместимы:
  - выполнить:

    ```
    ping $(hostname)
    ```

  - если в файле нет нужной записи, то добавить ее;
- установить пакет `termidesk-tera`:

```
sudo apt install termidesk-tera
```

- на запрос «Разрешить монтирование ресурсов WebDAV непривилегированным пользователем?» нажать экранную кнопку **[Да]**. При необходимости изменить решение после установки нужно выполнить команду:

```
sudo dpkg-reconfigure davfs2
```

- на запрос «Выберите режим управления экранами мониторов» выбрать пункт «default» и нажать экранную кнопку **[Ok]**. При необходимости изменить решение после установки нужно выполнить команду:

```
sudo dpkg-reconfigure tera-vdagent
```

При установке пакета `termidesk-tera` также будут установлены:

- `tera-audio` - пакет поддержки вывода звука через динамики. Вывод звука управляется службой `tera-audio`;
- `tera-folder-redirection` - пакет поддержки перенаправления каталога и его монтирования в гостевую ОС;
- `tera-record` - пакет поддержки захвата звука с микрофона. Захват звука управляется службой `tera-record`;
- `libtera-server` - библиотека, предоставляющая удаленный доступ к РМ и необходимая для корректной работы TERA;
- `tera-vdagent` - пакет, предоставляющий управление изменениями

графического окружения (например, динамического изменения разрешения экрана в зависимости от разрешения монитора пользователя);

- tera-qxl - драйвер виртуального графического устройства QXL.

Следующие пакеты являются рекомендованными к установке:

- tera-router - пакет, обеспечивающий проксирование подключений пользователей с одного общего порта на несколько внутренних и поддержку протокола UDP для TERA. Пакет требуется для обеспечения подключения по UDP через шлюз, во всех других случаях (без UDP через шлюз, прямое подключение без шлюза) проксирование подключений не требуется;
- termidesk-pcsc-vscard - компонент «Агент виртуальных смарт-карт»;
- tera-usb - пакет, обеспечивающий перенаправление USB-устройств.

- для возможности поддержки перенаправления USB-устройств с пользовательской рабочей станции:

Если репозиторий Termidesk в ОС настроен корректно (см. подраздел **TERA. Получение пакетов установки**), то ручная установка пакетов не потребуется. Команды приведены для случая, если не удалось корректно перечислить репозитории получения пакетов.

- узнать версию ОС:

```
cat /etc/astra_version
```

- узнать версию ядра ОС:

```
uname -r
```

- установить пакеты: tera-usb_<номер_версии_пакета> и пакет с модулем ядра tera-usb-<версия_ядра>_<номер_версии_пакета> для нужной версии ядра ОС (пакеты размещены в специальном каталоге для каждой версии ОС - /repos/astra/dists/ (в Интернет-репозитории - https://repos.termidesk.ru/astra/dists/)):

```
sudo apt install tera-usb_<номер_версии_пакета>
sudo apt install tera-usb-<версия_ядра>_<номер_версии_пакета>
```

- настроить параметр TeraUsbChannelNum в конфигурационном файле /etc/X11/xorg.conf.d/30-teraqxl.xorg.conf;

- настроить параметры TeraPort и TeraTlsPort в конфигурационном файле /etc/X11/xorg.conf.d/30-teraqxl.xorg.conf;
- убедиться, что пользователь fly-dm добавлен в группу sasl. Если пользователя в группе нет, то добавить его:

```
sudo usermod -a -G sasl fly-dm
```

- добавить в автоматическую загрузку и запустить службу `tera-router`, если установлен пакет `tera-router`:

> До активации службы `tera-router` нужно выполнить ее настройку (см. подраздел **Параметры запуска службы** `tera-router`).
>
> Пакет `tera-router` требуется для обеспечения подключения по UDP через шлюз, во всех других случаях (без UDP через шлюз, прямое подключение без шлюза) проксирование подключений не требуется.
>
> ```
> sudo systemctl enable tera-router
> sudo systemctl start tera-router
> ```

- убедиться, что после установки запущены обязательные службы `tera-vdagentd`,`tera-mounting-shdir-service`:

> Начиная с Termidesk версии 7.0 служба `tera-mounting-shdir-service` входит в состав компонента «Агент виртуального рабочего места».

```
systemctl status tera-vdagentd
systemctl status tera-mounting-shdir-service
```

- если служба не активирована, то активировать ее:

```
sudo systemctl enable tera-vdagentd
sudo systemctl enable tera-mounting-shdir-service
```

- выполнить настройку компонента «Агент виртуальных смарт-карт» для работы функционала перенаправления смарт-карт;
- рекомендуется выполнить перезагрузку ОС, поскольку некоторые компоненты загружают модуль ядра.

> На этапе установки будут сгенерированы файлы сертификатов и ключей, которые затем будут расположены в директории `/etc/termidesk/tera/sasl/`.

После перезагрузки ОС:

- убедиться, что запущены службы `tera-router` и `tera-usb-service`, если пакеты `tera-router` и `tera-usb` были установлены:

```
systemctl status tera-router
systemctl status tera-usb-service
```

- если служба не активирована, то активировать ее:

```
sudo systemctl enable tera-router
```

```
sudo systemctl enable tera-usb-service
```

Установка в ОС Astra Linux Special Edition для физической машины

Для установки TERA в среде физической машины с ОС Astra Linux Special Edition нужно:

- предварительно установить компоненты «Агент виртуального рабочего места», «Видеоагент», «Агент виртуальных смарт-карт»;
- удалить пакеты `spice-vdagent` и `xserver-xspice`, если они были установлены:

```
sudo apt purge spice-vdagent
sudo apt remove xserver-xspice
```

- убедиться, что имя хоста (`hostname`) и информация в `/etc/hosts` совместимы:
  - выполнить:

    ```
    ping $(hostname)
    ```

  - если в файле нет нужной записи, то добавить ее;
- установить пакет `termidesk-tera-x11`:

```
sudo apt install termidesk-tera-x11
```

- на запрос «Разрешить монтирование ресурсов WebDAV непривилегированным пользователем?» нажать экранную кнопку **[Да]**. При необходимости изменить решение после установки нужно выполнить команду:

```
sudo dpkg-reconfigure davfs2
```

- на запрос «Выберите режим управления экранами мониторов» выбрать пункт «near» и нажать экранную кнопку **[Ok]**. При необходимости изменить решение после установки нужно выполнить команду:

```
sudo dpkg-reconfigure tera-vdagent
```

При установке пакета `termidesk-tera-x11` также будут установлены:

- `tera-audio` - пакет поддержки вывода звука через динамики. Вывод звука управляется службой `tera-audio`;
- `tera-folder-redirection` - пакет поддержки перенаправления каталога и его монтирования в гостевую ОС;
- `tera-record` - пакет поддержки захвата звука с микрофона. Захват звука управляется службой `tera-record`;
- `libtera-server` - библиотека, предоставляющая удаленный доступ к РМ и необходимая для корректной работы TERA;

- tera-vdagent - пакет, предоставляющий управление изменениями графического окружения (например, динамического изменения разрешения экрана в зависимости от разрешения монитора пользователя);
- tera-x11 - пакет управления удаленным доступом к физической машине, реализующийся ПО x11tera. ПО x11tera может работать в режиме службы и в режиме приложения.

Следующие пакеты являются рекомендованными к установке:

- termidesk-pcsc-vscard - компонент «Агент виртуальных смарт-карт»;
- tera-usb - пакет, обеспечивающий перенаправление USB-устройств.

- для возможности поддержки перенаправления USB-устройств с пользовательской рабочей станции:
  - узнать версию ОС:

```
cat /etc/astra_version
```

  - узнать версию ядра ОС:

```
uname -r
```

  - установить пакеты: tera-usb_<номер_версии_пакета> и пакет с модулем ядра tera-usb-<версия_ядра>_<номер_версии_пакета> для нужной версии ядра ОС (пакеты размещены в специальном каталоге для каждой версии ОС - /repos/astra/dists/ (в Интернет-репозитории - https://repos.termidesk.ru/astra/dists/)):

```
sudo apt install tera-usb_<номер_версии_пакета>
sudo apt install tera-usb-<версия_ядра>_<номер_версии_пакета>
```

  - настроить параметр usb-channel-num в конфигурационном файле /etc/xdg/x11tera/x11tera.conf;
- убедиться, что пользователь fly-dm добавлен в группу sasl. Если пользователя в группе нет, то добавить его:

```
sudo usermod -a -G sasl fly-dm
```

- для возможности работы TERA по протоколу UDP:
  - установить пакет tera-router:

Пакет требуется для обеспечения подключения по UDP через шлюз, во всех других случаях (без UDP через шлюз, прямое подключение без шлюза) проксирование подключений не требуется

```
sudo apt install tera-router
```

- выполнить настройку службы `tera-router` для работы по протоколу UDP (см. подраздел **Параметры запуска службы `tera-router`**);
- добавить в автоматическую загрузку и запустить службу `tera-router`:

```
sudo systemctl enable tera-router
sudo systemctl start tera-router
```

- активировать и запустить службы `x11tera_unlock.service` и `x11tera_controls.service`:

```
sudo systemctl enable x11tera_unlock.service
sudo systemctl start x11tera_unlock.service
sudo systemctl enable x11tera_controls.service
sudo systemctl start x11tera_controls.service
```

- после установки убедиться, что запущены службы `tera-vdagentd`, `tera-mounting-shdir-service`, `x11tera`, `x11tera_unlock`, `x11tera_controls`:

Начиная с Termidesk версии 7.0 служба `tera-mounting-shdir-service` входит в состав компонента «Агент виртуального рабочего места».

```
sudo systemctl status tera-vdagentd
sudo systemctl status tera-mounting-shdir-service
sudo systemctl status x11tera
sudo systemctl status x11tera_unlock
sudo systemctl status x11tera_controls
```

- если служба не активирована, то активировать ее:

```
sudo systemctl enable tera-vdagentd
sudo systemctl enable tera-mounting-shdir-service
sudo systemctl enable x11tera
sudo systemctl enable x11tera_unlock
sudo systemctl enable x11tera_controls
```

- выполнить настройку компонента «Агент виртуальных смарт-карт» для работы функционала перенаправления смарт-карт;
- отключить автоматический запуск `kscreend`:
  - в файл `/etc/xdg/autostart/kscreen.desktop` добавить строку `Hidden=true`;
  - предварительно сохранить файлы и данные в графической среде, затем перезапустить службу `display-manager`:

```
sudo systemctl restart display-manager
```

- завершить установку TERA, выбрав режим запуска ПО x11tera и выполнив

соответствующие команды (см. подраздел **Режимы запуска ПО x11tera**);

- рекомендуется выполнить перезагрузку ОС, поскольку некоторые компоненты загружают модуль ядра ОС.

После перезагрузки ОС:

- убедиться, что запущены службы `tera-router`, `tera-usb-service`, если пакеты `tera-router` и `tera-usb` соответственно были установлены:

```
systemctl status tera-router
systemctl status tera-usb-service
```

- если служба не активирована, то активировать ее:

```
sudo systemctl enable tera-router
sudo systemctl enable tera-usb-service
```

Если физическая машина является постоянным РМ пользователя и новые мониторы не добавляются и не отключаются от физической машины, то после установки рекомендуется создать постоянную конфигурацию мониторов и сохранить ее в конфигурационных файлах `/etc/termidesk/tera/x11tera_user_lock.conf`, `/etc/termidesk/tera/x11tera_greeter_lock.conf` (конфигурация мониторов при подключении пользователя и на экране greeter) и `/etc/termidesk/tera/x11tera_user_unlock.conf`, `/etc/termidesk/tera/x11tera_greeter_unlock.conf` (конфигурация мониторов при отключении пользователя и выходе из экрана greeter). Для этого:

Если физическая машина представляет собой ноутбук, подключающийся к различным мониторам, док-станциям и не имеющий постоянной конфигурации рабочего стола и дисплеев, то команду выполнять не рекомендуется.

- убедиться, что пользователь выполнил вход в графическое окружение ОС физической машины;
- выполнить сохранение конфигурации мониторов:

```
sudo x11tera_on_lock save-config
```

Сценарии, при которых использование `save-config` не требуется (но требуется во всех остальных случаях):

- если у пользователя один монитор;
- если у пользователя не дублируются мониторы на графическом экране приветствия (greeter);
- если у пользователя одинаковые мониторы с одинаковым размером.

Создание и использование постоянной конфигурации мониторов рекомендуется выполнять для избежания ситуации с отображением черного экрана после перезапуска физической машины или службы `x11tera_unlock` в частности.

При выполнении команды выбирается основной пользовательский

монитор и его режимы разрешений, которые будут транслироваться в ПО Termidesk Viewer.

Сохраненная конфигурация используется для восстановления расположения мониторов при:

- отключении пользователя (и ПО Termidesk Viewer);
- неожиданной перезагрузке физической машины;
- перезапуске и останове службы `x11tera_unlock`.

Для очистки конфигурации мониторов используется команда:

```
sudo x11tera_on_lock clear-config
```

Для проверки работоспособности после установки следует проверить готовность ПО x11tera к подключениям:

- выполнить:

```
sudo ss -tlpn | grep ":590. "
```

- убедиться, что в выводе содержится порт подключения 5900 (или 5901, в зависимости от настроек):

```
# tcp   LISTEN 0      4096               *:5900             *:*
users:(("systemd",pid=1,fd=111))
```

Если установка выполняется в ОС Astra Linux Special Edition 1.7, то нужно убедиться, что служба `x11tera` и графический менеджер работают с одинаковыми правами пользователя. Для этого перезагрузить физическую машину, затем:

- нажать сочетание клавиш **<Alt>** + **<Ctrl>** + **<F1-F6>**, переключившись в дополнительный виртуальный терминал. Либо подключиться к узлу по протоколу SSH;
- выполнить проверку прав графического менеджера и службы `x11tera`:

```
pgrep -x Xorg | xargs ps -f -o user -p
systemctl show x11tera.service | grep -E "^User=|^Group="
```

- если права не совпадают, то отредактировать файл `/lib/systemd/system/x11tera.service`, указав имя пользователя, с которым запустился и работает графический менеджер. Пример:

```
[Service]
User=root
Group=root
```

- применить изменения, перезагрузив физическую машину, либо выполнив команды:

```
sudo systemctl daemon-reload
sudo systemctl restart x11tera
```

После установки TERA в среде физической машины с ОС Astra Linux Special Edition:

- будет доступно удаленное подключение пользователя к этой физической машине;
- будет доступно локальное подключение пользователя к этой физической машине;
- пользователь обязательно должен локально авторизоваться со своей учетной записью в ОС физической машины при первом использовании.

При необходимости изменить параметры доступа пользователя следует обратиться к подразделу **Блокирование локального доступа при подключении к физической машине**. Изменение параметров должно производиться после того, как пользователь первый раз локально авторизовался в ОС физической машины.

Для решения нештатных ситуаций или донастройки ОС рекомендуется использовать удаленный доступ, например, по протоколу SSH. Нужно проверить доступность SSH сервера заблаговременно (сервис должен быть в состояниях `enabled` и `active`):

```
systemctl status ssh.service
```

Установка в режиме ЗПС

Замкнутая программная среда (ЗПС) является средством повышения безопасности ОС путем контроля целостности (неизменности) файлов.

Механизм контроля реализован в виде невыгружаемого модуля ядра ОС Astra Linux Special Edition (модуль `digsig_verif`), выполняющего проверку электронной цифровой подписи файлов (ЭЦП).

Перед установкой компонентов Termidesk VDI необходимо установить пакет `termidesk-digsig-keys`, для этого:

- подключить репозиторий Termidesk VDI или получить отдельный пакет `termidesk-digsig-keys` из репозитория;
- выполнить установку с использованием репозитория:

```
sudo apt -y install termidesk-digsig-keys
```

- либо выполнить установку из `deb`-пакета:

```
sudo apt install -y /home/user/termidesk-digsig-keys-XXXXXX_amd64.deb
```

где:

`-y` - ключ для пропуска подтверждения установки;

`/home/user/termidesk-digsig-keys-XXXXXX_amd64.deb` - расположение пакета `termidesk-digsig-keys-XXXXXX_amd64.deb`.

- перезагрузить ОС:

```
sudo reboot
```

- выполнить установку компонента Termidesk VDI.

Для ЗПС может быть активирован режим проверки встроенной ЭЦП в расширенных атрибутах (`DIGSIG_XATTR_MODE`). В этом случае потребуется подписать файлы, которые будут проходить проверку, имеющимися в организации ключами. Информация о процессе подписи и активации механизма проверки встроенной ЭЦП в расширенных атрибутах приведена в справочном центре Astra Linux: https://wiki.astralinux.ru/pages/viewpage.action?pageId=41190634.

Постановка на контроль целостности

После установки и настройки TERA необходимо поставить компонент на контроль целостности.

Для контроля целостности используются встроенные в ОС Astra Linux Special Edition программные средства на основе `Another File Integrity Checker`, представленного пакетом `afick`.

Настройка регламентного контроля целостности выполняется в конфигурационном файле `/etc/afick.conf`.

> Настройку следует производить только после окончательного внедрения компонента, поскольку с файлов конфигурации и исполняемых файлов будут сняты эталонные контрольные суммы.

Для постановки на контроль целостности TERA необходимо добавить в конфигурационный файл `/etc/afick.conf` следующие строки:

- для ВМ:

```
/usr/lib/x86_64-linux-gnu/libtera-server.so PARSEC
/usr/lib/x86_64-linux-gnu/libtera-server.so.6 PARSEC
/usr/lib/x86_64-linux-gnu/libtera-server.so.6.0.0 PARSEC

/usr/lib/xorg/modules/drivers/teraqxl_drv.so PARSEC

/usr/bin/tera-vdagent
/usr/bin/tera-vdagent.sh
/usr/sbin/tera-vdagentd
```

```
/usr/lib/systemd/user/tera-vdagent.service PARSEC

/lib/systemd/system/tera-mounting-shdir-service.service PARSEC
/usr/bin/tera-mounting-shdir-service PARSEC
/usr/lib/systemd/user/tera-webdav-service.service PARSEC
/usr/bin/tera-webdav PARSEC
/usr/bin/tera-webdav-service-start PARSEC

/usr/bin/tera-audio-service PARSEC
/usr/bin/tera-audio-start PARSEC
/usr/lib/systemd/user/tera-audio.service PARSEC

/usr/bin/tera-record-service PARSEC
/usr/bin/tera-record-start PARSEC
/usr/lib/systemd/user/tera-record.service PARSEC

#Репозиторий Termidesk
/var/repos/ PARSEC
```

- для физической машины:

```
/usr/lib/x86_64-linux-gnu/libtera-server.so PARSEC
/usr/lib/x86_64-linux-gnu/libtera-server.so.6 PARSEC
/usr/lib/x86_64-linux-gnu/libtera-server.so.6.0.0 PARSEC

/lib/systemd/system/x11tera.service PARSEC
/lib/systemd/system/x11tera_controls.service PARSEC
/lib/systemd/system/x11tera_unlock.service PARSEC
/usr/bin/x11tera
/usr/bin/x11tera.sh PARSEC
/usr/lib/xorg/modules/drivers/libteradummy_drv.so PARSEC

/usr/bin/tera-vdagent
/usr/bin/tera-vdagent.sh
/usr/sbin/tera-vdagentd
/usr/lib/systemd/user/tera-vdagent.service PARSEC

/lib/systemd/system/tera-mounting-shdir-service.service PARSEC
/usr/bin/tera-mounting-shdir-service PARSEC
/usr/lib/systemd/user/tera-webdav-service.service PARSEC
/usr/bin/tera-webdav PARSEC
/usr/bin/tera-webdav-service-start PARSEC

/usr/bin/tera-audio-service PARSEC
/usr/bin/tera-audio-start PARSEC
/usr/lib/systemd/user/tera-audio.service PARSEC

/usr/bin/tera-record-service PARSEC
```

```
/usr/bin/tera-record-start PARSEC
/usr/lib/systemd/user/tera-record.service PARSEC

#Репозиторий Termidesk
/var/repos/ PARSEC
```

Для снятия эталонных значений контрольных сумм используется команда:

```
afick -i
```

Для проверки соответствия контрольных сумм эталонным значениям автоматически создаются задания в системном планировщике заданий `cron`.

Для ручной проверки соответствия контрольных сумм используется команда:

```
afick -k
```

В случае отсутствия по какой-либо причине исполняемых фалов `*.pyc`, они будут повторно сгенерированы при перезапуске сервера Python. В этом случае нужно повторно проинициализировать средство регламентного контроля целостности `afick`.

Обновление в ОС Astra Linux Special Edition

Обновление производится установкой новой версии пакета `termidesk-tera` (для ВМ) или `termidesk-tera-x11` (для физической машины) поверх предыдущей.

Перед обновлением пакетов нужно убедиться, что подключен актуальный репозиторий.

Для обновления TERA в ОС Astra Linux Special Edition выполнить:

- для ВМ:

```
sudo apt reinstall termidesk-tera
```

- для физической машины:

```
sudo apt reinstall termidesk-tera-x11
```

Удаление в ОС Astra Linux Special Edition

Для удаления TERA из ОС Astra Linux Special Edition выполнить:

- для ВМ:

```
sudo apt purge --autoremove termidesk-tera
```

- для физической машины:

```
sudo apt purge --autoremove termidesk-tera-x11
```

ОС Microsoft Windows

Установка в ОС Microsoft Windows для ВМ

Для установки в ОС Microsoft Windows используется `msi`-пакет `termidesk-tera`.

Для установки TERA нужно:

- предварительно включить службы удаленных рабочих столов. Для этого:
  - в меню «Пуск» выбрать путь «Параметры - Система - Удаленный рабочий стол» и нажать экранную кнопку **[Включить удаленный рабочий стол]**;
  - убрать активацию параметра (снять галочку) «Разрешить подключения только с компьютеров, на которых работает удаленный рабочий стол с проверкой подлинности на уровне сети» (рекомендуется выполнить при подключении с пользовательской рабочей станции на основе ОС Linux);
- установить компонент «Агент виртуального рабочего места» и выбрать при установке пункты: «Temidesk PCSC Driver» и «Temidesk Video Agent»;
- запустить установочный файл TERA и нажать экранную кнопку **[Далее]**;
- ознакомиться с лицензионным соглашением. Для принятия условий лицензионного соглашения и продолжения установки следует отметить поле «Я принимаю условия лицензионного соглашения» и нажать экранную кнопку **[Далее]** (см. рисунок Лицензионное соглашение);

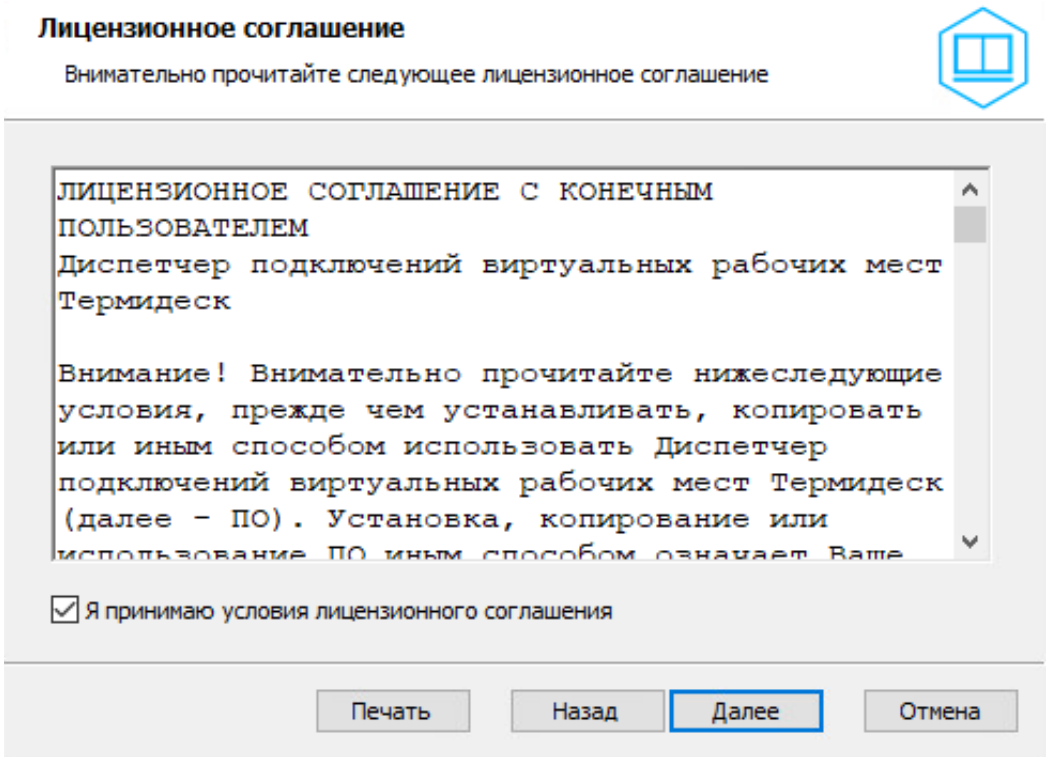


Рисунок 142. Лицензионное соглашение

- выбрать каталог установки или оставить значение по умолчанию (`C:\Program Files\UVEON\Termidesk TERA`) и нажать экранную кнопку **[Далее]** (см. рисунок Каталог установки TERA);

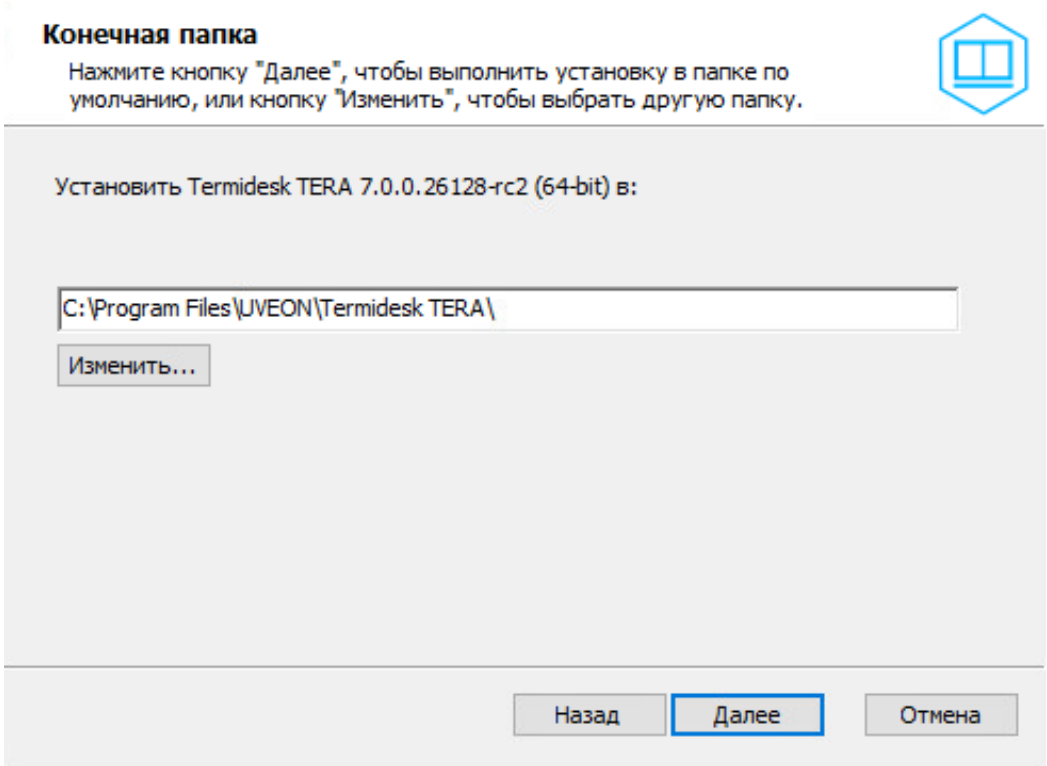


Рисунок 143. Каталог установки TERA

- подтвердить установку, нажав экранную кнопку **[Установить]** (см. рисунок Подтверждение установки);

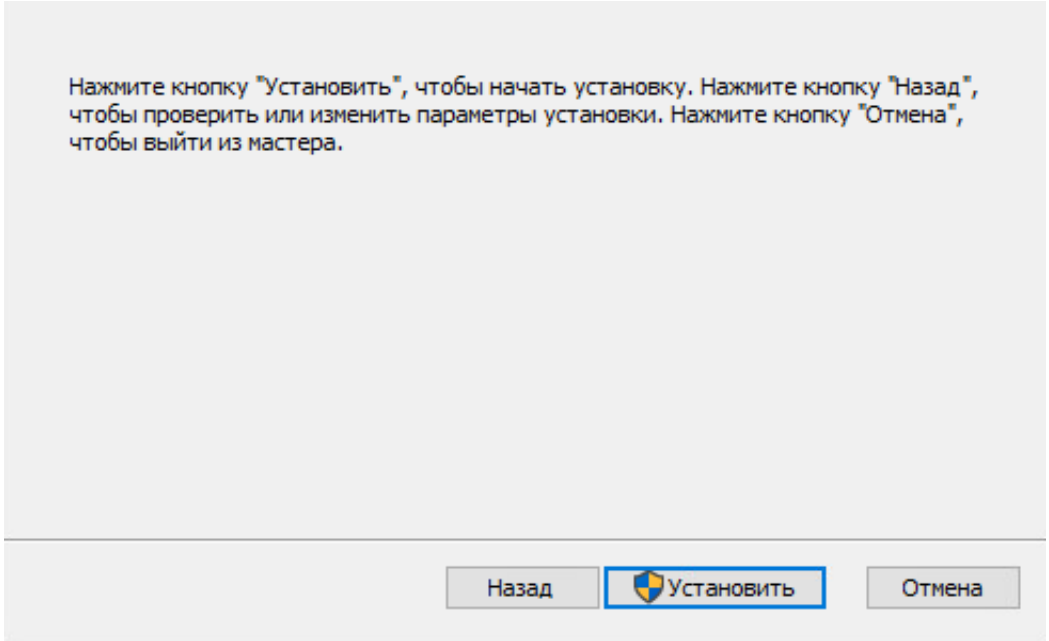


Рисунок 144. Подтверждение установки

- в окне запроса контроля учетных записей нажать экранную кнопку **[Да]** (см. рисунок Окно запроса разрешений);

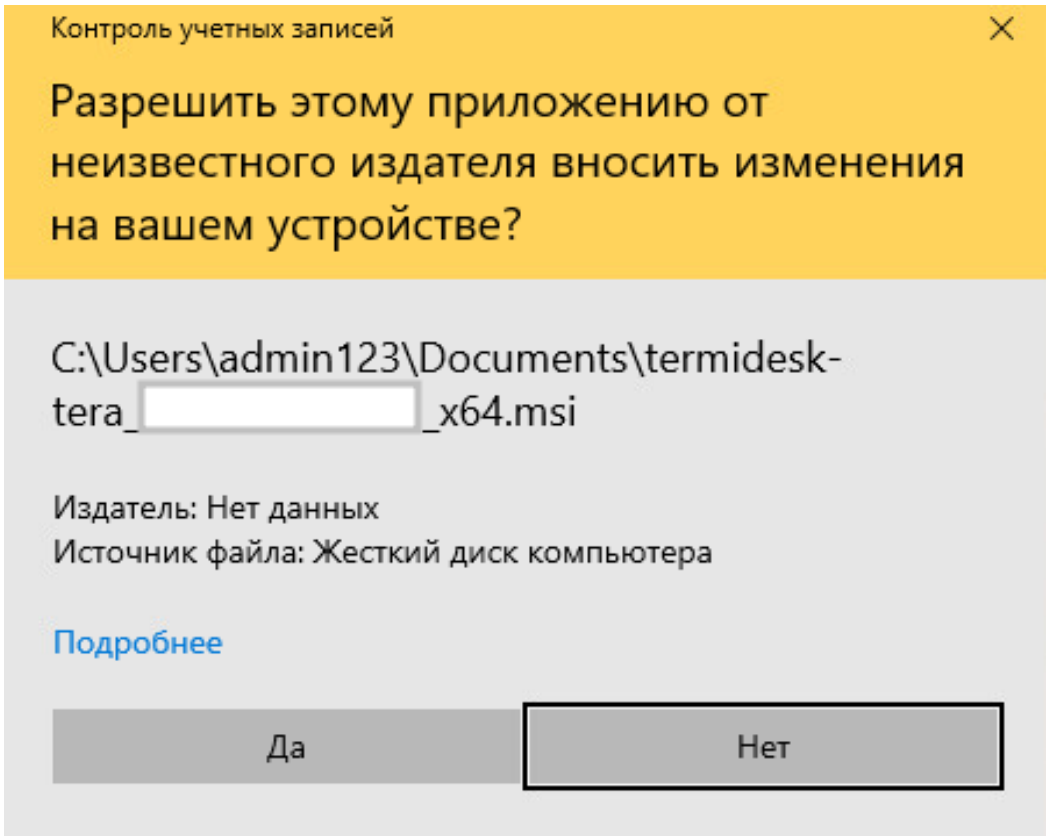


Рисунок 145. Окно запроса разрешений

- дождаться завершения установки и нажать экранную кнопку **[Готово]** (см. рисунок Успешное завершение установки);

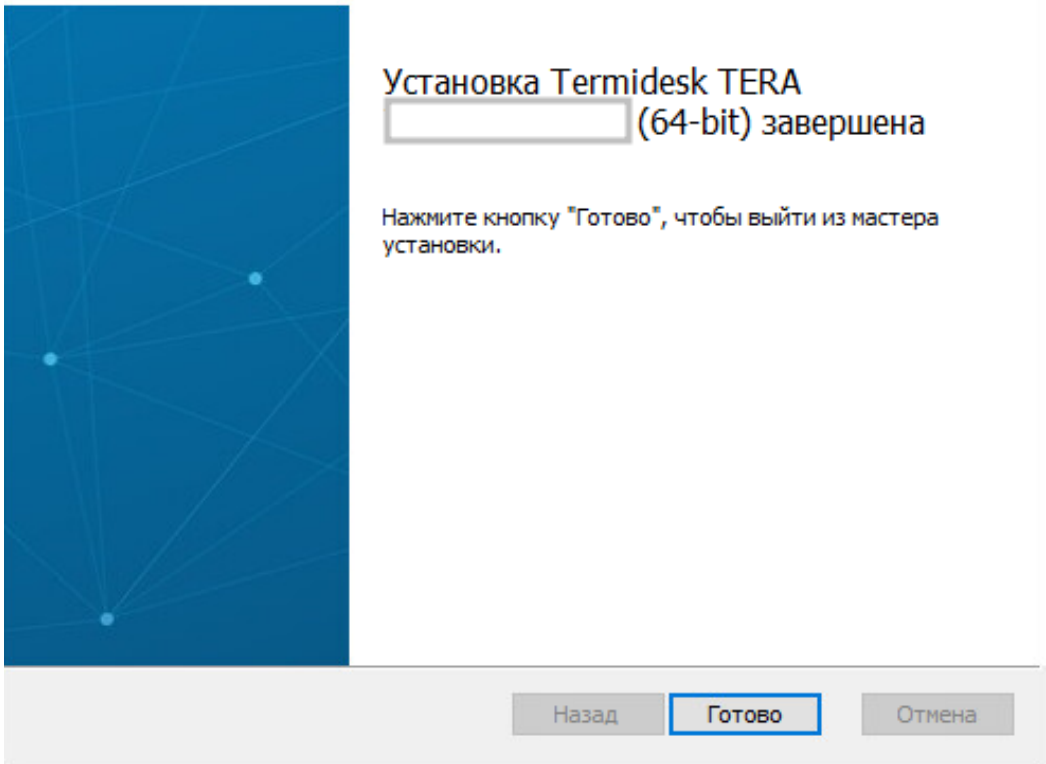


Рисунок 146. Успешное завершение установки

- при появлении сообщения о необходимости перезагрузки нужно согласиться с перезагрузкой системы, нажав экранную кнопку **[OK]**.

После установки:

- убедиться, что служба `TERA Agent` запущена;
- убедиться, что пользователь, подключающийся по протоколу TERA к ВРМ добавлен в группу «Пользователи удаленного рабочего стола»;
- будет установлено значение 1 (тип `REG_DWORD`) для параметра реестра `fForceRDVHLicensing` в `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService\` для регистрации провайдера TERA и включения удаленного доступа к ВМ (будут активированы функции «Удаленный рабочий стол» и «Разрешить удаленные подключения к этому компьютера» в настройках ОС);
- добавится раздел реестра `TERA` в `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations` для регистрации провайдера TERA;
- в ОС будет зарегистрирован драйвер видеоадаптера, обеспечивающего работу многомониторного режима - `TERAIddDriver`;
- в хранилищах сертификатов ОС («Доверенные корневые центры сертификации» и «Доверенные издатели») будет установлен сертификат ООО «УВЕОН».

Файлы, службы и процессы, создаваемые после установки, перечислены в подразделе **Общие сведения о параметрах в ОС Microsoft Windows**.

После подключения пользователя в его сессии появится графическое изображение `TERA Server` в системном трее ОС.

Обновление TERA в ОС Microsoft Windows

Обновление производится операцией установки более новой версии поверх предыдущей.

При обновлении пакета TERA, входившего в Termidesk VDI версии 6.1, на Termidesk VDI версии 7.0 потребуется удалить устаревшие настройки реестра, т.к. были обновлены пути к параметрам (см. подраздел **Конфигурационные файлы TERA в ОС Microsoft Windows**).

Восстановление TERA в ОС Microsoft Windows

В установочном файле TERA предусмотрена возможность исправления ошибок, возникших при установке или использовании компонента. Исправление ошибок выполняется путем восстановления отсутствующих и поврежденных файлов, ярлыков и записей реестра.

Для восстановления работоспособности:

- запустить установочный файл, в окне приветствия мастера установки нажать экранную кнопку **[Далее]**;
- нажать экранную кнопку **[Восстановить]**. Далее необходимо подтвердить восстановление и дождаться завершения операции. Для успешного восстановления необходимо разрешить внесение изменений при появлении соответствующего окна уведомления.

Удаление TERA в ОС Microsoft Windows

Удаление TERA выполняется одним из способов:

- для удаления с использованием стандартных средств ОС Microsoft Windows:
  - открыть меню «Пуск», перейти «Панель управления - Программы - Удаление программы», выбрать пункт «Termidesk TERA» и нажать на экранную кнопку **[Удалить]**. Далее подтвердить удаление и дождаться завершения операции;
- для удаления с использованием установочного файла:
  - запустить установочный файл, в окне приветствия мастера установки нажать экранную кнопку **[Далее]**;
  - нажать экранную кнопку **[Удалить]** и дождаться завершения операции. Для успешного удаления необходимо разрешить внесение изменений при появлении соответствующего окна уведомления.

При удалении:

- будут перезапущены службы удаленных рабочих столов ОС Microsoft Windows;
- параметр реестра `fForceRDVHLicensing` в `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService\` будет возвращен к первоначальному значению. Параметры «Удаленный рабочий стол» и «Разрешить удаленные подключения к этому компьютера» в настройках ОС будут возвращены к значениям до установки TERA.

TERA. НАСТРОЙКИ В ОС LINUX

Конфигурационные файлы TERA в ОС Linux

Общие сведения о параметрах конфигурирования TERA

Для настройки параметров TERA используются конфигурационные и исполняемые файлы, перечисленные в таблице (см. таблицу Список конфигурационных и исполняемых файлов TERA).

Таблица 252. Список конфигурационных и исполняемых файлов TERA

Файл	Применимость	Описание
`/etc/default/tera-vdagent`	ВМ, физическая машина	Настройка дополнительных параметров запуска ПО tera-vdagent
`/etc/default/tera-vdagentd`	ВМ, физическая машина	Настройка дополнительных параметров для автоматического запуска службы `tera-vdagentd`
`/etc/default/tera-usb-service`	ВМ, физическая машина	Настройка дополнительных параметров для автоматического запуска службы `tera-usb-service`
`/etc/default/x11tera`	Физическая машина	Настройка дополнительных параметров для автоматического запуска службы `x11tera`
`/etc/termidesk/tera-router.conf`	ВМ, физическая машина	Настройка дополнительных параметров для автоматического запуска службы `tera-router`
`/etc/termidesk/tera/sasl/*`	ВМ	Файлы сертификатов и ключей для настройки SSL/TLS-подключений (см. подраздел **Защита TCP-подключения с использованием SSL/TLS**), автоматически сгенерированные на этапе установки и использующиеся службой `tera-keyagent.service`: • `server-key.pem`; • `server-cert.pem`; • `ca-cert.pem`. Файлы создаются, если директории `/etc/termidesk/tera/sasl/` не существует в момент установки. Сертификаты формируются с использованием имени узла (`hostname`), заданного на момент запуска установки Не рекомендуется: • использовать директорию `/etc/termidesk/tera/sasl/` для хранения собственных файлов сертификатов и ключей; • использовать существующие в директории `/etc/termidesk/tera/sasl/` файлы для подписи других файлов.

Файл	Применимость	Описание
/etc/termidesk/tera/tera-mounting-shdir.yaml	ВМ, физическая машина	Используется для настройки запуска службы tera-mounting-shdir-service и определяет параметры монтирования каталога. Служба tera-mounting-shdir-service при запуске считывает параметры из этого конфигурационного файла Начиная с Termidesk версии 7.0 конфигурационный файл и служба tera-mounting-shdir-service входят в состав компонента «Агент виртуального рабочего места».
/etc/termidesk/tera/x11tera_greeter_lock.conf	Физическая машина	Постоянная конфигурация мониторов, применяемая на экране greeter. При создании права на файл устанавливаются в: rw-rw-rw (в восьмеричной записи - 666). Файл может быть изменен пользователем, исключение: ОС Astra Linux Special Edition в режиме «Смоленск» (ограничение ОС)
/etc/termidesk/tera/x11tera_greeter_unlock.conf	Физическая машина	Постоянная конфигурация мониторов, применяемая при выходе из экрана greeter. При создании права на файл устанавливаются в: rw-rw-rw (в восьмеричной записи - 666). Файл может быть изменен пользователем, исключение: ОС Astra Linux Special Edition в режиме «Смоленск» (ограничение ОС)
/etc/termidesk/tera/x11tera_user_lock.conf	Физическая машина	Постоянная конфигурация мониторов, применяемая при подключении пользователя. При создании права на файл устанавливаются в: rw-rw-rw (в восьмеричной записи - 666). Файл может быть изменен пользователем, исключение: ОС Astra Linux Special Edition в режиме «Смоленск» (ограничение ОС)
/etc/termidesk/tera/x11tera_user_unlock.conf	Физическая машина	Постоянная конфигурация мониторов, применяемая при отключении пользователя. При создании права на файл устанавливаются в: rw-rw-rw (в восьмеричной записи - 666). Файл может быть изменен пользователем, исключение: ОС Astra Linux Special Edition в режиме «Смоленск» (ограничение ОС)
/etc/polkit-1/rules.d/10-x11tera.rules	Физическая машина	Используется для настройки доставки сигналов службе x11tera_controls.service о событиях отключения или подключения удаленного пользователя
/etc/polkit-1/localauthority/50-local.d/50-x11tera.pkla	Физическая машина с ОС Astra Linux Special Edition 1.7	Используется для настройки доставки сигналов службе x11tera_controls.service о событиях отключения или подключения удаленного пользователя
/etc/sasl2/host.conf	ВМ, физическая машина	Используется для настройки аутентификации при активированной службе saslauthd
/etc/X11/xorg.conf.d/30-teraqxl.xorg.conf	ВМ	Используется для настройки параметров работы с виртуальным графическим процессором QXL
/etc/xdg/autostart/tera-audio.desktop	ВМ, физическая машина	Используется для настройки автоматического запуска службы tera-audio при авторизации пользователя
/etc/xdg/autostart/tera-record.desktop	ВМ, физическая машина	Используется для настройки автоматического запуска службы tera-record при авторизации пользователя

Файл	Применимость	Описание
`/etc/xdg/autostart/tera-vdagent.desktop`	ВМ, физическая машина	Используется для настройки автоматического запуска ПО tera-vdagent при авторизации пользователя
`/etc/xdg/autostart/tera-webdav-service.desktop`	ВМ, физическая машина	Используется для настройки автоматического запуска скрипта `/usr/bin/tera-webdav-service-start` при авторизации пользователя при создании оконной сессии
`/etc/xdg/autostart/x11tera.desktop`	Физическая машина	Используется для настройки запуска ПО x11tera в режиме приложения
`/etc/xdg/x11tera/x11tera.conf`	Физическая машина	Используется для настройки параметров ПО x11tera
`/etc/xdg/x11tera/cert/`	Физическая машина	Файлы сертификатов и ключей для настройки SSL/TLS-подключений (см. подраздел **Защита TCP-подключения с использованием SSL/TLS**), автоматически сгенерированные на этапе установки и использующиеся службой `tera-keyagent.service`: • `server-key.pem`; • `server-cert.pem`; • `ca-cert.pem`. Файлы создаются, если директории `/etc/xdg/x11tera/cert/` не существует в момент установки. Сертификаты формируются с использованием имени узла (`hostname`), заданного на момент запуска установки Не рекомендуется: • использовать директорию `/etc/xdg/x11tera/cert/` для хранения собственных файлов сертификатов и ключей; • использовать существующие в директории `/etc/xdg/x11tera/cert/` файлы для подписи других файлов.
`/lib/systemd/system/tera-keyagent.service`	ВМ, физическая машина	Настройка работы службы `tera-keyagent.service` (см. подраздел **Параметры запуска службы `tera-keyagent`**). Служба `tera-keyagent.service` выполняет сокрытие в файловой системе любой чувствительной информации и предоставление ее по запросу аутентифицированным процессам

Файл	Применимость	Описание
/lib/systemd/system/tera-mounting-shdir-service.service	ВМ, физическая машина	Настройка работы службы tera-mounting-shdir-service. Служба tera-mounting-shdir-service выполняет автоматическое монтирование в гостевую ОС перенаправляемого с пользовательской рабочей станции каталога Начиная с Termidesk версии 7.0 служба tera-mounting-shdir-service входит в состав компонента «Агент виртуального рабочего места».
/lib/systemd/system/tera-vdagentd.service	ВМ, физическая машина	Настройка работы службы tera-vdagentd
/lib/systemd/system/x11tera.service	Физическая машина	Настройка работы службы x11tera
/lib/systemd/system/x11tera_unlock.service	Физическая машина	Настройка работы службы x11tera_unlock
/lib/systemd/system/x11tera_controls.service	Физическая машина	Настройка работы службы x11tera_controls
/usr/bin/tera-audio-start	ВМ, физическая машина	Используется для контроля запуска и остановки пользовательской службы tera-audio. Запускается в каждой оконной сессии пользователя
/usr/bin/tera-mounting-shdir-service	ВМ, физическая машина	Используется для настройки работы службы tera-mounting-shdir-service. Служба tera-mounting-shdir-service выполняет автоматическое монтирование в гостевую ОС каталога, перенаправляемого с пользовательской рабочей станции Начиная с Termidesk версии 7.0 служба tera-mounting-shdir-service входит в состав компонента «Агент виртуального рабочего места».
/usr/bin/tera-record-start	ВМ, физическая машина	Используется для контроля запуска и остановки пользовательской службы tera-record. Запускается в каждой оконной сессии пользователя
/usr/bin/tera-vdagent.sh	ВМ, физическая машина	Используется для автоматического выбора режима запуска ПО tera-vdagent
/usr/bin/tera-webdav	ВМ, физическая машина	Используется для перенаправления каталога с пользовательской рабочей станции. Вызывается в /usr/lib/systemd/user/tera-webdav-service.service
/usr/bin/tera-webdav-service-start	ВМ, физическая машина	Используется для контроля запуска и остановки пользовательской службы tera-webdav-service. Запускается в каждой оконной сессии пользователя
/usr/bin/x11tera.sh	Физическая машина	Используется для запуска и останова выполнения служб ПО x11tera, является альтернативным методом управления состоянием этих служб
/usr/bin/x11tera_on_unlock	Физическая машина	Используется для управления периферийными устройствами физической машины при отключении пользователя

Файл	Применимость	Описание
/usr/bin/x11tera_on_lock	Физическая машина	Используется для управления периферийными устройствами физической машины при подключении пользователя
/usr/lib/udev/rules.d/70-tera-vdagentd.rules	ВМ, физическая машина	Используются для настройки работы службы tera-vdagentd
/usr/lib/systemd/user/tera-audio.service	ВМ, физическая машина	Настройка работы пользовательской службы tera-audio
/usr/lib/systemd/user/tera-record.service	ВМ, физическая машина	Настройка работы пользовательской службы tera-record
/usr/lib/systemd/user/tera-webdav-service.service	ВМ, физическая машина	Настройка работы пользовательской службы tera-webdav
/usr/lib/tmpfiles.d/tera-vdagentd.conf	ВМ, физическая машина	Используются для настройки работы службы tera-vdagentd
/usr/share/fly-dm/autostart/greeter/tera-vdagent.desktop	ВМ, физическая машина	Используется для настройки автоматического запуска ПО tera-vdagent до авторизации пользователя, на экране выбора учетной записи и до ввода пароля
/usr/share/fly-dm/autostart/greeter/x11tera.desktop	Физическая машина	Используется для настройки запуска ПО x11tera в режиме приложения. Запуск выполняется на экране выбора пользователей

Конфигурационный файл 30-teraqxl.xorg.conf

Конфигурационный файл /etc/X11/xorg.conf.d/30-teraqxl.xorg.conf используется для настройки параметров работы с виртуальным графическим процессором QXL и доступен только при установке TERA в среде функционирования ВМ.

При изменении конфигурационных параметров файла не рекомендуется изменять секции: Device, InputDevice, Monitor, Screen, Display, ServerLayout. Параметры данных секций автоматически управляются сервером Xorg.

После изменения параметров конфигурации нужно выполнить перезапуск гостевой ОС РМ.

В Termidesk версии 7.0.1 в наименования параметров конфигурационного файла были внесены изменения. Переименование затрагивает работу Xorg, поэтому если установка TERA производилась через обновление с предыдущей версии следует переименовать:

- xspice mouse в xtera mouse;
- xspice keyboard в xtera keyboard;
- xspice tablet в xtera tablet (если параметр ранее был, по умолчанию он отсутствует).

Параметры имеют значения по умолчанию. Для изменения значения закомментированого параметра его следует предварительно раскомментировать.

Перечень параметров, задающихся через файл /etc/X11/xorg.conf.d/30-teraqxl.xorg.conf, приведен в таблице (см. таблицу Параметры конфигурирования протокола TERA).

Таблица 253. Параметры конфигурирования протокола TERA

Параметр	Значение по умолчанию	Описание
Настройки аутентификации		
`TeraDisableTicketing`	`True`	Управление механизмом парольной аутентификации при подключении к гостевой ОС. По умолчанию после установки параметр закомментирован. Возможные значения: • `True` - разрешить подключение без предоставления пароля; • `False` - для подключения будет использоваться пароль, указанный в `TeraPassword`
`TeraPassword`	`Не задано`	Задание пароля для подключения к гостевой ОС. По умолчанию после установки параметр закомментирован. Использовать параметр не рекомендуется. По умолчанию параметр не задан (закомментирован)
`TeraSasl`	`False`	Управление использованием механизма аутентификации SASL. По умолчанию после установки TERA этот механизм аутентификации не используется. Требуется дополнительная настройка узла (см. подраздел **SASL-аутентификация**). Возможные значения: • `True` - разрешить аутентификацию SASL; • `False` - запретить аутентификацию SASL. При использовании библиотекой SASL механизма аутентификации GSSAPI требуется наличие и доступность SPN-записи в службе каталогов (FreeIPA, ALDPro, Microsoft Active Directory) для успешного прохождения аутентификации. Формат `SPN`-записи: `<имя_службы>/<полное_доменное_имя@имя_домена>`. При присоединении РМ к домену SPN-запись с именем службы «host» (`host/<полное_доменное_имя@имя_домена>`) должна быть создана автоматически. Если запись не появилась, то ее гарантированно создаст компонент «Агент виртуального рабочего места».

Параметр	Значение по умолчанию	Описание
`TeraGssUseProxy`	`False`	Управление использованием механизма аутентификации GSSAPI (Kerberos) в механизме SASL. По умолчанию после установки параметр закомментирован. Возможные значения: • `True` - разрешить Kerberos-аутентификацию в механизме SASL; • `False` - запретить Kerberos-аутентификацию в механизме SASL
Настройки журналирования		
`TeraDebug`	`False`	Управление использованием отладочного режима. По умолчанию после установки параметр закомментирован. Возможные значения: • `True` - использовать отладочный режим при журналировании событий; • `False` - не использовать отладочный режим при журналировании событий
Сетевые настройки TCP		
`TeraPort`	`0`	Порт для незащищенного подключения TERA. При организации резервного канала для подключения следует указать два порта: основной и резервный через запятую. Пример использования: `TeraPort=5900,5902` Значение `0` отключает использование незащищенного соединения. По умолчанию после установки используется значение `5900`

Параметр	Значение по умолчанию	Описание
`TeraTlsPort`	`0`	Порт для защищенного подключения TERA. По умолчанию после установки параметр закомментирован. Для использования только защищенного соединения нужно присвоить параметру `TeraPort` значение `0` или закомментировать его. При одновременном использовании защищенного и незащищенного соединения нужно указывать разные порты для параметров `TeraTlsPort` и `TeraPort`. При организации резервного канала для подключения следует указать два порта: основной и резервный через запятую. Пример использования: `TeraTlsPort=5901,5903` Значение `0` отключает использование защищенного соединения
`TeraAddr`	`Не задано`	Адрес прослушивания входящих подключений. По умолчанию после установки параметр закомментирован. Если параметр не задан, то используется адрес `0.0.0.0`
`TeraIPV4Only`	`False`	Управление прослушиванием входящих подключений только на IPv4-адресах. По умолчанию после установки параметр закомментирован. Возможные значения: • `True` - прослушивать только IPv4-адреса; • `False` - прослушивать IPv4 и IPv6-адреса
`TeraIPV6Only`	`False`	Управление прослушиванием входящих подключений только на IPv6-адресах. По умолчанию после установки параметр закомментирован. Возможные значения: • `True` - прослушивать только IPv6-адреса; • `False` - прослушивать IPv4 и IPv6-адреса
Сетевые настройки UDP		

Параметр	Значение по умолчанию	Описание
TeraUdpSupport	False	Управление использованием протокола UDP. По умолчанию после установки параметр закомментирован
TeraUdpAddress	Не задано	Адрес для приема UDP-данных. По умолчанию после установки параметр закомментирован: выбирается адрес, соответствующий сетевому интерфейсу, к которому подключен клиент, если он не указан. В некоторых случаях может потребоваться: • принудительно указать область действия для адреса. Пример (ens192 - область действия IPv6-адреса): fe80::b3b2:760d:35c8:f927%ens192; • или указать какой-либо адрес, на котором TERA-сервер будет получать UDP-данные
TeraUdpPortStart	5900	Начальное значение диапазона UDP-портов, который будет использоваться для приема UDP-данных. По умолчанию после установки параметр закомментирован. Пример: "TeraUdpPortStart" "5900"
TeraUdpPortEnd	5910	Конечное значение диапазона UDP-портов, который будет использоваться для приема UDP-данных. По умолчанию после установки параметр закомментирован. Пример: "TeraUdpPortEnd" "5910"
TeraUdpExclude	Не задано	Список каналов, которые не должны переключаться в режим UDP. Если имя канала есть в списке, то он не переключится в режим UDP, даже если отправлена команда со стороны клиентского приложения (ПО Termidesk Viewer). По умолчанию после установки параметр закомментирован. Имена вводятся строчными символами и разделяются запятыми, пример: "inputs,record,playback". Переключение в режим UDP для каналов records и playback произойдёт только при использовании кодека opus. Режим кодирования raw (без кодирования, только оцифрованный сигнал) не будет передаваться в режиме UDP
Настройки безопасности SSL поверх TCP и UDP		

Параметр	Значение по умолчанию	Описание
`TeraPreferServerCiphers`	`False`	Управление режимом выбора стороны, определяющей алгоритм шифрования во время TLS-рукопожатия. По умолчанию после установки параметр закомментирован. Возможные значения: • `True` - алгоритм определяется TERA-сервером. Из списка доступных выбирается первый (самый приоритетный) алгоритм, поддерживаемый и на стороне клиентского приложения. Значение рекомендуется для использования, т.к. выбирается наиболее стойкий алгоритм; • `False` - алгоритм определяется клиентским приложением. TERA-сервер выбирает первый поддерживаемый обеими сторонами алгоритм из списка клиента. Значение обычно используется для снижения нагрузки на CPU при использовании устаревших клиентских приложений (например, если клиентское приложение использует аппаратное ускорение для конкретного алгоритма, отсутствующего в списке приоритетных у TERA-сервера) Если указан `TeraTlsMinVer=TLSv1.3`, или системные настройки включат использование TLSv1.3, то назначение параметра не будет нести практического смысла, поскольку этот параметр нужен для тонкой настройки TLSv1.2.

Параметр	Значение по умолчанию	Описание
`TeraTlsVerifyClient`	`none`	Режим проверки клиентского сертификата TERA-сервером (использование mTLS). По умолчанию после установки параметр закомментирован. Возможные значения: • `none` - запрос клиентского сертификата отключен, выполняется защищенное TLS-соединение без mTLS; • `optional` - запрос клиентского сертификата включен и если сертификат предоставлен, то он проверяется. Если проверка подлинности не пройдена, соединение все равно установится (режим нестрогой проверки); • `require` - запрос клиентского сертификата включен и если сертификат предоставлен, то он проверяется. Если проверка подлинности не пройдена (сертификат не подписан доверенным УЦ, указанным в TeraCacertFile`), соединение немедленно разорвется (режим строгой проверки)  При использовании режимов `optional` или `require` требуется настроить SSL-сертификаты и ключи (см. подраздел **Защита TCP-подключения с использованием SSL/TLS**), в противном случае проверка сертификата завершится ошибкой.
Настройки безопасности SSL поверх TCP		
`TeraTlsMinVer`	`TLSv1.2`	Минимальная версия протокола TLS, которую будет поддерживать TERA-сервер при подключении клиентского приложения. По умолчанию после установки параметр закомментирован. Возможные значения: • `TLSv1` или `TLSv1.0` (небезопасный); • `TLSv1.2` (более безопасный, поддерживает современные алгоритмы шифрования); • `TLSv1.3` (самый безопасный). Перед использованием следует убедиться, что алгоритм поддерживается, для этого воспользоваться командой ниже. Если значение не указано, то используется системная настройка в соответствии с `/etc/ssl/openssl.cnf`. Поддерживаемые ОС алгоритмы можно получить командой: `openssl s_client -help 2\>&1 | grep -E "tls|timeout"`

Параметр	Значение по умолчанию	Описание
TeraTlsMaxVer	Не задано	Максимальная версия протокола TLS, которую будет поддерживать TERA-сервер при подключении клиентского приложения. По умолчанию после установки параметр закомментирован. Возможные значения и условия их использования аналогичны параметру TeraTlsMinVer
TeraTlsCiphers	HIGH:!aNULL:!kRSA:!PSK:!SRP:!MD5:!RC4	Список разрешенных наборов алгоритмов шифрования для протоколов до TLSv1.2 включительно. Если значение не указано, то используется системная настройка в соответствии с /etc/ssl/openssl.cnf. По умолчанию после установки параметр закомментирован. Пример задания значения: HIGH:!aNULL:!kRSA:!PSK:!SRP:!MD5:!RC4. Где: • HIGH - группа алгоритмов с длиной ключа 128 бит и выше, устойчивых к методу перебора паролей; • !aNULL - отключение алгоритмов, не использующих аутентификацию. Если не указывать, то стороны смогут установить защищенное соединение, но без проверки сертификата. Если указать, то это повысит устойчивость к MITM-атакам; • !aRSA - отключение устаревшего способа обмена ключами, при котором сессионный ключ шифруется публичным ключом сервера. Если указать, то это повысит устойчивость к отложенному взлому по записанному трафику, перехваченному ранее; • !PSK - отключения шифрования на основе заранее известного обеим сторонам пароля (без сертификатов). Если указать, то снизится вектор атак; • !SRP - отключение протокола аутентификации по паролю. Если указать, то снизится вектор атак; • !MD5 - отключение устаревшей функции хеширования. Если указать, то снизится вектор атак; • !RC4 - отключение потокового алгоритма с уязвимостями. Использование этого алгоритма запрещено стандартами TLS. Если указать, то снизится вектор атак
TeraTls13Ciphers	Не задано	Список разрешенных наборов алгоритмов шифрования для протокола TLSv1.3. Если значение не указано, то используется системная настройка в соответствии с /etc/ssl/openssl.cnf. По умолчанию после установки параметр закомментирован

Параметр	Значение по умолчанию	Описание
Настройки безопасности DTLS поверх UDP		
`TeraUdpDtlsMode`	`similar`	Режим использования шифрования в UDP-канале. По умолчанию после установки параметр закомментирован. Возможные значения: • `disable` - использование шифрования в UDP-канале отключено, даже если оно включено в TCP-канале; • `similar` - использование шифрования в UDP-канале подобно настройкам шифрования для TCP-канала. Если используется TLS в TCP-канале, то DTLS в UDP-канале тоже будет использоваться. Если шифрование в TCP-канале отключено, то и в UDP -канале оно не будет использоваться; • `require` - использование шифрования в UDP-канале включено, даже если оно отключено в TCP-канале. Если TLS для TCP-канала выключен, а DTLS для UDP-канала включен, то общие для обоих режимов параметры настройки SSL будут использоваться для UDP-канала (см. пункт таблицы «Настройки безопасности SSL поверх TCP и UDP»). Процедура перехода клиентского приложения в режим шифрования в UDP-канале будет выполняться автоматически в соответствии с настройками TERA-сервера
`TeraDtlsMinVer`	`Не задано`	Минимальная версия протокола DTLS, которую будет поддерживать TERA-сервер при подключении клиентского приложения. По умолчанию после установки параметр закомментирован. Возможные значения: • `DTLSv1` или `DTLSv1.0` (небезопасный); • `DTLSv1.2` (более безопасный, поддерживает современные алгоритмы шифрования); • `DTLSv1.3` (самый безопасный). Перед использованием следует убедиться, что алгоритм поддерживается, для этого воспользоваться командой ниже. Если значение не указано, то используется системная настройка в соответствии с `/etc/ssl/openssl.cnf`. Поддерживаемые ОС алгоритмы можно получить командой: `openssl s_client -help 2\>&1 | grep -E "dtls|timeout"`

Параметр	Значение по умолчанию	Описание
TeraDtlsMaxVer	Не задано	Максимальная версия протокола DTLS, которую будет поддерживать TERA-сервер при подключении клиентского приложения. По умолчанию после установки параметр закомментирован. Возможные значения и условия их использования аналогичны параметру TeraDtlsMinVer
TeraDtlsCiphers	HIGH:!aNULL:!eNULL:!kRSA:!PSK:!SRP:!MD5:!RC4:!3DES	Список разрешенных наборов алгоритмов шифрования для протоколов до DTLSv1.2 включительно. Если значение не указано, то используется системная настройка в соответствии с /etc/ssl/openssl.cnf. По умолчанию после установки параметр закомментирован
TeraDtls13Ciphers	Не задано	Список разрешенных наборов алгоритмов шифрования для протокола DTLSv1.3. Если значение не указано, то используется системная настройка в соответствии с /etc/ssl/openssl.cnf. По умолчанию после установки параметр закомментирован
Настройки поведения		
TeraExitOnDisconnect	False	Управление сервером TERA при отключении пользователя. По умолчанию после установки параметр закомментирован. Возможные значения: • True - сервер TERA завершит сессию, и все связанные с ней ресурсы будут освобождены; • False - сервер TERA продолжит работу, и будет доступен для подключения даже после отключения всех текущих пользователей

Параметр	Значение по умолчанию	Описание
AllowSingleClientOnly	0	Управление возможностью подключения нескольких пользователей одновременно. По умолчанию после установки параметр закомментирован. Возможные значения: • 0 - разрешены новые пользовательские подключения при завершении (отключении) уже установленных; • число от 1 до 10 - подключение нескольких пользователей одновременно отключено. Число является кодом завершения, которое будет отправлено клиентскому ПО пользователя при попытке подключиться к TERA. Соответствие кодов: • 1 - ERROR; • 2 - MAGIC; • 3 - INVALID_DATA; • 4 - VERSION_MISMATCH; • 5 - NEED_SECURED; • 6 - NEED_UNSECURED; • 7 - PERMISSION_DENIED; • 8 - BAD_CONNECTION_ID; • 9 - CHANNEL_NOT_AVAILABLE; • 10 - EMERGENCY
Настройки аудио		

Параметр	Значение по умолчанию	Описание

TeraAudioCodec	opus	Выбор аудиокодека, используемого для кодирования и декодирования аудиопотока.
		
		По умолчанию после установки параметр закомментирован.
		
		Возможные значения:
		
		• opus - действующими параметрами являются количество каналов, заданное в параметре TeraAudioChannels, и частота дискретизации, заданная в параметре TeraAudioSampleRate. Требуемая скорость (занимаемая полоса) составляет до 150 Кбит/с (для канала record и аналогично для playback). Это рекомендованное значение параметра;
		
		• pcm - действующие параметры определяются правилами:
		
		  - если заданная частота дискретизации в параметре TeraAudioSampleRate не равна нулю, то действующими параметрами являются количество каналов TeraAudioChannels и частота дискретизации TeraAudioSampleRate;
		
		  - если заданная частота дискретизации в параметре TeraAudioSampleRate равна нулю, то действующими параметрами являются количество каналов TeraAudioChannels, битрейт TeraAudioBitrate, переменный битрейт TeraAudioVBR. При этом если битрейт TeraAudioBitrate равен нулю, то при одноканальном режиме будет применяться значение 64, а при двухканальном - 96

TeraAudioChannels	2	Управление количеством аудиоканалов. По умолчанию после установки параметр закомментирован. Возможные значения: 1,2
TeraAudioSampleRate	0	Управление частотой дискретизации (Гц). По умолчанию после установки параметр закомментирован. Возможные значения: • для аудиокодека opus: 0, 8000, 12000, 16000, 24000, 48000; • для аудиокодека pcm: 0, 2000, 4000, 6000, 8000, 12000, 16000, 24000, 44100. Если для параметра используется значение 0, то ключевым параметром кодирования становится битрейт

Параметр	Значение по умолчанию	Описание
`TeraAudioBitrate`	`0`	Задание битрейта (Кбит/с) на один канал. По умолчанию после установки параметр закомментирован. Возможные значения: `0`, `8`, `12`, `16`, `24`, `32`, `48`, `64`, `128`. Если для параметра используется значение `0`, то используется битрейт, поддерживаемый аудиокодеком
`TeraAudioVBR`	`True`	Управление использованием среднего (переменного) битрейта (Кбит/с) аудиопотока на один канал. По умолчанию после установки параметр закомментирован. Возможные значения: • `True` - используется среднее значение битрейта для аудиопотока; • `False` - значение битрейта задается параметром `TeraAudioBitrate`
`TeraAudioRecSwitch`	`True`	Управление перенаправлением микрофона. По умолчанию после установки параметр закомментирован. Возможные значения: • `True` - события открытия и закрытия микрофона пересылаются в `tera-record-service`; • `False` - события открытия и закрытия микрофона не пересылаются
Настройки многомониторной конфигурации		
`NumHeads`	`2`	Управление количеством виртуальных мониторов, доступных для гостевой ОС
Настройки пропускной способности протокола		

Параметр	Значение по умолчанию	Описание
`TeraZlibGlzWanCompression`	`always`	Управление сжатием данных для оптимизации пропускной способности сети. По умолчанию после установки параметр закомментирован. Возможные значения: • `auto` - автоматическое управление сжатием данных в зависимости от состояния сети; • `never` - отключение сжатия данных. Может привести к увеличению объема передаваемой информации и обеспечить минимальную задержку при передаче данных. Значение может использоваться для снижения нагрузки на пользовательских рабочих станциях с низкой однопоточной производительностью; При отключении сжатия данных возможен значительный объема (трафика) видеопотока. В таком случае пропускной способности сети может оказаться недостаточно для стабильной работы. • `always` - включение сжатия данных. Может привести к уменьшению объема передаваемой информации и обеспечить высокую скорость передачи данных в условиях ограниченной пропускной способности сети
`TeraJpegWanCompression`	`always`	Управление сжатием изображения. По умолчанию после установки параметр закомментирован. Возможные значения: • `auto` - автоматическое управление сжатием изображения в зависимости от состояния сети; • `never` - отключение сжатия данных. Может привести к увеличению объема передаваемой информации и обеспечить максимальное качество изображения. Значение может использоваться для снижения нагрузки на пользовательских рабочих станциях с низкой однопоточной производительностью; При отключении сжатия данных возможен значительный рост объема (трафика) видеопотока. В таком случае пропускной способности сети может оказаться недостаточно для стабильной работы. • `always` - включение сжатия данных. Может привести к уменьшению качества изображения и обеспечить высокую скорость передачи изображения в условиях ограниченной пропускной способности сети

Параметр	Значение по умолчанию	Описание
`TeraImageCompression`	`auto_glz`	Управление алгоритмом сжатия изображения. По умолчанию после установки параметр закомментирован. Возможные значения: • `off` - отключить алгоритм сжатия данных. Может использоваться для снижения нагрузки на пользовательских рабочих станциях с низкой однопоточной производительностью; При отключении сжатия данных возможен значительный рост объема (трафика) видеопотока. В таком случае пропускной способности сети может оказаться недостаточно для стабильной работы. • `auto_glz` - автоматическое управление алгоритмом сжатия glz; • `auto_lz` - автоматическое управление алгоритмом сжатия lz; • `quic` - использование алгоритма сжатия данных quick; • `glz` - использование алгоритма сжатия данных glz; • `lz` - использование алгоритма сжатия данных lz
`TeraDeferredFPS`	`10`	Управление частотой следования опорных кадров (в секунду) видеоизображения. Параметр позволяет сгладить визуальное представление, используя опорные кадры. Возможные значения: • `0` - значение зарезервировано для автоматического режима, в котором скорость потока автоматически адаптируется под пропускную способность сети; • другое положительное целочисленное значение, которое отключит автоматическую адаптацию частоты следования опорных кадров На пользовательских рабочих станциях с низкой однопоточной производительностью не рекомендуется использовать значения, отличные от `0`.

Параметр	Значение по умолчанию	Описание
`TeraImageDiffBlockSize`	`32`	Управление механизмом сравнения кадров. Драйвер TERA определяет размер области изменений кадра (в пикселях), при достижении которого формируется и отправляется обновленный кадр. Для корректной работы параметра `TeraImageDiffBlockSize` параметрам `TeraDeferredFPS` и `TeraImageDiffBlockSize` нужно присвоить значение больше `0`. Использование параметра в ОС Astra Linux Special Edition не рекомендуется. По умолчанию после установки параметр закомментирован. Возможные значения: • `0` - механизм сравнения отключен. При этом драйвер TERA всегда доверяет накопленной области изменений; • другое положительное целочисленное значение - задает минимально допустимый размер (в пикселях) области изменений. Уменьшение значения позволяет более точно передавать область изменения кадра, увеличивая нагрузку на CPU сервера. Уменьшение значения снижает нагрузку на CPU сервера и увеличивает передаваемую область изменения кадра
`TeraStreamingVideo`	`filter`	Выбор режима передачи видеоизображения. При включении параметра на экране будут выявляться зоны с медиаактивностью, содержимое которых может передаваться в режиме реального времени. По умолчанию после установки параметр закомментирован. Возможные значения: • `off` - отключить передачу потокового видео. Параметр снижает нагрузку на сеть, но увеличивает задержку при отображении видеоизображения; • `filter` - включить передачу потокового видео. При этом поточной трансляции не будут подвергаться зоны на экране площадью меньше 96x96 (режим рекомендуется к использованию); • `all` - включить передачу потокового видео. При этом поточной трансляции будут подвергаться все зоны с медиаактивностью, в том числе малого размера (не рекомендуется к использованию из-за неоптимальности и повышения накладных расходов на работу сети)

Параметр	Значение по умолчанию	Описание
TeraVideoCodecs	Не задано	Выбор видеокодека, используемого для кодирования и декодирования видеопотока. По умолчанию после установки параметр закомментирован. Возможные значения: • mjpeg; • vp8; • h264
EnableImageCache	True	Управление кешированием изображений. По умолчанию после установки параметр закомментирован. Возможные значения: • True - включить кеширование изображений; • False - отключить кеширование изображений
EnableFallbackCache	True	Управление резервным кешированием. По умолчанию после установки параметр закомментирован. Возможные значения: • True - включить резервное кеширование; • False - отключить резервное кеширование
EnableSurfaces	True	Управление обновлением областей экрана. По умолчанию после установки параметр закомментирован. Возможные значения: • True - включить обновление областей экрана. Параметр позволяет оптимизировать отображение сложной графики и ускоряет отрисовку, кешируя объекты на пользовательской стороне; • False - отключить обновление областей экрана
Настройки буферизации потока видеодрайвера		
SurfaceBufferSize	512	Управление максимальным размером буфера (в мегабайтах) для хранения обновленных областей экрана. По умолчанию после установки параметр закомментирован
CommandBufferSize	512	Управление максимальным размером буфера (в мегабайтах) для хранения команд видеодрайвера. По умолчанию после установки параметр закомментирован

Параметр	Значение по умолчанию	Описание
FrameBufferSize	64	Управление максимальным размером буфера (в мегабайтах) для хранения кадров перед их отправкой с сервера на клиентскую часть. По умолчанию после установки параметр закомментирован
Настройки tera-vdagent		
TeraVdagentEnabled	True	Управление взаимодействием видеодрайвера с сервисом tera-vdagentd. По умолчанию после установки параметр закомментирован. Возможные значения: • True - разрешить взаимодействие с сервисом. Параметр позволяет использовать динамическое изменение разрешения экрана, буфер обмена с гостевой ОС; • False - запретить взаимодействие с сервисом
TeraVdagentVirtioPath	/tmp/xtera-virtio	Путь к виртуальному устройству virtio для взаимодействия сервиса tera-vdagentd с гостевой ОС. По умолчанию после установки параметр закомментирован
TeraVdagentUinputPath	/tmp/xtera-uinput	Путь к устройству uinput, используемому сервисом tera-vdagentd для отправки сигналов клавиатуры и мыши в гостевую ОС. По умолчанию после установки параметр закомментирован
TeraVdagentUid	0	Идентификатор пользователя по умолчанию для сокетов Virtio и Uinput. По умолчанию после установки параметр закомментирован, его не рекомендуется менять
TeraVdagentGid	0	Идентификатор группы по умолчанию для сокетов Virtio и Uinput. По умолчанию после установки параметр закомментирован, его не рекомендуется менять
TeraAgentMouse	True	Управление определением абсолютных или относительных координат мыши. Отключение параметра рекомендуется в случаях, когда курсор мыши плохо позиционируется в приложениях. По умолчанию после установки параметр закомментирован. Возможные значения: • True - использовать определение абсолютных координат мыши; • False - использовать определение относительных координат мыши

Параметр	Значение по умолчанию	Описание
`TeraDisableCopyPaste`	`False`	Управление буфером обмена для передачи данных между гостевой ОС и пользовательской рабочей станцией. По умолчанию после установки параметр закомментирован. Возможные значения: • `True` - отключить использование и обмен информацией в буферах обмена. Информация с пользовательской рабочей станции перестает синхронизироваться при операциях копирования и вставки; • `False` - разрешить использование и обмен информацией в буферах обмена
`TeraDisableKeyboardLocks`	`False`	Управление перенаправлением клавиатурных модификаторов между гостевой ОС и пользовательской рабочей станцией. По умолчанию после установки параметр закомментирован. Возможные значения: • `True` - запретить перенаправление клавиатурных модификаторов; • `False` - разрешить перенаправление клавиатурных модификаторов. При выборе значения `True`: • будет отсутствовать возможность доставлять в ПО Termidesk Viewer уведомления об автоматической смене клавиатурных модификаторов, например с помощью настроек графического менеджера; • будет отсутствовать возможность использования переключателей на экранной клавиатуре гостевой ОС при удаленном подключении к ней

Параметр	Значение по умолчанию	Описание

`TeraDisableTimeSync`	`True`	Управление синхронизацией времени в гостевой ОС по информации от пользовательской рабочей станцией.
		
		При настройке синхронизации времени может быть выбран один из способов (оба способа одновременно использовать нельзя):
		• либо использование службы `ntp` (рекомендуемый способ);
		• либо использование настроек TERA (`TeraDisableTimeSync=False`).
		
		По умолчанию после установки параметр закомментирован.
		
		Возможные значения:
		• `True` - запретить синхронизацию времени;
		• `False` - разрешить синхронизацию времени. Требуется отключение службы синхронизации времени в гостевой ОС.
		
		Для отключения службы синхронизации времени в гостевой ОС нужно:
		• проверить состояние служб:
		`sudo systemctl status systemd-timesyncd`
		`sudo systemctl status ntp`
		`sudo systemctl status chronyd`
		• отключить службу `ntp`:
		`sudo systemctl stop ntp`
		`sudo systemctl disable ntp`

Параметр	Значение по умолчанию	Описание

`TeraDisableTimezoneSync`	`False`	Управление синхронизацией временной зоны в гостевой ОС по информации от пользовательской рабочей станции.
		
		По умолчанию после установки параметр закомментирован.
		
		Возможные значения:
		
		• `True` - запретить синхронизацию временной зоны;
		• `False` - разрешить синхронизацию временной зоны.
		
		При смене временной зоны через службу `tera-vdagentd`:
		
		• если временная зона не будет найдена, то пользователю будет выдана ошибка в ПО Termidesk Viewer;
		• если полученная временная зона будет отсутствовать в гостевой ОС, то будет автоматически выбран регион временной зоны, заменяющий отсутствующий;
		• атомарно поменяется символьная ссылка `/etc/localtime` на файл новой временной зоны;
		• в файле `/etc/timezone` будет записано название новой временной зоны;
		• будет подана команда смены временной зоны в ОС:
		
		`timedatectl set-timezone`
		
		• будут перезагружены следующие службы (если они запущены и работают):
		  - для ОС на базе подсистемы systemd: `rsyslog`, `syslog-ng`, `cron`, `anacron`, `systemd-timesyncd`, `chronyd`, `ntpd`, `ntp`, `openntpd`;
		  - для других ОС: `cron`, `rsyslog`

`TeraDisableKeyboardLayout`	`False`	Управление режимом синхронизации клавиатурных раскладок (языков ввода). По умолчанию после установки параметр закомментирован. Возможные значения: • `True` - запретить синхронизацию клавиатурных раскладок; • `False` - разрешить синхронизацию клавиатурных раскладок
Настройки перенаправления USB-устройств		

Параметр	Значение по умолчанию	Описание
TeraUsbChannelNum	4	Количество каналов для перенаправления USB-устройств. По умолчанию после установки параметр закомментирован. Диапазон значений: от 0 до 8. Значение 0 отключает перенаправление USB-устройств
Настройки перенаправления каталога		
EnableWebdav	True	Управление перенаправлением каталога из пользовательской рабочей станции в гостевую ОС. По умолчанию после установки параметр закомментирован. Возможные значения: • True - разрешить перенаправление каталога; • False - запретить перенаправление каталога
Настройки перенаправления портов и каналов ввода/вывода		
TeraPortCount	0	Управление количеством последовательных портов, которые используются для обмена информацией между TERA-сервером и TERA-клиентом. По умолчанию после установки параметр закомментирован. Диапазон значений: от 0 до 4. Значение 0 отключает перенаправление последовательных портов
Секция ServerFlags		
AutoAddDevices	False	Управление автоматическим добавлением устройств в гостевую ОС при подключении по протоколу TERA. Возможные значения: • True - разрешить автоматическое добавление устройств; • False - запретить автоматическое добавление устройств

Конфигурационный файл x11tera.conf

Конфигурационный файл /etc/xdg/x11tera/x11tera.conf используется для настройки ПО x11tera.

Перечень параметров, задающихся через файл /etc/xdg/x11tera/x11tera.conf, приведен в таблице (см. таблицу Параметры конфигурирования TERA для физических машин).

После изменения параметров конфигурации нужно выполнить перезапуск ОС физической машины.

Таблица 254. Параметры конфигурирования TERA для физических машин

Параметр	Значение по умолчанию	Описание
Настройки журналирования		

Параметр	Значение по умолчанию	Описание
verbose	false	Управление использованием отладочного режима. Возможные значения: • true - использовать отладочный режим при журналировании событий; • false - не использовать отладочный режим при журналировании событий
Сетевые настройки TCP		
tcp-listen	5900	Порт прослушивания для входящих подключений. По умолчанию адрес прослушивания устанавливается как localhost. Может задаваться: • значение порта; • диапазон значений. Примеры: • 5900; • 5900-5910 - будет выбран свободный порт из указанного диапазона
Сетевые настройки UDP		
udp-support	false	Управление использованием протокола UDP. По умолчанию параметр не используется (закомментирован)
udp-address	Не задано	Адрес для приема UDP-данных. По умолчанию выбирается адрес, соответствующий сетевому интерфейсу, к которому подключен клиент, если он не указан. В некоторых случаях может потребоваться: • принудительно указать область действия для адреса. Пример (ens192 - область действия IPv6-адреса): fe80::b3b2:760d:35c8:f927%ens192; • или указать какой-либо адрес, на котором TERA-сервер будет получать UDP-данные По умолчанию параметр не используется (закомментирован)
udp-pool	5900-5910	Диапазон UDP-портов, который будет использоваться для приема UDP-данных. По умолчанию параметр не используется (закомментирован)

Параметр	Значение по умолчанию	Описание
udp-exclude	Не задано	Список каналов, которые не должны переключаться в режим UDP. Если имя канала есть в списке, то он не переключится в режим UDP, даже если отправлена команда со стороны клиентского приложения (ПО Termidesk Viewer). Имена вводятся строчными символами и разделяются запятыми, пример: inputs,record,playback. Переключение в режим UDP для каналов records и playback произойдёт только при использовании кодека opus. Режим кодирования raw (без кодирования, только оцифрованный сигнал) не будет передаваться в режиме UDP
Настройки использования пароля для подключения		
password	spicey	Задание пароля для подключения пользователя к ОС физической машины. По умолчанию параметр не используется (закомментирован) Должен задаваться только один из перечисленных параметров данной секции. Использовать параметр не рекомендуется.
generate-password	8	Задание длины пароля. Если параметр используется, то для подключения пользователя к ОС физической машины будет автоматически сгенерирован пароль заданной длины. Пароль будет показан в интерфейсе командной строки при запуске службы с соответствующим параметром. По умолчанию параметр не используется (закомментирован) Должен задаваться только один из перечисленных параметров данной секции. Использовать параметр не рекомендуется.

Параметр	Значение по умолчанию	Описание
`password-file`	`-`	Задание файла, хранящего пароль для подключения пользователя к ОС физической машины. Значение «-» соответствует чтению со стандартного устройства ввода. Пример использования (`P@s$w0rd` будет использован как пароль, т.к. задано стандартное устройство ввода): `cat "P@s$w0rd" | x11tera --password -file=-` По умолчанию параметр не используется (закомментирован) Должен задаваться только один из перечисленных параметров данной секции. Использовать параметр не рекомендуется.
`disable-ticketing`	`true`	Управление механизмом аутентификации при подключении к ОС физической машины. Возможные значения: • `true` - разрешить подключение без предоставления пароля; • `false` - запретить подключение без предоставления пароля Должен задаваться только один из перечисленных параметров данной секции.
Настройки аутентификации		

Параметр	Значение по умолчанию	Описание
`credentials-auth`	`false`	Управление возможностью использования поставщика учетных данных (Credentials Provider). Параметр приведен для справки и на данный момент не поддерживается. По умолчанию параметр не используется (закомментирован). Возможные значения: • `true` - разрешить использование поставщика учетных данных для аутентификации; • `false` - запретить использование поставщика учетных данных для аутентификации
`gss_use_proxy`	`false`	Управление использованием механизма аутентификации GSSAPI (Kerberos) в механизме SASL. По умолчанию параметр не используется (закомментирован). Возможные значения: • `true` - разрешить Kerberos-аутентификацию в механизме SASL; • `false` - запретить Kerberos-аутентификацию в механизме SASL
Настройки поведения		

Параметр	Значение по умолчанию	Описание
`allow-single-client-only`	`0`	Управление возможностью подключения нескольких пользователей одновременно. По умолчанию параметр не используется (закомментирован). Возможные значения: • `0` - разрешены новые пользовательские подключения при завершении (отключении) уже установленных; • число от 1 до 10 - подключение нескольких пользователей одновременно отключено. Число является кодом завершения, которое будет отправлено клиентскому ПО пользователя при попытке подключиться к TERA. Соответствие кодов: • `1` - `ERROR`; • `2` - `MAGIC`; • `3` - `INVALID_DATA`; • `4` - `VERSION_MISMATCH`; • `5` - `NEED_SECURED`; • `6` - `NEED_UNSECURED`; • `7` - `PERMISSION_DENIED`; • `8` - `BAD_CONNECTION_ID`; • `9` - `CHANNEL_NOT_AVAILABLE`; • `10` - `EMERGENCY`
Настройки `tera-vdagent`		
`virtio-path`	`/tmp/xtera-virtio`	Путь к виртуальному устройству `virtio` для взаимодействия сервиса `tera-vdagentd` с ОС физической машины
`uinput-path`	`/tmp/xtera-uinput`	Путь к устройству `uinput`, используемому сервисом `tera-vdagentd` для отправки сигналов клавиатуры и мыши в ОС физической машины
Настройки доступа к периферийным устройствам		
`on-connect`	`/usr/bin/x11tera_on_connect`	Путь к исполняемому файлу, задающему настройку периферийных устройств физической машины при подключении пользователя
`on-disconnect`	`/usr/bin/x11tera_on_disconnect`	Путь к исполняемому файлу, задающему настройку периферийных устройств физической машины при отключении пользователя
Настройки использования мыши и клавиатуры		

Параметр	Значение по умолчанию	Описание
`allow-control`	`true`	Управление возможностью для подключенного пользователя перемещать мышь и нажимать клавиши. Возможные значения: • `true` - разрешить перемещать мышь и нажимать клавиши; • `false` - запретить перемещать мышь и нажимать клавиши
Настройки времени ожидания соединения		
`timeout`	`0`	Задает время ожидания (в секундах), по истечении которого приложение `x11tera` прекратит работу, если соединение не было установлено. Пример использования: `x11tera --timeout=5 127.0.0.1:5902` Значение `0` означает, что время ожидания не задано
Настройки параметров аудита		
`audit`	`false`	Управление режимом аудита событий в системе аудита ОС. Для включения режима требуются расширенные права пользователя (в большинстве ОС права пользователя `root`) для подключения к системе аудита ОС. Если режим включен, но требования не выполнены, то приложение `x11tera` завершит работу. Возможные значения: • `true` - режим аудита включен; • `false` - режим аудита отключен
`audit-message-type`	`1196`	Задание типа сообщения для регистрации в системе аудита ОС. Значение `1196` используется для событий ПО x11tera. Параметр работает совместно с `audit`. Для просмотра событий указанного типа можно выполнить: `sudo ausearch --message 1196`

Параметр	Значение по умолчанию	Описание
Настройки пропускной способности протокола		
`zlib-glz-compression`	`always`	Управление сжатием данных для оптимизации пропускной способности сети. Возможные значения: • `auto` - автоматическое управление сжатием данных в зависимости от состояния сети; • `never` - отключение сжатия данных. Может привести к увеличению объема передаваемой информации и обеспечить минимальную задержку при передаче данных. Значение может использоваться для снижения нагрузки на пользовательских рабочих станциях с низкой однопоточной производительностью; При отключении сжатия данных возможен значительный рост объема (трафика) видеопотока. В таком случае пропускной способности сети может оказаться недостаточно для стабильной работы. • `always` - включение сжатия данных. Может привести к уменьшению объема передаваемой информации и обеспечить высокую скорость передачи данных в условиях ограниченной пропускной способности сети

Параметр	Значение по умолчанию	Описание
`jpeg-compression`	`always`	Управление сжатием изображения. Возможные значения: • `auto` - автоматическое управление сжатием изображения в зависимости от состояния сети; • `never` - отключение сжатия данных. Может привести к увеличению объема передаваемой информации и обеспечить максимальное качество изображения. Значение может использоваться для снижения нагрузки на пользовательских рабочих станциях с низкой однопоточной производительностью; При отключении сжатия данных возможен значительный рост объема (трафика) видеопотока. В таком случае пропускной способности сети может оказаться недостаточно для стабильной работы. • `always` - включение сжатия данных. Может привести к уменьшению качества изображения и обеспечить высокую скорость передачи изображения в условиях ограниченной пропускной способности сети

Параметр	Значение по умолчанию	Описание
`image-compression`	`auto_glz`	Управление алгоритмом сжатия изображения. Возможные значения: • `off` - отключить алгоритм сжатия данных. Может использоваться для снижения нагрузки на пользовательских рабочих станциях с низкой однопоточной производительностью; При отключении сжатия данных возможен значительный рост объема (трафика) видеопотока. В таком случае пропускной способности сети может оказаться недостаточно для стабильной работы. • `auto_glz` - автоматическое управление алгоритмом сжатия glz; • `auto_lz` - автоматическое управление алгоритмом сжатия lz; • `quic` - использование алгоритма сжатия данных quick; • `glz` - использование алгоритма сжатия данных glz; • `lz` - использование алгоритма сжатия данных lz
Настройки доверия к уведомлениям об изменении экрана		
`trust-damage`	`auto`	Управление режимом доверия к повторяющимся уведомлениям об изменении экрана. Некоторые оконные менеджеры могут слишком часто уведомлять о полном изменении экрана. Для настройки доверия к таким уведомлениям используется параметр `trust-damage`. Возможные значения: • `auto` - не доверять уведомлениям, начиная с третьего; • `always` - доверять каждому уведомлению; • `never` - не доверять всем уведомлениям
Настройки частоты передачи экрана		

Параметр	Значение по умолчанию	Описание
`full-screen-fps`	`0`	Задание режима передачи изображения экрана в ПО Termidesk Viewer. При установке `0` включается автоматический режим: передаются только изменившиеся области экрана, а частота обновления подстраивается под активность пользователя. Нижняя и верхняя границы этой частоты задаются параметрами `region-update-fps-lower` и `region-update-fps-upper`. Если задано значение, отличное от `0`, полное изображение экрана отправляется с указанной частотой (`<значение>` кадров в секунду). По умолчанию используется значение `0` В ОС Astra Linux Special Edition для дисплейного менеджера fly-dm изменять параметр не рекомендуется, следует оставить значение `0`. В других ОС и дисплейных менеджерах (например, GNOME) экран может обновляться целиком даже при небольших изменениях, что повышает нагрузку на сеть. Для ограничения частоты таких обновлений параметру задаётся значение, отличное от `0`.
`region-update-fps-upper`	`20`	Верхняя граница частоты обновления экрана (кадров в секунду) в автоматическом режиме. Чем выше значение, тем плавнее изображение при активных действиях пользователя, но тем больше сетевой трафик. Максимальное допустимое значение: `30`. По умолчанию используется значение `20` Параметр действует только при `full-screen-fps=0`.

Параметр	Значение по умолчанию	Описание
`region-update-fps-lower`	`1`	Нижняя граница частоты обновления экрана (кадров в секунду) в автоматическом режиме. До этого значения частота снижается, когда на экране ничего не меняется. Минимальное допустимое значение: `1`. По умолчанию используется значение `1` Параметр действует только при `full-screen-fps=0`.
`region-update-fps-jumpy`	`5`	Частота обновления экрана (кадров в секунду), на которую система сразу переходит при первом действии пользователя после паузы. Чем больше значение, тем выше отзывчивость интерфейса после паузы, но тем сильнее нагрузка на процессор. Чем меньше значение, тем ниже отзывчивость и меньше нагрузка. Если параметр не задан, частота нарастает плавно от нижней границы. Значение должно быть больше, чем `region-update-fps-lower`, и меньше или равно `region-update-fps-upper`. По умолчанию используется значение `5` Параметр действует только при `full-screen-fps=0`.
Настройки кодирования видеопотока		
`codecs`	`spice:mjpeg`	Выбор видеокодека, используемого для кодирования и декодирования видеопотока. Возможные значения: • `spice:mjpeg`; • `gstreamer:vp8`; • `gstreamer:h264`

Параметр	Значение по умолчанию	Описание
`streaming-video`	`filter`	Выбор режима передачи видеоизображения. При включении параметра на экране будут выявляться зоны с медиаактивностью, содержимое которых может передаваться в режиме реального времени. Возможные значения: • `off` - отключить передачу потокового видео. Параметр снижает нагрузку на сеть, но увеличивает задержку при отображении видеоизображения; • `filter` - включить передачу потокового видео. При этом поточной трансляции не будут подвергаться зоны на экране площадью меньше 96x96 (режим рекомендуется к использованию); • `all` - включить передачу потокового видео. При этом поточной трансляции будут подвергаться все зоны с медиаактивностью, в том числе малого размера (не рекомендуется к использованию из-за неоптимальности и повышения накладных расходов на работу сети).
Настройки запуска и отображения графического интерфейса		
`minimize`	`false`	Запуск графического интерфейса приложения `x11tera` в оконном режиме. По умолчанию графический интерфейс не отображается, т.к. ПО x11tera запускается как служба ОС. Параметр является унарным аргументом и может использоваться при вызове приложения `x11tera`. Пример использования: `x11tera --minimize 127.0.0.1:5905`
`hide`	`false`	Сокрытие графического интерфейса приложения `x11tera` в трей. По умолчанию графический интерфейс не отображается, т.к. ПО x11tera запускается как служба ОС. Параметр является унарным аргументом и может использоваться при вызове приложения `x11tera`. Пример использования: `x11tera --hide 127.0.0.1:5905`

Параметр	Значение по умолчанию	Описание
Настройки дисплея		
`display`	`:0`	Выбор дисплея для подключения пользователя. По умолчанию используется значение, полученное из переменной окружения ОС `DISPLAY` Не рекомендуется менять параметр.
Настройки завершения выполнения ПО x11tera		
`exit-on-disconnect`	`false`	Управление режимом завершения приложения `x11tera` после отключения первого пользователя. Параметр не используется, приведен для справки. Возможные значения: • `true` - ПО x11tera завершится после отключения первого пользователя от сессии; • `false` - ПО x11tera не завершится после отключения первого пользователя от сессии
Настройки вывода диагностической информации		
`debug-draws`	`0`	Управление режимом вывода диагностической информации в стандартное устройство вывода. Возможные значения: • `0` - вывод диагностической информации отключен; • `1` - вывод базовой диагностической информации; • `2` - вывод подробной диагностической информации
Настройки синхронизации клавиатурных раскладок и модификаторов		
`disable-keyboard-layout`	`false`	Управление режимом синхронизации клавиатурных раскладок (языков ввода). Возможные значения: • `true` - запретить синхронизацию клавиатурных раскладок; • `false` - разрешить синхронизацию клавиатурных раскладок
Настройки перенаправления USB-устройств		
`usb-channel-num`	`0`	Задание количества каналов для перенаправления USB-устройств. Диапазон значений: от 0 до 8. Значение `0` - перенаправление отключено

Параметр	Значение по умолчанию	Описание
Настройки перенаправления каталога		
webdav-channel-enable	true	Управление перенаправлением каталога из пользовательской рабочей станции в ОС физической машины. Возможные значения: • true - разрешить перенаправление каталога; • false - запретить перенаправление каталога
Настройки перенаправления портов и каналов ввода/вывода		
port-count	0	Управление количеством последовательных портов, которые используются для обмена информацией между TERA-сервером и TERA-клиентом. Диапазон значений: от 0 до 4. Значение 0 - перенаправление отключено
Настройки аудио		
audio-codec	opus	Выбор аудиокодека, используемого для кодирования и декодирования аудиопотока. Возможные значения: • opus. Требуемая скорость (занимаемая полоса) составляет до 150 Кбит/с (для канала record и аналогично для playback). Это рекомендованное значение параметра; • pcm
audio-channels	2	Управление количеством аудиоканалов. Возможные значения: 1,2
audio-sample-rate	0	Управление частотой дискретизации (Гц). Возможные значения: • для аудиокодека opus: 0, 8000, 12000, 16000, 24000, 48000; • для аудиокодека pcm: 0, 2000, 4000, 6000, 8000, 12000, 16000, 24000, 44100. Если для параметра используется значение 0, то ключевым параметром кодирования становится битрейт
audio-bitrate	0	Задание битрейта (Кбит/с) на один канал. Возможные значения: 0, 8, 12, 16, 24, 32, 48, 64, 128. Если для параметра используется значение 0, то используется битрейт, поддерживаемый аудиокодеком

Параметр	Значение по умолчанию	Описание
audio-vbr	true	Управление использованием среднего (переменного) битрейта (Кбит/с) аудиопотока на один канал. Возможные значения: • true - используется среднее значение битрейта для аудиопотока; • false - значение битрейта задается параметром audio-bitrate
audio-rec-switch	true	Управление перенаправлением микрофона. Возможные значения: • true - события открытия и закрытия микрофона пересылаются в tera-record-service; • false - события открытия и закрытия микрофона не пересылаются
Настройки SSL/TLS и DTLS (часть настроек являются общими)		
Настройки SSL		
ca-cert-file	Не задано	Путь к файлу корневого сертификата для SSL/TLS. Начиная с Termidesk VDI версии 7.0 параметр не поддерживается. Расположение сертификата передается в сервисном файле /usr/lib/systemd/system/tera-keyagent.service (см. подраздел **Параметры запуска службы tera-keyagent**). По умолчанию параметр не используется (закомментирован)
certs-file	Не задано	Путь к файлу серверного сертификата SSL/TLS. Начиная с Termidesk VDI версии 7.0 параметр не поддерживается. Расположение сертификата передается в сервисном файле /usr/lib/systemd/system/tera-keyagent.service (см. подраздел **Параметры запуска службы tera-keyagent**). По умолчанию параметр не используется (закомментирован)

Параметр	Значение по умолчанию	Описание
`private-key-file`	`Не задано`	Путь к файлу ключа для SSL/TLS. Начиная с Termidesk VDI версии 7.0 параметр не поддерживается. Расположение ключа передается в сервисном файле `/usr/lib/systemd/system/tera-keyagent.service` (см. подраздел **Параметры запуска службы** `tera-keyagent`). По умолчанию параметр не используется (закомментирован)
`dh-key-file`	Не задано	Путь к файлу с ключами Диффи-Хеллмана для SSL/TLS. Начиная с Termidesk VDI версии 7.0 параметр не поддерживается. По умолчанию параметр не используется (закомментирован)

Параметр	Значение по умолчанию	Описание
`verify-client`	`none`	Режим проверки клиентского сертификата TERA-сервером (использование mTLS). Возможные значения: • `none` - запрос клиентского сертификата отключен, выполняется защищенное TLS-соединение без mTLS; • `optional` - запрос клиентского сертификата включен и если сертификат предоставлен, то он проверяется. Если проверка подлинности не пройдена, соединение все равно установится (режим нестрогой проверки); • `require` - запрос клиентского сертификата включен и если сертификат предоставлен, то он проверяется. Если проверка подлинности не пройдена (сертификат не подписан доверенным УЦ, указанным в TeraCacertFile`), соединение немедленно разорвется (режим строгой проверки).  ! При использовании режимов `optional` или `require` требуется настроить SSL-сертификаты и ключи (см. подраздел **Защита TCP-подключения с использованием SSL/TLS**), в противном случае проверка сертификата завершится ошибкой. По умолчанию параметр закомментирован

Параметр	Значение по умолчанию	Описание
`prefer-server-ciphers`	`true`	Управление режимом выбора стороны, определяющей алгоритм шифрования во время TLS-рукопожатия. Возможные значения: • `true` - алгоритм определяется TERA-сервером. Из списка доступных выбирается первый (самый приоритетный) алгоритм, поддерживаемый и на стороне клиентского приложения. Значение рекомендуется для использования, т.к. выбирается наиболее стойкий алгоритм; • `false` - алгоритм определяется клиентским приложением. TERA-сервер выбирает первый поддерживаемый обеими сторонами алгоритм из списка клиента. Значение обычно используется для снижения нагрузки на CPU при использовании устаревших клиентских приложений (например, если клиентское приложение использует аппаратное ускорение для конкретного алгоритма, отсутствующего в списке приоритетных у TERA-сервера) Если указан `min-proto-ver=TLSv1.3`, или системные настройки включат использование TLSv1.3, то назначение параметра не будет нести практического смысла, поскольку этот параметр нужен для тонкой настройки TLSv1.2. По умолчанию параметр закомментирован
Настройки TLS		
`enabled`	`false`	Управление режимом использования защищенного соединения TLS для TCP. Возможные значения: • `true` - SSL/TLS используется, должны быть указаны валидные сертификаты в соответствующих параметрах; • `false` - SSL/TLS не используется

Параметр	Значение по умолчанию	Описание
cipher-list	HIGH:!aNULL:!kRSA:!PSK:!SRP:!MD5:!RC4	Список разрешенных наборов алгоритмов шифрования для протоколов до TLSv1.2 включительно. Если значение не указано, то используется системная настройка в соответствии с /etc/ssl/openssl.cnf. Пример задания значения: HIGH:!aNULL:!kRSA:!PSK:!SRP:!MD5:!RC4. Где: • `HIGH ` - группа алгоритмов с длиной ключа 128 бит и выше, устойчивых к методу перебора паролей; • !aNULL - отключение алгоритмов, не использующих аутентификацию. Если не указывать, то стороны смогут установить защищенное соединение, но без проверки сертификата. Если указать, то это повысит устойчивость к MITM-атакам; • !aRSA - отключение устаревшего способа обмена ключами, при котором сессионный ключ шифруется публичным ключом сервера. Если указать, то это повысит устойчивость к отложенному взлому по записанному трафику, перехваченному ранее; • !PSK - отключения шифрования на основе заранее известного обеим сторонам пароля (без сертификатов). Если указать, то снизится вектор атак; • !SRP - отключение протокола аутентификации по паролю. Если указать, то снизится вектор атак; • !MD5 - отключение устаревшей функции хеширования. Если указать, то снизится вектор атак; • !RC4 - отключение потокового алгоритма с уязвимостями. Использование этого алгоритма запрещено стандартами TLS. Если указать, то снизится вектор атак
ciphersuites	Не задано	Список разрешенных наборов алгоритмов шифрования для протокола TLSv1.3. Если значение не указано, то используется системная настройка в соответствии с /etc/ssl/openssl.cnf. По умолчанию параметр закомментирован

Параметр	Значение по умолчанию	Описание
`min-proto-ver`	`TLSv1.2`	Минимальная версия протокола TLS, которую будет поддерживать TERA-сервер при подключении клиентского приложения. Возможные значения: • `TLSv1` или `TLSv1.0` (небезопасный); • `TLSv1.2` (более безопасный, поддерживает современные алгоритмы шифрования); • `TLSv1.3` (самый безопасный). Перед использованием следует убедиться, что алгоритм поддерживается, для этого воспользоваться командой ниже. Если значение не указано, то используется системная настройка в соответствии с `/etc/ssl/openssl.cnf`. Поддерживаемые ОС алгоритмы можно получить командой: `openssl s_client -help 2\>&1 | grep -E "tls|timeout"`
`max-proto-ver`	Не задано	Максимальная версия протокола TLS, которую будет поддерживать TERA-сервер при подключении клиентского приложения. Возможные значения и условия их использования аналогичны параметру `min-proto-ver`. По умолчанию параметр не используется (закомментирован)
Настройки DTLS		

Параметр	Значение по умолчанию	Описание
enabled	similar	Режим использования шифрования в UDP-канале. Возможные значения: • false - использование шифрования в UDP-канале отключено, даже если оно включено в TCP-канале; • similar - использование шифрования в UDP-канале подобно настройкам шифрования для TCP-канала. Если используется TLS в TCP-канале, то DTLS в UDP-канале тоже будет использоваться. Если шифрование в TCP-канале отключено, то и в UDP -канале оно не будет использоваться; • require - использование шифрования в UDP-канале включено, даже если оно отключено в TCP-канале. Если TLS для TCP-канала выключен, а DTLS для UDP-канала включен, то общие для обоих режимов параметры настройки SSL будут использоваться для UDP-канала (см. пункт таблицы «Настройки безопасности SSL поверх TCP и UDP»). Процедура перехода клиентского приложения в режим шифрования в UDP-канале будет выполняться автоматически в соответствии с настройками TERA-сервера. По умолчанию параметр не используется (закомментирован)
cipher-list	HIGH:!aNULL:!eNULL:!kRSA:!PSK:!SRP:!MD5:!RC4:!3DES	Список разрешенных наборов алгоритмов шифрования для протоколов до DTLSv1.2 включительно. Если значение не указано, то используется системная настройка в соответствии с /etc/ssl/openssl.cnf
ciphersuites	Не задано	Список разрешенных наборов алгоритмов шифрования для протокола DTLSv1.3. Если значение не указано, то используется системная настройка в соответствии с /etc/ssl/openssl.cnf. По умолчанию параметр закомментирован

Параметр	Значение по умолчанию	Описание
min-proto-ver	DTLSv1.2	Минимальная версия протокола DTLS, которую будет поддерживать TERA-сервер при подключении клиентского приложения. Возможные значения: • DTLSv1 или DTLSv1.0 (небезопасный); • DTLSv1.2 (более безопасный, поддерживает современные алгоритмы шифрования); • DTLSv1.3 (самый безопасный). Перед использованием следует убедиться, что алгоритм поддерживается, для этого воспользоваться командой ниже. Если значение не указано, то используется системная настройка в соответствии с /etc/ssl/openssl.cnf. Поддерживаемые ОС алгоритмы можно получить командой: `openssl s_client -help 2\>&1 | grep -E "dtls|timeout"`
max-proto-ver	Не задано	Максимальная версия протокола DTLS, которую будет поддерживать TERA-сервер при подключении клиентского приложения. Возможные значения и условия их использования аналогичны параметру min-proto-ver

Конфигурационный файл tera.conf

Конфигурационный файл /etc/sasl2/tera.conf используется для настройки аутентификации TERA.

Перечень параметров, задающихся через файл /etc/sasl2/tera.conf, приведен в таблице (см. таблицу Параметры конфигурирования службы SASL для протокола TERA).

Таблица 255. Параметры конфигурирования службы SASL для протокола TERA

Параметр	Значение по умолчанию	Описание
mech_list	plain	Задание механизма запроса пароля. Значение по умолчанию: plain - пароль в виде текста. TERA использует защищенное подключение через TLS для аутентификации пользователя, поэтому пароль передается в преобразованном виде
log_level	7	Управление уровнем регистрации событий. Значение по умолчанию: 7

Параметр	Значение по умолчанию	Описание
pwcheck_method	saslauthd	Задание компонента аутентификации, используемого для проверки паролей. Значение по умолчанию: saslauthd - используется компонент Saslauthd
auxprop_plugin	pam	Задание модуля аутентификации, используемого для компонента, заданного в параметре pwcheck_method. Значение по умолчанию: pam

Конфигурационный файл tera-mounting-shdir.yaml

Конфигурационный файл /etc/termidesk/tera/tera-mounting-shdir.yaml используется для настройки параметров монтирования перенаправленного каталога.

Начиная с Termidesk версии 7.0 конфигурационный файл и служба tera-mounting-shdir-service входят в состав компонента «Агент виртуального рабочего места».

Перечень параметров, задающихся через файл /etc/termidesk/tera/tera-mounting-shdir.yaml, приведен в таблице (см. таблицу Параметры конфигурирования монтирования каталога).

Таблица 256. Параметры конфигурирования монтирования каталога

Параметр	Значение по умолчанию	Описание
mount_dir	$HOME/davfs/	Задание точки монтирования каталога, перенаправленного с пользовательской рабочей станции
debug	False	Управление отладочным режимом регистрации событий монтирования. Запись событий ведется в /var/syslog
use_locks	False	Управление блокированием файла при его открытии для записи. Блокировка предотвращает одновременное изменение одного файла несколькими пользователями или процессами
gui_optimize	True	Ускоряет работу графических оболочек с каталогами, содержащими большое количество файлов. При открытии файла mount.davfs обычно проверяется наличие новой версии каждого отдельного файла. Графические оболочки часто открывают множество файлов (например, для чтения метаданных), что вызывает множество запросов и замедляет работу. Данный параметр включает оптимизацию: вместо отдельных проверок для каждого файла выполняется один групповой запрос для всего каталога
unmount_task_timeout	40	Задание интервала времени (в секундах) между повторными попытками размонтирования (отключения) перенаправленных каталогов, если предыдущая попытка завершилась неудачно. Такая ситуация может возникнуть, например, из-за ошибок доступа или если каталог используется другими процессами. Параметр определяет, как часто будет предприниматься новая попытка размонтирования до тех пор, пока ресурс не будет успешно отключен

Исполняемые файлы TERA в ОС Linux

Исполняемый файл x11tera_on_lock

Исполняемый файл /usr/bin/x11tera_on_lock используется для настройки параметров блокирования периферийных устройств при подключении пользователя.

Перечень параметров, задающихся через файл /usr/bin/x11tera_on_lock, приведен в таблице (Параметры конфигурирования периферийных устройств при подключении пользователя).

Таблица 257. Параметры конфигурирования периферийных устройств при подключении пользователя

Параметр	Значение по умолчанию	Описание
WITH_MONITORS_OFF	1	Управление режимом отключения мониторов и удаления их из схемы расположения. Возможные значения: • 0 - режим отключен. В этом случае: ◦ мониторы не отключаются и не удаляются из схемы расположения; ◦ экраны мониторов не гаснут; ◦ окна приложений остаются в позициях, в которых они были открыты; ◦ посторонние лица могут наблюдать за действиями подключившегося удаленного пользователя; ◦ подключившемуся удаленному пользователю транслируется содержимое всех экранов, в том числе нерабочие области между мониторами на схеме расположения; • 1 - режим включен. В этом случае: ◦ мониторы отключаются и удаляются из схемы расположения; ◦ экраны мониторов гаснут; ◦ окна приложений перемещаются на оставшийся не отключенный монитор (как правило, это основной монитор); ◦ посторонние лица не могут наблюдать за действиями подключившегося удаленного пользователя; ◦ подключившемуся удаленному пользователю транслируется содержимое лишь одного экрана (это соответствует штатному рабочему режиму)

Параметр	Значение по умолчанию	Описание

WITH_PRIMARY_MONITOR_OFF	1	Управление режимом отключения отображения на основном мониторе.
		
		Возможные значения:
		
		• 0 - режим отключен. В этом случае:
		  изображение будет отображаться на основном мониторе;
		  посторонние лица могут наблюдать за действиями подключившегося удаленного пользователя;
		• 1 - режим включен. В этом случае:
		  изображение не будет отображаться на основном мониторе;
		  посторонние лица не могут наблюдать за действиями подключившегося удаленного пользователя

WITH_DPMS_OFF	1	Управление режимом отключения электропитания монитора.
		
		Не все мониторы могут быть отключены по электропитанию: в общем случае (например, если используется монитор ноутбука) оно возобновится при активности подключившегося пользователя на физической машине.
		
		Если к физической машине подключен внешний монитор, являющийся основным, то включенный режим можно использовать для индикации подключения пользователя к физической машине.
		
		Возможные значения:
		
		• 0 - режим отключен. В этом случае электропитание монитора не отключается, его состояние фиксируется в момент подключения удаленного пользователя;
		• 1 - режим включен. В этом случае:
		  электропитание монитора отключается;
		  если используется внешний монитор, то индикаторы электропитания погаснут. Такое поведение может использоваться для индикации подключения пользователя к физической машине.

Параметр	Значение по умолчанию	Описание

WITH_LOGINCTRL	lock	Управление поведением экрана физической машины для подключившегося авторизованного пользователя.
		
		Возможные значения:
		
		• lock - экран будет заблокирован. В этом случае:
		  - если пользователь подключился к физической машине удаленно, то вход для локальной сессии ОС не произойдет;
		  - подключившемуся удаленному пользователю требуется ввести пароль для авторизации в ОС;
		• unlock - экран будет разблокирован. В этом случае:
		  - произойдет автоматическая авторизация в локальную сессию ОС физической машины;
		  - подключившемуся удаленному пользователю не потребуется ввод пароля для авторизации в ОС;
		• keep - экран будет сохранен в состоянии, зафиксированном в момент подключения удаленного пользователя

WITH_LOCK_KEYBOARDS	1	Управление режимом отключения клавиатуры в момент подключения удаленного пользователя.
		
		Возможные значения:
		
		• 0 - режим отключен. В этом случае:
		  - подключенная к физической машине клавиатура не блокируется;
		  - посторонние лица могут вмешиваться в работу подключившегося удаленного пользователя, а также управлять работой ПО и ОС физической машины;
		• 1 - режим включен. В этом случае:
		  - подключенная к физической машине клавиатура блокируется;
		  - посторонние лица не могут вмешиваться в работу подключившегося удаленного пользователя, а также не могут управлять работой ПО и ОС физической машины;
		
		Рекомендуется включить режимы для параметров WITH_MONITORS_OFF и WITH_PRIMARY_MONITOR_OFF для затруднения вмешательства посторонних лиц в работу подключившегося пользователя.
		
		Разблокировка и принудительное отключение удаленного пользователя возможна и через интерфейсы ввода (см. подраздел **Разблокирование физической машины с помощью интерфейсов ввода**)

Параметр	Значение по умолчанию	Описание

WITH_LOCK_POINTERS	1	Управление режимом отключения указательных устройств (мыши, тачпадов и других) в момент подключения удаленного пользователя.
		
		Возможные значения:
		
		• 0 - режим отключен. В этом случае:
		  подключенное к физической машине устройство не блокируется;
		  посторонние лица могут вмешиваться в работу подключившегося удаленного пользователя, а также управлять работой ПО и ОС физической машины;
		• 1 - режим включен. В этом случае:
		  подключенная к физической машине мышь блокируется;
		  посторонние лица не могут вмешиваться в работу подключившегося удаленного пользователя, а также не могут управлять работой ПО и ОС физической машины;
		
		Рекомендуется включить режимы для параметров WITH_MONITORS_OFF и WITH_PRIMARY_MONITOR_OFF для затруднения вмешательства посторонних лиц в работу подключившегося пользователя.
		
		Разблокировка и принудительное отключение удаленного пользователя возможна и через интерфейсы ввода (см. подраздел **Разблокирование физической машины с помощью интерфейсов ввода**)

Исполняемый файл x11tera_on_unlock

Исполняемый файл /usr/bin/x11tera_on_unlock используется для настройки параметров разблокирования периферийных устройств при отключении пользователя.

Перечень параметров, задающихся через файл /usr/bin/x11tera_on_unlock, приведен в таблице (см. таблицу Параметры конфигурирования периферийных устройств при отключении пользователя).

Восстановление работоспособности мониторов и восстановление схемы их расположения (если их было подключено несколько) происходит автоматически, если был включен режим для параметра WITH_MONITORS_OFF.

Таблица 258. Параметры конфигурирования периферийных устройств при отключении пользователя

Параметр	Значение по умолчанию	Описание
WITH_UNLOCK_INPUTS	1	Управление режимом отключения указательных устройств (мыши, тачпадов и других) в момент отключения пользователя. Возможные значения: • 0 - режим отключен. В этом случае указательные устройства не будут разблокированы; • 1 - режим включен. В этом случае указательные устройства будут разблокированы

Параметр	Значение по умолчанию	Описание

WITH_LOCK_SESSION	1	Управление режимом блокирования локальной сессии.
		
		Возможные значения:
		
		• 0 - режим отключен. В этом случае:
		  автоматическое блокирование локальной сессии не происходит;
		  рабочий стол ОС физической машины (и все открытые программы) будут доступны без ввода пароля;
		• 1 - режим включен. В этом случае:
		  происходит автоматическое блокирование локальной сессии;
		  требуется ввод пароля для работы в локальной сессии ОС физической машины

WITH_DPMS_ON	0	Управление режимом отключения электропитания мониторов. Возможные значения: • 0 - режим отключен. В этом случае электропитание монитора не отключается; • 1 - режим включен. В этом случае электропитание монитора отключается
WITH_FORCED_STOP	0	Управление режимом принудительного останова ПО x11tera. Возможные значения: • 0 - режим отключен. В этом случае принудительный останов ПО x11tera не выполняется; • 1 - режим включен. В этом случае выполняется принудительный останов ПО x11tera

Параметры запуска служб TERA

Параметры запуска службы tera-vdagentd

Параметры запуска службы tera-vdagentd задаются в файле /lib/systemd/system/tera-vdagentd.service.

В зависимости от дистрибутива ОС путь может отличаться.

При запуске службы tera-vdagentd передаются дополнительные аргументы командной строки ПО tera-vdagentd (см. подраздел **Интерфейс командной строки ПО tera-vdagentd**), что обеспечивает гибкую настройку работы ПО.

Одним из параметров службы tera-vdagentd является аргумент EnvironmentFile, задающий путь к переменным окружения, а также дополнительные аргументы, перечисленные в файле /etc/default/tera-vdagentd.

Файл /etc/default/tera-vdagentd:

- является необязательным и может отсутствовать в ОС;
- может содержать необязательный параметр TERA_VDAGENTD_EXTRA_ARGS, задающий дополнительные аргументы командной строки ПО tera-vdagentd.Если при

определении параметра TERA_VDAGENTD_EXTRA_ARGS используются несколько аргументов, то все они задаются в кавычках.

Пример содержимого файла /etc/default/tera-vdagentd:

```
TERA_VDAGENTD_EXTRA_ARGS="-Q -l"
```

Для изменения настроек ПО можно воспользоваться режимом реконфигурирования пакета - внести правки в интерактивном диалоге с пояснениями и подсказками (изменения автоматически применятся в файлы /etc/default/tera-vdagent и /etc/default/tera-vdagentd):

```
sudo dpkg-reconfigure tera-vdagent
```

Параметры запуска службы x11tera

Параметры запуска службы x11tera задаются в файле /lib/systemd/system/x11tera.service.

В зависимости от дистрибутива ОС путь может отличаться.

При запуске службы x11tera передаются дополнительные аргументы командной строки ПО x11tera (см. подраздел **Интерфейс командной строки ПО x11tera**), что обеспечивает гибкую настройку работы ПО.

Одним из параметров службы x11tera является аргумент EnvironmentFile, задающий путь к переменным окружения, а также дополнительные аргументы, перечисленные в файле /etc/default/x11tera.

Файл /etc/default/x11tera:

- является необязательным и может отсутствовать в ОС;
- может содержать необязательный параметр TERA_X11_EXTRA_ARGS, задающий дополнительные аргументы командной строки ПО x11tera. Если при определении параметра TERA_X11_EXTRA_ARGS используются несколько аргументов, то все они задаются в кавычках.

Пример файла /etc/default/x11tera:

```
TERA_X11_EXTRA_ARGS="—ssl --password-file=/etc/x11tera/private/some-secret-file"
```

Параметры запуска службы tera-usb-service

Параметры запуска службы tera-usb-service задаются в файле /lib/systemd/system/tera-usb-service.service.

В зависимости от дистрибутива ОС путь может отличаться.

Одним из параметров службы tera-usb-service является аргумент EnvironmentFile, задающий путь к переменным окружения, а также дополнительные аргументы, перечисленные в файле /etc/default/tera-usb-service.

Файл /etc/default/tera-usb-service:

- является необязательным и может отсутствовать в ОС;
- может содержать необязательный параметр TERA_VHCI_EXTRA_ARGS, задающий дополнительные аргументы командной строки ПО tera-usb. Если при определении параметра TERA_VHCI_EXTRA_ARGS используются несколько аргументов, то все они задаются в кавычках.

Пример содержимого файла /etc/default/tera-usb-service:

В аргументе count задается количество создаваемых виртуальных USB-устройств. Возможные значения: от 1 до 8.

После перенаправления USB-устройства оно будет зарегистрировано в /var/run/termidesk/tera-usb-%d.

```
TERA_VHCI_EXTRA_ARGS="--count 3"
```

Параметры запуска службы tera-webdav-service

Параметры запуска службы tera-webdav-service задаются в файле /lib/systemd/system/tera-webdav.service.

В зависимости от дистрибутива ОС путь может отличаться.

При запуске службы tera-webdav-service одним из параметров может быть передан TERA_WEBDAVD_EXTRA_ARGS, задающий дополнительные аргументы командной строки ПО tera-webdav (см. подраздел **Интерфейс командной строки ПО tera-webdav**).

Параметр TERA_WEBDAVD_EXTRA_ARGS задается как системная переменная.

Если при определении параметра TERA_WEBDAVD_EXTRA_ARGS используются несколько аргументов, то все они задаются в кавычках.

Параметры запуска службы tera-router

Пакет tera-router требуется для обеспечения подключения по UDP через шлюз, во всех других случаях (без UDP через шлюз, прямое подключение без шлюза) проксирование подключений не требуется

Параметры запуска службы tera-router задаются в файле /lib/systemd/system/tera-router.service.

В зависимости от дистрибутива ОС путь может отличаться.

При запуске службы tera-route передаются дополнительные аргументы командной строки ПО tera-router (см.подраздел **Интерфейс командной строки ПО tera-router**),что обеспечивает гибкую настройку работы ПО.

Одним из параметров службы tera-router является аргумент EnvironmentFile, задающий путь к переменным окружения, а также дополнительные аргументы, перечисленные в файле /etc/termidesk/tera-router.conf.

Файл /etc/termidesk/tera-router.conf:

- является необязательным и может отсутствовать в ОС;
- содержит параметры, задающие дополнительные аргументы для запуска службы tera-router.

Пример содержимого файла /etc/termidesk/tera-router.conf по умолчанию:

```
TERA_SRV_PRIMARY_ARGS="-c 0:0:0:127.0.0.1:5900"
#TERA_ROUTER_ADDRESS=0.0.0.0
#TERA_ROUTER_PORT=6000
#TERA_SRV_FALLBACK_ARGS="-c 0:0:0:127.0.0.1:5902"
#TERA_ROUTER_UDP_ARGS="-l 20:21 -b 3:0:0:${TERA_ROUTER_ADDRESS:-0.0.0.0}:6010:1
#TERA_ROUTER_EXTRA_ARGS="-d"
```

Настройка службы tera-router зависит от настроек конфигурационного файла /etc/X11/xorg.conf.d/30-teraqxl.xorg.conf.

Например, для направления всех подключений на порт 5900 используются следующие настройки в /etc/termidesk/tera-router.conf:

- если заданы Option "TeraPort" "5902,5904" и Option "TeraAddr" "127.0.0.1", то:

```
TERA_ROUTER_PORT=5900
TERA_SRV_PRIMARY_ARGS="-c 0:0:0:127.0.0.1:5902"
TERA_SRV_FALLBACK_ARGS="-c 0:0:0:127.0.0.1:5904"
```

- если заданы Option "TeraPort" "5903,5905" и Option "TeraAddr" "127.0.0.1", то:

```
TERA_ROUTER_PORT=5901
TERA_SRV_PRIMARY_ARGS="-c 0:0:0:127.0.0.1:5903"
TERA_SRV_FALLBACK_ARGS="-c 0:0:0:127.0.0.1:5905"
```

Перечень параметров, задающихся через файл приведен в таблице (см. таблицу Параметры запуска службы tera-router).

Таблица 259. Параметры запуска службы tera-router

Параметр	Значение по умолчанию	Описание
TERA_ROUTER_ADDRESS	0.0.0.0	Адрес прослушивания входящих подключений. Значение 0.0.0.0 - зарезервированный адрес, задающий прослушивание подключений на всех сетевых интерфейсах. При необходимости его можно заменить на IP-адрес какого-то одного сетевого интерфейса

Параметр	Значение по умолчанию	Описание
TERA_ROUTER_PORT	6000	Порт прослушивания входящих подключений
TERA_SRV_PRIMARY_ARGS	"-c 0:0:0:127.0.0.1:5900"	Основные настройки для подключения к TERA, которые будут использоваться для всех входящих подключений
TERA_SRV_FALLBACK_ARGS	Не задано	Резервные настройки для подключения к TERA, которые будут использоваться для всех входящих подключений, если интерфейс с основными настройками недоступен
TERA_ROUTER_UDP_ARGS	Не задано	Настройки для UDP-трафика. Описание параметров приведено в таблице (см. таблицу Ключи, используемые в параметре TERA_ROUTER_EXTRA_ARGS)
TERA_ROUTER_EXTRA_ARGS	Не задано	Переменная окружения для передачи дополнительных аргументов командной строки в ПО tera-router (см. подраздел **Интерфейс командной строки ПО tera-router**)

Таблица 260. Ключи, используемые в параметре TERA_ROUTER_EXTRA_ARGS

Ключ	Описание
-l	Включение определения типа канала по пакету состояния канала. Ключ применим только для открытого трафика. Формат значения: [type_offset]:[id_offset] Пример значения: 20:21
-b	Прослушиваемый интерфейс. Можно указать несколько. По умолчанию используется 0.0.0.0. Значение рекомендуется переопределить, указав реальный IP-адрес. При использовании значения по умолчанию будет использоваться адрес первого доступного сетевого интерфейса (не localhost). Формат значения: [тип_канала]:[идентификатор_канала]:[метка]:[IP-адрес]:[порт]<:[протокол]>. Информация по параметрам, передающимся в значении, приведена в таблице (см. таблицу Параметры для значений ключей). Пример значения: 3:0:0:0.0.0.0:6010:1

Таблица 261. Параметры для значений ключей

Параметр	Описание
[тип_канала]	Тип канала. Обязательный параметр. Возможные значения: • 1 - MAIN; • 2 - DISPLAY; • 3 - INPUTS; • 4 - CURSOR; • 5 - PLAYBACK; • 6 - RECORD; • 7 - TUNNEL; • 8 - SMARTCARD; • 9 - USBREDIR; • 10 - PORT; • 11 - WEBDAV
[идентификатор_канала]	Идентификатор канала. Обязательный параметр
[метка]	Метка, выставляемая на пакеты. Обязательный параметр
[IP-адрес]	IP-адрес. Обязательный параметр
[порт]	Порт. Обязательный параметр
[протокол]	Протокол. Необязательный параметр Возможные значения: • 0 (умолчанию) для TCP; • любое другое целочисленное значение для UDP

Примеры использования приведены в таблице (см. таблицу Примеры использования для UDP).

Таблица 262. Примеры использования для UDP

Сценарий	Пример

Настройка для UDP-канала INPUTS (3) с идентификатором 0 и меткой 0	Значение для ключа -b: 3:0:0.
	
	Примеры задания TERA_ROUTER_UDP_ARGS:
	
	`TERA_ROUTER_UDP_ARGS="-l 20:21 -b 3:0:0:0.0.0.0:6010:1"`
	
	`TERA_ROUTER_UDP_ARGS="-l 20:21 -b 3:0:0:${TERA_ROUTER_ADDRESS:-0.0.0.0}:6010:1"`

Сценарий	Пример

Настройка для UDP-каналов INPUTS и CURSOR	Значения для ключа `-b`: `3:0:0` и `4:0:0`.
	
	Примеры задания `TERA_ROUTER_UDP_ARGS`:
	
	`TERA_ROUTER_UDP_ARGS="-l 20:21 -b 3:0:0:0.0.0.0:6010:1 -b 4:0:0:0.0.0.0:6020:1`
	
	`TERA_ROUTER_UDP_ARGS="-l 20:21 -b 3:0:0:${TERA_ROUTER_ADDRESS:-0.0.0.0}:6010:1 -b 4:0:0:${TERA_ROUTER_ADDRESS:-0.0.0.0}:6020:1"`

Параметры запуска службы `tera-keyagent`

Параметры запуска службы `tera-keyagent` задаются в файле `/lib/systemd/system/tera-keyagent.service`.

В зависимости от дистрибутива ОС путь может отличаться.

В настройки запуска службы `tera-keyagent` передаются пути к сертификатам и закрытому ключу для настройки SSL-подключений (см. подраздел **Защита TCP-подключения с использованием SSL/TLS**):

- `LoadCredential=ca_cert:<путь>` - путь к корневому сертификату УЦ;
- `LoadCredential=server_cert:<путь>` - путь к серверному SSL-сертификату;
- `LoadCredential=server_key:<путь>` - путь к закрытому ключу.

По умолчанию после установки используется конфигурация:

- для ВМ:

```
LoadCredential=ca_cert:/etc/termidesk/tera/sasl/ca-cert.pem
LoadCredential=server_cert:/etc/termidesk/tera/sasl/server-cert.pem
LoadCredential=server_key:/etc/termidesk/tera/sasl/server-key.pem
```

- для физической машины:

```
LoadCredential=ca_cert:/etc/xdg/x11tera/cert/ca-cert.pem
LoadCredential=server_cert:/etc/xdg/x11tera/cert/server-cert.pem
LoadCredential=server_key:/etc/xdg/x11tera/cert/server-key.pem
```

Указанные настройки позволяют передать сертификаты и ключи в защищенную среду процесса `tera-keyagent`. При запуске службы содержимое файлов копируется в защищенную память, `systemd` применяет механизм виртуального монтирования и реализует строгое ограничение доступа в целях безопасности.

При использовании самоподписанного серверного сертификата достаточно указать только параметры `server_key` и `server_cert`. Параметр

> `ca_cert` указывается только при подписи серверного сертификата УЦ, при необходимости его можно закомментировать.

Параметры запуска службы `tera-record`

Параметры запуска службы `tera-record` задаются в файле `/usr/lib/systemd/user/tera-record.service`.

> В зависимости от дистрибутива ОС путь может отличаться.

Одним из параметров службы `tera-record` является аргумент `EnvironmentFile`, задающий путь к переменным окружения, а также дополнительные аргументы, перечисленные в файле `/etc/default/tera-record`.

Файл `/etc/default/tera-record`:

- является необязательным и может отсутствовать в ОС;
- может содержать необязательный параметр `TERA_REC_BUFFER_SIZE`, определяющий размер буфера для хранения аудиоданных, полученных с микрофона.

> Параметр `TERA_REC_BUFFER_SIZE` рекомендуется задавать при использовании шлюза.
>
> Возможные значения: от 2 до 500.
>
> Для применения параметра нужно предоставить всем пользователям право на чтение файла `/etc/default/tera-record`:
>
> ```
> sudo chmod a+r /etc/default/tera-record
> ```
>
> Значение параметра определяет количество фрагментов аудиоданных для хранения в буфере.
>
> Пример расчета: (52 * 2) / 10 = 10,4. Полученное значение округляется до ближайшего большего целого числа - 11. Результат указывается в параметре.
>
> Где:
>
> - 52 - максимальная задержка канала (в миллисекундах), взятая из окна «Статистика сеанса» ПО Termidesk Viewer на продолжительном участке времени (следует провести несколько замеров и выбрать максимальный показатель из всех);
> - 2 - множитель. Увеличивает лимит максимальной задержки канала относительно значения, полученного в результате замеров. Значение множителя определяется администратором в зависимости от требуемого запаса по задержке канала;
> - 10 - константа. Определяет длительность (в миллисекундах) одного фрагмента аудиоданных;
> - 11 - результирующее количество фрагментов аудиоданных после округления.

Пример содержимого файла `/etc/default/tera-record`:

```
TERA_REC_BUFFER_SIZE=11
```

Для применения изменений нужно воспользоваться одним из способов:

- завершить сеанс пользователя и повторно войти в графический интерфейс ОС;
- перезапустить службу `tera-record` командой (перезапуск выполняется пользователем):

```
systemctl --user restart tera-record
```

Переменные окружения

Переменные окружения используются для указания параметров настройки TERA и позволяют переопределить значения, заданные в конфигурационных файлах. Для этого нужно внести переменные окружения и их значения в файл `/etc/environment`, затем перезапустить ОС. Перечень переменных окружения приведен в таблице (см. таблицу Переменные окружения TERA).

Таблица 263. Переменные окружения TERA

Переменная окружения	Параметр файла `30-teraqxl.xorg.conf`	Параметр файла `x11tera.conf`	Примечание
XTERA_DISABLE_TICKETING	TeraDisableTicketing	[tera] disable-ticketing	-
XTERA_PASSWORD	TeraPassword	[tera] password, [tera] generate-password,[tera] password-file	-
XTERA_SASL	TeraSasl	-	-
XTERA_GSS_USE_PROXY	TeraGssUseProxy	[tera] gss_use_proxy	-
XTERA_REMOTE_TPM_AUTH	TeraRemoteTpmAuth	-	-
XTERA_CREDENTIALS_AUTH	TeraCredentialsAuth	[tera] credentials-auth	-
TERA_DEBUG	TeraDebug	[tera] verbose	-
XTERA_PORT	TeraPort	[tera] listen	-
XTERA_TLS_PORT	TeraTlsPort	[tera] listen	-
XTERA_ADDR	TeraAddr	[tera] listen	-
XTERA_IPV4_ONLY	TeraIPV4Only	-	-
XTERA_IPV6_ONLY	TeraIPV6Only	-	-
XTERA_UDP_SUPPORT	TeraUdpSupport	[tera] udp-support	-
XTERA_UDP_ADDR	TeraUdpAddress	[tera] udp-address	-
XTERA_UDP_PORT_START	TeraUdpPortStart	[tera] udp-pool	-

Переменная окружения	Параметр файла 30-teraqxl.xorg.conf	Параметр файла x11tera.conf	Примечание
XTERA_UDP_PORT_END	TeraUdpPortEnd	[tera] udp-pool	-
XTERA_UDP_EXCLUDE	TeraUdpExclude	[tera] udp-exclude	-
XTERA_PREFER_SERVER_CIPHERS	TeraPreferServerCiphers	[ssl] prefer-server-ciphers	-
XTERA_TLS_VERIFY_CLIENT	TeraTlsVerifyClient	[ssl] verify-client	-
XTERA_TLS_MIN_VER	TeraTlsMinVer	[tls] min-proto-ver	-
XTERA_TLS_MAX_VER	TeraTlsMaxVer	[tls] max-proto-ver	-
XTERA_TLS_CIPHERS	TeraTlsCiphers	[tls] cipher-list	-
XTERA_TLS13_CIPHERSUITES	TeraTls13Ciphers	[tls] ciphersuites	-
XTERA_UDP_DTLS_MODE	TeraUdpDtlsMode	[dtls] enabled	-
XTERA_DTLS_MIN_VER	TeraDtlsMinVer	[dtls] min-proto-ver	-
XTERA_DTLS_MAX_VER	TeraDtlsMaxVer	[dtls] max-proto-ver	-
XTERA_DTLS_CIPHERS	TeraDtlsCiphers	[dtls] cipher-list	-
XTERA_DTLS13_CIPHERSUITES	TeraDtls13Ciphers	[dtls] ciphersuites	-
XTERA_EXIT_ON_DISCONNECT	TeraExitOnDisconnect	[tera] exit-on-disconnect	-
XTERA_ALLOW_SINGLE_CLIENT_ONLY	AllowSingleClientOnly	[tera] allow-single-client-only	-
TERA_AUDIO_CODEC	TeraAudioCodec	[tera] audio-codec	-
TERA_AUDIO_CHANNELS	TeraAudioChannels	[tera] audio-channels	-
TERA_AUDIO_SAMPLE_RATE	TeraAudioSampleRate	[tera] audio-sample-rate	-
TERA_AUDIO_BITRATE	TeraAudioBitrate	[tera] audio-bitrate	-
TERA_AUDIO_VBR	TeraAudioVBR	[tera] audio-vbr	-
TERA_AUDIO_REC_SWITCH	TeraAudioRecSwitch	[tera] audio-rec-switch	-
QXL_NUM_HEADS	NumHeads	-	-

Переменная окружения	Параметр файла 30-teraqxl.xorg.conf	Параметр файла x11tera.conf	Примечание
XTERA_ZLIB_GLZ_WAN_COMPRESSION	TeraZlibGlzWanCompression	[tera] zlib-glz-compression	-
XTERA_JPEG_WAN_COMPRESSION	TeraJpegWanCompression	[tera] jpeg-compression	-
XTERA_IMAGE_COMPRESSION	TeraImageCompression	[tera] image-compression	-
XTERA_DEFERRED_FPS	TeraDeferredFPS	-	-
IMAGE_DIFF_BLOCK_SIZE	TeraImageDiffBlockSize	-	-
XTERA_STREAMING_VIDEO	TeraStreamingVideo	[tera] streaming-video	-
XTERA_VIDEO_CODECS	TeraVideoCodecs	[tera] codecs	-
QXL_ENABLE_IMAGE_CACHE	EnableImageCache	-	-
QXL_ENABLE_FALLBACK_CACHE	EnableFallbackCache	-	-
QXL_ENABLE_SURFACES	EnableSurfaces	-	-
QXL_SURFACE_BUFFER_SIZE	SurfaceBufferSize	-	-
QXL_COMMAND_BUFFER_SIZE	CommandBufferSize	-	-
QXL_FRAME_BUFFER_SIZE	FrameBufferSize	-	-
XTERA_VDAGENT_ENABLED	TeraVdagentEnabled	-	-
XTERA_VDAGENT_VIRTIO_PATH	TeraVdagentVirtioPath	[tera] virtio-path	-
XTERA_VDAGENT_UINPUT_PATH	TeraVdagentUinputPath	[tera] uinput-path	-
XTERA_VDAGENT_UID	TeraVdagentUid	-	-
XTERA_VDAGENT_GID	TeraVdagentGid	-	-
XTERA_AGENT_MOUSE	TeraAgentMouse	-	-
XTERA_DISABLE_COPY_PASTE	TeraDisableCopyPaste	-	-
XTERA_DISABLE_KEYBOARD_LOCKS	TeraDisableKeyboardLocks	-	-

Переменная окружения	Параметр файла 30-teraqxl.xorg.conf	Параметр файла x11tera.conf	Примечание
XTERA_DISABLE_TIME_SYNC	TeraDisableTimeSync	-	-
XTERA_DISABLE_TIMEZONE_SYNC	TeraDisableTimezoneSync	-	-
XTERA_DISABLE_KEYBOARD_LAYOUT	TeraDisableKeyboardLayout	[tera] disable-keyboard-layout	-
TDSK_DEBUG	-	-	Включает отладочный уровень логирования (см. подраздел **Отладочный режим**)
SPICE_DEBUG_ALLOW_MC_ENV	-	-	Разрешает одновременное подключение множества пользователей
TERA_VERBOSE_GATEWAY_INFO	-	-	Включает подробное логирование взаимодействия со Шлюзом (Termidesk Connect) при коммутации UDP-каналов

Блокирование локального доступа при подключении к физической машине

Для приема входящих подключений и настройки TERA для физических машин используется ПО x11tera.

По умолчанию после установки TERA на физическую машину:

- будет доступно удаленное подключение пользователя к этой физической машине;
- будет доступно локальное подключение пользователя к этой физической машине.

Для ограничения локального доступа при удаленном подключении пользователя нужно:

- выбрать и настроить режим запуска ПО x11tera (см. подраздел **Режимы запуска ПО x11tera**);
- настроить блокирование периферийных устройств через исполняемый файл /usr/bin/x11tera_on_lock (см. подраздел **Исполняемый файл x11tera_on_lock**);
- настроить разблокирование устройств через исполняемый файл /usr/bin/x11tera_on_unlock (см. подраздел **Исполняемый файл x11tera_on_unlock**).

Настройки работы ПО x11tera по умолчанию, если к физической машине подключился удаленный пользователь:

- интерфейсы ввода (клавиатура, тачпад, мышь или другие) отключены;
- вывод информации на подключенные к физической машине мониторы блокируется;
- графическое окружение ОС будет заблокировано для всех пользователей (как локального, так и удаленного), если удаленный пользователь нештатно отключился или не авторизовался в ОС.

Настройки работы ПО x11tera по умолчанию, если удаленный пользователь отключился от физической машины (штатно или нештатно):

- все устройства ввода разблокированы;

- расположение экранов восстановлено;
- физическая машина переходит в режим ввода пароля для локального входа пользователя в ОС.

В случае блокирования экрана физической машины (например, утилитой `screensaver` или иным способом) во время работы подключенного пользователя, будет открыто стандартное окно ввода пароля. Пользователю потребуется:

- ввести пароль;
- повторно удаленно подключиться к физической машине и пройти этап автоматической разблокировки рабочего стола.

В этом случае на физической машине на некоторое время разблокируются монитор, клавиатуры, мыши в ожидании нового подключения.

Разблокирование физической машины с помощью интерфейсов ввода

По умолчанию ПО x11tera запускается, блокируя ввод с клавиатуры, управление мышью, а также отключая вывод информации на монитор до тех пор, пока не отключится удаленный пользователь.

Для восстановления локального доступа к физической машине (и принудительного отключения удаленного пользователя) могут использоваться следующие действия:

- перемещение мыши влево и вправо с большой амплитудой в течении не менее трех секунд;
- нажатие пяти раз подряд одной из следующих клавиш на клавиатуре в интервале до пяти секунд:
  - **<Esc>**;
  - **<Fn>**;
  - **<Ctrl>** (левая или правая клавиши);
  - **<Alt>** (левая или правая клавиши);
- нажатие пяти раз подряд левой кнопкой мыши в интервале до пяти секунд.

При выполнении любого из перечисленных действий:

- удаленный пользователь будет отключен;
- удаленное управление физической машиной будет прекращено;
- работоспособность мониторов и интерфейсов ввода (клавиатуры и указательных устройств) будет восстановлено. Видимость изображения на мониторах будет восстановлена.;
- сессия локального пользователя будет заблокирована, продолжение работы на физической машине будет возможно только после ввода пароля пользователя.

Настройка процедуры разблокирования периферийных устройств при отключении пользователя приведена в подразделе **Исполняемый файл** `x11tera_on_unlock`.

Режимы запуска ПО x11tera

Режимы запуска ПО x11tera для физической машины

Общие сведения о режимах запуска ПО x11tera

ПО x11tera поддерживает работу в следующих режимах:

- режим службы. Переключение на режим службы может понадобиться для решения нештатных ситуаций;
- режим приложения с автоматическим запуском графического окружения (включен по умолчанию после установки).

Запуск ПО x11tera в режиме службы

Для переключения ПО x11tera на режим службы следует выполнить команды:

```
sudo systemctl enable x11tera.service
sudo systemctl restart x11tera.service
```

При включенном запуске в режиме службы автоматически отключается работа ПО x11tera в режиме приложения. При этом не будет выполняться автоматическое блокирование графического окружения, если настроена автоматическая авторизация пользователя в ОС.

Запуск ПО x11tera в режиме приложения

ПО x11tera автоматически запускается и начинает работать при выполнении одного из условий:

- если включена автоматическая авторизация локального пользователя в ОС. В этом случае графическое окружение будет автоматически заблокировано сразу же после успешной авторизации;
- если пользователь вручную выполнил локальную авторизацию в ОС. В этом случае графическое окружение не будет заблокировано после успешной авторизации.

Для переключения ПО x11tera на режим приложения следует выполнить:

- включить автоматический вход локального пользователя, следуя инструкции в справочном центре Astra Linux: https://wiki.astralinux.ru/pages/viewpage.action?pageId=3276870;
- выполнить команды:

```
sudo systemctl disable x11tera.service
sudo systemctl stop x11tera.service
```

Для начала работы ПО x11tera требуется перезагрузка физической машины. Также можно выполнить перезапуск ПО x11tera без перезагрузки, для этого:

- предварительно сохранить файлы и работу с ПО, т.к. далее все запущенные графические приложения будут закрыты;
- выполнить перезапуск службы графического менеджера:

```
sudo systemctl restart display-manager
```

- выполнить повторную авторизацию в ОС.

Аутентификация подключений к TERA в ОС Linux

Механизм работы при аутентификации сетевого подключения:

- TCP-соединение устанавливается с TERA-сервером;
- TERA-сервер инициирует обмен, чтобы убедиться, что сторона, подключившаяся к сокету, имеет право получать графическую сессию;
- аутентификация подключения: проверка учетных данных соединения (не путать с логином и паролем пользователя для графической сессии);
- результат подключения:
  - либо соединение устанавливается и TERA-сервер начинает трансляцию изображения, если аутентификация пройдена успешно;
  - либо соединение разрывается, если аутентификация пройдена неуспешно.

> Описание не затрагивает аутентификацию пользователя в ОС. Инициализация и запуск графической сессии, взаимодействие с PAM или Kerberos, взаимодействие с ПО Termidesk Viewer выполняется «Агентом виртуального рабочего места».

Протокол TERA поддерживает несколько методов аутентификации подключения клиентской части (TERA-клиента) к серверной (TERA-серверу):

> Метод аутентификации - механизм проверки аутентификационных данных при подключении к TERA-серверу. Он выбирается клиентской частью пользовательского ПО (ПО Termidesk Viewer) из набора методов, сконфигурированных на TERA-сервере.
>
> Методы аутентификации по паролю и через поставщика учетных данных могут быть включены одновременно (SASL-аутентификация при этом должна быть отключена). В этом случае TERA будет ожидать либо предъявления пароля, либо передачи аутентификационных данных.

- без аутентификации;
- SASL-аутентификация. При включении SASL-аутентификации в настройках TERA она будет выбрана принудительно для подключения пользовательским ПО, независимо от настроек других методов:
  - клиентская часть пользовательского ПО (ПО Termidesk Viewer) будет обязана пройти аутентификацию;
  - если клиентская часть пользовательского ПО (ПО Termidesk Viewer) не поддерживает этот метод или он не сконфигурирован в настройках протокола доставки в «Портале администратора» Termidesk VDI, то пользователь не сможет подключиться;
- поставщик учетных данных (Credentials Provider, в версии 6.1 только для ОС Microsoft Windows);
- пароль. Относится к простой проверке подключения к TERA-серверу:
  - указывается в настройках протокола доставки в «Портале администратора» Termidesk VDI, если используется;
  - не вводится пользователем при подключении, поскольку передается в параметрах подключения компонентом «Клиент» автоматически.

Использование методов аутентификации настраивается через конфигурационные файлы (см. подразделы **Конфигурационный файл** `x11tera.conf` и **Конфигурационный файл** `30-teraqxl.xorg.conf`):

- без аутентификации: включается при установке `TeraDisableTicketing` = `True`;
- SASL-аутентификация: включается при установке `TeraSasl` = `True`. Требуется дополнительная настройка узла для SASL-аутентификации (см. подраздел **Kerberos-аутентификация**)
- поставщик учетных данных: включается при установке `TeraCredentialsAuth` = `True`, при этом автоматически включает использование билетов аутентификации (`TeraDisableTicketing` = `False`, даже если он был `True`);
- пароль: включается при установке `TeraPassword` в непустое значение, автоматически включает использование билетов аутентификации (`TeraDisableTicketing` = `False`, даже если он был `True`).

Если все методы аутентификации будут включены одновременно, то приоритет их использования будет следующим (от более приоритетного к менее приоритетному):

- SASL-аутентификация;
- поставщик учетных данных;
- пароль;
- без аутентификации.

Особенности функционирования:

- отключение всех методов и установка `TeraDisableTicketing` = `True` приведет к разрешению подключения к TERA без аутентификации;
- включение либо пароля, либо поставщика учетных данных приведет к включению использования билетов аутентификации;
- все методы аутентификации, кроме SASL, имеют встроенную процедуру безопасного обмена учетными данными: данные не передаются в открытом виде даже при условии, что протокол SSL/TLS не включен и не используется. Использование SASL потребует настройку и задействование протокола SSL/TLS, в противном случае подключение пользователя через ПО Termidesk Viewer не произойдет.

TERA не допускает передачу логина и пароля в открытом виде, поэтому возникает потребность в обязательном использовании SSL-режима в канале связи.

SASL-аутентификация в TERA

Настройка SASL-аутентификации

Информация о работе аутентификации в TERA приведена в подразделе **Аутентификация подключений к TERA в ОС Linux**.

Для основной настройки SASL-аутентификации следует:

- проверить наличие установленных пакетов `sasl2-bin`, `libsasl2-2`, `libsasl2-modules`, `libsasl2-modules-gssapi-mit`, `gssproxy`. Если пакеты не найдены, то установить их:

```
sudo apt install sasl2-bin libsasl2-2 libsasl2-modules libsasl2-modules-gssapi-mit
gssproxy
```

- выполнить настройку службы `saslauthd`:

- убедиться, что в файле /etc/default/saslauthd установлены параметры:

```
MECHANISMS="pam"
START=yes
OPTIONS="-r -c -m /var/run/saslauthd"
```

Настройка приведена с учетом использования формата имени пользователя в виде UPN (с доменной частью - это предпочтительный формат в современных системах): ключ -r в секции OPTIONS объединяет домен (realm) с логином пользователя через разделитель - @. Например, при значении логина - user, а домена - local будет передано: user@local.

Если используется имя пользователя в формате sAMAccountName (без доменной части), то:

- ключ -r в секции OPTIONS использовать не нужно;
- файл конфигурации службы sssd (/etc/sssd/conf.d/*.conf) в секции описания домена (например, domain/local.domain) должен содержать:

```
use_fully_qualified_names = False
```

- если в конфигурационном файле /etc/sasl2/host.conf в секции mech_list есть plain, то убедиться, что пользователь fly-dm добавлен в группу sasl. Если пользователя в группе нет, то добавить его:

```
sudo usermod -a -G sasl fly-dm
```

- активировать и запустить службы sssd, saslauthd, gssproxy:

```
sudo systemctl enable sssd saslauthd gssproxy
sudo systemctl start sssd saslauthd gssproxy
```

- в конфигурационном файле /etc/X11/xorg.conf.d/30-teraqxl.xorg.conf задать параметру TeraSasl значение True;
- проверить корректность конфигурационного файла /etc/sasl2/host.conf. Пример файла по умолчанию после установки:

```
mech_list: plain
log_level: 7
pwcheck_method: saslauthd
auxprop_plugin: pam
```

После завершения настройки рекомендуется перезагрузить узел TERA.

Для дополнительной настройки SASL-аутентификации в режиме Kerberos следует (см. подраздел **Kerberos-аутентификация**):

- настроить прокси-сервис `gssproxy` для протокола GSSAPI:
  - создать файл конфигурации `/etc/gssproxy/30-xorg-sasl.conf`:

    ```
    sudo touch /etc/gssproxy/30-xorg-sasl.conf
    ```

  - внести в созданный файл следующую конфигурацию:

    ```
    [service/xorg-sasl]
    mechs = krb5
    cred_store = keytab:/etc/krb5.keytab
    cred_usage = accept
    euid = 0
    allow_any_uid = yes
    program = /usr/lib/xorg/Xorg
    ```

  - в конфигурационном файле `/etc/X11/xorg.conf.d/30-teraqxl.xorg.conf` задать параметру `TeraGssUseProxy` значение `True`;
- привести конфигурационный файл `/etc/sasl2/host.conf` к виду:

```
mech_list: gssapi
log_level: 7
```

- при изменении файла `/etc/sasl2/host.conf` нужно перезапустить службу `display-manager`:

```
sudo systemctl restart display-manager
```

- выполнить настройку службы `SSSD`:
  - убедиться, что используется имя пользователя в формате UPN и в файле конфигурации службы `sssd` (`/etc/sssd/conf.d/*.conf`) в секции описания домена (например, `domain/local.domain`) присутствует строка:

    ```
    use_fully_qualified_names = True
    ```

  - перезапустить службы `sssd`, `saslauthd`, `gssproxy`:

    ```
    sudo systemctl restart sssd saslauthd gssproxy
    ```

SASL-аутентификация может быть настроена на одновременную работу как в режиме авторизации по логину и паролю, так и в Kerberos. Для этого нужно объединить настройки необходимых параметров в один файл `/etc/sasl2/host.conf`:

```
mech_list: plain gssapi
log_level: 7
pwcheck_method: saslauthd
auxprop_plugin: pam
```

Необходимо убедиться, что для конфигурационных файлов службы `sssd` (`/etc/sssd/conf.d/*.conf`) установлены корректные права доступа. При необходимости следует изменить права на файлы:

```
sudo chmod 0600 <файл_конфигурации_sssd>
```

На ОС Astra Linux Special Edition в зависимости от версии права доступа на файлы могут отличаться, поэтому следует руководствоваться документацией ОС.

Kerberos-аутентификация в TERA

Настройка Kerberos-аутентификации

Kerberos-аутентификация для TERA возможна, если:

- для доступа к РМ используется домен аутентификации Termidesk VDI, поддерживающий функционал Kerberos и настроенный на его использование;
- РМ и пользовательская рабочая станция введены в домен;
- в DNS-зоне домена присутствуют корректные A (или AAAA) и PTR-записи узлов - членов домена;
- выполнена настройка TERA, как приведено ниже.

Для основной настройки Kerberos-аутентификации следует:

- проверить наличие установленных пакетов `krb5-user`, `krb5-config`, `libpam-sss`. Если пакеты не найдены, то установить их:

При установке потребуется указать параметры центра распространения ключей (KDC). Пример:

- «Realm»: `EXAMPLE.COM`;
- «KDC-сервер»: `kdc.example.com`;
- «Административный сервер»: `server.example.com`.

```
sudo apt install krb5-user krb5-config libpam-sss
```

- проверить соответствие конфигурационного файла `/etc/krb5.conf` настроенной инфраструктуре в организации;
- если Kerberos-аутентификация будет использоваться в сценарии единого входа в доменную гостевую ОС, то убедиться, что выполнены настройки гостевой ОС (см. подраздел **Технология единого входа** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»).

Для дополнительной настройки Kerberos-аутентификации на уровне сети следует:

- убедиться, что выполнена настройка SASL-аутентификации (см. подраздел **SASL-аутентификация**);
- убедиться, что конфигурационный файл `/etc/sasl2/host.conf` приведен к виду:

```
mech_list: gssapi
log_level: 7
```

После выполнения настройки убедиться, что в модуле `PAM` используется профиль «SSS authentication» и не используется «Kerberos authentication» (см. рисунок Настройка профилей PAM), для этого выполнить:

```
sudo pam-auth-update
```

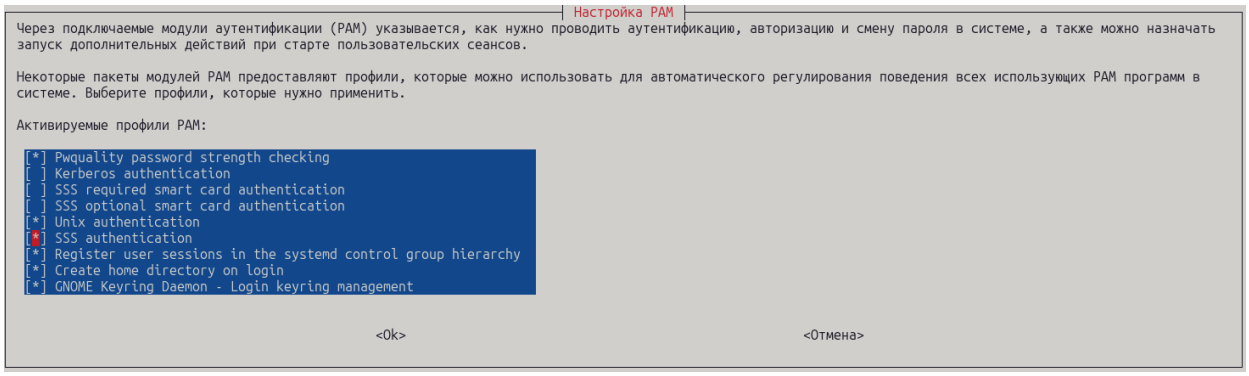


Рисунок 147. Настройка профилей PAM

Разделение каналов и их приоритизация в TERA

Протокол TERA поддерживает разделение каналов на несколько сетевых потоков и их приоритизацию на основе приоритетов сокетов для управления очередями пакетов. Управление функционалом осуществляется из «Портала администратора» Termidesk VDI (см. подраздел **Группы каналов протокола TERA**).

Управление очередями пакетов на уровне ОС полезно в случаях:

- низкой пропускной способности сетевых интерфейсов;
- высокой загрузки сетевых интерфейсов.

Функционал приоритизации сокетов реализован для ОС Linux (в ОС Microsoft Windows и ОС macOS нет аналога Linux-опции `SO_PRIORITY`). Приоритет сокета позволяет TERA задать приоритет для всех пакетов, отправляемых через конкретный сокет, а ядро ОС использует это значение для управления сетевыми очередями и маршрутизации трафика.

Изменение сокетов недоступно.

Сопоставление приоритетов канала TERA приоритетам сокетов приведено в таблице (см. таблицу Сопоставление приоритетов канала TERA приоритетам сокетов).

Пример влияния приоритета на обработку трафика:

- пусть в «Портале администратора» установлены следующие приоритеты:
  - канал «webdav» - «Real-Time stream» (приоритет «3»);
  - канал «playback» - «Background» (приоритет «0»);
  - канал «display» - «Background» (приоритет «0»);
- тогда:
  - при воспроизведении видео не будет наблюдаться задержек;
  - однако если дополнительно начать копировать файл в перенаправленный каталог, то при воспроизведении видео появятся задержки.

Эти задержки будут более значительными, чем при установке параметров следующим образом:

- канал «webdav» - «Real-Time stream» (приоритет «3»);
- канал «playback» - «Background» (приоритет «3»);
- канал «display» - «Background» (приоритет «3»).

Эти задержки будут минимальными при установке параметров следующим образом:

- канал «webdav» - «Real-Time stream» (приоритет «0»);
- канал «playback» - «Background» (приоритет «3»);
- канал «display» - «Background» (приоритет «3»).

Алгоритм обработки конфигурации:

- администратор через «Портал администратора» вносит изменения в конфигурацию приоритетов каналов;
- пользователь подключается через «Клиент» к РМ по протоколу TERA;
- «Клиент» получает конфигурацию приоритетов каналов от «Универсального диспетчера» («Портала администратора») и передает ее в ПО Termidesk Viewer;
- ПО Termidesk Viewer отправляет полученную конфигурацию в TERA-сервер, конфигурация применяется.

Таблица 264. Сопоставление приоритетов канала TERA приоритетам сокетов

Номер приоритета канала TERA	Номер приоритета сокета
3	6
2	4 - 5
1	2 - 3
0`	0 - 1

Переключение протоколов TCP и UDP в TERA

TERA поддерживает динамическое переключение режима работы каналов:

- из протокола TCP в UDP;
- обратное переключение из UDP в TCP при превышении порога пропущенных кадров.

Помимо переключения для указанных каналов поддерживается защищенный режим работы (протоколы: TLS для TCP, DTLS для UDP). Управление переключением и защитой соединений производится через конфигурационные файлы `30-teraqxl.xorg.conf` (см. подраздел **Конфигурационный файл `30-teraqxl.xorg.conf`**) или `/etc/xdg/x11tera/x11tera.conf` (см. подраздел **Конфигурационный файл `x11tera.conf`**).

Функционал позволяет адаптировать работу каналов TERA к текущим сетевым условиям (в том числе, качеству сети) и задачам (например, переход на UDP медиапотоки для минимизации задержки и потерь).

Процесс переключения всегда инициируется клиентским приложением (ПО Termidesk Viewer), TERA-сервер либо обеспечивает переключение, либо отказывает в нем. Переключение режимов выполняется для каждого канала TERA индивидуально.

Гарантированная последовательность приема сообщений при переключении с TCP на UDP обеспечивается следующим алгоритмом:

- при запросе на переключение в UDP пересылка управляющих сообщений продолжается в TCP-канале;
- сведения о подключении передаются TERA-сервером также в TCP-канале;
- клиентское приложение, получив параметры подключения, начинает процедуру, называемую «проталкиванием» UDP-датаграмм (NAT hole punching) для обеспечения работы при использовании NAT. Ответные UDP-датаграммы TERA-сервер отправляет, используя адрес отправителя, полученный от клиентского приложения. UDP-канал на этом еще не работает;
- решение о функционировании UDP-канала принимается клиентским приложением после получения ответных UDP-датаграмм от TERA-сервера. Но на этом этапе продолжается использование TCP-канала, т.к. переключение еще не выполнено;
- после получения ответных UDP-датаграмм от TERA-сервера клиентское приложение начинает процедуру пересылки накопленных данных (forwarding) для досылки по UDP всех данных из буфера TCP-канала. После этого клиентское приложение переходит к использованию UDP для всех последующих сообщений. При этом:
  - данные, переданные по TCP до момента переключения, уже упорядочены;
  - данные, переданные по UDP в процессе пересылки, нумеруются или снабжаются последовательными метками (имплементация зависит от версии протокола);
  - для разделения данных используется маркер `forwarding_notify`: все, что передавалось до него по TCP/UDP-каналам, считается доставленным. Все, что после, передается по UDP-каналу с собственной нумерацией;
- TERA-сервер, получив `forwarding_notify`, завершает процедуру пересылки со своей стороны и переходит в режим работы по UDP. С этого момента стороны работают только по UDP.

Если клиентское приложение подключается к TERA-серверу, не поддерживающему протокол UDP (или его поддержка была отключена на TERA-сервере), то оно не сможет начать взаимодействие по UDP.

TCP-канал не закрывается при переключении в UDP, т.к. он сохраняется для критически важных данных (например, нажатие клавиш на клавиатуре передаются в TCP-канале, а перемещение мыши в UDP-канале).

В TERA предусмотрен останов попыток переключения в UDP, если клиентским приложением обнаружены неудачные попытки (когда TERA-сервер присылает не «строгий» ответ) через переменные `TERA_UDP_FAILURE_TIMEOUT` и `TERA_UDP_QUALITY_TIMEOUT`. Переменные задаются в

> ОС пользовательской рабочей станции, откуда происходит подключение через клиентское приложение (см. подраздел **Интерфейс командной строки ПО Termidesk Viewer** документа СЛЕТ.10001-01 92 01 «Руководство пользователя. Настройка и эксплуатация компонента «Клиент»).

Защита TCP-подключения с использованием SSL/TLS

Базовая настройка

TERA поддерживает использование SSL/TLS для шифрования трафика между TERA-клиентом и TERA-сервером. Для работы SSL/TLS требуется выполнение условий:

- на узле TERA-сервера:
  - должен быть загружен серверный сертификат и закрытый ключ к нему;
  - поскольку в ОС Linux любой доступ к файлу серверного сертификата/ключа должен быть запрещен, то ограничить права доступа:

    ```
    sudo chmod 400 <путь_к_файлу>
    ```

  - закрытый ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению (без пароля), например:

    ```
    openssl rsa -in <путь_к_файлу_ключа.key> -out
    <путь_к_преобразованному_ключу.key>
    ```

  - (опционально) могут быть загружены промежуточные сертификаты, которые составляют цепочку доверия с существующими корневыми. Их содержимое можно перечислить в файле `ca-cert.pem`;
- на узле TERA-клиента (пользовательской рабочей станции):
  - должен быть загружен и добавлен в доверенные корневой сертификат УЦ, которым подписан серверный сертификат. Если используется самоподписанный серверный сертификат, то в доверенные должен добавляться он.

TERA-сервер будет принимать как обычные, так и SSL-подключения (на отдельном TCP-порте) и будет согласовывать использование SSL с каждым клиентом. Режим подключения (защищенный SSL/TLS или незащищенный) обусловлен настройками протокола доставки.

Конфигурация ПО tera-keyagent

Работа с чувствительной информацией (сертификатами и закрытыми ключами) выполняется ПО tera-keyagent (службой `tera-keyagent.service`), которое:

- безопасно хранит и предоставляет доступ к SSL-ключам;
- решает проблему безопасности ключей, когда TERA-сервер вынужден работать в режиме непривилегированного пользователя. ПО tera-keyagent надежно скрывает SSL-ключи в файловой системе от непривилегированного пользователя и предоставляет их по запросу только аутентифицированным процессам.

Надежность сокрытия информации обеспечивается:

- белым списком процессов: ПО tera-keyagent отдает ключи строго только двум процессам - графическому серверу Xorg (в случае использования ВМ) и GПО x11tera (в случае использования физической машины):

  - /usr/lib/xorg/Xorg;
  - /usr/bin/Xorg;
  - /usr/libexec/Xorg;
  - /usr/bin/x11tera;
- требованием существования абсолютного реального пути к исполняемому файлу, запросившему доступ;
- требованием принадлежности исполняемого файла суперпользователю (root);
- получением содержимого SSL-ключей через защищенный механизм systemd. При этом изменить настройки расположения SSL-ключей может только суперпользователь.

В более ранних версиях Termidesk расположение SSL-ключей указывалось в в конфигурационных файлах /etc/X11/xorg.conf.d/30-teraqxl.xorg.conf и /etc/xdg/x11tera/x11tera.conf. Начиная с Termidesk версии 7.0 и появления ПО tera-keyagent расположение ключей передается в сервисном файле /usr/lib/systemd/system/tera-keyagent.service (см. подраздел **Параметры запуска службы tera-keyagent**).

При смене имени узла сертификаты необходимо перевыпустить:

- если используется ВМ:

```
sudo /var/lib/dpkg/info/tera-qxl.preinst cert-create
```

- если используется физическая машина:

```
sudo /var/lib/dpkg/info/tera-x11.preinst cert-create
```

TERA. НАСТРОЙКИ В ОС MICROSOFT WINDOWS

Конфигурационные файлы TERA в ОС Microsoft Windows

Общие сведения о параметрах в ОС Microsoft Windows

Для настройки и функционирования TERA используются объекты, перечисленные в таблице (см. таблицу Список файлов TERA для ОС Microsoft Windows).

Таблица 265. Список файлов TERA для ОС Microsoft Windows

Объект	Применимость	Описание
Служба TERA Server	ВМ	Служба, управляющая функционированием TERA
Служба TERA Agent	ВМ	Служба, управляющая изменением графического окружения
Процесс tera-service	ВМ	Исполняемый файл службы TERA Server
Процесс Termidesk Remote Access Server	ВМ	Исполняемый файл TERA
Процесс TERA vdagent	ВМ	Исполняемый файл ПО TERA vdagent. Предназначен для работы передачи позиции мыши, буфера обмена, файлов, многомониторного режима

Объект	Применимость	Описание
Процесс `TERA vdservice`	ВМ	Исполняемый файл службы `TERA Agent`
Каталог `C:\Program Files\UVEON\Termidesk TERA`	ВМ	Каталог по умолчанию для установки TERA
Каталог `C:\Program Files\UVEON\Termidesk TERA\certs`	ВМ	Каталог по умолчанию для размещения серверных сертификатов TERA, используемых для безопасной аутентификации по протоколу TLS. По умолчанию после установки используются самоподписанные сертификаты
Каталог `C:\Program Files\UVEON\Termidesk TERA\Driver`	ВМ	Каталог по умолчанию для размещения драйвера видеоадаптера `TERAIddDriver`, обеспечивающего работу многомониторного режима. В версии 6.1 доступен только один монитор при создании сессии. Для просмотра наличия видеоадаптера следует: • перейти в «Диспетчер устройств» ОС; • активировать просмотр скрытых устройств, выбрав во вкладке «Вид» пункт «Показать скрытые устройства»; • в области просмотра устройств раскрыть список «Видеоадаптеры» и убедиться, что отображен «TERA IDD Adapter» Видеоадаптер «TERA IDD Adapter» появляется при подключении пользователя по протоколу TERA
Каталог реестра `HKEY_LOCAL_MACHINE\SOFTWARE\UVEON\Termidesk TERA`	ВМ	Каталог реестра для настройки TERA
Каталог реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\TERA`	ВМ	Каталог реестра для регистрации провайдера TERA Менять параметры не рекомендуется.

Каталог реестра `HKEY_LOCAL_MACHINE\SOFTWARE\UVEON\Termidesk TERA`

Каталог реестра `HKEY_LOCAL_MACHINE\SOFTWARE\UVEON\Termidesk TERA` используется для настройки TERA в ОС Microsoft Windows. Также поддерживается настройка параметров через переменные окружения с аналогичным именем.

Для применения настроек необходимо:

- перезагрузить службу `TERA Server`;
- выполнить переподключение пользователя к РМ по протоколу TERA.

Перечень параметров, задающихся через реестр, приведен в таблице (см. таблицу Список параметров TERA в реестре ОС Microsoft Windows).

Таблица 266. Список параметров TERA в реестре ОС Microsoft Windows

Параметр	Значение по умолчанию	Описание
Сетевые настройки		
TERA_ADDRESS	0.0.0.0	Адрес прослушивания входящих подключений
TERA_PORT	5900	Порт прослушивания входящих подключений (используется как для стандартного подключения, так и для SSL/TLS)
TERA_USE_IPV4	true	Управление прослушиванием входящих подключений на IPv4-адресах. Возможные значения: • true - прослушивать IPv4-адреса; • false - прослушивать IPv6-адреса
Настройки перенаправления портов и каналов ввода/вывода		
TERA_PORT_COUNT	0	Управление количеством последовательных портов, которые используются для обмена информацией между TERA-сервером и TERA-клиентом. Диапазон значений: от 0 до 4
Настройки журналирования		
TERA_DEBUG	false	Управление использованием отладочного режима. Возможные значения: • true - использовать отладочный режим при журналировании событий; • false - не использовать отладочный режим при журналировании событий
TERA_LOG_FILENAME	C:/ProgramData/UVEON/logs/Termidesk TERA/tera-server.log	Задание пути к файлу журнала TERA
Настройки завершения работы TERA		
TERA_EXIT_ON_DISCONNECT	false	Управление режимом завершения работы TERA при отключении пользователя. Возможные значения: • true - после отключения пользователя работа TERA будет завершена; • false - после отключения пользователя TERA продолжит работать
Настройки пропускной способности протокола		
TERA_FPS	10	Задание количества кадров в секунду

Параметр	Значение по умолчанию	Описание
TERA_IMAGE_COMPRESSION	auto_glz	Управление алгоритмом сжатия изображения. Возможные значения: • off - отключить алгоритм сжатия данных; • auto_glz - автоматическое управление алгоритмом сжатия glz; • quic - использование алгоритма сжатия данных quick; • glz - использование алгоритма сжатия данных glz; • lz - использование алгоритма сжатия данных lz
TERA_JPEG_WAN_COMPRESSION	always	Управление сжатием изображения. Возможные значения: • auto - автоматическое управление сжатием изображения в зависимости от состояния сети; • never - отключение сжатия данных. Параметр может привести к увеличению объема передаваемой информации и обеспечить максимальное качество изображения; • always - включение сжатия данных. Параметр может привести к уменьшению качества изображения и обеспечить высокую скорость передачи изображения в условиях ограниченной пропускной способности сети
TERA_ZLIB_WAN_COMPRESSION	always	Управление сжатием данных для оптимизации пропускной способности сети. Возможные значения: • auto - автоматическое управление сжатием данных в зависимости от состояния сети; • never - отключение сжатия данных. Параметр может привести к увеличению объема передаваемой информации и обеспечить минимальную задержку при передаче данных; • always - включение сжатия данных. Параметр может привести к уменьшению объема передаваемой информации и обеспечить высокую скорость передачи данных в условиях ограниченной пропускной способности сети
Настройки многомониторной конфигурации		
TERA_NUM_MONITORS	1	Управление количеством виртуальных мониторов, доступных для гостевой ОС
Настройки SSL/TLS		

Параметр	Значение по умолчанию	Описание
TERA_USE_TLS	false	Управление режимом использования защищенного соединения SSL/TLS. Возможные значения: • true - использовать защищенное соединение SSL/TLS; • false - не использовать защищенное соединение SSL/TLS
TERA_TLS_CIPHERS	Не задано	Список алгоритмов преобразования для использования в соединении SSL/TLS. По умолчанию не используется. Список алгоритмов приведен после таблицы
TERA_CA_CERT_FILE	Не задано	Полный путь к файлу корневого сертификата для SSL/TLS. По умолчанию не используется. Если заданы параметры TERA_USE_TLS и TERA_X509_DIR, а параметр TERA_CA_CERT_FILE пустой, то используется файл ca-cert.pem из каталога, заданного в TERA_X509_DIR
TERA_DH_FILE	Не задано	Полный путь к файлу с ключами Диффи-Хеллмана для SSL/TLS. По умолчанию не используется
TERA_X509_CERT_FILE	Не задано	Полный путь к файлу серверного сертификата SSL/TLS. По умолчанию не используется. Если заданы параметры TERA_USE_TLS и TERA_X509_DIR, а параметр TERA_X509_CERT_FILE пустой, то используется файл server-cert.pem из каталога, заданного в TERA_X509_DIR
TERA_X509_DIR	C:/Program Files/UVEON/Termidesk TERA/certs	Путь к каталогу, в котором размещаются сертификаты и закрытые ключи, используемые для защищенного соединения SSL/TLS. По умолчанию самоподписанные сертификаты и закрытые ключи к ним появляются в каталоге C:\Program Files\UVEON\Termidesk TERA\certs автоматически после установки TERA
TERA_X509_KEY_FILE	Не задано	Полный путь к файлу закрытого ключа для SSL/TLS. По умолчанию не используется. Если заданы параметры TERA_USE_TLS и TERA_X509_DIR, а параметр TERA_X509_KEY_FILE пустой, то используется файл server-key.pem из каталога, заданного в TERA_X509_DIR
TERA_X509_KEY_PASSWORD	Не задано	Пароль для доступа к закрытому ключу для SSL/TLS. По умолчанию не используется
Настройки перенаправления веб-камеры		

Параметр	Значение по умолчанию	Описание
TERA_WEBCAM_CHANNEL_ENABLE	true	Управление режимом использования канала веб-камеры. Возможные значения: • true - включить канал. Пользователь сможет выполнить перенаправление веб-камеры в гостевую ОС с установленным TERA через ПО Termidesk Viewer; • false - отключить канал. Пользователь не сможет выполнять перенаправление веб-камеры в гостевую ОС с установленным TERA
Настройки перенаправления каталогов		
TERA_WEBDAV_CHANNEL_ENABLE	true	Управление режимом использования канала для перенаправления каталогов. Возможные значения: • true - включить канал. Пользователь сможет выполнить перенаправление каталога в гостевую ОС с установленным TERA через ПО Termidesk Viewer; • false - отключить канал. Пользователь не сможет выполнять перенаправление каталога в гостевую ОС с установленным TERA
Настройки перенаправления клавиатурных модификаторов		
TERA_KEYBOARD_LAYOUT_SYNC	true	Управление перенаправлением раскладки клавиатуры между гостевой ОС и пользовательской рабочей станцией. Возможные значения: • true - разрешить перенаправление раскладки клавиатуры; • false - запретить перенаправление раскладки клавиатуры
TERA_KEYBOARD_LOCKS_SYNC	true	Управление перенаправлением клавиатурных модификаторов между гостевой ОС и пользовательской рабочей станцией. Возможные значения: • true - разрешить перенаправление клавиатурных модификаторов; • false - запретить перенаправление клавиатурных модификаторов
Настройки аутентификации		

Параметр	Значение по умолчанию	Описание
TERA_CRED_PROVIDER	true	Управление режимом использования поставщика учетных данных При наличии активного подключения ПО Termidesk Viewer второе подключение произойдет в ту же сессию. Возможные значения: • true - разрешить использование поставщика учетных данных; • false - запретить использование поставщика учетных данных
TERA_DISABLE_TICKETING	false	Управление механизмом парольной аутентификации при подключении к гостевой ОС. Возможные значения: • true - разрешить подключение без предоставления пароля; • false - для подключения будет использоваться пароль, указанный в TERA_PASSWORD
TERA_PASSWORD	Не задано	Задание пароля для подключения к гостевой ОС. Использовать параметр не рекомендуется.
TERA_TPM	false	Управление механизмом аутентификации в гостевой ОС с использованием TPM-модуля. В Termidesk версии 7.0 параметр не поддерживается. Возможные значения: • true - разрешить использование TPM-модуля при аутентификации в гостевой ОС; • false - запретить использование TPM-модуля при аутентификации в гостевой ОС

Список поддерживаемых алгоритмов и их формат:

- TLS_AES_256_GCM_SHA384;
- TLS_CHACHA20_POLY1305_SHA256;
- TLS_AES_128_GCM_SHA256;
- ECDHE-ECDSA-AES256-GCM-SHA384;
- ECDHE-RSA-AES256-GCM-SHA384;
- DHE-RSA-AES256-GCM-SHA384;
- ECDHE-ECDSA-CHACHA20-POLY1305;
- ECDHE-RSA-CHACHA20-POLY1305;
- DHE-RSA-CHACHA20-POLY1305;
- ECDHE-ECDSA-AES128-GCM-SHA256;
- ECDHE-RSA-AES128-GCM-SHA256;

- DHE-RSA-AES128-GCM-SHA256;
- ECDHE-ECDSA-AES256-SHA384;
- ECDHE-RSA-AES256-SHA384;
- DHE-RSA-AES256-SHA256;
- ECDHE-ECDSA-AES128-SHA256;
- ECDHE-RSA-AES128-SHA256;
- DHE-RSA-AES128-SHA256;
- ECDHE-ECDSA-AES256-SHA;
- ECDHE-RSA-AES256-SHA;
- DHE-RSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:RSA-PSK-AES256-GCM-SHA384:DHE-PSK-AES256-GCM-SHA384:RSA-PSK-CHACHA20-POLY1305;
- DHE-PSK-CHACHA20-POLY1305;
- ECDHE-PSK-CHACHA20-POLY1305;
- AES256-GCM-SHA384;
- PSK-AES256-GCM-SHA384;
- PSK-CHACHA20-POLY1305;
- RSA-PSK-AES128-GCM-SHA256;
- DHE-PSK-AES128-GCM-SHA256;
- AES128-GCM-SHA256;
- PSK-AES128-GCM-SHA256;
- AES256-SHA256; AES128-SHA256;
- ECDHE-PSK-AES256-CBC-SHA384;
- ECDHE-PSK-AES256-CBC-SHA;
- SRP-RSA-AES-256-CBC-SHA;
- SRP-AES-256-CBC-SHA;
- RSA-PSK-AES256-CBC-SHA384;
- DHE-PSK-AES256-CBC-SHA384;
- RSA-PSK-AES256-CBC-SHA;
- DHE-PSK-AES256-CBC-SHA;
- AES256-SHA;
- PSK-AES256-CBC-SHA384;
- PSK-AES256-CBC-SHA;
- ECDHE-PSK-AES128-CBC-SHA256;
- ECDHE-PSK-AES128-CBC-SHA;
- SRP-RSA-AES-128-CBC-SHA;
- SRP-AES-128-CBC-SHA;
- RSA-PSK-AES128-CBC-SHA256;
- DHE-PSK-AES128-CBC-SHA256;
- RSA-PSK-AES128-CBC-SHA;
- DHE-PSK-AES128-CBC-SHA;
- AES128-SHA;

- PSK-AES128-CBC-SHA256;
- PSK-AES128-CBC-SHA.

Каталог реестра HKEY_LOCAL_MACHINE\SOFTWARE\UVEON\Termidesk TERA\vdagent

Каталог реестра HKEY_LOCAL_MACHINE\SOFTWARE\UVEON\Termidesk TERA\vdagent используется для настройки ПО TERA vdagent в ОС Microsoft Windows. Также поддерживается настройка параметров через переменные окружения с аналогичным именем.

Для применения настроек необходимо:

- перезагрузить службу TERA Server;
- выполнить переподключение пользователя к РМ по протоколу TERA.

Перечень параметров, доступных для настройки ПО TERA vdagent приведен в таблице (см. таблицу Список параметров ПО TERA vdagent в реестре ОС Microsoft Windows).

Таблица 267. Список параметров ПО TERA vdagent в реестре ОС Microsoft Windows

Параметр	Значение по умолчанию	Описание
TERA_VDAGENT_DEBUG	false	Использование режима отладки. Возможные значения: • true - использовать режим отладки; • false - не использовать режим отладки
TERA_VDAGENT_SCALING_ENABLE	false	Управление поведением на запросы клиентского приложения (ПО Termidesk Viewer) на изменение коэффициента масштабирования в настройках мониторов. Возможные значения: • true - обработать запросы клиентского приложения (ПО Termidesk Viewer) на изменение коэффициента масштабирования в настройках мониторов (включение масштабирования); • false - игнорировать запросы клиентского приложения (ПО Termidesk Viewer) на изменение коэффициента масштабирования в настройках мониторов (отключение масштабирования)

Просмотр списка сессий TERA в ОС Microsoft Windows

Посмотреть список активных пользовательских сессий можно несколькими способами. Например:

- из «Диспетчера задач» ОС. Для этого открыть «Диспетчер задач» и перейти во вкладку «Пользователи». TERA-подключение будет содержать в имени сеанса «TERA» и идентификатор (номер открытого консольного сеанса, см. Пример отображения сеанса из «Диспетчера задач»);

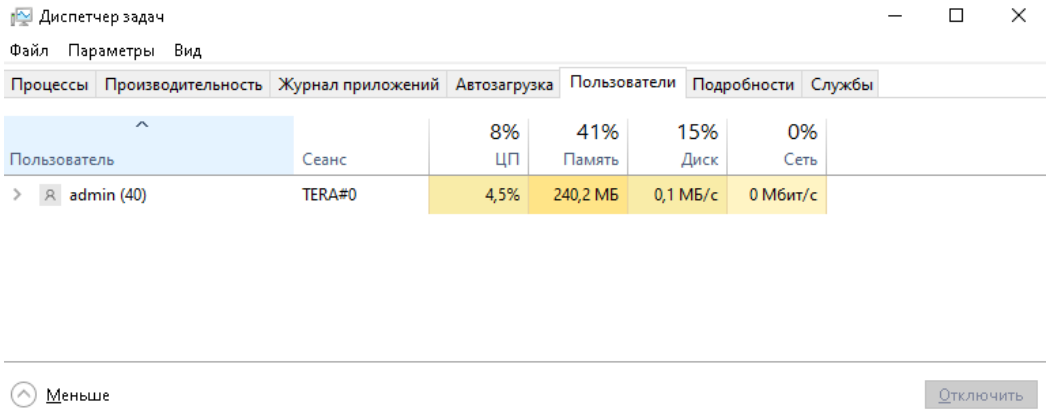


Рисунок 148. Пример отображения сеанса из «Диспетчера задач»

- из интерфейса командной строки (см. рисунок Пример отображения сеанса из интерфейса командной строки). Для этого воспользоваться встроенной в ОС утилитой `qwinsta`:

```
qwinsta
```

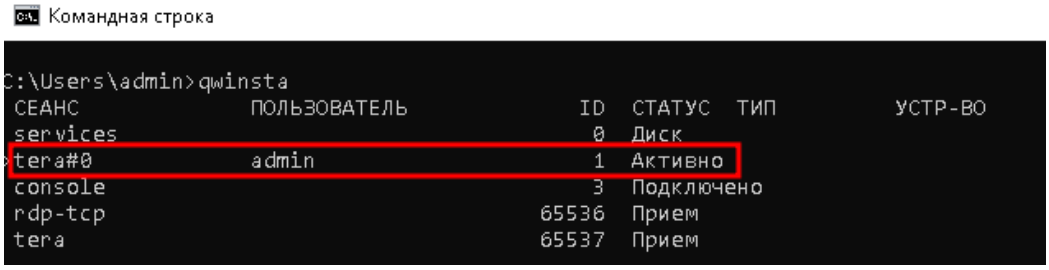


Рисунок 149. Пример отображения сеанса из интерфейса командной строки

Аутентификация подключений к TERA в ОС Microsoft Windows

Механизм работы при аутентификации сетевого подключения:

- TCP-соединение устанавливается с TERA-сервером;
- TERA-сервер инициирует обмен, чтобы убедиться, что сторона, подключившаяся к сокету, имеет право получать графическую сессию;
- аутентификация подключения: проверка учетных данных соединения (не путать с логином и паролем пользователя для графической сессии);
- результат подключения:
  - либо соединение устанавливается и TERA-сервер начинает трансляцию изображения, если аутентификация пройдена успешно;
  - либо соединение разрывается, если аутентификация пройдена неуспешно.

Описание не затрагивает аутентификацию пользователя в ОС. Аутентификация пользователя в графическую сессию происходит внутри протокола с помощью поставщика учетных данных (Credential Provider), который входит в состав «Агента виртуального рабочего места».

Протокол TERA поддерживает несколько методов аутентификации подключения клиентской части (TERA-клиента) к серверной (TERA-серверу):

Метод аутентификации - механизм проверки аутентификационных данных

при подключении к TERA-серверу. Он выбирается клиентской частью пользовательского ПО (ПО Termidesk Viewer) из набора методов, сконфигурированных на TERA-сервере.

Методы аутентификации по паролю и через поставщика учетных данных могут быть включены одновременно. В этом случае TERA будет ожидать либо предъявления пароля, либо передачи аутентификационных данных.

- без аутентификации;
- поставщик учетных данных;
- пароль. Относится к простой проверке подключения к TERA-серверу:
  - указывается в настройках протокола доставки в «Портале администратора» Termidesk, если используется;
  - не вводится пользователем при подключении, поскольку передается в параметрах подключения компонентом «Клиент» автоматически.

Использование методов аутентификации настраивается через конфигурационные файлы (см. подраздел **Каталог реестра** `HKEY_LOCAL_MACHINE\SOFTWARE\UVEON\Termidesk TERA`):

- для подключения без аутентификации параметру `TERA_CRED_PROVIDER` нужно присвоить значение `false`. При этом:
  - параметру `TERA_DISABLE_TICKETING` присвоить значение `true`;
  - в «Портале администратора» политике «Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)» присвоить значение «Выключен»;
- для аутентификации с использованием поставщика учетных данных:
  - параметру `TERA_CRED_PROVIDER` присвоить значение `true`;
  - в «Портале администратора» политике «Автоматический вход в систему при подключении к РМ» присвоить значение «Включен»;
- для подключения с аутентификацией по паролю параметру `TERA_CRED_PROVIDER` нужно присвоить значение `false`. При этом:
  - параметру `TERA_DISABLE_TICKETING` присвоить значение `false`;
  - указать пароль в параметре `TERA_PASSWORD`;
  - в «Портале администратора» политике «Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)» присвоить значение «Выключен».

При некорректной настройке параметров в ПО Termidesk Viewer отобразит сообщение об ошибке: «Ошибка подключения: ошибка аутентификации».

Если все методы аутентификации будут включены одновременно, то приоритет их использования будет следующим (от более приоритетного к менее приоритетному):

- поставщик учетных данных;
- пароль;
- без аутентификации.

Особенности функционирования:

- отключение всех методов и установка `TERA_DISABLE_TICKETING = true` приведет к разрешению подключения к TERA без аутентификации;
- включение либо пароля, либо поставщика учетных данных приведет к включению использования билетов аутентификации;

- выбор метода аутентификации не зависит от использования протоколов SSL/TLS.

Сценарии подключений к TERA в ОС Windows

Протокол TERA поддерживает следующие сценарии подключения:

- подключение пользователя к РМ при отсутствии авторизованного пользователя;
- первое подключение второго пользователя к РМ с авторизованным пользователем;
- повторное подключение пользователя к РМ с авторизованным пользователем.

При подключении пользователя к РМ, в котором отсутствует авторизованный пользователь дополнительные действия со стороны пользователя не требуются.

При первом подключении второго пользователя к РМ с авторизованным пользователем:

- отобразится сообщение: «В систему вошел другой пользователь. Если вы продолжите, он будет отключен. Вы все равно хотите войти в систему?». Для продолжения подключения нужно нажать экранную кнопку **[Да]**;
- авторизованному пользователю отобразится сообщение: «Вы хотите разрешить подключение к этому компьютеру?». Для разрешения подключения авторизованному пользователю нужно нажать экранную кнопку **[OK]**. После подтверждения сеанс авторизованного пользователя будет отключен. Если авторизованный пользователь будет бездействовать в течение 30 секунд, то его сеанс будет отключен автоматически;
- после отключения авторизованного пользователя выполняется подключение второго пользователя к РМ.

При повторном подключении пользователя к РМ с авторизованным пользователем:

- отобразится сообщение: «В систему вошел другой пользователь. Если вы продолжите, он будет отключен. Вы все равно хотите войти в систему?». Для продолжения подключения нужно нажать экранную кнопку **[Да]**;
- авторизованному пользователю отобразится сообщение: «Вы хотите разрешить подключение к этому компьютеру?». Для разрешения подключения авторизованному пользователю нужно нажать экранную кнопку **[OK]**. После подтверждения сеанс авторизованного пользователя будет отключен. Если авторизованный пользователь будет бездействовать в течение 30 секунд, то его сеанс будет отключен автоматически;
- затем ПО Termidesk Viewer выполнит переподключение к РМ и автоматически подключит пользователя к ранее созданному пользовательскому сеансу.

TERA. ОБЩИЕ НАСТРОЙКИ ДЛЯ ВСЕХ ОС

Масштабирование элементов клиентского приложения

TERA поддерживает масштабирование элементов клиентского приложения с учетом коэффициента масштабирования экрана пользовательского монитора. Функционал обеспечивает корректный размер и разборчивость текста и элементов интерфейса клиентского приложения.

При подключении пользователя через компонент «Клиент» на TERA-сервер отправляется коэффициент масштабирования экрана пользовательского монитора, который обрабатывается ПО tera-vdagent и службой `tera-vdagentd` и применяется.

Функционал является экспериментальным и управляется:

- ОС Linux: параметром `--scaling` (включение масштабирования, по умолчанию отключено) (см. подраздел **Интерфейс командной строки ПО tera-vdagent**);

- ОС Microsoft Windows: параметром `TERA_VDAGENT_SCALING_ENABLE` (см. подраздел **Каталог реестра** `HKEY_LOCAL_MACHINE\SOFTWARE\UVEON\Termidesk TERA`).

> Коэффициент масштабирования экрана применяется в момент подключения пользователя (при запуске или перезапуске менеджера графического сервера на стороне ОС РМ) и не применяется на экране приветствия. Если во время работы пользователя параметры экрана изменились, пользователю нужно:
>
> - либо отключиться (отключить сеанс) и затем повторно подключиться к РМ;
> - либо перезапустить менеджер графического сервера на стороне ОС РМ. В ОС Astra Linux Special Edition это служба `fly-dm`.

Учет коэффициента масштабирования экрана гарантируется для наборов ОС (пользовательская ОС - ОС РМ):

- ОС Astra Linux Special Edition - ОС Astra Linux Special Edition;
- ОС Astra Linux Special Edition - ОС Microsoft Windows;
- ОС Microsoft Windows - ОС Astra Linux Special Edition;
- ОС Microsoft Windows - ОС Microsoft Windows.

TERA. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

Интерфейс командной строки ПО x11tera

Параметры запуска ПО x11tera могут быть заданы с помощью конфигурационного файла (см. подраздел **Параметры запуска службы** `x11tera`).

Параметры работы ПО x11tera могут быть переопределены как конфигурационным файлом (см. подраздел **Конфигурационный файл** `x11tera.conf`), так и аргументами командной строки.

Для получения краткой информации по доступным параметрам командной строки следует вызвать приложение `x11tera` с аргументом `--help`:

```
x11tera --help
```

Для запуска ПО x11tera из командной строки используется следующий формат вызова:

```
x11tera <параметры> <адрес_прослушивания>
```

Где:

`<адрес_прослушивания>` - адрес и порт (или диапазон портов) для входящих подключений. По умолчанию используется localhost и порт 5900.

Пример:

```
x11tera 127.0.0.1:5900-5910
```

Список доступных параметров приведен в таблице (см. таблицу Параметры командной строки ПО x11tera).

Таблица 268. Параметры командной строки ПО x11tera

Параметр	Описание
`--allow-control`	Включение возможности удаленному пользователю перемещать мышь и нажимать клавиши. Параметр является унарным аргументом
`--no-allow-control`	Отключение возможности удаленному пользователю перемещать мышь и нажимать клавиши. Параметр является унарным аргументом
`--timeout`	Задание времени ожидания (в секундах), по истечении которого ПО x11tera прекратит работу, если соединение не было установлено. Значение `0` - время ожидания не задано. Пример использования: `x11tera --timeout=5 127.0.0.1:5902`

`--display`	Выбор дисплея для подключения пользователя.
	
	По умолчанию параметр используется как `--display=:0`.
	
	Примеры использования:
	
	• указание конкретного дисплея в параметре:
	
	`x11tera --display=:1`
	
	• использование значения переменной окружения `DISPLAY` в параметре:
	
	`x11tera --display=$DISPLAY`

`--generate -password`	Задание длины пароля. Если параметр используется, то для подключения пользователя к ОС физической машины будет автоматически сгенерирован пароль заданной длины. Пример использования: `x11tera --generate-password=5 127.0.0.1:5902`
`--password`	Задание пароля для подключения пользователя к ОС физической машины. Пример использования: `x11tera --password=password 127.0.0.1:5902`

Параметр	Описание
`--password-file`	Задание файла, хранящего пароль для подключения пользователя к ОС физической машины. Значение «-» соответствует чтению со стандартного устройства ввода. Пример использования: `x11tera --password-file=<путь_к_файлу> 127.0.0.1:5902`
`--config`	Задание конфигурационного файла ПО x11tera. Пример использования: `x11tera --config=/etc/xdg/x11tera/x11tera.conf 127.0.0.1:5902`
`--ssl`	Задание настроек SSL/TLS
`--hide`	Сокрытие графического интерфейса ПО x11tera в трей. По умолчанию графический интерфейс не отображается, т.к. ПО x11tera запускается как служба ОС. Параметр является унарным аргументом. Пример использования: `x11tera --hide 127.0.0.1:5905`
`--minimize`	Запуск графического интерфейса ПО x11tera. По умолчанию графический интерфейс не отображается, т.к. ПО x11tera запускается как служба ОС. Параметр является унарным аргументом. Пример использования: `x11tera --minimize 127.0.0.1:5905`
`--exit-on -disconnect`	Завершение ПО x11tera после отключения первого пользователя. Параметр является унарным аргументом. Пример использования: `x11tera --exit-on-disconnect 127.0.0.1:5905`

Интерфейс командной строки утилиты `x11tera_unlock`

Утилита `x11tera_unlock` является утилитой командной строки, используется в работе служб `x11tera_unlock.service` и `x11tera_controls.service`.

Для получения краткой информации по доступным параметрам командной строки следует вызвать `x11tera_unlock` с аргументом `--help`:

```
x11tera_unlock --help
```

Для запуска `x11tera_unlock` из командной строки используется следующий формат вызова:

```
x11tera_unlock [режим] [параметры]
```

Утилита `x11tera_unlock` поддерживает несколько режимов работы (см. таблицу Режимы работы утилиты x11tera_unlock).

Таблица 269. Режимы работы утилиты x11tera_unlock

Режим	Описание
`list`	Отображает список подключенных интерфейсов ввода (клавиатура, мышь, тачпад, трекбол, сенсорный дисплей). Поддерживаются опциональные параметры: • `--all` (по умолчанию) - вывод списка всех подключенных интерфейсов ввода; • `--keyboards` - вывод списка подключенных клавиатур; • `--pointers` - вывод списка подключенных указателей (например, мыши)
`track`	Отображает список подключенных интерфейсов ввода (клавиатура, мышь, тачпад, трекбол, сенсорный дисплей). Используется в составе службы `x11tera_unlock.service`. Если будет найдено хоть одно совместимое устройство, утилита начинает отслеживать события нажатия комбинаций клавиш, жестов и других интерфейсов ввода. Если в процессе работы какое-либо устройство окажется недоступным, отслеживание его ввода прекратится. При обнаружении последовательности разблокировки (см. подраздел **Разблокирование физической машины с помощью интерфейсов ввода**) утилитой будет выполнена команда: `/usr/bin/x11tera.sh disconnect`

`controls`	Используется в составе службы `x11tera_controls.service`. Выполняет:
	
	• либо команду блокировки интерфейсов управления физической машиной (см. подраздел **Исполняемый файл `x11tera_on_lock`**):
	
	`/usr/bin/x11tera.sh siglock`
	
	• либо команду разблокировки интерфейсов управления физической машиной (см. подраздел **Исполняемый файл `x11tera_on_unlock`**):
	
	`/usr/bin/x11tera.sh sigunlock`
	
	Для того чтобы служба `x11tera_controls.service` могла получать сигналы от непривилегированных процессов ПО x11tera, нужно настроить правила PolicyKit (см. подраздел **Общие сведения о параметрах конфигурирования TERA**)

Интерфейс командной строки ПО tera-vdagent

ПО tera-vdagent автоматически запускается при входе пользователя на свойрабочий стол, а также при появлении экрана выбора пользователей (экрана приветствия). Запуск существляется через исполняемый файл `/usr/bin/tera-vdagent.sh`.

Во время запуска применяются дополнительные аргументы командной строки ПО tera-vdagent, которые могут быть заданы в специальном конфигурационном файле `/etc/default/tera-vdagent`. Это обеспечивает гибкую настройку работы ПО.

Файл `/etc/default/tera-vdagent`:

- является необязательным и может отсутствовать в ОС;
- может содержать необязательный параметр `TERA_VDAGENT_EXTRA_ARGS`, задающий дополнительные аргументы командной строки ПО tera-vdagent. Если при определении параметра `TERA_VDAGENT_EXTRA_ARGS` используются несколько аргументов, то все они задаются в кавычках.

Пример содержимого файла `/etc/default/tera-vdagent`:

```
TERA_VDAGENT_EXTRA_ARGS="--render-mode=near"
```

Для получения краткой информации по доступным параметрам командной строки следует вызвать ПО tera-vdagent с аргументом` --help`:

```
tera-vdagent --help
```

Для запуска `tera-vdagent` из командной строки используется следующий формат вызова:

```
tera-vdagent [параметр] [значение]
```

Пример:

```
tera-vdagent --render-mode near
```

Для изменения настроек ПО можно воспользоваться режимом реконфигурирования пакета - внести правки в интерактивном диалоге с пояснениями и подсказками (изменения автоматически применятся в файлы `/etc/default/tera-vdagent` и `/etc/default/tera-vdagentd`):

```
sudo dpkg-reconfigure tera-vdagent
```

Список доступных параметров приведен в таблице (см. таблицу Параметры командной строки утилиты tera-vdagent).

Таблица 270. Параметры командной строки утилиты tera-vdagent

Параметр	Ключ параметра	Описание
`--debug`	`-d`	Включение отладочного режима логирования
`--virtio-serial-port-path`	`-s`	Путь к виртуальному устройству `virtio` для взаимодействия службы `tera-vdagentd` с ОС. По умолчанию `/tmp/xtera-virtio`
`--vdagentd-socket`	`-S`	Программный интерфейс службы `tera-vdagentd`. По умолчанию `/run/tera-vdagentd/tera-vdagent-sock`
`--foreground`	`-x`	Включение фонового режима работы ПО tera-vdagent
`--file-xfer-save-dir=<значение>`	`-f`	Путь к директории для сохранения переданных файлов. Возможные значения: • `<путь к директории>`; • `xdg-desktop` - директория рабочего стола; • `xdg-download` - директория загрузок
`--file-xfer-open-dir=<значение>`	`-o`	Управление режимом открытия директории после завершения передачи файлов. Возможные значения: • `0` - не открывать директорию; • `1` - открыть директорию
`--render-mode=<значение>`	`-R`	Управление разрешением экрана физической машины для отображения в ПО Termidesk Viewer. По умолчанию разрешение экрана определяется на основе размера окна ПО Termidesk Viewer и устанавливается с точностью до пикселя. Возможные значения: • `near` - управляет разрешением экрана в соответствии со сведениями о характеристиках оборудования физической машины и устанавливает минимально доступное значение; • `mutter` - выполняет масштабирование изображения под размер окна ПО Termidesk Viewer
`--no-scaling`	Не задано	Игнорирование запросов клиентского приложения (ПО Termidesk Viewer) на изменение коэффициента масштабирования в настройках мониторов (отключение масштабирования). Параметр используется по умолчанию

Параметр	Ключ параметра	Описание
`--scaling`	Не задано	Обработка запросов клиентского приложения (ПО Termidesk Viewer) на изменение коэффициента масштабирования в настройках мониторов (включение масштабирования)

Интерфейс командной строки ПО tera-vdagentd

Параметры запуска ПО tera-vdagentd могут быть заданы:

- через конфигурационный файл, используемый при автоматическом запуске ПО (см. подраздел **Параметры запуска службы** `tera-vdagentd`);
- аргументами командной строки.

Для получения краткой информации по доступным параметрам командной строки следует вызвать исполняемый файл ПО `/usr/sbin/tera-vdagentd` с аргументом `--help`:

```
/usr/sbin/tera-vdagentd --help
```

Для запуска `tera-vdagentd` из командной строки используется следующий формат вызова:

```
/usr/sbin/tera-vdagentd [параметр] [значение]
```

Пример:

```
/usr/sbin/tera-vdagentd --virtio-serial-port-path /tmp/xtera-virtio
```

Для изменения настроек ПО можно воспользоваться режимом реконфигурирования пакета - внести правки в интерактивном диалоге с пояснениями и подсказками (изменения автоматически применятся в файлы `/etc/default/tera-vdagent` и `/etc/default/tera-vdagentd`):

```
sudo dpkg-reconfigure tera-vdagent
```

Список доступных параметров приведен в таблице (см. таблицу Параметры командной строки ПО tera-vdagentd).

Таблица 271. Параметры командной строки ПО tera-vdagentd

Параметр	Ключ параметра	Описание
`--debug`	`-d`	Включение отладочного режима логирования. Повторное указание параметра позволяет установить повышенный уровень логирования

Параметр	Ключ параметра	Описание
`--virtio -serial-port -path`	`-s`	Путь к виртуальному устройству `virtio` для взаимодействия ПО tera-vdagentd с драйвером QXL или ПО x11tera. По умолчанию `/tmp/xtera-virtio`
`--vdagentd -socket`	`-S`	Программный интерфейс службы `tera-vdagentd`. По умолчанию `/run/tera-vdagentd/tera-vdagent-sock`
`--uinput -device`	`-u`	Путь к устройству `uinput` для эмуляции ввода с клавиатуры и мыши
`--fake-uinput`	`-f`	Использование устройства uinput в режиме фиктивного ввода
`--foreground`	`-x`	Включение фонового режима работы ПО tera-vdagentd
`--one-session`	`-o`	Обработка только одной клиентской сессии по каналу `virtio-serial`. Программа остановит работу при отключении: • либо драйвера QXL (в среде ВМ); • либо ПО x11tera (в среде физической машины). Если ПО запущено службой `tera-vdagentd`, то это приведет к ее перезапуску
`--one-agent`	`-O`	Обработка только одной сессии ПО tera-vdagent. Программа остановит работу при обнаружении отключения ПО tera-vdagent. Если ПО запущено службой `tera-vdagentd`, то это приведет к ее перезапуску
`--one-seat`	`-l`	Обработка только одной сессии РМ. Программа остановит работу при обнаружении смены РМ: например, при обнаружении смены окна выбора пользователя на окно рабочего стола пользователя. Если ПО запущено службой `tera-vdagentd`, то это приведет к ее перезапуску. Параметр не может использоваться при отключенной интеграции служб `console kit` и `systemd-logind` В ОС AstraLinux Special Edition режим используется по умолчанию
`--disable -session -integration`	`-X`	Отключение интеграции служб `console kit` и `systemd-logind`. Использование параметра совместно с аргументом `--one-seat` не допускается

Параметр	Ключ параметра	Описание
`--without-qxl-pci`	`-Q`	Вызов ПО tera-vdagentd без обращения к драйверу виртуального графического процессора QXL и без внесения изменений в файл `xorg.conf.tera` при изменении разрешения экрана. Параметр позволяет активировать дополнительные мониторы, указанные в настройках ПО Termidesk Viewer

Интерфейс командной строки ПО tera-router

Пакет `tera-router` требуется для обеспечения подключения по UDP через шлюз, во всех других случаях (без UDP через шлюз, прямое подключение без шлюза) проксирование подключений не требуется

Параметры запуска ПО tera-router могут быть заданы:

- через конфигурационный файл, используемый при автоматическом запуске ПО (см. подраздел **Параметры запуска службы** `tera-router`);
- аргументами командной строки.

Для получения краткой информации по доступным параметрам командной строки следует выполнить:

```
tera-router --help
```

Для запуска ПО tera-router из командной строки используется следующий формат вызова:

```
tera-router [ключ] [значение]
```

Список доступных параметров приведен в таблице (см. таблицу Параметры командной строки ПО tera-router).

Таблица 272. Параметры командной строки ПО tera-router

Ключ	Описание
`-d`	Включение отладочного уровня журналирования событий. Альтернативный метод: задать переменную окружения `TDSK_DEBUG`. Не требует указания значения
`-a`	Клиентская часть: включение запроса схем маршрутизации с сервера. Не требует указания значения
`-l`	Включение определения типа канала по пакету состояния канала. Ключ применим только для открытого трафика. Формат значения: `[type_offset]:[id_offset]` Пример значения: `20:21`

Ключ	Описание
-b	Прослушиваемый интерфейс. Можно указать несколько. По умолчанию используется 0.0.0.0. Значение рекомендуется переопределить, указав реальный IP-адрес. При использовании значения по умолчанию будет использоваться адрес первого доступного сетевого интерфейса (не localhost). Формат значения: [тип_канала]:[идентификатор_канала]:[метка]:[IP-адрес]:[порт]<:[протокол]><:[время_ожидания]><:[размер_буфера]>. Информация по параметрам, передающимся в значении, приведена в таблице (см. таблицу Параметры для значений ключей ПО tera-router). Пример значения: 0:0:0:192.0.2.1:5800
-r	Маршрут для TCP/UDP трафика: • если применяется на клиентской стороне, то определяет маршрутизацию для TCP и UDP трафика; • если применяется на серверной стороне, то определяет обратную маршрутизацию UDP трафика. Особенности функционирования: • для корректной работы TCP-маршрутизации необходимо, чтобы конфигурации сервера и клиента соответствовали друг другу; • при использовании UDP обязательна двусторонняя настройка маршрутов (-r) на обоих концах. Формат значения: [тип_канала]:[идентификатор_канала]:[метка]:[IP-адрес]:[порт]<:[протокол]><:[время_ожидания]><:[размер_буфера]>. Информация по параметрам, передающимся в значении, приведена в таблице (см. таблицу Параметры для значений ключей ПО tera-router). Пример значения: 0:0:0:192.0.2.2:5800
-c	Интерфейс для подключения. Можно указать несколько, в этом случае будет использоваться первый доступный. Формат значения: [тип_канала]:[идентификатор_канала]:[метка]:[IP-адрес]:[порт]<:[протокол]><:[время_ожидания]><:[размер_буфера]>. Информация по параметрам, передающимся в значении, приведена в таблице (см. таблицу Параметры для значений ключей ПО tera-router). Пример значения: 0:0:0:127.0.0.1:5900

Таблица 273. Параметры для значений ключей ПО tera-router

Параметр	Описание
[тип_канала]	Тип канала. Обязательный параметр. Возможные значения: • 1 - MAIN; • 2 - DISPLAY; • 3 - INPUTS; • 4 - CURSOR; • 5 - PLAYBACK; • 6 - RECORD; • 7 - TUNNEL; • 8 - SMARTCARD; • 9 - USBREDIR; • 10 - PORT; • 11 - WEBDAV
[идентификатор_канала]	Идентификатор канала. Обязательный параметр
[метка]	Метка, выставляемая на пакеты. Обязательный параметр, устанавливается только для ключа -r
[IP-адрес]	IP-адрес. Обязательный параметр
[порт]	Порт. Обязательный параметр
[протокол]	Протокол. Необязательный параметр. Возможные значения: • 0 (умолчанию) для TCP; • любое другое целочисленное значение для UDP
[время_ожидания]	Время ожидания (в миллисекундах) для операций чтения или записи. Необязательный параметр. Значение по умолчанию: 1200 (1,2 секунды)
[размер_буфера]	Размер буфера (в Кбайтах) для чтения или записи данных. Необязательный параметр. Значение по умолчанию: • 16 КБ (TCP); • 8 КБ (UDP)

Примеры использования приведены в таблице (см. таблицу Сценарии вызова ПО tera-router).

Таблица 274. Сценарии вызова ПО tera-router

Сценарий	Пример

Передача всех каналов по протоколу TCP	Серверная часть (IP-адрес: 192.0.2.1):
	
	`tera-router -l 20:21 -b 0:0:0:192.0.2.1:5800 -c 0:0:0:127.0.0.1:5900`
	
	Клиентская часть (IP-адрес: 192.0.2.2):
	
	`tera-router -l 20:21 -b 0:0:0:127.0.0.1:5900 -r 0:0:0:192.0.2.2:5800`

Раздельная маршрутизация по протоколам	Серверная часть (IP-адрес: 192.0.2.1):
	
	`tera-router -l 20:21 \ -b 0:0:0:192.0.2.1:5800 \ -b 10:0:0:192.0.2.1:5810:1 \ -r 10:0:0:192.0.2.2:5810:1 \ -c 0:0:0:127.0.0.1:5900`
	
	Клиентская часть (IP-адрес: 192.0.2.2):
	
	`tera-router -l 20:21 \ -b 0:0:0:127.0.0.1:5900 \ -r 0:0:0:192.0.2.1:5800 \ -b 10:0:0:192.0.2.2:5810:1 \ -r 10:0:0:192.0.2.1:5810:1`
	
	Пояснение:
	
	• канал `0:0` передается по TCP через порт 5800;
	• канал `10:0` передается по UDP (протокол = 1) через порт 5810;
	• на сервере и клиенте настроены взаимные UDP-маршруты для канала `10:0`

Настройка серверной части для UDP-канала INPUTS (3) с идентификатором 0 и меткой 0	Значение для ключа `-b`: `3:0:0`.
	
	Примеры запуска:
	
	`tera-router -l 20:21 \ -b 3:0:0:0.0.0.0:6010:1`
	
	`tera-router -l 20:21 \ -b 3:0:0:${TERA_ROUTER_ADDRESS:-0.0.0.0}:6010:1`

Сценарий	Пример

Настройка серверной части для UDP-каналов INPUTS и CURSOR	`tera-router -l 20:21 \`
	`  -b 3:0:0:0.0.0.0:6010:1 \`
	`  -b 4:0:0:0.0.0.0:6020:1`
	
	`tera-router -l 20:21 \`
	`  -b 3:0:0:${TERA_ROUTER_ADDRESS:-0.0.0.0}:6010:1 \`
	`  -b 4:0:0:${TERA_ROUTER_ADDRESS:-0.0.0.0}:6020:1`

Интерфейс командной строки ПО tera-gateway

ПО tera-gateway устанавливается из пакета `tera-router` и предназначен для эмуляции шлюза.

Для получения краткой информации по доступным параметрам командной строки следует выполнить:

```
tera-gateway --help
```

Для запуска ПО tera-gateway из командной строки используется следующий формат вызова:

```
tera-gateway [ключ] [значение]
```

Список доступных параметров приведен в таблице (см. таблицу Параметры командной строки ПО tera-gateway).

Таблица 275. Параметры командной строки ПО tera-gateway

Ключ	Описание
`-d`	Включение отладочного уровня журналирования событий. Не требует указания значения
`-u`	Прослушиваемый интерфейс. Формат значения: `[IP-адрес]:[порт]<:[протокол]><:[время_ожидания]><:[размер_буфера]`. Информация по параметрам, передающимся в значении, приведена в таблице (см. таблицу Параметры для значений ключей ПО tera-gateway). Пример значения: `192.0.2.1:5800:0:2000:16384`

Ключ	Описание
-w	Интерфейс для подключения. Формат значения: [IP-адрес]:[порт]<:[протокол]><:[время_ожидания]><:[размер_буфера]. Информация по параметрам, передающимся в значении, приведена в таблице (см. таблицу Параметры для значений ключей ПО tera-gateway). Пример значения: 192.0.2.2:5900:0:2000:16384
-j	Схема маршрутизации в формате base64, сформированная серверной стороной ПО tera-router (значение ключа cli из файла /var/run/termidesk/tera-router.json)

Таблица 276. Параметры для значений ключей ПО tera-gateway

Параметр	Описание
[IP-адрес]	IP-адрес. Обязательный параметр
[порт]	Порт. Обязательный параметр
[протокол]	Протокол. Необязательный параметр. Возможные значения: • 0 (умолчанию) для TCP; • любое другое целочисленное значение для UDP
[время_ожидания]	Время ожидания (в миллисекундах) для операций чтения или записи.Необязательный параметр. Значение по умолчанию: 1200 (1,2 секунды)
[размер_буфера]	Размер буфера (в Кбайтах) для чтения или записи данных. Необязательный параметр. Значение по умолчанию: 8 КБ

Интерфейс командной строки ПО tera-webdav

Для получения краткой информации по доступным параметрам командной строки следует вызвать исполняемый файл ПО tera-webdav с аргументом --help:

```
tera-webdav --help
```

Для запуска tera-webdav из командной строки используется следующий формат вызова:

```
tera-webdav [параметр] [значение]
```

Список доступных параметров приведен в таблице (см. таблицу Параметры командной строки ПО tera-webdav).

Таблица 277. Параметры командной строки ПО tera-webdav

Параметр	Ключ параметра	Описание
--port	-p	Порт прослушивания службы tera-webdav-service

TERA. ЖУРНАЛИРОВАНИЕ

Журналы TERA-сервера

Среда функционирования ВМ

Журналы работы TERA для ОС Linux расположены в директориях:

- `/var/log/termidesk/tera/` при запуске TERA с правами системного пользователя. При удалении директории требуется переустановка TERA;
- `$HOME/.local/share/termidesk/tera` при запуске TERA с правами несистемного пользователя. При удалении директории переустановка не требуется - она пересоздается.

Журналы работы TERA для ОС Linux:

- журнал TERA-сервера: `/var/log/termidesk/tera/tera-server.log`;
- журнал ПО tera-router: `/var/log/termidesk/tera/tera-router.log`;
- журнал ПО tera-webdav: `$HOME/.local/share/termidesk/tera/tera-webdav.log`.

Журналы работы TERA для ОС Microsoft Windows расположены в каталоге `C:\ProgramData\UVEON\logs\Termidesk TERA`:

- `tera-server.log` - журнал событий непосредственно TERA;
- `tera-service.log` - журнал событий службы `TERA Server`;
- `tera-vdagent.log` - журнал событий ПО TERA vdagent;
- `tera-vdservice.log` - журнал событий службы `TERA Agent`.

Права доступа для ОС Linux:

- для директории `/var/log/termidesk/tera/`: `rwxr-xr-x` (в восьмеричной записи - `755`);
- для файлов журналов: `rw-r—r-` (в восьмеричной записи - `644`).

Файл журнала `tera-server.log` дополняется, а не пересоздаются при перезапуске Xorg. Для исключения ситуации безграничного роста файлов журналов настроена их ротация со следующими настройками по умолчанию:

- файлы архивируются раз в сутки;
- архивация происходит в той же директории, где расположен файл журнала;
- максимальное количество архивных файлов - 10;
- архивация по размеру файла не используется.

Настройки ротации расположены в файлах:

- `/etc/logrotate.d/tera-qxl`;
- `/etc/logrotate.d/tera-router`.

При изменении пути к файлам журналов следует также изменить пути в файлах настройки ротации. Для применения настроек после изменения файлов следует выполнить:

```
sudo /usr/sbin/logrotate -f /etc/logrotate.d/tera-qxl
```

Статус обработки ротации можно посмотреть командой:

```
sudo cat /var/lib/logrotate/status | grep tera
```

По умолчанию ротация запускается раз в сутки с помощью планировщика задач ОС Linux cron (настройки хранятся в файле `/etc/cron.daily`). При изменении периода архивации в файле `/etc/logrotate.d/tera-qxl` нужно дополнительно создать соответствующую задачу для планировщика cron.

Для ручного запуска ротации с опережением графика следует выполнить:

```
sudo /usr/sbin/logrotate --verbose -f /etc/logrotate.d/tera-qxl
```

Среда функционирования физической машины

Журналы работы TERA для ОС Linux расположены в директориях:

- `/var/log/termidesk/tera/` при запуске TERA с правами системного пользователя. При удалении директории `/var/log/termidesk/tera` требуется переустановка TERA;
- `$HOME/.local/share/termidesk/tera` при запуске TERA с правами несистемного пользователя. При удалении директории переустановка не требуется - она пересоздается.

Журналы работы TERA для ОС Linux:

- журнал ПО x11tera: `/var/log/termidesk/tera/x11tera.log`;
- журнал ПО tera-router: `/var/log/termidesk/tera/tera-router.log`;
- журнал ПО tera-webdav: `$HOME/.local/share/termidesk/tera/tera-webdav.log`.

Права доступа для ОС Linux:

- для директории `/var/log/termidesk/tera/`: `rwxr-xr-x` (в восьмеричной записи - `755`);
- для файлов журналов: `rw-r—r-` (в восьмеричной записи - `644`).

Файл журнала `x11tera.log` дополняется, а не пересоздаются при перезапуске ПО x11tera. Настройки ротации файлов журналов аналогичны среде функционирования ВМ.

Настройки ротации расположены в файлах:

- `/etc/logrotate.d/tera-x11`;
- `/etc/logrotate.d/tera-router`.

При изменении пути к файлам журналов следует также изменить пути в файлах настройки ротации. Для применения настроек после изменения файлов следует выполнить:

```
sudo /usr/sbin/logrotate -f /etc/logrotate.d/x11tera
```

Статус обработки ротации можно посмотреть командой:

```
sudo cat /var/lib/logrotate/status | grep tera
```

По умолчанию ротация запускается раз в сутки с помощью планировщика задач ОС Linux cron (настройки хранятся в файле `/etc/cron.daily`). При изменении периода архивации в файле `/etc/logrotate.d/tera-x11` нужно дополнительно создать соответствующую задачу для планировщика cron.

Для ручного запуска ротации с опережением графика следует выполнить:

```
sudo /usr/sbin/logrotate --verbose -f /etc/logrotate.d/tera-x11
```

Журналы ПО tera-vdagent

Журнал работы ПО tera-vdagent можно посмотреть командой:

```
sudo journalctl -f | grep vdagent
```

Журналы ПО tera-vdagentd

Журнал работы ПО tera-vdagentd можно посмотреть командой:

```
sudo journalctl -fu tera-vdagentd
```

Журналы ПО tera-keyagent

Журнал работы ПО tera-keyagent можно посмотреть командой:

```
sudo journalctl -f -u tera-keyagent
```

Отладочный режим

Начиная с Termidesk версии 7.0 TERA поддерживает включение отладочного режима через переменную окружения `TDSK_DEBUG` (достаточно наличие переменной, ее значение неважно).

Переменная может быть указана:

- в запуске каждого приложения отдельно (например через `/etc/default/<имя_службы>`);
- в запуске всех приложений сразу. Для этого используется глобальная настройка.

Для включения глобальной настройки в ОС Linux:

- внести переменную в файл `/etc/systemd/system.conf`:

```
[Manager]
```

```
DefaultEnvironment="TDSK_DEBUG=1"
```

- перезагрузить ОС.

Для отключения использования глобальной настройки в ОС Linux:

- удалить переменную `TDSK_DEBUG` из файла `/etc/systemd/system.conf`;
- перезагрузить ОС.

После завершения диагностики переменную `TDSK_DEBUG` необходимо удалить.

Для включения глобальной настройки в ОС Microsoft Windows:

- открыть командную строку от имени администратора и выполнить:

```
setx TDSK_DEBUG 1 /M
```

- перезагрузить ОС.

Для отключения использования глобальной настройки в ОС Microsoft Windows:

- открыть командную строку от имени администратора и выполнить:

```
reg delete "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment" /v
TDSK_DEBUG /f
```

- перезагрузить ОС.

TERA. НЕШТАТНЫЕ СИТУАЦИИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

Возможные неисправности при работе с TERA и способы их устранения приведены в таблице (см. таблицу Перечень возможных нештатных ситуаций и способов их устранения).

Таблица 278. Перечень возможных нештатных ситуаций и способов их устранения

Индикация	Описание	Возможное решение
Невозможно подключиться по TERA к физической машине с ОС Astra Linux Special Edition	Пользователь не может подключиться по TERA к физической машине	Необходимо проверить работоспособность ПО `x11tera` согласно подразделу **Установка в ОС Astra Linux Special Edition для физической машины**. Если нужный порт не отображается в ОС, то следует: • проверить, выполнялся ли первый вход пользователя локально в ОС физической машины; • выбрать и настроить режим запуска ПО `x11tera` (см. подраздел **Режимы запуска ПО x11tera для физической машины**)
Клавиатура и мышь заблокированы на физической машине с ОС Astra Linux Special Edition	Клавиатура и мышь заблокированы на физической машине после подключения пользователя по TERA	При стандартной настройке TERA для физической машины ввод с клавиатуры, управление указательными устройствами, а также вывод информации на экран дисплея блокируются до тех пор, пока от этой физической машины не отключится удаленный пользователь. Для восстановления локального доступа к физической машине (и отключения удаленного пользователя) могут использоваться следующие способы: • действия, перечисленные в подразделе **Разблокирование физической машины с помощью интерфейсов ввода**; • повторное подключение и отключение пользователя по TERA к физической машине; • отключение сетевого адаптера физической машины от информационной сети. В течение 5 секунд после события отключения мониторы, клавиатуры и указательные устройства должны разблокироваться автоматически; • подключение к физической машине других периферийных устройств (монитора, клавиатуры, мыши) с последующей авторизацией в ОС; • включение заблокированных устройств через удаленное подключение к физической машине по протоколу SSH. Подробно действия приведены после таблицы
Черный экран монитора физической машины с установленной ОС Astra Linux Special Edition	Монитор физической машины перестает отображать изображение, даже при отключении удаленного пользователя	Поведение означает, что настройки монитора не восстановились до штатных, и он остается в выключенном состоянии (фактически уменьшается до нуля яркость монитора). Для решения ситуации следует выполнить удаленное подключение к физической машине по протоколу SSH и выполнить действия по решению ситуации, приведенные после таблицы

Индикация	Описание	Возможное решение
Не происходит изменение размера окна ПО Termidesk Viewer, не работает передача файлов и буфер обмена	При подключении к физической машине с установленной ОС Astra Linux Special Edition не происходит изменение экрана, не работает передача файла и буфер обмена	Для разрешения ситуации следует выполнить переподключение удаленного пользователя через ПО Termidesk Viewer
Масштаб окна ПО Termidesk Viewer меняется с резкими переходами при подключении к физической машине с установленной ОС Astra Linux Special Edition	При подключении к физической машине с установленной ОС Astra Linux Special Edition масштаб окна ПО Termidesk Viewer меняется с резкими переходами, без плавности	Для разрешения ситуации следует исключить использование параметра `--render-mode` со значением `near` для ПО tera-vdagent (см. подраздел **Интерфейс командной строки ПО tera-vdagent**)

Не работает звук в ВМ с установленной ОС Astra Linux Special Edition	После подключения пользователя к ВМ с ОС Astra Linux Special Edition перестает работать звук	Для воспроизведения звука используется виртуальное устройство `pulseaudio`. Звуковые устройства TERA отображаются в настройках звука гостевой ОС с названиями:
		• «Динамики TERA»;
		• «Микрофон TERA».
		Для восстановления работы звука после сбоя следует выполнить в гостевой ОС (команды выполняются подключенным пользователем):
		• перезапустить службу `pulseaudio`:
		`systemctl restart pulseaudio`
		• если первый способ не помог, то перезапустить службы TERA:
		`systemctl --user restart tera-audio.service tera-record.service`

Индикация	Описание	Возможное решение
Отображается диалоговое окно «Ваша предыдущая сессия не завершена! Продолжить?» при подключении к физической машине с установленной ОС Astra Linux Special Edition	При подключении удаленного пользователя к физической машине с установленной ОС Astra Linux Special Edition отображается диалоговое окно «Ваша предыдущая сессия не завершена! Продолжить?». При этом не выключается экран этой физической машины	Поведение означает, что к физической машине уже существует подключение, например, по протоколу SSH. Для решения ситуации следует завершить открытые сессии пользователя и выполнить повторное подключение к физической машине через компонент «Клиент»
Отображается диалоговое окно с текстом «Ваша предыдущая сессия не завершена! Начать новую?»	Диалоговое окно появляется на этапе выхода из сессии и может присутствовать на экране до 15 секунд	Для разрешения ситуации нужно в файле `$HOME/.fly/sessrc` изменить параметры в следующие значения: `UseConfirmDialog=false` и `UseSM=false`
Работа TERA на физической машине происходит с задержками, при этом процессор и сеть на машине не нагружены	При подключении удаленного пользователя к физической машине по протоколу TERA наблюдаются задержки	Для разрешения ситуации следует отключить управление дисплеями, назначив параметр `--render-mode` со значением `mutter` для ПО tera-vdagent (см. подраздел **Интерфейс командной строки ПО tera-vdagent**)
Сообщение «Этот принтер недоступен или настроен неправильно», не распечатывается файл из браузера Chromium	Файл не отправляется на печать из веб-браузера Chromium	Для разрешения ситуации следует: • открыть файл в программе, отличной от веб-браузера Chromium: например, в веб-браузере Mozilla Firefox или в офисном приложении OpenOffice; • распечатать файл через выбранную программу

Индикация	Описание	Возможное решение

Видеоизображение транслируется с задержками, наблюдается снижение производительности	На пользовательской рабочей станции наблюдается снижение производительности, видеоизображение воспроизводится прерывисто и с задержками. Диагностика показывает 100% загрузку центрального процессора	Для разрешения ситуации со снижением производительности пользовательской рабочей станции следует изменить настройки драйвера виртуального графического процессора QXL. Для этого нужно отключить сжатие данных и включить автоматический режим адаптации скорости потока под пропускную способность сети.
		
		Таким образом, нужно убедиться, что группа настроек пропускной способности протокола в конфигурационном файле `/etc/X11/xorg.conf.d/30-teraqxl.xorg.conf` соответствует следующим значениям:
		
		`TeraStreamingVideo=filter`
		`TeraZlibGlzWanCompression=never`
		`TeraJpegWanCompression=never`
		`TeraImageCompression=off`
		`TeraDeferredFPS=0`

Звук передается с задержками при использовании систем видеоконференцсвязи	При использовании систем видеоконференцсвязи в гостевой ОС РМ наблюдаются некомфортные для общения задержки звука	Некоторые модели Bluetooth-наушников могут вносить задержку передачи звука, при которой становится некомфортным общение в видеоконференцсвязи. При этом наличие или отсутствие задержки не зависит от ОС, в которой используются наушники. Для разрешения ситуации нужно убедиться, что используемая модель Bluetooth-наушников не обладает этим недостатком
Нестабильная работа ОС Astra Linux Special Edition при попытке проверить звук для устройства «Микрофон TERA» через системное приложение	При попытке проверить звук с устройства «Микрофон TERA» через встроенное в ОС Astra Linux Special Edition приложение звуковых устройств («Параметры - Звуковые устройства») наблюдается нестабильная работа ОС	Поведение связано с архитектурными ограничениями звукового сервера PulseAudio. Для проверки работы звука для устройства «Микрофон TERA» не следует использовать системное приложение («Параметры - Звуковые устройства», вкладка «Устройства записи»). Для проверки работы звука следует использовать один из способов: • проверка через сторонние приложения, например, веб-браузер Chromium или платформу видеоконференций Dion; • проверка воспроизведения звука с микрофона на устройство «Динамики TERA» в системном приложении звуковых устройств («Параметры - Звуковые устройства», вкладка «Воспроизведение»)

Индикация	Описание	Возможное решение
Не происходит изменение разрешения экрана при подключении к физической машине	При подключении к физической машине не происходит изменение разрешения экрана	Необходимо проверить наличие монитора, подключенного к физической машине. Если ни один монитор не подключен, изменение разрешения экрана работать не будет (при этом экран будет масштабироваться)
Некорректная работа клавиши **<↓>**, отсутствие реакции на клавиши **<←>**, **<↑>**,**<→>**	При подключении к гостевой ОС Astra Linux Special Edition с включенным режимом ЗПС («Смоленск») нажатие клавиши **<↓>** транслируется как клавиша **<ENTER>**, отсутствует реакция на нажатие клавиш **<←>**, **<↑>** ,**<→>**	В TERA из состава Termidesk версии 7.0.1 проблема устранена и дополнительные манипуляции не потребуются. При возникновении проблемы на более старых версиях рекомендуется обновить TERA. Для разрешения ситуации следует: • скорректировать файл `/etc/default/tera-vdagent`, указав `TERA_VDAGENT_RESTORE_XKBMAP=yes`; • выполнить перезапуск службы `tera-vdagentd`
Отсутствуют звуковые устройства в ВМ с установленной ОС Astra Linux Special Edition	После установки TERA на ВМ с ОС Astra Linux Special Edition отсутствуют звуковые устройства	Для разрешения ситуации следует в свойствах ВМ на платформе виртуализации добавить звуковое устройство
Мониторы, подключенные к физической машине, самопроизвольно включаются	На физической машине с ОС Astra Linux Special Edition наблюдается самопроизвольное включение мониторов	Чаще всего ситуация возникает при подключении к физической машине оборудования KVM. Для разрешения ситуации рекомендуется отключить автоматический запуск `kscreend`. Для этого: Ранее требовалось удаление пакета `kscreen`, начиная с TERA из состава Termidesk версии 7.0.1 требуется только отключение его автоматического запуска. • в файл `/etc/xdg/autostart/kscreen.desktop` добавить строку `Hidden=true`; • предварительно сохранить файлы и данные в графической среде, затем перезапустить службу `display-manager`: `sudo systemctl restart display-manager`

Индикация	Описание	Возможное решение
При подключении к РМ ОС Microsoft Windows ПО Termidesk Viewer отображает сообщение: «Ошибка подключения: ошибка аутентификации»	ПО Termidesk Viewer отображает сообщение: «Ошибка подключения: ошибка аутентификации» при подключении к РМ ОС Microsoft Windows	Сообщение отображается в следующих случаях: • выполняется попытка подключения под другой учетной записью к существующему пользовательскому сеансу; • выполнена некорректная настройка поставщика учетных данных. Если в каталоге реестра `HKEY_LOCAL_MACHINE\SOFTWARE\UVEON\Termidesk TERA` параметру `TERA_CRED_PROVIDER` присвоено значение `true`, необходимо убедиться, что в «Портале администратора» активирована политика «Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)».
Отображается экран ввода учетных данных пользователя при использовании поставщика учетных данных при подключении к РМ ОС Microsoft Windows	При подключении к РМ ОС Microsoft Windows отображается экран ввода учетных данных пользователя при использовании поставщика учетных данных	Ситуация возникает при отсутствии пользователя в ОС РМ. В случае бездействия сессия завершится через 30 секунд. Время ожидания аутентификации пользователя задается в параметре `LogonTimeout` в каталоге реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\TERA`

Действия для решения ситуации «Клавиатура и мышь заблокированы». Для восстановления локального доступа к физической машине при удаленном подключении по протоколу SSH:

- выполнить команду:

```
x11tera_on_disconnect
```

- если команда не помогла, то:
  - проверить активные сессии:

    ```
    who
    ```

  - выбрать сессию с обозначением `:0` или `:1` (и др.);
  - назначить полученное обозначение параметру `DISPLAY`:

    ```
    export DISPLAY=:0
    ```

  - получить список заблокированных устройств и запомнить их идентификаторы (параметр `id=`):

    ```
    xinput
    ```

  - включить нужные устройства, указав их идентификатор:

    ```
    xinput enable 9
    xinput enable 11
    ```

  - получить список заблокированных мониторов:

    ```
    xrandr
    ```

  - включить нужный монитор (в примере `HDMI-1`, который не являлся основным):

    ```
    xrandr --output HDMI-1 --auto
    ```

  - восстановить работу основного монитора (в примере `eDP-1`):

    ```
    xrandr --output eDP-1 --brightness 1
    ```

  - убедиться, что работоспособность восстановлена. После выполнения всех шагов может потребоваться ручное восстановление расположения экранов;

- перезагрузить ОС физической машины.

Действия для решения ситуации «Черный экран монитора». Для решения ситуации следует выполнить удаленное подключение к физической машине по протоколу SSH и затем:

- выполнить команду:

```
x11tera_on_disconnect
```

- если команда не помогла, то:
  - проверить активные сессии:

    ```
    who
    ```

  - выбрать сессию с обозначением `:0` или `:1` (и др.);
  - назначить полученное обозначение параметру `DISPLAY`:

    ```
    export DISPLAY=:0
    ```

  - получить список подключенных к физической машине мониторов:

    ```
    xrandr \| grep " connected" \| cut -d' ' -f1
    ```

  - восстановить работу мониторов (в примере `eDP-1` и `HDMI-2`):

    ```
    xrandr --output eDP-1 --auto
    xrandr --output HDMI-2 --auto
    xrandr --output eDP-1 --brightness 1
    xrandr --output HDMI-2 --brightness 1
    ```

Если это не помогло, следует:

- подключить к физической машине второй монитор. Убедиться, что изображение отображается на нем;
- перейти в настройки монитора из ОС. В ОС Astra Linux Special Edition 1.7 нужно перейти «Звезда - Панель управления - Настройка монитора»;
- в поле «Устройство» выбрать основной монитор (проблемный);
- нажать экранную кнопку **[Цветовая коррекция]** и в открывшемся окне изменить значения для парамеров «Гамма», «Красный», «Зеленый», «Синий» при помощи ползунков. При этом применять изменения не требуется.

Если монитор по-прежнему не включается, следует задать параметр `--render-mode` со значением `near` для ПО tera-vdagent (см. подраздел **Интерфейс командной строки ПО tera-vdagent**)

ТЕРМИНЫ

Гостевая ОС

ОС, функционирующая на ВМ

Ключ

Применяется в контексте файла, не опции в команде. Последовательность псевдослучайных чисел, сгенерированная особым образом

Рабочее место

Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа

Сертификат

Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу

Физическая машина

Выделенный компьютер с установленной ОС

СОКРАЩЕНИЯ

ВМ	Виртуальная машина
ЗПС	Замкнутая программная среда
ОС	Операционная система
ПО	Программное обеспечение
РМ	Рабочее место
ЭЦП	Электронная цифровая подпись
API	Application Programming Interface (интерфейс прикладного программирования)
GSSAPI	Generic Security Services API (стандартизированный программный интерфейс для доступа к сервисам безопасности)
GTK	GIMP ToolKit (фреймворк элементов интерфейса)
IP	Internet Protocol (межсетевой протокол)
KVM	Kernel Virtual Machine (виртуальная машина на основе ядра, технология аппаратной виртуализации)
LTSC	Long-Term Servicing Channel (канал долгосрочного обслуживания продуктов)
QXL	Виртуальный графический процессор
SASL	Simple Authentication and Security Layer (фреймворк для аутентификации и обеспечения безопасности)
SPN	Service Principal Name (уникальный идентификатор экземпляра службы в сети)
SSH	Secure Shell Protocol (протокол защищенной передачи информации)

SSL	Secure Sockets Layer (криптографический протокол)
SSO	Single Sign-On (технология единого входа)
TCP	Transmission Control Protocol (протокол управления передачей)
TERA	Termidesk Remote Access protocol (протокол удаленного доступа разработкиООО «УВЕОН»)
TLS	Transport Layer Security (протокол защиты транспортного уровня)
UDP	User Datagram Protocol (протокол пользовательских датаграмм)
USB	Universal Serial Bus (последовательный интерфейс для подключения периферийных устройств)
WebDAV	Web Distributed Authoring and Versioning (расширение протокола HTTP, превращающее веб-сервер в сетевое хранилище)
Xorg	X.Org Server (сервер графической подсистемы X Window System)

СЛЕТ.10001-01 90 10. РУКОВОДСТВО АДМИНИСТРАТОРА. НАСТРОЙКА КОМПОНЕНТА «РЕТРАНСЛЯТОР»

ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ

Назначение документа

Настоящий документ является десятой частью руководства администратора на программный комплекс «Диспетчер подключений виртуальных рабочих мест Термидеск» (далее - Termidesk VDI, Termidesk VDI). Документ предназначен для администраторов системы и сети.

В этом руководстве приведено назначение, установка и настройка компонента «Ретранслятор». Для того чтобы получить информацию о месте компонента в программном комплексе, необходимо обратиться ко второй части руководства администратора - СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

Типографские соглашения

Приняты следующие типографские соглашения:

- `моноширинный шрифт` – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk VDI, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

РЕТРАНСЛЯТОР. ОБЩИЕ СВЕДЕНИЯ

Назначение «Ретранслятора»

Компонент «Ретранслятор» Termidesk VDI (далее - «Ретранслятор») - это программное обеспечение (ПО), предназначенное для сбора и фильтрации записей журналов, поступающих от компонентов Termidesk VDI, и их перенаправления в централизованное хранилище журналов или базу данных (БД).

Функции «Ретранслятора»:

- сбор данных (журналов событий) компонентов Termidesk VDI;
- обработка и преобразование данных;
- отправка результатов в централизованное хранилище.

Требования к аппаратному и программному обеспечению

Для установки минимальные аппаратные требования узла должны соответствовать следующим:

- процессор архитектуры x86-64 (AMD, Intel), не менее 4 шт.;
- оперативная память, не менее 4 ГБ;
- свободное дисковое пространство, не менее 1 ГБ;
- сетевое соединение, не менее 100 Мбит/с.

В среде функционирования должны быть предварительно установлены:

- операционная система (ОС) Astra Linux Special Edition версии 1.8 (1.8.1, 1.8.2, 1.8.3, 1.8.4, 1.8.5, 1.8.6);
- система управления БД (СУБД) PostgreSQL версии 15 из состава репозитория ОС Astra Linux Special Edition версии 1.8. Из внешних по отношению к ОС Astra Linux Special Edition версии 1.8 СУБД поддерживается СУБД PostgreSQL версии 12 и выше.

ОС Astra Linux Special Edition версии 1.8 должна быть установлена из `iso`-образа, доступного в личном кабинете на портале Astra Linux: https://lk.astra.ru/. Работа на преднастроенных образах ОС не гарантируется.

РЕТРАНСЛЯТОР. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ

Получение пакетов установки в ОС Astra Linux Special Edition

Дистрибутив представлен бинарным файлом пакета ПО в `deb`-формате. Установка в ОС Astra Linux Special Edition производится из локального репозитория, распространяемого в формате `iso`-образа.

Получить `iso`-образ можно двумя способами:

- заполнив запрос через сайт Termidesk VDI: https://termidesk.ru/support/#request-support;
- через личный кабинет:https://lk.astra.ru/.

Для подключения локального репозитория Termidesk VDI на узле, где предполагается установка, нужно:

- скопировать в домашний каталог пользователя образ диска `termidesk-<версия>.iso`;
- подключить образ диска к файловой системе в каталог `/mnt`:

```
sudo mount -o loop termidesk-<версия>.iso /mnt
```

где:

`-o loop` - параметры для привязки петлевого устройства (`/dev/loop`) к файлу `termidesk-<версия>.iso`, устройство затем монтируется в указанный каталог `/mnt`;

- скопировать содержимое каталога `repos` подключенного образа диска в каталог `/var` локальной файловой системы:

```
sudo cp -Rp /mnt/repos /var
```

где:

`-Rp` - ключ для рекурсивного копирования подкаталогов и файлов с сохранением исходных

свойств;

- отключить подключенный ранее образ диска от узла:

```
sudo umount /mnt
```

- установить пакет `lsb-release`:

```
sudo apt install -y lsb-release
```

- добавить локальный репозиторий Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list` через командный интерпретатор `sh`:
  - выяснить установленную версию ОС:

    ```
    sudo cat /etc/astra_version
    ```

  - определить актуальное имя каталога с пакетами в `/var/repos`;
  - указать в файле конфигурации APT корректное (фактическое) имя каталога:

    ```
    sudo sh -c 'echo "deb file:/var/repos/astra 1.8_x86-64 non-free" >
    /etc/apt/sources.list.d/termidesk_local.list'
    ```

    где:

    `-c` - ключ для чтения команд из вводимой строки (стандартный ввод);

    `echo` - команда вывода текста, совместно с символом «>» используется для перенаправления строки в файл;

    `deb file:/var/repos/astra 1.8_x86-64 non-free` - добавляемый репозиторий с вложенной командой получения версии ОС;

    Приведенный пример команды актуален для установки основных компонентов Termidesk, пакеты которых расположены в каталоге `1.8_x86-64`.

- для корректной установки компонентов TERA потребуется корректно подключить дополнительные репозитории и настроить их приоритет:
  - для версий ОС Astra Linux Special Edition меньше или равных 1.7.6, а также для версий 1.8.X:
    - подключить два репозитория:

      ```
      sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
      non-free" > /etc/apt/sources.list.d/termidesk_local.list'
      sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
      /dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
      ```

- добавить повышенный приоритет для репозитория с требуемой версией ОС (значение `$(cat /etc/astra_version)` может подходить не для всех репозиториев, т.к. версия может указываться без точек - в этом случае нужно вручную указать корректную версию):

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000
EOF"
```

- для версий ОС Astra Linux Special Edition 1.7.7 и 1.7.8:
  - подключить три репозитория:

```
sudo sh -c 'echo "deb file:/var/repos/astra 1.7.6 non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
/dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

  - настроить два приоритета:

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=1.7.6
Pin-Priority: 950

Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000

EOF"
```

- выполнить поиск ключа репозитория Termidesk VDI `GPG-KEY-PUBLIC` и добавить его:

```
sudo cat /var/repos/astra/GPG-KEY-PUBLIC | sudo gpg --dearmour -o
/etc/apt/trusted.gpg.d/termidesk.gpg
```

- убедиться, что ключ `release@uveon.ru` был успешно добавлен:

```
apt-key list
```

В случае, если ключ не отображен в выводе команды, необходимо убедиться, что ключ `GPG-KEY-PUBLIC` существует:

```
cat /var/repos/astra/GPG-KEY-PUBLIC
```

Если ключ все же существует, следует проверить правильность выполнения шагов по добавлению репозитория Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list`.

При успешном выполнении всех шагов команда выведет содержимое ключа в формате Base64.

В зависимости от используемой версии ОС команды добавления ключа репозитория Termidesk VDI могут отличаться. Если для ОС Astra Linux Special Edition 1.8 ключ репозитория был добавлен командой, применимой к другой версии ОС, то для исправления нужно:

- узнать идентификатор добавленного ключа репозитория:

```
apt-key list
```

- удалить ключ:

```
apt-key --keyring /etc/apt/trusted.gpg del 4E1632CC
```

где `4E1632CC` - последние 8 символов идентификатора ключа;

- вновь добавить ключ репозитория.

- обновить данные пакетного менеджера:

```
sudo apt update
```

- проверить настройку приоритетов репозиториев:

```
apt-cache policy
```

Команду `sudo apt update` необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.

РЕТРАНСЛЯТОР. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ

Подготовка среды функционирования для «Ретранслятора»

Перед установкой «Ретранслятора» должна быть предварительно подготовлена среда функционирования узла, а именно установлена и настроена система управления базами данных (СУБД) PostgreSQL.

Рекомендуется использовать отдельную инсталляцию СУБД для «Ретранслятора».

«Ретранслятор» может использовать ту же СУБД, что и ферма Termidesk

VDI, но имя БД должно быть отличным от уже существующего (termidesk).

Установка СУБД PostgreSQL осуществляется аналогично подразделу **Установка и настройка СУБД PostgreSQL** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса».

Для настройки БД следует перейти в интерфейс командной строки и выполнить:

- переключиться на пользователя postgres:

```
sudo su postgres
```

- запустить терминальный клиент СУБД PostgreSQL:

```
psql
```

Если после выполнения команды отображается ошибка «could not change directory to "/home/": Отказано в доступе» и не появляется приглашение командной строки postgres=, необходимо вместо su postgres использовать конструкцию su - postgres. Если приглашение postgres= появилось, то сообщение об ошибке можно проингорировать.

Если приглашение postgres=# не появляется, то вероятнее всего ОС Astra Linux Special Edition используется в более защищенном режиме, например, «Смоленск». В таком случае нужно для пользователя postgres назначить высокий уровень целостности:

```
sudo pdpl-user -i 63 postgres
```

- используя интерактивный интерфейс терминального клиента СУБД PostgreSQL, создать БД termidesk (символ ; в конце строки при работе с интерактивным интерфейсом обязателен):

```
postgres=# CREATE DATABASE fluentbit LC_COLLATE 'ru_RU.utf8' LC_CTYPE 'ru_RU.utf8'
TEMPLATE template0;
```

где:

LC_COLLATE - порядок сортировки для использования в БД, влияет на порядок сортировки, применяемый к строкам. Значение ru_RU.utf8 указывает на использование русской локализации;

LC_CTYPE - классификация символов для использования в БД, влияет на категоризацию символов;

TEMPLATE - имя шаблона, из которого создается БД. Шаблон template0 используется для системной БД самой СУБД PostgreSQL.

- создать пользователя fluentbit с паролем Password! для дальнейшего подключения к БД:

```
postgres=# CREATE USER fluentbit WITH PASSWORD 'Password!';
```

В приведенной команде имя пользователя и пароль используются в качестве примера. Имя пользователя и пароль должны задаваться в соответствии с внутренними стандартами организации по применению парольной защиты. Для задания пароля разрешено использовать только латинские буквы A-Z, a-z, цифры 0-9 и символы $!@%^&#_-=+~`;:.,?()*{}[]\|/.

- назначить права по использованию БД `fluentbit` созданному пользователю `fluentbit`:

```
postgres=# GRANT ALL PRIVILEGES ON DATABASE fluentbit TO fluentbit;
```

- в случае, если используется СУБД PostgreSQL из состава ОС Astra Linux Special Edition 1.8, то сделать пользователя `fluentbit` владельцем БД `fluentbit`, тем самым предоставив ему все возможные права:

```
postgres=# ALTER DATABASE fluentbit OWNER TO fluentbit;
```

- выйти из интерактивного интерфейса терминального клиента СУБД PostgreSQL:

```
postgres=# \q
```

- выйти из сеанса пользователя `postgres`:

```
exit
```

- отредактировать файл `/etc/parsec/mswitch.conf`, установив параметр `zero_if_notfound` в значение `yes`, точно соблюдая отступы и пробелы:

```
# Return zero data instead of ENOENT/ENODATA in the absence of record
zero_if_notfound: yes
```

- для пользователя `fluentbit` БД назначить классификационную метку:

```
sudo pdpl-user -i 0 fluentbit
```

- предоставить пользователю `fluentbit` права на чтение файла, содержащего классификационную метку:

```
sudo setfacl -m u:postgres:r /etc/parsec/macdb/$(id -u fluentbit)
```

- создать системного пользователя `fluentbit` (имя должно совпадать с именем пользователя в БД):

```
sudo useradd -M fluentbit -s /usr/sbin/nologin -d /home/fluentbit
```

В случае последующего обновления СУБД PostgreSQL может понадобиться пересоздать БД. В этом случае следует предусмотреть экспорт БД перед обновлением СУБД PostgreSQL.

ОС Astra Linux Special Edition

Установка «Ретранслятора» в ОС Astra Linux Special Edition

Для установки «Ретранслятора» нужно:

- подключить локальный репозиторий Termidesk VDI;
- выполнить:

```
sudo apt install termidesk-repeater
```

При установке пакета `termidesk-repeater` возможно активировать режим отладки инсталлятора через переменную окружения `TDSK_DEBUG` (например, `TDSK_DEBUG=1`).

После установки нужно:

- задать актуальные параметры подключения к БД в конфигурационном файле `fluent-bit.conf`;
- выполнить перезапуск службы:

```
sudo systemctl restart termidesk-repeater
```

- убедиться, что служба активна:

```
sudo systemctl status termidesk-repeater
```

Установка в режиме ЗПС

Замкнутая программная среда (ЗПС) является средством повышения безопасности ОС путем контроля целостности (неизменности) файлов.

Механизм контроля реализован в виде невыгружаемого модуля ядра ОС Astra Linux Special Edition (модуль `digsig_verif`), выполняющего проверку электронной цифровой подписи файлов (ЭЦП).

Перед установкой компонентов Termidesk VDI необходимо установить пакет `termidesk-digsig-keys`, для этого:

- подключить репозиторий Termidesk VDI или получить отдельный пакет `termidesk-digsig-keys` из репозитория;
- выполнить установку с использованием репозитория:

```
sudo apt -y install termidesk-digsig-keys
```

- либо выполнить установку из deb-пакета:

```
sudo apt install -y /home/user/termidesk-digsig-keys-XXXXXX_amd64.deb
```

где:

-y - ключ для пропуска подтверждения установки;

/home/user/termidesk-digsig-keys-XXXXXX_amd64.deb - расположение пакета termidesk-digsig-keys-XXXXXX_amd64.deb.

- перезагрузить ОС:

```
sudo reboot
```

- выполнить установку компонента Termidesk VDI.

Для ЗПС может быть активирован режим проверки встроенной ЭЦП в расширенных атрибутах (DIGSIG_XATTR_MODE). В этом случае потребуется подписать файлы, которые будут проходить проверку, имеющимися в организации ключами. Информация о процессе подписи и активации механизма проверки встроенной ЭЦП в расширенных атрибутах приведена в справочном центре Astra Linux: https://wiki.astralinux.ru/pages/viewpage.action?pageId=41190634.

Обновление «Ретранслятора» в ОС Astra Linux Special Edition

Обновление выполняется установкой новой версии поверх предыдущей.

Перед любым обновлением рекомендуется выполнить резервное копирование БД «Ретранслятора»:

```
pg_dump -d <наименование БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь> -W >
<имя_файла_для_сохранения_БД.sql>
```

где:

-d <наименование БД> - имя БД. Например, repeater;

-h <IP-адрес_хоста> - IP-адрес узла, где расположена БД. Если БД устанавливалась локально, нужно указать localhost;

-p <порт> - порт для подключения к БД. При стандартных настройках используется 5432;

-U <пользователь> - имя пользователя для подключения. При стандартных настройках используется имя termideskdb;

-W - запрос пароля для подключения к БД. При стандартных настройках при появлении запроса нужно указать ksedimret;

`<имя_файла_для_сохранения_БД.sql>` - имя и формат файла (`sql`) для сохранения БД.

Для обновления «Ретранслятора» нужно:

- подключить репозиторий Termidesk VDI;
- выполнить:

```
sudo apt install termidesk-repeater
```

Удаление «Ретранслятора» из ОС Astra Linux Special Edition

Для удаления нужно выполнить:

```
sudo apt purge termidesk-repeater
```

Для удаления БД следует выполнить следующие действия, строго соблюдая их последовательность:

- переключиться на пользователя `postgres` (через пользователя `root`):

```
sudo su postgres
```

- запустить терминальный клиент СУБД:

```
psql
```

- используя интерактивный интерфейс терминального клиента СУБД, удалить БД:

```
postgres=# DROP DATABASE fluentbit;
```

- выйти из интерактивного интерфейса терминального клиента СУБД:

```
postgres=# \q
```

- выйти из сеанса пользователя `postgres`:

```
exit
```

РЕТРАНСЛЯТОР. НАСТРОЙКИ

Конфигурационные файлы «Ретранслятора»

Конфигурационный файл fluent-bit.conf

Для настройки «Ретранслятора» используется основной конфигурационный файл /etc/opt/termidesk-repeater/fluent-bit.conf.

Конфигурационный файл структурирован по секциям, каждая из которых описывает определенный компонент конвейера данных:

- [SERVICE] - описываются глобальные настройки termidesk-repeater;
- [INPUT] - описываются настройки для получения входящих событий;
- [OUTPUT] - описываются настройки для сохранения обработанных событий.

Описание секций и параметров приведено в таблице (см. таблицу [Параметрыфайлаfluent-bit.conf]).

При изменении файла fluent-bit.conf потребуется перезапуск службы termidesk-repeater:

```
sudo systemctl restart termidesk-repeater
```

Пример конфигурационного файла:

```
[SERVICE]
    flush        1
    daemon       Off
    log_level    info
    parsers_file parsers.conf
    plugins_file plugins.conf
    http_server  Off
    http_listen  0.0.0.0
    http_port    2020
    storage.metrics on

[INPUT]
    Name              forward
    Listen            0.0.0.0
    Port              24224
    Buffer_Chunk_Size 1M
    Buffer_Max_Size   6M

[OUTPUT]
    Name                pgsql
    Match               *
    Host                127.0.0.1
    Port                5432
    User                fluentbit
    Password            Password!
    Database            fluentbit
    Table               logs
```

```
    Time_Key            timestamp
    Time_Format         %Y-%m-%d %H:%M:%S.%LZ
    min_pool_size       1
    max_pool_size       20
```

Таблица 279. Параметры файла `fluent-bit.conf`

Параметр	Значение по умолчанию	Описание
		Секция `[SERVICE]`
`flush`	1	Частота отправки данных (в секундах) из внутреннего буфера в выходные плагины
`daemon`	`Off`	Управление режимом работы в фоновом режиме
`log_level`	`info`	Уровень детализации журнала событий. Может быть: • `error`; • `warning`; • `info`; • `debug`
`parsers_file`	`parsers.conf`	Путь к конфигурационному файлу настройки обработчиков данных (парсеров). Можно задать несколько путей
`plugins_file`	`plugins.conf`	Путь к конфигурационному файлу настройки внешних расширений (плагинов)
`http_server`	`Off`	Управление режимом работы встроенного HTTP-сервера, предоставляющего API для мониторинга и управления. Возможные значения: • `on` - встроенный HTTP-сервер включен; • `off` - встроенный HTTP-сервер выключен
`http_listen`	`0.0.0.0`	IP-адрес прослушивания встроенного HTTP-сервера
`http_port`	`2020`	Порт встроенного HTTP-сервера
`storage.metrics`	`on`	Управление режимом сохранения в постоянное хранилище. Возможные значения: • `on` - «Ретранслятор» сохраняет внутренние метрики производительности в то же постоянное хранилище, что и обычные данные событий. Метрики будут экспортироваться только при включенном параметре `http_server`; • `off` - «Ретранслятор» не сохраняет внутренние метрики в постоянное хранилище
`storage.path`	`/tmp/storage`	По умолчанию параметр закомментирован. Абсолютный путь для хранения буферов данных файловой системы (chunk)

Параметр	Значение по умолчанию	Описание
storage.sync	normal	По умолчанию параметр закомментирован. Управление режимом синхронизации, используемого для хранения данных в файловой системе. Возможные значения: • normal; • full
storage.checksum	off	По умолчанию параметр закомментирован. Управление режимом проверки целостности данных при записи и чтении данных из файловой системы, используется алгоритм CRC32
storage.backlog.mem_limit	5M	По умолчанию параметр закомментирован. Максимальное значение памяти, используемое при обработке резервных данных. Резервные данные - это данные, которые не были отправлены и находятся на уровне хранилища. Такие данные проверяются, если задан и используется параметр storage.path
Секция [INPUT]		
Name	forward	Тип входного плагина. Значение forward используется для получения событий от других узлов «Ретранслятора»
Listen	0.0.0.0	IP-адрес прослушивания входящих событий. Значение 0.0.0.0 позволяет принимать соединения на всех интерфейсах
Port	24224	Порт прослушивания входящих событий
Buffer_Chunk_Size	1M	Размер буфера для хранения временных меток (chunk). Значение 1M зарезервировало 1 МБ для хранения данных
Buffer_Max_Size	6M	Максимальный размер буфера в случае очереди данных
Секция [OUTPUT]		
Name	pgsql	Определение типа выходного плагина. Значение pgsql указывает на отправку данных в СУБД PostgreSQL
Match	*	Указывает на тег и суффикс записи, обрабатываемой выходным плагином. Параметр используется для вывода событий с определенным тегом и суффиксом в другие системы. Формат: <тег>.<суффикс>. Значение * соответствует всем записям
Host	127.0.0.1	Адрес сервера СУБД PostgreSQL
Port	5432	Порт, на котором работает СУБД PostgreSQL
User	fluentbit	Имя пользователя для подключения к БД
Password	Password!	Пароль пользователя для подключения к БД
Database	fluentbit	Имя БД, в которую будут отправлены события
Table	logs	Название таблицы БД, в которую будут записываться события
Time_Key	timestamp	Ключ, под которым будет храниться временная метка

Параметр	Значение по умолчанию	Описание
Time_Format	%Y-%m-%d %H:%M:%S.%LZ	Формат временной метки
min_pool_size	1	Минимальный размер пула соединений
max_pool_size	20	Максимальный размер пула соединений

Конфигурационный файл parsers.conf

Конфигурационный файл /etc/opt/termidesk-repeater/parsers.conf предназначен для определения и управления обработчиками (парсерами) журналов. Обработчики необходимы для преобразования неструктурированных записей журнала в структурированный формат, что упрощает их обработку, фильтрацию и анализ.

Пример файла:

```
[PARSER]
    Name   apache
    Format regex
    Regex  ^(?<host>[^ ]*) [^ ]* (?<user>[^ ]*) \[(?<time>[^\]]*)\]
"(?<method>\S+)(?: +(?<path>[^\"]*?)(?: +\S*)?)?" (?<code>[^ ]*) (?<size>[^ ]*)(?:
"(?<referer>[^\"]*)" "(?<agent>[^\"]*)")?$
    Time_Key time
    Time_Format %d/%b/%Y:%H:%M:%S %z

[PARSER]
    Name   apache2
    Format regex
    Regex  ^(?<host>[^ ]*) [^ ]* (?<user>[^ ]*) \[(?<time>[^\]]*)\]
"(?<method>\S+)(?: +(?<path>[^ ]*) +\S*)?" (?<code>[^ ]*) (?<size>[^ ]*)(?:
"(?<referer>[^\"]*)" "(?<agent>.*)")?$
    Time_Key time
    Time_Format %d/%b/%Y:%H:%M:%S %z

[PARSER]
    Name   apache_error
    Format regex
    Regex  ^\[[^ ]* (?<time>[^\]]*)\] \[(?<level>[^\]]*)\](?: \[pid
(?<pid>[^\]]*)\])?( \[client (?<client>[^\]]*)\])? (?<message>.*)$

[PARSER]
    Name   nginx
    Format regex
    Regex ^(?<remote>[^ ]*) (?<host>[^ ]*) (?<user>[^ ]*) \[(?<time>[^\]]*)\]
"(?<method>\S+)(?: +(?<path>[^\"]*?)(?: +\S*)?)?" (?<code>[^ ]*) (?<size>[^ ]*)(?:
"(?<referer>[^\"]*)" "(?<agent>[^\"]*)")
    Time_Key time
    Time_Format %d/%b/%Y:%H:%M:%S %z

[PARSER]
```

```
    # https://rubular.com/r/IhIbCAIs7ImOkc
    Name        k8s-nginx-ingress
    Format      regex
    Regex       ^(?<host>[^ ]*) - (?<user>[^ ]*) \[(?<time>[^\]]*)\]
"(?<method>\S+)(?: +(?<path>[^\"]*?)(?: +\S*)?)?" (?<code>[^ ]*) (?<size>[^ ]*)
"(?<referer>[^\"]*)" "(?<agent>[^\"]*)" (?<request_length>[^ ]*) (?<request_time>[^
]*) \[(?<proxy_upstream_name>[^ ]*)\] (\[(?<proxy_alternative_upstream_name>[^
]*)\] )?(?<upstream_addr>[^ ]*) (?<upstream_response_length>[^ ]*)
(?<upstream_response_time>[^ ]*) (?<upstream_status>[^ ]*) (?<reg_id>[^ ]*).*$
    Time_Key    time
    Time_Format %d/%b/%Y:%H:%M:%S %z

[PARSER]
    Name   json
    Format json
    Time_Key time
    Time_Format %d/%b/%Y:%H:%M:%S %z

[PARSER]
    Name   logfmt
    Format logfmt

[PARSER]
    Name         docker
    Format       json
    Time_Key     time
    Time_Format  %Y-%m-%dT%H:%M:%S.%L
    Time_Keep    On
    # --
    # Since Fluent Bit v1.2, if you are parsing Docker logs and using
    # the Kubernetes filter, it's not longer required to decode the
    # 'log' key.
    #
    # Command      |  Decoder | Field | Optional Action
    # =============|==================|=================
    #Decode_Field_As    json     log

[PARSER]
    Name        docker-daemon
    Format      regex
    Regex       time="(?<time>[^ ]*)" level=(?<level>[^ ]*) msg="(?<msg>[^ ].*)"
    Time_Key    time
    Time_Format %Y-%m-%dT%H:%M:%S.%L
    Time_Keep   On

[PARSER]
    Name        syslog-rfc5424
    Format      regex
    Regex       ^\<(?<pri>[0-9]{1,5})\>1 (?<time>[^ ]+) (?<host>[^ ]+) (?<ident>[^
```

```
]+) (?<pid>[-0-9]+) (?<msgid>[^ ]+) (?<extradata>(\[(.*?)\]|-)) (?<message>.+)$
    Time_Key    time
    Time_Format %Y-%m-%dT%H:%M:%S.%L%z
    Time_Keep   On

[PARSER]
    Name        syslog-rfc3164-local
    Format      regex
    Regex       ^\<(?<pri>[0-9]+)\>(?<time>[^ ]* {1,2}[^ ]* [^ ]*) (?<ident>[a-zA-
Z0-9_\/\.\-]*)(?:\[(?<pid>[0-9]+)\])?(?:[^\:]*\:)? *(?<message>.*)$
    Time_Key    time
    Time_Format %b %d %H:%M:%S
    Time_Keep   On

[PARSER]
    Name        syslog-rfc3164
    Format      regex
    Regex       /^\<(?<pri>[0-9]+)\>(?<time>[^ ]* {1,2}[^ ]* [^ ]*) (?<host>[^ ]*)
(?<ident>[a-zA-Z0-9_\/\.\-]*)(?:\[(?<pid>[0-9]+)\])?(?:[^\:]*\:)? *(?<message>.*)$/
    Time_Key    time
    Time_Format %b %d %H:%M:%S
    Time_Keep   On

[PARSER]
    Name    mongodb
    Format  regex
    Regex   ^(?<time>[^ ]*)\s+(?<severity>\w)\s+(?<component>[^
]+)\s+\[(?<context>[^\]]+)]\s+(?<message>.*?) *(?<ms>(\d+))?(:?ms)?$
    Time_Format %Y-%m-%dT%H:%M:%S.%L
    Time_Keep   On
    Time_Key time

[PARSER]
    # https://rubular.com/r/0VZmcYcLWMGAp1
    Name    envoy
    Format  regex
    Regex ^\[(?<start_time>[^\]]*)\] "(?<method>\S+)(?: +(?<path>[^\"]*?)(?:
+\S*)?)? (?<protocol>\S+)" (?<code>[^ ]*) (?<response_flags>[^ ]*)
(?<bytes_received>[^ ]*) (?<bytes_sent>[^ ]*) (?<duration>[^ ]*)
(?<x_envoy_upstream_service_time>[^ ]*) "(?<x_forwarded_for>[^ ]*)"
"(?<user_agent>[^\"]*)" "(?<request_id>[^\"]*)" "(?<authority>[^ ]*)"
"(?<upstream_host>[^ ]*)"
    Time_Format %Y-%m-%dT%H:%M:%S.%L%z
    Time_Keep   On
    Time_Key start_time

[PARSER]
    # https://rubular.com/r/hbsTIxFFMozLmh
    Name    istio-envoy-proxy
```

```
    Format  regex
    Regex ^\[(?<start_time>[^\]]*)\] "(?<method>\S+)(?: +(?<path>[^\"]*?)(?:
+\S*)?)? (?<protocol>\S+)" (?<response_code>[^ ]*) (?<response_flags>[^ ]*)
(?<response_code_details>[^ ]*) (?<connection_termination_details>[^ ]*)
"(?<upstream_transport_failure_reason>[^ ]*)" (?<bytes_received>[^ ]*)
(?<bytes_sent>[^ ]*) (?<duration>[^ ]*) (?<x_envoy_upstream_service_time>[^ ]*)
"(?<x_forwarded_for>[^ ]*)" "(?<user_agent>[^\"]*)" "(?<x_request_id>[^\"]*)"
"(?<authority>[^ ]*)" "(?<upstream_host>[^ ]*)" (?<upstream_cluster>[^ ]*)
(?<upstream_local_address>[^ ]*) (?<downstream_local_address>[^ ]*)
(?<downstream_remote_address>[^ ]*) (?<requested_server_name>[^ ]*)
(?<route_name>[^  ]*)$
    Time_Format %Y-%m-%dT%H:%M:%S.%L%z
    Time_Keep   On
    Time_Key start_time

[PARSER]
    # http://rubular.com/r/tjUt3Awgg4
    Name cri
    Format regex
    Regex ^(?<time>[^ ]+) (?<stream>stdout|stderr) (?<logtag>[^ ]*) (?<message>.*)$
    Time_Key    time
    Time_Format %Y-%m-%dT%H:%M:%S.%L%z
    Time_Keep   On

[PARSER]
    Name    kube-custom
    Format  regex
    Regex   (?<tag>[^.]+)?\.?(?<pod_name>[a-z0-9](?:[-a-z0-9]*[a-z0-9])?(?:\.[a-z0-
9]([-a-z0-9]*[a-z0-9])?)*)_(?<namespace_name>[^_]+)_(?<container_name>.+)-
(?<docker_id>[a-z0-9]{64})\.log$

[PARSER]
    # Examples: TCP: https://rubular.com/r/Q8YY6fHqlqwGI0  UDP:
https://rubular.com/r/B0ID69H9FvN0tp
    Name    kmsg-netfilter-log
    Format  regex
    Regex   ^\<(?<pri>[0-9]{1,5})\>1 (?<time>[^ ]+) (?<host>[^ ]+) kernel - - -
\[[0-9\.]*\] (?<logprefix>[^ ]*)\s?IN=(?<in>[^ ]*) OUT=(?<out>[^ ]*)
MAC=(?<macsrc>[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-
f]{2}):(?<macdst>[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-f]{2}:[0-9a-
f]{2}):(?<ethtype>[0-9a-f]{2}:[0-9a-f]{2}) SRC=(?<saddr>[^ ]*) DST=(?<daddr>[^ ]*)
LEN=(?<len>[^ ]*) TOS=(?<tos>[^ ]*) PREC=(?<prec>[^ ]*) TTL=(?<ttl>[^ ]*)
ID=(?<id>[^ ]*) (D*F*)\s*PROTO=(?<proto>[^ ]*)\s?((SPT=)?(?<sport>[0-
9]*))\s?((DPT=)?(?<dport>[0-9]*))\s?((LEN=)?(?<protolen>[0-
9]*))\s?((WINDOW=)?(?<window>[0-9]*))\s?((RES=)?(?<res>0?x?[0-9]*))\s?(?<flag>[^
]*)\s?((URGP=)?(?<urgp>[0-9]*))
    Time_Key  time
    Time_Format  %Y-%m-%dT%H:%M:%S.%L%z
```

Конфигурационный файл plugins.conf

Конфигурационный файл /etc/opt/termidesk-repeater/plugins.conf предназначен для определения и загрузки внешних или пользовательских плагинов. По умолчанию после установки никакие внешние плагины не подключены.

РЕТРАНСЛЯТОР. ЖУРНАЛИРОВАНИЕ

Для просмотра журнала «Ретранслятора» можно выполнить:

```
sudo journalctl -f -u termidesk-repeater.service
```

или:

```
sudo less /var/log/syslog
```

РЕТРАНСЛЯТОР. НЕШТАТНЫЕ СИТУАЦИИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

Возможные неисправности при работе с «Ретранслятором» и способы их устранения приведены в таблице (см. таблицу Перечень возможных нештатных ситуаций и способов их устранения).

Таблица 280. Перечень возможных нештатных ситуаций и способов их устранения

Индикация	Описание	Возможное решение

Статус службы termidesk-repeater отображается как failed	«Ретранслятор» не запускается:
	• статус службы termidesk-repeater отображается как failed;
	• в журнале отображаются сообщения:
	`termidesk-repeater.service: Failed with result 'exit-code'. Failed to start termidesk-repeater.service - Termidesk Repeater.`
		Для работы «Ретранслятор» требуется указать актуальные параметры подключения к БД в конфигурационном файле fluent-bit.conf.
		Для исправления ситуации:
		• задать актуальные параметры подключения к БД в конфигурационном файле fluent-bit.conf;
		• выполнить перезапуск службы:
		`sudo systemctl restart termidesk-repeater`
		• убедиться, что служба активна:
		`sudo systemctl status termidesk-repeater`

ТЕРМИНЫ

Ферма Termidesk VDI

Ферма, объединяющая установку основных узлов Termidesk VDI, взаимодействующих с

одной БД

СОКРАЩЕНИЯ

БД	База данных
ПО	Программное обеспечение
ОС	Операционная система
СУБД	Система управления базами данных
IP	Internet Protocol (межсетевой протокол)
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста)
HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
API	Application Programming Interface (интерфейс прикладного программирования)

СЛЕТ.10001-01 90 11. РУКОВОДСТВО АДМИНИСТРАТОРА. УСТАНОВКА И НАСТРОЙКА TERMIDESK PROFILES

ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ

Назначение документа

Настоящий документ является руководством администратора Termidesk Profiles. Документ предназначен для администраторов системы и сети.

В документе приведено назначение, установка и конфигурирование Termidesk Profiles.

Типографские соглашения

Приняты следующие типографские соглашения:

- `моноширинный шрифт` – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk VDI, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

TERMIDESK PROFILES. ОБЩИЕ СВЕДЕНИЯ

Назначение Termidesk Profiles

Termidesk Profiles обеспечивает создание и использование образов дисков с пользовательскими данными и настройками рабочего места (Перемещаемый Профиль). Перемещаемый Профиль хранится в централизованном хранилище и обеспечивает перенос рабочего окружения между устройствами.

Termidesk Profiles включают в себя серверную и агентскую части.

Требования к аппаратному и программному обеспечению

Для установки серверной части Termidesk Profiles минимальные аппаратные и программные требования узла должны соответствовать следующим:

- процессор архитектуры Intel x86 с разрядностью 64 бит;
- оперативная память, не менее 8 ГБ;
- свободное дисковое пространство, не менее 1 ГБ;
- сетевое соединение, не менее 100 Мбит/с.

Серверная часть Termidesk Profiles устанавливается на операционную систему (ОС):

- Astra Linux Special Edition 1.8 (минимальная версия - 1.8.4).

Для установки агентской части Termidesk Profiles минимальные аппаратные требования

узла должны соответствовать следующим:

- процессор архитектуры Intel x86 с разрядностью 64 бит;
- оперативная память, не менее 1 ГБ;
- свободное дисковое пространство, не менее 200 МБ;
- сетевое соединение, не менее 100 Мбит/с.

Агентская часть Termidesk Profiles устанавливается на ОС:

- Astra Linux Special Edition 1.8 (минимальная версия - 1.8.4).

TERMIDESK PROFILES. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ

Получение пакетов установки через Интернет-репозиторий

Для получения пакетов установки может использоваться Интернет-репозиторий: https://repos.termidesk.ru/.

Для подключения репозитория в ОС Astra Linux Special Edition нужно:

- установить пакеты:

```
sudo apt install -y lsb-release wget apt-transport-https debian-keyring
```

где:

`-y` - ключ для пропуска подтверждения установки;

- добавить Интернет-репозиторий Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list` через командный интерпретатор `sh`:
  - выяснить установленную версию ОС:

    ```
    sudo cat /etc/astra_version
    ```

  - определить актуальное имя каталога с пакетами в `https://repos.termidesk.ru/astra`;
  - указать в файле конфигурации APT корректное (фактическое) имя каталога:

    ```
    sudo sh -c 'echo "deb https://repos.termidesk.ru/astra 1.8_x86-64 non-free" >
    /etc/apt/sources.list.d/termidesk_local.list'
    ```

    где:

    `-c` - ключ для чтения команд из вводимой строки (стандартный ввод);

    `echo` - команда вывода текста, совместно с символом «>» используется для перенаправления строки в файл;

    `deb https://repos.termidesk.ru/astra <···>` - добавляемый репозиторий;

    Приведенный пример команды актуален для установки основных

компонентов Termidesk, пакеты которых расположены в каталоге `1.8_x86-64`.

- для корректной установки компонентов TERA потребуется корректно подключить дополнительные репозитории и настроить их приоритет:
  - для версий ОС Astra Linux Special Edition меньше или равных 1.7.6, а также для версий 1.8.X:
    - подключить два репозитория:

```
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(cat
/etc/astra_version) non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(lsb_release -cs
2> /dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

    - добавить повышенный приоритет для репозитория с требуемой версией ОС (значение `$(cat /etc/astra_version)` может подходить не для всех репозиториев, т.к. версия может указываться без точек - в этом случае нужно вручную указать корректную версию):

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000
EOF"
```

  - для версий ОС Astra Linux Special Edition 1.7.7 и 1.7.8:
    - подключить три репозитория:

```
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra 1.7.6 non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(cat
/etc/astra_version) non-free" >>
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(lsb_release -cs
2> /dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

    - настроить два приоритета:

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=1.7.6
Pin-Priority: 950

Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000
```

```
EOF"
```

- получить ключ репозитория Termidesk VDI `GPG-KEY-PUBLIC` и добавить его в ОС:
  - для ОС Astra Linux Special Edition 1.7:

```
wget --no-check-certificate -qO - https://repos.termidesk.ru/astra/GPG-KEY-PUBLIC | sudo apt-key add -
```

  - для ОС Astra Linux Special Edition 1.8:

```
wget --no-check-certificate -qO - https://repos.termidesk.ru/astra/GPG-KEY-PUBLIC |  sudo gpg --dearmour -o /etc/apt/trusted.gpg.d/termidesk.gpg
```

- обновить данные пакетного менеджера:

```
sudo apt update
```

- проверить настройку приоритетов репозиториев:

```
apt-cache policy
```

Команду `sudo apt update` необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.

Команды добавления ключа репозитория Termidesk VDI отличаются в зависимости от используемой версии ОС.

Если для ОС Astra Linux Special Edition 1.8 ключ репозитория был добавлен командой, применимой к другой версии ОС, то для исправления нужно:

- узнать идентификатор добавленного ключа репозитория:

```
apt-key list
```

- удалить ключ:

```
apt-key --keyring /etc/apt/trusted.gpg del 4E1632CC
```

где `4E1632CC` - последние 8 символов идентификатора ключа;

- вновь добавить ключ репозитория.

TERMIDESK PROFILES. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ

Подготовка среды функционирования

Установка и настройка СУБД PostgreSQL

Установка СУБД PostgreSQL

Перед установкой серверной части Termidesk Profiles должна быть предварительно подготовлена среда функционирования узла, а именно установлена и настроена система управления базами данных (СУБД) PostgreSQL.

> Рекомендуется использовать отдельную БД для серверной части Termidesk Profiles и не использовать БД Termidesk VDI.
>
> Серверная часть Termidesk Profiles может использовать ту же СУБД, что и Termidesk VDI, но имя БД должно быть отличным от уже существующего (`termidesk`).

Для установки СУБД PostgreSQL нужно:

- отредактировать файл `/etc/apt/sources.list`, оставив в качестве источников получения пакетов сетевые репозитории. Пример файла `/etc/apt/sources.list` для ОС Astra Linux Special Edition 1.8:

> Приведен только пример файла! Он должен быть скорректирован, исходя из используемой и поддерживаемой версии ОС. Подробную информацию о сетевых репозиториях ОС Astra Linux Special Edition можно получить в справочном центре Astra Linux для ОС Astra Linux Special Edition 1.8: https://wiki.astralinux.ru/pages/viewpage.action?pageId=302043111.
>
> Если в файле `/etc/apt/sources.list` присутствует репозиторий `astra-ce`, то необходимо закомментировать его, чтобы избежать установки несовместимых версий пакетов.

```
deb https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-main/
1.8_x86-64 main contrib non-free
deb https://download.astralinux.ru/astra/stable/1.8_x86-64/repository-extended/
1.8_x86-64 main contrib non-free
```

- перейти в интерфейс командной строки и обновить списков пакетов:

```
sudo apt update
```

- установить СУБД PostgreSQL. Команда установки выбирается в зависимости от того, требуется ли использование СУБД Tantor Basic Edition:
  - с СУБД Tantor Basic Edition:

```
sudo apt install -y postgresql
```

> Начиная с версии ОС Astra Linux Special Edition 1.8.0 при

> подключенных основном и расширенном репозиториях данная команда устанавливает СУБД Tantor Basic Edition, лицензия на которую приобретается отдельно.

- без СУБД Tantor Basic Edition:

```
sudo apt install -y tantor-free-server-16
```

Где:

`-y` - ключ для пропуска подтверждения установки.

Настройка СУБД PostgreSQL

Для настройки БД нужно:

- отредактировать файл `/etc/postgresql/15/main/postgresql.conf`, задать соответствующее значение параметру `listen_address`:

```
# Для приема подключений на всех сетевых интерфейсах
listen_addresses = '0.0.0.0'

# Для приема подключений только с указанного IP-адреса
listen_addresses = '<IP-адрес_серверной_части_Termidesk_Profiles>'
```

- для ограничения доступа к СУБД PostgreSQL по сети нужно отредактировать файл `/etc/postgresql/15/main/pg_hba.conf`, приведя его к виду:

```
host    all             all             192.80.255.0/16          scram-sha-256
```

Где:

`192.80.255.0/16` - сеть серверной части Termidesk Profiles.

- затем следует перейти в интерфейс командной строки и переключиться на пользователя `postgres`:

```
sudo su postgres
```

- запустить терминальный клиент СУБД PostgreSQL:

```
psql
```

> Если после выполнения команды отображается ошибка «could not change directory to "/home/": Отказано в доступе» и не появляется приглашение командной строки `postgres=`, необходимо вместо `su postgres` использовать конструкцию `su - postgres`. Если приглашение `postgres=` появилось, то сообщение об ошибке можно проингорировать.

> Если приглашение postgres=# не появляется, то вероятнее всего ОС Astra Linux Special Edition используется в более защищенном режиме, например, «Смоленск». В таком случае нужно для пользователя postgres назначить высокий уровень целостности:
>
> ```
> sudo pdpl-user -i 63 postgres
> ```

- используя интерактивный интерфейс терминального клиента СУБД PostgreSQL, создать БД trp_base01 (символ ; в конце строки при работе с интерактивным интерфейсом обязателен):

```
CREATE DATABASE trp_base01 LC_COLLATE 'ru_RU.utf8' LC_CTYPE 'ru_RU.utf8' TEMPLATE
template0;
```

Где:

LC_COLLATE - порядок сортировки для использования в БД, влияет на порядок сортировки, применяемый к строкам. Значение ru_RU.utf8 указывает на использование русской локализации;

LC_CTYPE - классификация символов для использования в БД, влияет на категоризацию символов;

TEMPLATE - имя шаблона, из которого создается БД. Шаблон template0 используется для системной БД самой СУБД PostgreSQL;

- создать пользователя termidesktrp с паролем ksedimret для дальнейшего подключения к БД:

```
CREATE USER termidesktrp WITH PASSWORD 'ksedimret';
```

> В приведенной команде имя пользователя и пароль используются в качестве примера. Имя пользователя и пароль должны задаваться в соответствии с внутренними стандартами организации по применению парольной защиты. Для задания пароля разрешено использовать только латинские буквы A-Z, a-z, цифры 0-9 и символы $!@%^&#_-=+~`;:.,?()*{}[]\|/.

- предоставить пользователю termidesktrp права доступа ко всем таблицам схемы public:

```
GRANT ALL ON ALL TABLES IN SCHEMA public TO termidesktrp;
```

- настроить автоматическое предоставление прав пользователю termidesktrp на таблицы, создаваемые в схеме public:

```
ALTER DEFAULT PRIVILEGES IN SCHEMA public GRANT ALL ON TABLES TO termidesktrp;
```

- назначить права по использованию БД trp_base01 пользователю termidesktrp:

```
GRANT ALL PRIVILEGES ON DATABASE trp_base01 TO termidesktrp;
```

- сделать пользователя `termidesktrp` владельцем БД `trp_base01`, тем самым предоставив ему все возможные права:

```
ALTER DATABASE trp_base01 OWNER TO termidesktrp;
```

- выйти из интерактивного интерфейса терминального клиента СУБД PostgreSQL:

```
\q
```

- выйти из сеанса пользователя `postgres`:

```
exit
```

- отредактировать файл `/etc/parsec/mswitch.conf`, установив параметр `zero_if_notfound` в значение `yes`, точно соблюдая отступы и пробелы:

```
# Return zero data instead of ENOENT/ENODATA in the absence of record
zero_if_notfound: yes
```

В случае последующего обновления СУБД PostgreSQL может понадобиться пересоздать БД. В этом случае следует предусмотреть экспорт БД перед обновлением СУБД PostgreSQL.

Установка и настройка NFS-хранилища

Перед установкой серверной части Termidesk Profiles нужно выполнить предварительную установку и настройку NFS-хранилища для хранения данных Перемещаемых Профилей.

Для установки NFS-хранилища нужно выполнить:

```
sudo apt install nfs-kernel-server
```

Для настройки NFS-хранилища нужно:

- определить диск для хранения данных. Просмотреть список дисков и их разделов можно, выполнив команду:

  ```
  sudo fdisk -l
  ```

- в результате выполнения команды будет отображен список доступных дисков и их разделов:

```
Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
  ... (Existing OS disk)

  Disk /dev/sdb: 100 GiB, 107374182400 bytes, 209715200 sectors
  Units: sectors of 1 * 512 = 512 bytes
  Sector size (logical/physical): 512 bytes / 512 bytes
  I/O size (minimum/optimal): 512 bytes / 512 bytes
```

Где:

`/dev/sdb` - диск, который в дальнейшем будет использован для хранения данных;

Наименование диска `/dev/sdb` приведено в качестве примера и должно быть заменено на имя диска, используемого в инфраструктуре NFS-хранилища.

- создать раздел на диске `/dev/sdb`:

```
sudo fdisk /dev/sdb
```

- в интерфейсе утилиты `fdisk` выполнить следующие действия:
  - нажать клавишу **<n>** для создания раздела;
  - нажать клавишу **<p>** для создания основного раздела;
  - указать номер раздела, нажав соответствующую клавишу на цифровом блоке клавиатуры;
  - указать значение начального сектора раздела и нажать клавишу **<Enter>**. Для принятия значения по умолчанию (2048) нажать клавишу **<Enter>** без указания значения;
  - указать значение конечного сектора раздела и нажать клавишу **<Enter>**. Для использования всего доступного пространства диска нажать клавишу **<Enter>** без указания значения;
  - убедиться в создании раздела на диске, нажав клавишу **<p>**. Наличие значения `/dev/sdb1` в интерфейсе утилиты свидетельствует об успешном создании раздела;
  - нажать клавишу **<w>** для записи изменений на диске и выхода из утилиты `fdisk`. Для выхода без сохранения изменений нажать клавишу **<q>**;
- после завершения работы утилиты `fdisk` раздел должен быть автоматически обнаружен системой. Если раздел не обнаружен, обновить таблицу разделов командой:

```
sudo partprobe
```

- в созданном разделе `/dev/sdb1` нужно создать файловую систему, для этого выполнить:

```
sudo mkfs.xfs /dev/sdb1
```

Где:

`xfs` - тип файловой системы;

`/dev/sdb1` - раздел диска, на котором создается файловая система;

Наименование раздела `/dev/sdb1` приведено в качестве примера и должно быть заменено на имя раздела, используемого в инфраструктуре NFS-хранилища.

- затем создать каталог точки монтирования:

```
sudo mkdir /trp_share
```

Где:

`/trp_share` - наименование каталога точки монтирования;

- временно смонтировать раздел `/dev/sdb1` в каталог монтирования `/trp_share`:

```
sudo mount /dev/sdb1 /trp_share
```

- убедиться, что диск смонтирован:

```
df -h
```

- отображение раздела `/dev/sdb1` и каталога `/trp_share` в выводе команды `df -h` свидетельствует об успешном монтировании диска;
- для автоматического монтирования диска при загрузке ОС нужно определить UUID раздела `/dev/sdb1`:

```
sudo blkid
```

- полученное значение внести в файл `/etc/fstab`. Пример содержимого файла:

```
UUID=a1b2c3d4-e5f6-7890-1234-567890abcdef /trp_share ext4 defaults 0 2
```

Где:

`UUID` - уникальный идентификатор раздела;

`/trp_share` - каталог монтирования;

`ext4` - тип файловой системы;

`defaults` - использование стандартных параметров монтирования;

`0` - параметр отключения резервного копирования;

`2` - параметр проверки файловой системы при загрузке;

- убедиться, что записи в файле /etc/fstab внесены корректно. Для этого размонтировать раздел, если он был смонтирован ранее:

```
sudo umount /trp_share
```

- выполнить монтирование всех файловых систем, указанных в файле /etc/fstab:

```
sudo mount -a
```

- отсутствие ошибок в выводе команды mount -a свидетельствует о корректных записях в файле /etc/fstab;
- далее задать владельца (nobody) и идентификатор группы (nogroup) каталога монтирования:

```
sudo chown -R nobody:nogroup /trp_share
```

Где:

-R - ключ для рекурсивного применения свойств для каталога и его содержимого;

Для корректного применения прав к каталогу /trp_share их следует назначать после монтирования.

- затем предоставить общий доступ к каталогу /trp_share:

```
/trp_share 192.80.255.0/16(rw,sync,no_subtree_check,no_root_squash,all_squash)
```

Где:

/trp_share - каталог общего доступа;

192.80.255.0/16 - сеть, из которой разрешен доступ к каталогу;

rw - разрешение на запись и чтение данных каталога;

sync - синхронная запись данных;

no_subtree_check - отключение проверки подкаталогов;

no_root_squash - сохранение прав привилегированного пользователя при подключении к каталогу;

all_squash - сопоставление всех пользователей к анонимному пользователю при подключении к каталогу.

ОС Astra Linux Special Edition

Установка серверной части в ОС Astra Linux Special Edition

Серверная часть Termidesk Profiles устанавливается на отдельно подготовленный узел.

Перед установкой необходимо подключить локальный репозиторий Termidesk, как указано в подразделе **Получение пакетов установки в ОС Astra Linux Special Edition**.

Для установки серверной части Termidesk Profiles выполнить:

```
sudo apt install trp-server
```

Установку можно также выполнить из `deb`-пакета без подключения репозитория командой:

```
sudo apt install /home/user/trp-server_XXX_amd64.deb
```

Где:

`/home/user/trp-server_XXX_amd64.deb` - путь к пакету установки.

Затем нужно создать файл `/etc/default/trp-server`. Подробное описание файла приведено в подразделе **Файл `/etc/default/trp-server`**.

После установки серверной части автоматически запускается и добавляется в автозагрузку ОС служба `trp-server`.

Проверка состояния службы выполняется командой:

```
sudo systemctl status trp-server
```

Строка `Active` отображает состояние сервиса, где статус `active (running)` означает успешный запуск.

Для ручного перезапуска службы выполнить:

```
sudo systemctl restart trp-server
```

Обновление серверной части в ОС Astra Linux Special Edition

Обновление серверной части Termidesk Profiles выполняется установкой новой версии поверх предыдущей.

Удаление серверной части в ОС Astra Linux Special Edition

Для удаления серверной части Termidesk Profiles из среды ОС Astra Linux Special Edition выполнить:

```
sudo apt purge -y trp-server
```

Где:

`-y` - ключ для пропуска подтверждения удаления.

После этого необходимо очистить оставшиеся зависимости и конфигурации:

```
sudo apt purge ~c -y
```

Команда полностью удалит оставшиеся настройки и зависимости.

Для удаления БД и роли пользователя следует выполнить следующие действия, строго соблюдая их последовательность:

- переключиться на пользователя `postgres` (через пользователя `root`):

  ```
  sudo su postgres
  ```

- запустить терминальный клиент СУБД:

  ```
  psql
  ```

- используя интерактивный интерфейс терминального клиента СУБД, удалить БД:

  ```
  DROP DATABASE trp_base01;
  ```

- удалить роль пользователя БД:

  ```
  DROP ROLE termidesktrp;
  ```

- выйти из интерактивного интерфейса терминального клиента СУБД:

  ```
  \q
  ```

- выйти из сеанса пользователя `postgres`:

  ```
  exit
  ```

- удалить оставшийся каталог с файлами:

  ```
  sudo rm -R /opt/termidesk/trp-server/
  ```

  Где:

  `-R` - ключ для рекурсивного действия. Будут удалены все вложенные подкаталоги.

Установка агентской части в ОС Astra Linux Special Edition

Агентская часть Termidesk Profiles устанавливается в гостевую ОС РМ.

Перед установкой необходимо подключить локальный репозиторий Termidesk, как указано в подразделе **Получение пакетов установки в ОС Astra Linux Special Edition**.

Для установки агентской части Termidesk Profiles выполнить:

```
sudo apt install trp-agent
```

Установку можно также выполнить из `deb`-пакета без подключения репозитория командой:

```
sudo apt install /home/user/trp-agent_XXX_amd64.deb
```

Где:

`/home/user/trp-agent_XXX_amd64.deb` - путь к пакету установки.

После установки агентской части нужно:

- остановить службу `trp-agent`:

  ```
  sudo systemctl stop trp-agent
  ```

- убедиться, что в PAM включен модуль создания директории `mkhomedir`:

  ```
  grep pam_mkhomedir /etc/pam.d/common-session
  ```

- убедиться, что результат выполнения команды содержит строку:

  ```
  session required pam_mkhomedir.so umask=0022 skel /etc/skel
  ```

- если в результате выполнения команды отобразилась пустая строка, то:
  - отредактировать файл `/etc/pam.d/common-session`, добавив строку:

    ```
    session required pam_mkhomedir.so umask=0022 skel /etc/skel
    ```

  - убедиться, что в файле теперь содержатся строки:

    ```
    session required pam_mkhomedir.so umask=0022 skel /etc/skel
    session required        pam_unix.so
    ```

- добавить `pam_trp` в конец файла `/etc/pam.d/common-session`:

```
session optional pam_exec.so log=/var/log/termidesk/trp/mount.log
/opt/termidesk/trp-agent/sbin/pam_trp
```

- выполнить настройку запуска агентской части (см. подраздел **Параметры конфигурирования агентской части**);
- при использовании защищенного подключения к серверной части по протоколу HTTPS убедиться, что сертификат центра сертификации, выдавший сертификат сервера, является доверенным и содержится в файле `/etc/ssl/certs/ca-certificates.crt`;
- затем создать файл `/etc/default/trp-agent`. Подробное описание файла приведено в подразделе **Файл `/etc/default/trp-agent`**;
- сделать исполняемым файл `/opt/termidesk/trp-agent/sbin/pam_trp`:

```
chmod +x /opt/termidesk/trp-agent/sbin/pam_trp
```

- добавить в автоматическую загрузку и запустить службу `trp-agent`:

```
sudo systemctl enable trp-agent
sudo systemctl start trp-agent
```

Проверка состояния службы выполняется командой:

```
sudo systemctl status trp-agent
```

Строка `Active` отображает состояние сервиса, где статус `active (running)` означает успешный запуск.

Для ручного перезапуска службы выполнить:

```
sudo systemctl restart trp-agent
```

Обновление агентской части в ОС Astra Linux Special Edition

Обновление агентской части Termidesk Profiles выполняется установкой новой версии поверх предыдущей.

Удаление агентской части в ОС Astra Linux Special Edition

Для удаления агентской части Termidesk Profiles из среды ОС Astra Linux Special Edition нужно:

- выполнить команду:

```
sudo apt purge -y trp-agent
```

Где:

`-y` - ключ для пропуска подтверждения удаления.

- удалить оставшийся каталог с файлами:

```
sudo rm -R /opt/termidesk/trp-agent
```

Где:

`-R` - ключ для рекурсивного действия. Будут удалены все вложенные подкаталоги.

- очистить оставшиеся зависимости и конфигурации:

```
sudo apt purge ~c -y
```

Команда полностью удалит оставшиеся настройки и зависимости.

- очистить настройки PAM, удалив строку из файла `/etc/pam.d/common-session`:

```
session optional pam_exec.so log=/var/log/termidesk/trp/mount.log
/opt/termidesk/trp-agent/sbin/pam_trp
```

Установка в режиме замкнутой программной среды

Замкнутая программная среда (ЗПС) является средством повышения безопасности ОС путем контроля целостности (неизменности) файлов.

Механизм контроля реализован в виде невыгружаемого модуля ядра ОС Astra Linux Special Edition (модуль `digsig_verif`), выполняющего проверку электронной цифровой подписи файлов (ЭЦП).

Перед установкой компонентов Termidesk Profiles необходимо установить пакет `termidesk-digsig-keys`, для этого:

- подключить репозиторий Termidesk или получить отдельный пакет `termidesk-digsig-keys` из репозитория;
- выполнить установку с использованием репозитория:

```
sudo apt -y install termidesk-digsig-keys
```

- либо выполнить установку из `deb`-пакета:

```
sudo apt install -y /home/user/termidesk-digsig-keys-XXXXXX_amd64.deb
```

Где:

`-y` - ключ для пропуска подтверждения установки;

`/home/user/termidesk-digsig-keys-XXXXXX_amd64.deb` - расположение пакета `termidesk-digsig-`

keys-XXXXXX_amd64.deb.

- перезагрузить ОС:

```
sudo reboot
```

- выполнить установку компонента Termidesk Profiles.

Для ЗПС может быть активирован режим проверки встроенной ЭЦП в расширенных атрибутах (DIGSIG_XATTR_MODE). В этом случае потребуется подписать файлы, которые будут проходить проверку, имеющимися в организации ключами. Информация о процессе подписи и активации механизма проверки встроенной ЭЦП в расширенных атрибутах приведена в справочном центре Astra Linux: https://wiki.astralinux.ru/pages/viewpage.action?pageId=41190634.

Постановка серверной и агентской части на контроль целостности

После установки и настройки серверной и агентской части Termidesk Profiles необходимо поставить их на контроль целостности.

В подразделе приведена процедура только для серверной и агентской части Termidesk Profiles, установленных в ОС Astra Linux Special Edition.

Для контроля целостности используются встроенные в ОС Astra Linux Special Edition программные средства на основе Another File Integrity Checker, представленного пакетом afick.

Настройка регламентного контроля целостности выполняется в конфигурационном файле /etc/afick.conf.

Настройку следует производить только после окончательного внедрения компонента, поскольку с файлов конфигурации и исполняемых файлов будут сняты эталонные контрольные суммы.

Для постановки на контроль целостности серверной части необходимо добавить в конфигурационный файл /etc/afick.conf следующие строки:

```
/opt/termidesk/trp-server/
/usr/lib/systemd/system/trp-server.service

#Репозиторий Termidesk VDI (если используется)
/var/repos/ PARSEC
```

Для постановки на контроль целостности агентской части необходимо добавить в конфигурационный файл /etc/afick.conf следующие строки:

```
/opt/termidesk/trp-agent/
/opt/termidesk/trp-agent/bin/trp_agent
/usr/lib/systemd/system/trp-agent.service

#Репозиторий Termidesk VDI (если используется)
```

```
/var/repos/ PARSEC
```

Для снятия эталонных значений контрольных сумм используется команда:

```
afick -i
```

Для проверки соответствия контрольных сумм эталонным значениям автоматически создаются задания в системном планировщике заданий `cron`.

Для ручной проверки соответствия контрольных сумм используется команда:

```
afick -k
```

В случае отсутствия по какой-либо причине исполняемых фалов `*.pyc`, они будут повторно сгенерированы при перезапуске сервера Python. В этом случае нужно повторно проинициализировать средство регламентного контроля целостности `afick`.

Проверка работоспособности после установки

Сервер Termidesk Profiles является работоспособным, если в результате перехода в веб-браузере по адресу https://localhost:31337/ или https://<IP-адрес_или_FQDN_узла>:31337/ отобразилась страница входа в Termidesk Profiles (см. рисунок Начальная веб-страница). Если страница сразу не отобразилась, следует подождать 10-15 секунд и обновить ее.

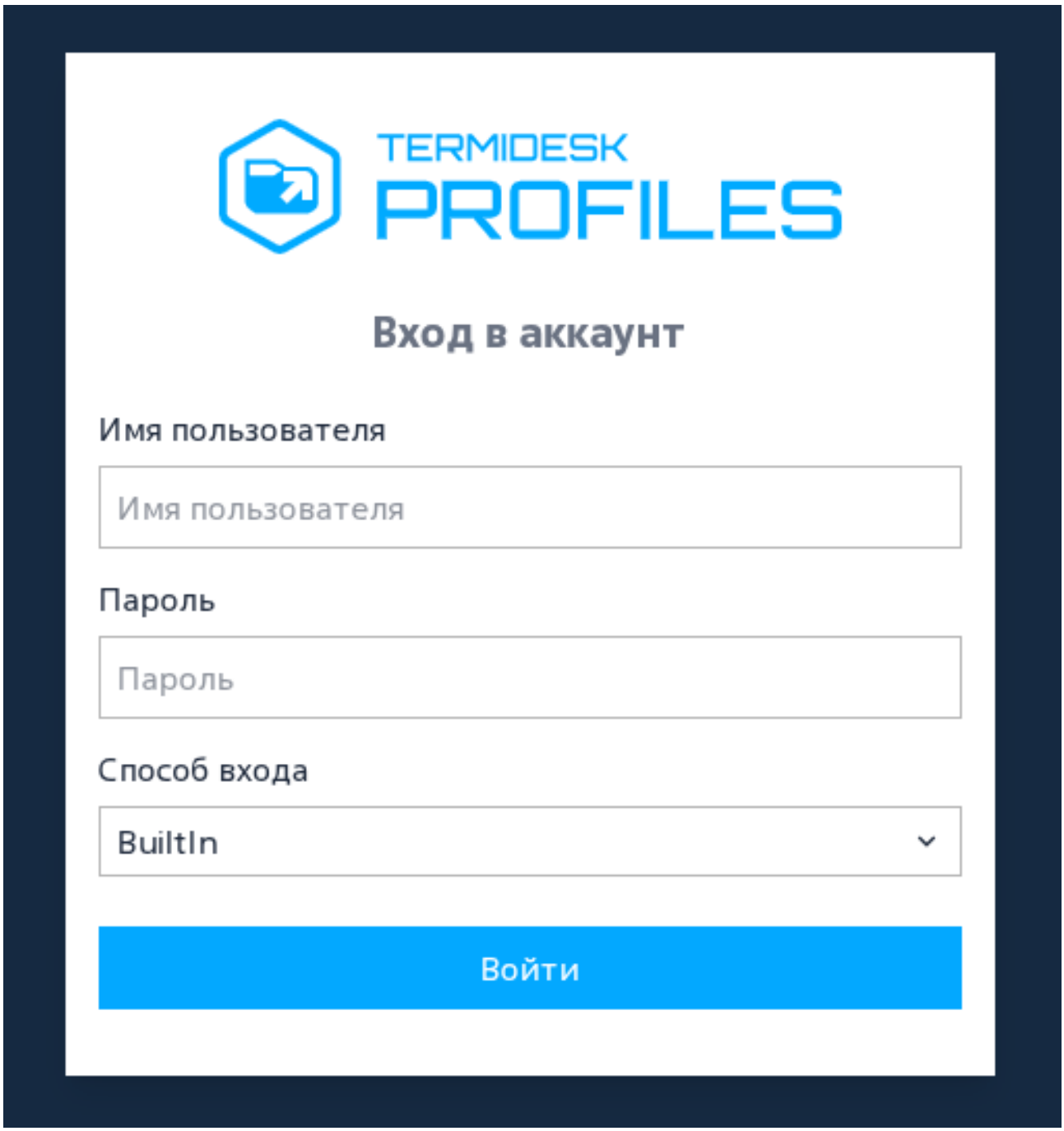


Рисунок 150. Начальная веб-страница

По умолчанию после установки вход в интерфейс управления Termidesk Profiles доступен только авторизованному пользователю ОС, являющемуся членом группы `termidesk`. Для добавления нужного пользователя в группу выполнить:

- создать нового пользователя (опционально, можно добавлять уже существующего):

```
sudo useradd <имя_пользователя>
```

- назначить пароль новому пользователю (не требуется, если добавляется существующий):

```
sudo passwd <имя_пользователя>
```

- добавить пользователя в группу `termidesk`:

```
sudo usermod -aG termidesk <имя_пользователя>
```

Проверка состояния службы сервера Termidesk Profiles выполняется командой:

```
sudo systemctl status trp-server
```

Строка `Active` отображает состояние сервиса, где статус `active (running)` означает успешный запуск.

TERMIDESK PROFILES. НАЧАЛО РАБОТЫ

Общая последовательность шагов по работе с Termidesk Profiles:

- устанавливается серверная часть Termidesk Profiles (см. разделы и подразделы **Подготовка среды функционирования**, **Установка серверной части в ОС Astra Linux Special Edition**);
- выполняется переход в графический интерфейс серверной части Termidesk Profiles (см. раздел **Доступ к веб-интерфейсу серверной части**);
- добавляется хранилище, используемое для хранения Перемещаемых Профилей (см. раздел **Добавление хранилища**);
- добавляется домен аутентификации (см. раздел **Добавление доменов аутентификации**);
- настраивается шаблон Перемещаемого Профиля (см. раздел **Настройка шаблона**);
- создается шаблон Перемещаемого Профиля (см. раздел **Создание шаблона**);
- настраивается агентская часть Termidesk Profiles (см. раздел **Добавление группы агентов**);
- устанавливается агентская часть Termidesk Profiles (см. подраздел **Установка агентской части в ОС Astra Linux Special Edition**);
- настраивается запуск агентской части Termidesk Profiles (см. раздел **Параметры конфигурирования агентской части**);
- создается конфигурация доставки Перемещаемого Профиля (см. раздел **Добавление конфигурации доставки**).

TERMIDESK PROFILES. ХРАНИЛИЩА

Общие сведения о хранилищах

Хранилище - это внешняя система хранения данных, используемая для хранения Перемещаемых Профилей. Профиль размещается на хранилище в виде базового образа.

Хранилище должно быть одинаково доступно как для серверной части, так и для агентской части Termidesk Profiles.

Для хранения Перемещаемых Профилей используется NFS-хранилище.

Для отображения списка хранилищ следует перейти в раздел «Хранилища». Основные параметры списка приведены в таблице Параметры списка хранилищ.

Таблица 281. Параметры списка хранилищ

Параметр	Описание
«UUID»	Уникальный идентификатор записи в таблице. По умолчанию параметр не отображается
«Название»	Наименование хранилища
«Тип хранилища»	Тип хранилища
«FQDN»	FQDN хранилища
«IP-адрес»	IP-адрес хранилища
«Общий ресурс»	Путь к общему каталогу хранилища Перемещаемых Профилей
«Точка монтирования»	Путь к каталогу монтирования хранилища Перемещаемых Профилей
«Директория пользователей»	Каталог хранения Перемещаемых Профилей пользователей
«Директория шаблонов»	Каталог хранения шаблонов Перемещаемых Профилей
«Временная директория»	Каталог хранения временных файлов Перемещаемых Профилей
«Дата создания»	Дата создания записи в таблице об объекте. По умолчанию параметр не отображается
«Дата обновления»	Дата внесения последних изменений. По умолчанию параметр не отображается
«Комментарий»	Информационное сообщение, используемое для описания хранилища

Структура хранилища формируется согласно настройкам, заданным в подразделе **Добавление хранилища**. Пример итоговой структуры хранилища:

```
/mnt/storage/
├──── profiles
│    └──── EXAMPLE.LAN
│        ├──── configuration-uuid-01
│        │    ├──── user01
│        │    │    └──── user01_base.qcow2
│        │    └──── user02
│        │        └──── user02_base.qcow2
│        └──── configuration-uuid-02
│            ├──── user01
│            │    └──── user01_base.qcow2
│            └──── user02
│                └──── user02_base.qcow2
├──── temp
└──── templates
    ├──── template01.qcow2
    └──── template02.qcow2
```

Где:

`/mnt/storage/` - каталог монтирования;

`/mnt/storage/templates/` - каталог хранения шаблонов Перемещаемых Профилей;

`/mnt/storage/templates/template01.qcow2` - шаблон базового образа Перемещаемого Профиля;

`/mnt/storage/profiles/` - каталог хранения Перемещаемых Профилей пользователей;

`/mnt/storage/profiles/EXAMPLE.LAN/` - каталог домена аутентификации;

`/mnt/storage/profiles/EXAMPLE.LAN/configuration-uuid-01/user01` - каталог пользователя;

`/mnt/storage/profiles/EXAMPLE.LAN/configuration-uuid-01/user01/user01_base.qcow2` - файл базового образа Перемещаемого Профиля;

`/mnt/storage/temp/` - каталог хранения временных файлов Перемещаемых Профилей.

Добавление хранилища

Для добавления хранилища следует перейти в раздел «Хранилища», нажать экранную кнопку **[Создать]**. Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления хранилища).

Для сохранения параметров конфигурации хранилища следует нажать экранную кнопку **[Сохранить]**.

Таблица 282. Данные для добавления хранилища

Параметр	Описание
«Название»	Наименование хранилища
«Комментарий»	Информационное сообщение, используемое для описания хранилища
«Тип хранилища»	Тип хранилища. В Termidesk Profiles версии 1.0.0 поддерживается только NFS-хранилище. Возможные значения: • «nfs»
«FQDN сервера»	FQDN хранилища
«IP-адрес»	IP-адрес хранилища
«Путь к общей папке хранилища»	Путь к общему каталогу хранилища Перемещаемых Профилей
«Точка монтирования хранилища»	Путь к каталогу монтирования хранилища Перемещаемых Профилей. Указанный каталог используется для создания структуры каталогов Перемещаемых Профилей
«Директория пользователя»	Наименование каталога для хранения Перемещаемых Профилей пользователей. Каталог создается автоматически
«Директория шаблонов дисков»	Наименование каталога для хранения шаблонов Перемещаемых Профилей. Каталог создается автоматически
«Директория временного хранения»	Наименование каталога для хранения временных файлов Перемещаемых Профилей. Каталог создается автоматически

TERMIDESK PROFILES. ДОМЕНЫ АУТЕНТИФИКАЦИИ

Общие сведения о доменах аутентификации

Домен аутентификации - источник сведений о субъектах и их полномочиях.

Поддерживаются следующие домены аутентификации:

В Termidesk Profiles версии 1.0.0 домен аутентификации OIDC поддерживается только для аутентификации пользователей в веб-интерфейсе управления.

- MS AD или LDAP;
- OIDC.

Для отображения списка доменов аутентификации следует перейти в раздел «Домены аутентификации». Основные параметры списка приведены в таблице Параметры списка доменов аутентификации.

Таблица 283. Параметры списка доменов аутентификации

Параметр	Описание
«UUID»	Уникальный идентификатор записи в таблице. По умолчанию параметр не отображается
«Название»	Имя домена аутентификации
«Тип домена»	Тип домена аутентификации
«Дата создания»	Дата создания записи в таблице об объекте
«Дата обновления»	Дата внесения последних изменений
«Комментарий»	Информационное сообщение, используемое для описания домена аутентификации

Добавление доменов аутентификации

Домен аутентификации MS AD

Добавление домена аутентификации MS AD

Для добавления домена аутентификации MS AD следует перейти в раздел «Домены аутентификации», затем нажать экранную кнопку **[Добавить]** и выбрать из выпадающего списка «Microsoft AD DS». Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления домена аутентификации MS AD).

Для сохранения параметров подключения к домену аутентификации следует нажать экранную кнопку **[Сохранить]**.

Таблица 284. Данные для добавления домена аутентификации MS AD

Параметр	Описание
«Имя домена»	DNS-имя домена аутентификации в формате FQDN. Примеры: «example.ru», «corp.domain.lan»
«Комментарий»	Информационное сообщение, используемое для описания домена аутентификации
«Адрес сервера»	IP-адрес или FQDN контроллера домена

Параметр	Описание
«Search DN»	Корень поиска в службе каталогов в формате DN. Параметру следует задавать значение, соответствующее записи верхнего уровня в иерархии службы каталогов: в корне поиска будет выполняться поиск всех участвующих объектов (групп, пользователей, компьютеров). Учетная запись, используемая для подключения к службе каталогов, должна иметь права на чтение групп, учетных записей пользователей и компьютеров в указанном корне поиска. Пример использования: «OU=user,DC=test,DC=desk»
«LDAPS»	Использование защищенного соединения по протоколу LDAPS. При использовании защищенного подключения к службе каталогов по протоколу HTTPS нужно убедиться, что сертификат доменного центра сертификации, выдавший сертификат сервера (контроллера домена), является доверенным и содержится в файле `/etc/ssl/certs/ca-certificates.crt`. Возможные значения: • «Включено» - использовать защищенное соединение; • «Выключено» (по умолчанию) - не использовать защищенное соединение
«Пользователь»	Наименование учетной записи с правами чтения каталога
«Пароль»	Набор символов, подтверждающий полномочия объекта для подключения к службе каталогов

Добавление группы домена аутентификации MS AD

Для добавления группы домена аутентификации MS AD нужно перейти в раздел «Домены аутентификации», выбрать нужный домен аутентификации и нажать экранную кнопку **[Группы домена]**.

В открывшемся окне добавить группу домена аутентификации. Для этого:

- выбрать тип группы в выпадающем списке «Тип группы»:
  - «users» - группа, содержащая учетные записи пользователей;
  - «computers» - группа, содержащая учетные записи компьютеров;
- ввести полное или частичное наименование группы в поле «Поиск групп» и нажать экранную кнопку **[Найти]**;
- выбрать нужные группы в списке и нажать экранную кнопку **[Добавить группу]**.

Для удаления группы домена аутентификации выбрать нужные группы в списке и нажать экранную кнопку **[Удалить]**.

Домен аутентификации OIDC

Добавление домена аутентификации OIDC

OIDC - это механизм, позволяющий приложению связаться со службой идентификации IdP, получить данные о пользователе и вернуть их обратно в приложение. Таким образом OIDC обеспечивает аутентификацию администраторов и пользователей без необходимости ввода логина и пароля.

Служба идентификации IdP (например, Keycloak) должна быть предварительно настроена в инфраструктуре организации для возможности использования OIDC как домена аутентификации.

Для добавления домена аутентификации OIDC следует перейти в раздел «Домены аутентификации», затем нажать экранную кнопку **[Добавить]** и выбрать из выпадающего списка «OIDC».

Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления аутентификации через OIDC).

Для сохранения параметров подключения к домену аутентификации следует нажать экранную кнопку **[Сохранить]**.

Таблица 285. Данные для добавления аутентификации через OIDC

Параметр	Описание
«Имя домена»	Наименование домена аутентификации
«Комментарий»	Информационное сообщение, используемое для описания домена аутентификации
«Issuer URL»	URL-адрес авторизации службы идентификации IdP. Пример: «http://192.0.2.2:8080/realms/trp»
«Client ID»	Уникальный идентификатор приложения, полученный от службы идентификации IdP. Пример: «openid-test-cl»
«Client Secret»	Ключ приложения, полученный от службы идентификации IdP
«Scopes»	Набор областей действия, поддерживаемый в службе идентификации IdP. Области действия определяются спецификацией протокола OAuth 2.0. Неполный список возможных значений (указываются через пробел): • «openid» (обязательное значение для OIDC) - запуск аутентификации с использованием OIDC; • «profile» - доступ к профилю пользователя; • «email» - доступ к адресу электронной почты пользователя; • «offline_access» - обновление токена доступа без необходимости повторной аутентификации; • «groups» - доступ к списку ролей пользователя. Значение по умолчанию: «openid email profile groups». Если нужно указать другой набор значений, следует убедиться, что он поддерживается используемой службой идентификации IdP

TERMIDESK PROFILES. ШАБЛОНЫ

Общие сведения о шаблонах

Шаблон - это набор параметров, согласно которым будет создан базовый образ Перемещаемого Профиля.

Последовательность шагов для создания шаблона выглядит следующим образом:

- создаются параметры конфигурации шаблона согласно подразделу **Настройка шаблона**;
- выполняется создание шаблона согласно подразделу **Создание шаблона**.

Для отображения списка параметров конфигурации шаблонов следует перейти «Шаблоны - Наборы параметров шаблона». Основные параметры списка приведены в таблице

Параметры списка настроек шаблонов Перемещаемого Профиля.

Таблица 286. Параметры списка настроек шаблонов Перемещаемого Профиля

Параметр	Описание
«UUID»	Уникальный идентификатор записи в таблице. По умолчанию параметр не отображается
«Название»	Наименование параметров конфигурации шаблона
«Тип файловой системы»	Тип файловой системы базового образа Перемещаемого Профиля
«Тип предраспределения»	Метод выделения дискового пространства для шаблона и связанных с ним базовых образов Перемещаемого Профиля
«Тип сжатия»	Алгоритм сжатия дискового пространства базового образа Перемещаемого Профиля
«Размер»	Максимальный объем (в гигабайтах) шаблона и связанных с ним базовых образов Перемещаемого Профиля
«Шифрование»	Использование алгоритма преобразования базового образа Перемещаемого Профиля
«Шаблоны»	Список шаблонов, созданных на основе указанных параметров конфигурации шаблона
«Дата создания»	Дата создания записи в таблице об объекте
«Дата обновления»	Дата внесения последних изменений. По умолчанию параметр не отображается
«Комментарий»	Информационное сообщение, используемое для описания параметров конфигурации шаблона

Для отображения списка шаблонов следует перейти «Шаблоны - Шаблоны». Основные параметры списка приведены в таблице Параметры списка шаблонов.

Таблица 287. Параметры списка шаблонов

Параметр	Описание
«UUID»	Уникальный идентификатор записи в таблице. По умолчанию параметр не отображается
«Название»	Наименование шаблона
«Набор параметров шаблона»	Параметры конфигурации, присвоенные шаблону. При выборе значения отображаются сведения о параметрах конфигурации шаблона (см. таблицу Параметры списка настроек шаблонов Перемещаемого Профиля)
«Хранилище»	Хранилище, в котором размещаются шаблоны. При выборе значения отображаются сведения о хранилище (см. подраздел **Общие сведения о хранилищах**)
«Конфигурации»	Конфигурация доставки, присвоенная шаблону. При выборе значения отображаются сведения о конфигурации доставки (см. подраздел **Общие сведения о конфигурациях доставки**)
«Базовые образы»	Список базовых образов Перемещаемых Профилей, созданных на основе шаблона. При выборе значения отображается пользователь, использующий базовый образ
«Дата создания»	Дата создания записи в таблице об объекте
«Дата обновления»	Дата внесения последних изменений. По умолчанию параметр не отображается
«Комментарий»	Информационное сообщение, используемое для описания шаблона

Настройка шаблона

Для настройки шаблона следует перейти в раздел «Шаблоны - Наборы параметров шаблона», нажать экранную кнопку **[Создать]**. Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для настройки набора параметров шаблона Перемещаемого Профиля).

Для сохранения параметров конфигурации шаблона следует нажать экранную кнопку **[Сохранить]**.

Таблица 288. Данные для настройки набора параметров шаблона Перемещаемого Профиля

Параметр	Описание
«Название»	Наименование параметров конфигурации шаблона Перемещаемого Профиля
«Комментарий»	Информационное сообщение, используемое для описания параметров конфигурации шаблона Перемещаемого Профиля
«Тип файловой системы»	Выбор типа файловой системы базового образа Перемещаемого Профиля. В Termidesk Profiles версии 1.0.0 поддерживается только файловая система XFS. Возможное значение: • «xfs»
«Тип предраспределения»	Метод выделения дискового пространства для шаблона и связанных с ним базовых образов Перемещаемого Профиля. Возможные значения: • «off» - выделение пространства не выполняется; • «falloc» - резервирование пространства с его заполнением по мере использования
«Тип сжатия»	Алгоритм сжатия дискового пространства базового образа Перемещаемого Профиля. В Termidesk Profiles версии 1.0.0 поддерживается только алгоритм сжатия ZLIB. Возможное значение: • «zlib»
«Размер (GB)»	Максимальный объем (в гигабайтах) шаблона и связанных с ним базовых образов Перемещаемого Профиля. Значение по умолчанию: «10»
«Шифрование»	Использование алгоритма преобразования базового образа Перемещаемого Профиля. Возможные значения: • «Выключено» (по умолчанию); • «Включено»

Создание шаблона

Для создания шаблона следует перейти в раздел «Шаблоны - Шаблоны», нажать экранную кнопку **[Создать]**. Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для создания шаблона Перемещаемого Профиля).

Для сохранения шаблона следует нажать экранную кнопку **[Сохранить]**.

Таблица 289. Данные для создания шаблона Перемещаемого Профиля

Параметр	Описание
«Название»	Наименование шаблона
«Комментарий»	Информационное сообщение, используемое для описания шаблона
«Набор параметров шаблона»	Выбор параметров конфигурации шаблона
«Хранилище шаблона»	Выбор хранилища шаблона

TERMIDESK PROFILES. КОНФИГУРАЦИИ ДОСТАВКИ

Общие сведения о конфигурациях доставки

Конфигурации доставки используются для назначения Перемещаемых Профилей группам пользователей доменов аутентификации.

Экранная кнопка **[Удалить]** может быть недоступна, если выбранная конфигурация доставки имеет связанный с ней базовый образ.

Для отображения списка конфигураций доставки следует перейти в раздел «Конфигурации». Основные параметры списка приведены в таблице Параметры списка конфигураций доставки.

Таблица 290. Параметры списка конфигураций доставки

Параметр	Описание
«UUID»	Уникальный идентификатор записи в таблице. По умолчанию параметр не отображается
«Название»	Наименование конфигурации доставки
«Шаблон»	Наименование шаблона, присвоенного конфигурации доставки. При выборе значения отображаются сведения о параметрах конфигурации шаблона (см. подраздел **Общие сведения о шаблонах**)
«Хранилище шаблона»	Наименование хранилища, в котором расположен шаблон и Профили пользователей. При выборе значения отображаются сведения о хранилище (см. подраздел **Общие сведения о хранилищах**)
«Домен аутентификации»	Наименование домена аутентификации, связанного с конфигурацией доставки. При выборе значения отображаются сведения о домене аутентификации (см. подраздел **Общие сведения о доменах аутентификации**)
«Название группы домена аутентификации»	Наименование группы домена аутентификации, к которой применяется конфигурация доставки
«Комментарий»	Информационное сообщение, используемое для описания конфигурации доставки

Добавление конфигурации доставки

Для добавления конфигурации доставки следует перейти в раздел «Конфигурации», нажать экранную кнопку **[Создать]**. Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления конфигурации доставки).

Для сохранения параметров конфигурации следует нажать экранную кнопку **[Создать]**.

Таблица 291. Данные для добавления конфигурации доставки

Параметр	Описание
«Название»	Наименование конфигурации доставки
«Комментарий»	Информационное сообщение, используемое для описания конфигурации доставки
«Шаблон»	Выбор шаблона, применяемого для создания Перемещаемых Профилей пользователей конфигурации доставки
«Домен аутентификации»	Выбор домена аутентификации, с которым связана конфигурация доставки
«Группы пользователей»	Выбор группы домена аутентификации, к которой применяется конфигурация доставки
«Тип привязки»	Выбор способа привязки агентов к объектам домена аутентификации. Возможные значения: • «Доменная группа компьютеров» - агенты привязываются к доменной группе компьютеров; • «DN подразделения» - агенты привязываются по имени организационного подразделения Distinguished Name (DN)
«Группы агентов»	Выбор групп агентов, используемых в конфигурации доставки. Доступные значения зависят от параметра «Тип привязки»
«Приоритет»	В Termidesk Profiles версии 1.0.0 параметр находится в разработке и не влияет на функциональность.

TERMIDESK PROFILES. ОБРАЗЫ ПЕРЕМЕЩАЕМЫХ ПРОФИЛЕЙ

Общие сведения об образах Перемещаемых пПофилей

Образы Перемещаемых Профилей используются для хранения пользовательских данных.

Для хранения пользовательских данных используются следующие типы образов Перемещаемых Профилей:

- базовый образ - образ создается на основе шаблона. При подключении пользователя к РМ из базового образа создается активный образ;
- активный образ - образ создается на основе базового образа. Содержит изменения, выполняемые пользователем при работе в РМ. После отключения пользователя от РМ все изменения сохраняются в базовом образе, а активный образ удаляется.

Образы Перемещаемых Профилей хранятся в сетевом хранилище в соответствии с настроенной структурой каталогов (см. раздел **Общие сведения о хранилищах**).

Просмотр списка базовых образов

Для отображения списка базовых образов следует перейти в раздел «Базовые образы». Основные параметры списка приведены в таблице Параметры списка базовых образов.

Для удаления базового образа следует выбрать нужный образ в списке и нажать экранную кнопку **[Удалить]**.

Экранная кнопка **[Удалить]** может быть недоступна, если выбранный базовый образ имеет связанный с ним активный образ.

Таблица 292. Параметры списка базовых образов

Параметр	Описание
«UUID»	Уникальный идентификатор записи в таблице. По умолчанию параметр не отображается
«Служебное название»	Идентификатор базового образа. По умолчанию параметр не отображается. Отображается в формате: user_base_ab1234c5. Где: • user - пользователь, которому назначен базовый образ; • base - тип образа (базовый); • ab1234c5 - уникальный идентификатор конфигурации доставки
«Пользователь»	Пользователь, которому назначен базовый образ
«Конфигурация»	Наименование конфигурации доставки базового образа
«Шаблон»	Шаблон, который используется для создания базового образа
«Хранилище»	Хранилище базового образа
«Тип хранилища»	Тип хранилища
«Активный образ»	Активный образ, созданный из базового образа
«Путь»	При выборе значения «Путь» отображается путь к файлу базового образа в хранилище
«Дата создания»	Дата создания записи в таблице об объекте
«Дата обновления»	Дата внесения последних изменений
«Комментарий»	Информационное сообщение, используемое для описания базового образа

Просмотр списка активных образов

Для отображения списка активных образов следует перейти в раздел «Активные образы». Основные параметры списка приведены в таблице Параметры списка активных образов.

Таблица 293. Параметры списка активных образов

Параметр	Описание
«UUID»	Уникальный идентификатор записи в таблице. По умолчанию параметр не отображается
«Служебное название»	Идентификатор активного образа. По умолчанию параметр не отображается
«Базовый образ»	Базовый образ, из которого создан активный образ
«Пользователь»	Пользователь, который использует базовый образ
«Хранилище»	Хранилище активного образа
«Тип хранилища»	Тип хранилища
«Путь»	При выборе значения «Путь» отображается путь к файлу активного образа в хранилище
«Дата создания»	Дата создания записи в таблице об объекте

TERMIDESK PROFILES. АГЕНТЫ

Общие сведения об агентах

Агентская часть Termidesk Profiles устанавливается в гостевую ОС РМ. Агентская часть взаимодействует с серверной частью, применяет параметры конфигурирования, обеспечивает подключение и отключение Перемещаемых Профилей в процессе работы пользователя.

Последовательность шагов для настройки агентской части:

- создать параметры конфигурации агентской части (см. подраздел **Добавление группы агентов**);
- выполнить установку агентской части в гостевую ОС РМ (см. подраздел **Установка, обновление, удаление агентской части**).

Для отображения списка параметров конфигурации групп агентов следует перейти «Агенты - Группы агентов». Основные параметры списка приведены в таблице Параметры списка групп агентов.

Таблица 294. Параметры списка групп агентов

Параметр	Описание
«UUID»	Уникальный идентификатор записи в таблице. По умолчанию параметр не отображается
«Название»	Наименование группы агентов
«Макс. количество NBD»	Максимальное количество устройств `/dev/nbd` в системе, доступных для единовременного подключения образов Перемещаемых Профилей пользователей
«Макс. количество разделов»	Максимальное количество разделов файловой системы в образах Перемещаемых Профилей пользователей, разрешенное для подключения в системе
«DN подразделения»	Distinguished Name (DN) организационного подразделения, в котором хранятся учетные записи компьютеров
«Домен аутентификации»	Имя домена аутентификации, членами которого являются агенты, входящие в группу агентов
«Доменная группа компьютеров»	Группа домена аутентификации, членами которой являются агенты, входящие в группу агентов
«Агенты»	Список зарегистрированных агентов, входящих в группу агентов. При выборе значения отображаются сведения об агенте (см. подраздел **Просмотр сведений об агенте**)
«Комментарий»	Информационное сообщение, используемое для описания группы агентов

Добавление группы агентов

Для добавления группы агентов следует перейти «Агенты - Группы агентов», нажать экранную кнопку **[Создать]**. Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. таблицу Данные для добавления группы агентов).

Для сохранения параметров конфигурации следует нажать экранную кнопку **[Сохранить]**.

Таблица 295. Данные для добавления группы агентов

Параметр	Описание
«Название»	Наименование группы агентов

Параметр	Описание
«Комментарий»	Информационное сообщение, используемое для описания группы агентов
«Макс. количество NBD»	Максимальное количество устройств `/dev/nbd` в системе, доступных для единовременного подключения образов Перемещаемых Профилей пользователей. Значение по умолчанию: «10»
«Макс. количество разделов»	Максимальное количество разделов файловой системы в образах Перемещаемых Профилей пользователей, разрешенное для подключения в системе. Значение по умолчанию: «2»
«Домен аутентификации»	Выбор домена аутентификации, членами которого будут являться агенты, входящие в группу агентов В Termidesk Profiles версии 1.0.0 для выбора доступен только домен аутентификации MS AD.
«Тип привязки»	Выбор способа привязки агентов к объектам домена аутентификации. Возможные значения: • «Доменная группа компьютеров» - агенты привязываются к доменной группе компьютеров; • «DN подразделения» - агенты привязываются по имени организационного подразделения Distinguished Name (DN)
«Доменная группа компьютеров»	Выбор группы домена аутентификации, членами которой будут являться агенты, входящие в группу агентов Параметр задается при использовании домена аутентификации MS AD и доступен при выборе значения «Доменная группа компьютеров» в поле «Тип привязки».
«DN Подразделения»	DN организационного подразделения, в котором хранятся учетные записи компьютеров. Пример: «OU=trp,DC=tst,DC=loc» Параметр задается при использовании домена аутентификации MS AD и доступен при выборе значения «DN Подразделения» в поле «Тип привязки».

Просмотр сведений об агенте

Для просмотра сведений об агенте следует перейти «Агенты - Группы агентов», и в сводной таблице в столбце «Агенты» нажать на IP-адрес агента.

Для удаления агента из списка группы агентов нужно нажать экранную кнопку **[Удалить]**.

Список доступных сведений об агенте перечислен в столбце «Параметр» следующей таблицы (см. таблицу Параметры списка сведений об агенте).

Таблица 296. Параметры списка сведений об агенте

Параметр	Описание
«UUID»	Уникальный идентификатор записи в таблице. По умолчанию параметр не отображается
«Название»	Имя узла, на котором установлен агент
«IP-адрес»	IP-адрес агента
«Домен аутентификации»	Имя домена аутентификации, членом которого является агент
«Первое появление»	Дата первого взаимодействия агента с серверной частью
«Последнее появление»	Дата последнего взаимодействия агента с серверной частью

Просмотр списка агентов

Для отображения списка агентов следует перейти «Агенты - Агенты» и выбрать группу агентов в выпадающем списке «Группа агентов».

Для удаления агента из списка группы агентов нужно выбрать нужный агент в списке и нажать экранную кнопку **[Удалить]**.

Основные параметры списка приведены в таблице Параметры списка агентов.

Таблица 297. Параметры списка агентов

Параметр	Описание
«UUID»	Уникальный идентификатор записи в таблице. По умолчанию параметр не отображается
«Название»	Имя узла агента
«IP-адрес»	IP-адрес агента
«Домен аутентификации»	Имя домена аутентификации, членом которого является агент
«Первое появление»	Дата первого взаимодействия агента с серверной частью
«Последнее появление»	Дата последнего взаимодействия агента с серверной частью

TERMIDESK PROFILES. РАЗГРАНИЧЕНИЕ РОЛЕЙ АДМИНИСТРАТОРОВ И ПОЛЬЗОВАТЕЛЕЙ

Разграничение ролей

Предусмотрено следующее разграничение ролей по управлению Termidesk Profiles:

- роль администратора Termidesk Profiles. После успешного прохождения процедуры идентификации и аутентификации администратору будут доступны настройка и управление Termidesk Profiles. По умолчанию с администратором ассоциируется локальный пользователь операционной системы (ОС) с полномочиями администратора на узле с установленным Termidesk Profiles;
- роль персонала (оператора) Termidesk Profiles. Персонал Termidesk Profiles задается администратором Termidesk Profiles. Ему будут доступны ограниченные возможности управления Termidesk Profiles;
- роль аудитора Termidesk Profiles. Аудитор Termidesk Profiles задается администратором Termidesk Profiles. Ему будут доступны возможности просмотра журналов и событий аудита.

Тип авторизованного пользователя отображается в правом верхнем углу веб-интерфейса

управления:

- «admin» - администратор Termidesk Profiles;
- «staff» - персонал Termidesk Profiles;
- «audit» - аудитор Termidesk Profiles.

Для отображения списка ролей, назначенных пользователям следует перейти «Системные параметры - Управление ролями». Основные параметры списка приведены в таблице Параметры списка сведений о назначенных ролях.

Поддерживается фильтрация списка. Для этого в выпадающем списке «Роль» нужно выбрать соответствующий фильтр:

- «Пользователи всех ролей» - формирует список пользователей с любыми ролями;
- «Администратор» - формирует список пользователей с ролью администратора;
- «Персонал» - формирует список пользователей с ролью оператора;
- «Аудитор» - формирует список пользователей с ролью аудитора.

Таблица 298. Параметры списка сведений о назначенных ролях

Параметр	Описание
«UUID»	Уникальный идентификатор записи в таблице. По умолчанию параметр не отображается
«Логин»	Наименование учетной записи пользователя
«Роль»	Роль пользователя
«UUID роли»	Уникальный идентификатор роли пользователя. По умолчанию параметр не отображается
«Домен аутентификации»	Домен аутентификации, в котором состоит учетная запись пользователя

Управление ролями

Для назначения роли пользователю следует перейти «Системные параметры - Управление ролями» и нажать экранную кнопку **[Назначить роль]**.

Для сохранения роли пользователя нужно нажать экранную кнопку **[Сохранить]**.

Список параметров, доступных при назначении роли пользователю приведен в таблице (см. таблицу Список доступных параметров при назначении роли пользователю).

Таблица 299. Список доступных параметров при назначении роли пользователю

Параметр	Описание
«Логин»	Наименование учетной записи пользователя
«Домен аутентификации»	Выбор домена аутентификации, в котором состоит учетная запись пользователя

Параметр	Описание
«Роль»	Выбор роли пользователя. Возможные значения: • «Администратор» - пользователю будут доступны настройка и управление Termidesk Profiles; • «Персонал» - пользователю будут доступны ограниченные возможности управления Termidesk Profiles; • «Аудитор» - пользователю будут доступны возможности просмотра журналов и событий аудита

TERMIDESK PROFILES. СИСТЕМНЫЕ НАСТРОЙКИ

Общие системные параметры Termidesk Profiles

Системные параметры позволяют задать основные значения, необходимые для успешного функционирования Termidesk Profiles.

Для конфигурации общих системных параметров следует перейти «Системные параметры - Системные настройки», выбрать раздел «Общие».

Доступные для редактирования параметры перечислены в столбце «Параметр» следующей таблицы (см. таблицу Общие системные параметры Termidesk Profiles).

Изменения системных параметров вступают в силу только после перезагрузки Termidesk Profiles.

Экранная кнопка **[Сохранить]** сохраняет общие системные параметры.

Таблица 300. Общие системные параметры Termidesk Profiles

Параметр	Описание
«Кол-во NBD-устройств»	Максимальное количество шаблонов и базовых образов Перемещаемого Профиля, доступных для одновременной настройки и подключения. Значение по умолчанию: «16»
«Кол-во разделов на одном NBD-устройстве»	Максимальное количество разделов шаблона или базового образа Перемещаемого Профиля, доступных для одновременного монтирования. Значение по умолчанию: «1»
«URL сервера»	IP-адрес или FQDN для подключения к серверной части Termidesk Profiles. Значение по умолчанию: «0.0.0.0»
«Порт сервера»	Порт для подключения к серверной части Termidesk Profiles. Значение по умолчанию: «31337»
«Интервал проверки монтирования хранилища, сек.»	Периодичность (в секундах) проверок состояния монтирования хранилища. Если хранилище не смонтировано, выполняется попытка его смонтировать. Значение по умолчанию: «60»

Параметр	Описание
«Кол-во повторов проверки монтирования хранилища»	Количество проверок состояния монтирования хранилища. Если хранилище не смонтировано, выполняется попытка его смонтировать. Значение по умолчанию: «0»
«Интервал синхронизации NBD-слотов, сек.»	Периодичность (в секундах) проверок соответствия доступного количества NBD для подключения шаблонов и базовых образов Перемещаемого Профиля значению параметра «Кол-во NBD-устройств». Значение по умолчанию: «60»
«Кол-во повторов синхронизации NBD-слотов»	Количество проверок соответствия доступного количества NBD для подключения шаблонов и базовых образов Перемещаемого Профиля значению параметра «Кол-во NBD-устройств». Значение по умолчанию: «0»

Параметры безопасности Termidesk Profiles

Для конфигурации системных параметров безопасности следует перейти «Системные параметры - Системные настройки», выбрать раздел «Безопасность».

Доступные для редактирования параметры перечислены в столбце «Параметр» следующей таблицы (см. таблицу Параметры безопасности Termidesk Profiles).

Изменения параметров безопасности вступают в силу только после перезагрузки Termidesk Profiles.

Экранная кнопка **[Сохранить]** сохраняет параметры безопасности.

Таблица 301. Параметры безопасности Termidesk Profiles

Параметр	Описание
«Схема URL»	Протокол для подключения к серверной части Termidesk Profiles. Значение по умолчанию: «https»
«Путь к ключу сертификата»	Путь к ключу сертификата для защищенного подключения к серверной части Termidesk Profiles. Значение по умолчанию: «/etc/opt/termidesk/trp/certs/key.pem»
«Путь к сертификату»	Путь к файлу сертификата для защищенного подключения к серверной части Termidesk Profiles. Значение по умолчанию: «/etc/opt/termidesk/trp/certs/cert.crt»
«Разрешённые источники»	Список разрешенных источников для взаимодействия с API серверной части Termidesk Profiles. Значение по умолчанию: «*»

Параметр	Описание
«Разрешённые HTTP-методы»	Выбор разрешенных запросов для взаимодействия с API серверной части Termidesk Profiles. Возможные значения: • «GET»; • «POST»; • «PUT»; • «DELETE»; • «OPTIONS»; • «PATCH» Значение по умолчанию: «GET, POST, PUT, DELETE, OPTIONS, PATCH»
«Разрешённые заголовки»	Список разрешенных заголовков для взаимодействия с API серверной части Termidesk Profiles. Значение по умолчанию: «*»
«Разрешить отправку учётных данных»	Разрешение передачи учетных данных при взаимодействии с API серверной части Termidesk Profiles. Возможные значения: • «Включено» - разрешить передачу; • «Выключено» - запретить передачу
«Макс. время кеширования CORS, сек.»	Время (в секундах) кэширования результатов проверки CORS API серверной части Termidesk Profiles. Значение по умолчанию: «86400»

Параметры конфигурирования агентской части

Параметры конфигурирования агентской части Termidesk Profiles могут быть заданы в конфигурационном файле `/etc/opt/termidesk/trp/trp-agent.toml`.

Для применения параметров конфигурирования нужно выполнить перезапуск службы `trp-agent`:

```
sudo systemctl restart trp-agent
```

Описание параметров файла приведено в таблице Параметры конфигурационного файла агентской части Termidesk Profiles.

Таблица 302. Параметры конфигурационного файла агентской части Termidesk Profiles

Параметр	Значение по умолчанию	Описание
Секция `[agent]`		
`url`	`"0.0.0.0"`	IP-адрес или FQDN для подключения к агентской части
`port`	`31337`	Порт для подключения к агентской части
`schema`	`"http"`	Протокол для подключения к агентской части
`cert`	`"/etc/opt/termidesk/trp/certs/cert.crt"`	Путь к файлу сертификата для защищенного подключения к агентской части

Параметр	Значение по умолчанию	Описание
key	"/etc/opt/termidesk/trp/certs/key.pem"	Путь к ключу сертификата для защищенного подключения к агентской части
Секция [server]		
server_name	"trp.example.ru"	IP-адрес или FQDN для подключения к серверной части
server_schema	"https"	Протокол для подключения к серверной части
server_port	31337	Порт для подключения к серверной части
Секция [cors]		
allowed_origins	["*",]	Список разрешенных источников для взаимодействия с API агентской части
allowed_methods	["GET", "POST", "PUT", "DELETE", "OPTIONS", "PATCH",]	Список разрешенных запросов для взаимодействия с API агентской части
allowed_headers	["*",]	Список разрешенных заголовков для взаимодействия с API агентской части
allow_credentials	true	Разрешение передачи учетных данных при взаимодействии с API агентской части. Возможные значения: • «true» - разрешить передачу; • «false» - запретить передачу
max_age	86400	Время (в секундах) кэширования результатов проверки CORS API агентской части
Секция [logging]		
level	"DEBUG"	Уровень журналирования агентской части. Возможные значения: • «DEBUG»; • «INFO»; • «ERROR»; • «WARNING»
backup_count	5	Количество резервных копий файла журнала
max_size_bytes	2097152	Максимальный размер (в байтах) файла журнала
file_path	"/var/log/termidesk/trp/trp-agent.log"	Путь к файлу журнала агентской части

Файл /etc/default/trp-server

Одним из параметров службы trp-server является аргумент EnvironmentFile, задающий путь к дополнительным аргументам запуска, перечисленным в файле /etc/default/trp-server.

Файл /etc/default/trp-server:

- является обязательным и создается после установки серверной части (см. подраздел **Установка, обновление и удаление серверной части**);
- если он существует, то происходит его построчное чтение в формате <ключ>=<значение> и в запускаемый процесс добавляются переменные окружения, которые указаны в этом

файле (см. подраздел **Переменные окружения**).

Файл /etc/default/trp-agent

Одним из параметров службы trp-agent является аргумент EnvironmentFile, задающий путь к дополнительным аргументам запуска, перечисленным в файле /etc/default/trp-agent.

Файл /etc/default/trp-agent:

- является обязательным и создается после установки агентской части (см. подраздел **Установка, обновление и удаление агентской части**);
- если он существует, то происходит его построчное чтение в формате <ключ>=<значение> и в запускаемый процесс добавляются переменные окружения, которые указаны в этом файле (см. подраздел **Переменные окружения**).

Переменные окружения

Перечень переменных окружения, используемых серверной частью Termidesk Profiles, приведена в таблице Перечень переменных окружения серверной части Termidesk Profiles.

Для задания переменных окружения в ОС Linux для серверной части должен использоваться файл /etc/default/trp-server (см. подраздел **Файл /etc/default/trp-server**).

Таблица 303. Перечень переменных окружения серверной части Termidesk Profiles

Параметр	Значение по умолчанию	Описание
TRP_SERVER__DB__USER	termidesktrp	Имя пользователя БД для подключения к БД. Параметр задавался при создании БД
TRP_SERVER__DB__PASSWORD	ksedimret	Пароль для подключения к БД. Параметр задавался при создании БД
TRP_SERVER__DB__HOST	127.0.0.1	IP-адрес или FQDN узла с установленной СУБД
TRP_SERVER__DB__PORT	5432	Номер порта, используемого для соединения с сервером СУБД
TRP_SERVER__DB__NAME	trp_base01	Наименование БД. Параметр задавался при создании БД
TRP_SERVER__DB__POOL_MIN_SIZE	10	Минимальное количество постоянных подключений к БД
TRP_SERVER__DB__POOL_MAX_SIZE	200	Максимальное количество подключений к БД
TRP_SERVER__DB__POOL_TIMEOUT	30	Время ожидания (в секундах) подключения к БД
TRP_SECRET_KEY	Не задано	Секретный ключ для преобразования пароля сервисной учетной записи, используемой для подключения к службам каталогов. После сохранения пароля значение параметра изменять не рекомендуется. При изменении параметра ранее сохраненные значения не смогут быть преобразованы. Значение ключа задается произвольно

Перечень переменных окружения, используемых агентской частью Termidesk Profiles, приведена в таблице Перечень переменных окружения агентской части Termidesk Profiles.

Для задания переменных окружения в ОС Linux для агентской части должен использоваться файл `/etc/default/trp-agent` (см. подраздел **Файл `/etc/default/trp-agent`**).

Таблица 304. Перечень переменных окружения агентской части Termidesk Profiles

Параметр	Значение по умолчанию	Описание
`TRP_AGENT_TIMEOUT_REQUEST`	`30`	Время ожидания (в секундах) выполнения запросов агентской частью Termidesk Profiles
`DB_FILE_PATH`	`/opt/trp/src/trp-agent/trp_agent.db`	Путь к файлу БД агентской части Termidesk Profiles
`TRP_AGENT_VERIFY_REQUEST`	`True`	Управление проверкой SSL-сертификата в режиме использования протокола HTTPS. Возможные значения: • `True` - проверка SSL-сертификата включена. Режим работы: HTTPS с проверкой сертификата; • `False` (по умолчанию) - проверка SSL-сертификата отключена. Режим работы: HTTPS без проверки сертификата, или HTTP (режим работы задается в параметре `schema` конфигурационного файла `/etc/opt/termidesk/trp/trp-agent.toml`); • `<путь_к_файлу_сертификата>` - проверка SSL-сертификата включена. Режим работы: HTTPS с проверкой сертификата, указанного в значении этого параметра

TERMIDESK PROFILES. СИСТЕМА АУДИТА

Системные параметры аудита

Для конфигурации системных параметров аудита следует перейти «Системные параметры - Системные настройки», выбрать раздел «Аудит».

Доступные для редактирования параметры перечислены в столбце «Параметр» следующей таблицы (см. таблицу Параметры аудита Termidesk Profiles).

Изменения параметров аудита вступают в силу только после перезагрузки Termidesk Profiles.

Экранная кнопка **[Сохранить]** сохраняет параметры аудита.

Таблица 305. Параметры аудита Termidesk Profiles

Параметр	Описание
«Сохранять в файл аудита»	Управление сохранением событий аудита серверной части Termidesk Profiles в файл журнала. Возможные значения: • «Включено» (по умолчанию) - записывать сообщения в файл журнала; • «Выключено» - не записывать сообщения в файл журнала
«Путь до файла»	Путь к файлу журнала серверной части Termidesk Profiles. Значение по умолчанию: «/var/log/termidesk/trp/trp-server-audit.log»

Параметр	Описание
«Макс. размер файла журнала, байт»	Максимальный размер (в байтах) файла журнала. Значение по умолчанию: «2097152»
«Количество резервных копий»	Количество резервных копий файла журнала. Значение по умолчанию: «5»
«Сохранять в БД»	Управление сохранением событий аудита серверной части Termidesk Profiles в БД. Возможные значения: • «Включено» (по умолчанию) - записывать сообщения в БД; • «Выключено» - не записывать сообщения в БД
«Время хранения записи в БД, сут.»	Время хранения (в сутках) событий аудита серверной части Termidesk Profiles в БД. Значение по умолчанию: «365»
«Отправлять в Syslog»	Управление перенаправлением потока событий аудита серверной части Termidesk Profiles на отдельный syslog-сервер. Syslog-сервер должен быть предварительно настроен для корректного получения событий аудита серверной части Termidesk Profiles. Возможные значения: • «Включено» - перенаправлять сообщения на отдельный syslog-сервер; • «Выключено» (по умолчанию) - не перенаправлять сообщения на отдельный syslog-сервер
«Адреса узлов Syslog»	IP-адреса или имена узлов, на которых развернута служба syslog-сервера
«Протокол»	Выбор протокола работы для службы syslog-сервера. Возможные значения: «UDP», «TCP», «TLS»
«Категория сообщения»	Выбор категории сообщений syslog для их классификации при передаче в журнал мониторинга. Параметр не влияет на состав регистрируемых событий и запись сообщений в файл журнала. Значение по умолчанию: «local7»

Просмотр событий аудита серверной части Termidesk Profiles

Просмотр списка событий аудита

Для просмотра списка событий, связанных с действиями субъектов доступа, следует перейти «Журналы - Аудит» (см. рисунок Отображение событий аудита в графическом интерфейсе управления Termidesk Profiles).

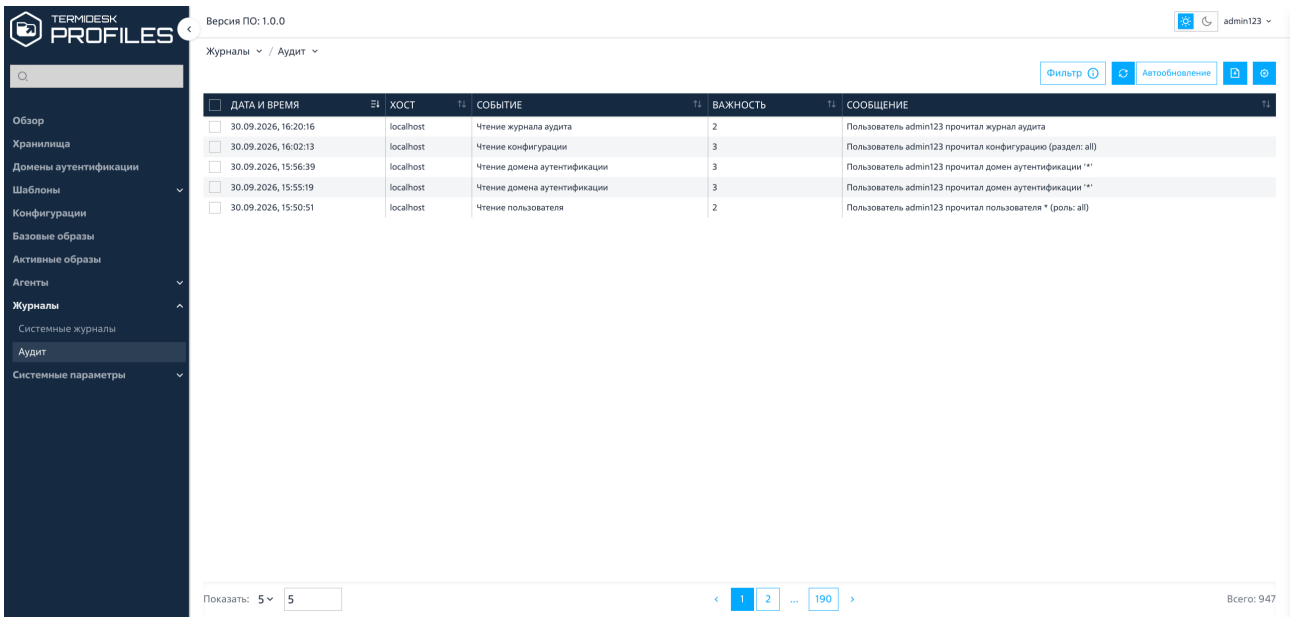


Рисунок 151. Отображение событий аудита в графическом интерфейсе управления Termidesk Profiles

Фильтрация списков событий аудита

Для списка событий аудита доступен механизм фильтрации («Умный фильтр»). Фильтрация осуществляется путем задания значений для параметров «Атрибут», «Условие» и «Значение».

Для добавления дополнительного фильтра следует нажать экранную кнопку **[+]**. Для удаления фильтра нужно использовать экранную кнопку **[-]** в соответствующей строке.

Чтобы применить установленные параметры фильтрации, следует нажать экранную кнопку **[Применить]**.

Экранная кнопка **[Очистить]** возвращает параметры фильтра к исходному состоянию: удаляются дополнительные строки фильтра, все значения сбрасываются, поля «Условие» и «Значение» блокируются.

При ручном вводе данных в поле фильтра «Значение» допускается полный или частичный ввод только одного параметра фильтрации.

При применении нескольких одинаковых фильтров к списку фильтрация выполняется с учетом только последнего заданного фильтра.

Подробное описание параметров механизма фильтрации списка событий приведено в таблице (см. таблицу Параметры фильтрации событий аудита).

Таблица 306. Параметры фильтрации событий аудита

Атрибут	Условия	Значение
«Дата и время»	Формирование списка событий по времени создания: • «В пределах» – в указанном временном промежутке; • «Не в пределах» – исключая указанный временной промежуток	Ручной ввод посредством выбора даты и времени (графический элемент)

Атрибут	Условия	Значение
«Идентификатор события»	Формирование списка событий по идентификатору. Возможное значение: «Содержит» - формирует список событий, включающих указанную часть идентификатора	Ручной ввод
«Событие»	Формирование списка событий по событию. Возможное значение: «Содержит» - формирует список событий, включающих указанную часть события	Ручной ввод
«Важность»	Формирование списка событий по уровню важности: • «Выше или равен» - выше или равных указанному уровню; • «Ниже или равен» - ниже или равных указанному уровню	Ручной ввод
«Хост»	Формирование списка событий по IP-адресу или FQDN узла. Возможное значение: «Содержит» - формирует список событий, включающих указанную часть IP-адреса или FQDN узла	Ручной ввод
«Сообщение»	Формирование списка событий по сообщению. Возможное значение: «Содержит» - формирует список событий, включающих указанную часть сообщения	Ручной ввод

TERMIDESK PROFILES. ЖУРНАЛИРОВАНИЕ

Системные параметры журналирования

Для конфигурации системных параметров журналирования следует перейти «Системные параметры - Системные настройки», выбрать раздел «Журналы».

Доступные для редактирования параметры перечислены в столбце «Параметр» следующей таблицы (см. таблицу Параметры журналирования Termidesk Profiles).

Изменения параметров журналирования вступают в силу только после перезагрузки Termidesk Profiles.

Экранная кнопка **[Сохранить]** сохраняет параметры журналирования.

Таблица 307. Параметры журналирования Termidesk Profiles

Параметр	Описание
«Уровень логирования»	Выбор минимального уровня событий, записываемых в журнал мониторинга. Возможные значения: • «ERROR» - запись сообщений уровней «ERROR», «CRITICAL»; • «WARNING» - запись сообщений уровней «WARNING», «ERROR», «CRITICAL»; • «INFO» - запись сообщений уровней «INFO», «WARNING», «ERROR», «CRITICAL»; • «DEBUG» - запись сообщений уровней «DEBUG», «INFO», «WARNING», «ERROR», «CRITICAL». Значение по умолчанию: «INFO»
«Сохранять в файл журнала»	Управление сохранением событий серверной части Termidesk Profiles в файл журнала. Возможные значения: • «Включено» (по умолчанию) - записывать сообщения в файл журнала; • «Выключено» - не записывать сообщения в файл журнала
«Путь до файла»	Путь к файлу журнала серверной части Termidesk Profiles. Значение по умолчанию: «/var/log/termidesk/trp/trp-server.log»
«Макс. размер файла журнала, байт»	Максимальный размер (в байтах) файла журнала. Значение по умолчанию: «2097152»
«Количество резервных копий»	Количество резервных копий файла журнала. Значение по умолчанию: «5»
«Сохранять в БД»	Управление сохранением событий серверной части Termidesk Profiles в БД. Возможные значения: • «Включено» (по умолчанию) - записывать сообщения в БД; • «Выключено» - не записывать сообщения в БД
«Время хранения записи в БД, сут.»	Время хранения (в сутках) событий серверной части Termidesk Profiles в БД. Значение по умолчанию: «365»
«Отправлять в Syslog»	Управление перенаправлением потока событий серверной части Termidesk Profiles на отдельный syslog-сервер. Syslog-сервер должен быть предварительно настроен для корректного получения событий журналов серверной части Termidesk Profiles. Возможные значения: • «Включено» - перенаправлять сообщения на отдельный syslog-сервер; • «Выключено» (по умолчанию) - не перенаправлять сообщения на отдельный syslog-сервер
«Адреса узлов Syslog»	IP-адреса или имена узлов, на которых развернута служба syslog-сервера

Параметр	Описание
«Протокол»	Выбор протокола работы для службы syslog-сервера. Возможные значения: «UDP», «TCP», «TLS»
«Категория сообщения»	Выбор категории сообщений syslog для их классификации при передаче в журнал мониторинга. Параметр не влияет на состав регистрируемых событий и запись сообщений в файл журнала. Значение по умолчанию: «local6»

Журналы

Журналы серверной части Termidesk Profiles

Журналы работы серверной части Termidesk Profiles ведутся в файлах:

- `/var/log/termidesk/trp/trp-server-audit.log` - используется для записи событий аудита серверной части Termidesk Profiles;
- `/var/log/termidesk/trp/trp-server.log`- используется для записи событий серверной части Termidesk Profiles.

Журналы агентской части Termidesk Profiles

Журналы работы агентской части Termidesk Profiles ведутся в файлах:

- `/var/log/termidesk/trp/mount.log` - используется для записи событий и ошибок модуля монтирования;
- `/var/log/termidesk/trp/agent.log` - используется для записи событий агентской части Termidesk Profiles.

Просмотр журналов серверной части Termidesk Profiles

Просмотр системного журнала

Для просмотра общего журнала событий, связанного с функционированием Termidesk Profiles, следует перейти «Журналы - Системные журналы», где визуализируются системные события с указанием уровня важности (CRITICAL, ERROR, WARNING, INFO, DEBUG) и источника возникновения события (см. рисунок Отображение общего журнала в графическом интерфейсе управления Termidesk Profiles).

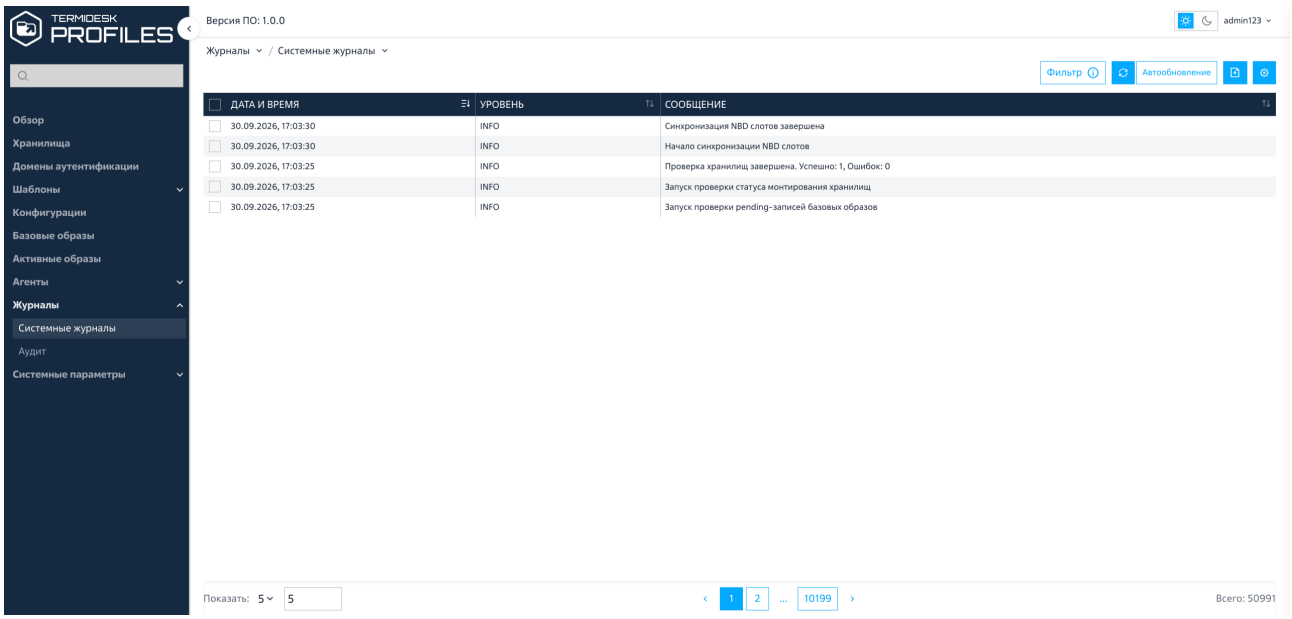


Рисунок 152. Отображение общего журнала в графическом интерфейсе управления Termidesk Profiles

Фильтрация списков событий журналов

Для списка событий журналов доступен механизм фильтрации («Умный фильтр»). Фильтрация осуществляется путем задания значений для параметров «Атрибут», «Условие» и «Значение».

Для добавления дополнительного фильтра следует нажать экранную кнопку **[+]**. Для удаления фильтра нужно использовать экранную кнопку **[-]** в соответствующей строке.

Чтобы применить установленные параметры фильтрации, следует нажать экранную кнопку **[Применить]**.

Экранная кнопка **[Очистить]** возвращает параметры фильтра к исходному состоянию: удаляются дополнительные строки фильтра, все значения сбрасываются, поля «Условие» и «Значение» блокируются.

При ручном вводе данных в поле фильтра «Значение» допускается полный или частичный ввод только одного параметра фильтрации.

При применении нескольких одинаковых фильтров к списку фильтрация выполняется с учетом только последнего заданного фильтра.

Подробное описание параметров механизма фильтрации списка событий приведено в таблице (см. таблицу Параметры фильтрации событий журналов).

Таблица 308. Параметры фильтрации событий журналов

Атрибут	Условия	Значение
«Дата и время»	Формирование списка событий по времени создания: • «В пределах» - в указанном временном промежутке; • «Не в пределах» - исключая указанный временной промежуток	Ручной ввод посредством выбора даты и времени (графический элемент)

Атрибут	Условия	Значение
«Уровень»	Формирование списка событий по уровню: • «Выше» - выше указанного уровня; • «Выше или равен» - выше или равных указанному уровню; • «Ниже» - ниже указанного уровня; • «Ниже или равен» - ниже или равных указанному уровню; • «Равен» - равных указанному уровню	• «DEBUG»; • «INFO»; • «WARNING»; • «ERROR»; • «CRITICAL»
«Сообщение»	Формирование списка событий по сообщению: • «Является» - по указанному сообщению; • «Не является» - исключая указанное сообщение; • «Начинается с» - по начальной части сообщения; • «Оканчивается на» - по конечной части сообщения; • «Содержит» - включая указанную часть сообщения; • «Не содержит» - исключая указанную часть сообщения	Ручной ввод

TERMIDESK PROFILES. ВЕБ-ИНТЕРФЕЙС СЕРВЕРНОЙ ЧАСТИ

Доступ к веб-интерфейсу серверной части

Веб-интерфейс является приоритетным способом настройки и управления серверной частью Termidesk Profiles.

Доступ к веб-интерфейсу серверной части Termidesk Profiles осуществляется из веб-браузера с указанием URL-адреса: `https://<IP-адрес_или_FQDN_узла>:31337`.

После установки вход в интерфейс управления Termidesk Profiles доступен только авторизованному пользователю ОС, являющемуся членом группы `termidesk`.

При наличии только домена аутентификации с типом «Встроенный» на странице подключения нужно заполнить экранные поля:

- «Имя пользователя» – идентификатор субъекта с ролью «Администратор»;
- «Пароль» – набор символов, подтверждающий назначение полномочий.

При последующих сеансах входа после добавления нового домена аутентификации заполняется дополнительное экранное поле:

- «Способ входа» – источник сведений о субъектах и их полномочиях.

Обзор доступных функций веб-интерфейса

Функции системной панели

Системная панель представляет собой фиксированную область в верхней части веб-

интерфейса, предназначенную для отображения служебной информации и элементов управления (см. рисунок Системная панель в графическом интерфейсе управления Termidesk Profiles).

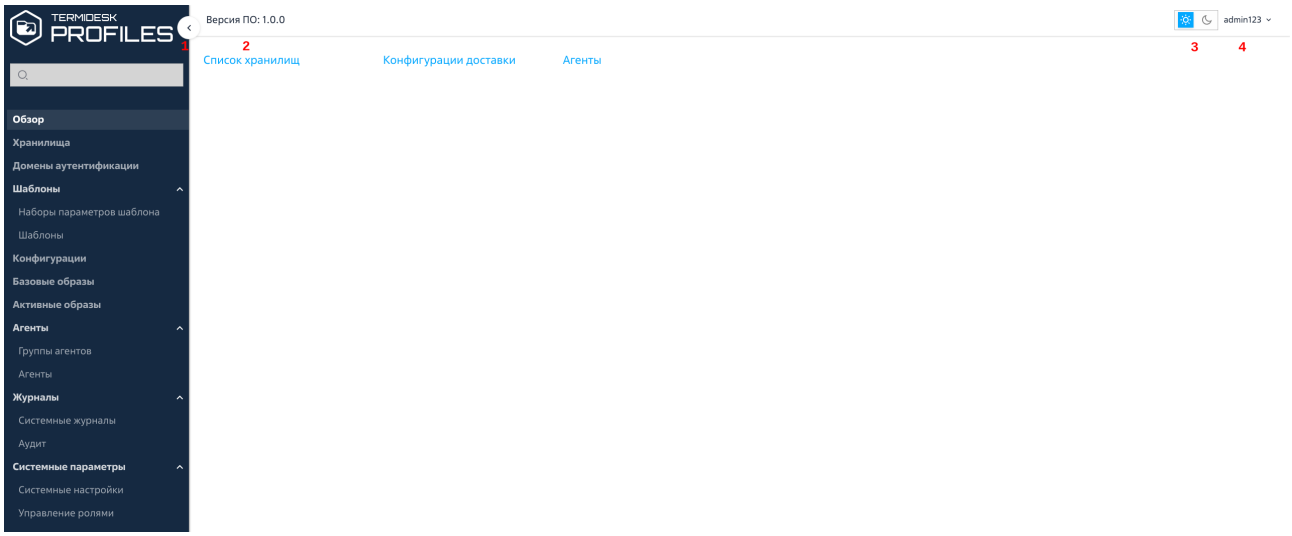


Рисунок 153. Системная панель в графическом интерфейсе управления Termidesk Profiles

Системная панель представлена следующими элементами:

- элемент (1): скрывает или отображает список функций в левой части веб-интерфейса;
- элемент (2): отображает сведения о текущей версии Termidesk Profiles;
- элемент (3): изменяет тему оформления графического интерфейса;
- элемент (4): позволяет выполнить выход из веб-интерфейса.

Доступные функции веб-интерфейса

Список функций, доступных для настройки через веб-интерфейс, приведен в таблице Описание разделов веб-интерфейса.

Таблица 309. Описание разделов веб-интерфейса

Параметр	Описание
«Обзор»	Содержит ссылки для быстрого перехода на страницы: • «Список хранилищ» - выполняет переход на страницу «Хранилища»; • «Конфигурации доставки» - выполняет переход на страницу «Конфигурации»; • «Агенты» - выполняет переход на страницу «Группы агентов»
«Хранилища»	Определяет настройку взаимодействия с сетевыми хранилищами
«Домены аутентификации»	Определяет настройку взаимодействия с источниками сведений о субъектах и их полномочиях
«Шаблоны»	При нажатии в левой части веб-интерфейса на функцию «Шаблоны» открывается список процедур для управления шаблонами и параметрами конфигурации шаблонов
«Наборы параметров шаблона»	Позволяет управлять параметрами конфигурации шаблонов
«Шаблоны»	Позволяет создавать шаблоны Перемещаемых Профилей
«Конфигурации»	Определяет параметры доставки Перемещаемых Профилей группам пользователей доменов аутентификации

Параметр	Описание
«Базовые образы»	Позволяет просматривать список базовых образов Перемещаемых Профилей
«Активные образы»	Позволяет просматривать список активных образов Перемещаемых Профилей
«Агенты»	При нажатии в левой части веб-интерфейса на функцию «Агенты» открывается список процедур для управления группами агентов и просмотра списка агентов
«Группы агентов»	Позволяет управлять параметрами конфигурации группы агентов
«Агенты»	Позволяет просматривать список агентов
«Журналы»	При нажатии в левой части веб-интерфейса на функцию «Журналы» открывается список процедур для просмотра и выгрузки в файл событий действий субъектов доступа в интерфейсе управления, а также событий функционирования Termidesk Profiles
«Системные журналы»	Позволяет просматривать и выгружать в log-файл события функционирования Termidesk Profiles
«Аудит»	Позволяет просматривать, выгружать в log-файл и копировать отдельные строки событий действий пользователей и администраторов
«Системные параметры»	При нажатии в левой части веб-интерфейса на функцию «Системные параметры» открывается список процедур для конфигурации системных параметров Termidesk Profiles
«Системные настройки»	Определяет системную конфигурацию Termidesk Profiles
«Управление ролями»	Задает параметры доступа к интерфейсу управления на основе ролевой модели

Доступные элементы управления веб-интерфейсом

Для повышения удобства работы с веб-интерфейсом предусмотрены элементы управления, позволяющие настраивать отображение данных.

Список элементов управления, доступных для настройки отображения данных, приведен в таблице Элементы управления веб интерфейсом.

Таблица 310. Элементы управления веб интерфейсом

Графический элемент	Описание
Фильтр	Фильтрация значений таблицы. Если фильтр задан, то при наведении на графический элемент отображаются параметры фильтрации. Для сброса параметров фильтрации следует воспользоваться экранной кнопкой **[Очистить]**
	Ручное обновление значений таблицы
Автообновление	Интервал автоматического обновления значений таблицы. Если интервал задан, то отображается периодичность обновления значений таблицы. Пример: 30 секунд

Графический элемент	Описание
	Выгрузка значений таблицы в `log`-файл. Поддерживается: • выгрузка всех записей таблицы; • выгрузка выбранных записей таблицы
	Управление составом и порядком следования столбцов таблицы. Для изменения списка отображаемых столбцов нужно отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться соответствующей экранной кнопкой: **[Сбросить видимость]** или **[Сбросить порядок]**. Экранная кнопка будет заблокирована, если нет изменений для возврата к исходному состоянию
ДАТА И ВРЕМЯ УРОВЕНЬ 25.08.2026, 18:25:06 INFO	Управление шириной столбца таблицы. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить ширину]** графического элемента
ДАТА И ВРЕМЯ УРОВЕНЬ 25.08.2026, 18:25:06 INFO	Управление сортировкой записей таблицы. Поддерживается: • - сортировка по убыванию; • - сортировка по возрастанию; • - применение сортировки к другому столбцу таблицы
ДАТА И ВРЕМЯ УРОВЕНЬ 25.08.2026, 18:25:06 INFO 25.08.2026, 18:25:06 ERROR 25.08.2026, 18:25:06 ERROR	Множественный выбор записей таблицы. Для множественного выбора записей нужно: • пометить строки флажком; • зажать клавишу **<Ctrl>** и нажать левой кнопкой мыши по нужным строкам
Показать: 10	Выбор количества отображаемых записей на одной странице. Для настройки нужно выбрать одно из предлагаемых значений, отображаемых в выпадающем списке графического элемента или ввести свой вариант в поле ввода
‹ 1 2 ... 6859 ›	Переход между страницами списка записей таблицы

TERMIDESK PROFILES. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

Интерфейс командной строки серверной части Termidesk Profiles

Утилита trp_cli

Утилита trp_cli используется для настройки серверной части Termidesk Profiles из интерфейса командной строки.

Доступные команды утилиты trp_cli приведены в таблице (см. таблицу Список доступных команд утилиты trp_cli).

Таблица 311. Список доступных команд утилиты trp_cli

Параметр	Описание
--help	Вывод справки по использованию аргументов командной строки. Для вызова справки нужно выполнить: `sudo /opt/termidesk/trp-server/sbin/trp_cli --help`
--version	Вывод версии приложения. Для вывода версии нужно выполнить: `sudo /opt/termidesk/trp-server/sbin/trp_cli --version`
--admin-username, -U	Запуск приложения от имени администратора. При использовании домена аутентификации MS AD учетная запись администратора указывается в формате UPN (admin@domain.local) или в формате короткого имени учетной записи (admin). При использовании домена аутентификации OIDC формат учетной записи администратора зависит от используемой службы идентификации IdP. Например: • при использовании Keycloak указывается имя учетной записи (admin); • при использовании Google указывается адрес электронной почты (admin@idp.local). Пример использования: `sudo /opt/termidesk/trp-server/sbin/trp_cli --admin-username <admin@domain.local>`

Параметр	Описание
`config`	Управление системными настройками серверной части Termidesk Profiles. Управление параметрами конфигурирования доступно только авторизованному пользователю ОС, являющегося членом группы `termidesk`. Список параметров, доступных для управления системными настройками приведен в таблице Перечень доступных параметров для управления системными настройками. Поддерживаются подкоманды: • `list` - вывод конфигурационных параметров и их значений; • `update` - обновление значения параметра. Подкоманда `list` принимает аргументы: • `-s` - секция. Подкоманда `update` принимает аргументы: • `-s` - секция; • `-k` - ключ; • `-v` - значение. Пример использования: `sudo /opt/termidesk/trp-server/sbin/trp_cli config update -s general -k nbds.nbds_max -v 32`
`passphrase`	Получение пароля преобразованного образа Перемещаемого Профиля пользователя. Команда `passphrase` принимает аргументы: • `-u` - имя пользователя в домене аутентификации MS AD; • `-d` - имя домена аутентификации MS AD; • `-i` - наименование преобразованного образа. Пример использования: `sudo /opt/termidesk/trp-server/sbin/trp_cli passphrase -u <username> -d <domain.local> -i <win10>`

Таблица 312. Перечень доступных параметров для управления системными настройками

Параметр	Описание
Секция `audit`	

Параметр	Описание
`audit.file.enable`	Управление сохранением событий аудита серверной части Termidesk Profiles в файл журнала. Возможные значения: • «True» - записывать сообщения в файл журнала; • «False» - не записывать сообщения в файл журнала
`audit.file.path`	Путь к файлу журнала серверной части Termidesk Profiles
`audit.file.backup_count`	Количество резервных копий файла журнала
`audit.file.max_size`	Максимальный размер (в байтах) файла журнала
`audit.database.enable`	Управление сохранением событий аудита серверной части Termidesk Profiles в БД. Возможные значения: • «True» - записывать сообщения в БД; • «False» - не записывать сообщения в БД
`audit.database.record_ttl`	Время хранения (в сутках) событий аудита серверной части Termidesk Profiles в БД
`audit.syslog.enable`	Управление перенаправлением потока событий аудита серверной части Termidesk Profiles на отдельный syslog-сервер. Возможные значения: • «True» - перенаправлять сообщения на отдельный syslog-сервер; • «False» - не перенаправлять сообщения на отдельный syslog-сервер
`audit.syslog.addresses`	IP-адреса или имена узлов, на которых развернута служба syslog-сервера
`audit.syslog.socktype`	Выбор протокола работы для службы syslog-сервера. Возможные значения: • «UDP»; • «TCP»; • «TLS»
`audit.syslog.facility`	Категория сообщений syslog для их классификации при передаче в журнал мониторинга
Секция `general`	
`nbds.nbds_max`	Максимальное количество шаблонов и базовых образов Перемещаемого Профиля, доступных для одновременной настройки и подключения
`nbds.max_part`	Максимальное количество разделов шаблона или базового образа Перемещаемого Профиля, доступных для одновременного монтирования
`server.url`	IP-адрес или FQDN для подключения к серверной части Termidesk Profiles
`server.port`	Порт для подключения к серверной части Termidesk Profiles
`tasks.storage_mount.interval`	Периодичность (в секундах) проверок состояния монтирования хранилища
`tasks.storage_mount.repetitions`	Количество проверок состояния монтирования хранилища
`tasks.nbd_sync.interval`	Периодичность (в секундах) проверок соответствия доступного количества NBD для подключения шаблонов и базовых образов Перемещаемого профиля значению параметра `nbds.nbds_max`

Параметр	Описание
tasks.nbd_sync.repetitions	Количество проверок соответствия доступного количества NBD для подключения шаблонов и базовых образов Перемещаемого Профиля значению параметра nbds.nbds_max
Секция monitoring	
logging.level	Минимальный уровень событий, записываемых в журнал мониторинга. Возможные значения: • «ERROR»; • «WARNING»; • «INFO»; • «DEBUG»
logging.file.enable	Управление сохранением событий серверной части Termidesk Profiles в файл журнала. Возможные значения: • «True» - записывать сообщения в файл журнала; • «False» - не записывать сообщения в файл журнала
logging.file.path	Путь к файлу журнала серверной части Termidesk Profiles
logging.file.backup_count	Количество резервных копий файла журнала
logging.file.max_size	Максимальный размер (в байтах) файла журнала
logging.database.enable	Управление сохранением событий серверной части Termidesk Profiles в БД. Возможные значения: • «True» - записывать сообщения в БД; • «False» - не записывать сообщения в БД
logging.database.record_ttl	Время хранения (в сутках) событий серверной части Termidesk Profiles в БД
logging.syslog.enable	Управление перенаправлением потока событий серверной части Termidesk Profiles на отдельный syslog-сервер. Возможные значения: • «True» - перенаправлять сообщения на отдельный syslog-сервер; • «False» - не перенаправлять сообщения на отдельный syslog-сервер
logging.syslog.addresses	IP-адреса или имена узлов, на которых развернута служба syslog-сервера
logging.syslog.socktype	Выбор протокола работы для службы syslog-сервера. Возможные значения: • «UDP»; • «TCP»; • «TLS»
logging.syslog.facility	Категория сообщений syslog для их классификации при передаче в журнал мониторинга
Секция security	
server.schema_url	Протокол для подключения к серверной части Termidesk Profiles

Параметр	Описание
server.cert_key	Путь к ключу сертификата для защищенного подключения к серверной части Termidesk Profiles
server.cert_path	Путь к файлу сертификата для защищенного подключения к серверной части Termidesk Profiles
cors.allowed_origins	Список разрешенных источников для взаимодействия с API серверной части. Пример использования: `sudo /opt/termidesk/trp-server/sbin/trp_cli config update -s security -k cors.allowed_origins -v "['*']"`
cors.allowed_methods	Список разрешенных запросов для взаимодействия с API серверной части. Возможные значения: «"GET"», «"POST"», «"PUT"», «"DELETE"», «"OPTIONS"», «"PATCH"» Пример использования: `sudo /opt/termidesk/trp-server/sbin/trp_cli config update -s security -k cors.allowed_methods -v "['GET', 'POST']"`
cors.allowed_headers	Список разрешенных заголовков для взаимодействия с API серверной части. Пример использования: `sudo /opt/termidesk/trp-server/sbin/trp_cli config update -s security -k cors.allowed_headers -v "['*']"`
cors.allow_credentials	Разрешение передачи учетных данных при взаимодействии с API серверной части. Возможные значения: • «True» - разрешить передачу; • «False» - запретить передачу. Пример использования: `sudo /opt/termidesk/trp-server/sbin/trp_cli config update -s security -k cors.allow_credentials -v True`
cors.max_age	Время (в секундах) кэширования результатов проверки CORS API серверной части Пример использования: `sudo /opt/termidesk/trp-server/sbin/trp_cli config update -s security -k cors.max_age -v 86400`

TERMIDESK PROFILES. НЕШТАТНЫЕ СИТУАЦИИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

Возможные неисправности при работе с Перемещаемыми профилями и способы их устранения приведены в таблице Перечень возможных нештатных ситуаций и способов их устранения.

Таблица 313. Перечень возможных нештатных ситуаций и способов их устранения

Индикация	Описание	Возможное решение
При повторном подключении преобразованного образа Перемещаемого Профиля отсутствуют созданные ранее файлы	После отключения и повторного подключения преобразованного образа Перемещаемого Профиля файлы, созданные пользователем в предыдущем сеансе, отсутствуют	Для сохранения изменений пользователь должен завершить сеанс штатными средствами ОС: например, в ОС Astra Linux Special Edition перейти «Звезда - Управление сеансами - Завершение сеанса»

ТЕРМИНЫ

Базовый образ Перемещаемого Профиля

Образ файловой системы Перемещаемого Профиля. Используется для создания активного образа Перемещаемого Профиля

Активный образ Перемещаемого Профиля

Временный образ Перемещаемого Профиля, созданный на основе базового образа. Активный образ Перемещаемого Профиля используется для записи данных, меняющихся в течение сессии пользователя, и последующего их сохранения в базовый образ

Домен аутентификации

Способ проверки субъектов и их полномочий

Ключ

Применяется в контексте файла, не опции в команде. Последовательность псевдослучайных чисел, сгенерированная особым образом

Перемещаемый Профиль

Размещенный в централизованном хранилище образ диска или каталог с пользовательскими данными и настройками, автоматически подключающийся при авторизации в ОС РМ

Рабочее место

Гостевая ОС виртуальной машины или ОС, установленная на выделенном компьютере, к которой подключается пользователь

Сертификат

Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу

Шаблон

Файл образа Перемещаемого Профиля с набором параметров

Хранилище

Централизованная система хранения данных, используемая для размещения базовых образов и файлов, необходимых для работы Перемещаемого Профиля

СОКРАЩЕНИЯ

БД	База данных
ЗПС	Замкнутая программная среда
ОС	Операционная система
РМ	Рабочее место
СУБД	Система управления базами данных
ЭЦП	Электронная цифровая подпись
API	Application Programming Interface (интерфейс прикладного программирования)
CORS	Cross-Origin Resource Sharing (междоменный обмен ресурсами)
DN	Domain Name (доменное имя)
FQDN	Fully Qualified Domain Name (полностью определенное имя домена)
FreeIPA	Free Identity, Policy and Audit (открытое решение по безопасности Linux-систем)
HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
IdP	Identity Provider (сервис, управляющий идентификационной информацией)
IP	Internet Protocol (межсетевой протокол)
JSON	JavaScript Object Notation (стандартный текстовый формат для структурированных данных)
LDAP	Lightweight Directory Access Protocol (легковесный протокол доступа к службам каталогов)
LDAPS	Lightweight Directory Access Protocol over SSL/TSL (расширение протокола LDAP)
MS AD	Microsoft Active Directory (службы каталогов Microsoft)
NBD	Network Block Device (сетевое блочное устройство)
NFS	Network File System (сетевая файловая система)
OU	Organizational Unit (организационная единица)
PAM	Pluggable Authentication Module (подключаемый модуль аутентификации)
SMB	Server Message Block (протокол для удалённого доступа к сетевым ресурсам)
SSL	Secure Sockets Layer (криптографический протокол)
URL	Uniform Resource Locator (унифицированный указатель ресурса)
UUID	Universally Unique Identifier (уникальный идентификатор)

СЛЕТ.10001-01 92 01. РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ. НАСТРОЙКА И ЭКСПЛУАТАЦИЯ КОМПОНЕНТА «КЛИЕНТ»

ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ

Назначение документа

Настоящий документ является руководством пользователя на компонент «Клиент» программного комплекса «Диспетчер подключений виртуальных рабочих мест Termidesk» (далее - Termidesk VDI, Termidesk VDI).

В этом руководстве приведено назначение, установка, настройка и эксплуатация компонента «Клиент».

Типографские соглашения

Приняты следующие типографские соглашения:

- `моноширинный шрифт` – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk VDI, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

КЛИЕНТ. ОБЩИЕ СВЕДЕНИЯ

Назначение компонента «Клиент»

Компонент «Клиент» (далее - Клиент) реализован в виде устанавливаемого пакета (`termidesk-client`), необходим для обработки URI, предоставляемых Termidesk VDI, и позволяет подключиться к рабочим местам (РМ) через протоколы SPICE, RDP, Loudplay, TERA.

Клиент устанавливается на пользовательскую рабочую станцию, с которой будет производиться подключение к РМ.

В Termidesk VDI предусмотрены следующие модели доставки:

- коллективные РМ - РМ создается в автоматическом режиме, назначается первому подключившемуся к нему пользователю и удаляется после выхода пользователя из гостевой операционной системы (ОС);
- индивидуальные РМ - РМ создается в автоматическом режиме и назначается определенному пользователю, который владеет им на протяжении жизненного цикла РМ. Жизненный цикл РМ определяется администратором.

Для отображения экрана РМ на пользовательской рабочей станции должна быть установлена программа доставки для соответствующего протокола (см. таблицу Протоколы и соответствующие им программы доставки).

Установка программного обеспечения (ПО Termidesk Viewer) обязательна, если используются протоколы доставки, отличные от HTML5.

Таблица 314. Протоколы и соответствующие им программы доставки

Протокол	Программа доставки	ОС	Примечание
HTML5	Веб-браузер	Любая ОС с веб-браузером	Веб-клиент Termidesk VDI позволяет получить экран РМ по протоколам HTML5 SPICE и HTML5 TERA через веб-браузер без необходимости установки Клиента, для этого администратором должен быть настроен протокол доставки «HTML5»
Loudplay	`LoudPlay-client`	Astra Linux Special Edition	Для подключения к РМ по протоколу доставки Loudplay необходимо дополнительно установить ПО LoudPlay-client, не входящее в состав Termidesk
	`streaming.exe`	Microsoft Windows	Для подключения к РМ по протоколу доставки Loudplay необходимо дополнительно установить ПО LoudPlay-client, не входящее в состав Termidesk
RDP	ПО Termidesk Viewer	Astra Linux Special Edition; Debian; Альт Рабочая станция; РЕД ОС; Ubuntu; macOS; Microsoft Windows	Требуется активировать опцию «Соединение по RDP через Termidesk Viewer» в настройках Клиента. Поддерживается запуск приложения Клиента при подключении к РМ из веб-браузера
SPICE	ПО Termidesk Viewer	Debian; Альт Рабочая станция; РЕД ОС; Ubuntu; macOS; Microsoft Windows	Установка ПО Termidesk Viewer выполняется после установки Клиента и приведена в соответствующих подразделах. Поддерживается запуск приложения Клиента при подключении к РМ из веб-браузера
TERA	ПО Termidesk Viewer	Astra Linux Special Edition; macOS; Debian 11; Microsoft Windows	Установка ПО Termidesk Viewer выполняется после установки Клиента и приведена в соответствующих подразделах. Поддерживается запуск приложения Клиента при подключении к РМ из веб-браузера

Работа с РМ через веб-браузер накладывает следующие ограничения:

- невозможность перенаправления аппаратных устройств в РМ;

- невозможность получения статистики сеанса и состояния канала.

Требования к аппаратному и программному обеспечению

Для установки Клиента и ПО Termidesk Viewer минимальные аппаратные требования пользовательской рабочей станции должны соответствовать следующим:

- процессор архитектуры Intel x86 с разрядностью 64 бит. Для некоторых ОС поддерживаются другие архитектуры, это указано в списке поддерживаемых ОС;
- оперативная память, не менее 1 ГБ;
- свободное дисковое пространство, не менее 200 МБ;
- сетевое соединение, не менее 100 Мбит/с.

Для установки Клиента и ПО Termidesk Viewer требования к ПО должны соответствовать следующим:

- должна быть установлена ОС из списка поддерживаемых;
- должен быть установлен веб-браузер с поддержкой спецификации W3C HTML5 (Яндекс.Браузер версии 15.9 и выше, Google Chrome версии 46 и выше, Mozilla Firefox версии 41 и выше).

Начиная с Termidesk VDI версии 6.1 в ПО Termidesk Viewer входит библиотека FreeRDP 3.x, что исключает зависимость от версии библиотеки FreeRDP, установленной в ОС.

Список поддерживаемых ОС:

- Astra Linux Special Edition 1.7 (1.7.5, 1.7.6, 1.7.7, 1.7.8, 1.7.9). Есть поддержка протокола TERA;
- Astra Linux Special Edition 1.8 (1.8.1, 1.8.2, 1.8.3, 1.8.4, 1.8.5, 1.8.6). Есть поддержка протокола TERA;
- Astra Linux Special Edition 4.7 (только архитектура ARM);
- Debian 11 LTS (дополнительно поддерживаются архитектуры x86_32, ARM). Есть поддержка протокола TERA;
- Debian 12 LTS;
- Альт Рабочая станция 10 (среда рабочего стола MATE не поддерживается);
- Альт Рабочая станция 11;
- РЕД ОС 7.3;
- РЕД ОС 8;
- Ubuntu 22.04 LTS;
- Ubuntu 24.04 LTS;
- macOS 14 (Sonoma). Есть поддержка протокола TERA, если он настроен без UDP и без механизма SASL;
- macOS 15 (Sequoia). Есть поддержка протокола TERA, если он настроен без UDP и без механизма SASL;
- macOS 26 (Tahoe). Есть поддержка протокола TERA, если он настроен без UDP и без механизма SASL;
- Microsoft Windows 10 1809 LTS. Есть поддержка протокола TERA, если он настроен без UDP;
- Microsoft Windows 10 2021 LTS. Есть поддержка протокола TERA, если он настроен без UDP;

- Microsoft Windows 11 LTSC 2024. Есть поддержка протокола TERA, если он настроен без UDP.

Требования к уровню подготовки персонала

Эксплуатация Клиента осуществляется субъектом доступа с ролью «Пользователь».

Субъект доступа должен иметь опыт работы с персональным компьютером на базе ОС GNU/Linux или Microsoft Windows на уровне пользователя и уверенно осуществлять базовые операции в этих ОС.

КЛИЕНТ. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ

Получение пакетов установки в ОС Astra Linux Special Edition

Дистрибутив представлен бинарным файлом пакета ПО в `deb`-формате. Установка в ОС Astra Linux Special Edition производится из локального репозитория, распространяемого в формате `iso`-образа.

Получить `iso`-образ можно двумя способами:

- заполнив запрос через сайт Termidesk VDI: https://termidesk.ru/support/#request-support;
- через личный кабинет:https://lk.astra.ru/.

Для подключения локального репозитория Termidesk VDI на узле, где предполагается установка, нужно:

- скопировать в домашний каталог пользователя образ диска `termidesk-<версия>.iso`;
- подключить образ диска к файловой системе в каталог `/mnt`:

```
sudo mount -o loop termidesk-<версия>.iso /mnt
```

где:

`-o loop` - параметры для привязки петлевого устройства (`/dev/loop`) к файлу `termidesk-<версия>.iso`, устройство затем монтируется в указанный каталог `/mnt`;

- скопировать содержимое каталога `repos` подключенного образа диска в каталог `/var` локальной файловой системы:

```
sudo cp -Rp /mnt/repos /var
```

где:

`-Rp` - ключ для рекурсивного копирования подкаталогов и файлов с сохранением исходных свойств;

- отключить подключенный ранее образ диска от узла:

```
sudo umount /mnt
```

- установить пакет `lsb-release`:

```
sudo apt install -y lsb-release
```

- добавить локальный репозиторий Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list` через командный интерпретатор `sh`:
  - выяснить установленную версию ОС:

    ```
    sudo cat /etc/astra_version
    ```

  - определить актуальное имя каталога с пакетами в `/var/repos`;
  - указать в файле конфигурации APT корректное (фактическое) имя каталога:

    ```
    sudo sh -c 'echo "deb file:/var/repos/astra 1.8_x86-64 non-free" >
    /etc/apt/sources.list.d/termidesk_local.list'
    ```

    где:

    `-c` - ключ для чтения команд из вводимой строки (стандартный ввод);

    `echo` - команда вывода текста, совместно с символом «>» используется для перенаправления строки в файл;

    `deb file:/var/repos/astra 1.8_x86-64 non-free` - добавляемый репозиторий с вложенной командой получения версии ОС;

    > Приведенный пример команды актуален для установки основных компонентов Termidesk, пакеты которых расположены в каталоге `1.8_x86-64`.

- для корректной установки компонентов TERA потребуется корректно подключить дополнительные репозитории и настроить их приоритет:
  - для версий ОС Astra Linux Special Edition меньше или равных 1.7.6, а также для версий 1.8.X:
    - подключить два репозитория:

      ```
      sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
      non-free" > /etc/apt/sources.list.d/termidesk_local.list'
      sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
      /dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
      ```

    - добавить повышенный приоритет для репозитория с требуемой версией ОС (значение `$(cat /etc/astra_version)` может подходить не для всех репозиториев, т.к. версия может указываться без точек - в этом случае нужно вручную указать корректную версию):

      ```
      sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
      ```

```
Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000
EOF"
```

- для версий ОС Astra Linux Special Edition 1.7.7 и 1.7.8:
  - подключить три репозитория:

```
sudo sh -c 'echo "deb file:/var/repos/astra 1.7.6 non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
/dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

  - настроить два приоритета:

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=1.7.6
Pin-Priority: 950

Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000

EOF"
```

- выполнить поиск ключа репозитория Termidesk VDI `GPG-KEY-PUBLIC` и добавить его:

```
sudo cat /var/repos/astra/GPG-KEY-PUBLIC | sudo gpg --dearmour -o
/etc/apt/trusted.gpg.d/termidesk.gpg
```

- убедиться, что ключ `release@uveon.ru` был успешно добавлен:

```
apt-key list
```

В случае, если ключ не отображен в выводе команды, необходимо убедиться, что ключ `GPG-KEY-PUBLIC` существует:

```
cat /var/repos/astra/GPG-KEY-PUBLIC
```

Если ключ все же существует, следует проверить правильность выполнения шагов по добавлению репозитория Termidesk VDI в файл

/etc/apt/sources.list.d/termidesk_local.list.

При успешном выполнении всех шагов команда выведет содержимое ключа в формате Base64.

В зависимости от используемой версии ОС команды добавления ключа репозитория Termidesk VDI могут отличаться. Если для ОС Astra Linux Special Edition 1.8 ключ репозитория был добавлен командой, применимой к другой версии ОС, то для исправления нужно:

- узнать идентификатор добавленного ключа репозитория:

```
apt-key list
```

- удалить ключ:

```
apt-key --keyring /etc/apt/trusted.gpg del 4E1632CC
```

где 4E1632CC - последние 8 символов идентификатора ключа;

- вновь добавить ключ репозитория.

- обновить данные пакетного менеджера:

```
sudo apt update
```

- проверить настройку приоритетов репозиториев:

```
apt-cache policy
```

Команду sudo apt update необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.

Получение пакетов установки через Интернет-репозиторий

Для получения пакетов установки может использоваться Интернет-репозиторий: https://repos.termidesk.ru/.

Для подключения репозитория в ОС Astra Linux Special Edition нужно:

- установить пакеты:

```
sudo apt install -y lsb-release wget apt-transport-https debian-keyring
```

где:

-y - ключ для пропуска подтверждения установки;

- добавить Интернет-репозиторий Termidesk VDI в файл

/etc/apt/sources.list.d/termidesk_local.list через командный интерпретатор sh:

- выяснить установленную версию ОС:

```
sudo cat /etc/astra_version
```

- определить актуальное имя каталога с пакетами в https://repos.termidesk.ru/astra;
- указать в файле конфигурации APT корректное (фактическое) имя каталога:

```
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra 1.8_x86-64 non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
```

где:

-c - ключ для чтения команд из вводимой строки (стандартный ввод);

echo - команда вывода текста, совместно с символом «>» используется для перенаправления строки в файл;

deb https://repos.termidesk.ru/astra <···> - добавляемый репозиторий;

Приведенный пример команды актуален для установки основных компонентов Termidesk, пакеты которых расположены в каталоге 1.8_x86-64.

- для корректной установки компонентов TERA потребуется корректно подключить дополнительные репозитории и настроить их приоритет:
  - для версий ОС Astra Linux Special Edition меньше или равных 1.7.6, а также для версий 1.8.X:
    - подключить два репозитория:

```
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(cat
/etc/astra_version) non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(lsb_release -cs
2> /dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

    - добавить повышенный приоритет для репозитория с требуемой версией ОС (значение $(cat /etc/astra_version) может подходить не для всех репозиториев, т.к. версия может указываться без точек - в этом случае нужно вручную указать корректную версию):

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000
EOF"
```

- для версий ОС Astra Linux Special Edition 1.7.7 и 1.7.8:
  - подключить три репозитория:

```
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra 1.7.6 non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(cat
/etc/astra_version) non-free" >>
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(lsb_release -cs
2> /dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

  - настроить два приоритета:

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=1.7.6
Pin-Priority: 950

Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000

EOF"
```

- получить ключ репозитория Termidesk VDI `GPG-KEY-PUBLIC` и добавить его в ОС:
  - для ОС Astra Linux Special Edition 1.7:

```
wget --no-check-certificate -qO - https://repos.termidesk.ru/astra/GPG-KEY-
PUBLIC | sudo apt-key add -
```

  - для ОС Astra Linux Special Edition 1.8:

```
wget --no-check-certificate -qO - https://repos.termidesk.ru/astra/GPG-KEY-
PUBLIC |  sudo gpg --dearmour -o /etc/apt/trusted.gpg.d/termidesk.gpg
```

- обновить данные пакетного менеджера:

```
sudo apt update
```

- проверить настройку приоритетов репозиториев:

```
apt-cache policy
```

Команду `sudo apt update` необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.

Команды добавления ключа репозитория Termidesk VDI отличаются в зависимости от используемой версии ОС.

Если для ОС Astra Linux Special Edition 1.8 ключ репозитория был добавлен командой, применимой к другой версии ОС, то для исправления нужно:

- узнать идентификатор добавленного ключа репозитория:

```
apt-key list
```

- удалить ключ:

```
apt-key --keyring /etc/apt/trusted.gpg del 4E1632CC
```

где `4E1632CC` - последние 8 символов идентификатора ключа;

- вновь добавить ключ репозитория.

КЛИЕНТ. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ

ОС Astra Linux Special Edition

Установка Клиента и ПО Termidesk Viewer в ОС Astra Linux Special Edition

Для установки Клиента и ПО Termidesk Viewer нужно:

Минимальная необходимая версия ПО Termidesk Viewer - 7.0, поскольку в зависимости от версии ПО Termidesk Viewer передача Клиентом параметров подключения к РМ будет отличаться:

- если версия выше или соответствует 7.0, то параметры будут переданы Клиентом в преобразованном виде и ПО Termidesk Viewer запустится;
- если версия ниже 7.0, то Клиент не передаст параметры и ПО Termidesk Viewer не запустится.

- подключить сетевой или локальный репозиторий Termidesk VDI;
- открыть программу «Терминал Fly» и получить доступ к интерфейсу командной строки;
- выполнить установку Клиента:

```
sudo apt -y install termidesk-client
```

Для ОС Astra Linux Special Edition 4.7 необходимо установить также `libtera-client` и `termidesk-viewer`:

```
sudo apt -y install libtera-client
```

```
sudo apt -y install termidesk-viewer
```

Начиная с Termidesk VDI версии 7.0 отдельная установка пакетов `libtera-client` и `termidesk-viewer` не требуется, поскольку их функционал включен в пакет `termidesk-client`.

После установки Клиента в ОС автоматически добавится в автозагрузку и запустится служба `termidesk-tbus`, необходимая для взаимодействия компонентов Termidesk VDI.

Установка в режиме ЗПС

Замкнутая программная среда (ЗПС) является средством повышения безопасности ОС путем контроля целостности (неизменности) файлов.

Механизм контроля реализован в виде невыгружаемого модуля ядра ОС Astra Linux Special Edition (модуль `digsig_verif`), выполняющего проверку электронной цифровой подписи файлов (ЭЦП).

Перед установкой компонентов Termidesk VDI необходимо установить пакет `termidesk-digsig-keys`, для этого:

- подключить репозиторий Termidesk VDI или получить отдельный пакет `termidesk-digsig-keys` из репозитория;
- выполнить установку с использованием репозитория:

```
sudo apt -y install termidesk-digsig-keys
```

- либо выполнить установку из `deb`-пакета:

```
sudo apt install -y /home/user/termidesk-digsig-keys-XXXXXX_amd64.deb
```

где:

`-y` - ключ для пропуска подтверждения установки;

`/home/user/termidesk-digsig-keys-XXXXXX_amd64.deb` - расположение пакета `termidesk-digsig-keys-XXXXXX_amd64.deb`.

- перезагрузить ОС:

```
sudo reboot
```

- выполнить установку компонента Termidesk VDI.

Для ЗПС может быть активирован режим проверки встроенной ЭЦП в расширенных атрибутах (`DIGSIG_XATTR_MODE`). В этом случае потребуется подписать файлы, которые будут проходить проверку, имеющимися в организации ключами. Информация о процессе подписи и активации механизма проверки встроенной ЭЦП в расширенных атрибутах приведена в справочном центре Astra Linux: https://wiki.astralinux.ru/pages/viewpage.action?pageId=41190634.

Постановка Клиента и ПО Termidesk Viewer на контроль целостности

После установки и настройки Клиента и ПО Termidesk Viewer необходимо поставить их на контроль целостности.

Для контроля целостности используются встроенные в ОС Astra Linux Special Edition программные средства на основе `Another File Integrity Checker`, представленного пакетом `afick`.

Настройка регламентного контроля целостности выполняется в конфигурационном файле `/etc/afick.conf`.

Настройку следует производить только после окончательного внедрения компонента, поскольку с файлов конфигурации и исполняемых файлов будут сняты эталонные контрольные суммы.

Для постановки на контроль целостности Клиента и ПО Termidesk Viewer необходимо добавить в конфигурационный файл `/etc/afick.conf` следующие строки:

```
/usr/bin/termidesk-client PARSEC
/usr/share/applications/termidesk-client.desktop PARSEC
/usr/share/applications/vdi-viewer.desktop PARSEC
/usr/share/doc/termidesk-client PARSEC
/usr/share/doc/termidesk-viewer PARSEC
/usr/share/termidesk-client PARSEC
/usr/share/termidesk-viewer PARSEC
/usr/bin/vdi-viewer PARSEC
/usr/bin/vdi-proxy  PARSEC

#Репозиторий Termidesk VDI (если используется)
/var/repos/ PARSEC
```

Для снятия эталонных значений контрольных сумм используется команда:

```
afick -i
```

Для проверки соответствия контрольных сумм эталонным значениям автоматически создаются задания в системном планировщике заданий `cron`.

Для ручной проверки соответствия контрольных сумм используется команда:

```
afick -k
```

В случае отсутствия по какой-либо причине исполняемых фалов `*.pyc`, они будут повторно сгенерированы при перезапуске сервера Python. В этом случае нужно повторно проинициализировать средство регламентного контроля целостности `afick`.

Обновление Клиента и ПО Termidesk Viewer в ОС Astra Linux Special Edition

Обновление Клиента и ПО Termidesk Viewer в среде ОС Astra Linux Special Edition выполняется установкой новой версии поверх предыдущей.

Начиная с Termidesk VDI версии 7.0 отдельное обновление пакетов `libtera-client` и `termidesk-viewer` не требуется, поскольку их функционал включен в пакет `termidesk-client`. Для обновления нужно установить новую версию пакета `termidesk-client` поверх предыдущей. Ранее установленные пакеты `libtera-client` и `termidesk-viewer` будут автоматически удалены.

Минимальная необходимая версия ПО Termidesk Viewer - 7.0, поскольку в зависимости от версии ПО Termidesk Viewer передача Клиентом параметров подключения к РМ будет отличаться:

- если версия выше или соответствует 7.0, то параметры будут переданы Клиентом в преобразованном виде и ПО Termidesk Viewer запустится;
- если версия ниже 7.0, то Клиент не передаст параметры и ПО Termidesk Viewer не запустится.

Удаление Клиента и ПО Termidesk Viewer в ОС Astra Linux Special Edition

Удаление Клиента и ПО Termidesk Viewer из среды ОС Astra Linux Special Edition выполняется командами:

```
sudo apt purge --autoremove termidesk-client
sudo apt purge --autoremove termidesk-viewer
```

Другие ОС Linux

Установка Клиента и ПО Termidesk Viewer в других ОС Linux

Установка Клиента и ПО Termidesk Viewer в ОС Ubuntu, Debian 12 выполняется командой:

```
sudo apt -y install <путь_к_пакету_termidesk-client>
```

Для всех остальных поддерживаемых ОС установка Клиента и ПО Termidesk Viewer выполняется командами:

```
sudo apt -y install <путь_к_пакету_termidesk-client>
sudo apt -y install <путь_к_пакету_termidesk-viewer>
```

Где:

`-y` - ключ для пропуска подтверждения установки.

Минимальная необходимая версия ПО Termidesk Viewer - 7.0, поскольку в зависимости от версии ПО Termidesk Viewer передача Клиентом параметров подключения к РМ будет отличаться:

- если версия выше или соответствует 7.0, то параметры будут переданы Клиентом в преобразованном виде и ПО Termidesk Viewer запустится;
- если версия ниже 7.0, то Клиент не передаст параметры и ПО Termidesk Viewer не запустится.

После установки Клиента в ОС автоматически добавится в автозагрузку и запуститься служба `termidesk-tbus`, необходимая для взаимодействия компонентов Termidesk VDI.

В зависимости от дистрибутива ОС Linux, а именно пакетного менеджера, команда установки может отличаться от приведенной.

Например, для пакетного менеджера `yum` команда будет:

```
sudo yum -y install <путь_к_пакету_termidesk-client>
```

Обновление Клиента и ПО Termidesk Viewer в других ОС Linux

Обновление Клиента и ПО Termidesk Viewer выполняется установкой новой версии пакетов `termidesk-client` и `termidesk-viewer` поверх предыдущих.

Минимальная необходимая версия ПО Termidesk Viewer - 7.0, поскольку в зависимости от версии ПО Termidesk Viewer передача Клиентом параметров подключения к РМ будет отличаться:

- если версия выше или соответствует 7.0, то параметры будут переданы Клиентом в преобразованном виде и ПО Termidesk Viewer запустится;
- если версия ниже 7.0, то Клиент не передаст параметры и ПО Termidesk Viewer не запустится.

Удаление Клиента и ПО Termidesk Viewer в других ОС Linux

Удаление Клиента и ПО Termidesk Viewer выполняется командами:

```
sudo apt purge --autoremove termidesk-client
sudo apt purge --autoremove termidesk-viewer
```

Где:

`-y` - ключ для пропуска подтверждения удаления.

В зависимости от дистрибутива ОС Linux, а именно пакетного менеджера, команда удаления может отличаться от приведенной.

Например, для пакетного менеджера `yum` команда будет:

```
sudo yum -y remove termidesk-client
```

ОС macOS

Установка Клиента и ПО Termidesk Viewer в ОС macOS

Установка Клиента и ПО Termidesk Viewer в ОС macOS производится из образа, распространяемого в формате `dmg`.

Пример наименования образов:

- `termidesk-client-<версия>.dmg`;
- `termidesk-viewer-<версия>.dmg`.

Для установки Клиента и ПО Termidesk Viewer в ОС macOS в графическом интерфейсе нужно:

> Минимальная необходимая версия ПО Termidesk Viewer - 7.0, поскольку в зависимости от версии ПО Termidesk Viewer передача Клиентом параметров подключения к РМ будет отличаться:
>
> - если версия выше или соответствует 7.0, то параметры будут переданы Клиентом в преобразованном виде и ПО Termidesk Viewer запустится;
> - если версия ниже 7.0, то Клиент не передаст параметры и ПО Termidesk Viewer не запустится.

- открыть `dmg`-образ (образ будет автоматически примонтирован к файловой системе ОС);
- открыть файловый менеджер «Finder», скопировать содержимое `dmg`-образов в каталог «Программы».

> Для корректного взаимодействия Клиента и ПО Termidesk Viewer их нужно разместить в каталоге «Программы». Возможность установки Клиента и ПО Termidesk Viewer в другие каталоги не поддерживается.
>
> Для подключения к РМ с проверкой сертификата нужно установить сертификаты в соответствии с подразделом **Установка корневых сертификатов в ОС macOS**.

Для установки Клиента и ПО Termidesk Viewer в ОС macOS через интерфейс командной строки нужно:

- подключить `dmg`-образы к файловой системе ОС:

```
hdiutil attach <путь_к_файлу_termidesk-client-<версия>.dmg>
hdiutil attach <путь_к_файлу_termidesk-viewer-<версия>.dmg>
```

- скопировать содержимое `dmg`-образов в каталог `/Applications`:

```
cp -R /Volumes/termidesk-client/Termidesk Client.app /Applications
cp -R /Volumes/termidesk-viewer/Termidesk Viewer.app /Applications
```

- отключить подключенные ранее образы.

Отключить образ можно:

- либо командами:

```
hdiutil detach /Volumes/termidesk-client
hdiutil detach /Volumes/termidesk-viewer
```

- либо через файловый менеджер «Finder» (см. рисунок Отключение образа через «Finder»), для этого:
  - найти иконку смонтированного образа в боковой панели «Finder»;
  - щелкнуть левой кнопкой мыши по иконке отключения образа.

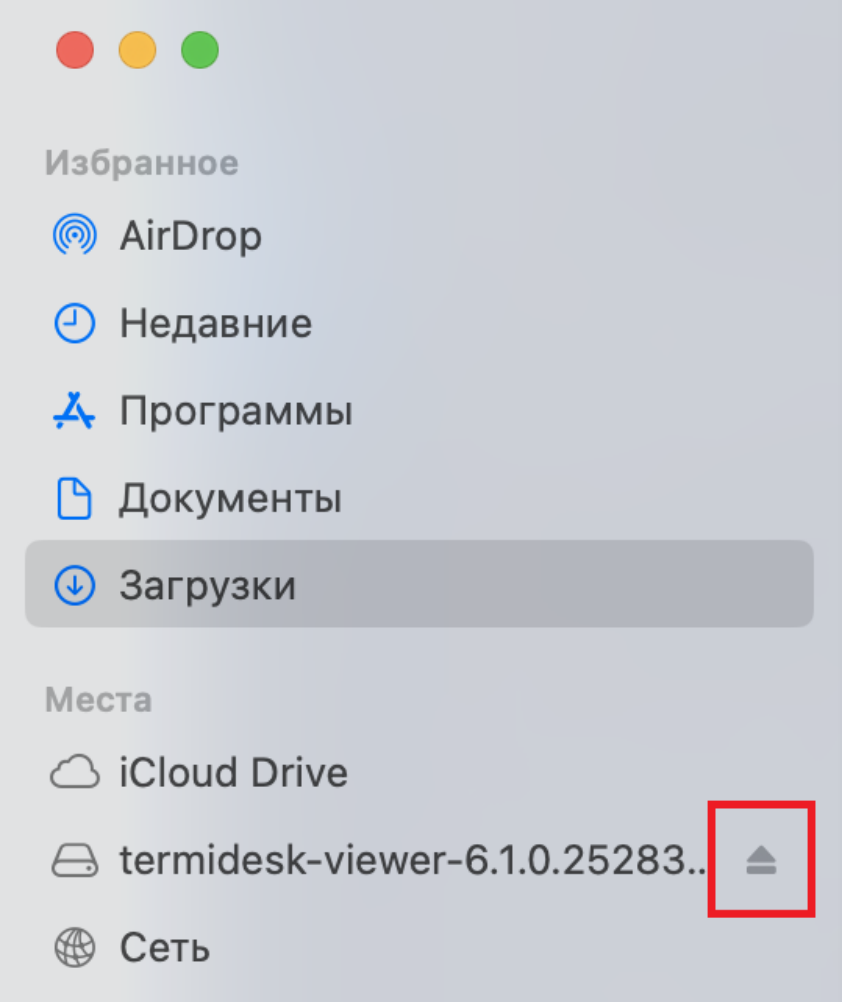


Рисунок 154. Отключение образа через «Finder»

Обновление Клиента и ПО Termidesk Viewer в ОС macOS

Обновление Клиента и ПО Termidesk Viewer в ОС macOS выполняется установкой новой версии поверх предыдущей.

Минимальная необходимая версия ПО Termidesk Viewer - 7.0, поскольку в зависимости от версии ПО Termidesk Viewer передача Клиентом параметров подключения к РМ будет отличаться:

- если версия выше или соответствует 7.0, то параметры будут переданы Клиентом в преобразованном виде и ПО Termidesk Viewer запустится;
- если версия ниже 7.0, то Клиент не передаст параметры и ПО Termidesk Viewer не запустится.

Удаление Клиента и ПО Termidesk Viewer в ОС macOS

Для удаления Клиента и ПО Termidesk Viewer в ОС macOS в графическом интерфейсе нужно (см. рисунок Удаление через «Finder»):

- открыть файловый менеджер «Finder» и перейти в каталог «Программы»;
- выбрать «Termidesk Client», нажать правой кнопкой мыши и в контекстном меню выбрать пункт «Переместить в Корзину»;
- выбрать «Termidesk Client», нажать правой кнопкой мыши и в контекстном меню выбрать пункт «Переместить в Корзину».

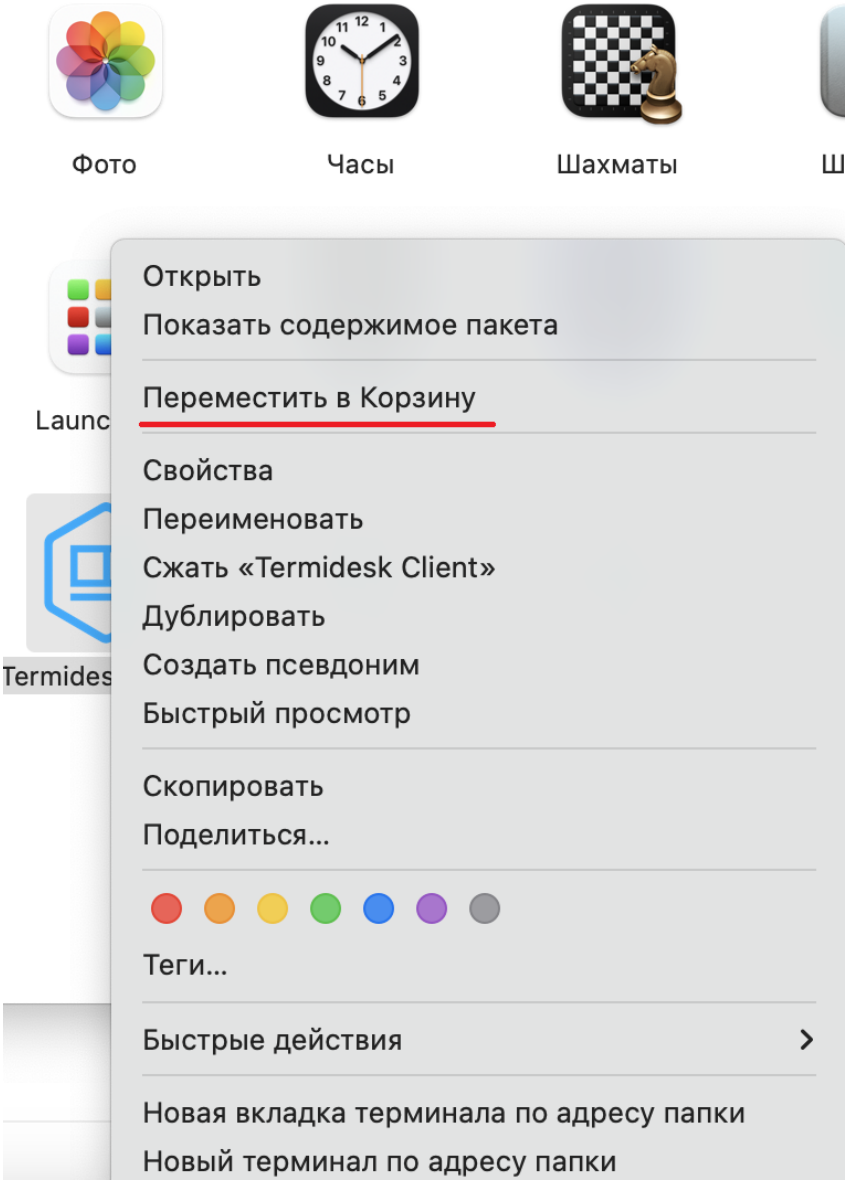


Рисунок 155. Удаление через «Finder»

После удаления следует очистить оставшиеся конфигурационные файлы, для этого:

- нажать «Переход - Переход к папке» и перейти в каталог `~/.config`;
- удалить каталог «UVEON».

Удаление Клиента и ПО Termidesk Viewer в ОС macOS через интерфейс командной строки выполняется командами:

```
rm -rf /Applications/Termidesk Client.app
rm -rf /Applications/Termidesk Viewer.app
```

Затем нужно очистить оставшиеся конфигурационные файлы:

```
rm -rf ~/.config/UVEON
```

ОС Microsoft Windows

Установка Клиента и ПО Termidesk Viewer в ОС Microsoft Windows

Клиент для ОС Microsoft Windows распространяется в виде установочного файла с расширением `msi`.

Для подключения к РМ по протоколу доставки Loudplay необходимо дополнительно установить ПО LoudPlay-client, не входящее в состав Termidesk VDI.

Уменьшение версии через операцию установки не поддерживается. Для перехода к предыдущей версии следует удалить текущую установленную версию.

Для корректного функционирования Клиента необходимо, чтобы установка, запуск и подключение к РМ выполнялось от пользователя, имя которого задано на латинице. Подключение по протоколу RDP от пользователя с кириллическим именем может завершиться ошибкой.

Если в ОС включен контроль учетных записей пользователя (User Account Control, UAC), то для успешной установки компонентов нужно разрешить внесение изменений в системе в соответствующем окне уведомления.

Для установки Клиента на пользовательской рабочей станции нужно:

Минимальная необходимая версия ПО Termidesk Viewer - 7.0, поскольку в зависимости от версии ПО Termidesk Viewer передача Клиентом параметров подключения к РМ будет отличаться:

- если версия выше или соответствует 7.0, то параметры будут переданы Клиентом в преобразованном виде и ПО Termidesk Viewer запустится;
- если версия ниже 7.0, то Клиент не передаст параметры и ПО Termidesk Viewer не запустится.

- запустить установочный файл и нажать экранную кнопку **[Далее]**;
- ознакомиться с лицензионным соглашением (см. рисунок Лицензионное соглашение). Для принятия условий лицензионного соглашения и продолжения установки следует отметить поле «Я принимаю условия лицензионного соглашения» и нажать экранную кнопку **[Далее]**;

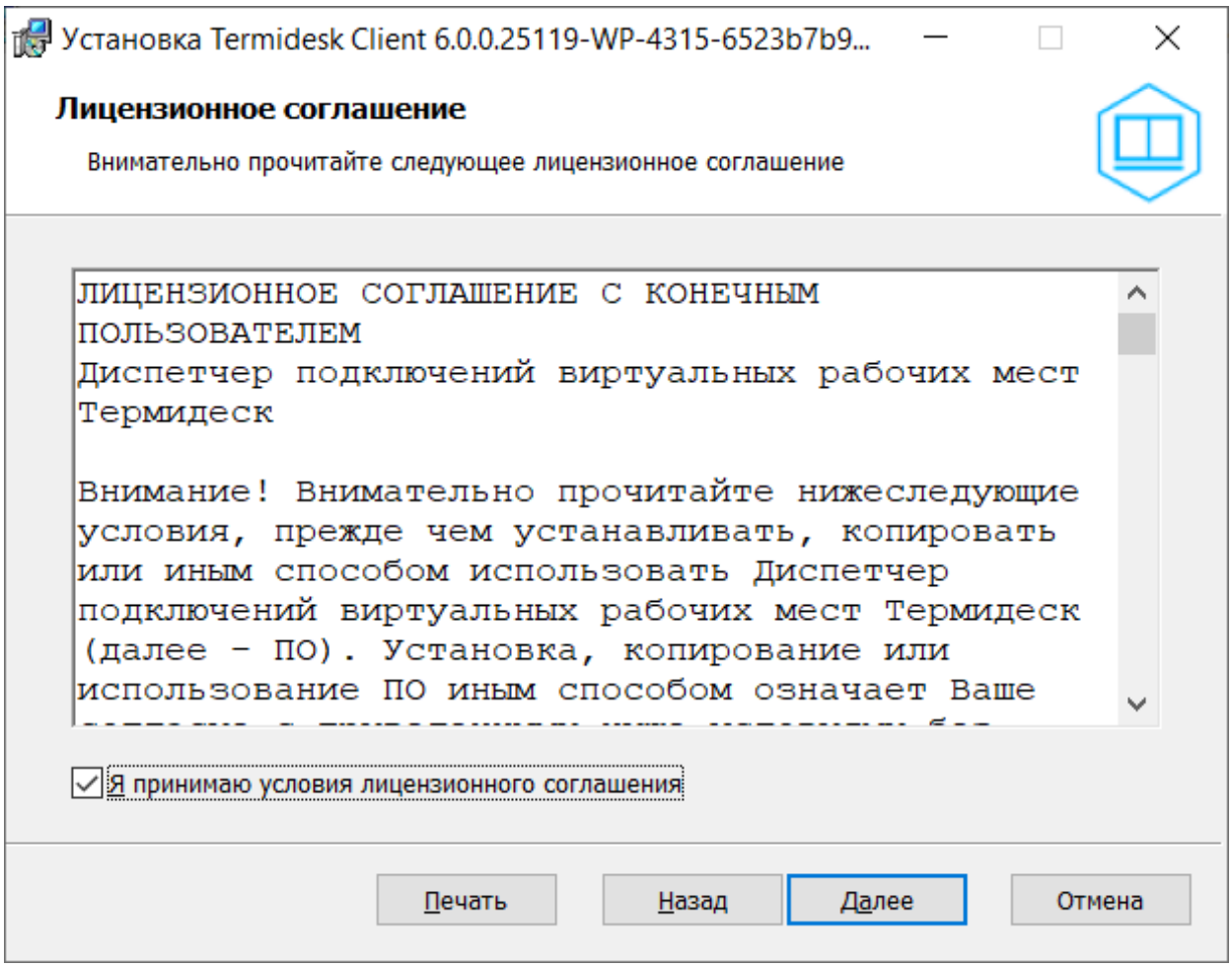


Рисунок 156. Лицензионное соглашение

- выбрать тип установки (см. рисунок Окно выбора типа установки в ОС Windows):
  - «Только для меня»: установка будет выполнена в каталог `%LocalAppData%\Programs\UVEON\Termidesk Client`. Каталог установки поменять нельзя;
  - «Для всех пользователей (требуются права администратора)»: по умолчанию установка будет выполнена в каталог `C:\Program Files\UVEON\Termidesk Client`. Каталог установки можно поменять;

Для работы функционала Kerberos-аутентификации нужно выбрать установку с типом «Для всех пользователей (требуются права администратора)». С этим типом установки потребуется разрешить внесение изменений в системе в соответствующем окне уведомления.

При установке с типом «Только для меня» у пользователя не будет возможности изменить список компонентов после установки, экранная кнопка **[Изменить]** будет недоступна.

Путь установки должен содержать только символы латиницы. Установка в каталог с кириллическими символами может привести к ошибкам при подключении к РМ по протоколу RDP.

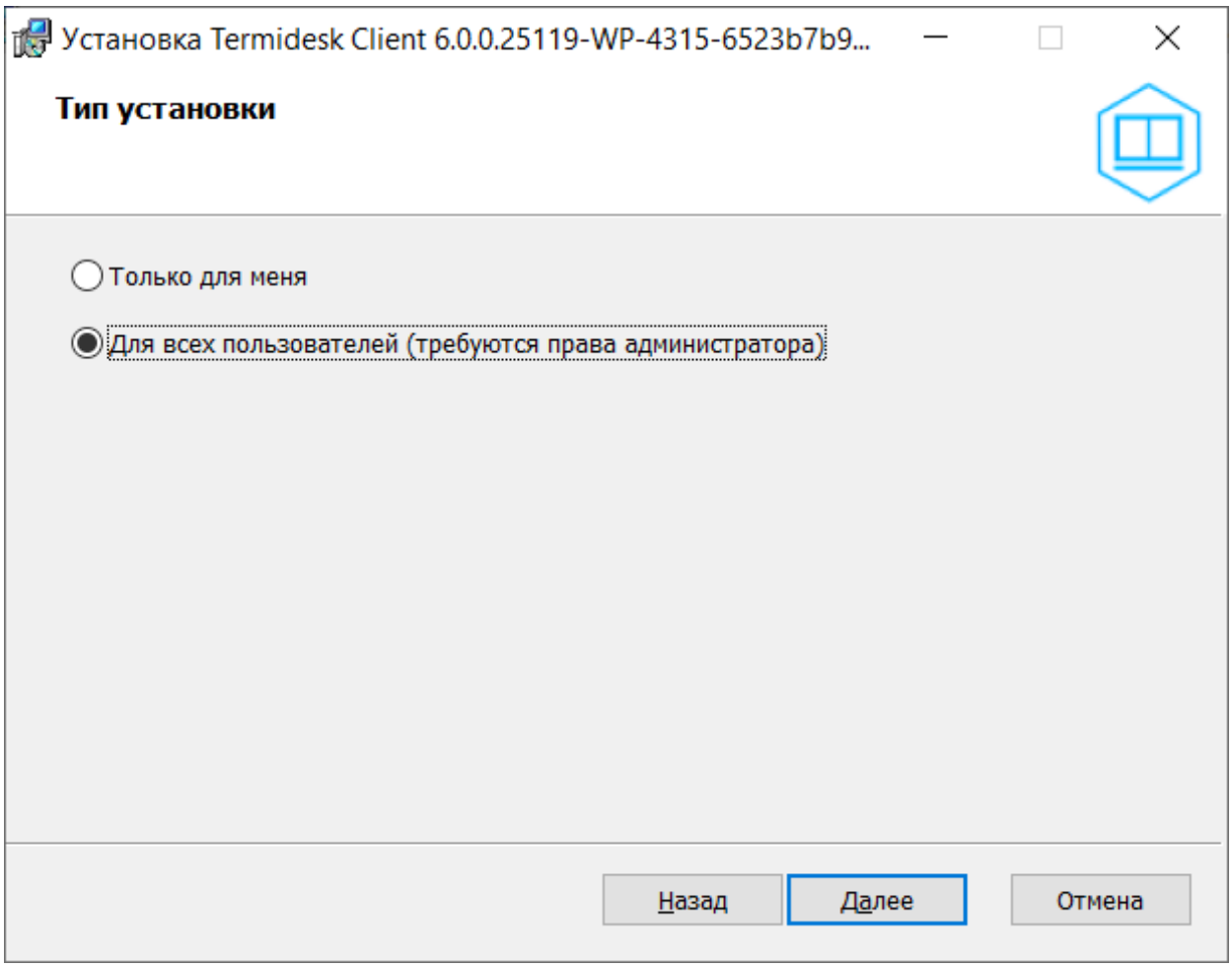


Рисунок 157. Окно выбора типа установки в ОС Windows

- выбрать, какие ярлыки программы должны быть созданы рисунок ОкновыборатипаустановкивОСWindows>>);

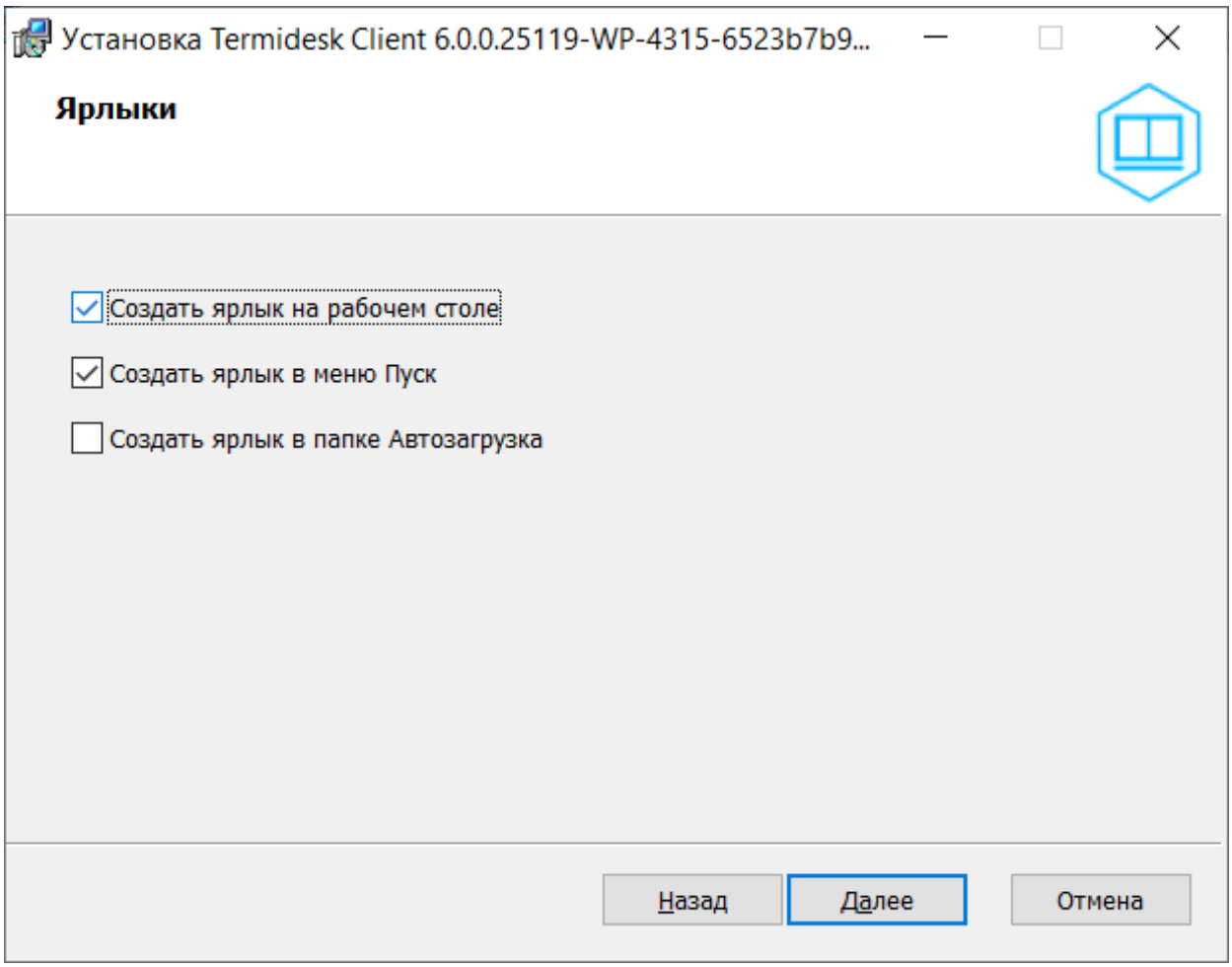


Рисунок 158. Окно выбора ярлыков

- отметить все компоненты в окне «Выборочная установка» (см. рисунок Окно установки компонентов в ОС Windows). При необходимости выбрать каталог установки или оставить значение по умолчанию, и нажать экранную кнопку **[Далее]**;

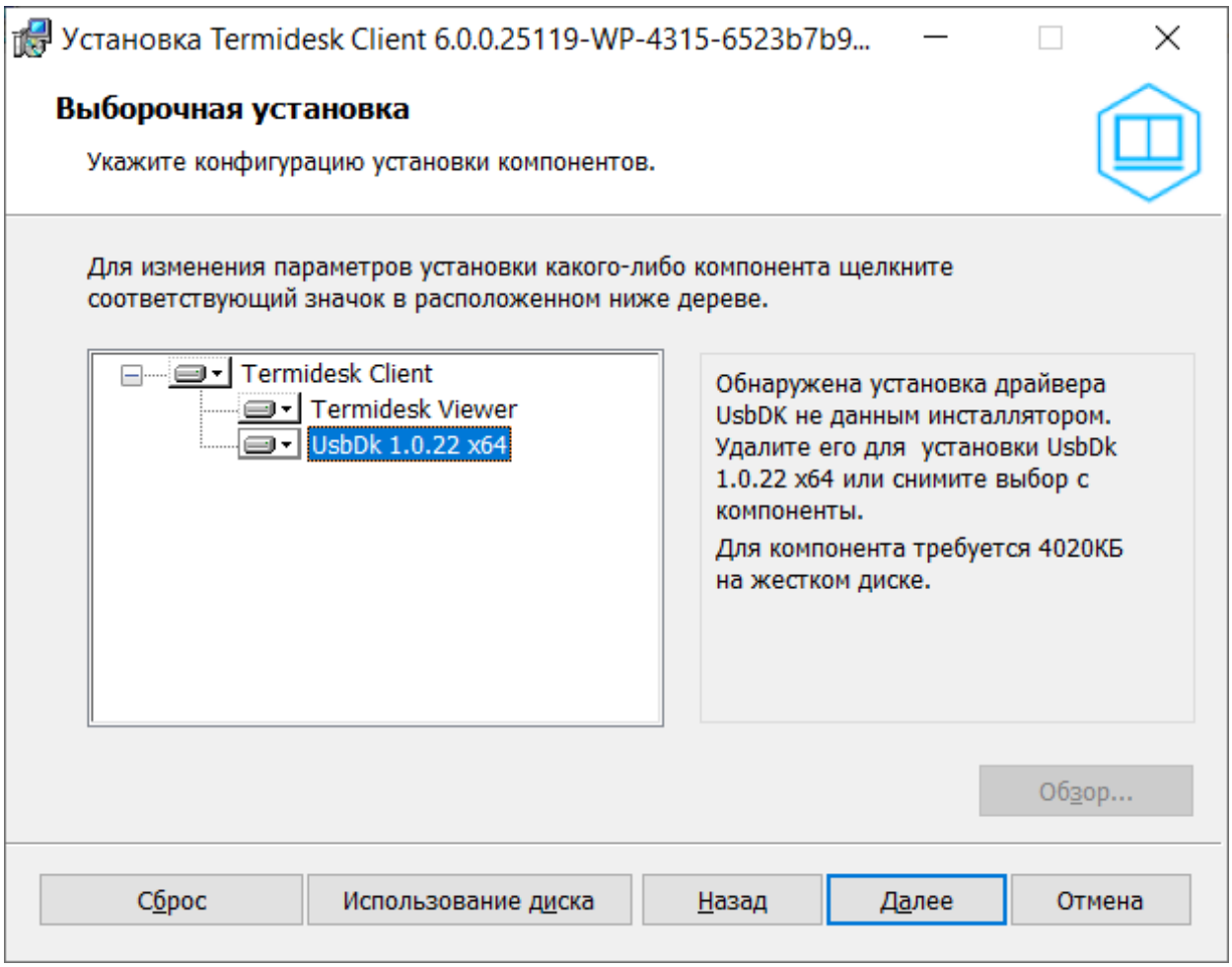


Рисунок 159. Окно установки компонентов в ОС Windows

- подтвердить установку,нажав экранную кнопку **[Установить]** (см. рисунок Подтверждение установки);

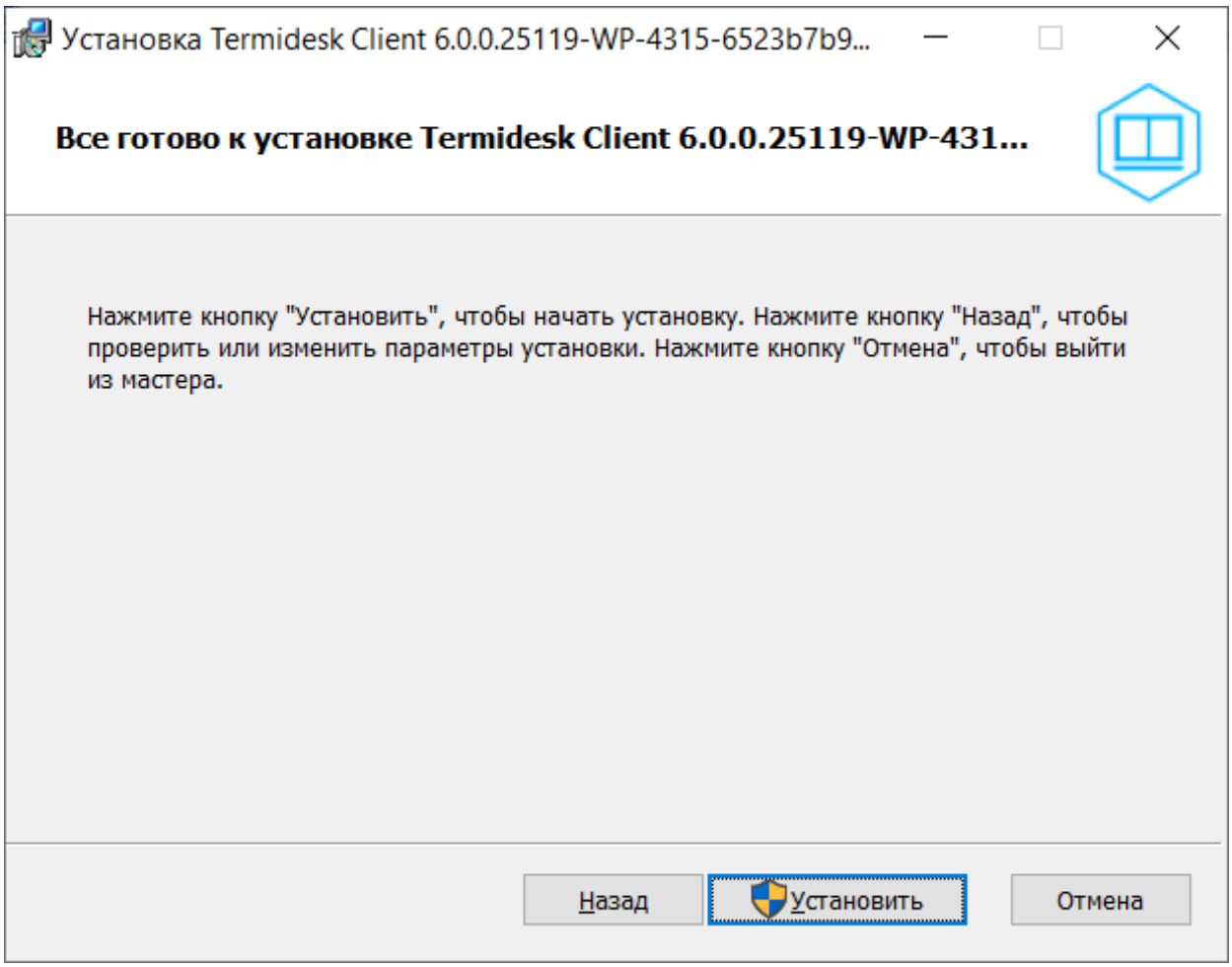


Рисунок 160. Подтверждение установки

- дождаться завершения установки и нажать экранную кнопку **[Готово]** (см. рисунок Успешное завершение установки).

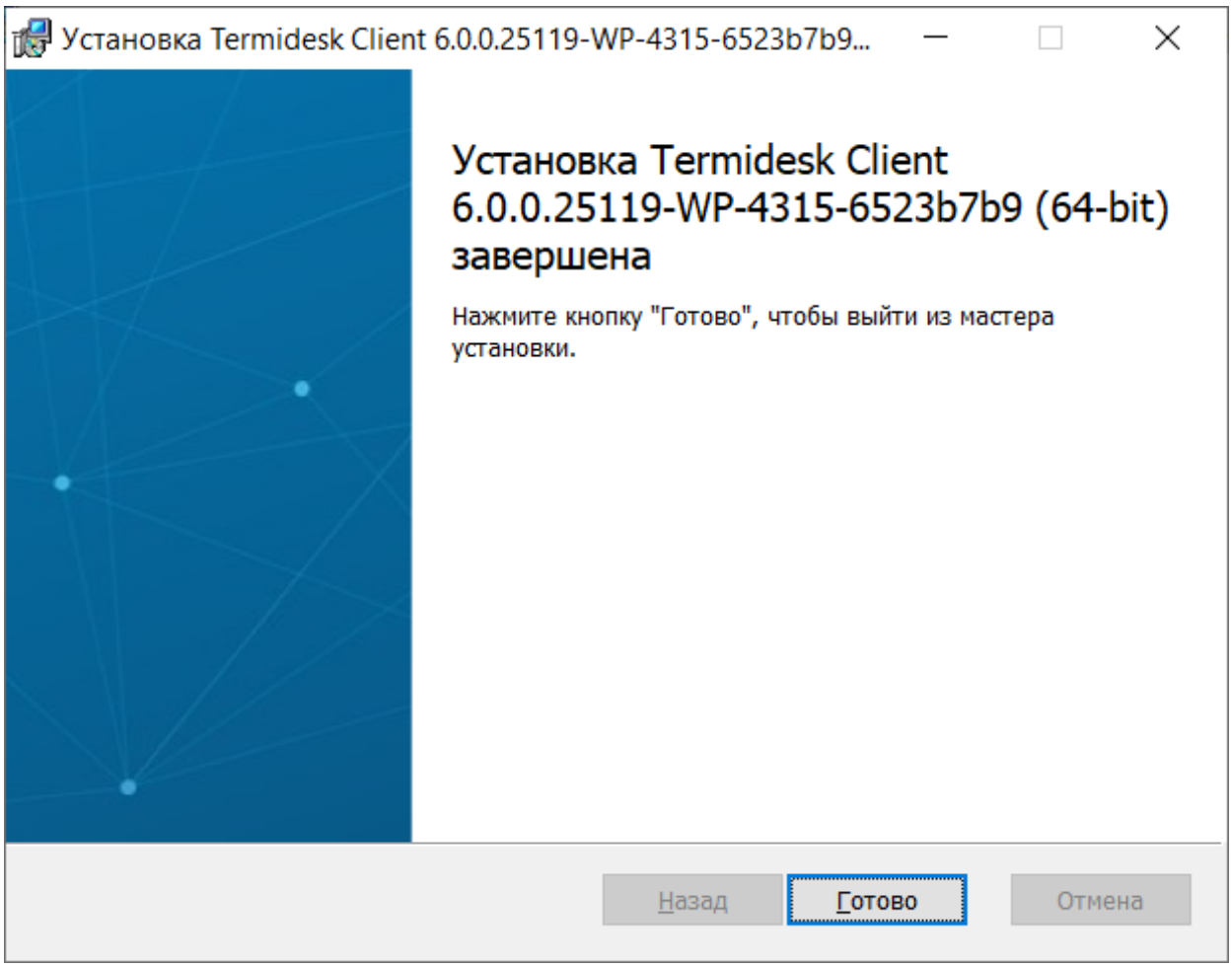


Рисунок 161. Успешное завершение установки

Если был выбран тип установки «Для всех пользователей (требуются права администратора)», то после установки:

- будет добавлена служба `Termidesk VDI TBUS`, необходимая для взаимодействия компонентов Termidesk VDI;
- будет установлено значение 00000001 (тип `dword`) для параметра реестра `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters\AllowTGTSessionKey`.

Установка Клиента и ПО Termidesk Viewer в ОС Microsoft Windows через интерфейс командной строки

Уменьшение версии через операцию установки не поддерживается. Для перехода к предыдущей версии следует удалить текущую установленную версию.

Для корректного функционирования Клиента необходимо, чтобы установка, запуск и подключение к РМ выполнялось от пользователя, имя которого задано на латинице. Подключение по протоколу RDP от пользователя с кириллическим именем может завершиться ошибкой.

Для выполнения установки для всех пользователей через командную строку `cmd.exe` нужно:

- открыть интерфейс командной строки от имени администратора;
- выполнить команду `msiexec`:

```
msiexec /i <путь_к_пакету_termidesk-client.msi> /qn
```

где:

`/qn` - обеспечивает тихую установку, без отображения окон и сообщений.

Для выполнения тихой установки для конкретного пользователя через командную строку `cmd.exe` нужно:

Для работы функционала Kerberos-аутентификации нужно выполнять установку для всех пользователей.

- открыть интерфейс командной строки;
- выполнить команду `msiexec`:

```
msiexec /i <путь_к_пакету_termidesk-client.msi> ALLUSERS=2 MSIINSTALLPERUSER=1 /qn
```

По умолчанию вместе с Клиентом будут установлены ПО Termidesk Viewer и UsbDk. Для управления установкой компонентов нужно воспользоваться свойством `ADDLOCAL`:

После установки идентификатор продукта `ProductCode` будет один, соответствующий Termidesk Client.

UsbDk - компонент, необходимый для корректной работы перенаправления периферийных устройств. Поскольку проверка установки этого компонента вызывает диалоговые окна, то рекомендуется в команду установки добавлять свойство `MSGBOX="N"` для их отключения.

- команда установки только компонента UsbDk (при этом Клиент все равно будет установлен):

```
msiexec /i <путь_к_пакету_termidesk-client.msi> ADDLOCAL="UsbDk" /qn
```

- команда установки только компонента ПО Termidesk Viewer (при этом Клиент все равно будет установлен):

```
msiexec /i <путь_к_пакету_termidesk-client.msi> ADDLOCAL="Termidesk_Viewer" /qn
```

- команда установки только Клиента, без остальных компонентов:

```
msiexec /i <путь_к_пакету_termidesk-client.msi> ADDLOCAL="Termidesk_Client" /qn
```

Если установка выполняется для всех пользователей, то после установки:

- будет добавлена служба `Termidesk VDI TBUS`, необходимая для взаимодействия компонентов Termidesk VDI;
- будет установлено значение 00000001 (тип `dword`) для параметра

реестра `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters\AllowTGTSessionKey`.

Обновление Клиента и ПО Termidesk Viewer в ОС Microsoft Windows

Обновление Клиента и ПО Termidesk Viewer производится операцией установки более новой версии поверх предыдущей.

Обновление следует производить с теми же типами установки, с которыми была установлена предыдущая версия. В противном случае возможна ситуация появления у пользователя двух ярлыков приложения.

Более новая версия, устанавливаемая для всех пользователей, не будет обновлять версию приложения, установленную для одного пользователя.

Минимальная необходимая версия ПО Termidesk Viewer - 7.0, поскольку в зависимости от версии ПО Termidesk Viewer передача Клиентом параметров подключения к РМ будет отличаться:

- если версия выше или соответствует 7.0, то параметры будут переданы Клиентом в преобразованном виде и ПО Termidesk Viewer запустится;
- если версия ниже 7.0, то Клиент не передаст параметры и ПО Termidesk Viewer не запустится.

Восстановление Клиента и ПО Termidesk Viewer в ОС Microsoft Windows

В установочных файлах Клиента и ПО Termidesk Viewer предусмотрена возможность исправления ошибок, возникших при установке или использовании компонентов. Исправление ошибок выполняется путем восстановления отсутствующих и поврежденных файлов, ярлыков и записей реестра.

Для восстановления работоспособности нужно:

- запустить установочный файл, в окне приветствия мастера установки нажать экранную кнопку **[Далее]**;
- нажать экранную кнопку **[Восстановить]**. Далее необходимо подтвердить восстановление и дождаться завершения операции. Для успешного восстановления необходимо разрешить внесение изменений при появлении соответствующего окна уведомления.

Удаление Клиента и ПО Termidesk Viewer в ОС Microsoft Windows

Удаление Клиента и ПО Termidesk Viewer выполняется одним из способов:

- для удаления с использованием стандартных средств ОС Microsoft Windows нужно:
  - открыть меню «Пуск», перейти «Панель управления - Программы - Удаление программы», выбрать «Termidesk Client» и нажать на экранную кнопку **[Удалить]**. Далее подтвердить удаление и дождаться завершения операции;
- для удаления с использованием установочного файла нужно:
  - запустить установочный файл, нажать экранную кнопку **[Удалить]** и дождаться завершения операции. Для успешного удаления необходимо разрешить внесение изменений при появлении соответствующего окна уведомления.

Из системной переменной `PATH` будет удален путь к каталогу с исполняемым файлом `vdi-viewer.exe`.

КЛИЕНТ. ПОДКЛЮЧЕНИЕ К СЕРВЕРУ TERMIDESK

Добавление сервера подключений в Клиенте

Для добавления сервера с «Универсальным диспетчером» Termidesk VDI необходимо щелкнуть левой кнопкой мыши по надписи «Добавить сервер» и в открывшемся окне ввести адрес сервера подключений (см. рисунок Окно добавления сервера подключений).

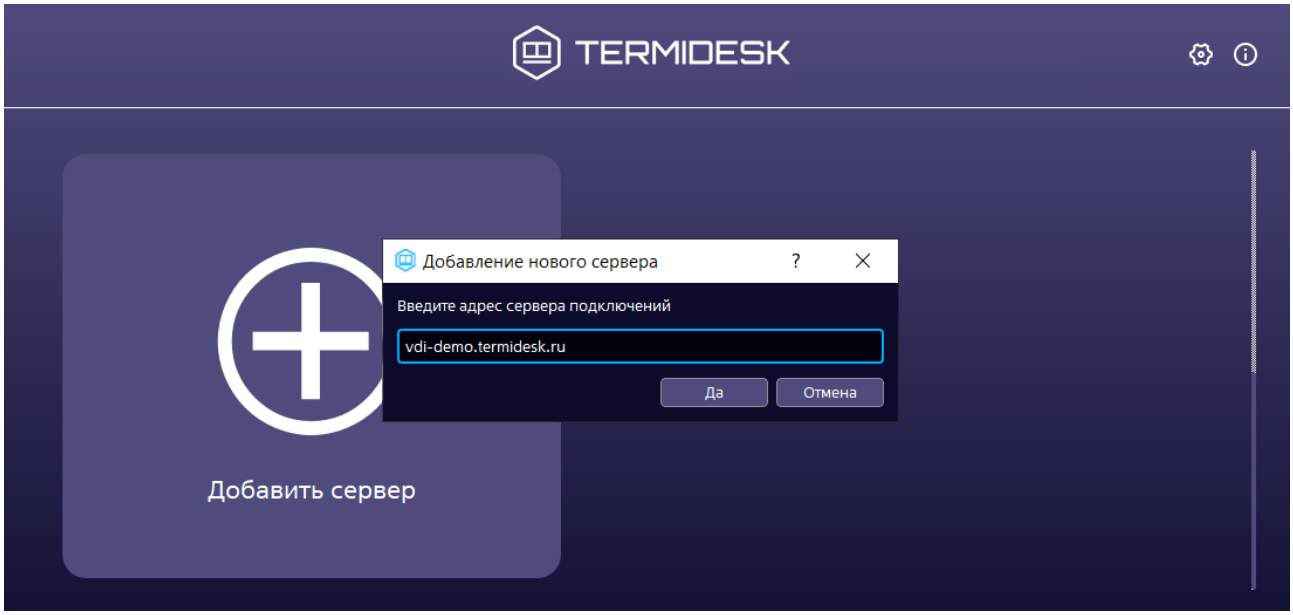


Рисунок 162. Окно добавления сервера подключений

Адрес сервера подключений может быть указан в формате:

- IP-адреса или доменного имени узла, пример: `vdi-demo.termidesk.ru`. Такой формат может использоваться, например, для подключения к компоненту «Универсальный диспетчер», установленному с ролью «Портал пользователя»;
- IP-адреса или доменного имени узла с указанием URI сайта, пример: `192.168.0.2/site`. Такой формат может использоваться, например, для подключения к определенному сайту портала «Агрегатор».

Дополнительно может быть указан протокол и порт для подключения, пример: `https://vdi-demo.termidesk.ru:443`, `https://192.168.0.2:443/site`.

Субъект, имеющий права администратора портала «Агрегатор», может подключиться к нему как с указанием определенного сайта, так и без его указания. В последнем случае он получит ресурсы всех активных сайтов портала «Агрегатор» после авторизации.

Информацию о том, какой адрес сервера подключений использовать, можно получить у администратора.

После добавления адреса сервера подключений в открывшемся окне «Настройка подключения к серверу» на вкладке «Общие» нужно заполнить следующие поля (см. рисунок Окно настройки подключения к серверу):

- «Описание» - текстовое сообщение, используемое для описания сервера (необязательно). Длина сообщения не может превышать 1024 символа;
- «Аутентификация» - выбор ресурса, являющегося источником сведений о субъектах и их полномочиях, настроенного на сервере в качестве домена аутентификации;
- «Логин» - идентификатор субъекта в домене аутентификации (совпадает с

идентификатором субъекта в службе каталогов);

- «Тип пароля» - выбор типа пароля для аутентификации. Можно выбрать:
  - «Клавиатурный пароль», значение доступно при стандартных средствах аутентификации, когда ввод пароля осуществляется с клавиатуры;
  - «Touch Memory пароль», значение доступно, если средством аутентификации является Touch Memory и выполнена настройка согласно аутентификации через носитель TouchMemory. Пароль будет прочитан с носителя TouchMemory, для этого нужно приложить его к считывателю;
  - «Touch Memory пароль (комбинированный)», значение доступно при условиях, аналогичных предыдущему варианту, но при этом нужно дополнительно ввести пароль с клавиатуры;
- «Пароль» - набор символов, подтверждающий назначение полномочий.

После заполнения указанных полей для подключения к выбранному серверу нужно нажать экранную кнопку **[Подключиться]**.

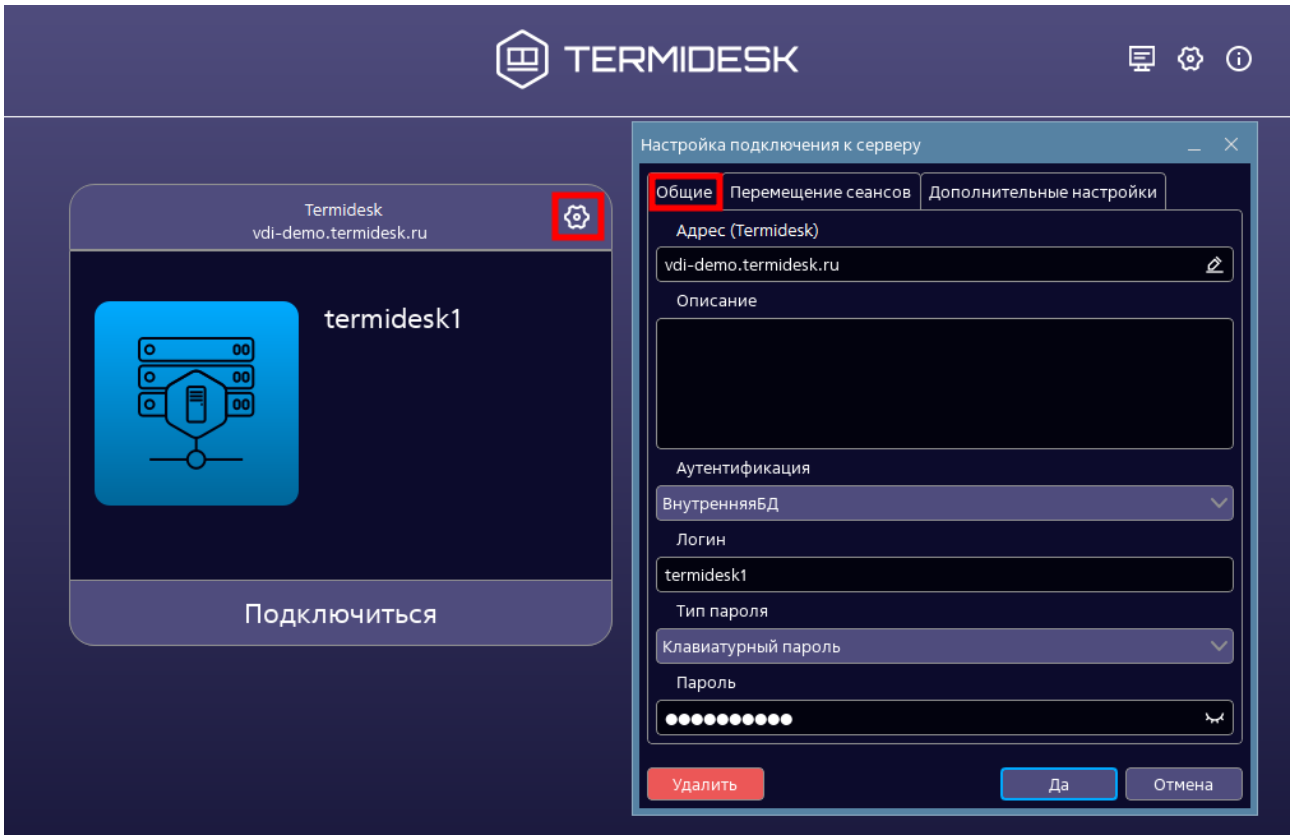


Рисунок 163. Окно настройки подключения к серверу

Ввод логина и пароля в настройках подключения может быть заблокирован, если на сервере активированы параметры, запрещающие сохранение логина и/или пароля в Клиенте. В этом случае их нужно будет ввести непосредственно при подключении к серверу, введенные значения не будут сохранены в конфигурационном файле `Termidesk Client.ini` и безопасном хранилище. Если пароль ранее был сохранен в безопасном хранилище, то он будет проигнорирован.

Запрет сохранения логинов и паролей применяется, если полученная при подключении версия компонента «Универсальный диспетчер» больше или равна 4.3.1 и соответствующие параметры на сервере активированы. При каждом обновлении списка аутентификаторов версия компонента запрашивается повторно.

В случае ошибки аутентификации будет показано соответствующее сообщение: «Ошибка аутентификации!» и дополнительная информация от сервера: подробный текст ошибки и (или) сообщение, заданное Администратором Termidesk VDI на «Портале администратора».

Для изменения параметров аутентификации на сервере подключений нужно нажать на графический элемент в виде шестеренки в правом верхнем углу для выбранного сервера.

Подключение к серверу через веб-браузер

Для подключения к Termidesk VDI через веб-браузер нужно:

- открыть веб-браузер;
- в адресной строке ввести IP-адрес или FQDN сервера с «Агрегатором» или «Универсальным диспетчером»Termidesk VDI;
- на открывшейся странице заполнить экранные поля:
  - «Имя пользователя» - идентификатор пользователя в системе Termidesk VDI;
  - «Пароль» - набор символов, подтверждающий назначение полномочий;
  - «Способ входа» - выбор домена аутентификации для входа в систему.

Информацию о заполнении полей нужно запросить у администратора. После заполнения полей актуальными данными нажать на экранную кнопку **[Войти]**.

Автоматический поиск сервера подключений через службу DNS

Общие сведения по поиску сервера подключений

В Клиенте по умолчанию реализована возможность автоматического поиска сервера Termidesk VDI через службу DNS.

> Для корректного поиска сервера администратору необходимо создать запись типа `TXT` для узла `vdi` или `daas` в соответствующей DNS-зоне. `TXT` -запись должна содержать адрес сервера «Универсального диспетчера» с указанием протокола доступа.
>
> Пример:
>
> - `daas TXT https://termidesk.domain.local`;
> - или `vdi TXT https://termidesk.domain.local`.

На пользовательской рабочей станции следует настроить возможность поиска записей в соответствующей DNS-зоне, как это указано ниже.

Если запись в соответствующей DNS-зоне существует, то при первом запуске Клиент выполнит запрос информации о сервере. В случае успешного выполнения запроса в окне «Аутентификация на сервере» отобразится адрес сервера (см. рисунок Результат запроса информации о сервере Termidesk VDI).

Для авторизации на сервере нужно заполнить следующие поля:

- «Аутентификация» - выбор ресурса, являющегося источником сведений о субъектах и их полномочиях, настроенного на сервере в качестве домена аутентификации;
- «Логин» - идентификатор субъекта в домене аутентификации (совпадает с идентификатором субъекта в службе каталогов);
- «Пароль» - набор символов, подтверждающий назначение полномочий.

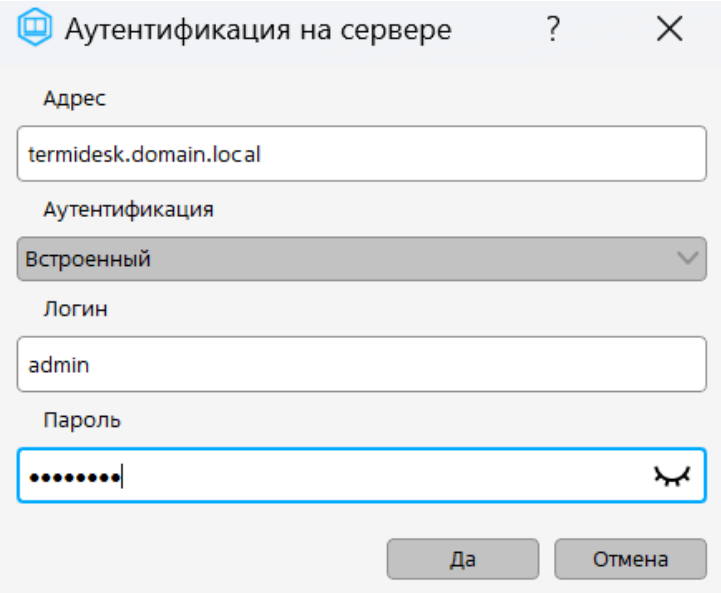


Рисунок 164. Результат запроса информации о сервере Termidesk VDI

Настройка DNS на пользовательской рабочей станции с ОС Microsoft Windows

Для настройки подключения к службе DNS на ОС Microsoft Windows нужно:

- нажать клавиши **<Win+R>**, в окне «Выполнить» ввести `ncpa.cpl` и нажать экранную кнопку **[OK]**;
- в окне «Сетевые подключения» выбрать соответствующий сетевой адаптер и нажать экранную кнопку **[Свойства]**;
- в окне «Название адаптера: свойства» выделить параметр «IP версии 4 (TCP/IPv4)» и нажать экранную кнопку **[Свойства]**;
- в окне «Свойства: IP версии 4 (TCP/IPv4)» нажать экранную кнопку **[Дополнительно...]**;
- в окне «Дополнительные параметры TCP/IP» перейти на вкладку «DNS» и активировать параметры (см. рисунок Подключение ОС Microsoft Windows к службе DNS):
  - «Дописывать основной DNS-суффикс и суффикс подключения»;
  - «Добавлять родительские суффиксы основного DNS-суффикса»;
  - «DNS-суффикс подключения» - указать домен, которому принадлежит машина;
  - «Зарегистрировать адреса этого подключения в DNS»;
  - «Использовать DNS-суффикс подключения при регистрации в DNS».

Для сохранения параметров подключения нужно нажать экранную кнопку **[OK]**.

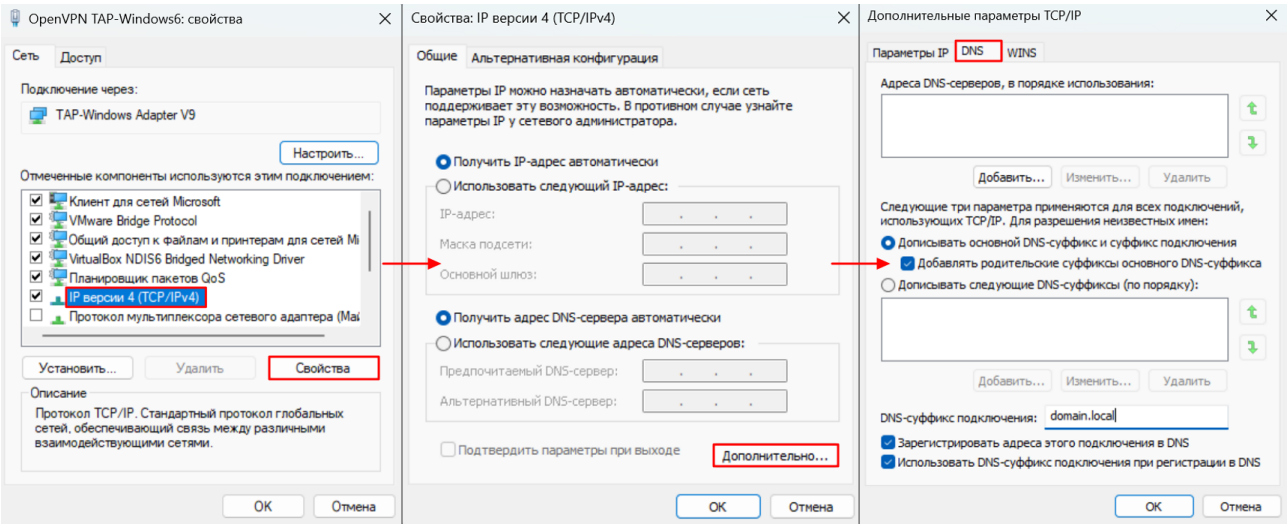


Рисунок 165. Подключение ОС Microsoft Windows к службе DNS

Настройка DNS на пользовательской рабочей станции с ОС Linux

Для настройки подключения к службе DNS на ОС Linux нужно отредактировать файл `/etc/resolv.conf`, внеся информацию по используемому домену и DNS-серверу:

```
domain domain.local
search domain.local
nameserver 198.51.100.11
nameserver 127.0.0.1
```

Где:

- `198.51.100.11` - IP-адрес DNS-сервера;
- `domain.local` - наименование домена.

Изменение сервера подключений

Возможность изменения сервера подключений зависит от значения параметра «Разрешать изменение адреса подключения в клиенте», заданного администратором в «Портале администратора».

Для изменения сервера подключений нужно нажать на графический элемент в виде шестеренки в правом верхнем углу для выбранного сервера.

В открывшемся окне «Настройка подключения к серверу» на вкладке «Общие» в поле «Адрес» нажать экранную кнопку **[Редактировать]** (см. рисунок Переход к редактированию адреса сервера подключений).

Адрес сервера подключений может быть указан в формате:

- IP-адреса или доменного имени узла, пример: `vdi-demo.termidesk.ru`;
- IP-адреса или доменного имени узла с указанием URI сайта, пример: `192.168.0.2/site`.

Дополнительно может быть указан протокол и порт для подключения, пример: `https://vdi-demo.termidesk.ru:443`, `https://192.168.0.2:443/site`.

Для применения изменений следует подтвердить назначение адреса сервера подключений и нажать экранную кнопку **[Да]**.

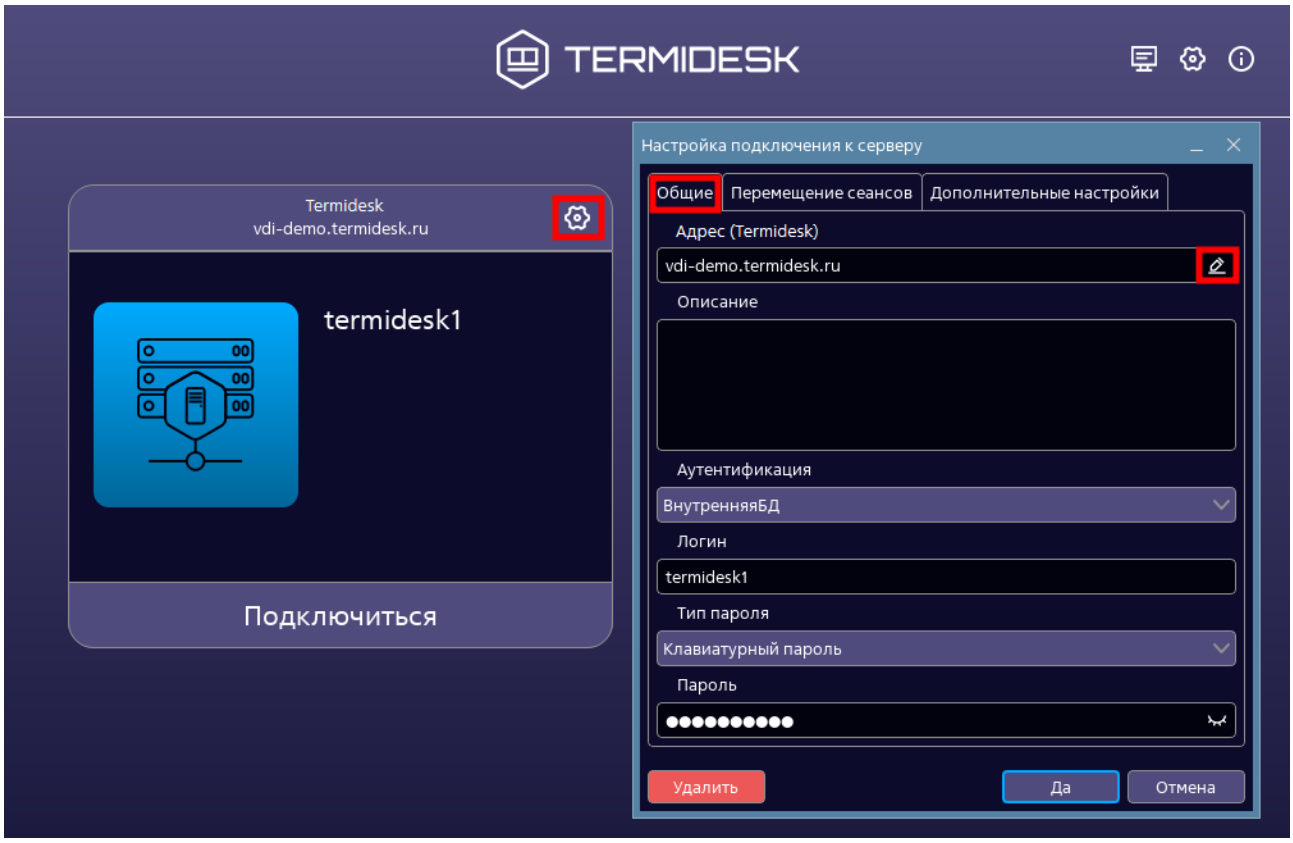


Рисунок 166. Переход к редактированию адреса сервера подключений

Просмотр сведений о параметрах подключения к серверу

Для просмотра сведений о параметрах подключения к серверу Termidesk VDI нужно нажать на наименование или IP-адрес сервера (см. рисунок Переход к просмотру сведений о параметрах подключения).

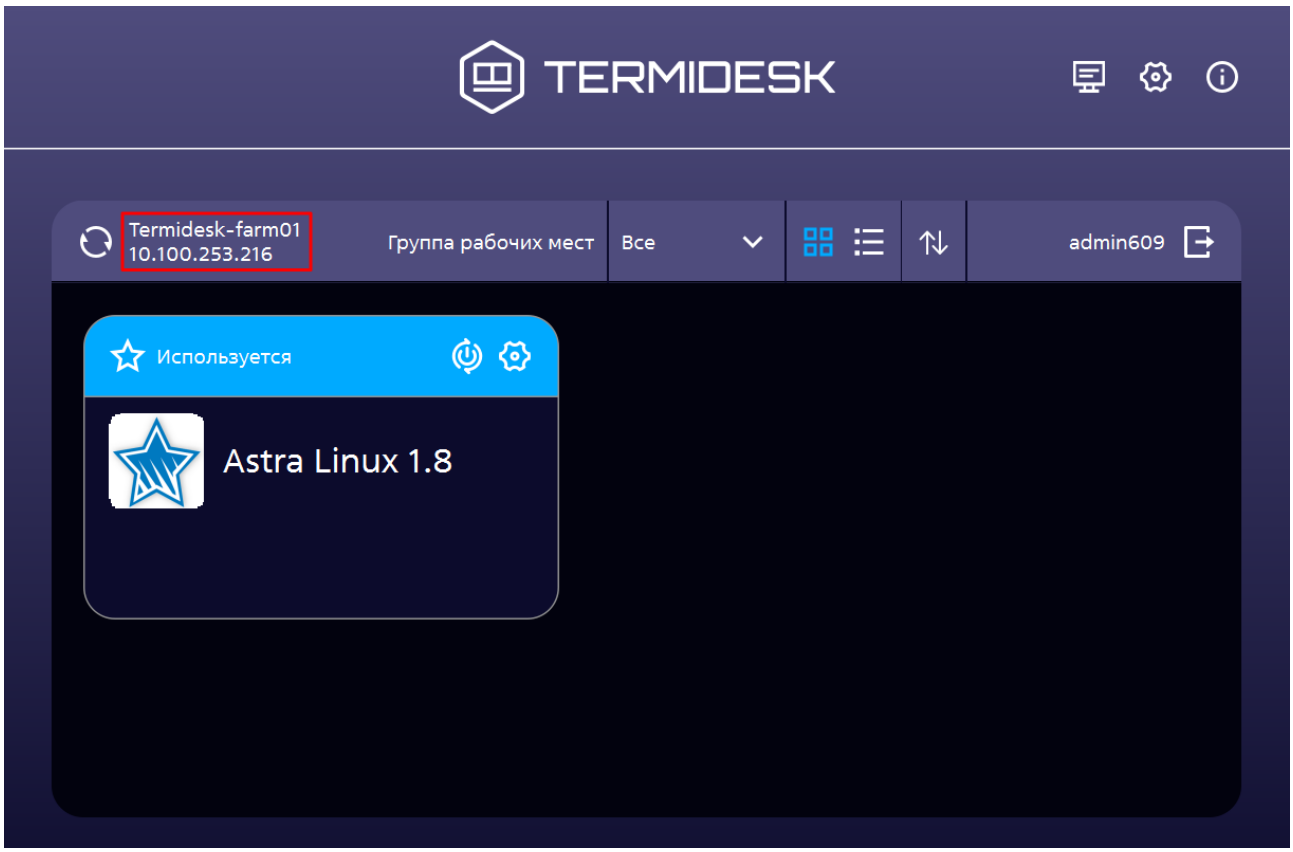


Рисунок 167. Переход к просмотру сведений о параметрах подключения

В открывшемся окне «Параметры подключения» будут отображены сведения о текущем подключении (см. рисунок Окно сведений о текущих параметрах подключения):

- «Название фермы» - наименование узла сервера подключений;
- «Адрес сервера» - IP-адрес, адрес сайта или доменное имя узла сервера подключений;
- «Доменное имя сервера» - FQDN узла сервера подключений;
- «Имя портала» - идентификатор узла сервера подключений;
- «IP-адрес» - IP-адрес узла сервера подключений.
- Для сохранения данных о текущем подключении в буфер обмена нужно нажать экранную кнопку **[Копировать]**.

Сведения о подключении фиксируются в момент открытия окна и не обновляются при изменении параметров.

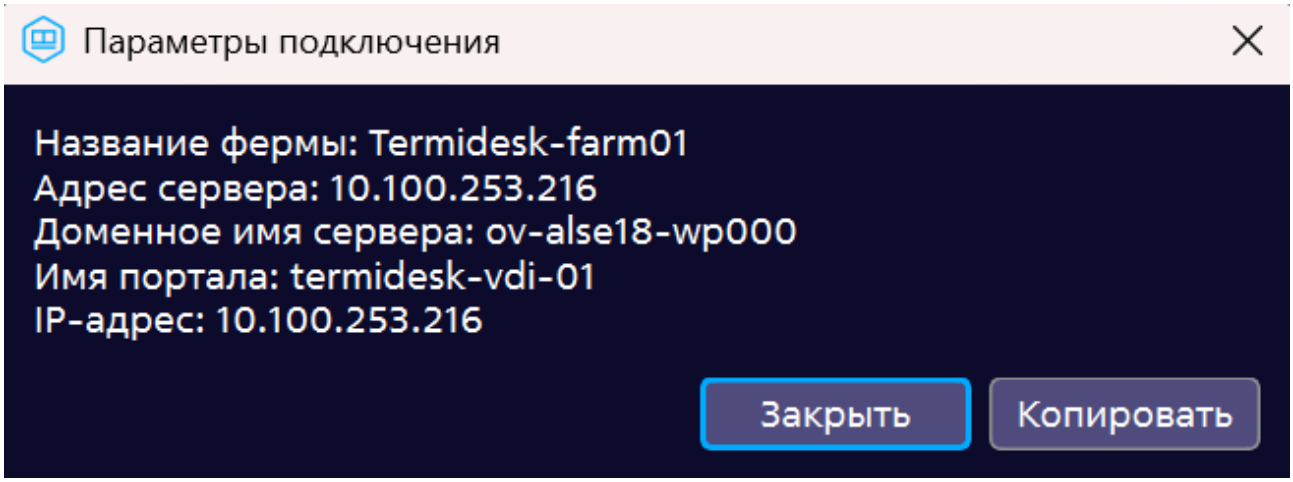


Рисунок 168. Окно сведений о текущих параметрах подключения

КЛИЕНТ. ПОДКЛЮЧЕНИЕ К РЕСУРСАМ

Подключение к РМ

Подключение к РМ через Клиент

После аутентификации и подключения программного Клиента к серверу Termidesk VDI доступен просмотр следующей информации о РМ:

При подключении к порталу «Агрегатор» ресурсы, находящиеся в режиме техобслуживания, не будут отображены в Клиенте.

- «Название» - текстовое поле, содержащее имя публикации РМ;
- «В избранном» - возможность добавить конкретную публикацию РМ в группу избранных или исключить его оттуда;
- «Статус» - отображение статуса использования РМ в фонде. Если в фонде используется хотя бы одно РМ, то статус с пустого изменится на «Используется». Если РМ недоступно для получения, то при наведении на «Статус» отобразится причина его недоступности, например: «Ресурс не готов к подключению, его статус - In maintenance»;
- «Протокол» - возможность выбора протокола доставки для каждого из отображаемых фондов;
- «Группа» - информация о наименовании группы, назначенной для отображения фондов;
- «Поддержка» - отображение иконки технической поддержки.

Для работы с перечнем фондов РМ используются следующие элементы управления (см. рисунок Элементы графического интерфейса):

- элемент (1) - обновляет список доступных фондов;
- элемент (2) - отображает сведения о текущем подключении (см. подраздел **Просмотр сведений о параметрах подключения к серверу**);
- элемент (3) - отображает перечень фондов из выбранной группы РМ;
- элемент (4) - отображает перечень фондов в плиточном формате;
- элемент (5) - отображает перечень фондов в списочном формате;
- элемент (6) - сортирует порядок отображения фондов в перечне по ряду параметров: «Название», «В избранном», «Статус», «Протокол», «Группа», «По убыванию» (по

умолчанию в отсутствие других параметров фонды РМ в перечне отображаются в алфавитном порядке по возрастанию).

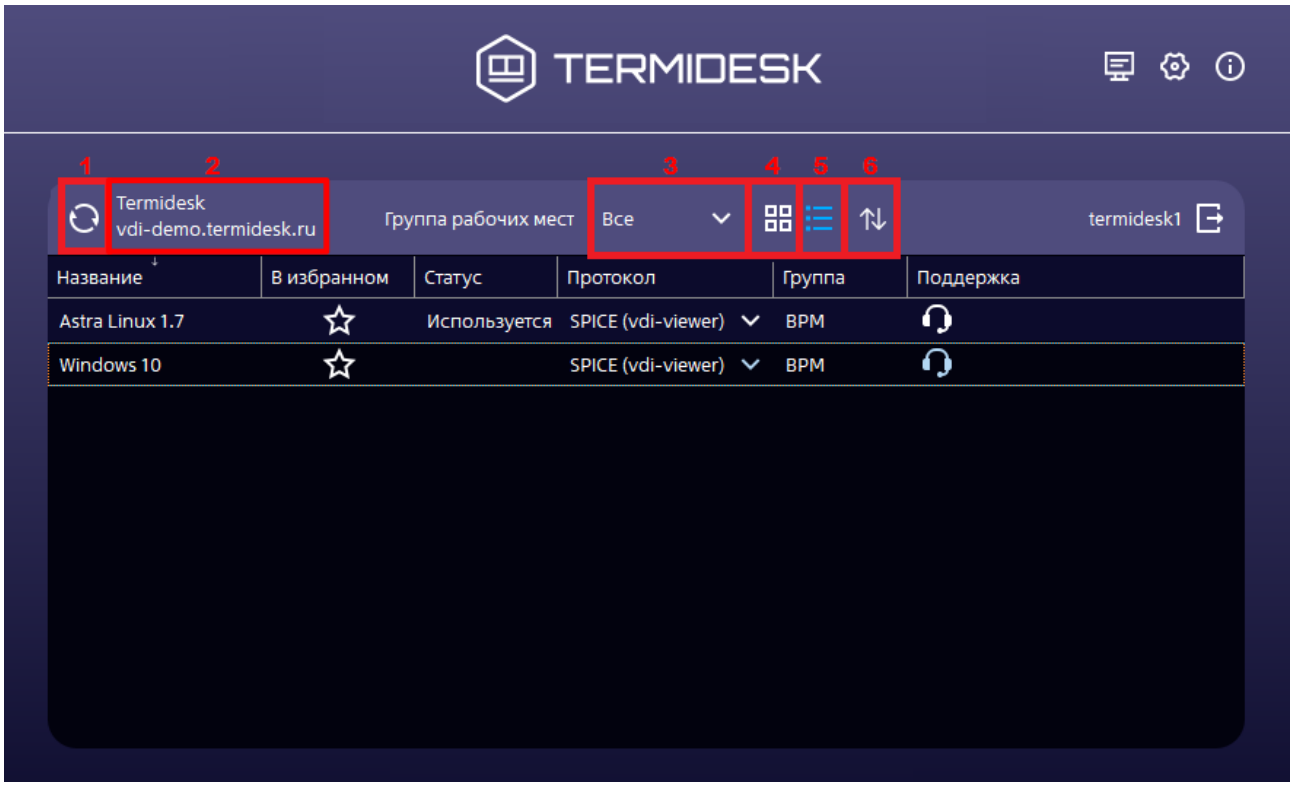


Рисунок 169. Элементы графического интерфейса

Для подключения к РМ нужно выбрать протокол доставки и дважды нажать левой кнопкой мыши на название фонда на РМ (см. рисунок Работа со списком рабочих мест). В случае перепубликации ресурсов при наведении мыши на заголовок фонда (в режиме плитка) или на столбец «Статус» будет показано всплывающее сообщение о необходимости завершить работу до указанного срока.

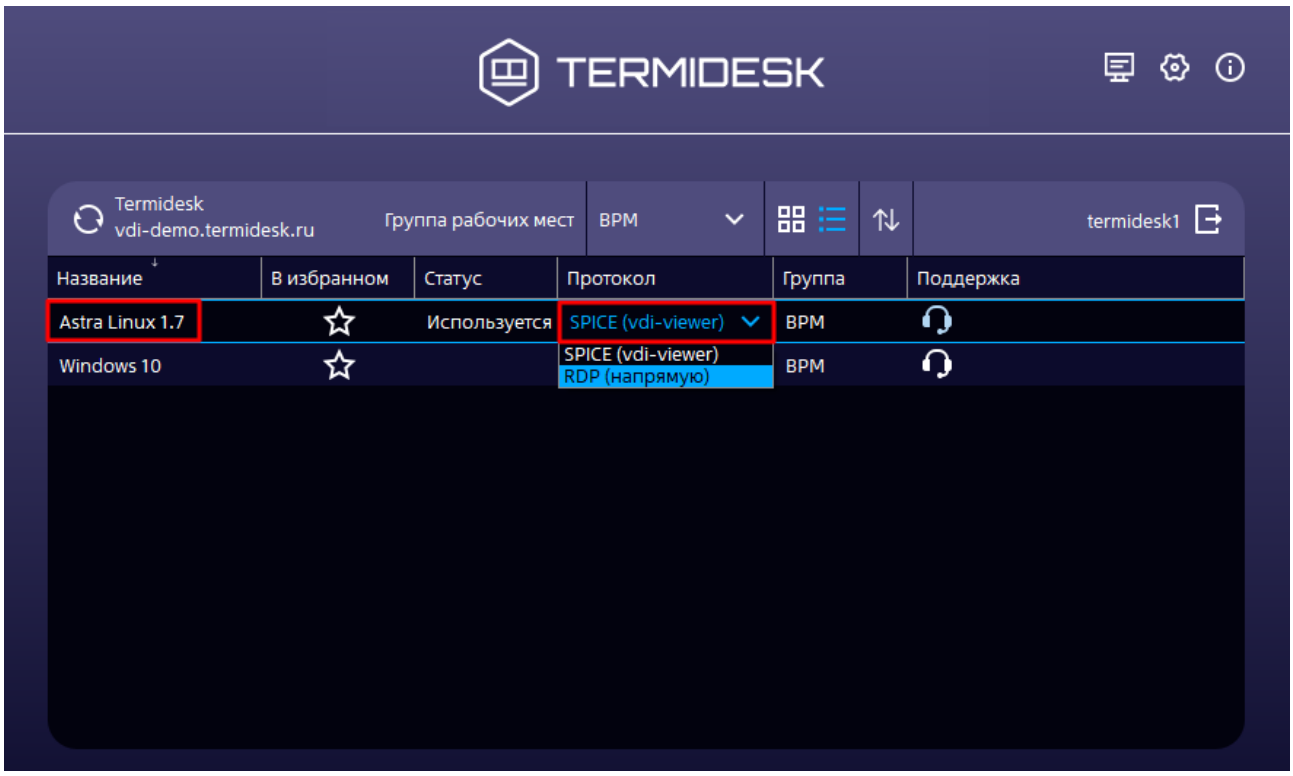


Рисунок 170. Работа со списком рабочих мест

В зависимости от выбранного протокола откроется окно соответствующей программы доставки, установленной на пользовательской рабочей станции, в которой будет отображаться РМ.

При невозможности подключиться по протоколу RDP будет отображено окно с текстом ошибки.

При подключении через домен «OpenID Connect» потребуется повторно пройти аутентификацию вне зависимости от того, активирована технология единого входа или нет.

При подключении к опубликованным приложениям или терминальным сессиям:

- при подключении через домен «OpenID Connect» или «SAML» будет показано окно ввода пароля для подключения (имя пользователя подставится автоматически);
- при использовании «Сервера терминалов Astra Linux» (STAL) логин и пароль необходимо вводить в том виде, в котором они заданы в ОС (если подключение происходит с учетными данными локального пользователя) или в контроллере домена (если подключение происходит с учетными данными доменного пользователя). Данное требование связано с чувствительностью к регистру вводимых символов в ОС Astra Linux Special Edition;
- при подключении с пользовательской рабочей станции с ОС Astra Linux Special Edition к опубликованным приложениям в режиме RAIL возможно обрамление окон приложений черной рамкой. Оно предназначено для корректной работы изменения размера экрана с помощью мыши. При необходимости включить прозрачность рамки можно так:
  - активировать композит-менеджер в ОС. Для этого нажать правой кнопкой мыши по рабочему столу и в контекстном меню выбрать «Оформление рабочего стола» и перейти в раздел «Эффекты» открывшегося окна;
  - активировать опцию «Прозрачность» в настройках композит-менеджера.

Для взаимодействия с РМ через контекстное меню нужно выбрать РМ в списке и нажать правой кнопкой мыши на наименование РМ (см. рисунок Взаимодействие с РМ через контекстное меню). При этом будут доступны следующие команды:

- «Открыть» - подключение к РМ с заданными параметрами;
- «Перезапустить» - выполнение принудительного перезапуска РМ. Возможность перезапуска РМ задается администратором в настройках компонента «Универсальный диспетчер».

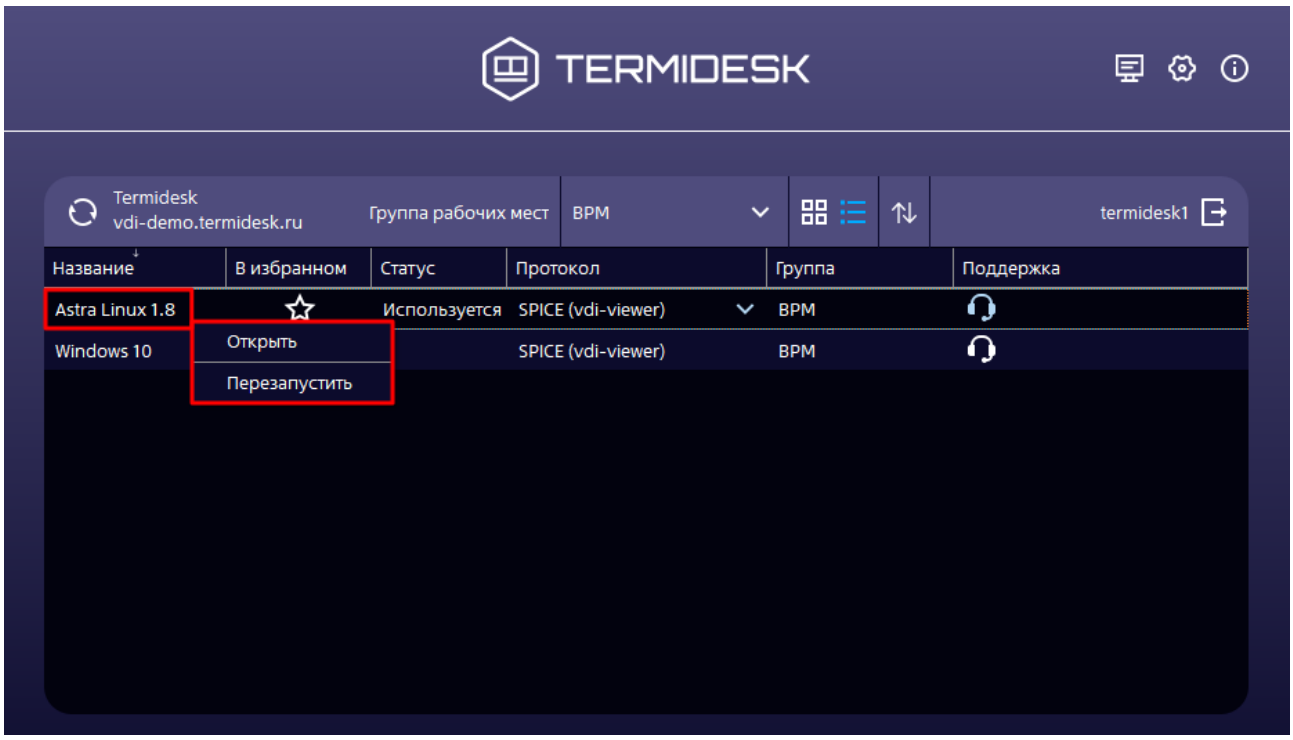


Рисунок 171. Взаимодействие с РМ через контекстное меню

Для перехода по URL-адресу технической поддержки следует:

- нажать на иконку в столбце на «Поддержка» (см. рисунок Обращение в техническую поддержку);
- дождаться отображения URL-адреса во встроенном в ОС веб-браузере. URL-адрес задается администратором в настройках компонента «Универсальный диспетчер».

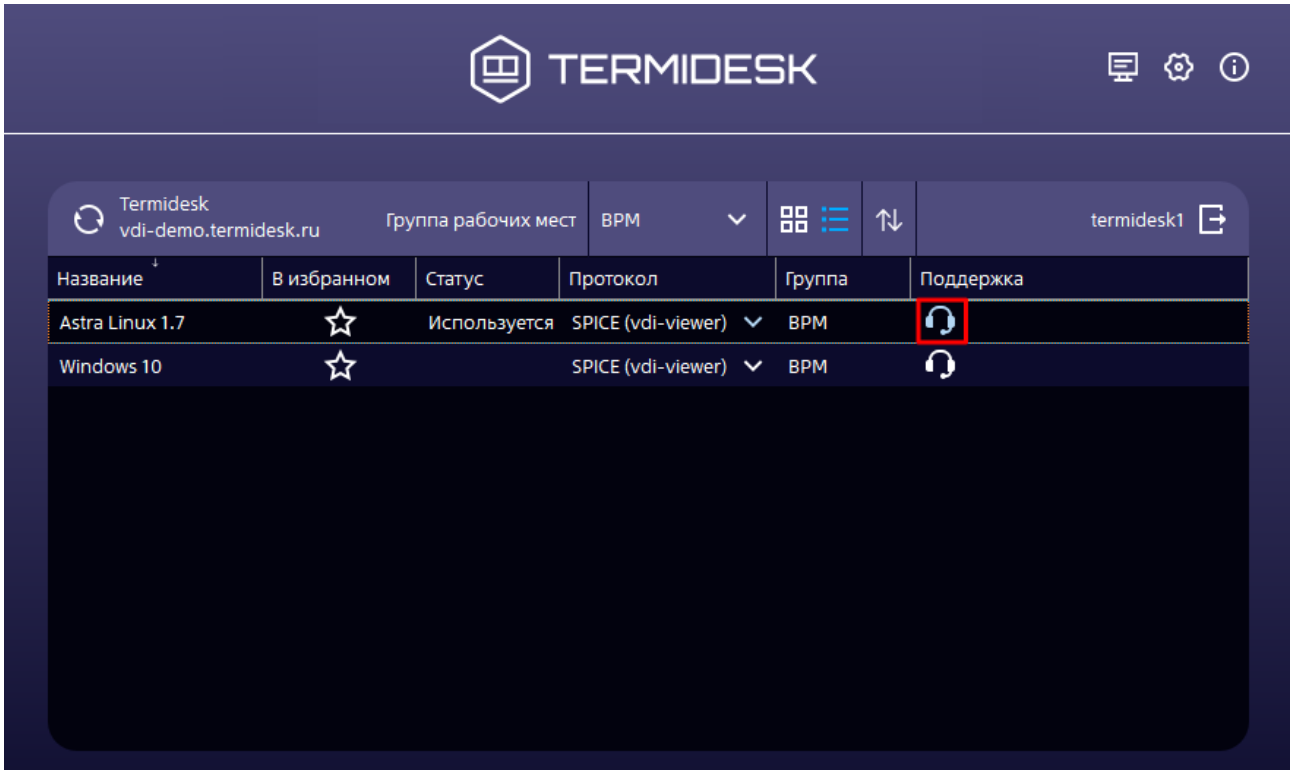


Рисунок 172. Обращение в техническую поддержку

Плиточный формат отображения изменяет визуальное представление фондов РМ и содержит следующие элементы взаимодействия (см. рисунок Отображение перечня

фондов РМ в плиточном виде):

- элемент (1) - добавление конкретной публикации РМ в группу избранных или исключение из нее;
- элемент (2) - статус использования РМ в фонде;
- элемент (3) - принудительный перезапуск РМ;
- элемент (4) - переход по URL-адресу технической поддержки;
- элемент (5) - выбор протокола доставки;
- элемент (6) - наименование публикации РМ в фонде;
- элемент (7) - дополнительные сведения о публикации РМ.

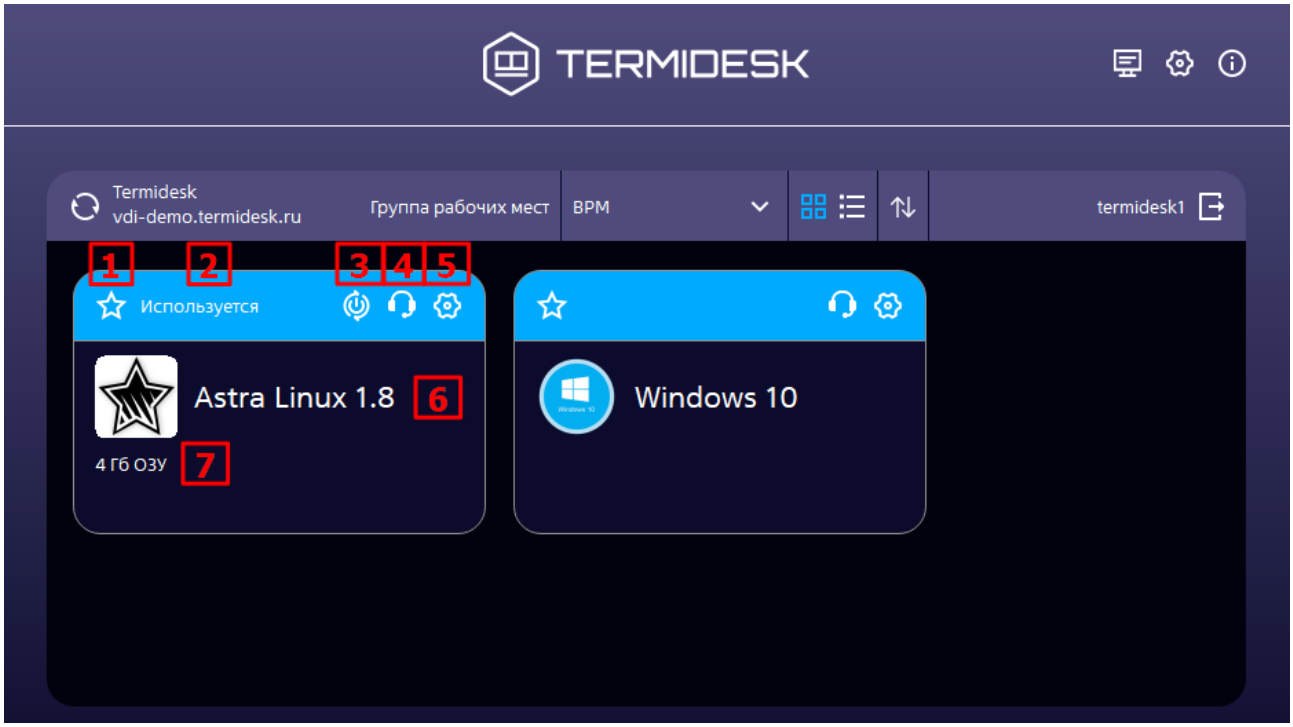


Рисунок 173. Отображение перечня фондов РМ в плиточном виде

Автоматическое подключение к фонду РМ

Автоматическое подключение к фонду РМ позволяет Клиенту выполнить поиск в сети сервера Termidesk VDI и реализовать автоматическое подключение к опубликованным фондам.

При запуске Клиент выполнит запрос информации и данных для авторизации на сервере. После аутентификации и подключения Клиента к серверу Termidesk VDI откроется окно с информацией о доступном фонде, с одновременным отображением РМ в окне ПО Termidesk Viewer.

Для работы функционала администратор должен выполнить настройку:

- активировать параметр «Автозапуск рабочего места» в «Портале администратора»;
- настроить группы доступа к фондам РМ так, чтобы пользователям из каждой группы был доступен только один фонд. Если пользователь является членом нескольких групп, и каждой из этих групп предоставлен доступ к отдельному фонду, то пользователь получает доступ к нескольким фондам одновременно. В таком случае, автоматическое подключение невыполнимо. При этом возможность ручного подключения сохраняется.

Подключение к РМ через веб-браузер

Предварительная подготовка узла

Если будет выполняться подключение к РМ по протоколу доставки HTML5 TERA, то для работы подключения следует:

> Настройка необходима, поскольку подключение выполняется по протоколу SSL/TLS.

- получить корневой сертификат сервера Termidesk VDI от администратора;
- в настройках веб-браузера добавить полученный корневой сертификат в список доверенных (пример для Mozilla Firefox):
  - перейти в меню «Настройки»;
  - выбрать раздел «Приватность и защита». На открывшейся странице переместиться к пункту «Защита - Сертификаты» и нажать экранную кнопку **[Просмотр сертификатов...]**;
  - в открывшемся окне перейти во вкладку «Центры сертификации» и нажать экранную кнопку **[Импортировать]**;
  - выбрать ранее сохраненный файл корневого сертификата и нажать экранную кнопку **[Открыть]**;
  - в открывшемся окне загрузки сертификата выбрать цели импорта. Рекомендуется отметить все предложенные варианты и затем нажать экранную кнопку **[OK]**;
- для подключения к Termidesk VDI в адресной строке ввести FQDN сервера Termidesk VDI.

Получение списка опубликованных ресурсов

Для получения списка опубликованных ресурсов необходимо предварительно аутентифицироваться на сервере подключений, после чего они отобразятся на странице веб-браузера. При этом есть различия в зависимости от используемого сервера подключений:

- при подключении к «Агрегатору» отобразятся сайты с опубликованными ресурсами;
- при подключении к ферме Termidesk VDI сразу отобразятся фонды РМ.

Подключение к фонду РМ

После перехода к списку опубликованных ресурсов станут доступны фонды РМ и следующие графические элементы (см. рисунок Элементы графического интерфейса при подключении через веб-браузер):

- элемент (1) - версия «Агрегатора» или «Универсального диспетчера»;
- элемент (2) - экранная кнопка, отображает окно «Параметры подключения»;
- элемент (3) - экранная кнопка выбора языка веб-интерфейса;
- элемент (4) - графический примитив, визуализирующий возможность изменения цветовой темы веб-интерфейса;
- элемент (5) - группа РМ;
- элемент (6) - наименование публикации РМ;
- элемент (7) - графический примитив, визуализирующий состояние РМ;
- элемент (8) - графический примитив, визуализирующий возможность перехода на URL-адрес технической поддержки. При нажатии на иконку будет открыт встроенный в ОС веб-браузер с указанным адресом. URL-адрес задается администратором в настройках

компонента «Универсальный диспетчер»;

- элемент (9) - графический примитив, визуализирующий возможность перезапуска РМ. При нажатии на иконку Termidesk VDI инициирует принудительный перезапуск РМ;
- элемент (10) - графический примитив, визуализирующий возможность выбора пользователем протокола доставки. При нажатии на иконку Termidesk VDI инициирует открытие вспомогательного окна, в котором перечислены доступные протоколы доставки. Доставка РМ по выбранному протоколу начинается после нажатия в окне «Подключения» ссылки с названием протокола;
- элемент (11) - графическая иллюстрация РМ.

Для подключения необходимо нажать на графическую иллюстрацию или наименование, описывающее РМ, затем:

- на запрос «Открыть приложение Termidesk Client»? ответить «Открыть приложение Termidesk Client»;
- дождаться подключения к РМ. Экран РМ отобразится в соответствующей программе доставки, установленной на пользовательской рабочей станции.

Если у фонда РМ отсутствует протокол доставки, подключиться к нему не получится.

В зависимости от выбранного протокола доставки и типа аутентификации может быть запрошен ввод пароля пользователя. Имя пользователя подставится автоматически и его нельзя изменить, если оно передано в параметрах протокола доставки. В ином случае имя пользователя можно ввести вручную.

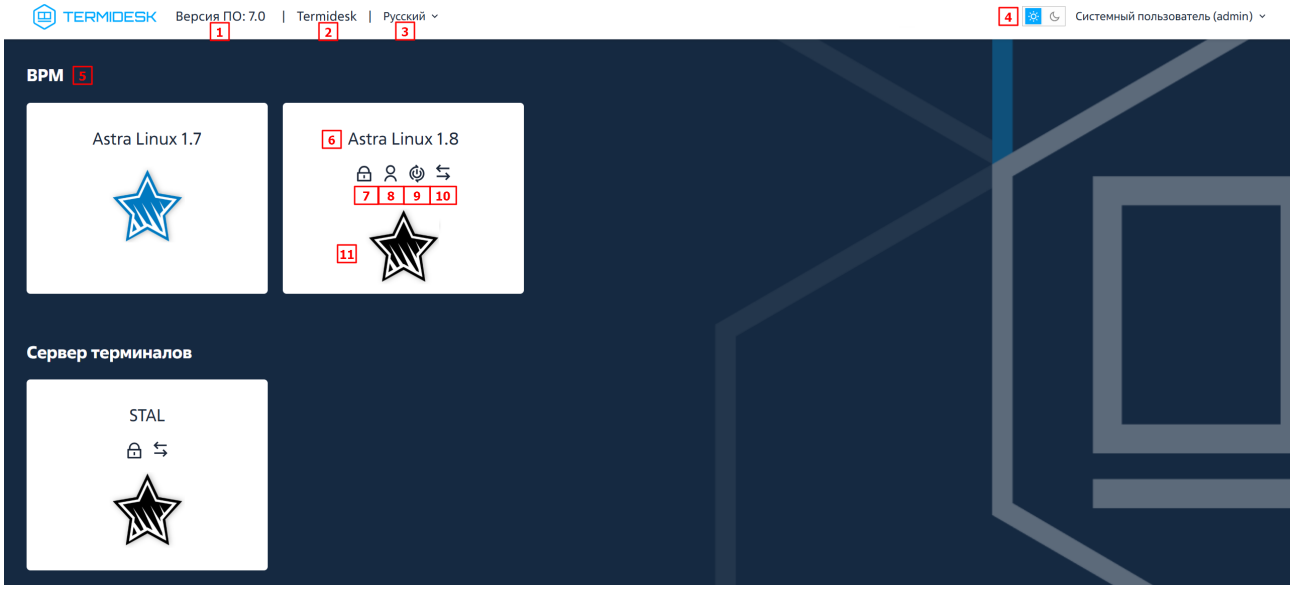


Рисунок 174. Элементы графического интерфейса при подключении через веб-браузер

Для просмотра сведений о текущем подключении нужно нажать на графический элемент (2). При этом в окне «Параметры подключения» будут отображены следующие сведения:

- «Имя фермы» - наименование фермы «Агрегатора» или «Универсального диспетчера»;
- «Доменное имя сервера» - имя узла «Агрегатора» или «Универсального диспетчера»;
- «Имя портала» - идентификатор узла «Агрегатора» или «Универсального диспетчера»;
- «IP-адрес» - IP-адрес узла «Агрегатора» или «Универсального диспетчера».

Параметры подключения можно сохранить в буфере обмена, нажав экранную кнопку **[Скопировать]** (см. рисунок Просмотр сведений о текущем подключении).

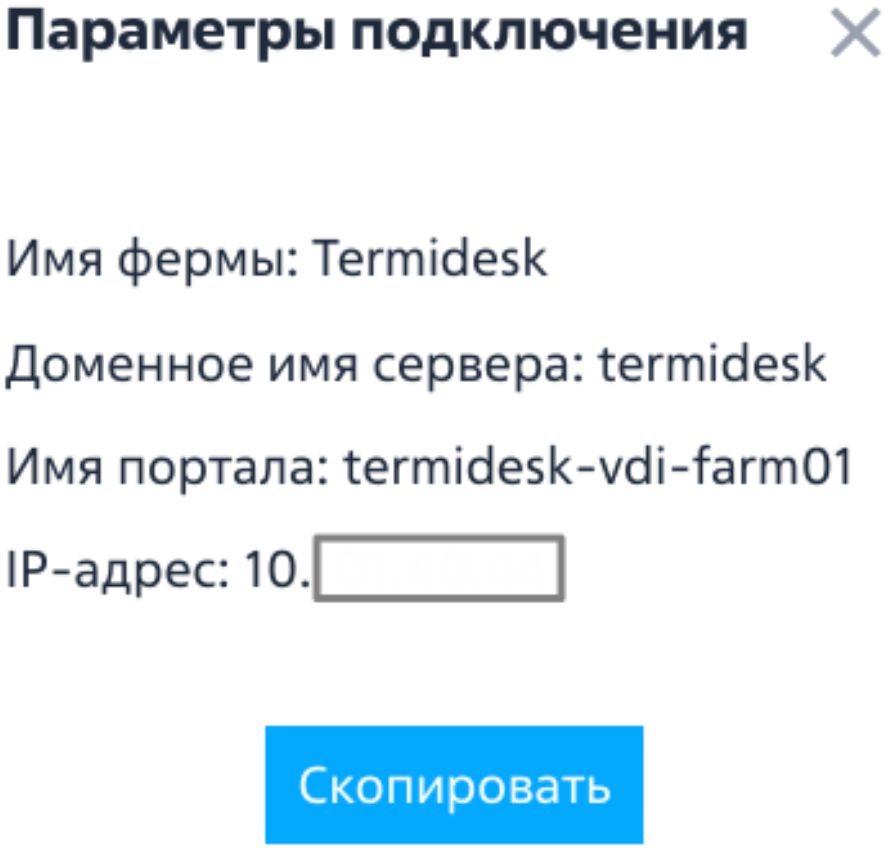


Рисунок 175. Просмотр сведений о текущем подключении

Подключение к РМ через веб-клиент

Веб-клиент позволяет получить экран РМ по протоколам SPICE и TERA через веб-браузер без необходимости установки дополнительного ПО на пользовательской рабочей станции. Для этого требуется настроить протокол доставки HTML5 в «Портале администратора».

Если администратором настроено защищенное подключение к компоненту «Шлюз» для протокола доставки HTML5, то в пользовательскую рабочую станцию необходимо установить (добавить в доверенные) соответствующий сертификат:

- корневой сертификат используемого центра сертификации;
- или самоподписанный сертификат, используемый на «Шлюзе».

Если соответствующие сертификаты не установлены, подключение может завершиться ошибкой.

При подключении к РМ через веб-браузер по протоколу HTML5 в дополнительном окне веб-браузера отобразится веб-клиент Termidesk Web Viewer.

РМ из разных фондов будут открыты в разных окнах веб-клиента Termidesk

Web Viewer.

В меню дополнительных действий веб-клиента Termidesk Web Viewer доступны информационные элементы со следующими возможностями (см. рисунок Интерфейс Termidesk Web Viewer):

- элемент (1):
  - закрепить окно;
- элемент (2):
  - получение информации о подключении;
  - создание снимка экрана;
  - управление буфером обмена;
- элемент (3):
  - передача файлов в РМ;
- элемент (4):
  - передача клавиш и сочетаний клавиш;
- элемент (5):
  - управление отображением в полноэкранном или оконном режимах;
- элемент (6):
  - отключение сессии (завершение работы с РМ).

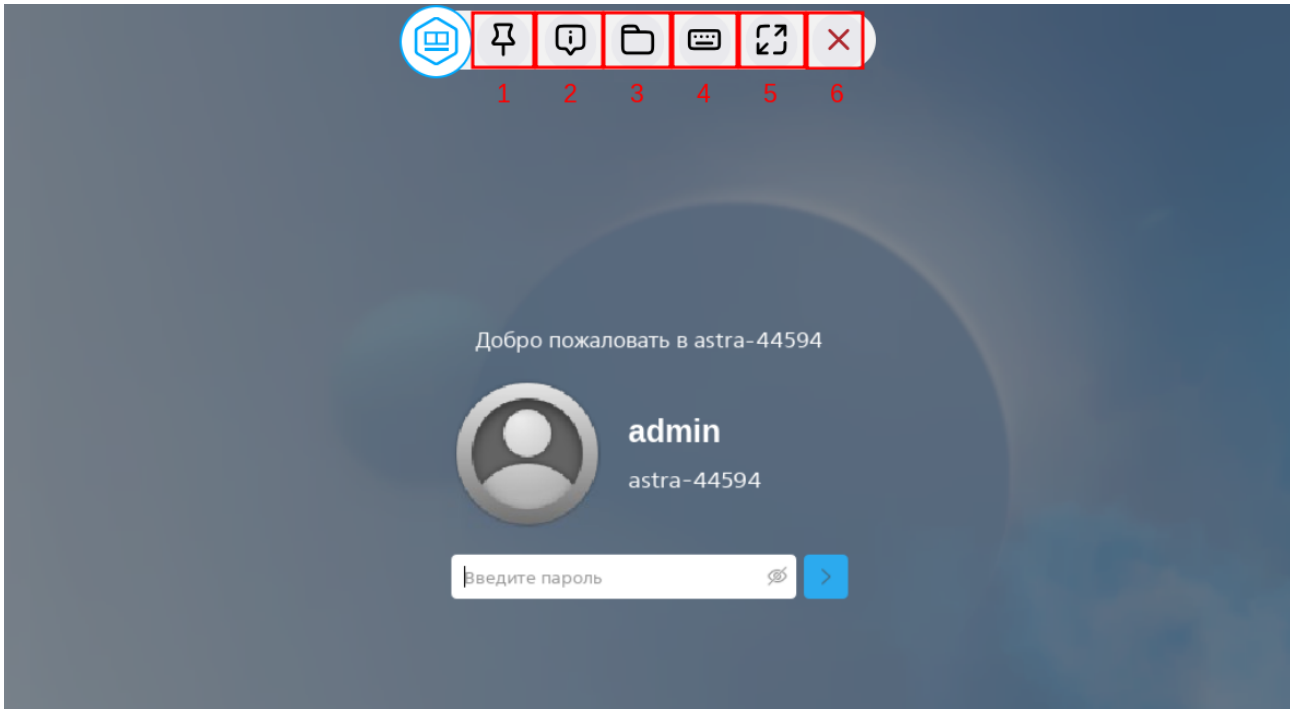


Рисунок 176. Интерфейс Termidesk Web Viewer

Настройки подключения к РМ

Прямое подключение к РМ

Прямое подключение к РМ обеспечивает быстрый доступ пользователя к РМ, которым он пользуется на постоянной основе.

Такой способ подключения исключает необходимость выполнения промежуточных

действий и минимизирует взаимодействие пользователя с графическим интерфейсом Клиента.

Для прямого запуска РМ на пользовательской рабочей станции нужно создать ярлык с параметрами запуска:

- пример запуска из ОС Microsoft Windows:

```
"C:\Program Files\UVEON\Termidesk Client\termidesk-client.exe" <https://IP-адрес_или_FQDN_сервера_Termidesk> --workplace-name <имя_публикации> --protocol <имя_протокола_доставки> --user-name <имя_пользователя> --user-auth <имя_домена_аутентификации> --user-password <пароль_пользователя>
```

- пример запуска из ОС Linux:

```
termidesk-client <https://IP-адрес_или_FQDN_сервера_Termidesk> --workplace-name <имя_публикации> --protocol <имя_протокола_доставки> --user-name <имя_пользователя> --user-auth <имя_домена_аутентификации> --user-password <пароль_пользователя>
```

Подробное описание параметров, необходимых для прямого запуска РМ, приведено подразделе **Интерфейс командной строки Клиента**.

Настройка обновления списка ресурсов

Функционал обновления списка ресурсов позволяет получить актуальный список перед подключением к нему пользователя.

Для настройки параметров обновления списка ресурсов нужно нажать на графический элемент в виде шестеренки в правом верхнем углу для выбранного сервера. В открывшемся окне «Настройка подключения к серверу» на вкладке «Дополнительные настройки» будут доступны следующие параметры управления:

- «Периодичность фонового обновления списка ресурсов» - параметр определяет периодичность (в секундах), с которой будет происходить обновление списка ресурсов;
- «Обновлять список ресурсов при каждом запуске ресурса» - параметр управления режимом обновления списка ресурсов. Если он активирован, то обновление списка ресурсов будет происходить при каждом запуске какого-либо ресурса.

Параметры могут быть заданы администратором в «Портале администратора» компонента «Универсальный диспетчер». В таком случае их нельзя будет изменить в указанном окне Клиента.

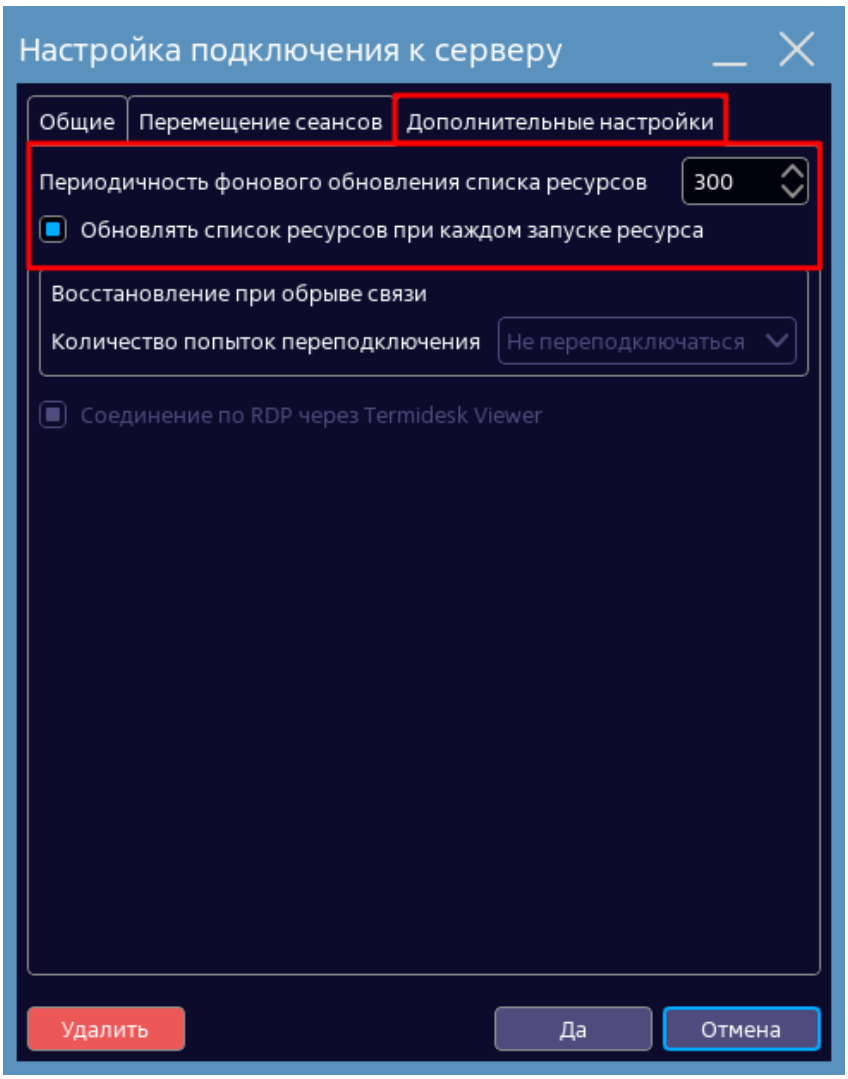


Рисунок 177. Настройка обновления списка ресурсов

Настройка переподключения Клиента к РМ

Функционал переподключения Клиента к РМ позволяет восстанавливать соединения с активными и отключенными сессиями в назначенном РМ после разрыва соединения или смены пользовательской рабочей станции.

Для настройки параметров переподключения нужно нажать на графический элемент в виде шестеренки в правом верхнем углу для выбранного сервера.

В открывшемся окне «Настройка подключения к серверу» на вкладке «Перемещение сеансов» (см. рисунок Настройка переподключения к РМ через Клиент) будут доступны следующие параметры управления:

- «Активировать управление перемещением сеансов» - параметр активации элементов управления повторным подключением:
  - «Повторно подключаться к активным и отключенным сеансам» - параметр повторного подключения к активным и отключенным сессиям в назначенном РМ. В этом случае при повторном подключении на РМ сначала будет произведена процедура отключения активного сеанса, после чего будет произведено повторное подключение к отключенному сеансу;
  - «Повторно подключаться только к отключенным сеансам» - параметр повторного подключения только к отключенным сессиям в назначенном РМ;
  - «Подключаться к сеансам при запуске ресурса» - информационная строка,

отображающая статус форсируемого режима перемещения сеансов. Настройка данного параметра выполняется администратором в настройках компонента «Универсальный диспетчер». При активации данного режима администратором элементы управления повторным подключением в Клиенте будут недоступны;

- «Подключаться к сеансам при аутентификации» - параметр подключения к назначенным сессиям в фонде РМ при аутентификации;
- «Подключаться к сеансам при обновлении списка ресурсов» - параметр подключения к назначенным сессиям в фонде РМ при обновлении списка ресурсов.

Для корректного переподключения Клиента к РМ требуется активировать параметры «Повторно подключаться к активным и отключенным сеансам» и «Подключаться к сеансам при аутентификации».

Параметры могут быть заданы администратором в «Портале администратора» компонента «Универсальный диспетчер». В таком случае их нельзя будет изменить в указанном окне Клиента.

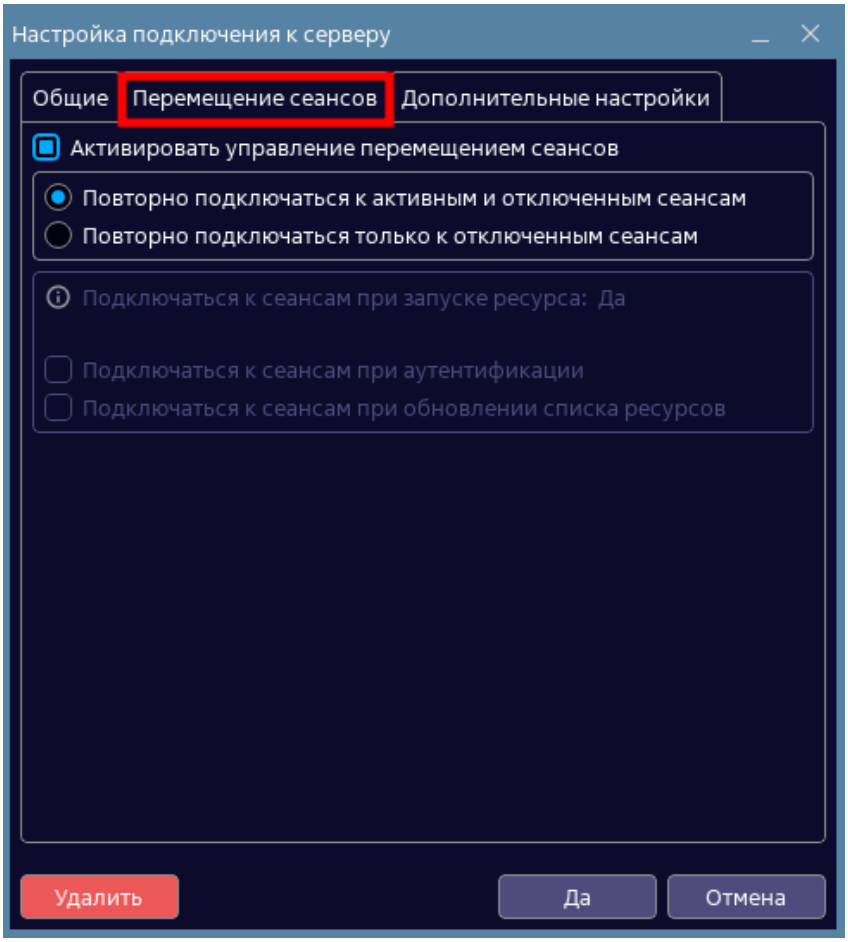


Рисунок 178. Настройка переподключения к РМ через Клиент

Настройка восстановления связи при потере соединения

Клиент поддерживает восстановление связи с РМ при потере соединения. Функционал поддерживается для протоколов RDP, SPICE, TERA.

Восстановление связи при потере соединения со STAL поддерживается в версии STAL 4.0 и выше.

Для настройки параметров обновления списка ресурсов нужно нажать на графический элемент в виде шестеренки в правом верхнем углу для выбранного сервера. В

открывшемся окне «Настройка подключения к серверу» на вкладке «Дополнительные настройки» (см. рисунок Настройка восстановления связи при потере соединения) будут доступны следующие параметры управления для восстановления связи:

- «Количество попыток переподключения» - параметр определяет количество запланированных попыток для восстановления подключения. Возможные значения:
  - «Не переподключаться» - попытки восстановления связи выполняться не будут. При потере соединения подключение к РМ останавливается и не возобновляется;
  - «5» - при потере соединения выполняются 5 попыток для восстановления подключения;
  - «10» - при потере соединения выполняются 10 попыток для восстановления подключения;
  - «30» - при потере соединения выполняются 30 попыток для восстановления подключения.

Параметры могут быть заданы администратором в «Портале администратора»компонента «Универсальный диспетчер». В таком случае их нельзя будет изменить в указанном окне Клиента.

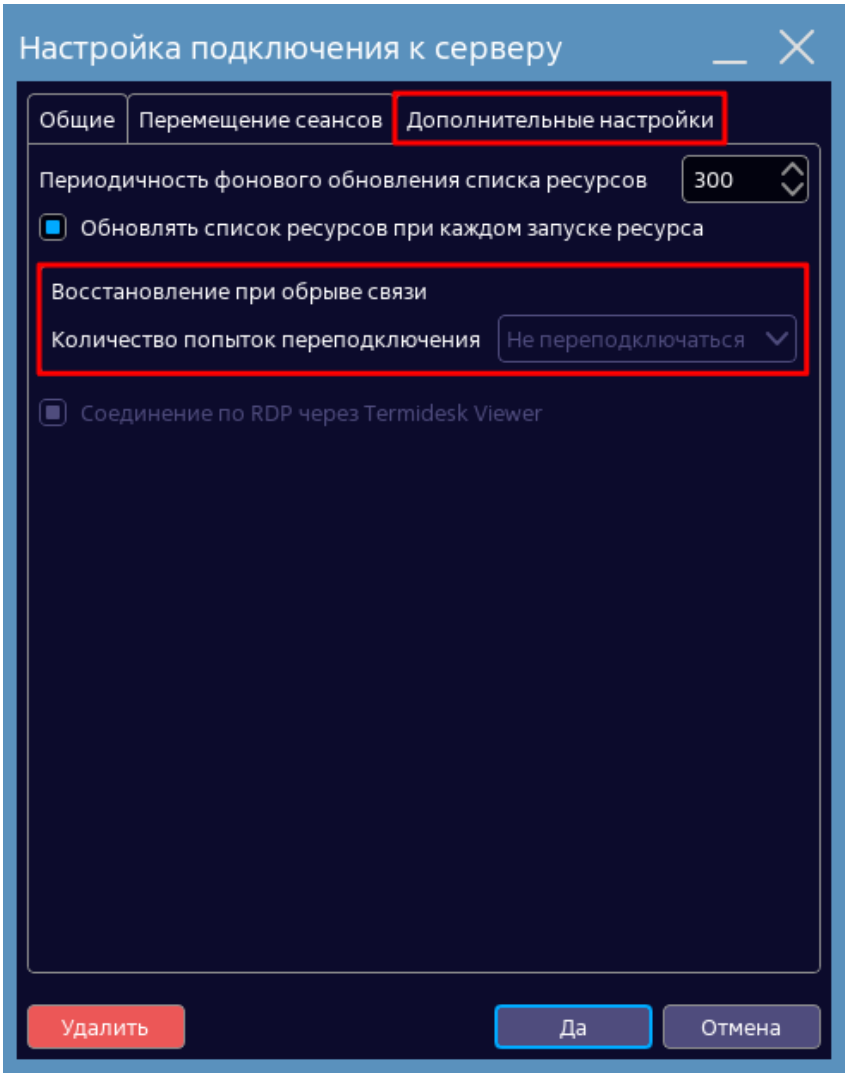


Рисунок 179. Настройка восстановления связи при потере соединения

Если соединение неожиданно оборвется, то в ПО Termidesk Viewer будет отображено сообщение о ходе восстановления соединения. При этом:

- в сообщении (см. рисунок Сообщение о попытке восстановления соединения с РМ) будет отражен номер текущей попытки восстановления соединения и общее количество запланированных попыток (пауза между попытками составляет не менее 5 секунд). При нажатии экранной кнопки **[Отмена]** или закрытии окна процесс восстановления будет прерван, работа ПО Termidesk Viewer будет остановлена (останов может произойти с некоторой задержкой);

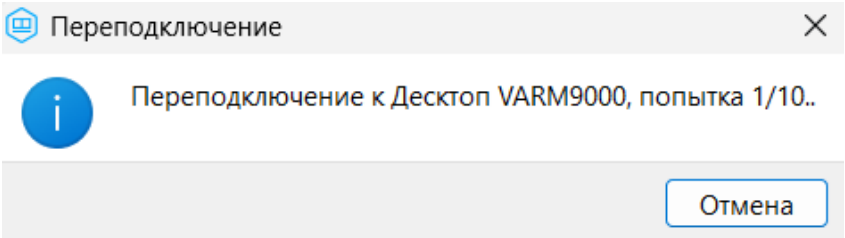


Рисунок 180. Сообщение о попытке восстановления соединения с РМ

- если восстановление соединения не удалось выполнить в течение всех запланированных попыток, то будет отображено окно (см. рисунок Запрос на повторную попытку восстановления соединения с РМ) с запросом на повторную попытку. При этом:
  - при нажатии экранной кнопки **[Да]** процесс восстановления начнется заново;
  - при нажатии экранной кнопки **[Нет]** или закрытии окна процесс восстановления не будет активирован, работа ПО Termidesk Viewer будет остановлена;
  - если никаких действий не было предпринято, то работа ПО Termidesk Viewer будет принудительно остановлена через 60 секунд.

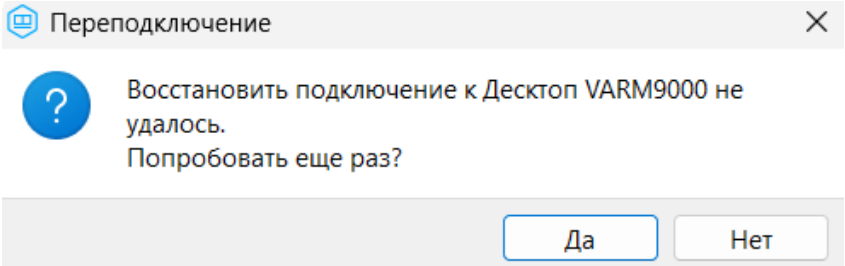


Рисунок 181. Запрос на повторную попытку восстановления соединения с РМ

Настройка подключения по RDP через ПО Termidesk Viewer

«Клиент» может использовать различные программы доставки РМ при подключении пользователя по протоколу RDP:

- ПО Termidesk Viewer (рекомендуется);
- системные программы (`mstsc.exe`, `xfreerdp`).

Для ОС macOS всегда используется ПО Termidesk Viewer.

Для настройки использования ПО Termidesk Viewer нужно нажать на графический элемент в виде шестеренки в правом верхнем углу для выбранного сервера. В открывшемся окне «Настройка подключения к серверу» на вкладке «Дополнительные настройки» будут доступны следующие параметры управления (см. рисунок Настройка использования ПО Termidesk Viewer):

- «Соединение по RDP через Termidesk Viewer» - параметр определяет использование ПО Termidesk Viewer при подключении к РМ по протоколу RDP. Если параметр не отмечен, то будут использоваться системные программы доставки.

Параметры могут быть заданы администратором в «Портале администратора» компонента «Универсальный диспетчер» или в «Агрегаторе администратора». В таком случае их нельзя будет изменить в указанном окне Клиента.

При подключении пользователя из веб-браузера используется встроенный веб-клиент Termidesk Web Viewer, использование сторонних программ настраивается через конфигурационный файл `Termidesk Client.ini`.

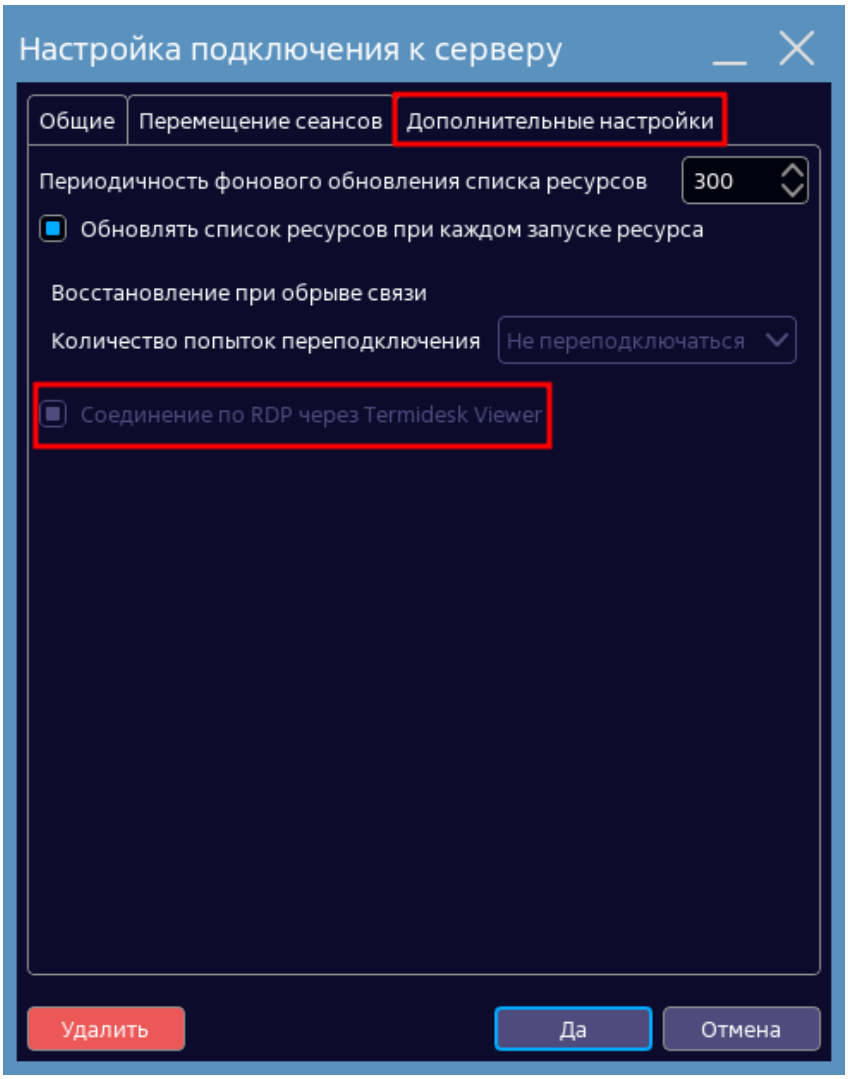


Рисунок 182. Настройка использования ПО Termidesk Viewer

КЛИЕНТ. АУТЕНТИФИКАЦИЯ В РАЗЛИЧНЫХ СЦЕНАРИЯХ

Аутентификация на сервере подключений по смарт-картам

Параметры и смарт-карты для аутентификации на сервере подключений

При добавлении сервера или при подключении к уже добавленному серверу пользователь может пройти аутентификацию на нем с использованием смарт-карты или токена.

Информация по поддержке сквозной аутентификаии в гостевой ОС РМ представлена в подразделе Аутентификация по смарт-картам в гостевой

ОС РМ.

Список поддерживаемых смарт-карт и токенов для аутентификации на сервере подключений через Клиент:

- Рутокен Lite (только для ОС Microsoft Windows);
- Рутокен ЭЦП 2.0 (2100);
- Рутокен ЭЦП 3.0 (3220);
- Рутокен ЭЦП PKI (1800);
- JaCarta PKI: JaCarta PKI (JC200-1), JaCarta-2 PKI/ГОСТ (JC207-12.F27), JaCarta-2 PKI, JaCarta-3 PKI (JC240 v.10);
- виртуальная смарт-карта на основе аппаратного модуля TPM (Trusted Platform Module). Требуется дополнительная настройка пользовательской рабочей станции (см. подраздел **Настройка аутентификации по виртуальной смарт-карте (TPM)**).

Подробная информация по настройке смарт-карт Рутокен для аутентификации приведена в официальной документации: https://dev.rutoken.ru/.

Поиск имени пользователя из сертификата выполняется в следующем порядке:

- Subject Alternative Name (атрибут Microsoft - UserPrincipalName);
- Subject Alternative Name (атрибут RFC822 Name - Email);
- Common Name.

Поддерживаются следующие типы доменов:

- SAML;
- OpenID Connect;
- LDAP (MS AD);
- ALD Pro.

Администратором должна быть выполнена настройка пользовательской рабочей станции для работы с Kerberos-аутентификацией в домене LDAP.

Для аутентификации по смарт-карте или токену в настройках подключения должен быть выбран домен аутентификации с настроенным функционалом PKINIT (аутентификация по смарт-картам).

После выбора необходимого домена аутентификации поля «Логин», «Тип пароля» и «Пароль» будут недоступны для заполнения.

Ввод учетных данных осуществляется:

- для SAML и OpenID Connect в дополнительном окне веб-браузера после подключения к выбранному серверу, как описано ниже;
- для LDAP и ALD Pro с настроенным функционалом PKINIT учетные данные будут прочитаны со смарт-карты, но при подключении в дополнительном окне потребуется выбрать имя пользователя из списка и ввести PIN-код к смарт-карте, как это описано ниже.

Если смарт-карта или токен не были подключены, будет отображено сообщение о необходимости ее подключить. В случае, если на устройстве отсутствует сертификат или

системе не удалось его прочесть, будет отображено сообщение «Не удалось загрузить сертификаты».

Если смарт-карта или токен не поддерживаются, будет отображено сообщение «Этот ключевой носитель не может быть использован. Пожалуйста, выберите другой носитель и повторите попытку», при этом в журнале Клиента будет записано событие об отсутствии поддержки устройства.

Подключение к доменам типа «SAML» или «OpenID Connect»

При подключении к выбранному серверу через домены типов «SAML» или «OpenID Connect» из ОС Astra Linux Special Edition:

- дополнительно отобразится окно веб-браузера. Для перехода в сервис аутентификации следует нажать экранную кнопку **[Войти]** (см. рисунок Окно перехода в сервис аутентификации);

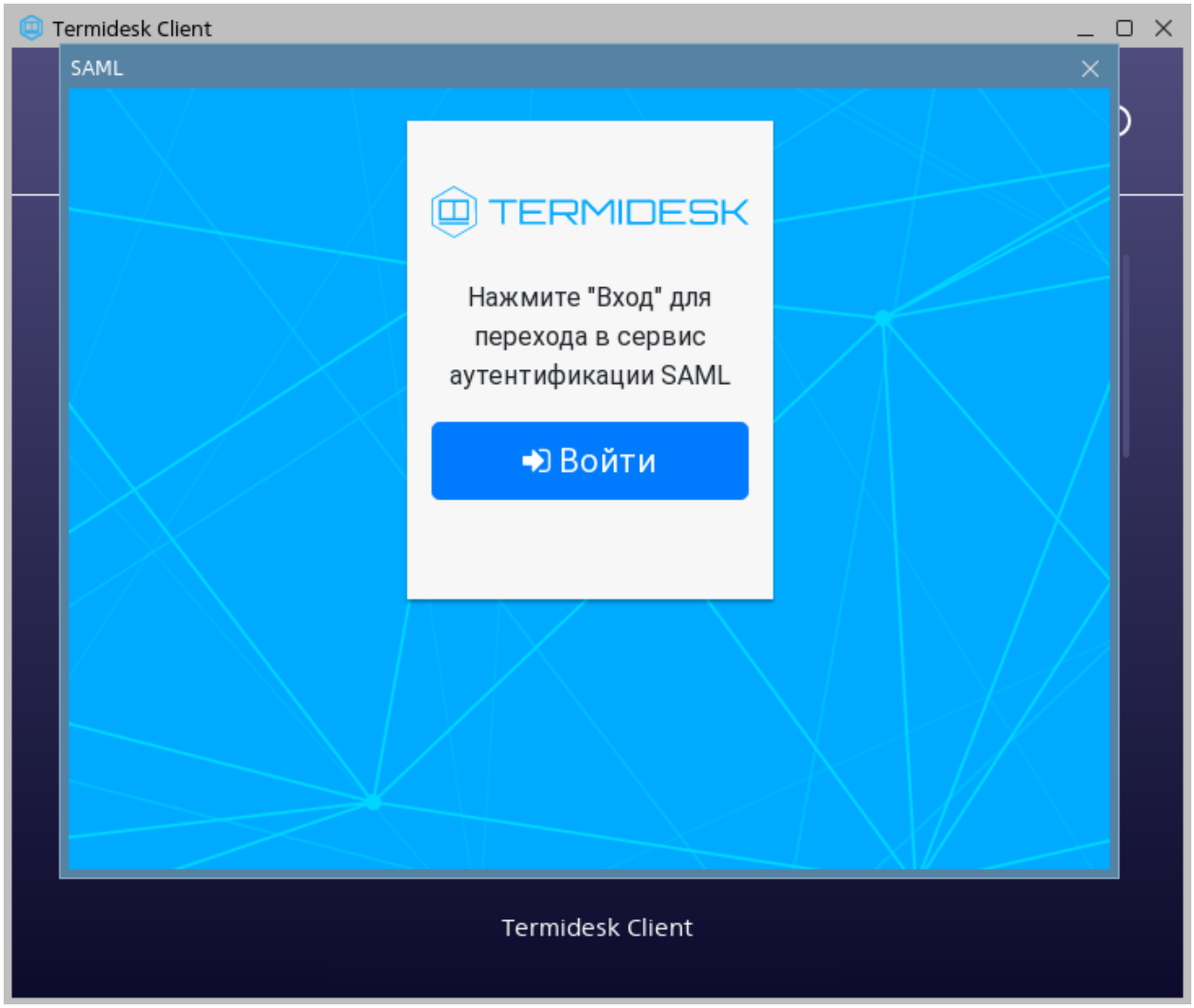


Рисунок 183. Окно перехода в сервис аутентификации

- откроется форма аутентификации, в которой нужно ввести учетные данные пользователя и нажать экранную кнопку **[Вход]** для подключения к серверу (см. рисунок Форма аутентификации в доменах «SAML»/«OpenID Connect»).

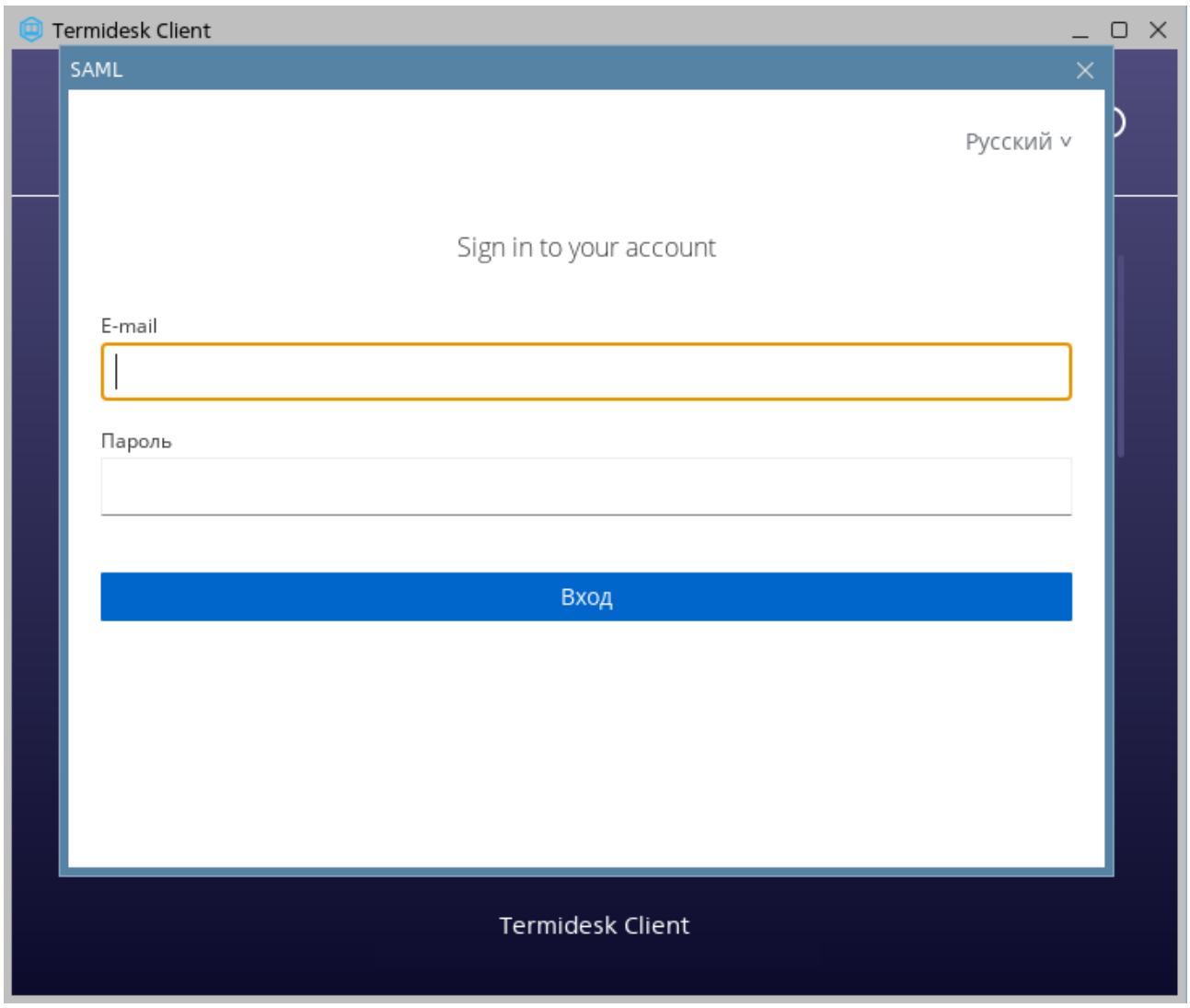


Рисунок 184. Форма аутентификации в доменах «SAML»/«OpenID Connect»

При подключении к выбранному серверу через домены типов «SAML» или «OpenID Connect» из ОС Microsoft Windows:

- откроется дополнительная вкладка в системном веб-браузере, в которой нужно нажать экранную кнопку **[Войти]** для подключения к серверу;
- откроется форма аутентификации, в которой нужно ввести учетные данные пользователя и нажать экранную кнопку **[Вход]** для подключения к серверу. При успешной аутентификации отобразится соответствующее сообщение. После появления сообщения вкладку в системном веб-браузере можно закрыть.

Подключение к доменам типа «LDAP (MS AD)» или «ALD Pro»

При подключении к выбранному серверу через домены типов «LDAP (MS AD)» или «ALD Pro» нужно:

- подключить смарт-карту или токен к считывателю и нажать экранную кнопку **[Да]** (см. рисунок Окно приглашения аутентификации по смарт-карте);

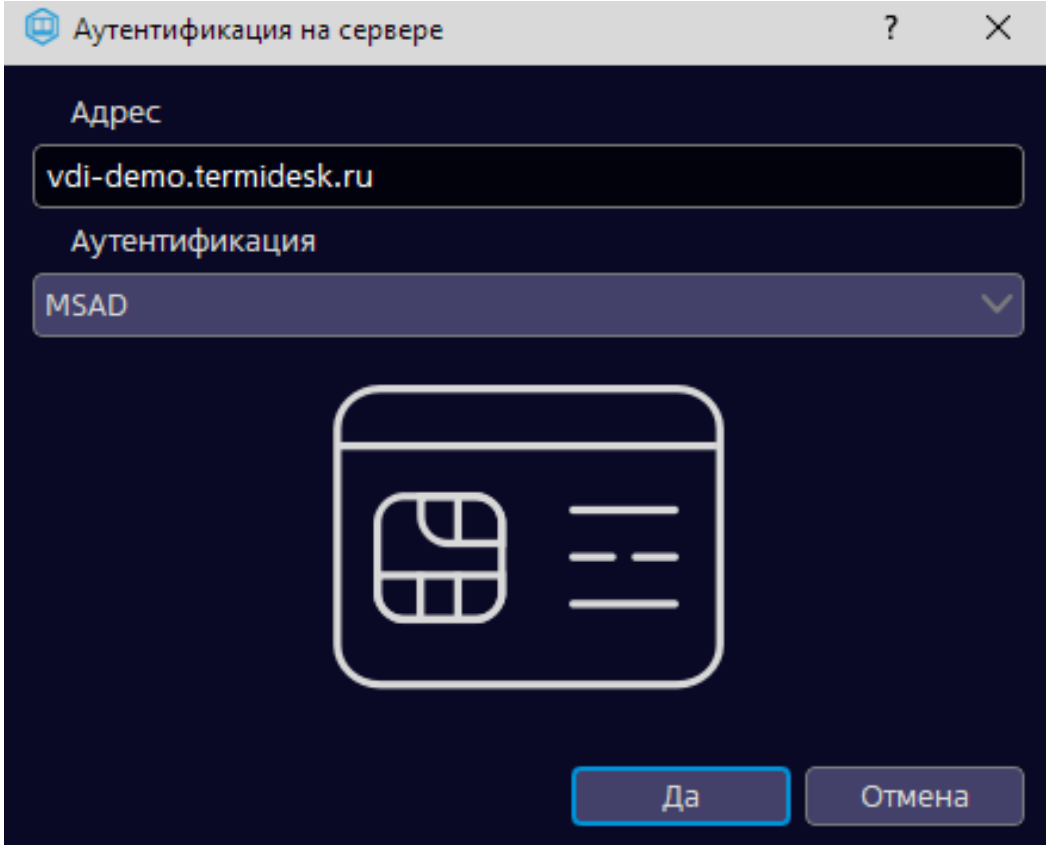


Рисунок 185. Окно приглашения аутентификации по смарт-карте

- если к пользовательской рабочей станции подключено несколько смарт-карт или токенов, то в поле «Ключевой носитель» выбрать нужное устройство;
- если на выбранном устройстве существует несколько сертификатов пользователя, то в поле «Имя пользователя» выбрать нужный сертификат;
- затем ввести PIN-код на смарт-карту или токен.

Настройка аутентификации по виртуальной смарт-карте (TPM)

Аутентификация по виртуальной смарт-карте выполняется по протоколу RDP для следующих сценариев:

- для пользовательской рабочей станции: ОС Microsoft Windows;
- для РМ: ОС Microsoft Windows.

Особенности функционирования:

- технология единого входа не работает для сценария ОС Microsoft Windows - ОС Microsoft Windows. Пользователю потребуется вводить PIN-код при каждом входе в сессию.

Для работы функционала на пользовательской рабочей станции с ОС Microsoft Windows нужно:

Используется встроенная утилита `tpmvscmgr.exe` для управления виртуальными смарт-картами.

- создать виртуальную смарт-карту (токен). Для этого запустить командную строку от имени администратора и выполнить (в ответе команды будет путь к созданному устройству, например, `ROOT\SMARTCARDREADER\0001`):

```
tpmvscmgr.exe create /name TPMContainerName /pin default /adminkey default
/generate
```

Где:

- /name – произвольное имя токена;
- /pin – PIN-код пользователя. Можно задать свой или использовать значение по умолчанию (12345678);
- /adminkey – административный PIN. Можно задать свой или использовать значение по умолчанию (12345678);
- /generate – создает новую пару ключей на TPM-токене (опционально, если планируется сразу генерировать ключ, а не импортировать готовый).

- записать сертификат на TPM-токен:

Используется оснастка certutil для импорта pfx-контейнера в TPM-токен.

```
certutil -csp "Microsoft Base Smart Card Crypto Provider" -f -p "PIN" -importpfx
"C:\Users\<User>\Documents\admin_cert.pfx"
```

Где:

- -csp – обязательно указывать провайдер Microsoft Base Smart Card;
- -p – PIN-код, которым был защищен pfx-контейнер при экспорте;
- -importpfx` – путь к pfx-контейнеру.

После успешного выполнения сертификат будет доступен для аутентификации.

Для удаления TPM-токена необходимо знать идентификатор устройства в диспетчере устройств. Получить его можно при создании или из ветки «Устройства и принтеры». Для удаления выполнить:

Не поддерживается удаление по имени контейнера, только по идентификатору устройства.

```
tpmvscmgr.exe destroy /instance ROOT\SMARTCARDREADER\0001
```

Аутентификация на сервере подключений с использованием механизма OTP

При добавлении сервера или при подключении к уже добавленному серверу пользователь может пройти аутентификацию на нем с использованием механизма OTP. Для этого необходимо, чтобы:

- администратор настроил поддержку использования OTP в домене аутентификации с типом «RADIUS»;

- в настройках подключения был выбран домен аутентификации с типом «RADIUS».

Аутентификация с использованием механизма OTP поддерживается:

- при подключении через веб-браузер;
- при подключении через Клиент. Для этого нужно выбрать сервер подключений и нажать экранную кнопку **[Подключиться]**.

При подключении через Клиент в зависимости от заданного администратором режима аутентификации потребуется:

- если используется многоэтапный режим аутентификации, то ввести код OTP в отдельном окне при подключении к серверу и нажать экранную кнопку **[Да]** (см. рисунок Окно запроса кода OTP в отдельном окне при подключении к серверу);

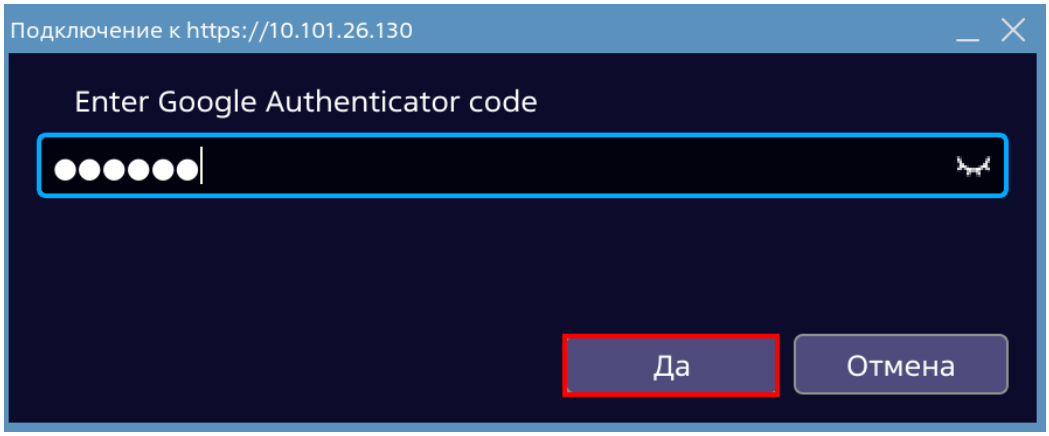


Рисунок 186. Окно запроса кода OTP в отдельном окне при подключении к серверу

- если используется одноэтапный режим аутентификации, то заполнить параметр «OTP» (параметры «Аутентификация» и «Пароль» должны быть также заполнены) в окне аутентификации на сервере и нажать экранную кнопку **[Да]** (см. рисунок Окно аутентификации на сервере подключений).

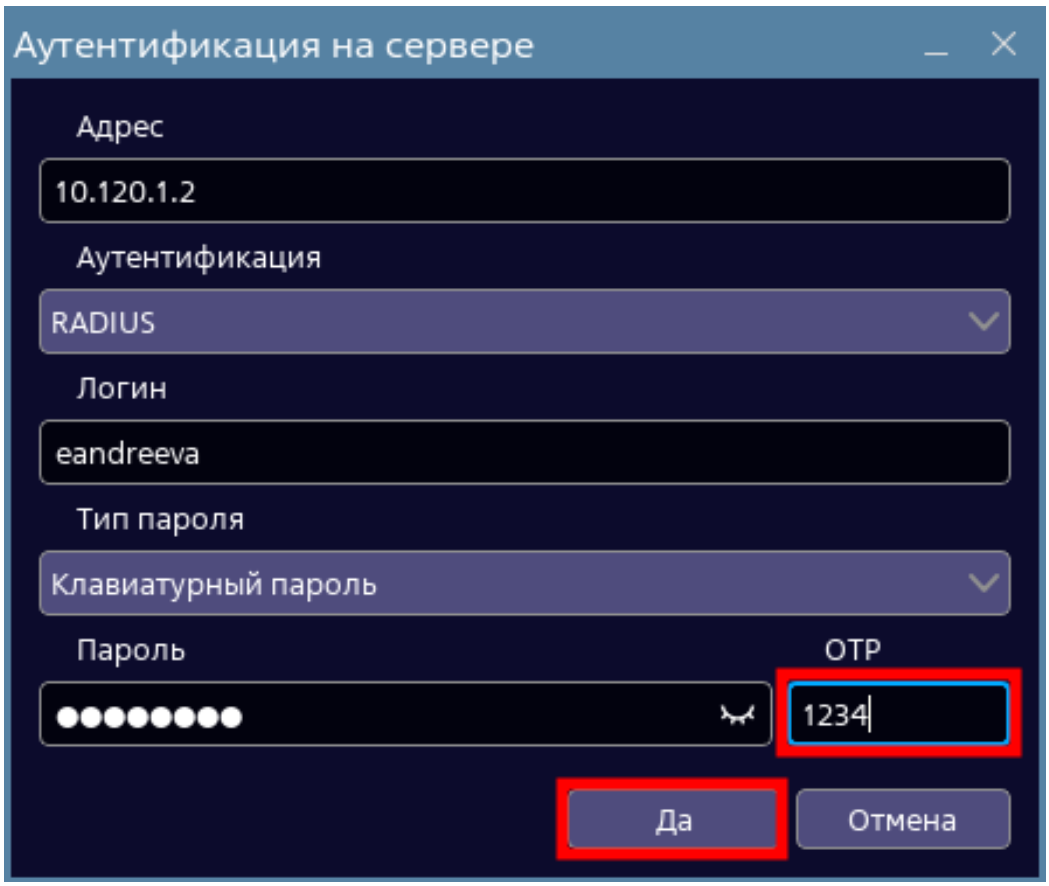


Рисунок 187. Окно аутентификации на сервере подключений

Kerberos-аутентификация на сервере подключений без смарт-карты

При добавлении сервера или при подключении к уже добавленному серверу пользователь может пройти аутентификацию на нем без использования смарт-карты или токена. Для этого необходимо, чтобы:

- пользовательская рабочая станция была введена в домен;
- пользователь авторизовался в ОС пользовательской рабочей станции.

Функционал поддерживается для:

- домена LDAP;
- при использовании Клиента и ПО Termidesk Viewer, поддерживающих библиотеку `FreeRDP 3`. Таким образом функциональность поддерживается, если подключение осуществляется из ОС:
  - macOS;
  - Astra Linux Special Edition 1.8;
  - РЕД ОС 8;
  - Microsoft Windows.

Kerberos-аутентификация без предъявления смарт-карты может использоваться:

- при подключении непосредственно из Клиента;
- при подключении из веб-браузера.

Администратором должна быть выполнена настройка пользовательской рабочей станции для работы с Kerberos-аутентификацией в домене LDAP.

> Для прохождения аутентификации нужно в настройках сервера подключения выбрать домен аутентификации с настроенным функционалом Kerberos-аутентификации.

При подключении к выбранному серверу через домен аутентификации типа «LDAP» нужно:

- в окне аутентификации на сервере нажать экранную кнопку **[Да]** (см. рисунок Окно приглашения Kerberos-аутентификации);

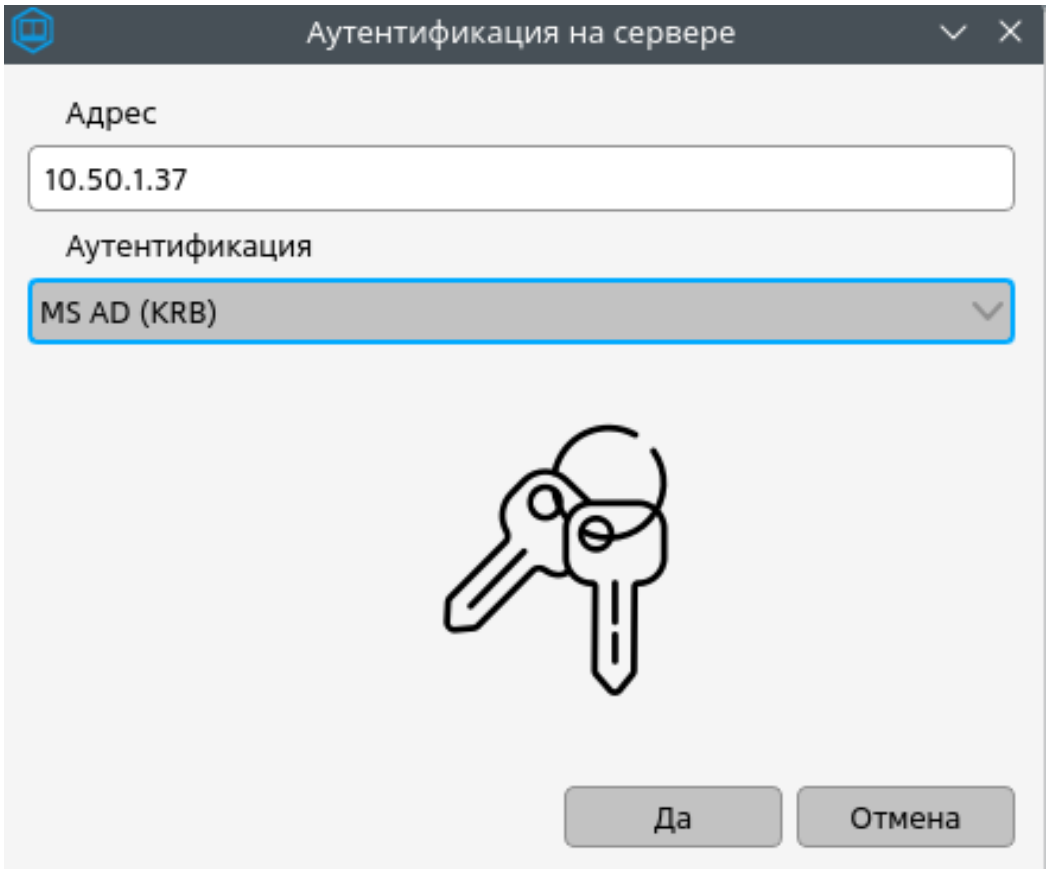


Рисунок 188. Окно приглашения Kerberos-аутентификации

- дождаться окончания процесса аутентификации и отображения списка ресурсов.

Настройка аутентификации через носитель TouchMemory

Клиент поддерживает аутентификацию пользователя через носитель TouchMemory, а именно - через программный продукт «Сетевой модуль TM-аутентификации WinNET» производства ООО «Фирма ИнфоКрипт».

> Функционал поддерживается Клиентом только для компонента «Универсальный диспетчер» версии 5.0 или выше.

Поддерживаемые ОС:

- для пользовательской рабочей станции: ОС Microsoft Windows;
- для РМ: ОС Microsoft Windows.

Для работы функционала нужно:

- установить на пользовательскую рабочую станцию ПО WinNET, при установке выбрать значение «Клиент с MsTs»;

- установить на пользовательскую рабочую станцию ПО Vitamin (клиент). ПО WinNET обеспечивает возможность восстанавливать пароль для доменных учетных записей. WinNET использует функционал ПО Vitamin для чтения и записи данных на носителе TouchMemory;
- установить на пользовательскую рабочую станцию драйверы для работы считывателя TouchMemory;
- модифицировать системную переменную окружения `PATH`, добавив значение `C:\msys64\mingw64\bin` (см. рисунок Модификация системной переменной PATH). Для этого перейти в «Пуск», найти «Этот компьютер» и нажать на этот пункт правой кнопкой мыши, выбрать «Свойства». В открывшемся окне перейти в «Дополнительные параметры системы» и во вкладке «Дополнительно» нажать экранную кнопку **[Переменные среды]**. Выбрать переменную «Path» в списке системных переменных, нажать экранную кнопку **[Изменить]**, добавить значение `C:\msys64\mingw64\bin`;
- подключить считыватель TouchMemory к пользовательской рабочей станции.

РМ должно быть подготовлено администратором для работы с носителем TouchMemory.

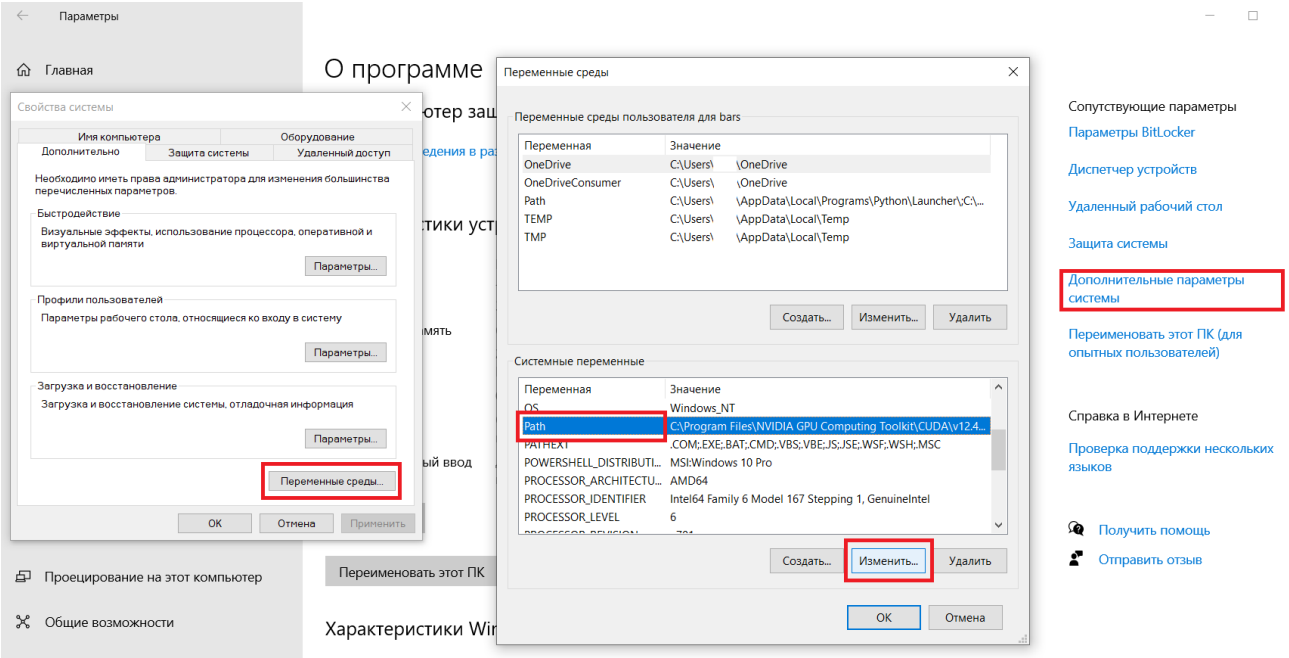


Рисунок 189. Модификация системной переменной PATH

Для доменной аутентификации непосредственно в ВРМ с носителем Touch Memory необходимо использовать полное имя пользователя, включая наименование домена.

При смене пароля на экране аутентификации в ВРМ будут показаны два списка с выбором способа формирования пароля: первый для старого пароля, второй для нового. При смене пароля Touch Memory на другой пароль с Touch Memory носитель необходимо приложить к считывателю дважды.

Аутентификация по смарт-картам в гостевой ОС РМ

После аутентификации по смарт-карте на сервере подключений (см. подраздел **Аутентификация на сервере подключений по смарт-картам**) пользователь также будет аутентифицирован по ней в гостевой ОС РМ.

В таблице приняты обозначения:

- «STAL» - терминальный сервер с установленным компонентом «Сервер терминалов Astra Linux».

Администратор должен:

- включить соответствующие политики фонда РМ:
  - для работы перенаправления смарт-карт;
  - для работы автоматического входа в систему при подключении к РМ;
- выполнить дополнительную настройку STAL:
  - узел STAL должен быть введен в домен с использованием инструмента `sssd` (для службы каталогов MS AD инструмент `winbind` не должен использоваться);
  - на узле STAL в параметре `use_fully_qualified_names` файла `sssd.conf` должно быть задано значение `True`.

При подключении по протоколу RDP из Клиента могут использоваться стандартные утилиты ОС, в этом случае возможность перенаправления смарт-карт регулируется на уровне протокола.

Поддерживаемые сценарии работы технологии единого входа в гостевую ОС РМ приведены в таблице (см. таблицу Сценарии работы технологии единого входа в гостевой ОС РМ по смарт-карте). Сценарии актуальны при подключении к РМ непосредственно из Клиента.

Рекомендуется подключать к пользовательской рабочей станции только одну смарт-карту для корректной работы аутентификации.

Таблица 315. Сценарии работы технологии единого входа в гостевой ОС РМ по смарт-карте

Комбинации ОС	RDP (termidesk-viewer)
Astra Linux Special Edition → Microsoft Windows	[1]
Astra Linux Special Edition → STAL	
Microsoft Windows → Microsoft Windows	[1]
Microsoft Windows → STAL	

Примечание:

[1] Не подтверждена работа сценария с виртуальной смарт-картой (TPM).

КЛИЕНТ. ДОСТУП К ДЕМОНСТРАЦИОННОМУ СТЕНДУ

Для ознакомления с функционалом Termidesk VDI можно подключиться к демонстрационному стенду.

Для подключения следует использовать значения параметров, перечисленные в таблице (см. таблицу Параметры для подключения к демонстрационному стенду).

Таблица 316. Параметры для подключения к демонстрационному стенду

Параметр	Значение	Примечание
Адрес подключения	https://vdi-demo.termidesk.ru/	
Аутентификация для доступа в Termidesk VDI		

Параметр	Значение	Примечание
Пользователь 1	Имя: `termidesk1` Пароль: `termidesk1` Домен аутентификации: «FreeIPA»	Все РМ
Пользователь 2	Имя: `termidesk2` Пароль: `termidesk2` Домен аутентификации: «FreeIPA»	Ограниченный набор РМ
Аутентификация в гостевых ОС рабочих мест		
Локальный пользователь в ОС Astra Linux и Windows	В зависимости от подключившегося пользователя (см. значения для параметров «Пользователь 1» и «Пользователь 2»)	Автоопределение разрешения экрана применяется

При использовании Клиента необходимо добавить сервер и настроить подключение, заполнив экранные поля вышеперечисленными значениями (см. рисунок Пример ввода параметров для подключения).

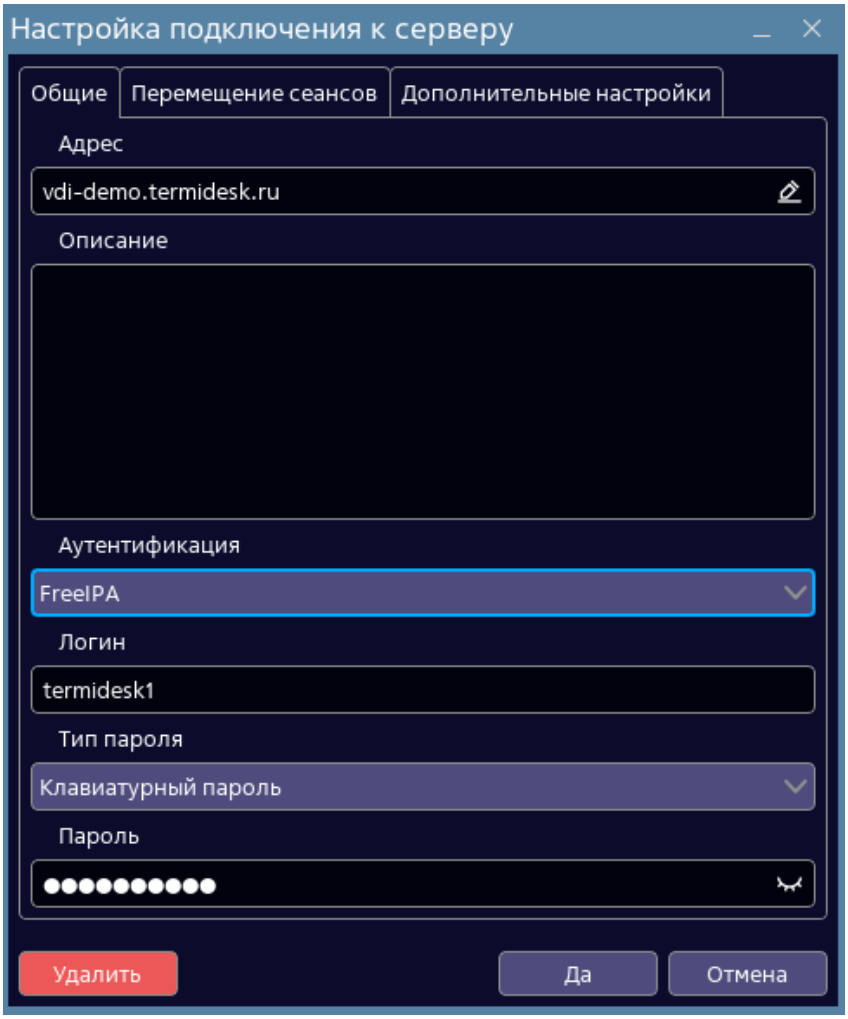


Рисунок 190. Пример ввода параметров для подключения

При использовании веб-браузера в адресную строку ввести адрес подключения, далее занести данные аутентификации для доступа на Termidesk VDI (см. рисунок Пример подключения через веб-браузер).

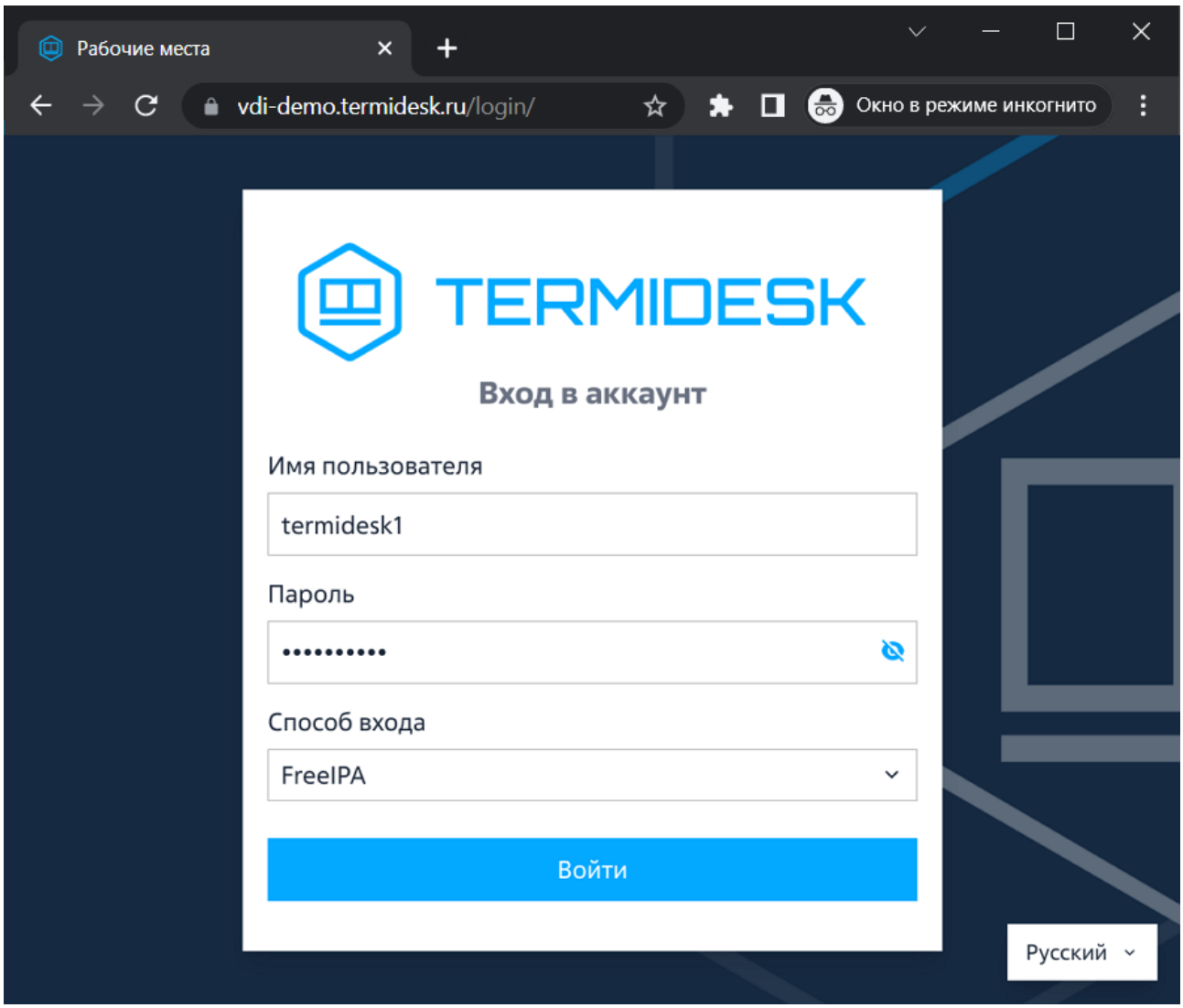


Рисунок 191. Пример подключения через веб-браузер

КЛИЕНТ. ЦЕНТР ПОДКЛЮЧЕНИЙ

Центр подключений позволяет централизованно просматривать и управлять открытыми сессиями, запущенными через Клиент с использованием ПО Termidesk Viewer.

Центр подключений недоступен для ОС macOS.

Для просмотра списка открытых сессий нужно нажать на графический элемент в виде монитора в правом верхнем углу графического интерфейса. Также можно просмотреть список открытых сессий через системный трей, нажав на изображение («иконку») Клиента правой кнопкой мыши.

В открывшемся окне «Центр подключений» список сессий представлен в табличном виде и содержит следующую информацию (см. рисунок Окно Центра подключений):

- «Адрес» - IP-адрес или FQDN узла, к которому выполнено подключение через Клиент;
- «Название» - название публикации РМ;
- «Пользователь» - имя пользователя, которому было выдано РМ.

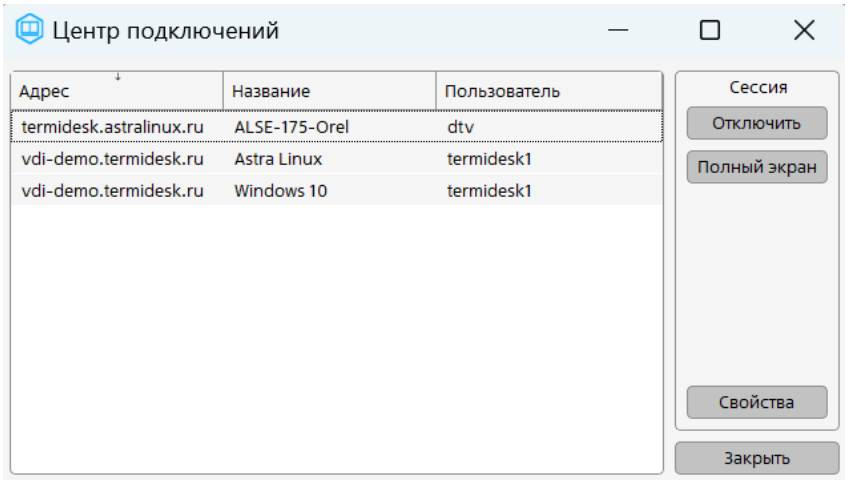


Рисунок 192. Окно Центра подключений

В текущей версии Termidesk VDI Центр подключений предоставляет следующие возможности по управлению ПО Termidesk Viewer:

- завершение работы ПО Termidesk Viewer. Для завершения работы следует выбрать нужную сессию в списке и нажать экранную кнопку **[Отключить]**. Если в ПО Termidesk Viewer была открыта терминальная сессия, она также завершится в компоненте «Универсальный диспетчер»;
- управление режимом окна ПО Termidesk Viewer. Для изменения режима окна следует выбрать нужную сессию в списке и нажать экранную кнопку:
  - **[Полный экран]** для перехода в полноэкранный режим. Кнопка доступна, если сессия пользователя открыта в оконном режиме;
  - **[Оконный]** для перехода в оконный режим. Кнопка доступна, если сессия пользователя открыта в полноэкранном режиме.

Для просмотра сведений о параметрах сессии пользователя следует выбрать нужную сессию в списке и нажать экранную кнопку **[Свойства]**. В открывшемся окне будет доступна следующая на информация (см. рисунок Окно сведений о параметрах сессии пользователя):

- «Версия клиента» - текущая версия установленного Клиента;
- «Версия просмотрщика» - текущая версия установленного ПО Termidesk Viewer;
- «Адрес сервера» - IP-адрес или FQDN узла, к которому выполнено подключение через Клиент;
- «Название» - название публикации РМ;
- «Идентификатор» - наименование РМ, выданного пользователю;
- «Пользователь» - имя пользователя, которому было выдано РМ;
- «Протокол» - название протокола, который используется для подключения к РМ.

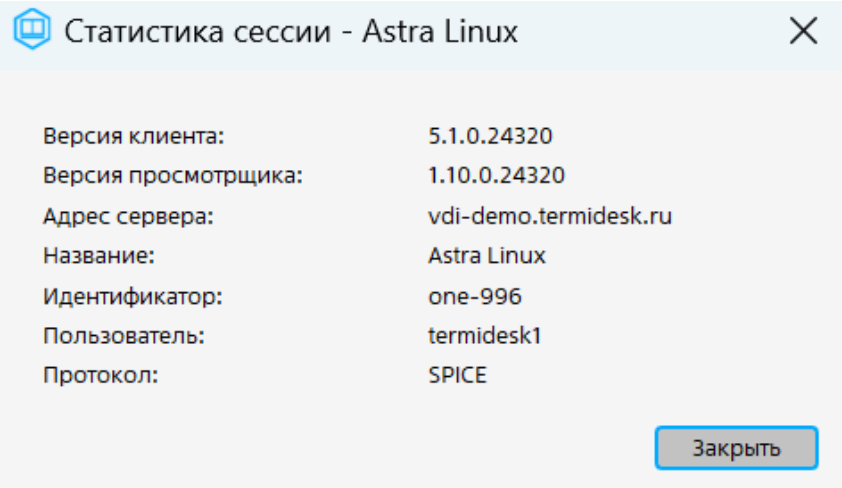


Рисунок 193. Окно сведений о параметрах сессии пользователя

КЛИЕНТ. НАСТРОЙКИ

Конфигурационные файлы Клиента и ПО Termidesk Viewer

Конфигурационный файл `Termidesk Client.ini`

Параметры конфигурирования Клиента могут быть заданы через файл:

- ОС Microsoft Windows - `C:\Users\<user>\AppData\Roaming\UVEON\Termidesk Client.ini`;
- ОС Linux - `/home/<user>/.config/UVEON/Termidesk Client.ini`.

Начиная с Termidesk VDI версии 7.0 управление режимом использования ПО Termidesk Viewer перемещено из секции `[Global]` в секцию `[Servers]` и подчиняется настройкам, полученным от сервера Termidesk VDI.

При подключении пользователя из веб-браузера используется встроенный веб-клиент Termidesk Web Viewer, при необходимости использовать сторонние программы доставки (например, системные `mstsc.exe`, `xfreerdp`) потребуется явным образом задать в секции `[Global]` параметр `UseTermideskRDP` со значением `false`. Такая настройка будет использоваться, если от сервера Termidesk VDI вернулось значение «Не задано» для параметра «Соединение по RDP через Termidesk Viewer».

Для ОС macOS ПО Termidesk Viewer используется всегда.

Пример конфигурационного файла:

```
[Global]
# Язык приложения (ru - русский, en - английский)
Language=ru
# Стиль приложения (light - светлый, dark - темный)
Style=light
# Запуск только одного экземпляра клиента
OneInstance=true
# Игнорирование ошибок SSL (4.0.0)
ignoreSslErrors=true
# Безопасное хранение паролей, возможные значения false/true
```

```
secureStorage=false
# Использовать Termidesk Viewer для RDP (4.3.0)
UseTermideskRDP=true
# Отпечаток сертификата для подписания rdp файла mstsc.exe при подключении через WS
(5.0.0)
RDPSignSHA256=76FC4AFA6967D8EDDB3786C0364F767BF9C10397
# Адрес, который будет слушать vdi-proxy (5.0.0)
VdiProxyIniHost=0.0.0.0
# Текущая версия ПО (7.0.0)
Version=7.0.0
# Величина задержки (в миллисекундах) показа панели инструментов ПО Termidesk
Viewer после наведения на него указателем мыши
ViewerToolBarShowDelay=1000

# Параметры перенаправления звука при подключении по RDP (кроме STAL). Аналогично
опциям freerdp
# Общий формат: sound[:
[sys:<sys>,][dev:<dev>,][format:<format>,][rate:<rate>,][channel:<channel>,][latenc
y:<latency>,][quality:<quality>]]
# Важно: выбранные параметры должны поддерживаться на стороне сервера
# rate: стандартное значение частоты звука в Гц (8000, 22050, 44100, 48000 и др.)
# channel: количество каналов звука (1 , 2 , 3 и др.)
# quality: качество передаваемого звука. Текст или число: dynamic - 0 (частота
будет меняться в зависимости от задержек канала), medium - 1, high - 2
# latency: величина задержки (в миллисекундах)

# Для ОС Linux рекомендуется использовать sys:alsa, для других ОС не задавать
RDPSound="format:0xA106,latency:200,quality:0"

# Параметры перенаправления звука при подключении по RDP для STAL
RDPSoundSTAL="format:1,latency:50,quality:medium"

[MainWindow]
# Скрытие клиента в трей (4.1.0)
CloseToTray=false
# Геометрия главного окна (формат Qt)
Geometry=01d9d0cb00030000000001fb000000d6000006fa00000387000001fb000000f3000006fa00
000387000000000000000000780000001fb000000f3000006fa00000387
# Порядок отображения серверов
ServersOrder=27d22dce-2255-4abe-b4e0-c0fee7100351, 2682d0e9-bb75-4e0e-8f61-
5216b5c95205
# Режим отображения рабочих мест 0 - список, 1 - плитки
WorkplacesViewMode=0

[Servers]
# {server-id} - идентификатор узла «Универсального диспетчера»
{server-id}\Auth=\x412\x43d\x443\x442\x440\x435\x43d\x43d\x44f\x44f \x411\x414
# Комментарий
{server-id}\Comment=
```

```
# Логин
{server-id}\Login=user1
# Тип пароля для аутентификации
{server-id}\PassType=Keyboard
# При значении параметра secureStorageEnabled=false, хранит пароль, преобразованный
с помощью алгоритма blowfish.
# При значении параметра secureStorageEnabled=true, в зависимости от ОС, хранит
префикс, указывающий на способ хранения.
# Для UNIX - secretservice:
# Для Windows - wincredential:
{server-id}\Password=blowfish:hidden
# Профиль настроек монитора в кодировке base64 (в примере -
b64%3AQXN0cmEgTGludXg%3D)
{server-
id}\Screens\b64%3AQXN0cmEgTGludXg%3D\SPICE\Displays\0\Monitors\0\IsPrimary=false
{server-
id}\Screens\b64%3AQXN0cmEgTGludXg%3D\SPICE\Displays\0\Monitors\0\LocalGeometry=@Rec
t(33 158 1322 935)
{server-
id}\Screens\b64%3AQXN0cmEgTGludXg%3D\SPICE\Displays\0\Monitors\0\RemoteGeometry=@Re
ct(0 0 1024 768)
{server-
id}\Screens\b64%3AQXN0cmEgTGludXg%3D\SPICE\Displays\0\Monitors\0\WindowState=0
{server-id}\Screens\b64%3AQXN0cmEgTGludXg%3D\SPICE\LocalMonitors\0\Geometry=@Rect(0
0 3440 1440)
# Хост сервера
{server-id}\Url=vdi-demo.termidesk.ru
# Последняя полученная версия сервера (4.3.1)
{server-id}\Version=5.0
# Идентификатор выбранного транспорта для рабочего места
{server-id}\Workplaces\{b64:workplaceName}\FavoriteTransportId=6ac1f9f5-9ae0-5ae0-
a304-cf967b582900
# Список избранных рабочих мест
{server-id}\FavoriteWorkplaces={b64:workplaceName}
# Название аутентификатора
{server-id}\Auth=termidesk-freeipa
# Запрет сохранения пароля и удаление ранее сохраненного (4.3.1)
{server-id}\KeepPassword=false
# Запрет сохранения логина и удаление ранее сохраненного (4.3.1)
{server-id}\KeepLogin=false
# Подключение к сессии при аутентификации, 2 — активировано, 0 — деактивировано
(5.1.0)
{server-id}\sessionReconnect=2
# Управление повторным подключением к сессии, 3 - активировано, 0 — деактивировано
(5.1.0)
{server-id}\sessionRoaming=3

# Список автоматически перенаправляемых USB-устройств для протоколов RDP/SPICE/TERA
и каждого известного сервера/рабочего места
```

```
{server-id}\Devices\{b64:workplaceName}\{protocol}\Usb\AutoConnect=false
# {server-id} - идентификатор узла «Универсального диспетчера»;
# {b64:workplaceName} - наименование рабочего места в кодировке base64;
# {protocol} - тип протокола доставки;
# AutoConnect - флаг, управляет автоматическим перенаправлением устройств, true -
устройства перенаправляются автоматически, false — автоматическое перенаправление
не выполняется

# Список перенаправленных USB-устройств для протокола RDP/SPICE/TERA, каждого
известного сервера/рабочего места и каждого известного устройства
{server-id}\Devices\{b64:workplaceName}\{protocol}\Usb\List\1\Id=(VID:13FE
PID:5200)
# Id - идентификатор устройства (пример: (VID:13FE PID:3423))
{server-id}\Devices\{b64:workplaceName}\{protocol}\Usb\List\1\Name=Silicon-Power32G
# Name - наименование устройства
{server-id}\Devices\{b64:workplaceName}\{protocol}\Usb\List\1\ExpiredAt=<
secsSinceEpoh + 30days, 0 >
# ExpiredAt - временная метка, при наступлении которой запись о перенаправленном
устройстве удалится. При каждом перенаправлении устройства значение обновляется и
устанавливается как текущее POSIX-время с добавлением срока хранения (30 дней).
{server-id}\Devices\{b64:workplaceName}\{protocol}\Usb\List\1\Enabled=true
# Enabled - флаг, управляет перенаправлением устройства в рабочее место, true -
перенаправлять устройство, false — не перенаправлять устройство
{server-id}\Devices\{b64:workplaceName}\{protocol}\Usb\List\1\UserInformed=false
# UserInformed - флаг, управляет отображением уведомления пользователя о
невозможности перенаправления устройства, true - уведомление отображено, false —
уведомление не отображено

# Список перенаправляемых каталогов для протокола RDP/SPICE/TERA, каждого
известного сервера/рабочего места и каждого известного каталога
{server-id}\Devices\{b64:workplaceName}\{protocol}\Drive\ReadOnly=false
# ReadOnly - флаг, определяет режим перенаправления каталога в режиме «Только
чтение», true - каталог доступен только для чтения, false — каталог доступен для
чтения и записи
{server-id}\Devices\{b64:workplaceName}\{protocol}\Drive\List\1\Path=H:/Downloads
# Path - путь к перенаправляемому каталогу
{server-id}\Devices\{b64:workplaceName}\{protocol}\Drive\List\1\ExpiredAt=0
# ExpiredAt - временная метка, при наступлении которой запись о перенаправленном
каталоге удалится. При каждом перенаправлении каталога значение обновляется и
устанавливается как текущее POSIX-время с добавлением срока хранения (30 дней).
{server-id}\Devices\{b64:workplaceName}\{protocol}\Drive\List\1\UserInformed=false
# UserInformed - флаг, управляет отображением уведомления пользователя о
невозможности перенаправления каталога, true - уведомление отображено, false —
уведомление не отображено
{server-id}\Devices\{b64:workplaceName}\{protocol}\Drive\List\size=1
# size - количество сохраненных каталогов

# Список перенаправляемых смарт-карт для протокола RDP/SPICE/TERA, каждого
известного сервера/рабочего места и каждого экземпляра смарт-карты
```

```
{server-
id}\Devices\{b64:workplaceName}\{protocol}\Smartcard\List\1\Atr="@ByteArray(;\xdc\x
18\xff\x81\x91\xfe\x1f\xc3\x80s\xc8!\x13\x66\x1\x6\x11Y\0\x1()"
# Atr - значение ATR (Answer To Reset), используется для идентификации модели
смарт-карты
{server-id}\Devices\{b64:workplaceName}\{protocol}\Smartcard\List\1\Name=Alladin
R.D. JCR
# Name - наименование смарт-карты
{server-id}\Devices\{b64:workplaceName}\{protocol}\Smartcard\List\1\ExpiredAt=<
secsSinceEpoh + 30days, 0 >
# ExpiredAt - временная метка, при наступлении которой запись о перенаправленной
смарт-карте удалится. При каждом перенаправлении смарт-карты значение обновляется и
устанавливается как текущее POSIX-время с добавлением срока хранения (30 дней).
{server-id}\Devices\{b64:workplaceName}\{protocol}\Smartcard\List\1\Enabled=true
# Enabled - флаг, управляет перенаправлением смарт-карты в рабочее место, true -
перенаправлять смарт-карту, false — не перенаправлять смарт-карту
{server-
id}\Devices\{b64:workplaceName}\{protocol}\Smartcard\List\1\UserInformed=true
# UserInformed - флаг, управляет отображением уведомления пользователя о
невозможности перенаправления смарт-карты, true - уведомление отображено, false —
уведомление не отображено
```

Конфигурационный файл `Termidesk Viewer.ini`

Параметры конфигурирования могут быть заданы через файл:

- ОС Microsoft Windows - `C:\Users\<user>\AppData\Roaming\UVEON\Termidesk Viewer.ini`;
- ОС Linux - `/home/<user>/.config/UVEON/Termidesk Viewer.ini`.

Пример конфигурационного файла:

```
# Диалог перенаправления принтеров
[Printers redirection]
# Сохранение геометрии диалога
Geometry=@ByteArray(\x1\xd9\xd0\xcb\0\x3\0\0\0\0\x4\x99\0\0\x3\n\0\0\x6\xaa\0\0\x4)
\0\0\x4\x9e\0\0\x3%\0\0\x6\xa5\0\0\x4$\0\0\0\0\0\0\0\0\n\0\0\0\x4\x9e\0\0\x3%\0\0\x
6\xa5\0\0\x4$)

# Диалог перенаправления каталога
[SharingDir]

# Выбранный каталог для перенаправления
Dir=/home/as/Documents

# Сохранение геометрии диалога
Geometry=@ByteArray(\x1\xd9\xd0\xcb\0\x3\0\0\0\0\x4\x97\0\0\x3\x43\0\0\x5\xb7\0\0\x
3\xf1\0\0\x4\x9c\0\0\x3^\0\0\x5\xb2\0\0\x3\xec\0\0\0\0\0\0\0\0\n\0\0\0\x4\x9c\0\0\x
3^\0\0\x5\xb2\0\0\x3\xec)
ReadOnly=0
```

```
# Диалог перенаправление USB устройств
[USB Redirection]
# Сохранение геометрии диалога
Geometry=@ByteArray(\x1\xd9\xd0\xcb\0\x3\0\0\0\0\x2\xbe\0\0\x11\0\0\x5\xa0\0\0\x2\x
af\0\0\x2\xc3\0\0\x1\x87\0\0\x5\x9b\0\0\x2\xaa\0\0\0\0\0\0\0\0\n\0\0\0\x2\xc3\0\0\x
1\x87\0\0\x5\x9b\0\0\x2\xaa)
```

Для ОС macOS по умолчнию действие клавиши **<Cmd>** соответствует **<Ctrl>**. Изменение назначения клавиши выполняется в конфигурационном файле `Termidesk Viewer.ini` в параметре `Mac_CommandKeyAs`. Доступные значения:

- `Win` - при нажатии **<Cmd>** в РМ отправится клавиша **<Win>**;
- `Ctrl` - при нажатии **<Cmd>** в РМ отправится клавиша **<Ctrl>**.

Установка корневых сертификатов в ОС macOS

Для установки корневого сертификата в ОС macOS нужно:

- скопировать сертификат в формате `.pem` или `.cer` в каталог `~/Downloads`;
- дважды нажать левой кнопкой мыши на название сертификата;
- в окне «Добавление сертификатов» выбрать соответствующий тип связки ключей и нажать экранную кнопку **[Добавить]**:
  - «Вход» - сертификат будет добавлен в связку ключей текущего пользователя;
  - «Система» - сертификат будет добавлен в связку ключейвсех пользователей;
- в процессе установки сертификата нужно разрешить внесение изменений в системе в соответствующем окне уведомления;
- после успешной установки откроется приложение «Связка ключей»;
- наличие файла сертификата в разделе «Вход - Сертификаты» или «Система - Сертификаты» свидетельствует об успешной установке сертификата.

Для настройки доверия установленному сертификату нужно:

- в окне «Связка ключей» дважды нажать левой кнопкой мыши на название сертификата;
- в окне сведений о сертификате раскрыть список «Доверие» и задать значение «Всегда доверять» в поле «Параметры использования сертификата»;
- разрешить внесение изменений в системе в соответствующем окне уведомления.

Настройки доверия установленному сертификату будут применены только после закрытия окна сведений о сертификате.

После установки корневых сертификатов нужно выполнить перезапуск Клиента.

КЛИЕНТ. ГРАФИЧЕСКИЙ ИНТЕРФЕЙС

Общие сведения по работе с графическим интерфейсом Клиента

Для запуска графического интерфейса Клиента: * в ОС Microsoft Windows необходимо дважды щелкнуть левой кнопкой мыши по ярлыку Клиента на рабочем столе; * в ОС Astra Linux Special Edition открыть меню «Звезда», выбрать пункт «Утилиты» и в выпадающем

меню щелкнуть левой кнопкой мыши по строке «Termidesk VDI client».

После запуска графического интерфейса будут доступны следующие функции:

- «Центр подключений»;
- «Настройки»;
- «Просмотр информации о программе»;
- «Добавление сервера подключений»;
- «Управление аутентификацией»;
- «Удаление сервера подключений»;
- «Просмотр информации о доступных для подключения фондах рабочих мест»;
- «Выбор протокола доставки рабочего места»;
- «Выбор групп фондов рабочих мест»;
- «Выбор отображения доступных для подключения фондов рабочих мест».

Общие настройки

Для изменения общих настроек Клиента нужно нажать на графический элемент в виде шестеренки в правом верхнем углу интерфейса. При этом откроется окно «Настройки» (см. рисунок Окно настроек Клиента).

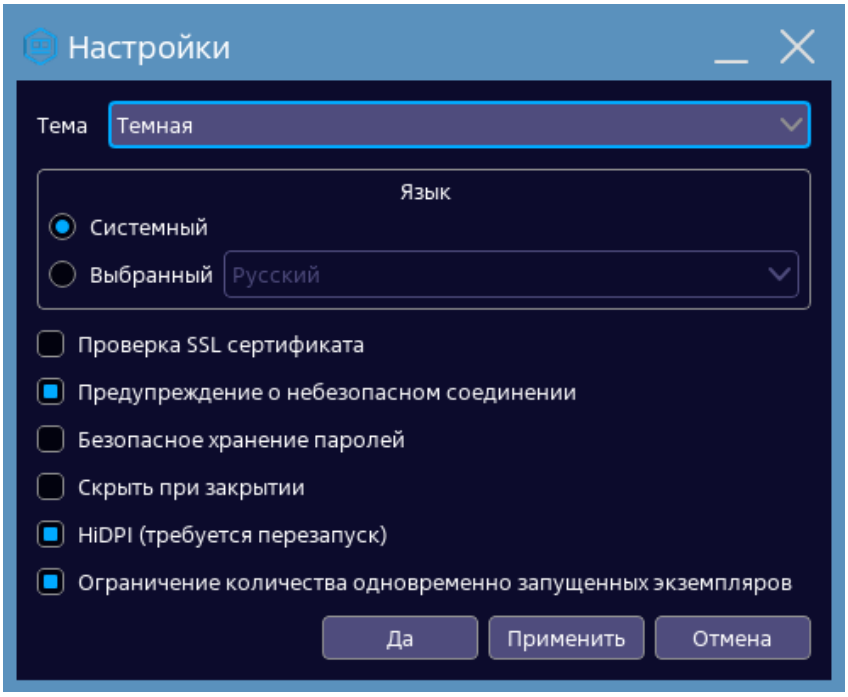


Рисунок 194. Окно настроек Клиента

В окне «Настройки» можно изменить следующие параметры:

- «Тема» - выбор темы оформления графического интерфейса;
- «Язык» - выбор поддерживаемого языка отображения;
- «Проверка SSL сертификата» - активация проверки валидности SSL-сертификата. Параметр необходимо отключить в случае, если проверку валидности пройти не удается:
  - на сервере подключения используются самоподписанные сертификаты;
  - или на сервере подключения используются сертификаты, выпущенные центром

сертификации, корневой сертификат которого не добавлен в список доверенных на узле Клиента;

> Для корректной работы Клиента проверка SSL-сертификатов должна быть отключена, если используются самоподписанные сертификаты.
>
> При подключении к РМ через компонент «Шлюз» с проверкой SSL-сертификатов они должны быть добавлены в ОС macOS:
>
> - в стандартную директорию ОС macOS - `/private/etc/ssl/`;
> - или в системное ПО Keychains («Связка ключей»).

- «Предупреждение о небезопасном соединении» - активация предупреждения о небезопасном подключении. При подключении к серверу по протоколу HTTP отобразится сообщение: «Ваше соединение небезопасно (http). Вы уверены, что хотите продолжить?»;

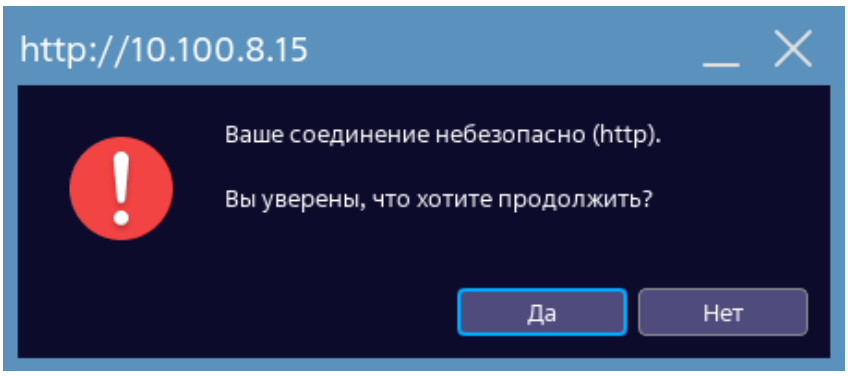


Рисунок 195. Сообщение о небезопасном подключении

- «Безопасное хранение паролей» - активация функции сохранения пароля при подключении к серверу, используя встроенные механизмы ОС. При активации параметра заданный пароль подключения к серверу будет храниться в преобразованном виде;
- «Скрыть при закрытии» - при закрытии окна Клиента не происходит выход из приложения, Клиент скрывается в системный трей;
- «HiDPI (требуется перезапуск)» - активация режима поддержки экранов с высокой плотностью пикселей. Для применения изменений требуется выполнить перезапуск Клиента;
- «Ограничение количества одновременно запущенных экземпляров» - при активации параметра нельзя будет запустить одновременно более одного экземпляра приложения. При попытке запустить еще одно приложение Клиента появится ошибка (см. рисунок Ошибка запуска второго экземпляра приложения). Соответственно, для активации возможности параллельного запуска нескольких окон Клиента, необходимо деактивировать данный параметр.

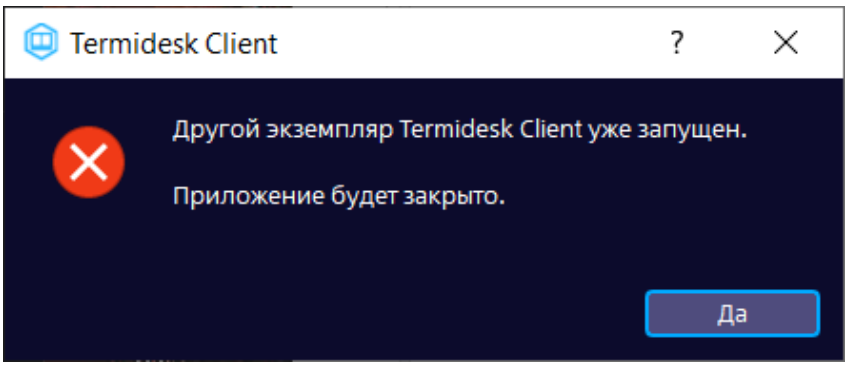


Рисунок 196. Ошибка запуска второго экземпляра приложения

Экранная кнопка **[Применить]** применяет параметры конфигурации Клиента.

Экранная кнопка **[Отменить]** отменяет параметры конфигурации Клиента и не сохраняет их.

Экранная кнопка **[Да]** сохраняет параметры конфигурации Клиента.

Для корректной работы с получением опубликованных через Microsoft Remote Desktop Services приложений необходимо выполнить дополнительную настройку ОС Microsoft Windows:

- нажать экранную кнопку **[Пуск]**, ввести `regedit` и выбрать `regedit.exe`;
- в открывшемся редакторе реестра открыть `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Terminal Server Client`;
- в меню «Правка» выбрать пункт «Создать», а затем «Параметр DWORD»;
- в поле «Новое значение 1» ввести `EnableAdvancedRemoteFXRemoteAppSupport` и нажать клавишу **<Enter>**;
- правой кнопкой мыши нажать на параметр `EnableAdvancedRemoteFXRemoteAppSupport` и выбрать пункт «Изменить»;
- в поле данных «Значение» ввести `0` и нажать экранную кнопку **[OK]**;
- закрыть редактор реестра.

Получение информации о версиях

Для просмотра информации о Клиенте нужно нажать на графический элемент в виде кружка с символом «i» в правом верхнем углу графического интерфейса.

В открывшемся окне будет доступна следующая информация (см. рисунок Информационное окно об установленной версии Клиента):

- «Название» - текстовое поле, содержащее текущее название Клиента;
- «Версия» - текущая версия установленного Клиента;
- «Версия ОС» - тип и версия ОС, на которую была проведена установка Клиента;
- «Версия Qt» - текущая версия установленного совместного компонента;
- «Необходимая версия сервера не ниже» - минимальная версия компонента «Универсальный диспетчер», с которым возможна работа текущей версии Клиента;
- «Сайт» - URL-сайта производителя;
- **[Информация для тех.поддержки]** - экранная кнопка, позволяющая выгружать диагностическую информацию (журналы событий и технические данные) о работе Клиента и ПО Termidesk Viewer в отдельное расположение файловой системы:

- при отсутствии подключения к серверу Termidesk VDI выгружается диагностическая информация только о работе Клиента и ПО Termidesk Viewer;
- при наличии активного подключения к серверу Termidesk VDI дополнительно формируется журнал со сведениями о текущем подключении к серверу.

Получить информацию о версиях можно также через системный трей, нажав на изображение («иконку») Клиента правой кнопкой мыши.

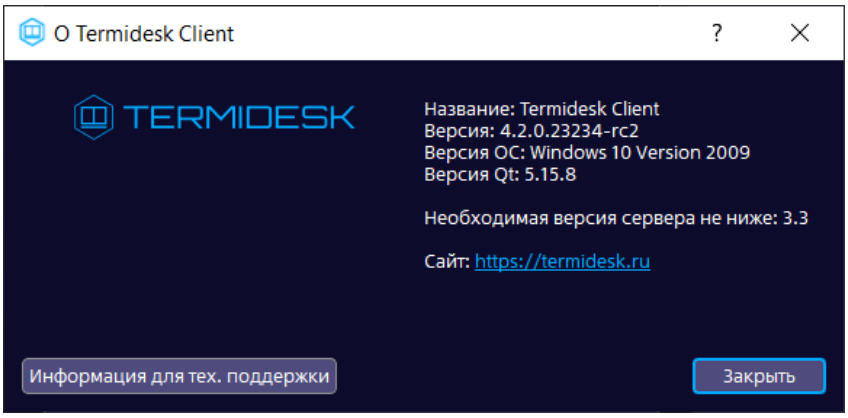


Рисунок 197. Информационное окно об установленной версии Клиента

КЛИЕНТ. ИнтерИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

Интерфейс командной строки Клиента

Параметры запуска и функционирования Клиента могут быть переопределены аргументами командной строки или переменными окружения.

Для получения краткой информации по доступным аргументам командной строки следует вызвать приложение `termidesk-client` с аргументом `--help`:

```
termidesk-client --help
```

Для получения полной информации по доступным аргументам командной строки следует вызвать приложение `termidesk-client` с аргументом `--help-all`:

```
termidesk-client --help-all
```

Для использования интерфейса командной строки Клиента в ОС Microsoft Windows нужно:

- открыть командную строку от имени администратора;
- вызывать Клиент из каталога `C:\Program Files\UVEON\Termidesk Client`;
- перенаправить вывод команды в файл. В указанном файле будет показан результат выполнения команды.

Пример получения полной информации по доступным аргументам командной строки с выводом в файл `C:\client_help_all.txt`:

```
"C:\Program Files\UVEON\Termidesk Client\termidesk-client.exe" --help-all >
C:\client_help_all.txt
```

Список доступных аргументов и переменных окружения приведен в таблице (см. таблицу Список аргументов командной строки и переменных окружения для Клиента).

В ОС Microsoft Windows указанные аргументы также воспринимаются, однако результат не выводится в командную строку.

После установки Клиента в ОС добавилась служба `Termidesk VDI TBUS`, необходимая для взаимодействия компонентов Termidesk VDI. Запуск службы осуществляется автоматически, через приложение `C:\Program Files\UVEON\Termidesk Client\termidesk-tbus.exe`.

Приложение `termidesk-tbus.exe` поддерживает ключ `-e`, позволяющий запустить `termidesk-tbus.exe` как исполняемый файл, а не как службу.

При задании переменных окружения стоит учесть, что они также влияют на настройки ПО Termidesk Viewer.

Таблица 317. Список аргументов командной строки и переменных окружения для Клиента

Параметр	Переменная окружения	Описание	Значение по умолчанию
`URL`	`TDSK_VDI_URL`	Адрес подключения к серверу или приложению. Параметр доступен с версии 4.3. Допустимые схемы: • `https://192.0.2.10` - подключение к серверу; • `daass://192.0.2.10/foo/bar` - подключение к приложению. Начиная с Termidesk VDI версии 5.1 поддерживается подключение к серверу с указанием URI сайта, например: `https://192.0.2.10/site`	`Не задано`
`--debug`	`TDSK_DEBUG`	Включение отладочного режима. Для включения режима через переменную окружения достаточно присвоить ей ненулевое значение. После диагностики рекомендуется отключать отладочный режим для исключения его влияния на качество подключения и воспроизведения медиаданных. В ОС macOS следует использовать: `TDSK_DEBUG=1 /Applications/Termidesk\ Client.app/Contents/MacOS/Termidesk\ Client`	`Не задано`
`--lang`	TDSK_LANG	Выбор языка для приложения. Параметр доступен с версии 5.0. По умолчанию язык будет определен из региональных настроек, установленных в ОС. Возможные значения: «ru», «en»	`auto`
`--timeout`	`TDSK_TIMEOUT`	Время ожидания сетевых подключений	`60`
`--user -auth`	`TDSK_USER_AUTH`	Имя домена аутентификации для подключения. Параметр доступен с версии 4.3.	`Не задано`

Параметр	Переменная окружения	Описание	Значение по умолчанию
`--user-name`	`TDSK_USER_NAME`	Имя пользователя для подключения. Параметр доступен с версии 4.3. Ограничения: • если имя содержит пробел, то нужно заключить его в двойные кавычки: `--user-name "User 1"`; • (только для ОС Linux) если имя содержит специальные символы, то нужно заключить его в одинарные кавычки: `--user-name 'User!123456'`; • (только для ОС Linux) если имя содержит и пробел, и специальные символы, то нужно заключить его в одинарные кавычки: `--user-name 'User! 123456'`	`Не задано`
`--user-password`	`TDSK_USER_PASSWORD`	Пароль пользователя для подключения. Параметр доступен с версии 4.3. Ограничения: • если пароль содержит пробел, то нужно заключить его в двойные кавычки: `--user-password "Password 1"`; • (только для ОС Linux) если пароль содержит специальные символы, то нужно заключить его в одинарные кавычки: `--user-password 'Password!123456'`; • (только для ОС Linux) если пароль содержит и пробел, и специальные символы, то нужно заключить его в одинарные кавычки: `--user-password 'Password! 123456'`	`Не задано`
`--version`	`Не задана`	Вывод текущей версии Клиента	`Не задано`

Параметр	Переменная окружения	Описание	Значение по умолчанию

`--workplace-name`	`Не задана`	Имя публикации для подключения к фонду РМ. Параметр доступен с версии 6.1. Пример использования приведен в подразделе **Прямое подключение к РМ**.
		
		Ограничения:
		
		• если имя содержит пробел, то нужно заключить его в двойные кавычки: `--workplace-name "Brest 1"`;
		• (только для ОС Linux) если имя содержит специальные символы, то нужно заключить его в одинарные кавычки: `--workplace-name 'Brest!123456'`;
		• (только для ОС Linux) если имя содержит и пробел, и специальные символы, то нужно заключить его в одинарные кавычки: `--workplace-name 'Brest! 123456'`.
		
		Пример команды для запуска из ОС Microsoft Windows:
		
		`"C:\Program Files\UVEON\Termidesk Client\termidesk-client.exe" <https://IP-адрес_или_FQDN_сервера_Termidesk> --workplace-name <имя_публикации> --protocol <имя_протокола_доставки> --user-name <имя_пользователя> --user-auth <имя_домена_аутентификации> --user-password <пароль_пользователя>`
		
		Пример команды для запуска из ОС Linux:
		
		`termidesk-client <https://IP-адрес_или_FQDN_сервера_Termidesk> --workplace-name <имя_публикации> --protocol <имя_протокола_доставки> --user-name <имя_пользователя> --user-auth <имя_домена_аутентификации> --user-password <пароль_пользователя>`
			`Не задано`

`--protocol`	`Не задана`	Протокол доставки для подключения к РМ. Параметр доступен с версии 6.1. Пример использования приведен в подразделе **Прямое подключение к РМ**. Допустимые значения: • идентификатор протокола доставки. Пример: `--protocol ce5ecd63-041f-5d5e-99c9-9de93a7a663d`; • наименование протокола доставки. Пример: `--protocol TERA`	`Не задано`
`Не задан`	`TDSK_RDS_GATEWAY HOSTNAME`	Имя шлюза (FQDN) для приложения `mstsc.exe`. Для корректной работы может потребоваться отредактировать файл `hosts` в ОС. Используется при подключении к шлюзу MS RDS через компонент «Шлюз»	`Не задано`

Параметр	Переменная окружения	Описание	Значение по умолчанию
Не задан	TDSK_RDP_SIGN_SHA256	Отпечаток сертификата для подписи файла формата RDP. Параметр доступен с версии 5.0. Может быть задан как через указанную переменную окружения, так и через конфигурационный файл Termidesk Client.ini в параметре RDPSignSHA256. Для использования идентификатора протокола доставки пользователь должен получить его у администратора. Администратор может получить идентификатор протокола доставки из: • таблиц базы данных Termidesk VDI; • журнала Клиента (в этом случае подключение к РМ по протоколу досавки должно произойти хотя бы один раз). Требуемый идентификатор можно найти в записи «transports». Задание параметра через конфигурационный файл, а не через переменную окружения, имеет бОльший приоритет. Используется для подключения к РМ через компонент «Шлюз» с использованием утилиты mstsc.exe. Параметр актуален только при подключении через утилиту mstsc.exe, соответственно, может работать только в среде ОС Microsoft Windows. Для использования подписи должны быть выполнены условия: • сертификат (открытый ключ), использующийся для подписи, должен быть передан на узел с Клиентом совместно с закрытым ключом к нему; • на узел с Клиентом должен быть установлен как сертификат, использующийся для подписи, так и закрытый ключ к нему. На узел должен быть установлен корневой сертификат, который использовался для выдачи сертификата, использующегося для подписи; • в поле «Common Name» сертификата, использующегося для подписи, должен быть задан FQDN узла с Клиентом. Подпись файла формата RDP и подключение на заданный в сертификате FQDN происходит только если отпечаток сертификата задан, иначе подключение инициируется на IP-адрес 127.0.0.1. Пример значения отпечатка сертификата при задании через переменную окружения: TDSK_RDP_SIGN_SHA256 = 76FC4AFA6967D8EDDB3786C0364F767BF9C10397	Не задано

Интерфейс командной строки ПО Termidesk Viewer

Параметры запуска и функционирования ПО Termidesk Viewer могут быть определены аргументами командной строки или переменными окружения.

Для получения краткой информации по доступным аргументам командной строки следует вызвать приложение vdi-viewer с аргументом --help:

```
vdi-viewer --help
```

Для получения полной информации по доступным аргументам командной строки следует вызвать приложение `vdi-viewer` с аргументом `--help-all`:

```
vdi-viewer --help-all
```

Для использования интерфейса командной строки ПО Termidesk Viewer в ОС Microsoft Windows нужно:

- открыть командную строку от имени администратора;
- вызывать приложение `vdi-viewer` из каталога `C:\Program Files\UVEON\Termidesk Viewer`;
- перенаправить вывод команды в файл. В указанном файле будет показан результат выполнения команды.

Пример получения полной информации по доступным аргументам командной строки с выводом в файл `C:\viewer_help_all.txt`:

```
"C:\Program Files\UVEON\Termidesk Viewer\vdi-viewer.exe" --help-all >
C:\viewer_help_all.txt
```

Список доступных аргументов приведен в таблице (см. таблицу Список аргументов командной строки и переменных окружения ПО Termidesk Viewer).

В ОС Microsoft Windows указанные аргументы также воспринимаются, однако результат не выводится в командную строку.

При задании переменных окружения стоит учесть, что они также влияют на настройки Клиента.

Таблица 318. Список аргументов командной строки и переменных окружения ПО Termidesk Viewer

Параметр	Переменная окружения	Описание	Значение по умолчанию
`--debug`	`TDSK_DEBUG`	Включение отладочного режима. Для включения режима через переменную окружения достаточно присвоить ей ненулевое значение. После диагностики рекомендуется отключать отладочный режим для исключения его влияния на качество подключения и воспроизведения медиаданных. В ОС macOS следует использовать: `TDSK_DEBUG=1 /Applications/Termidesk\ Client.app/Contents/MacOS/Termidesk\ Client`	Не задано

Параметр	Переменная окружения	Описание	Значение по умолчанию
`--lang`	`TDSK_LANG`	Выбор языка для приложения. Параметр доступен с версии ПО Termidesk Viewer 1.9.0. По умолчанию язык будет определен из региональных настроек, установленных в ОС. Возможные значения: `ru`, `en`	`auto`
`--timeout`	`TDSK_TIMEOUT`	Время ожидания подключения к компоненту «Шлюз» (в секундах). Параметр доступен с версии ПО Termidesk Viewer 1.5.0. С версии 1.10.0 параметр влияет также на время ожидания подключения к РМ по протоколу RDP. Для этого подключения может указан диапазон от 0 до 600 секунд. Крайне малые значения через переменную окружения задавать не рекомендуется, т.к. она влияет на настройки Клиента	`60`
`--version`	Не задана	Вывод текущей версии ПО Termidesk Viewer	Не задано
`--video-codec`	`TDSK_VIDEO_CODEC`	Кодек видеокамеры. Параметр доступен с версии ПО Termidesk Viewer 1.6. Возможные значения: • `libtheora` - нативный метод кодирования Theora; • `theora` - кодирование через конвейер Gstreamer	`libtheora`
Не задан	`TDSK_RDP_PRT_UNIVERSAL`	Определяет драйвер, который будет использован при перенаправлении принтера по протоколу RDP. Параметр доступен с версии ПО Termidesk Viewer 1.10.0. Наличие переменной `TDSK_RDP_PRT_UNIVERSAL` активирует перенаправление принтера с использованием универсального драйвера (Microsoft Software Printer Driver). Для перенаправления принтера с использованием нативного драйвера переменную нужно удалить	Не задано
Не задан	`TDSK_FILECOPY_BANDWIDTH`	Задает ограничение скорости передачи (Кбайт/с) файла по протоколу TERA. Отсутствие переменной эквивалентно значению `0`. Возможные значения: • `0` - скорость неограниченна; • `1 - 10000` - значение скорости	Не задано
Не задан	`TDSK_DISPLAY_BANDWIDTH`	Задает ограничение скорости (Кбайт/с) видеоканала при подключении по протоколу TERA. Отсутствие переменной эквивалентно значению `0`. Возможные значения: • `0` - скорость неограниченна; • `1 - 10000` - значение скорости	Не задано
Параметры для TERA-подключения			

Параметр	Переменная окружения	Описание	Значение по умолчанию

`--loginctrl`	`TDSK_LOGINCTRL`	Режим работы ПО Termidesk Viewer при завершении сессии. Параметр доступен с версии ПО Termidesk Viewer 6.1.
		
		Возможные значения:
		
		• `enable` - ПО Termidesk Viewer завершит работу при завершении или переключении сессии;
		• `disable` - ПО Termidesk Viewer не будет завершать работу при завершении или переключении сессии;
		• значение не задано - поведение зависит от режима аутентификации пользователя в РМ:
		  - если пользователь аутентифицировался с использованием технологии единого входа (SSO), то ПО Termidesk Viewer завершит работу при завершении или переключении сессии;
		  - если пользователь аутентифицировался с предъявлением пароля, то при завершении сессии отобразится экран блокировки с полем для ввода пароля для дальнейшей работы пользователя
			Не задано

`--keepalive`	Не задана	Время ожидания (в секундах) подтверждения приема от TERA. Если в течение заданного времени ответ не получен, то произойдет автоматическое рассоединение. Параметр доступен с версии ПО Termidesk Viewer 6.1. Параметр действует только для протокола TERA. Для протоколов RDP и SPICE используется значение по умолчанию (15 секунд). Возможные значения: • `0` - ожидание подтверждения приема отключено; • `1 - 7200`	`15`

Параметр	Переменная окружения	Описание	Значение по умолчанию
`--credentials_username`	Не задана	Идентификатор пользователя и контекст для аутентификации в TERA через поставщик учетных данных (Credentials Provider, в версии 6.1 только для ОС Microsoft Windows). Параметр доступен с версии ПО Termidesk Viewer 6.1. При вызове ПО Termidesk Viewer с этим параметром будет запрошен ввод пароля (аутентификатора Credentials Provider). Особенности: • параметр (параметры), введенный через интерактивный режим имеет приоритет выше, чем параметр (параметры), полученный из других источников; • если параметр задан в интерфейсе командной строки, то он переопределяет любые другие значения (например, из файла с расширением `.vv`); • если параметр не задан в интерфейсе командной строки, то используются значения из файла с расширением `.vv`); • если параметр не задан нигде, то будет передан признак отсутствия готовности аутентифицироваться через поставщик учетных данных. Формат: `<имя_пользователя>@<домен>`	Не задано
`--timezone_sync`	`TDSK_SYNC_TIMEZONE`	Режим работы ПО Termidesk Viewer для синхронизации временной зоны между пользовательской рабочей станцией и РМ. Параметр доступен с версии ПО Termidesk Viewer 6.1. Возможные значения: • `enable` - ПО Termidesk Viewer будет синхронизировать временную зону; • `disable` - ПО Termidesk Viewer не будет синхронизировать временную зону; • значение не задано - поведение зависит от настроек политик, пришедших от сервера и от настроек TERA	Не задано
`--time_sync`	`TDSK_SYNC_TIME`	Режим работы ПО Termidesk Viewer для синхронизации времени между пользовательской рабочей станцией и РМ. Параметр доступен с версии ПО Termidesk Viewer 6.1. Возможные значения: * `enable` - ПО Termidesk Viewer будет синхронизировать время; * `disable` - ПО Termidesk Viewer не будет синхронизировать время; * значение не задано - поведение зависит от настроек политик, пришедших от сервера и от настроек TERA	Не задано

Параметр	Переменная окружения	Описание	Значение по умолчанию
--audio_latency	TDSK_AUDIO_LATENCY	Время (в миллисекундах) длительности джиттер-буфера, отслеживающего неравномерность поступления сетевых пакетов, задерживающего и накапливающего их для плавности воспроизведения аудио-материала без прерываний и рывков. Параметр доступен с версии ПО Termidesk Viewer 6.1. Возможные значения: • 0 - задержка не используется; • 1 - 10 000. Рекомендуемое значение: 100 - 250. Особенности: • значение до 400 применяется для нестабильного подключения или далеко расположенных участников подключения; • при появлении помех в воспроизведении аудио-материала (щелчков, треска) джиттер-буфер можно увеличить на 100 мс. Следует помнить, что большое увеличение параметра не рекомендуется, т.к.может появиться дискомфорт при прослушивании голоса в аудиоконференциях	100
Не задан	TERA_UDP_FAILURE_TIMEOUT	Время ожидания (в миллисекундах) для повторных попыток взаимодействия с TERA-сервером по UDP-каналу. Время ожидания всегда постоянно. Если значение не задано, то используется значение по умолчанию (15 секунд). Значение не может быть меньше 10 000	15 000
Не задан	TERA_UDP_QUALITY_TIMEOUT	Время ожидания (в миллисекундах) повторного переключения в UDP-канал. Время ожидания адаптивно: каждая следующая неудачная попытка увеличивает интервал ожидания следующего подключения, но не более 5 раз. Таким образом при настройке по умолчанию следующие попытки произойдут: через 1.5 минут, 3 минуты, 4.5 минуты, 6 минут, 7.5 минут. Если в интервале не менее 5 секунд ошибок не будет обнаружено, то время ожидания сбросится к начальному значению. Если значение не задано, то используется значение по умолчанию (90 секунд). Значение не может быть меньше 10 000	90 000

КЛИЕНТ. ВОЗМОЖНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ПО TERMIDESK VIEWER

Интерфейс ПО Termidesk Viewer

Интерфейс ПО Termidesk Viewer в оконном режиме

В процессе доставки РМ в меню дополнительных действий доступны информационные элементы ПО Termidesk Viewer со следующими возможностями (см. рисунок Информационные элементы ПО Termidesk Viewer):

Настройка доступа к функциональным возможностям задается администратором в политиках фонда РМ.

- элемент (1):
  - перемещает панель инструментов при его удержании левой кнопкой мыши;
  - скрывает или отображает панель инструментов при нажатии на него левой кнопкой мыши;
- элемент «Закрепить» (2):
  - при нажатии на элемент панель инструментов закрепляется в заданном положении без возможности перемещения и сворачивания. Повторное нажатие отключает закрепление панели инструментов;
- элемент «Сведения» (3) позволяет:
  - просмотреть идентификатор РМ на платформе виртуализации;
  - просмотреть статистику сеанса;
  - просмотреть состояние каналов протокола доставки;
  - перейти по URL-адресу технической поддержки;
- элемент «Устройства» (4) управляет:
  - перенаправлением USB-устройств, подключенных к рабочей станции, в РМ;
  - перенаправлением веб-камер, подключенных к рабочей станции, в РМ;
  - перенаправлением микрофонов, подключенных к рабочей станции, в РМ. Параметр доступен только при подключении к РМ по протоколу SPICE или TERA;
  - перенаправлением принтеров, подключенных к рабочей станции, в РМ;
  - перенаправлением смарт-карт, подключенных к рабочей станции, в РМ;
- элемент «Передача данных» (5) позволяет:
  - передавать файлы в РМ или из РМ;
  - перенаправлять каталоги с пользовательской рабочей станции в РМ;
  - управлять буфером обмена;
- элемент «Клавиатура» (6) управляет:
  - отображением экранной клавиатуры РМ;
  - отображением списка горячих клавиш и их передачей в РМ;
  - передачей в РМ сочетания клавиш **<Ctrl>** + **<Alt>** +**<Delete>**;
- элемент «Настройки» (7) позволяет:
  - управлять мониторами в окне «Мониторы»;
  - управлять сглаженным режимом отображения экрана РМ. При активации параметра экран РМ отображается в сглаженном режиме. Для отображения экрана РМ без сглаживания параметр нужно отключить;
  - управлять компактным режимом отображения панели инструментов. При активации параметра графические элементы панели инструментов отображаются без подписей. Для отображения графических элементов с подписями параметр нужно отключить;
  - создавать снимок экрана РМ;
- элемент «Свернуть» (8):
  - сворачивает окно просмотра;
- элемент «Полный экран» (9):

- отображает окно просмотра в полноэкранном режиме;
- элемент «Отключить» (10):
  - отключает сеанс пользователя.

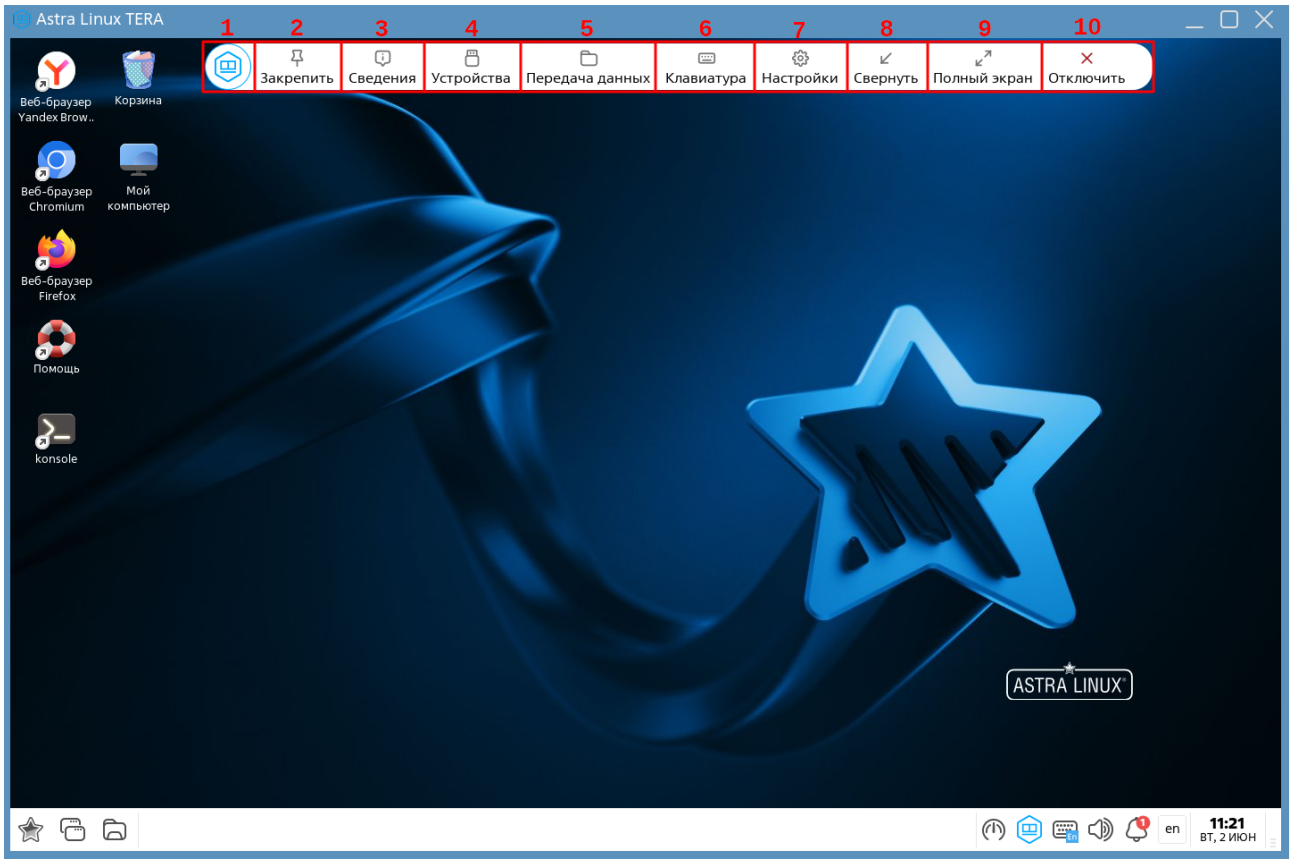


Рисунок 198. Информационные элементы ПО Termidesk Viewer

Интерфейс ПО Termidesk Viewer в полноэкранном режиме

При работе с РМ пользователь может управлять отображением окна ПО Termidesk Viewer (см. рисунок Отображение панели инструментов в полноэкранном режиме):

- переводить окно в полноэкранный режим одним из способов:
  - нажать графический элемент «Полный экран» (9);
  - нажать клавишу **<F11>**;
- сворачивать окно:
  - нажать графический элемент «Свернуть» (8);
- выходить из полноэкранного режима одним из способов:
  - нажать графический элемент «Оконный режим» (9);
  - нажать сочетание клавиш **<Ctrl>** + **<Alt>** + **<Enter>**.

Режим работы в полноэкранном режиме настраивается администратором с помощью политики «Полноэкранный режим (SPICE, TERA)».

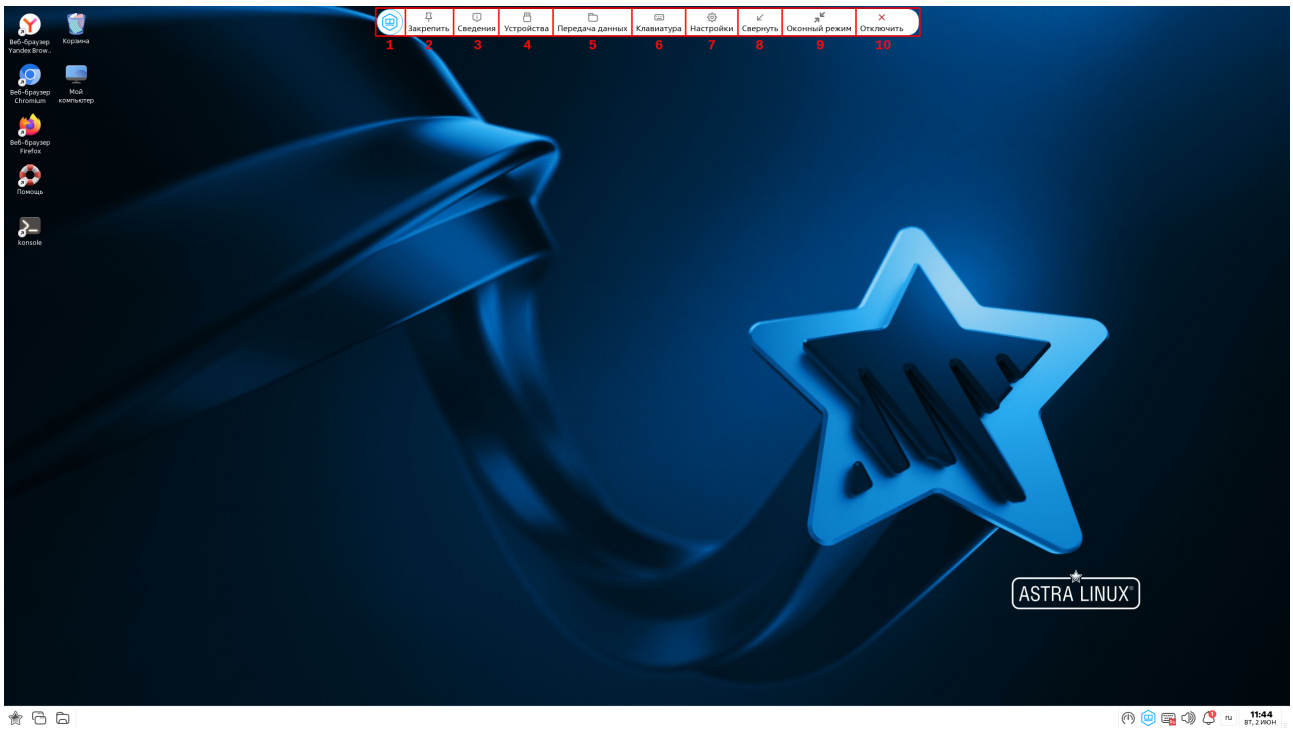


Рисунок 199. Отображение панели инструментов в полноэкранном режиме

Действия в ПО Termidesk Viewer

Переход по URL-адресу технической поддержки

Для перехода по URL-адресу технической поддержки в интерфейсе ПО Termidesk Viewer нужно раскрыть элемент «Сведения», выбрать строку «Поддержка» и дождаться отображения URL-адреса во встроенном в ОС веб-браузере. URL-адрес задается администратором в настройках фонда РМ в «Портале администратора».

Перенаправление USB-устройств в интерфейсе ПО Termidesk Viewer

Для перенаправления подключенного к пользовательской рабочей станции USB-устройства в РМ нужно:

- в интерфейсе ПО Termidesk Viewer раскрыть элемент «Устройства» и выбрать пункт «USB-устройства»;
- выбрать устройство для перенаправления, отметив его галочкой (см. рисунок Окно выбора USB-устройства);
- опционально отметить галочкой параметр «Автоподключение». При этом все устройства, соответствующие классам Image и CDC Data и физически переподключаемые к пользовательской рабочей станции, будут автоматически перенаправлены в РМ;
- нажать кнопку **[Выбор]** для применения настроек.

При перенаправлении USB-устройств по протоколу RDP ПО Termidesk Viewer отобразит запрос: «Для применения изменений необходимо выполнить переподключение». Для подтверждения перенаправления устройств следует нажать экранную кнопку **[Переподключиться]**.

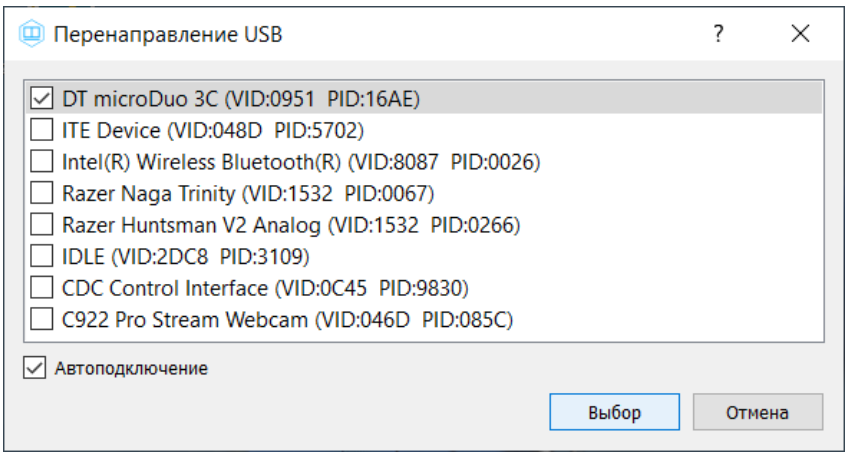


Рисунок 200. Окно выбора USB-устройства

Перенаправление смарт-карт в интерфейсе ПО Termidesk Viewer

Для перенаправления подключенной к пользовательской рабочей станции смарт-карты в РМ нужно:

- в интерфейсе ПО Termidesk Viewer раскрыть элемент «Устройства» и выбрать пункт «Смарткарты»;
- в открывшемся окне настроек выбрать нужную смарт-карту, отметив ее галочкой.

При подключении по протоколу RDP выбор конкретной смарт-карты и пункт меню может быть недоступен: для этого протокола по умолчанию перенаправляются все доступные смарт-карты.

Если при подключении к серверу была пройдена аутентификация по смарт-карте, то она автоматически перенаправится в ВРМ, если администратором включена политика «Перенаправление смарт-карт (RDP, SPICE, TERA)».

Перенаправление принтеров в интерфейсе ПО Termidesk Viewer

Для перенаправления подключенного к пользовательской рабочей станции принтера в РМ нужно:

- в интерфейсе ПО Termidesk Viewer раскрыть элемент «Устройства» и выбрать пункт «Перенаправление принтеров»;

Настройки по перенаправлению принтеров в гостевую ОС РМ выполняются администратором при подготовке РМ.

При подключении по протоколу RDP выбор конкретного принтера и пункт меню может быть недоступен: для этого протокола по умолчанию перенаправляются все доступные принтеры.

- выбрать устройство для перенаправления, отметив его галочкой (см. рисунок Пример доступного списка принтеров при подключении из ОС Windows). Список принтеров будет отличаться в зависимости от настроек и типа ОС, с которой происходит подключение;
- нажать экранную кнопку **[Выбор]** для применения настроек.

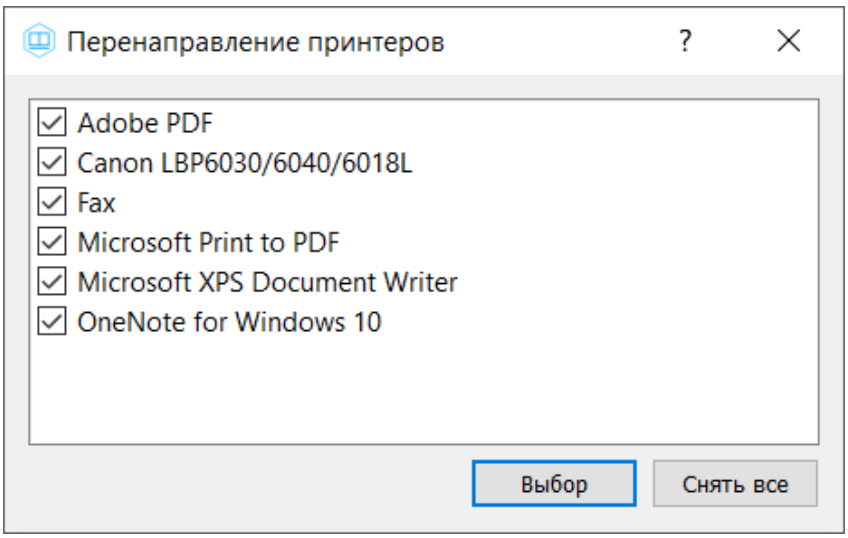


Рисунок 201. Пример доступного списка принтеров при подключении из ОС Windows

Перенаправление веб-камеры в интерфейсе ПО Termidesk Viewer

Для перенаправления подключенной к пользовательской рабочей станции веб-камеры в РМ нужно:

- в интерфейсе ПО Termidesk Viewer раскрыть элемент «Устройства» и выбрать пункт «Вебкамера»;

> На момент запуска Клиента веб-камера не должна использоваться другим устройством, иначе ее нельзя будет перенаправить.
>
> Передача изображения с веб-камеры происходит с момента активации перенаправления до его деактивации или до завершения подключения с РМ (закрытия ПО Termidesk Viewer).
>
> Если во время работы веб-камеры пользователем будет перезагружен компонент Termidesk VDI «Видеоагент» в РМ, то потребуется закрыть приложение, использующее веб-камеру в гостевой ОС.

- в открывшемся окне «Менеджер вебкамер»(см. рисунок Окно «Менеджер вебкамер») выбрать веб-камеру в поле «Устройство» и разрешение в поле «Разрешение/частота кадров». В окне должно отобразиться изображение с веб-камеры. Изменение изображения в зависимости от выбранного разрешения и частоты происходит в режиме реального времени;
- нажать экранную кнопку **[OK]**.

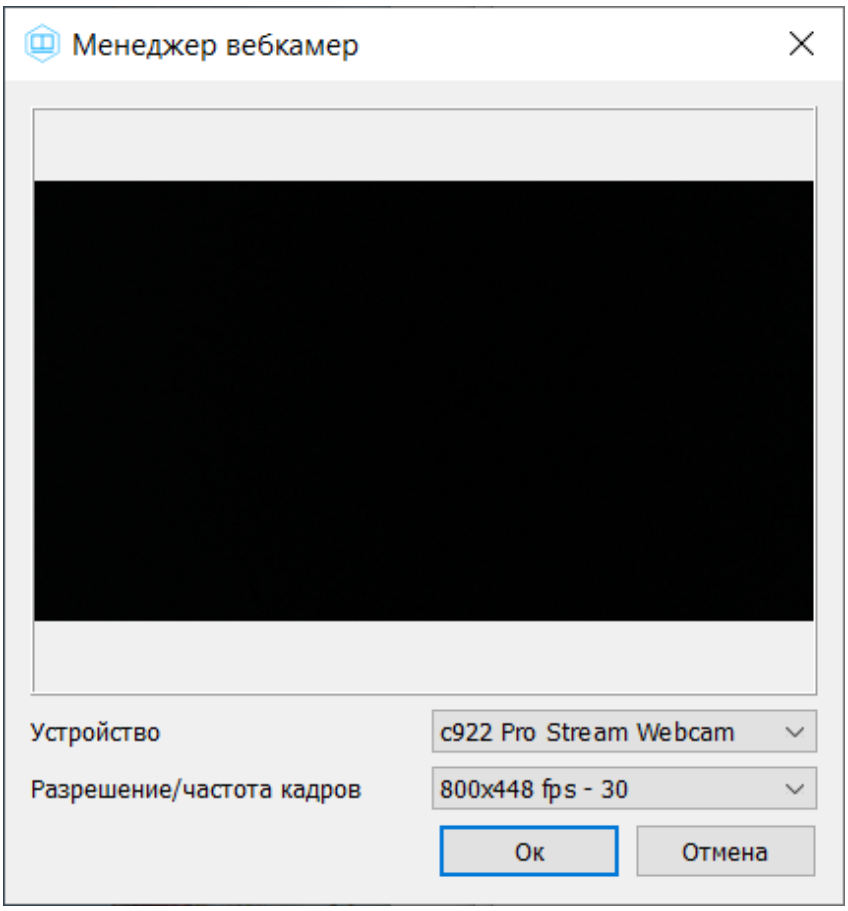


Рисунок 202. Окно «Менеджер вебкамер»

Особенности функционирования на ОС MacOS:

- при первом запуске ПО Termidesk Viewer и выборе пункта «Вебкамера» отобразится предупреждение, пример: «Приложение запрашивает доступ к камере». В этом случае нужно:
  - для разрешения доступа нажать экранную кнопку **[OK]**;
  - для запрета доступа нажать экранную кнопку **[Не разрешать]**. В этом случае окно «Менеджер вебкамер» отобразится, но предварительный просмотр изображения будет пуст, экранная кнопка **[Ок]** заблокируется. Веб-камера использоваться не будет. Для изменения доступа нужно перейти «Системные настройки - Конфиденциальность и безопасность - Камера» и активировать разрешение для приложения «Termidesk Client».

Выбор монитора в интерфейсе ПО Termidesk Viewer

В ПО Termidesk Viewer реализована возможность вывода изображения дисплея РМ на одном или нескольких мониторах с возможностью настройки их сопоставления. Выполненные настройки сохраняются после переподключения к РМ.

Если выполненная конфигурация не является корректной (например, один из двух мониторов был отключен), то при запуске РМ ПО Termidesk Viewer выведет окно настройки мониторов.

Особенности использования монитора:

- при подключении по протоколу RDP ПО Termidesk Viewer поддерживает настройку расположения и организации мониторов, исходя из системных настроек ОС пользовательской рабочей станции. При этом:

  - поддерживается ориентация экрана и масштаб каждого монитора;
  - не поддерживается сохранение настроек мониторов. После повторного подключения потребуется задать настройки сопоставления мониторов снова;
- поддерживаются экраны с высоким разрешением (HiDPI). При этом:
  - масштаб экрана монитора передается при подключении к РМ по протоколу RDP;
  - HiDPI применяется при подключении к терминальному серверу MS RDSH;
- поддерживается режим отображения RAIL;
- для одномониторной конфигурации поддерживается возможность перетаскивания окна ПО Termidesk Viewer на любой монитор и использование его в полноэкранном режиме на любом из мониторов;
- для многомониторной конфигурации:
  - соблюдается позиционирование окон ПО Termidesk Viewer с физическими мониторами при переходе в полноэкранный режим согласно настройкам пункта «Мониторы» (текущее соответствие мониторов);
  - протокол RDP: список доступных мониторов определяется количеством физически подключенных к пользовательской рабочей станции мониторов в момент запуска ПО Termidesk Viewer;
  - при использовании полноэкранного режима экран РМ будет отображен на мониторе, настроенном в окне «Мониторы», игнорируя текущее расположение окна ПО Termidesk Viewer.

Для выбора монитора, отображающего дисплей РМ, нужно:

- в интерфейсе ПО Termidesk Viewer раскрыть элемент «Настройки» и выбрать пункт «Мониторы»;

> Дисплей РМ представляет абстрактную сущность, рассматриваемую как графический буфер, куда записываются произошедшие в РМ изменения.
>
> Пункт «Мониторы» может быть доступен или недоступен для выбора в зависимости от значения политики «Многомониторный режим (RDP, SPICE, TERA)», настроенного администратором в «Портале администратора». Доступность работы в многомониторном режиме также зависит от значения указанной политики.

- в открывшемся окне настроек (см. рисунок Окно выбора монитора) выбрать монитор, отметив его галочкой. Если в окне выбора имеется более одного монитора, то вывод дисплея РМ возможен в отдельном окне или на физическом мониторе;
- нажать экранную кнопку **[Обновить]** для применения настроек.

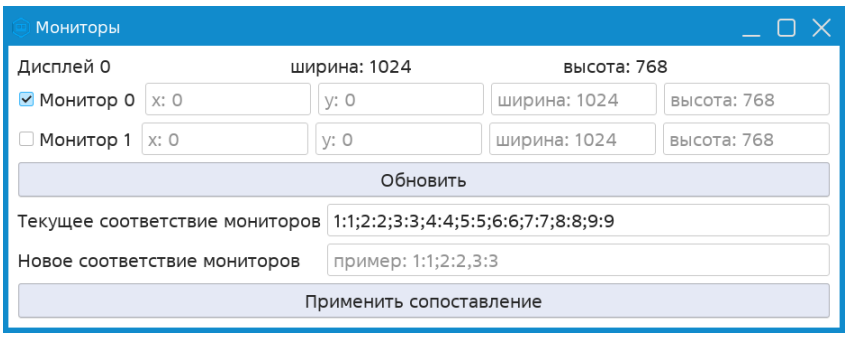


Рисунок 203. Окно выбора монитора

Одному дисплею может соответствовать несколько мониторов (зависит от конфигурации РМ). Определенная область графического буфера дисплея РМ задается и отображается для каждого монитора:

- «x» - смещение области дисплея по горизонтальной оси в пикселях;
- «y» - смещение области дисплея по вертикальной оси в пикселях;
- «ширина» - размер дисплея по ширине в пикселях;
- «высота» - размер дисплея по высоте в пикселях.

При настройке областей дисплея следует избегать их пересечения (монитор 0: [0, 0, 1024, 720]; монитор 1: [5, 10, 1920, 1080]) и отступов между ними (монитор 0: [0, 0, 1024, 720]; монитор 1: [1030, 0, 1920, 1080]).

При подключении по протоколу RDP в РМ с гостевой ОС Microsoft Windows доступен дополнительный параметр «Основной» в настройках монитора. Однако менять значения, определенные автоматически, не рекомендуется: смена основного монитора должна выполняться в ОС пользовательской рабочей станции.

При работе с несколькими мониторами рекомендуется использовать следующие конфигурации:

- несколько дисплеев с одним монитором (РМ с ОС Microsoft Windows);
- один дисплей с несколькими мониторами (РМ с ОС Linux).

Исходя из особенностей индексации и идентификации мониторов в протоколе SPICE использование других конфигураций не рекомендуется.

Для двухмониторной конфигурации нужно отметить в настройке оба дисплея и нажать экранную кнопку **[Обновить]**.

ПО Termidesk Viewer также поддерживает динамически формируемый и изменяемый массив [N:M] сопоставления виртуальных экранов к физическим мониторам хоста. Начальные значения массива [1:1;2:2;3:3;4:4;5:5;6:6;7:7;8:8;9:9], порядковые номера всех физических и виртуальных мониторов в массиве начинаются с 1.

Сопоставление мониторов должно быть [1:1;2:2;3:3;4:4] и т.д. Изменение, например, [2:1;1:2] при разном разрешении мониторов и масштабов может привести к непредсказуемым результатам.

Для изменения соответствия мониторов необходимо:

- в интерфейсе ПО Termidesk Viewer раскрыть элемент «Настройки» и выбрать в раскрывшемся списке пункт «Мониторы»;
- в открывшемся окне ввести новые значения для соответствия мониторов в поле «Новое соответствие мониторов»;
- нажать экранную кнопку **[Применить сопоставление]** для применения настроек.

Передача файлов и буфер обмена

Для передачи файлов нужно:

- если передача файлов выполняется из пользовательской рабочей станции в РМ:

Для этого направления передачи также поддерживается копирование и передача файлов через функцию Drag-and-drop.

- выполнить копирование файла (например, комбинацией клавиш **<Ctrl>** + **<C>**);

- раскрыть элемент «Передача данных» и выбрать строку «Передача файлов в сессию»;
- выбрать путь для сохранения файла;

- если передача файлов выполняется из РМ на пользовательскую рабочую станцию:

> Это направление передачи поддерживается только для протокола RDP. В зависимости от размера файлов копирование может занимать продолжительное время.
>
> Комбинация клавиш **<Ctrl>** + **<V>** для вставки файла из буфера обмена не применима.

- выполнить копирование файла (например, комбинацией клавиш **<Ctrl>** + **<C>**);
- раскрыть элемент «Передача данных» и выбрать строку «Передача файлов из сессии»;
- выбрать путь для сохранения файла.

Для активации буфера обмена между пользовательской рабочей станцией и РМ нужно раскрыть элемент «Передача данных» и выбрать строку «Буфер обмена».

Перенаправление каталога в интерфейсе ПО Termidesk Viewer

Для перенаправления каталога с пользовательской рабочей станции в РМ в графическом интерфейсе ПО Termidesk Viewer нужно раскрыть элемент «Передача данных» и выбрать строку «Перенаправление папки» и после этого выбрать каталог, который необходимо перенаправить.

Поддерживаемые варианты перенаправлений приведены в подразделе **Перенаправление каталогов**.

Содержимое выбранного каталога будет отображено:

- для ОС Astra Linux Special Edition (см. рисунок Перенаправленный каталог в ОС Astra Linux Special Edition):
  - при подключении по протоколу TERA: в директории `~/davfs/<имя_перенаправляемого_каталога>`;
  - при подключении по протоколу SPICE: в директории `/media/davfs` ;
  - при подключении к «Серверу терминалов Astra Linux»: по умолчанию в директории `${HOME}/Public` или в директории `/run/user/<идентификатор_пользователя>/stal/<наименование_диска>` (если выполнена настройка компонента);

> Директория может быть переопределена администратором при настройке гостевой ОС (базового РМ).
>
> Возможность перенаправления каталога настраивается в «Портале администратора» с помощью политики «Перенаправление дисков и папок (RDP, SPICE, TERA)». Если перенаправление каталога запрещено, то строка «Перенаправление папки» будет недоступна для выбора.

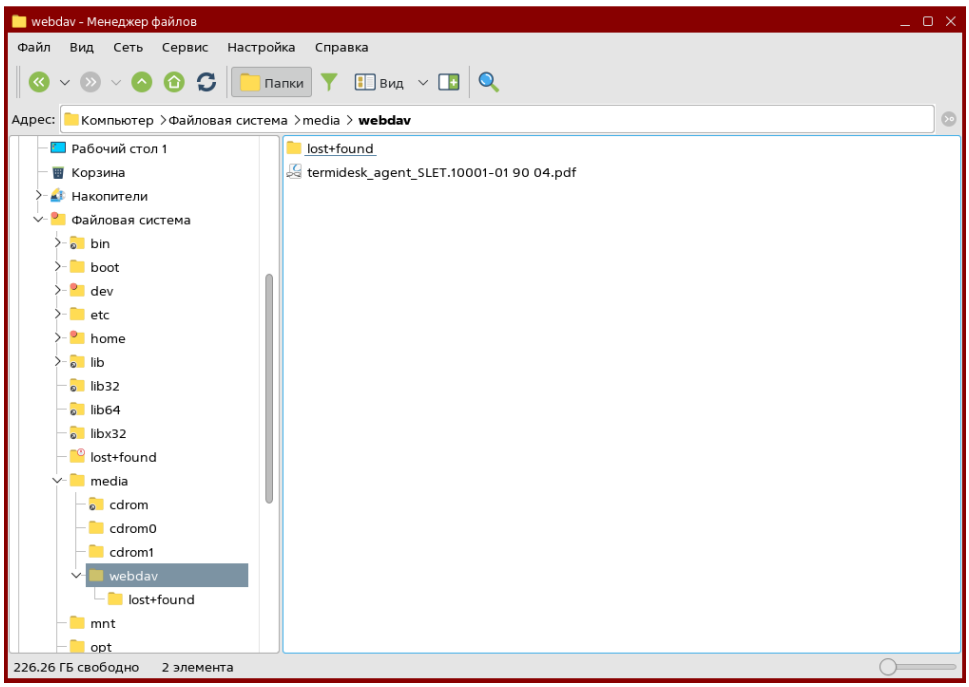


Рисунок 204. Перенаправленный каталог в ОС Astra Linux Special Edition

- в ОС Microsoft Windows (см. рисунок Перенаправленный каталог в ОС Microsoft Windows): в области навигации проводника. В случае, если каталог не появился в области навигации проводника ОС Windows, следует перейти в интерфейс командной строки («Пуск» - «Служебные - Windows» - «Командная строка») и выполнить команду подключения сетевого диска:

```
net use Z: http://localhost:9843
```

При переходе «Этот компьютер - Перенаправленные диски и папки» каталог может не отобразиться сразу, поэтому следует открывать перенаправленный каталог через меню навигации проводника Windows.

При завершении сессии пользователя или отключении ПО Termidesk Viewer сетевой диск будет отключен.

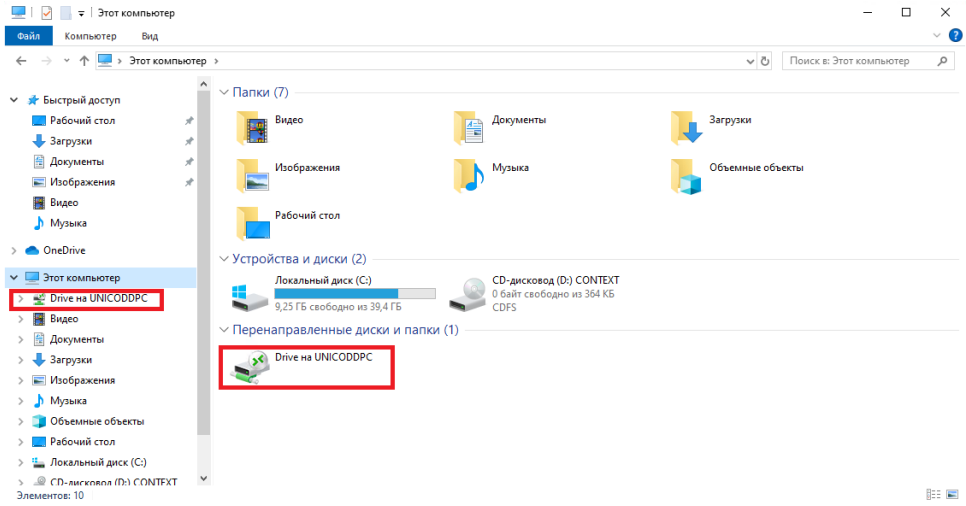


Рисунок 205. Перенаправленный каталог в ОС Microsoft Windows

Для протокола SPICE не поддерживается отключение перенаправления каталогов: можно выбрать другой каталог, но полное отключение

ограничивается возможностями протокола.

Снимок экрана в интерфейсе ПО Termidesk Viewer

Для выполнения снимка экрана в интерфейсе ПО Termidesk Viewer нужно раскрыть элемент «Настройки» и выбрать строку «Сделать снимок экрана», затем указать путь для сохранения файла.

Первоначально имя файла формируется на основе шаблона: `Termidesk_Viewer_ГГГГ-ММ-ДД-ЧЧ-ММ-СС.png`.

Вызов виртуальной клавиатуры РМ

Вызов виртуальной клавиатуры РМ отображает виртуальную клавиатуру в гостевой ОС. Это актуально для случаев, когда ОС не реагирует на передачу данных с физической клавиатуры пользовательской рабочей станции.

Для отображения виртуальной клавиатуры РМ нужно раскрыть элемент «Клавиатура» и выбрать пункт «Экранная клавиатура».

Для корректной работы вызова виртуальной клавиатуры РМ администратор должен предварительно настроить гостевую ОС РМ.

Перенаправление клавиш и комбинаций клавиш в интерфейсе ПО Termidesk Viewer

ПО Termidesk Viewer поддерживает перенаправление как одиночных клавиш, так и комбинаций клавиш с физической клавиатуры пользовательской рабочей станции в гостевую ОС РМ.

При подключении к РМ по протоколу TERA поведение клавиш **<Power>** и **<Sleep>** соответствует следующему:

- при нажатии клавиш **<Power>** или **<Sleep>** команда перенаправляется в РМ;
- РМ немедленно выключается (выполняется корректное завершение работы гостевой ОС).

Перенаправление комбинаций клавиш поддерживается как при их нажатии, так и из интерфейса ПО Termidesk Viewer, при выборе в графическом интерфейсе нужного сочетания.

Список поддерживаемых комбинаций:

- **<Ctrl>** + **<Alt>** + **<Delete>**;
- **<Ctrl>** + **<Alt>** + **<Backspace>**;
- **<Ctrl>** + **<Alt>** + **<F1>**;
- **<Ctrl>** + **<Alt>** + **<F2>**;
- **<Ctrl>** + **<Alt>** + **<F3>**;
- **<Ctrl>** + **<Alt>** + **<F4>**;
- **<Ctrl>** + **<Alt>** + **<F5>**;
- **<Ctrl>** + **<Alt>** + **<F6>**;
- **<Ctrl>** + **<Alt>** + **<F7>**;

- **<Ctrl>** + **<Alt>** + **<F8>**;
- **<Ctrl>** + **<Alt>** + **<F9>**;
- **<Ctrl>** + **<Alt>** + **<F10>**;
- **<Ctrl>** + **<Alt>** + **<F11>**;
- **<Ctrl>** + **<Alt>** + **<F12>**;
- **<Print Screen>**;
- **<Ctrl>** + **<F1>**;
- **<Ctrl>** + **<?>**;
- **<Shift>** + **<F11>**.

Перенаправление клавиатурных модификаторов

Клавиатурный модификатор - клавиша на клавиатуре, которая меняет поведение других клавиш. Пример: клавиши **<Ctrl>**, **<Alt>**, **<Shift>**, **<Caps>**, **<Num Lock>** и др.

Для ОС macOS по умолчанию действие клавиши **<Cmd>** соответствует **<Ctrl>**. Изменение назначения клавиши выполняется в конфигурационном файле `Termidesk Viewer.ini`.

ПО Termidesk Viewer поддерживает функционал перенаправления клавиатурных модификаторов в гостевую ОС (и из гостевой ОС).

При этом для протокола TERA функционал работает следующим образом:

- приоритетом является изменение клавиатурных модификаторов на пользовательской рабочей станции;
- при каждом следующем открытии окна ПО Termidesk Viewer в гостевую ОС передаются изменения клавиатурных модификаторов, произошедшие за время отсутствия активности (фокусировки) у окна ПО Termidesk Viewer;
- если окно ПО Termidesk Viewer было неактивным, но на пользовательской рабочей станции произошли изменения клавиатурных модификаторов, то при появлении активности в окне ПО Termidesk Viewer применятся настройки пользовательской рабочей станции;
- если в гостевой ОС происходят изменения клавиатурных модификаторов в то время, как ПО Termidesk Viewer остается активным, то они будут применены к пользовательской рабочей станции (с соответствующей индикацией на подключенной клавиатуре).

Перенаправление раскладки клавиатуры

Раскладка клавиатуры определяет используемый язык ввода при нажатии клавиш. Для переключения раскладки клавиатуры используются заданные пользователем гостевой ОС сочетания клавиш, например **<Alt>** + **<Shift>** или **<Win>** + **<Пробел>**. В зависимости от настроек гостевой ОС сочетание клавиш может отличаться.

ПО Termidesk Viewer поддерживает функционал перенаправления раскладки клавиатуры в гостевую ОС (и из гостевой ОС).

Для корректного перенаправления раскладки клавиатуры требуется настройка одинаковых раскладок на пользовательской рабочей станции и ВРМ. Если на пользовательской рабочей станции или ВРМ настроены различные раскладки, то переключение между неизвестными раскладками производиться не будет.

При этом для протокола TERA функционал работает следующим образом:

- приоритетом является изменение раскладки клавиатуры на пользовательской рабочей станции;
- при каждом следующем открытии окна ПО Termidesk Viewer в гостевую ОС передаются изменения раскладки клавиатуры, произошедшие за время отсутствия активности (фокусировки) у окна ПО Termidesk Viewer;
- если окно ПО Termidesk Viewer было неактивным, но на пользовательской рабочей станции была изменена раскладка клавиатуры, то при появлении активности в окне ПО Termidesk Viewer применятся настройки пользовательской рабочей станции;
- если в гостевой ОС происходят изменения раскладки клавиатуры в то время, как ПО Termidesk Viewer остается активным, то они будут применены к пользовательской рабочей станции (с соответствующей индикацией текущего языка ввода на языковой панели).

Получение статистики и проверка состояния каналов

Для получения статистики сеанса в интерфейсе ПО Termidesk Viewer нужно раскрыть элемент «Сведения» и выбрать строку «Статистика сеанса». Статистика отображает данные подключений по каналам SPICE и TERA.

Пункт недоступен при подключении по протоколу RDP с включенным параметром «Соединение по RDP через Termidesk Viewer».

Для проверки состояния каналов в интерфейсе ПО Termidesk Viewer нужно раскрыть элемент «Сведения» и выбрать строку «Состояние каналов». Каналы, которые в данный момент не используются, будут отображены как «ВЫКЛ».

На экране входа в ОС при подключении по протоколу TERA будет отображено ограниченное количество каналов, если:

- вход в сессию не был сделан;
- или администратором не активирована политика «Автоматический вход в систему при подключении к РМ (RDP, SPICE, TERA)».

Завершение работы в ПО Termidesk Viewer

Для завершения работы с РМ в интерфейсе ПО Termidesk Viewer нужно выбрать элемент «Отключить».

КЛИЕНТ. ПЕРЕНАПРАВЛЕНИЕ РЕСУРСОВ

Перенаправление USB-устройств

Общие сведения по перенаправлению USB-устройств

В текущей версии Termidesk VDI возможные сценарии перенаправления USB-устройств из пользовательской рабочей станции приведены в таблице (см. таблицу Возможные сценарии перенаправления USB-устройств из пользовательской рабочей станции).

Существующие ограничения:

- одновременное перенаправление устройств с одинаковыми значениями «Product ID» и «Vendor ID» не поддерживается;
- для протоколов SPICE и TERA: максимальное количество перенаправляемых устройств ограничено количеством каналов протокола доставки.

Начиная с Termidesk VDI версии 7.0 список USB-устройств, перенаправляемых через ПО

Termidesk Viewer, сохраняется автоматически. Срок хранения списка составляет 30 дней. Если устройство ни разу не было перенаправлено за это время, то сохраненные данные о его перенаправлении удаляются. При каждом перенаправлении устройства обновляется информация о сохранении его настроек перенаправления.

В таблице приняты обозначения:

- «MS RDSH» - терминальный сервер MS RDSH.

Администратор должен включить соответствующие политики фонда РМ для работы перенаправления.

Сценарии актуальны при подключении к РМ непосредственно из Клиента.

Начиная с Termidesk VDI версии 6.1 функционал подключения по протоколу RDP с использованием ПО Termidesk Viewer выведен из экспериментального режима и является основным вариантом подключения. Сценарии с использованием системных программ не гарантируются.

Таблица 319. Возможные сценарии перенаправления USB-устройств из пользовательской рабочей станции

Комбинации ОС	SPICE	RDP (termidesk-viewer)	TERA
Astra Linux Special Edition → Astra Linux Special Edition	□		□
Astra Linux Special Edition → Microsoft Windows	□	□[1]	
Astra Linux Special Edition → MS RDSH		□[1]	
Microsoft Windows → Astra Linux Special Edition	□		□
Microsoft Windows → Microsoft Windows	□	□	
Microsoft Windows → MS RDSH		□	
Microsoft Windows → РЕД ОС	□		
РЕД ОС → РЕД ОС	□		
РЕД ОС → Microsoft Windows	□		
Альт Рабочая станция → Microsoft Windows	□		
Альт Рабочая станция → Astra Linux Special Edition	□		

Примечание:

[1] - перенаправление работает только при запуске ПО Termidesk Viewer через пользователя `root`.

Для возможности перенаправления USB-устройств по протоколу RDP от имени обычного пользователя на пользовательской рабочей станции с ОС Astra Linux Special Edition нужно:

После настройки запуска ПО Termidesk Viewer от имени обычного пользователя его запуск от имени привилегированного пользователя не допускается.

Запуск ПО Termidesk Viewer от имени привилегированного пользователя приведет к созданию файлов, недоступных обычному пользователю. Это может привести к некорректной работе ПО Termidesk Viewer при его запуске от имени обычного пользователя.

В ОС Astra Linux Special Edition настройка прав доступа выполняется:

- с помощью файлов в формате `.pkla` для версии 1.7;
- с помощью файлов в формате `.rules` для версии 1.8.

- создать правило `99-usbaccess.rules` в каталоге `/etc/udev/rules.d/`;
- отредактировать правило `/etc/udev/rules.d/99-usbaccess.rules`, приведя его к виду:

```
SUBSYSTEM=="usb", MODE="0664", GROUP="astra"
```

где:

`GROUP="astra"` - группа пользователя, которому нужно предоставить доступ к перенаправлению USB-устройств;

- применить правило перенаправления USB-устройств:

```
sudo udevadm control --reload-rules
sudo udevadm trigger
```

- после применения правила нужно перезапустить пользовательскую рабочую станцию.

Перенаправление USB-гарнитуры

Общие сведения по перенаправлению USB-гарнитуры

Возможные сценарии перенаправления USB-гарнитуры из пользовательской рабочей станции в РМ приведены в таблице (см. таблицу Возможные сценарии перенаправления USB-гарнитуры из пользовательской рабочей станции).

Если при подключении из ОС MacOS к РМ микрофон будет использоваться ПО Termidesk Viewer, то пользователю будет отображено соответствующее предупреждение (см. рисунок Запрос доступа к микрофону), пример: «Приложение «Termidesk Client» запрашивает доступ к микрофону». В этом случае нужно:

- для разрешения доступа нажать экранную кнопку **[OK]**;
- для запрета доступа нажать экранную кнопку **[Не разрешать]**. В этом случае микрофон использоваться не будет. Для изменения доступа нужно перейти «Системные настройки - Конфиденциальность и безопасность - Микрофон» и активировать разрешение для приложения vdi-viewer.

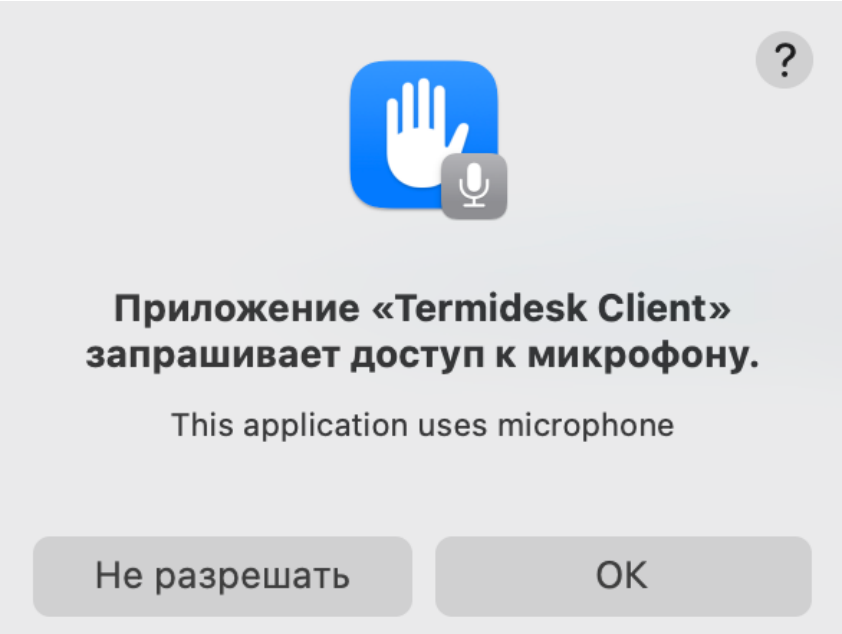


Рисунок 206. Запрос доступа к микрофону

В таблице приняты обозначения:

- «MS RDSH» - терминальный сервер MS RDSH;
- «STAL» - терминальный сервер с установленным компонентом «Сервер терминалов Astra Linux».

Возможность перенаправления по протоколу RDP управляется администратором через политику фонда РМ «Перенаправление воспроизведения и записи звука (RDP)».

Сценарии актуальны при подключении к РМ непосредственно из Клиента.

Начиная с Termidesk VDI версии 6.1 функционал подключения по протоколу RDP с использованием ПО Termidesk Viewer выведен из экспериментального режима и является основным вариантом подключения. Сценарии с использованием системных программ не гарантируются.

Для протоколов RDP и TERA устройства воспроизведения и записи звука определяются на момент подключения к РМ и при их отключении или смене потребуется переподключиться к РМ.

Таблица 320. Возможные сценарии перенаправления USB-гарнитуры из пользовательской рабочей станции

Комбинации ОС	SPICE	RDP (termidesk-viewer)	TERA
Astra Linux Special Edition → Astra Linux Special Edition			□
Astra Linux Special Edition → Microsoft Windows			
Astra Linux Special Edition → MS RDSH		□[1]	
Astra Linux Special Edition → STAL		□	
Microsoft Windows → Astra Linux Special Edition			□
Microsoft Windows → Microsoft Windows		□	
Microsoft Windows → MS RDSH		□[1]	

Комбинации ОС	SPICE	RDP (termidesk-viewer)	TERA
Microsoft Windows → STAL		□	
MacOS → Astra Linux Special Edition			□
MacOS → Microsoft Windows			
MacOS → STAL		□	

Примечания:

[1] - на сервере MS RDSH пользователю нужно разрешить приложениям доступ к микрофону. Для этого перейти в ОС: «Параметры - Конфиденциальность - Разрешения приложений - Микрофон» и активировать параметр «Разрешить приложениям доступ к микрофону».

Перенаправление принтеров

Общие сведения по перенаправлению принтеров

В текущей версии Termidesk VDI возможные сценарии перенаправления принтеров из пользовательской рабочей станции приведены в таблице (см. таблицу Возможные сценарии перенаправления принтеров из пользовательской рабочей станции).

В таблице приняты обозначения:

- «MS RDSH» - терминальный сервер MS RDSH;
- «STAL» - терминальный сервер с установленным компонентом «Сервер терминалов Astra Linux».

Администратор должен включить политику фонда РМ «Перенаправление принтеров (RDP, SPICE, TERA)» для работы перенаправления.

Сценарии актуальны при подключении к РМ непосредственно из Клиента.

Начиная с Termidesk VDI версии 6.1 функционал подключения по протоколу RDP с использованием ПО Termidesk Viewer выведен из экспериментального режима и является основным вариантом подключения. Сценарии с использованием системных программ не гарантируются.

Таблица 321. Возможные сценарии перенаправления принтеров из пользовательской рабочей станции

Комбинации ОС	SPICE	RDP (termidesk-viewer)	TERA
Astra Linux Special Edition → Astra Linux Special Edition	□[2]		□[2]
Astra Linux Special Edition → Microsoft Windows		□	
Astra Linux Special Edition → MS RDSH		□	
Astra Linux Special Edition → STAL		□	
Microsoft Windows → Astra Linux Special Edition	□[2]		□
Microsoft Windows → Microsoft Windows		□	
Microsoft Windows → MS RDSH		□[3]	
Microsoft Windows → STAL		□[1]	
Microsoft Windows → РЕД ОС	□		
РЕД ОС → РЕД ОС	□		

Комбинации ОС	SPICE	RDP (termidesk-viewer)	TERA
РЕД ОС → Microsoft Windows	□		
Альт Рабочая станция → Microsoft Windows	□		
Альт Рабочая станция → Astra Linux Special Edition	□		

Примечания:

[1] - необходимо задать политике «Глубина цвета (RDP)» значение «32 бит» для работы подключения к STAL;

[2] - печать работает не из всех приложений;

[3] - при использовании терминального сервера MS RDSH администратору нужно разрешить перенаправление принтера в групповых политиках.

Принтеры перенаправляются автоматически. Однако в случае необходимости можно вручную настроить перенаправление принтеров в гостевую ОС РМ, для этого следует обратиться к подразделу **Настройки для перенаправления принтеров**.

Для корректной работы перенаправления принтеров администратор должен выполнить настройки:

- по перенаправлению принтеров в гостевую ОС РМ при подготовке базового РМ;
- по перенаправлению принтеров в STAL.

Настройки для перенаправления принтеров

Для перенаправления принтера должны быть выполнены условия:

- в ОС пользовательской рабочей станции должен быть добавлен нужный принтер. Поддерживается перенаправление программных принтеров (например, программный виртуальный принтер PDF/XPS);
- в гостевой ОС РМ должен быть установлен нативный драйвер используемого принтера. При перенаправлении принтера в РМ через ПО Termidesk Viewer будет использован соответствующий драйвер:
  - «generic raw» - если печать будет выполняться в STAL или BPM;
  - нативный драйвер - при использовании полного функционала принтера;
- при использовании терминального сервера MS RDSH нужно разрешить перенаправление принтера в групповых политиках. Для этого:
  - открыть редактор групповой политики;
  - перейти «Конфигурация компьютера - Административные шаблоны - Компоненты Windows - Службы удаленных рабочих столов - Узел сеансов удаленных рабочих столов - Перенаправление принтеров» («Computer Configuration - Administrative Templates - Windows Components - Remote Desktop Services - Remote Desktop Session Host - Printer Redirection» в английской локализации);
  - задать параметру «Не разрешать перенаправление для клиентского принтера» значение «Отключена» («Do not allow client printer redirection» значение «Disabled» в английской локализации).

По умолчанию добавление принтера в гостевую ОС РМ не требуется.

Ручное добавление принтера может быть выполнено одним из способов:

- через существующую в гостевой ОС оснастку (например, «Менеджер печати Fly» для

ОС Astra Linux Special Edition);

- через веб-интерфейс службы CUPS (для гостевой ОС Linux).

Для ручного добавления принтера через веб-интерфейс службы CUPS нужно:

- открыть в браузере URL-адрес: http://127.0.0.1:631/;
- перейти во вкладку «Администрирование». Выбрать пункт «Добавить принтер» и авторизоваться, использовав логин и пароль для входа в гостевую ОС;
- доступные принтеры будут отображены в списке «Найденные сетевые принтеры» (см. рисунок Список найденных сетевых принтеров). Выбрать принтер для добавления;

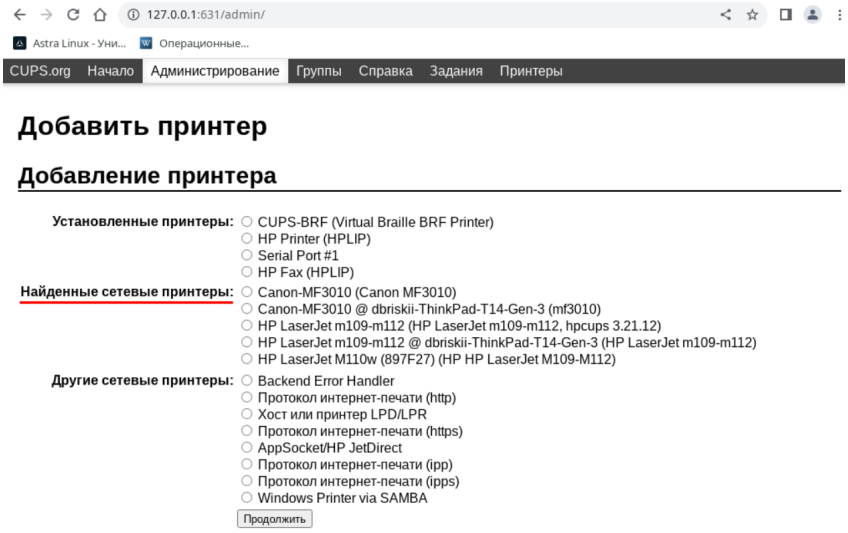


Рисунок 207. Список найденных сетевых принтеров

- убедиться, что в строке «Подключение» (см. рисунок Проверка URL) адрес начинается с «tdsk-prt»;

Настройка «tdsk-prt» актуальна при подключении по протоколу SPICE.

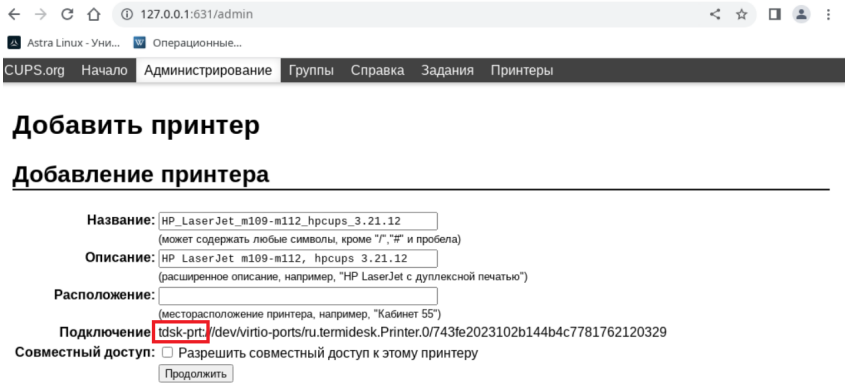


Рисунок 208. Проверка URL

- выбрать модель принтера из списка (см. рисунок Выбор модели принтера) или использовать файл драйвера принтера PPD;

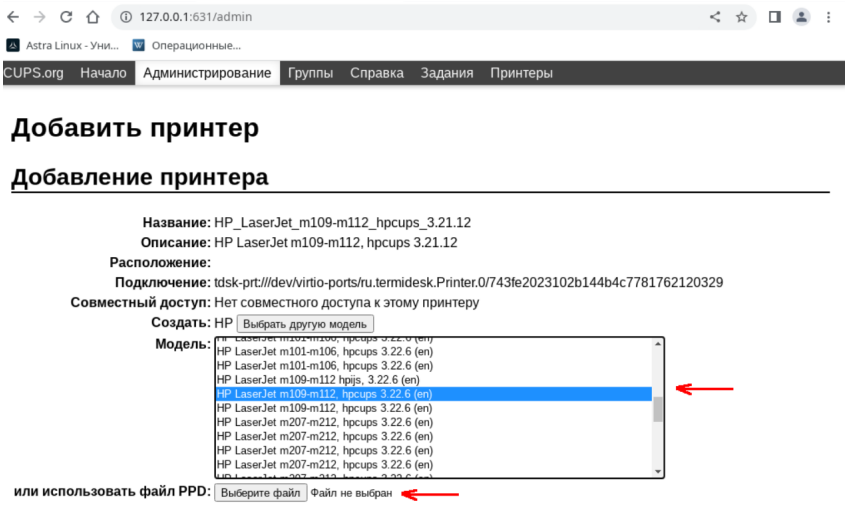


Рисунок 209. Выбор модели принтера

- завершить добавление принтера.

Если список «Найденные сетевые принтеры» пуст:

Настройка актуальна при подключении по протоколу SPICE.

- выбрать значение «Termidesk Virtual Printer» в списке «Другие сетевые принтеры» (см. рисунок Выбор другого сетевого принтера);

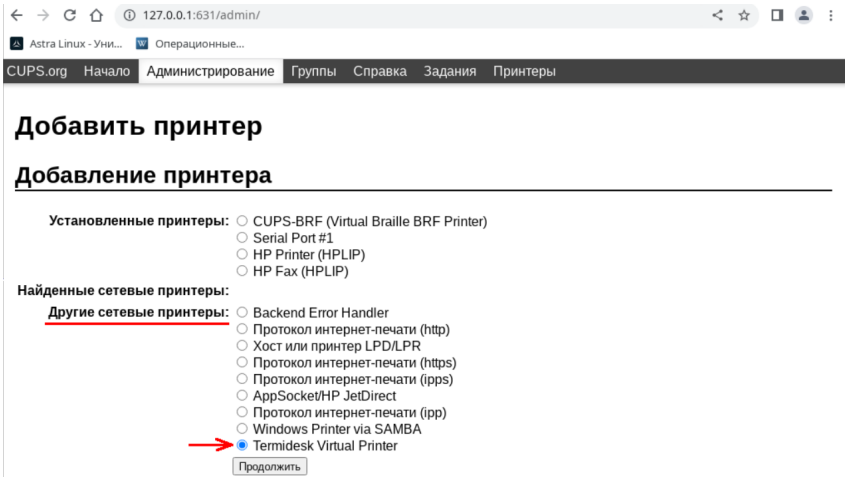


Рисунок 210. Выбор другого сетевого принтера

- перейти к интерфейсу командной строки (открыть программу «Терминал Fly») и выполнить:

```
cd /usr/lib/cups/backend
sudo ./tdsk-prt
```

- выбрать адрес нужного принтера и скопировать его в поле «Подключение» в браузере;

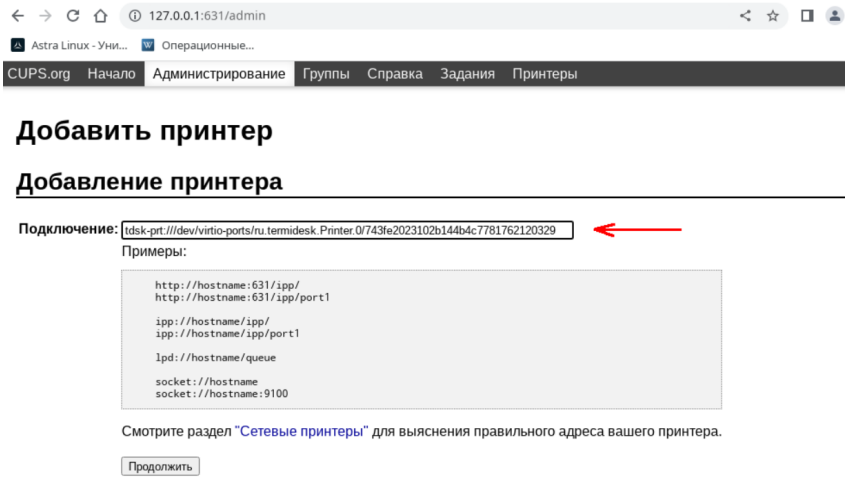


Рисунок 211. Добавление адреса принтера

- завершить добавление принтера аналогично описанию выше, когда список «Найденные сетевые принтеры» содержал записи.

Добавленный принтер должен отобразиться в менеджере печати (например, «Менеджер печати Fly») гостевой ОС.

При перенаправлении принтера из пользовательской рабочей станции на ОС Microsoft Windows в ВРМ на ОС Microsoft Windows доступны следующие конфигурации драйверов:

Настройка актуальна при подключении по протоколу RDP.

- использование нативных драйверов: установка нативных драйверов на пользовательской рабочей станции и ВРМ позволяет использовать весь функционал принтера, включая двустороннюю печать. Для корректного перенаправления принтера версии драйверов должны совпадать;
- использование универсального драйвера Microsoft Software Printer Driver: универсальный драйвер позволяет избежать установки драйверов для каждого принтера. При этом драйвер поддерживает только одностороннюю печать.

Для использования универсального драйвера на пользовательской рабочей станции с установленным ПО Termidesk Viewer нужно создать переменную окружения `TDSK_RDP_PRT_UNIVERSAL`. Для перенаправления принтера с использованием нативного драйвера переменную нужно удалить.

Перенаправление смарт-карт

Общие сведения по перенаправлению смарт-карт

В текущей версии Termidesk VDI возможные сценарии перенаправления смарт-карт из пользовательской рабочей станции приведены в таблице (см. таблицу Возможные сценарии перенаправления смарт-карт).

Следующие модели ключевых носителей прошли тестирование на перенаправление в РМ:

- Рутокен Lite;
- Рутокен ЭЦП 2.0 (2100);
- Рутокен ЭЦП PKI (1800);
- JaCarta PRO;

- JaCarta PKI;
- JaCarta-2 SE;
- eToken JC.

Начиная с Termidesk VDI версии 7.0 список смарт-карт, перенаправляемых через ПО Termidesk Viewer, сохраняется автоматически. Срок хранения списка составляет 30 дней. Если смарт-карта ни разу не была перенаправлена за это время, то сохраненные данные о ее перенаправлении удаляются. При каждом перенаправлении смарт-карты обновляется информация о сохранении ее настроек перенаправления.

Существующие ограничения:

- выборочное перенаправление смарт-карт поддерживается только для протоколов доставки TERA и SPICE;
- для протокола доставки RDP выполняется перенаправление всех смарт-карт, подключенных к пользовательской рабочей станции;
- максимальное количество смарт-карт, доступных для перенаправления ограничено количеством каналов протокола доставки;
- сохранение списка перенаправляемых смарт-карт не поддерживается, если к пользовательской рабочей станции подключены смарт-карты одной модели.

В таблице приняты обозначения:

- «MS RDSH» - терминальный сервер MS RDSH;
- «STAL» - терминальный сервер с установленным компонентом «Сервер терминалов Astra Linux».

Администратор должен включить соответствующие политики фонда РМ для работы перенаправления, если при подключении используется ПО Termidesk Viewer.

При подключении по протоколу RDP из Клиента могут использоваться стандартные утилиты ОС, в этом случае возможность перенаправления регулируется на уровне протокола доставки.

Сценарии актуальны при подключении к РМ непосредственно из Клиента.

Начиная с Termidesk VDI версии 6.1 функционал подключения по протоколу RDP с использованием ПО Termidesk Viewer выведен из экспериментального режима и является основным вариантом подключения. Сценарии с использованием системных программ не гарантируются.

Таблица 322. Возможные сценарии перенаправления смарт-карт

Комбинации ОС	SPICE	RDP (termidesk-viewer)	TERA
Astra Linux Special Edition → Astra Linux Special Edition	□		□
Astra Linux Special Edition → Microsoft Windows	□	□	
Astra Linux Special Edition → MS RDSH		□	
Astra Linux Special Edition → STAL		□	
Microsoft Windows → Astra Linux Special Edition	□		□
Microsoft Windows → Microsoft Windows	□	□	
Microsoft Windows → MS RDSH		□	

Комбинации ОС	SPICE	RDP (termidesk-viewer)	TERA
Microsoft Windows → STAL		□	
Microsoft Windows → РЕД ОС			
РЕД ОС → РЕД ОС			
РЕД ОС → Microsoft Windows			
Альт Рабочая станция → Microsoft Windows			
Альт Рабочая станция → Astra Linux Special Edition			

В гостевой ОС должны быть установлены рекомендованные производителем смарт-карт драйверы.

Для протокола TERA администратор должен выполнить дополнительную настройку компонента «Агент виртуальных смарт-карт».

Перенаправление каталогов

Общие сведения по перенаправлению каталогов

Возможные сценарии перенаправления каталогов из пользовательской рабочей станции приведены в таблице (см. таблицу Возможные сценарии перенаправления каталогов из пользовательской рабочей станции).

Начиная с Termidesk VDI версии 7.0 список каталогов, перенаправляемых через ПО Termidesk Viewer, сохраняется автоматически. Срок хранения списка составляет 30 дней. Если каталог ни разу не был перенаправлен за это время, то сохраненные данные о его перенаправлении удаляются. При каждом перенаправлении каталога обновляется информация о сохранении его настроек перенаправления.

Существующие ограничения:

- сохранение списка перенаправляемых каталогов поддерживается только для протокола RDP.

В таблице приняты обозначения:

- «MS RDSH» - терминальный сервер MS RDSH;
- «STAL» - терминальный сервер с установленным компонентом «Сервер терминалов Astra Linux».

Администратор должен включить политику фонда РМ «Перенаправление дисков и папок (RDP, SPICE, TERA)» для работы перенаправления.

Сценарии актуальны при подключении к РМ непосредственно из Клиента.

Таблица 323. Возможные сценарии перенаправления каталогов из пользовательской рабочей станции

Комбинации ОС	SPICE	RDP (termidesk-viewer)	TERA
Astra Linux Special Edition → Astra Linux Special Edition	□		□
Astra Linux Special Edition → Microsoft Windows	□	□	□
Astra Linux Special Edition → MS RDSH		□	
Astra Linux Special Edition → STAL		□	
Microsoft Windows → Astra Linux Special Edition	□		□

Комбинации ОС	SPICE	RDP (termidesk-viewer)	TERA
Microsoft Windows → Microsoft Windows	□	□	□
Microsoft Windows → MS RDSH		□	
Microsoft Windows → STAL		□	
Microsoft Windows → РЕД ОС	□		
РЕД ОС → РЕД ОС	□		
РЕД ОС → Microsoft Windows	□		□
Альт Рабочая станция → Microsoft Windows	□		□
Альт Рабочая станция → Astra Linux Special Edition	□		

Перенаправление домашнего каталога пользователя

Возможность перенаправления домашнего каталога пользователя в РМ управляется администратором через политики фонда РМ: «Перенаправление дисков и папок (RDP, SPICE, TERA)» и «Перенаправление домашнего каталога пользователя».

Если администратор разрешил перенаправление, то при подключении пользователя к РМ его домашний каталог будет смонтирован в РМ как сетевой диск, который будет доступен:

- для ОС Linux:
  - при подключении по протоколу TERA: в области навигации в разделе «Сетевые ресурсы» или в директории `/media/davfs`;
  - при подключении по протоколу SPICE: в области навигации в разделе «Сетевые ресурсы» или в директории `~/davfs/<имя пользователя>`;
  - при подключении по протоколу RDP: в области навигации в разделе «Сетевые ресурсы» или в директории `/home/<имя пользователя>/thinclient_drives/home`;
  - при подключении к «Серверу терминалов Astra Linux» в директории `/run/user/<идентификатор пользователя>/stal/`;
- для ОС Microsoft Windows: в области навигации проводника в разделе «Перенаправленные диски и папки».

Перенаправление домашнего каталога будет выполнено автоматически, без необходимости его выбора через интерфейс ПО Termidesk Viewer.

Перенаправление веб-камер

Общие сведения по перенаправлению веб-камер

Возможные сценарии перенаправления веб-камер из пользовательской рабочей станции в РМ приведены в таблице (см. таблицу Возможные сценарии перенаправления веб-камер из пользовательской рабочей станции).

Особенности функционирования на ОС MacOS:

- при первом запуске ПО Termidesk Viewer и выборе пункта «Вебкамера» отобразится предупреждение (см. рисунок Запрос доступа к камере), пример: «Приложение «Termidesk Client» запрашивает доступ к камере». В этом случае нужно:
  - для разрешения доступа нажать экранную кнопку **[OK]**;
  - для запрета доступа нажать экранную кнопку **[Не разрешать]**. В этом случае окно «Менеджер вебкамер» отобразится, но предварительный просмотр изображения будет пуст, экранная кнопка **[Ок]** заблокируется. Веб-камера использоваться не будет. Для изменения доступа нужно перейти «Системные настройки -

Конфиденциальность и безопасность - Камера» и активировать разрешение для приложения «Termidesk Client».

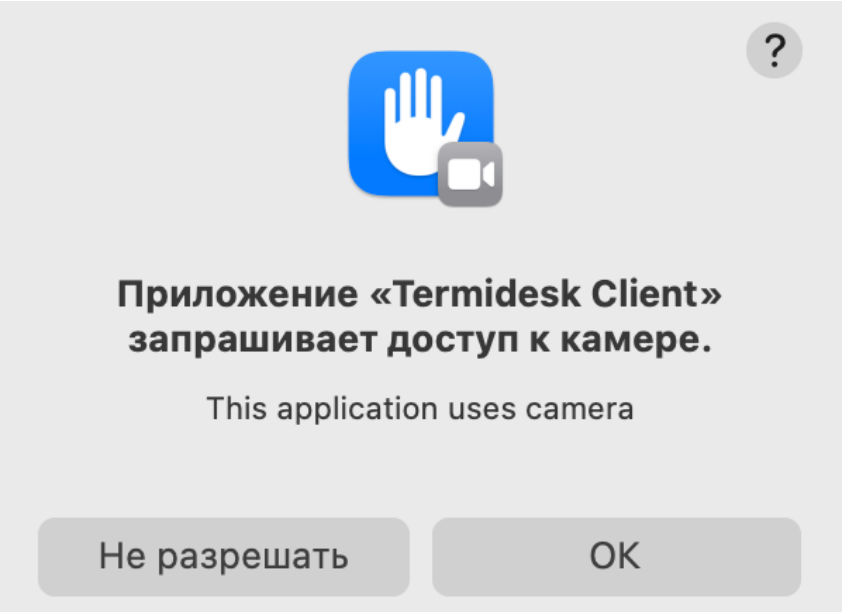


Рисунок 212. Запрос доступа к камере

В таблице приняты обозначения:

- «MS RDSH» - терминальный сервер MS RDSH;
- «STAL» - терминальный сервер с установленным компонентом «Сервер терминалов Astra Linux».

Возможность перенаправления управляется администратором через политику фонда РМ «Перенаправление веб-камеры (RDP, SPICE, TERA)».

Сценарии актуальны при подключении к РМ непосредственно из Клиента.

Начиная с Termidesk VDI версии 6.1 функционал подключения по протоколу RDP с использованием ПО Termidesk Viewer выведен из экспериментального режима и является основным вариантом подключения. Сценарии с использованием системных программ не гарантируются.

Таблица 324. Возможные сценарии перенаправления веб-камер из пользовательской рабочей станции

Комбинации ОС	SPICE	RDP (termidesk-viewer)	TERA
Astra Linux Special Edition → Astra Linux Special Edition	□		□
Astra Linux Special Edition → Microsoft Windows	□[2]	□[2]	□[2]
Astra Linux Special Edition → STAL		□[1]	
Astra Linux Special Edition → MS RDSH		□[2]	
Microsoft Windows → Astra Linux Special Edition	□		□
Microsoft Windows → Microsoft Windows	□[2]	□[2]	□[2]
Microsoft Windows → РЕД ОС			
Microsoft Windows → STAL		□[1]	
Microsoft Windows → MS RDSH		□[2]	

Комбинации ОС	SPICE	RDP (termidesk-viewer)	TERA
MacOS → Astra Linux Special Edition	□		□
MacOS → Microsoft Windows	□[2]	□[2]	□[2]
MacOS → STAL		□[1]	
MacOS → MS RDSH		□[2]	
РЕД ОС → РЕД ОС			
РЕД ОС → Microsoft Windows			
Альт Рабочая станция → Microsoft Windows			
Альт Рабочая станция → Astra Linux Special Edition			

Примечание:

[1] Перенаправление и работа с веб-камерами поддерживается в STAL, однако в некоторых случаях потребуется дополнительная настройка:

- если STAL установлен в ОС Альт Рабочая станция с графической средой KDE Plasma: потребуется замена стандартного звукового сервера PulseAudio на PipeWire;

[2] При перенаправлении веб-камеры в ВРМ с ОС Microsoft Windows или на терминальный сервер MS RDSH пробрасываемая камера «Termidesk Stream» является виртуальным устройством DirectShow. Это означает:

- камера не отображается в диспетчере устройств ОС Microsoft Windows;
- камера не отображается в приложениях, которые не используют фреймворк DirectShow (например, встроенное в ОС Microsoft Windows приложение «Камера»).

КЛИЕНТ. ЗАВЕРШЕНИЕ РАБОТЫ

Завершение работы с РМ

Пользователь Termidesk VDI может завершить работу с РМ двумя штатными способами:

- выйти из гостевой ОС РМ - выход осуществляется стандартным способом завершения работы с ОС (см. рисунок Пример завершения работы в ОС);

В зависимости от модели доставки после выхода из гостевой ОС РМ может быть удалено с последующим созданием другого или может остаться в актуальном состоянии.

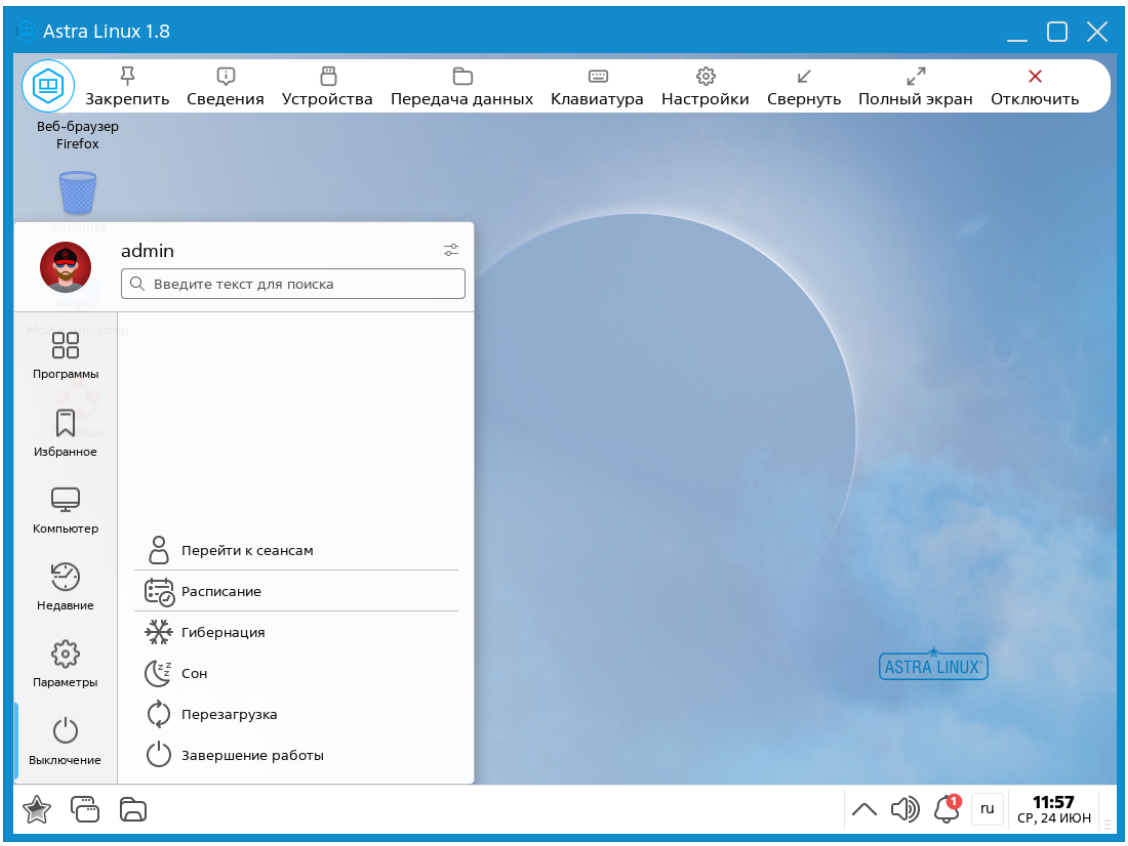


Рисунок 213. Пример завершения работы в ОС

- завершить работу протокола доставки - пользователь закрывает приложение, осуществляющее доставку РМ (см. рисунок Пример завершения работы ПО Termidesk Viewer);

В этом случае, независимо от модели доставки, РМ не удаляется, а блокируется для будущего использования пользователем, осуществившим выход из приложения протокола доставки.

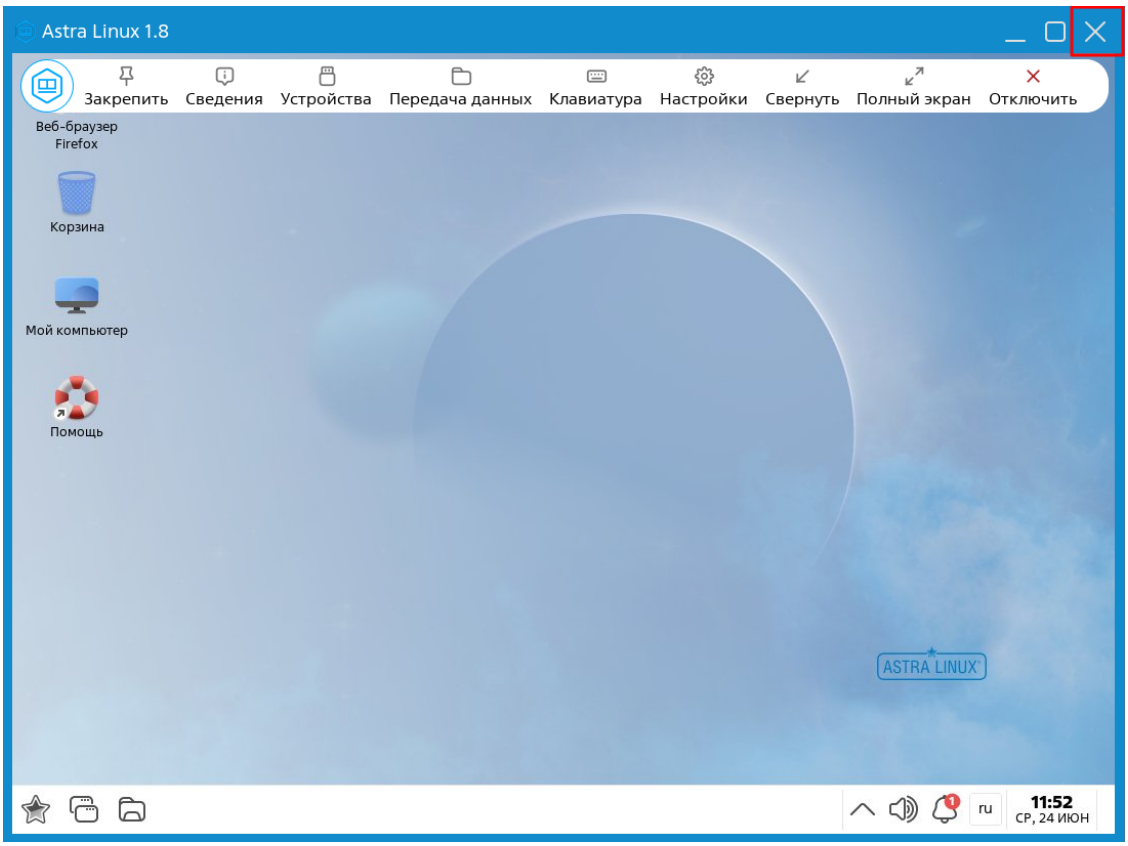


Рисунок 214. Пример завершения работы ПО Termidesk Viewer

- отключиться от РМ – пользователь разрывает подключение к текущему сеансу без завершения работы приложений (см. рисунок Пример разрыва подключения к сеансу).

Возможность разрыва подключения к сеансу доступна при подключении к РМ ОС Microsoft Windows по протоколу TERA и при подключении по протоколу RDP к рабочему столу сервера терминалов MS RDS.

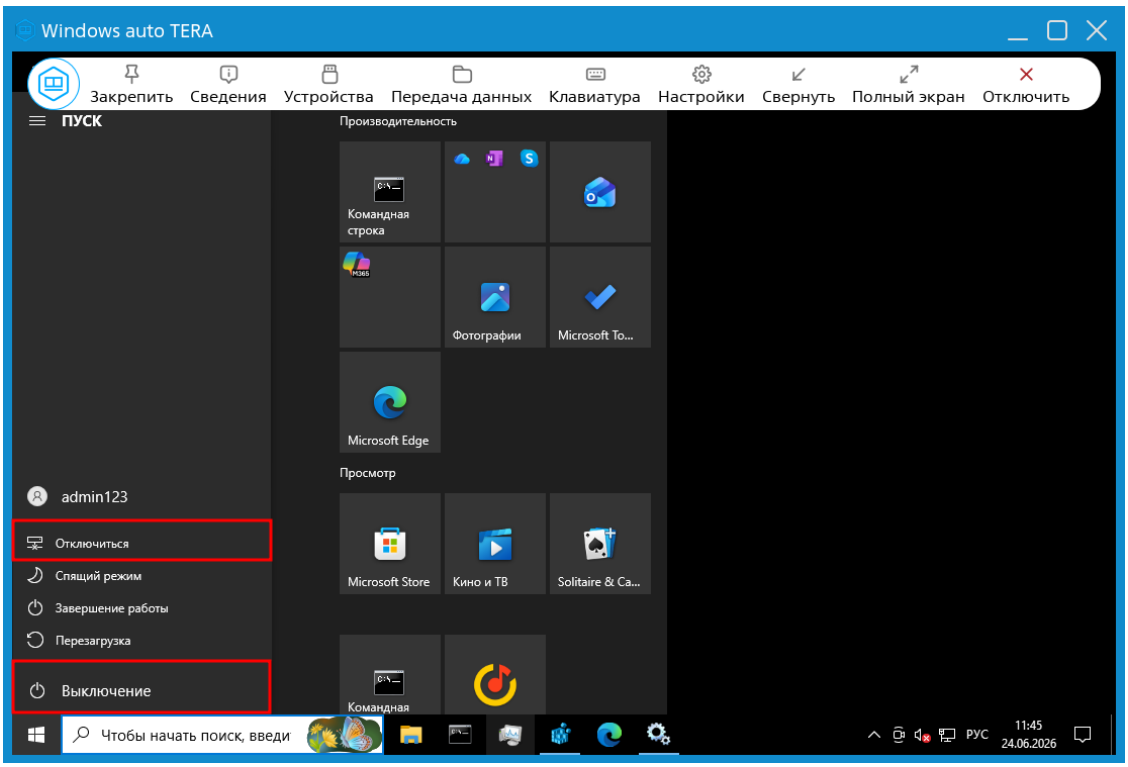


Рисунок 215. Пример разрыва подключения к сеансу

Завершение работы с приложением

Для завершения работы Клиента нужно:

- перейти в область уведомлений ОС;
- нажать правой кнопкой мыши по значку Termidesk VDI;
- выбрать пункт «Выйти» (см. рисунок Завершение работы с Клиентом через область уведомлений ОС).

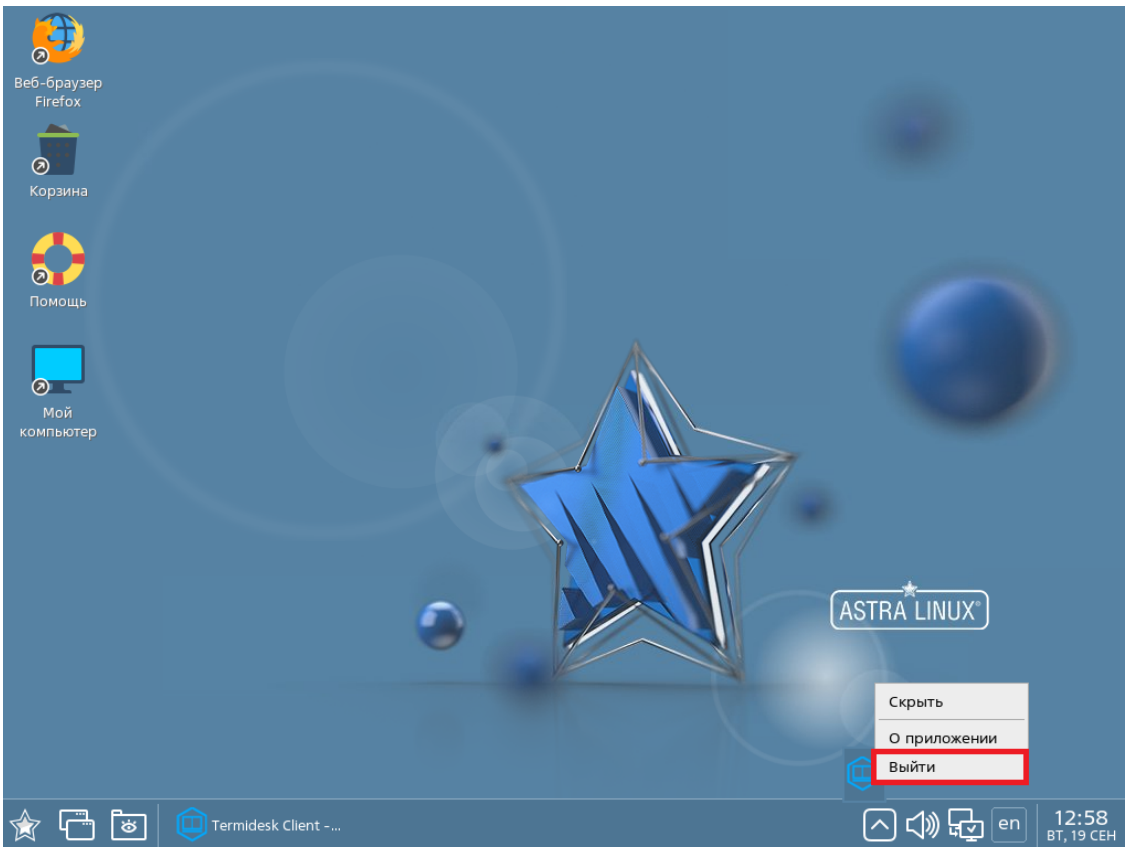


Рисунок 216. Завершение работы с Клиентом через область уведомлений ОС

Завершение работы с выбранным сервером

При необходимости подключения к другому серверу Termidesk VDI следует завершить работу с текущим сервером.

Для завершения работы с сервером нужно нажать на экранную кнопку **[Выход]** в Клиенте (см. рисунок Завершение работы с сервером).

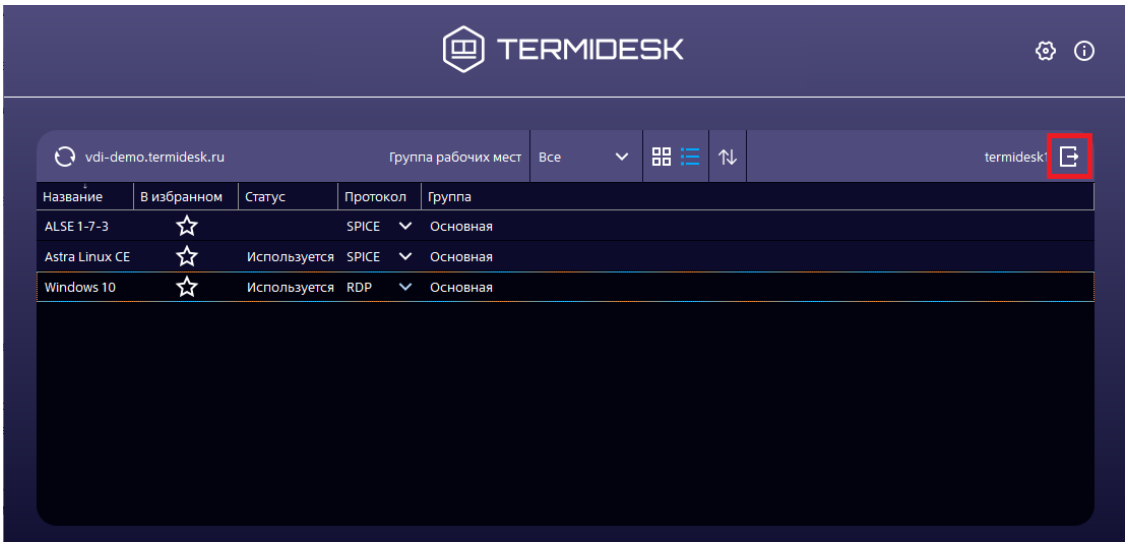


Рисунок 217. Завершение работы с сервером

Время подключения к серверу Termidesk VDI определяется администратором через параметр «Длительность сессии пользователя, с» в «Портале администратора».

При достижении установленного лимита времени сессии в системном трее отобразится

уведомление от приложения «Клиент»: «Ваш сеанс завершился». В журнале «Клиента» отражаются события как получения значения лимита сессии («userSessionLength»), так и завершения сессии по таймауту.

КЛИЕНТ. ЖУРНАЛИРОВАНИЕ

В ОС Microsoft Windows журналы расположены:

- журнал работы Клиента в файле `C:\Users\<user>\AppData\Roaming\UVEON\logs\Termidesk Client.log`;
- журнал работы ПО Termidesk Viewer в файле `C:\Users\<user>\AppData\Roaming\UVEON\logs\Termidesk Viewer.log`;
- журнал работы утилиты `vdi-proxy` в файле `C:\Users\<user>\AppData\Roaming\UVEON\logs\Termidesk Proxy.log`;
- журнал работы службы Termidesk VDI TBUS в файле `C:\ProgramData\UVEON\logs\Termidesk BUS.log`.

В ОС Astra Linux журналы работы расположены:

- журнал работы Клиента в файле `/home/<user>/.config/UVEON/logs/Termidesk Client.log`
- журнал работы ПО Termidesk Viewer в файле `/home/<user>/.config/UVEON/logs/Termidesk Viewer.log`;
- журнал работы утилиты `vdi-proxy` в файле `/home/<user>/.config/UVEON/logs/Termidesk Proxy.log`;
- журнал работы службы `Termidesk VDI TBUS` в файле `/var/log/termidesk/tbus.log`.

В ОС macOS журналы работы расположены:

- журнал работы Клиента в файле `/Users/<user>/.config/UVEON/logs/Termidesk Client.log`;
- журнал работы ПО Termidesk Viewer в файле `/Users/<user>/.config/UVEON/logs/Termidesk Viewer.log`;
- журнал работы утилиты `vdi-proxy` в файле `/Users/<user>/.config/UVEON/logs/Termidesk Proxy.log`.

Журналы клиента Loudplay (при использовании протокола Loudplay) копируются Клиентом в следующие каталоги:

> Ротация журналов Loudplay выполняется средствами и настройками клиента Loudplay. Очистка журналов Loudplay находится в зоне ответственности пользователей Loudplay.

- ОС Microsoft Windows: `C:\Users\<user>\AppData\Roaming\UVEON\logs\Loudplay_Client.log`;
- ОС Linux: `/home/<user>/.config/UVEON/logs/Loudplay_Client.log`.

> Утилита `vdi-proxy` используется для создания WebSocket-туннеля между запускаемой программой и опубликованным ресурсом. Утилита `vdi-proxy` автоматически запускается Клиентом, когда происходит подключение к ресурсу через компонент «Шлюз» и через программу доставки, которая не имеет возможности самостоятельно создать WebSocket-туннель (например, `mstsc.exe`).

Для сбора журналов и сохранения их в архив необходимо в Клиенте нажать на графический элемент в виде кружка с символом «i» в правом верхнем углу графического интерфейса и нажать экранную кнопку **[Информация для тех.поддержки]**. Далее нажать

экранную кнопку **[Сохранить]**, выбрать каталог для сохранения и задать имя файлу.

КЛИЕНТ. НЕШТАТНЫЕ СИТУАЦИИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

Возможные неисправности при работе с Клиентом и способы их устранения приведены в таблице (см. таблицу Перечень возможных нештатных ситуаций и способов их устранения).

Таблица 325. Перечень возможных нештатных ситуаций и способов их устранения

Индикация	Описание	Возможное решение
Ошибка: «Выбранный поставщик не поддерживает работу с протоколом доставки RDP (терминальный доступ). Выберите корректный протокол доставки»	Ошибка появляется при попытке подключения к фонду ВРМ с использованием протокола доставки типа «RDP (терминальный доступ)»	Необходимо обратиться к администратору. Ошибка означает, что фонду ВРМ назначен протокол доставки с типом «RDP (терминальный доступ)», который не подходит для подключения к ВРМ. Администратору необходимо в настройках фонда назначить протокол доставки с типом «RDP»
Ошибка: «Не задан транспорт подключения»	Ошибка появляется при попытке получить РМ	Необходимо обратиться к администратору. Администратору необходимо добавить протоколы доставки в фонд РМ
Ошибка: «Number of service reached MAX for service poll»	Ошибка появляется при запросе РМ	Необходимо обратиться к администратору. Ошибка значит, что достигнуто максимальное количество РМ. Администратору необходимо либо перейти в фонд и принудительно завершить сессию, либо увеличить в фонде максимальное количество РМ

Индикация	Описание	Возможное решение
Ошибка: «INTERNAL ERROR: cannot create temporary directory!»	Ошибка появляется при входе в гостевую ОС Microsoft Windows	Необходимо обратиться к администратору. Возможные причины ошибки: • нет прав на каталог профиля пользователя (локальный/сетевой); • профиль не успел создаться в момент запуска компонента «Агент виртуального рабочего места». Администратору необходимо в гостевой ОС РМ перейти в «Управление компьютером - Службы и приложения - Службы - Termidesk Agent Daemon» и в свойствах службы на вкладке «Общие» установить «Тип запуска - Автоматически (отложенный запуск)»
Ошибка: «Прокси-сервер запретил подключение»	Ошибка появляется при подключении к фонду РМ	Необходимо обратиться к администратору. Необходимо настроить прокси-сервер на уровне ОС пользовательской рабочей станции
Статус «Подготовка рабочего места» висит неограниченно долго	При попытке подключиться к РМ по протоколу RDP (напрямую или через компонент «Шлюз») появляется статус «Подключение к рабочему месту», который потом сменяется на «Подготовка рабочего места» и отображается неограниченно долго	Необходимо обратиться к администратору. Ситуация возникает, если порт РМ недоступен: при запросе подключения к РМ по протоколу RDP перед выдачей подключения «Универсальный диспетчер» проводит проверку доступности порта затребованного протокола на целевом IP-адресе. Администратору необходимо в настройках фильтра трафика разрешить подключение из сегмента сети с инфраструктурой Termidesk VDI для узлов с компонентами «Универсальный диспетчер» в сегмент сети, где находятся РМ, на порт RDP 3389

Индикация	Описание	Возможное решение
Ошибка: «Не удалось установить соединение с сервером»	Ошибка появляется при попытке получить РМ	Необходимо выбрать корректный протокол доставки (SPICE) или обратиться к администратору. Ошибка сообщает, что ПО для визуализации РМ не смогло подключиться к платформе виртуализации. Отказ подключения происходит со стороны SPICE-сервера гипервизора. Причиной могут быть: • неправильный протокол доставки; • виртуальная машина (ВМ) выключается и отключает видеокарту; • проблемы с межсетевым экраном; • завис процесс `qemu` ВМ
Ошибка: «VMwareLinkedDeployment object has no attribute 'getConsoleConnection'»	Ошибка появляется при попытке получить РМ	Необходимо обратиться к администратору. С поставщиком ресурсов VMware vSphere необходимо использовать протокол RDP для РМ. Протокол SPICE не поддерживается данным поставщиком

Индикация	Описание	Возможное решение

Гостевая ОС Astra Linux не производит автоматическое масштабирование экрана	При подключении к РМ не происходит автоматическое масштабирование экрана	В гостевой ОС РМ открыть программу «Терминал fly» и выполнить следующее:
		• получить название активного монитора:
		`xrandr --listactivemonitors`
		• выполнить команду:
		`xrandr --output $MONITOR --auto`
		Где `$MONITOR` - название активного монитора, полученное предыдущей командой.
		Если действия не привели к желаемому результату, необходимо обратиться к администратору для проверки настроек масштабирования в гостевой ОС РМ

При попытке соединения к терминальному серверу или опубликованному на нем приложению соединение не устанавливается	При подключении к терминальному серверу соединение не устанавливается. При подключении к опубликованному приложению вместо приложения - черный фон. Ошибка может возникнуть при подключении к «Серверу терминалов Astra Linux» (STAL) или MS RDS	Необходимо обратиться к администратору. Для устранения проблемы необходимо в графическом интерфейсе управления Termidesk VDI перейти «Рабочие места - Фонды», выбрать фонд РМ и задать ему политику «Аутентификация на уровне сети (RDP)»: • «TLS», «RDP» или «Автостогласование» для STAL, при использовании Kerberos - «NLA» или «Автостогласование»; • «NLA» для MS RDS

Индикация	Описание	Возможное решение
Не отображается окно приложения, полученного через Microsoft Remote Desktop Services, в ОС Microsoft Windows	При запуске приложения на панели задач отображается иконка приложения, само приложение не отображается	Чтобы обойти эту проблему, нужно отключить режим `hi-Def` на пользовательской рабочей станции. Для этого выполнить последовательность действий: • нажать экранную кнопку **[Пуск]**, ввести `regedit` и выбрать `regedit.exe`; • в открывшемся редакторе реестра открыть подраздел «HKEY_CURRENT_USER\SOFTWARE\Microsoft\Terminal Server Client»; • в меню «Правка» выбрать пункт «Создать», а затем «Параметр DWORD»; • в поле «Новое значение 1» ввести `EnableAdvancedRemoteFXRemoteAppSupport` и нажать клавишу **<ENTER>**; • правой кнопкой мыши нажать на параметр `EnableAdvancedRemoteFXRemoteAppSupport` и выбрать пункт «Изменить»; • в поле данных «Значение» ввести `0` и нажать кнопку **[OK]**; • закрыть редактор реестра
Ошибка: «Фонд находится в режиме техобслуживания, подключение к рабочему месту временно недоступно»	Ошибка появляется при попытке получить РМ	Необходимо обратиться к администратору. Выбранный фонд находится в режиме техобслуживания. Чтобы фонд вновь был доступен для подключения, администратор должен отключить этот режим
Ошибка: «Ошибка сервера»	Ошибка появляется при попытке подключения к терминальному серверу STAL	Необходимо обратиться к администратору. Администратору необходимо подключиться к серверу с установленным STAL и проверить значение параметра `allowed_users` в файле `/etc/X11/Xwrapper.config`. Этот параметр должен соответствовать: `allowed_users=anybody`

Индикация	Описание	Возможное решение
Ошибка: «Этот сеанс будет прекращен из-за ошибки протокола. Попробуйте подключиться заново к удаленному компьютеру»	Ошибка появляется при попытке подключиться к терминальному серверу STAL через стандартную утилиту Windows `mstsc`	Необходимо обратиться к администратору. Администратор должен проверить значение политики «Глубина цвета (RDP)» в «Портале администратора» компонента «Универсальный диспетчер»: значение политики должно быть «32 бит»

Ошибка:
 	
«Сервис cups не запущен или работает некорректно»
	Ошибка появляется при нажатии на экранную кнопку **[Перенаправление принтеров]** в интерфейсе ПО Termidesk Viewer	Необходимо обратиться к администратору.
		Администратор должен:
		
		• проверить состояние службы `termidesk-cupsd`:
		
		`sudo systemctl status termidesk-cupsd`
		
		• если служба неактивна, то активировать ее:
		
		`sudo systemctl start termidesk-cupsd`
		
		• если служба не найдена или рекомендации не помогли, то переустановить компонент «Агент виртуальных рабочих мест»

Ошибка: «Достигнуто максимально допустимое количество подключений, разрешённое лицензией. Пожалуйста, обратитесь к администратору» или «Maximum allowed number of licensed connections has been reached. Please contact your adminstrator»	Ошибка появляется при запросе РМ	Необходимо обратиться к администратору. Ошибка значит, что достигнуто максимальное количество подключений, определенное лицензией. Администратору необходимо либо принудительно завершить сессии, либо получить и внести лицензию на большее количество подключений

Индикация	Описание	Возможное решение
Ошибка: «Не удалось авторизовать пользователя на фермах ресурсов» или «JWTAuthenticationError: Failed to get token from Server»	Ошибка появляется при попытке подключиться к РМ через веб-бразуер или через Клиент	Необходимо обратиться к администратору. Администратор должен: • убедиться, что для параметра `AGGREGATOR_JWT_SSL_KEY` в конфигурационном файле «Агрегатора» задан правильный путь к корректному файлу закрытого ключа; • убедиться, что для параметра `AGGREGATOR_JWT_SSL_CERT` в конфигурационном файле «Универсального диспетчера», использующегося в ферме, задан правильный путь к корректному файлу сертификата
Ошибка: «Неправильный формат имени пользователя. Имя пользователя должно соответствовать формату sAMAccountName» или «Неправильный формат имени пользователя. Имя пользователя должно соответствовать формату UPN»	Ошибка появляется при попытке авторизоваться в Клиенте или в «Портале пользователя»	Ошибка означает, что для авторизации в домене аутентификации используется неверный формат имени пользователя: • если ошибка относится к формату «sAMAccountName», то логин пользователя следует указывать в формате `UserPrincipalName` (`UPN`), с доменной частью. Например: `user@local`; • если ошибка относится к формату `UPN`, то логин пользователя следует указывать в формате `sAMAccountName`. Например: `user`. Если ошибка воспроизводится, следует обратиться к администратору. Администратор должен проверить, что в домене аутентификации установлено правильное значение для параметра «Формат имени пользователя для аутентификации»

Индикация	Описание	Возможное решение
Ошибка: «В данный момент создание новой сессии невозможно из-за удаления предыдущей. Попробуйте через несколько минут. Если проблема повторится, обратитесь к администратору»	Ошибка появляется при попытке подключиться к терминальному серверу	Ошибка означает, что предыдущая сессия в данный момент удаляется. Следует подождать некоторое время, затем снова подключиться к терминальному серверу. Если ошибка воспроизводится, следует обратиться к администратору. Администратор должен проверить: • доступность поставщика ресурсов экранной кнопкой **[Тест]** в «Портале администратора». Для этого нужно перейти «Инфраструктура - Поставщики ресурсов», выбрать наименование поставщика ресурсов и нажать экранную кнопку **[Изменить]**; • работоспособность службы компонента «Сессионный агент» на терминальном сервере; • работоспособность служб STAL, если используется терминальный сервер с этим компонентом
Индикация: «Администратор запретил доступ клиенту с этого IP адреса»	При подключении пользователя к Termidesk VDI отображается фонд, к которому невозможно подключиться. При этом при наведении мыши на фонд появляется сообщение «Администратор запретил доступ клиенту с этого IP адреса»	Индикация означает, что администратор запретил доступ к фонду с этого IP-адреса, но разрешил его отображение. Если доступ к фонду необходим, следует обратиться к администратору. Администратор должен: • добавить соответствующую сеть в настройках фонда; • проверить правильность значения параметра «Доступ из связанных сетей» в свойствах фонда; • проверить правильность значения параметра «Скрывать недоступные ресурсы» в «Портале администратора»

Индикация	Описание	Возможное решение
При работе с файлами и их сохранении возникают ошибки записи. При работе в офисных пакетах (например, LibreOffice) появляется ошибка: «Невозможно создать файл блокировки ...»	При подключении пользователя к РМ по протоколу TERA и работе с перенаправленным каталогом наблюдаются ошибки записи файлов при попытке их сохранения и при работе с ними в офисных пакетах (например, LibreOffice)	Для исправления ситуации нужно отредактировать файл `~/.davfs2/davfs2_termidesk.conf`, добавив строку: Для редактирования файла требуется повышение привилегий пользователя (`sudo`). `use_locks 0`
Не перенаправляется микрофон при подключении по протоколу RDP к ВРМ с гостевой ОС Microsoft Windows	При подключении по протоколу RDP к ВРМ с гостевой ОС Microsoft Windows с пользовательской рабочей станции, на которой микрофон отсутствует или отключен, соединение устанавливается корректно. Однако последующее подключение микрофона во время активного сеанса в ПО Termidesk Viewer не приводит к его перенаправлению в ВРМ	Для исправления ситуации нужно завершить текущий сеанс и повторно подключиться к ВРМ после подключения микрофона к пользовательской рабочей станции
Ошибка: «Не удалось установить доверительные отношения между этой рабочей станцией и основным доменом»	Ошибка появляется при попытке авторизоваться в гостевой ОС РМ	Необходимо обратиться к администратору. Администратор должен убедиться, что для РМ используются параметры гостевых ОС Windows с доменом MS AD
Ошибка: «Удаленный рабочий стол не готов. Повторите попытку позже»	Ошибка появляется при попытке получить РМ	Ошибка означает, что РМ еще не готово (не перешло в статус «Действительный») или не получен ответ от «Агента виртуального рабочего места». Необходимо дождаться подготовки РМ и повторно подключиться через некоторое время. Если ошибка сохранилась: • необходимо обратиться к администратору; • администатор должен убедиться в правильности настройки «Агента виртуального рабочего места»

Индикация	Описание	Возможное решение

Ошибка:
 	
«Ошибка подключения: Termidesk Agent не отвечает — возможно, он не установлен или не запущен на выбранном ВРМ»
	Ошибка появляется при попытке подключиться к назначенному РМ	Необходимо обратиться к администратору.
		Администратор должен:
		
		• проверить состояние службы `termidesk-agent`:
		
		`sudo systemctl status termidesk-agent`
		
		• убедиться в правильности настройки «Агента виртуального рабочего места»;
		• перезапустить службу `termidesk-agent`:
		
		`sudo systemctl restart termidesk-agent`
		
		• увеличить время ожидания ответа от «Агента виртуального рабочего места» в параметре «Таймаут обращения к агенту РМ, с» в «Портале администратора»;
		• если служба не найдена или рекомендации не помогли, то переустановить компонент «Агент виртуальных рабочих мест»

Не перенаправляется звук ВРМ на подключенное к пользовательской рабочей станции с ОС MacOS Bluetooth-устройство	При подключении к ВРМ через ПО Termidesk Viewer на Bluetooth-устройстве, подключенном к пользовательской рабочей станции с ОС MacOS, не воспроизводится звук ВРМ	Для исправления ситуации перед запуском ПО Termidesk Viewer на пользовательской рабочей станции с ОС MacOS нужно выбрать соответствующее Bluetooth-устройство в настройках: • «Настройки - Звук - Воспроизведение звуковых эффектов»; • «Настройки - Звук - Выход и вход»

Индикация	Описание	Возможное решение
После переподключения к сессии РМ или при разрыве сетевого соединения с РМ перенаправление каталога на сервер терминалов MS RDS становится недоступным	При активном использовании перенаправленного каталога (например, при копировании данных) переподключение к сессии РМ либо разрыв сетевого соединения с РМ приводит к нарушению работы механизма перенаправления. После восстановления соединения перенаправление каталога на сервер терминалов MS RDS для текущего пользователя становится недоступным: каталог не перенаправляется либо доступ к ранее перенаправленному каталогу отсутствует	Для исправления ситуации нужно выполнить выход из гостевой ОС РМ и повторно переподключиться к сессии РМ

При перенаправлении USB-гарнитуры или иного аудио USB-устройства процесс ПО Termidesk Viewer зависает и не отвечает	При перенаправлении USB-устройства с ОС Microsoft Windows в РМ по протоколу TERA ПО Termidesk Viewer зависает, действия с РМ невозможны, процесс ПО Termidesk Viewer находится в статусе «Не отвечает». При этом наблюдается рост событий журналирования	Для решения ситуации потребуется выполнить переустановку утилиты `UsbDk`. Для этого:
		• открыть командную строку PowerShell от имени администратора;
		• выполнить:
		`cd 'C:\Program Files\UVEON\Termidesk Client\UsbDk' \UsbDkController.exe -u`
		• перезагрузить пользовательскую рабочую станцию;
		• выполнить:
		`cd 'C:\Program Files\UVEON\Termidesk Client\UsbDk' \UsbDkController.exe -i`
		• перезагрузить пользовательскую рабочую станцию

ТЕРМИНЫ

Базовое виртуальное рабочее место

Также: золотой образ, базовый образ. Образ диска ВМ с предустановленным прикладным ПО. Этот образ далее будет использоваться для создания ВРМ для пользователей

Виртуальное рабочее место

Развернутая на ВМ ОС с установленным «Агентом виртуального рабочего места» и

необходимым прикладным ПО. Подключение к ВРМ происходит через протоколы удаленного доступа

Рабочее место

Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа. Под РМ подразумеваются как ВРМ, так и терминальный доступ или доступ к опубликованным на терминальном сервере приложениям

Гостевая ОС

ОС, функционирующая на ВМ

Группы рабочих мест

Функциональное объединение множества фондов РМ по определенному признаку

Домен аутентификации

Способ проверки субъектов и их полномочий

Поставщик ресурсов

ОС, платформа виртуализации или терминальный сервер (MS RDS/STAL), предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов РМ

Протокол доставки

Поддерживаемый в Termidesk VDI протокол удаленного доступа к РМ

Компонент «Универсальный диспетчер»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им РМ и контроля доставки РМ

Фонд рабочих мест

Совокупность подготовленных РМ для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей

Компонент «Шлюз»

Самостоятельный компонент, отвечающий за туннелирование протоколов доставки, использующих транспортный протокол TCP

Компонент «Сервер терминалов Astra Linux»

Компонент Termidesk VDI. Также: STAL. Обеспечивает подключение пользовательских рабочих станций к РМ с ОС Astra Linux Special Edition через сеанс удаленного терминала

Ключ

Применяется в контексте файла, не опции в команде. Последовательность псевдослучайных чисел, сгенерированная особым образом

Сертификат

Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу

СОКРАЩЕНИЯ

ВМ	Виртуальная машина
ВРМ	Виртуальное рабочее место
ЗПС	Замкнутая программная среда

ОС	Операционная система
ПО	Программное обеспечение
РМ	Рабочее место
ARM	Acorn RISC (Reduced Instruction Set Computer) Machine (архитектура процессора)
CUPS	Common Unix Printing System (система печати Unix)
DNS	Domain Name System (система доменных имен)
Email	Electronic mail (адрес электронной почты)
FQDN	Fully Qualified Domain Name (полностью определенное имя домена)
HiDPI	High Dots Per Inch (высокое разрешение при небольшом размере экрана)
HTML	Hypertext Markup Language (язык гипертекстовой разметки)
IP	Internet Protocol (межсетевой протокол)
LDAP	Lightweight Directory Access Protocol (легковесный протокол доступа к службам каталогов)
MS AD	Microsoft Active Directory (службы каталогов Microsoft)
MS RDS	Microsoft Remote Desktop Services (службы удаленного рабочего стола Microsoft)
MS RDSH	Microsoft Windows Server с ролью «Remote Desktop Session Host» из состава «Remote Desktop Services»
NLA	Network Level Authentication (аутентификация на сетевом уровне)
OTP	One-Time Password (одноразовый пароль)
PDF	Portable Document Format (открытый формат электронных документов)
PIN	Personal Identification Number (персональный идентификатор)
PKINIT	Public Key Cryptography for Initial Authentication (механизм Kerberos, позволяющий использовать сертификаты X.509)
PPD	PostScript Printer Description (описание возможностей конкретной модели принтера)
RAIL	Remote Applications Integrated Locally (предоставление удаленного приложения как локального пользовательского)
RDP	Remote Desktop Protocol (протокол удаленного рабочего стола)
SAML	Security Assertion Markup Language (открытый стандарт обмена данными аутентификации)
SPICE	Simple Protocol for Independent Computing Environments (простой протокол для независимой вычислительной среды)
SSL	Secure Sockets Layer (криптографический протокол)

SSO	Single Sign-On (технология единого входа)
STAL	Terminal Server Astra Linux (компонент «Сервер терминалов Astra Linux»)
TCP	Transmission Control Protocol (протокол управления передачей)
TERA	Termidesk Remote Access protocol (протокол удаленного доступа разработкиООО «УВЕОН»)
TLS	Transport Layer Security (протокол защиты транспортного уровня)
UAC	User Account Control User (контроль учетных записей пользователей)
UPN	User Principal Name (уникальное имя пользователя в формате адреса электронной почты)
URI	Uniform Resource Identifier (унифицированный идентификатор ресурса)
URL	Uniform Resource Locator (унифицированный указатель ресурса)
USB	Universal Serial Bus (последовательный интерфейс для подключения периферийных устройств)
W3C	World Wide Web Consortium (Консорциум Всемирной паутины)
XPS	XML Paper Specification (открытый графический формат фиксированной разметки на базе XML)

СЛЕТ.10001-01 91 01. ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ. REST API

ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ

Назначение документа

Настоящий документ является инструкцией по использованию интерфейса REST API программного комплекса «Диспетчер подключений виртуальных рабочих мест Termidesk» (далее - Termidesk VDI, Termidesk VDI).

В этом руководстве приведены шаги по началу работы с интерфейсом, а также список доступных команд.

Типографские соглашения

Приняты следующие типографские соглашения:

- `моноширинный шрифт` – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk VDI, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

REST API. НАЗНАЧЕНИЕ

REST API позволяет:

- получить данные (GET-запросы);
- создать новые элементы данных (POST-запросы);
- изменить данные (PUT-запросы);
- удалить данные (DELETE-запросы);
- обновить данные (PATCH-запросы).

Для передачи команд через REST API может использоваться утилита `curl`.

`Curl` - кроссплатформенная служебная программа командной строки, позволяющая взаимодействовать с множеством различных серверов по множеству различных протоколов с синтаксисом URL.

При работе с внешней утилитой `curl` необходимо:

- для отправки запроса GET использовать опцию `-X 'GET'`;
- для отправки запроса DELETE использовать опцию `-X 'DELETE'`;
- для отправки запроса PUT использовать опцию `-X 'PUT'`;
- для отправки запроса POST использовать опцию `-X 'POST'`;

- для отправки запроса PATCH использовать опцию `-X 'PATCH'`.

Возвращаемые форматы задаются заголовком `accept`, например:

```
curl ... -H "accept:application/json"
```

Пример POST-запроса для «Универсального диспетчера» Termidesk VDI:

```
curl -X 'POST' \
  'http://disp.termidesk.local/api/webui/v1/servicespools' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -H 'X-Auth-Token: 7bjqtodywjd69dkpdta9ncqprifkr3pu' \
  -d '{
  "name": "string",
  "comments": "string",
  "service_id": "string",
  "osmanager_id": "string",
  "image_id": "string",
  "help_url": "string",
  "servicesPoolGroup_id": "string",
  "cache_l1_srvs": 2147483647,
  "cache_l2_srvs": 2147483647,
  "max_srvs": 2147483647,
  "debug_mode": true,
  "backup": true,
  "fallbackAccess": "string"
}'
```

Результирующий формат указывается в ответном заголовке `content-type`.

«УНИВЕРСАЛЬНЫЙ ДИСПЕТЧЕР»

Начало работы с REST API компонента «Универсальный диспетчер» Termidesk VDI

Получение токена для доступа к REST API компонента «Универсальный диспетчер»

Перед использованием REST API нужно получить токен авторизации `X-Auth-Token`, который необходимо подставлять во все последующие запросы, кроме запросов `health`. Для получения токена нужно авторизоваться в Termidesk VDI, для этого:

- выполнить запрос «https://disp.termidesk.local/api/auth/v7.0/authenticators»;
- запомнить значение одного из параметров: `authUuid`, `authSmallName` или `auth`;
- выполнить запрос, подставив соответствующее значение параметра, полученного ранее:
  - либо с использованием утилиты `curl`. Пример (в поле `authId` подставляется значение из `authUuid`):

```
curl -X 'POST' \
  'https://disp.termidesk.local/api/auth/v7.0/login' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -d '{
  "username": "admin123",
  "password": "admin123",
  "authId": "a6ec7be4-93d1-4473-8471-6dfc8f734d78"
}'
```

- либо с использованием интерфейса Swagger, предоставляющего электронный справочник по командам.

В приведенных командах disp.termidesk.local - сетевой адрес или полное доменное имя узла компонента «Универсальный диспетчер» Termidesk VDI.

Для запросов проверки состояния сервера health используется токен,определенный в конфигурационном файле /etc/opt/termidesk-vdi/termidesk.conf в значении параметра HEALTH_CHECK_ACCESS_KEY.

Формат запроса к /api/health/check выглядит следующим образом:

```
curl -X 'GET' \
'https://disp.termidesk.local/api/health/check' \
-H 'accept: application/json' \
-H 'Authorization: Token
072bfec46ac7c42078bb41ff5f6d1ae201006f0824fb4b2bb8ab8befacb01058'
```

где:

Token 072⋯ - токен, определенный в параметре HEALTH_CHECK_ACCESS_KEY файла /etc/opt/termidesk-vdi/termidesk.conf.

Для форматированного вывода рекомендуется:

- установить пакет jq:

```
sudo apt install jq
```

- выполнить запрос, добавив в конец команды « |jq». Пример:

```
curl -X 'GET' \
'https://disp.termidesk.local/api/health/check' \
-H 'accept: application/json' \
-H 'Authorization: Token
072bfec46ac7c42078bb41ff5f6d1ae201006f0824fb4b2bb8ab8befacb01058' | jq
```

В случае, если запрос завершится ошибкой вида «curl: (60) SSL: no alternative certificate subject name matches target host name... curl failed to verify the legitimacy... », нужно дополнить запрос флагом `--insecure`, который отключит проверку валидности сертификатов:

> Выполнение запроса без использования проверки SSL допустимо только на тестовых стендах. Для исправления ошибки в производственной среде необходимо установить на сервер с порталом «Универсальный диспетчер» валидные сертификаты.

```
curl -X 'GET' \
'https://disp.termidesk.local/api/health/check' \
-H 'accept: application/json' \
-H 'Authorization: Token
072bfec46ac7c42078bb41ff5f6d1ae201006f0824fb4b2bb8ab8befacb01058' --insecure | jq
```

Формат URL-команд компонента «Универсальный диспетчер»

Общий вид команд реализован следующим образом:

`/api/<module>/<ver>/<name>/`,

где:

`<module>` - наименование модуля, реализованного в REST API;

`<ver>` - версия;

`<name>` - наименование элемента. После наименования элемента также могут быть включены уникальные номера объектов и наименования других элементов.

Пример команды через `curl`:

```
curl -X 'GET' \
  'https://disp.termidesk.local/api/discover/' \
  -H 'accept: application/json' \
  -H 'X-Auth-Token: 7bjqtodywjd69dkpdta9ncqprifkr3pu'
```

В REST API реализовано следующее логическое разделение на модули:

- «discover» - используется для отображения списка модулей API, предоставляемого сервером (команда `/api/discover/`);
- «agent» - модуль взаимодействия с компонентом «Агент виртуального рабочего места»;
- «aggregator» - модуль взаимодействия с порталом «Агрегатор»;
- «ssa» - модуль взаимодействия с компонентом «Сессионный агент»;
- «auth» - модуль для аутентификации пользователей веб-интерфейса;
- «client» - модуль взаимодействия с компонентом «Клиент»;
- «health» - модуль проверок состояния Termidesk VDI;
- «webui» - модуль управления функциями, доступными через веб-интерфейс Termidesk

VDI;

- «wsproxy» - модуль взаимодействия с компонентом «Шлюз»;
- «userinfo» - модуль получения информации о пользователе.

При этом список отображаемых модулей зависит от типа портала, который был выбран при установке «Универсального диспетчера»:

- «Портал администратора»: доступны «agent», «aggregator», «ssa», «auth», «discover», «health», «userinfo», «webui»;
- «Портал пользователя»: доступны «agent», «aggregator», «ssa», «auth», «discover», «health», «client», «userinfo», «wsproxy»;
- «Портал администратора» и «Портал пользователя»: доступны все модули.

Электронный справочник по командам компонента «Универсальный диспетчер»

Полная информация о параметрах и командах REST API доступна при вводе URL-команды `https://disp.termidesk.local/api/docs/`, где `disp.termidesk.local` - сетевой адрес или полное доменное имя узла «Универсального диспетчера» Termidesk VDI.

Для получения доступа пользователь должен быть аутентифицирован на «Портале администратора» фермы Termidesk VDI в этой же сессии веб-браузера.

Пример использования:

- нажать экранную кнопку **[Try it out]** в пространстве команд какого-либо модуля для составления запроса (см. рисунок Расположение экранных кнопок для получения доступа к формированию запроса);
- отправить запрос на выполнение экранной кнопкой **[Execute]** (см. рисунок Расположение экранной кнопки для формирования запроса). После нажатия будет отображена также команда для запроса через `curl`.

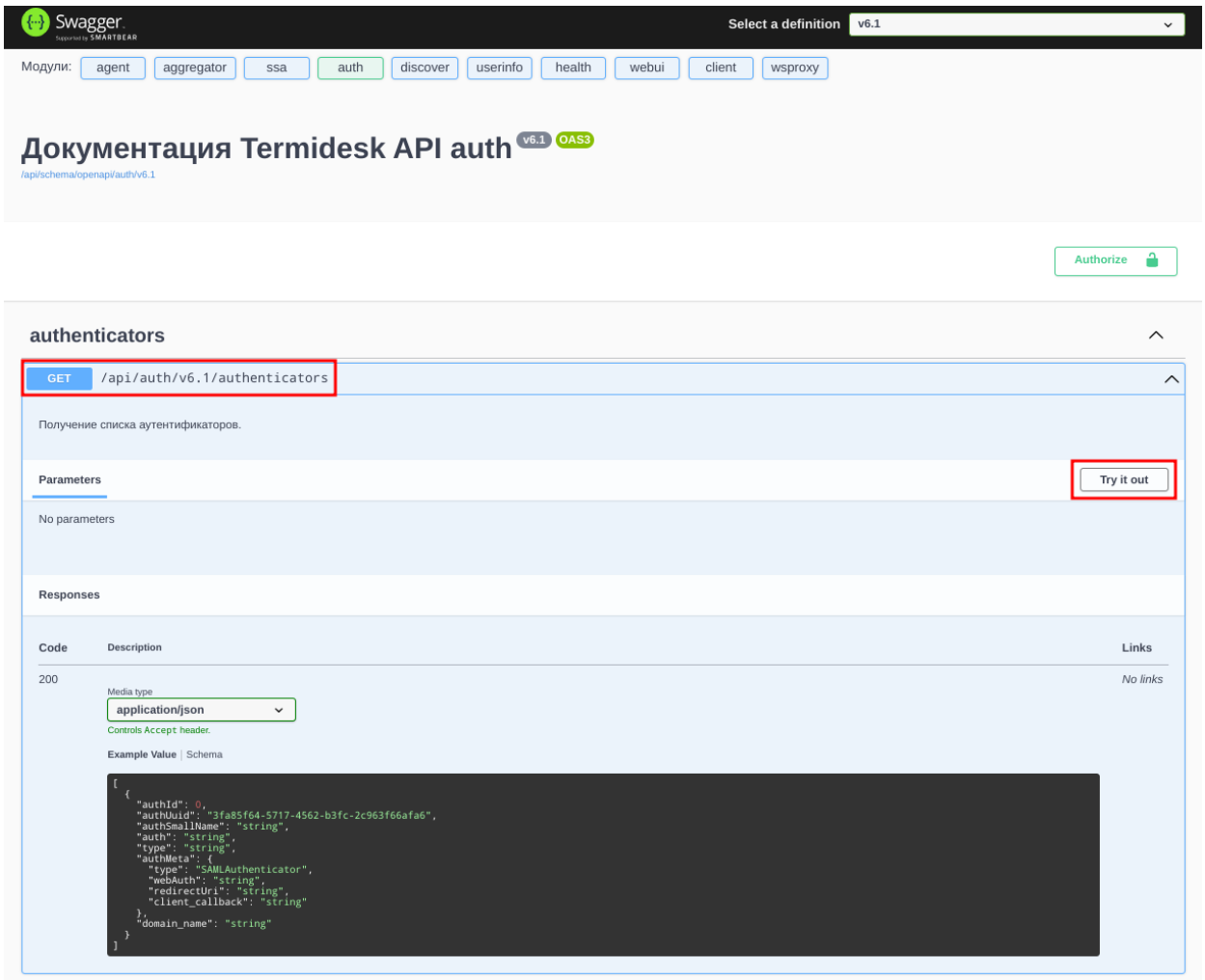


Рисунок 218. Расположение экранных кнопок для получения доступа к формированию запроса

- отправить запрос на выполнение экранной кнопкой **[Execute]** (см. рисунок Расположение экранной кнопки для формирования запроса).

После нажатия будет отображена также команда для запроса через `curl`.

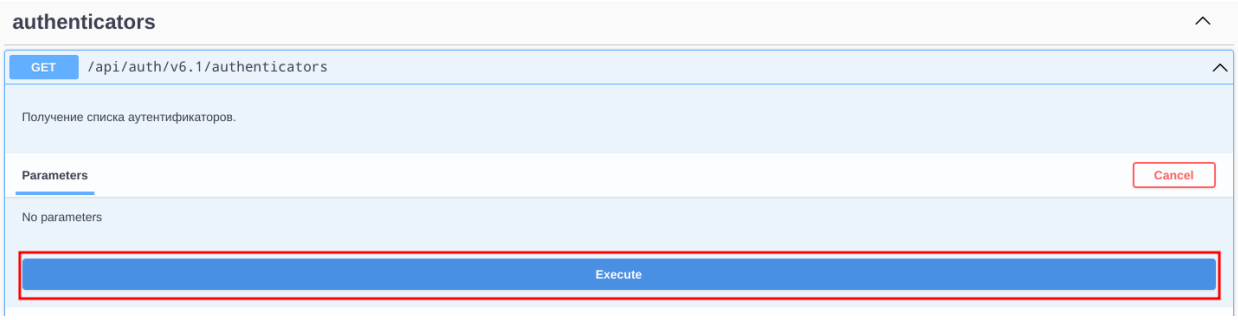


Рисунок 219. Расположение экранной кнопки для формирования запроса

Команды компонента «Универсальный диспетчер»

Доступные команды модуля «agent»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «agent»).

Таблица 326. Перечень URL-команд модуля «agent»

URL-команда	Тип	Описание
/api/agent/v7.0/{uuid}/assistant/events/connect	POST	Добавление записи о подключении к сеансу или отключении от сеанса «Удаленного помощника» в журнал РМ
/api/agent/v7.0/{uuid}/events/connected	PATCH	Уведомление о подключении пользователя к РМ
/api/agent/v7.0/{uuid}/events/disconnected	PATCH	Уведомление об отключении пользователя от РМ
/api/agent/v7.0/{uuid}/events/loggedin	PATCH	Уведомление о входе пользователя
/api/agent/v7.0/{uuid}/events/loggedout	PATCH	Уведомление о выходе пользователя
/api/agent/v7.0/{uuid}/legacy/osmanager	PATCH	Обработка внутренних процессов РМ
/api/agent/v7.0/{uuid}/log	PATCH	Добавление записи в журнал РМ
/api/agent/v7.0/{uuid}/notifyComms	PATCH	Сохранение URL для коммуникации в параметрах РМ
/api/agent/v7.0/{uuid}/policies	GET	Получение информации о политиках РМ
/api/agent/v7.0/{uuid}/scripts	GET	Получение информации о скриптах РМ
/api/agent/v7.0/{uuid}/service_info	GET	Получение информации о РМ
/api/agent/v7.0/{uuid}/settings	GET	Получение информации о настройках РМ
/api/agent/v7.0/{uuid}/version	PATCH	Сохранение версии агента
/api/agent/v7.0/boot_mode	GET	Запрос режима загрузки при работе ВМ с сетевым диском
/api/agent/v7.0/boot_script	GET	Запрос скрипта загрузки по MAC при работе ВМ с сетевым диском
/api/agent/v7.0/init	POST	Инициализация агента на РМ
/api/agent/v7.0/qcow_action	GET	Запрос на действие с qcow2 диском при выходе пользователя из ОС. Используется для РМ, созданных на основе шаблона «Сетевая загрузка» в поставщике ресурсов VMware. Возможные значения повторяют значения политики «Действие при выходе пользователя из ОС (RDP, SPICE, TERA)»: • «1» - «Не задано»; • «2» - «Удалить рабочее место»; • «3» - «Не сохранять изменения»; • «4» - «Не сохранять изменения и назначение ВРМ»; • «5» - «Перезагрузить ВРМ»
/api/agent/v7.0/test	PATCH	Запрос проверки корректности мастер-ключа
/api/agent/v7.0/settings	GET	Получение настроек компонента «Ретранслятор»

Доступные команды модуля «aggregator»

Команды, связанные со списками фондов, ассоциированных с определенными доменами аутентификации

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «aggregator», связанных с доменами аутентификации). Команды приведены для последней опубликованной версии API.

Доступность функционала зависит от типа редакции Termidesk VDI.

Таблица 327. Перечень URL-команд модуля «aggregator», связанных с доменами аутентификации

URL-команда	Тип	Описание
`/api/aggregator/v7.0/authenticators`	GET	Возвращает список доменов аутентификации
`/api/aggregator/v7.0/authenticators/{small_name}`	GET	Возвращает домен аутентификации, имеющего короткое наименование `{small_name}`
`/api/aggregator/v7.0/authenticators/{small_name}/permissions`	GET	Возвращает список разрешений для пользователя домена аутентификации `{small_name}`
`/api/aggregator/v7.0/authenticators/{small_name}/services`	GET	Возвращает список фондов, ассоциированных с доменом аутентификации, имеющего короткое наименование `{small_name}`

Команды, связанные со списками сертификатов

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «aggregator», связанных с сертификатами). Команды приведены для последней опубликованной версии API.

Таблица 328. Перечень URL-команд модуля «aggregator», связанных с сертификатами

URL-команда	Тип	Описание
`/api/aggregator/v7.0/certificates`	GET	Получение списка сертификатов
`/api/aggregator/v7.0/certificates/{id}`	GET	Получение сертификата с идентификатором `{id}`

Команды, связанные с предоставлением ресурсов

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «aggregator», связанных с получением ресурсов). Команды приведены для последней опубликованной версии API.

Таблица 329. Перечень URL-команд модуля «aggregator», связанных с получением ресурсов

URL-команда	Тип	Описание
`/api/aggregator/v7.0/enable/{service}/{transport}`	GET	API для работы с TicketStore

Команды, связанные с проверкой состояния

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «aggregator», связанных с проверкой состояния). Команды приведены для последней опубликованной версии API.

Таблица 330. Перечень URL-команд модуля «aggregator», связанных с проверкой состояния

URL-команда	Тип	Описание
/api/aggregator/v7.0/health_check	GET	Проверка состояния портала «Агрегатор»

Доступные команды модуля «auth»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «auth»).

Таблица 331. Перечень URL-команд модуля «auth»

URL-команда	Тип	Описание
/api/auth/v7.0/authenticators	GET	Получение списка аутентификаторов
/api/auth/v7.0/authenticators/{auth_uuid}/pkinit/finalize	PATCH	Завершение аутентификации Kerberos PKINIT
/api/auth/v7.0/authenticators/{auth_uuid}/pkinit/login	PATCH	Инициализация аутентификации Kerberos PKINIT и получение данных на подпись
/api/auth/v7.0/authenticators/{auth_uuid}/pkinit/raw	PATCH	Прямой запрос на сервер Kerberos PKINIT с подписанным сертификатом
/api/auth/v7.0/jwtauth	POST	Авторизация «Агрегатора» на «Универсальном диспетчере». В ответ на подписанный «Агрегатором» токен «Универсальный диспетчер» возвращает сеансовый ключ (токен)
/api/auth/v7.0/login	POST	Аутентификация пользователя на базе аутентификатора, логина и пароля. При отправке запроса необходимо обязательно указать один из параметров: • «authId»; • «auth»; • «authSmallName»
/api/auth/v7.0/login/2fa	POST	Двухфакторная аутентификация пользователя на базе аутентификатора, логина и пароля. При отправке запроса необходимо обязательно указать один из параметров: • «authId»; • «auth»; • «authSmallName»
/api/auth/v7.0/logout	POST	Прекращение действие токена/сессии пользователя. Токен аутентификации должен передаваться в заголовке X-Auth-Token
/api/auth/v7.0/settings	GET	Получение глобальных настроек сервера

Доступные команды модуля «client»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «client»).

Таблица 332. Перечень URL-команд модуля «client»

URL-команда	Тип	Описание
/api/client/v7.0/component_info/{uuid}	PATCH	API для получения дополнительной информации о подключении пользователя
/api/client/v7.0/connectionInfo/{uuid}	GET	API для выдачи параметров подключения компоненту «Клиент» для протоколов RDP и SPICE
/api/client/v7.0/enable/{service}/{transport}	GET	API для работы с TicketStore
/api/client/v7.0/enable_async	POST	API для создания задачи проверки статуса РМ по запросу компонента «Клиент»
/api/client/v7.0/enable_async/{uuid}	GET	API для выдачи информации о состоянии задачи проверки статуса РМ компоненту «Клиент»
/api/client/v7.0/images/srvimg/{image_id}	GET	API для выдачи изображения по идентификатору, либо для протокола доставки, либо установленное по умолчанию
/api/client/v7.0/images/transicon/{image_id}	GET	API для выдачи изображения по идентификатору для протокола доставки
/api/client/v7.0/preconnectionInfo/{uuid}	GET	API для выдачи параметров подключения компоненту «Клиент». Компонент «Клиент» использует метод для проверки готовности сервиса к подключению и уточнения используемого протокола. По полученным данным принимает решение: завершить неудачное подключение, подождать и повторить, подключаться новым/старым методом
/api/client/v7.0/reconnect	POST	Обновляет ссылку для переподключения к сессии РМ
/api/client/v7.0/service/{uuid}/machine_state	PATCH	Перезагружает РМ
/api/client/v7.0/servicesList	GET	Получение списка доступных фондов
/api/client/v7.0/weblink/{id_service}/{id_transport}	GET	Возвращает параметры подключения к РМ по конкретному протоколу доставки
/api/client/v7.0/workplaces	GET	Получение списка назначенных РМ

Доступные команды модуля «discover»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «discover»).

Таблица 333. Перечень URL-команд модуля «discover»

URL-команда	Тип	Описание
/api/discover/	GET	Возвращает список модулей API, предоставляемых компонентом «Универсальный диспетчер»

Доступные команды модуля «health»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «health»).

Таблица 334. Перечень URL-команд модуля «health»

URL-команда	Тип	Описание

/api/health/check	GET	Проверка состояния сервера. Собираются общие показатели и набор числовых метрик.
		
		Для авторизации при обращении к запросу используется токен, определенный в параметре HEALTH_CHECK_ACCESS_KEY конфигурационного файла /etc/opt/termidesk-vdi/termidesk.conf.
		
		Оценка состояния должна производиться в инициаторе запроса на основе набора правил и пороговых значений с учетом конкретной конфигурации системы.
		
		Для разных конфигураций системы один и тот же показатель в абсолютном выражении может соответствовать состоянию и «PASS», и «FAIL».
		
		Формат запроса:
		
		`curl --insecure -v -s -X 'GET' \`
		`  'https://$\{hostname}:$\{health_port}/api/health/check' \`
		`  -H 'accept: application/json' \`
		`  -H 'Authorization: Token $\{health_check_access_key}'`
		
		где:
		
		--insecure - отключение проверки валидности сертификатов. Выполнение запроса без использования проверки SSL допустимо только на тестовых стендах. В производственной среде необходимо установить валидные сертификаты;
		
		${hostname} - сетевой адрес или полное доменное имя узла;
		
		${health_port} - порт для запросов проверки состояния. По умолчанию используется порт веб-сервера, 443;
		
		${health_check_access_key} - токен, определенный в параметре HEALTH_CHECK_ACCESS_KEY файла /etc/opt/termidesk-vdi/termidesk.conf

URL-команда	Тип	Описание

/api/health/metrics	GET	Доступность функционала зависит от типа редакции Termidesk VDI.
		
		Возвращает список метрик сервера. Для авторизации при обращении к запросу используется токен, определенный в параметре METRICS_ACCESS_KEY конфигурационного файла /etc/opt/termidesk-vdi/termidesk.conf.
		
		Формат запроса:
		
		`curl --insecure -v -s -X 'GET' \`
		`  'https://$\{hostname}:$\{health_port}/api/health/metrics' \`
		`  -H 'accept: application/json' \`
		`  -H 'Authorization: Token $\{metrics_access_key}'`
		
		где:
		
		--insecure - отключение проверки валидности сертификатов. Выполнение запроса без использования проверки SSL допустимо только на тестовых стендах. В производственной среде необходимо установить валидные сертификаты;
		
		${hostname} - сетевой адрес или полное доменное имя узла;
		
		${health_port} - порт для запросов проверки состояния. По умолчанию используется порт веб-сервера, 443;
		
		${metrics_access_key} - токен, определенный в переменной METRICS_ACCESS_KEY файла /etc/opt/termidesk-vdi/termidesk.conf.
		
		Информацию по всем возвращаемым значениям можно получить в документации библиотеки psutil на сайте: https://psutil.readthedocs.io/en/latest.
		
		Вид возвращаемого списка метрик приведен после таблицы

Вид возвращаемого списка метрик:

```
# Версия компонента
version_info{version="5.1-dev-HEAD-20240614064304-c1d6651db"} 1.0
# Версия ОС
system_info{machine="x86_64",os="Linux 5.10.190-1-hardened",version="#astra1+ci6
SMP Fri Oct 6 14:47:06 UTC 2023"} 1.0
# Период в секундах, в течение которого система функционирует без проблем
uptime_seconds 66686.97834658623
# Общая загрузка процессора в процентах
cpu_total_percent 4.8
# Общее использование физической памяти в процентах
virtual_memory_total_percent 40.5
# Количество операций чтения с диска
disk_read_count 68201.0
# Количество операций записи на диск
disk_write_count 729848.0
# Число прочитанных с диска байт
```

```
disk_read_bytes 2.094142464e+09
# Число записанных на диск байт
disk_write_bytes 7.54249728e+09
# Общий размер физической памяти в байтах
virtual_memory_total_bytes 4.117311488e+09
# Размер доступной физической памяти в байтах
virtual_memory_available_bytes 2.447736832e+09
# Размер используемой физической памяти в байтах
virtual_memory_used_bytes 1.303724032e+09
# Размер свободной физической памяти в байтах
virtual_memory_free_bytes 3.78679296e+08
# Общий размер диска в байтах
disk_total_bytes 1.5742214144e+010
# Используемый размер диска в байтах
disk_used_bytes 1.4512279552e+010
# Свободный размер диска в байтах
disk_free_bytes 4.07957504e+08
# Количество авторизованных пользователей в портале пользователя
user_session_count 1.0
# Количество авторизованных администраторов в портале администратора
admin_session_count 17.0
# Количество сеансов пользователей РМ
VM_users_sessions{type="in_use"} 1.0
VM_users_sessions{type="vacant"} 4.0
# Количество сеансов пользователей терминальных сессий
RDS_STAL_users_sessions{type="in_use"} 1.0
RDS_STAL_users_sessions{type="vacant"} 0.0
# Общее количество виртуальных машин
total_vms 48.0
# Количество виртуальных машин с ошибкой запуска
failed_to_start_vms 38.0
# Количество зависших виртуальных машин
stuck_vms 0.0
# Количество незарегистрированных на «Универсальном диспетчере» «Агентов»
unregistered_agents 41.0
```

Доступные команды модуля «ssa»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «ssa»).

Таблица 335. Перечень URL-команд модуля «ssa»

URL-команда	Тип	Описание
/api/ssa/v7.0/event	POST	Регистрация событий от «Сессионного агента»
/api/ssa/v7.0/settings	GET	Получение настроек компонента «Ретранслятор»

Доступные команды модуля «userinfo»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «userinfo»).

Таблица 336. Перечень URL-команд модуля «userinfo»

URL-команда	Тип	Описание
`/api/userinfo/themes`	GET	Получение параметров брендирования
`/api/userinfo/themes`	PUT	Обновление параметров брендирования
`/api/userinfo/`	GET	Получение информации о пользователе

Доступные команды модуля «webui»

Команды, связанные со списками устройств доступа

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных со списками устройств доступа).

Версия API `/api/webui/draft/` будет удалена в следующем релизе.

Опубликована новая версия API `/api/webui/server`.

Таблица 337. Перечень URL-команд, связанных со списками устройств доступа

URL-команда	Тип	Описание
`/api/webui/server/access-devices`	GET	Возвращает список устройств доступа
`/api/webui/server/access-devices/{uuid}`	GET	Возвращает устройство доступа с идентификатором `{uuid}`
`/api/webui/server/access-devices/{uuid}/{status}`	PATCH	Изменяет статус устройства доступа с идентификатором `{uuid}`

Команды, связанные со списками доступа

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных со списками доступа).

Таблица 338. Перечень URL-команд, связанных со списками доступа

URL-команда	Тип	Описание
`/api/webui/server/acl`	GET	Возвращает список объектных разрешений
`/api/webui/server/acl/{group_pk}/{data_type}/{object_pk}`	GET	Возвращает набор операций для управления объектными разрешениями
`/api/webui/server/acl/{group_pk}/{data_type}/{object_pk}`	POST	Обновляет набор операций для управления объектными разрешениями
`/api/webui/server/acl/{group_pk}/{data_type}/{object_pk}`	PUT	Обновляет набор операций для управления объектными разрешениями
`/api/webui/server/acl/{group_pk}/{data_type}/{object_pk}`	DELETE	Удаляет объектное разрешение
`/api/webui/server/acl/export`	GET	Формирует файл экспорта объектных разрешений
`/api/webui/server/acl/export`	POST	Получает файл экспорта объектных разрешений
`/api/webui/server/acl/gui/{data_type}`	GET	Возвращает описание для графического интерфейса
`/api/webui/server/acl/permissions/{data_type}`	GET	Возвращает список разрешений для переданного типа объекта

URL-команда	Тип	Описание
/api/webui/server/acl/types	GET	Возвращает список доступных типов объектных разрешений

Команды, связанные с объектами инфраструктуры

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с объектами инфраструктуры).

Таблица 339. Перечень URL-команд, связанных с объектами инфраструктуры

URL-команда	Тип	Описание
/api/webui/server/appnodes/brokers	GET	Возвращает список объектов инфраструктуры («Универсальных диспетчеров»)
/api/webui/server/appnodes/brokers/{broker_uuid}/certificate/gui	GET	Управляет сертификатами объекта («Универсальный диспетчер»)
/api/webui/server/appnodes/brokers/{broker_uuid}/certificate/set	PATCH	Обновляет сертификаты объекта («Универсальный диспетчер»)
/api/webui/server/appnodes/brokers/{uuid}	DELETE	Удаляет объект инфраструктуры («Универсальный диспетчер») с идентификатором {uuid}
/api/webui/server/appnodes/brokers/{uuid}/metrics	GET	Возвращает список метрик объектов инфраструктуры («Универсальных диспетчеров»)
/api/webui/server/appnodes/brokers/{uuid}/tags	GET	Возвращает список тегов объектов инфраструктуры («Универсальных диспетчеров»)
/api/webui/server/appnodes/brokers/export	GET	Формирует файл экспорта объектов инфраструктуры («Универсальных диспетчеров»)
/api/webui/server/appnodes/brokers/export	POST	Получает файл экспорта объектов инфраструктуры («Универсальных диспетчеров»)
/api/webui/server/appnodes/gateways	GET	Возвращает список объектов инфраструктуры («Шлюзов»)
/api/webui/server/appnodes/gateways/{broker_uuid}/certificate/gui	GET	Управляет сертификатами объекта («Шлюз»)
/api/webui/server/appnodes/gateways/{broker_uuid}/certificate/set	PATCH	Обновляет сертификаты объекта («Шлюз»)
/api/webui/server/appnodes/gateways/{uuid}	DELETE	Удаляет объект инфраструктуры («Шлюз») с идентификатором {uuid}
/api/webui/server/appnodes/gateways/{uuid}/metrics	PATCH	Возвращает список метрик объектов инфраструктуры («Шлюзов»)
/api/webui/server/appnodes/gateways/{uuid}/tags	PATCH	Возвращает список тегов объектов инфраструктуры («Шлюзов»)
/api/webui/server/appnodes/gateways/export	GET	Формирует файл экспорта объектов инфраструктуры («Шлюзов»)
/api/webui/server/appnodes/gateways/export	POST	Получает файл экспорта объектов инфраструктуры («Шлюзов»)
/api/webui/server/appnodes/journal_storages	GET	Возвращает список объектов инфраструктуры («Хранилищ журналов»)
/api/webui/server/appnodes/journal_storages	POST	Обновляет список объектов инфраструктуры («Хранилищ журналов»)
/api/webui/server/appnodes/journal_storages/{uuid}	GET	Возвращает объект инфраструктуры («Хранилище журналов») с идентификатором {uuid}
/api/webui/server/appnodes/journal_storages/{uuid}	PUT	Обновляет объект инфраструктуры («Хранилище журналов») с идентификатором {uuid}

URL-команда	Тип	Описание
/api/webui/server/appnodes/journal_storages/{uuid}	DELETE	Удаляет объект инфраструктуры («Хранилище журналов») с идентификатором {uuid}
/api/webui/server/appnodes/journal_storages/{uuid}/activation	PATCH	Меняет состояние объекта инфраструктуры («Хранилища журналов») с идентификатором {uuid}
/api/webui/server/appnodes/journal_storages/export	GET	Формирует файл экспорта объектов инфраструктуры («Хранилищ журналов»)
/api/webui/server/appnodes/journal_storages/export	POST	Получает файл экспорта объектов инфраструктуры («Хранилищ журналов»)
/api/webui/server/appnodes/journal_storages/gui	GET	Возвращает описание для графического интерфейса для объектов инфраструктуры («Хранилищ журналов»)
/api/webui/server/appnodes/portals	GET	Возвращает список объектов инфраструктуры («Порталов»)
/api/webui/server/appnodes/portals/{broker_uuid}/certificate/gui	GET	Управляет сертификатами объекта («Порталов»)
/api/webui/server/appnodes/portals/{broker_uuid}/certificate/set	PATCH	Обновляет сертификаты объекта («Порталов»)
/api/webui/server/appnodes/portals/{uuid}	DELETE	Удаляет объект инфраструктуры («Портал») с идентификатором {uuid}
/api/webui/server/appnodes/portals/{uuid}/metrics	PATCH	Возвращает список метрик объектов инфраструктуры («Порталов»)
/api/webui/server/appnodes/portals/{uuid}/tags	PATCH	Возвращает список тегов объектов инфраструктуры («Порталов»)
/api/webui/server/appnodes/portals/export	GET	Формирует файл экспорта объектов инфраструктуры («Порталов»)
/api/webui/server/appnodes/portals/export	POST	Получает файл экспорта объектов инфраструктуры («Порталов»)
/api/webui/server/appnodes/repeaters	GET	Возвращает список объектов инфраструктуры («Ретрансляторов»)
/api/webui/server/appnodes/repeaters	POST	Обновляет список объектов инфраструктуры («Ретрансляторов»)
/api/webui/server/appnodes/repeaters/{uuid}	GET	Возвращает объект инфраструктуры («Ретранслятор») с идентификатором {uuid}
/api/webui/server/appnodes/repeaters/{uuid}	PUT	Обновляет объект инфраструктуры («Ретранслятор») с идентификатором {uuid}
/api/webui/server/appnodes/repeaters/{uuid}	DELETE	Удаляет объект инфраструктуры («Ретранслятор») с идентификатором {uuid}
/api/webui/server/appnodes/repeaters/{uuid}/activation	PATCH	Меняет состояние объекта инфраструктуры («Ретранслятора») с идентификатором {uuid}
/api/webui/server/appnodes/repeaters/export	GET	Формирует файл экспорта объектов инфраструктуры («Ретрансляторов»)
/api/webui/server/appnodes/repeaters/export	POST	Получает файл экспорта объектов инфраструктуры («Ретрансляторов»)
/api/webui/server/appnodes/repeaters/gui	GET	Возвращает описание для графического интерфейса для объектов инфраструктуры («Ретрансляторов»)
/api/webui/server/appnodes/vmcontrollers	GET	Возвращает список объектов инфраструктуры («Менеджеров рабочих мест»)
/api/webui/server/appnodes/vmcontrollers/{broker_uuid}/certificate/gui	GET	Управляет сертификатами объекта («Менеджер рабочих мест»)

URL-команда	Тип	Описание
/api/webui/server/appnodes/vmcontrollers/{broker_uuid}/certificate/set	PATCH	Обновляет сертификаты объекта («Менеджер рабочих мест»)
/api/webui/server/appnodes/vmcontrollers/{uuid}	DELETE	Удаляет объект инфраструктуры («Менеджер рабочих мест») с идентификатором {uuid}
/api/webui/server/appnodes/vmcontrollers/{uuid}/metrics	GET	Возвращает список метрик объектов инфраструктуры («Менеджеров рабочих мест»)
/api/webui/server/appnodes/vmcontrollers/{uuid}/tags	GET	Возвращает список тегов объектов инфраструктуры («Менеджеров рабочих мест»)
/api/webui/server/appnodes/vmcontrollers/export	GET	Формирует файл экспорта объектов инфраструктуры («Менеджеров рабочих мест»)
/api/webui/server/appnodes/vmcontrollers/export	POST	Получает файл экспорта объектов инфраструктуры («Менеджеров рабочих мест»)

Команды, связанные с журналами событий

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с журналами событий).

Таблица 340. Перечень URL-команд, связанных с журналами событий

URL-команда	Тип	Описание
/api/webui/server/audit/events	GET	Возвращает список событий аудита
/api/webui/server/audit/events/export	GET	Формирует файл экспорта событий журнала
/api/webui/server/audit/events/export	POST	Получает файл экспорта событий журнала
/api/webui/server/audit/events/types	GET	Возвращает список доступных типов событий аудита

Команды, связанные с доменами аутентификации

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с доменами аутентификации).

Таблица 341. Перечень URL-команд, связанных с доменами аутентификации

URL-команда	Тип	Описание
/api/webui/server/authenticators	GET	Возвращает список доменов аутентификации
/api/webui/server/authenticators	POST	Создает домен аутентификации
/api/webui/server/authenticators/{auth_uuid}/groups	GET	Возвращает список групп домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/groups	POST	Создает группу домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/groups/{group_uuid}/policies	GET	Возвращает список политик группы
/api/webui/server/authenticators/{auth_uuid}/groups/{group_uuid}/policies	POST	Создает политику группы
/api/webui/server/authenticators/{auth_uuid}/groups/{group_uuid}/policies/{uuid}	GET	Возвращает политику группы
/api/webui/server/authenticators/{auth_uuid}/groups/{group_uuid}/policies/{uuid}	PUT	Изменяет значение политики группы
/api/webui/server/authenticators/{auth_uuid}/groups/{group_uuid}/policies/{uuid}	DELETE	Удаляет политику группы. Будет использоваться глобальная политика

URL-команда	Тип	Описание
/api/webui/server/authenticators/{auth_uuid}/groups/{group_uuid}/policies/gui/{policy_type}	GET	Возвращает описание для графического интерфейса политики с типом {policy_type}
/api/webui/server/authenticators/{auth_uuid}/groups/{uuid}	GET	Возвращает группу с идентификатором {uuid} домена аутентификации с идентификатором {auth_uuid}
/api/webui/server/authenticators/{auth_uuid}/groups/{uuid}	PUT	Обновляет группу домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/groups/{uuid}	DELETE	Удаляет группу домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/groups/{uuid}/servicesPools	GET	Возвращает список РМ группы домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/groups/{uuid}/users	GET	Возвращает список пользователей группы домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/groups/external	GET	Возвращает список доступных групп для домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/groups/gui/{group_type}	GET	Возвращает описание для графического интерфейса группы с типом {group_type}
/api/webui/server/authenticators/{auth_uuid}/groups/types	GET	Возвращает список доступных типов групп домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/log	GET	Возвращает журнал домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/users	GET	Возвращает список пользователей домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/users	POST	Создает пользователя домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/users/{uuid}	GET	Возвращает пользователя с идентификатором {uuid} домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/users/{uuid}	PUT	Обновляет пользователя домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/users/{uuid}	DELETE	Удаляет пользователя домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/users/{uuid}/log	GET	Возвращает журнал пользователя домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/users/{uuid}/servicesPools	GET	Возвращает список РМ пользователя домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/users/{uuid}/userServices	GET	Возвращает список ассоциированных виртуальных машин (ВМ) для пользователя домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/users/bulk_destroy	PATCH	Удаляет пользователей домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/users/bulk_update	PATCH	Обновляет пользователей домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/users/external	GET	Возвращает список доступных пользователей для домена аутентификации
/api/webui/server/authenticators/{auth_uuid}/users/gui	GET	Возвращает описание для графического интерфейса
/api/webui/server/authenticators/{auth_uuid}/users/types	GET	Возвращает список доступных типов пользователей домена аутентификации
/api/webui/server/authenticators/{uuid}	GET	Возвращает домен аутентификации
/api/webui/server/authenticators/{uuid}	PUT	Обновляет домен аутентификации

URL-команда	Тип	Описание
/api/webui/server/authenticators/{uuid}	DELETE	Удаляет домен аутентификации
/api/webui/server/authenticators/{uuid}/attribute	PATCH	Добавить, изменить или удалить атрибут домена для сохранения в учетной записи пользователя
/api/webui/server/authenticators/gui/{data_type}	GET	Возвращает описание для графического интерфейса домена аутентификации с типом {data_type}
/api/webui/draft/authenticators/test/{type}	POST	Тестирует параметры домена аутентификации
/api/webui/draft/authenticators/types	GET	Возвращает список доступных типов доменов аутентификации

Команды, связанные с панелью мониторинга

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с панелью мониторинга).

Таблица 342. Перечень URL-команд, связанных с панелью мониторинга

URL-команда	Тип	Описание
/api/webui/server/dashboard	GET	Возвращает список объектов панели мониторинга
/api/webui/server/dashboard/admin	GET	Возвращает список объектов панели мониторинга для «Портала администратора»
/api/webui/server/dashboard/user	GET	Возвращает список объектов панели мониторинга для «Портала пользователя»

Команды, связанные с изображениями гостевых ОС

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с изображением гостевых ОС).

Таблица 343. Перечень URL-команд, связанных с изображением гостевых ОС

URL-команда	Тип	Описание
/api/webui/server/gallery/images	GET	Возвращает список изображений
/api/webui/server/gallery/images	POST	Создает изображение
/api/webui/server/gallery/images/{uuid}	GET	Возвращает изображение с идентификатором {uuid}
/api/webui/server/gallery/images/{uuid}	PUT	Обновляет изображение
/api/webui/server/gallery/images/{uuid}	DELETE	Удаляет изображение
/api/webui/server/gallery/images/gui	GET	Возвращает описание для графического интерфейса
/api/webui/server/gallery/images/srvimg/{image_id}	GET	Возвращает изображение по идентификатору, либо для протокола доставки, либо установленное по умолчанию
/api/webui/server/gallery/images/transicon/{image_id}	GET	Возвращает изображение для протокола доставки

Команды, связанные с профилями шлюзов

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с профилями шлюзов).

Таблица 344. Перечень URL-команд, связанных с профилями шлюзов

URL-команда	Тип	Описание
/api/webui/server/gateways	GET	Возвращает список профилей шлюзов
/api/webui/server/gateways	POST	Создает профиль шлюза
/api/webui/server/gateways/{uuid}	GET	Возвращает профиль шлюза
/api/webui/server/gateways/{uuid}	PUT	Обновляет профиль шлюза
/api/webui/server/gateways/{uuid}	DELETE	Удаляет профиль шлюза
/api/webui/server/gateways/gui/{gateway_type}	GET	Возвращает описание для графического интерфейса профиля шлюза с типом {gateway_type}
/api/webui/server/gateways/test/{gateway_type}	POST	Тестирует параметры профиля шлюза
/api/webui/server/gateways/types	GET	Возвращает список типов профилей шлюзов

Команды, связанные с графическим интерфейсом

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с вызовом функций графического интерфейса).

Таблица 345. Перечень URL-команд, связанных с вызовом функций графического интерфейса

URL-команда	Тип	Описание
/api/webui/server/gui/callback/{callback}	GET	Предоставляет доступ к callback-функциям графического интерфейса

Команды, связанные с получением индекса

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с получением индекса).

Таблица 346. Перечень URL-команд, связанных с получением индекса

URL-команда	Тип	Описание
/api/webui/server	GET	Определяет текущую версию REST API

Команды, связанные с лицензией

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с лицензией).

Таблица 347. Перечень URL-команд, связанных с лицензией

URL-команда	Тип	Описание
/api/webui/server/license	POST	Загружает новую лицензию
/api/webui/server/license/brokers	GET	Возвращает список идентификаторов узлов фермы Termidesk VDI (зарегистрированных в разделе «Инфраструктура»), для которых нужна лицензия. Список узлов в лицензии и по этой URL-команде будет различаться, если произошло изменение в составе узлов, а лицензия не была обновлена

URL-команда	Тип	Описание
/api/webui/server/license/history	GET	Генерирует и возвращает отчет об использованных лицензиях в данной инсталляции
/api/webui/server/license/info	GET	Получает информацию о лицензии
/api/webui/server/license/remove	DELETE	Удаляет лицензию
/api/webui/server/license/stats/licensed_connections/{interval}	GET	Возвращает статистику лицензируемых подключений по: • часам за последние 7 дней с учетом часового пояса сервера; • дням за последние 365 дней с учетом часового пояса сервера; • месяцам за весь период работы сервера
api/webui/server/license/stats/licensed_users/{interval}	GET	Возвращает статистику лицензируемых пользователей по: • часам за последние 7 дней с учетом часового пояса сервера; • дням за последние 365 дней с учетом часового пояса сервера; • месяцам за весь период работы сервера

Команды, связанные с отображением журнала

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с отображением журнала).

Таблица 348. Перечень URL-команд, связанных с отображением журнала

URL-команда	Тип	Описание
/api/webui/server/logs/journal	GET	Возвращает централизованный журнал
/api/webui/server/logs/journal/export	GET	Формирует файл экспорта событий журнала

Команды, связанные с функциями мониторинга

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с функциями мониторинга).

Таблица 349. Перечень URL-команд, связанных с функциями мониторинга

URL-команда	Тип	Описание
/api/webui/server/monitoring	GET	Возвращает все журналы в виде списка
/api/webui/server/monitoring/export	GET	Формирует файл экспорта событий журнала
/api/webui/server/monitoring/export	POST	Получает файл экспорта событий журнала

Команды, связанные с аутентификацией на основе адресов сети

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с IP-аутентификацией).

Таблица 350. Перечень URL-команд, связанных с IP-аутентификацией

URL-команда	Тип	Описание
/api/webui/server/networks	GET	Возвращает список сетей

URL-команда	Тип	Описание
/api/webui/server/networks	POST	Создает сеть
/api/webui/server/networks/{network_uuid}/policies	GET	Возвращает список политик сети
/api/webui/server/networks/{network_uuid}/policies	POST	Создает политику сети
/api/webui/server/networks/{network_uuid}/policies/{uuid}	GET	Возвращает политику сети
/api/webui/server/networks/{network_uuid}/policies/{uuid}	PUT	Изменяет значение политики сети
/api/webui/server/networks/{network_uuid}/policies/{uuid}	DELETE	Удаляет политику сети. Будет использоваться глобальная политика
/api/webui/server/networks/{network_uuid}/policies/gui/{policy_type}	GET	Возвращает описание для графического интерфейса политики сети с типом {policy_type}
/api/webui/server/networks/{uuid}	GET	Возвращает сеть с идентификатором {uuid}
/api/webui/server/networks/{uuid}	PUT	Обновляет сеть
/api/webui/server/networks/{uuid}	DELETE	Удаляет сеть
/api/webui/server/networks/gui	GET	Возвращает описание для графического интерфейса сети

Команды, связанные с параметрами гостевых ОС

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с параметрами гостевых ОС).

Таблица 351. Перечень URL-команд, связанных с параметрами гостевых ОС

URL-команда	Тип	Описание
/api/webui/server/osmanagers	GET	Возвращает список параметров гостевых ОС
/api/webui/server/osmanagers	POST	Создает параметры гостевых ОС
/api/webui/server/osmanagers/{uuid}	GET	Возвращает параметры гостевых ОС с идентификатором {uuid}
/api/webui/server/osmanagers/{uuid}	PUT	Обновляет параметры гостевых ОС
/api/webui/server/osmanagers/{uuid}	DELETE	Удаляет параметры гостевых ОС
/api/webui/server/osmanagers/gui/{data_type}	GET	Возвращает описание для графического интерфейса для параметров с типом {data_type}
/api/webui/server/osmanagers/types	GET	Возвращает список типов параметров гостевых ОС

Команды, связанные с глобальными политиками

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с глобальными политиками).

Таблица 352. Перечень URL-команд, связанных с глобальными политиками

URL-команда	Тип	Описание
/api/webui/server/policies	GET	Список всех доступных политик
/api/webui/server/policies	POST	Управляет глобальными политиками

URL-команда	Тип	Описание
/api/webui/server/policies/{uuid}	GET	Получает информацию о политике с идентификатором {uuid}
/api/webui/server/policies/{uuid}	PUT	Меняет значение политики с идентификатором {uuid}
/api/webui/server/policies/{uuid}	DELETE	Сбрасывает значение глобальной политики с идентификатором {uuid}
/api/webui/server/policies/export	GET	Формирует файл экспорта политик
/api/webui/server/policies/export	POST	Получает файл экспорта политик
/api/webui/server/policies/gui/{policy_type}	GET	Возвращает спецификацию полей графического интерфейса для политики конкретного типа

Команды, связанные с поставщиками ресурсов

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с поставщиками ресурсов).

Таблица 353. Перечень URL-команд, связанных с поставщиками ресурсов

URL-команда	Тип	Описание
/api/webui/server/providers	GET	Возвращает список поставщиков ресурсов
/api/webui/server/providers	POST	Создает поставщика ресурсов
/api/webui/server/providers/{provider_uuid}/services	GET	Возвращает список шаблонов РМ поставщика ресурсов
/api/webui/server/providers/{provider_uuid}/services	POST	Создает шаблон РМ
/api/webui/server/providers/{provider_uuid}/services/{uuid}	GET	Возвращает шаблон РМ с идентификатором {uuid} поставщика ресурсов
/api/webui/server/providers/{provider_uuid}/services/{uuid}	PUT	Обновляет шаблон РМ с идентификатором {uuid} поставщика ресурсов
/api/webui/server/providers/{provider_uuid}/services/{uuid}	DELETE	Удаляет шаблон РМ с идентификатором {uuid} поставщика ресурсов
/api/webui/server/providers/{provider_uuid}/services/export	GET	Формирует файл экспорта шаблонов поставщика ресурсов
/api/webui/server/providers/{provider_uuid}/services/export	POST	Получает файл экспорта шаблонов поставщика ресурсов
/api/webui/server/providers/{provider_uuid}/services/gui/{service_type}	GET	Возвращает описание для графического интерфейса для шаблона РМ с типом {service_type} поставщика ресурсов
/api/webui/server/providers/{provider_uuid}/services/snapshot	POST	Создает снимок ВМ (снапшот)
/api/webui/server/providers/{provider_uuid}/services/types	GET	Возвращает список доступных типов шаблонов РМ поставщика ресурсов
/api/webui/server/providers/{uuid}	GET	Возвращает поставщика ресурсов с идентификатором {uuid}
/api/webui/server/providers/{uuid}	PUT	Обновляет поставщика ресурсов
/api/webui/server/providers/{uuid}	DELETE	Удаляет поставщика ресурсов
/api/webui/server/providers/{uuid}/maintenance	PATCH	Переводит поставщика ресурсов в режим техобсуживания

URL-команда	Тип	Описание
/api/webui/server/providers/export	GET	Формирует файл экспорта поставщиков ресурсов
/api/webui/server/providers/export	POST	Получает файл экспорта поставщиков ресурсов
/api/webui/server/providers/gui/{prov_type}	GET	Возвращает описание для графического интерфейса
/api/webui/server/providers/test/{prov_type}	POST	Тестирует параметры поставщика ресурсов
/api/webui/server/providers/types	GET	Возвращает список доступных типов поставщиков техобслуживания

Команды, связанные с управлением полномочиями (ролями)

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с управлением ролями).

Таблица 354. Перечень URL-команд, связанных с управлением ролями

URL-команда	Тип	Описание
/api/webui/server/rbac	GET	Возвращает список ролей
/api/webui/server/rbac	POST	Создает роль
/api/webui/server/rbac/{id}	GET	Возвращает роль
/api/webui/server/rbac/{id}	PUT	Обновляет роль
/api/webui/server/rbac/{id}	DELETE	Удаляет роль
/api/webui/server/rbac/gui	GET	Возвращает описание для графического интерфейса
/api/webui/server/rbac/permissions	GET	Возвращает список разрешений для ролей

Команды, связанные с отчетами

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с отчетами).

Таблица 355. Перечень URL-команд, связанных с отчетами

URL-команда	Тип	Описание
/api/webui/server/reports	GET	Возвращает список отчетов
/api/webui/server/reports	POST	Создает отчет
/api/webui/server/reports/{id}	GET	Возвращает отчет с идентификатором {id}
/api/webui/server/reports/{id}	PUT	Обновляет отчет с идентификатором {id}
/api/webui/server/reports/{id}	DELETE	Удаляет отчет с идентификатором {id}
/api/webui/server/reports/{id}/generate	GET	Генерирует отчет с идентификатором {id}
/api/webui/server/reports/{id}/generate/export	GET	Формирует файл экспорта отчета с идентификатором {id}
/api/webui/server/reports/{id}/generate/export	POST	Получает файл экспорта отчета с идентификатором {id}
/api/webui/server/reports/gui/{data_type}	GET	Возвращает описание для графического интерфейса
/api/webui/server/reports/types	GET	Возвращает список доступных типов отчетов

Команды, связанные с расписаниями

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с расписаниями).

Таблица 356. Перечень URL-команд, связанных с расписаниями

URL-команда	Тип	Описание
/api/webui/server/scheduler	GET	Возвращает список расписаний
/api/webui/server/scheduler	POST	Создает расписание
/api/webui/server/scheduler/{id}	GET	Возвращает расписание с идентификатором {id}
/api/webui/server/scheduler/{id}	PUT	Обновляет расписание с идентификатором {id}
/api/webui/server/scheduler/{id}	DELETE	Удаляет расписание с идентификатором {id}
/api/webui/server/scheduler/{id}/activation	PATCH	Меняет состояние расписания с идентификатором {id}

Команды, связанные со скриптами

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных со скриптами).

Таблица 357. Перечень URL-команд, связанных со скриптами

URL-команда	Тип	Описание
/api/webui/server/script	GET	Возвращает список скриптов
/api/webui/server/script	POST	Создает скрипт
/api/webui/server/script/{uuid}	GET	Возвращает скрипт
/api/webui/server/script/{uuid}	PUT	Обновляет скрипт
/api/webui/server/script/{uuid}	DELETE	Удаляет скрипт

Команды, связанные с фондами РМ

Доступные администратору URL-команды перечислены в таблице (см. таблицу [ереченьURLкомандсвязанныхсфондамиРМ]).

Таблица 358. Перечень URL-команд, связанных с фондами РМ

URL-команда	Тип	Описание
/api/webui/server/servicespools	GET	Возвращает список фондов РМ
/api/webui/server/servicespools	POST	Создает фонд РМ
/api/webui/server/servicespools/{servicespool_uuid}/cache	GET	Получение списка РМ, находящихся в кеше фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/cache/{uuid}	GET	Возвращает РМ, находящееся в кеше фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/cache/{uuid}	DELETE	Удаляет РМ, находящееся в кеше из фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/cache/{uuid}/assign	PATCH	Назначает пользователю РМ, находящееся в кеше
/api/webui/server/servicespools/{servicespool_uuid}/cache/{uuid}/assign/gui	GET	Возвращает описание для графического интерфейса РМ, находящегося в кеше
/api/webui/server/servicespools/{servicespool_uuid}/cache/{uuid}/execute_script	PATCH	Выполняет скрипт для РМ, находящегося в кеше

URL-команда	Тип	Описание
/api/webui/server/servicespools/{servicespool_uuid}/cache/{uuid}/log	GET	Возвращает журнал РМ, находящегося в кеше
/api/webui/server/servicespools/{servicespool_uuid}/cache/{uuid}/machine	PATCH	Управляет состоянием питания выбранного РМ, находящегося в кеше
/api/webui/server/servicespools/{servicespool_uuid}/cache/{uuid}/maintenance	PATCH	Управляет режимом техобслуживания РМ, находящегося в кеше
/api/webui/server/servicespools/{servicespool_uuid}/cache/{uuid}/metrics	GET	Возвращает список метрик РМ, находящегося в кеше
/api/webui/server/servicespools/{servicespool_uuid}/cache/{uuid}/refresh	PATCH	Управляет кешированными РМ из фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/groups	GET	Возвращает список групп фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/groups	POST	Добавляет группу в фонд РМ
/api/webui/server/servicespools/{servicespool_uuid}/groups/{uuid}	DELETE	Удаляет группу с идентификатором {uuid} из фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/groups/gui	GET	Возвращает описание для графического интерфейса
/api/webui/server/servicespools/{servicespool_uuid}/networks	GET	Возвращает список сетей из фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/networks	POST	Добавляет сеть в фонд РМ
/api/webui/server/servicespools/{servicespool_uuid}/networks/{uuid}	DELETE	Удаляет сеть с идентификатором {uuid} из фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/networks/gui	GET	Возвращает описание для графического интерфейса
/api/webui/server/servicespools/{servicespool_uuid}/policies	GET	Возвращает список всех политик фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/policies	POST	Обновляет политику фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/policies/{uuid}	GET	Получает информацию о политике фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/policies/{uuid}	PUT	Обновляет параметры политики фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/policies/{uuid}	DELETE	Сбрасывает политику фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/policies/export	GET	Формирует файл экспорта политик фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/policies/export	POST	Получает файл экспорта политик фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/policies/gui/{policy_type}	GET	Возвращает спецификацию полей графического интерфейса для политики типа {policy_type}
/api/webui/server/servicespools/{servicespool_uuid}/publications	GET	Возвращает список публикаций фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/publications/{uuid}	GET	Возвращает публикацию с идентификатором {uuid}
/api/webui/server/servicespools/{servicespool_uuid}/publications/{uuid}/cancel	GET	Запускает отмену публикации фонда РМ. Повторный вызов запускает форсированную отмену публикации фонда РМ

URL-команда	Тип	Описание
/api/webui/server/servicespools/{servicespool_uuid}/publications/gui	GET	Возвращает описание для графического интерфейса
/api/webui/server/servicespools/{servicespool_uuid}/publications/publish	GET	Запускает процедуру публикации фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/script	GET	Возвращает список скриптов фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/script	POST	Добавляет скрипт для фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/script/{uuid}	GET	Возвращает скрипт фонда рабочих мест
/api/webui/server/servicespools/{servicespool_uuid}/script/{uuid}	PUT	Обновляет скрипт фонда рабочих мест
/api/webui/server/servicespools/{servicespool_uuid}/script/{uuid}	DELETE	Удаляет скрипт из фонда рабочих мест
/api/webui/server/servicespools/{servicespool_uuid}/services	GET	Получает список назначенных РМ из фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/services/{uuid}	GET	Возвращает назначенное РМ из фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/services/{uuid}	DELETE	Удаляет назначенное РМ из фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/services/{uuid}/execute_script	PATCH	Выполняет скрипт для назначенного РМ
/api/webui/server/servicespools/{servicespool_uuid}/services/{uuid}/log	GET	Возвращает журнал назначенного РМ
/api/webui/server/servicespools/{servicespool_uuid}/services/{uuid}/machine	PATCH	Управляет состоянием питания назначенного РМ
/api/webui/server/servicespools/{servicespool_uuid}/services/{uuid}/maintenance	PATCH	Управление режимом техобслуживания назначенного РМ
/api/webui/server/servicespools/{servicespool_uuid}/services/{uuid}/metrics	GET	Возвращает список метрик назначенного РМ
/api/webui/server/servicespools/{servicespool_uuid}/services/{uuid}/refresh	PATCH	Возвращает назначенную ВМ на базовый снапшот
/api/webui/server/servicespools/{servicespool_uuid}/services/{uuid}/replace	PATCH	Заменяет назначенный экземпляр ВМ на новый (запись в базе данных о РМ остается та же)
/api/webui/server/servicespools/{servicespool_uuid}/services/message	POST	Отправляет сообщения назначенным РМ
/api/webui/server/servicespools/{servicespool_uuid}/services/message/gui	GET	Возвращает описание для графического интерфейса метода отправки сообщения РМ
/api/webui/server/servicespools/{servicespool_uuid}/transports	GET	Возвращает список протоколов доставки из фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/transports	POST	Добавляет протокол доставки в фонд РМ
/api/webui/server/servicespools/{servicespool_uuid}/transports/{uuid}	DELETE	Удаляет протокол доставки с идентификатором {uuid} из фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/transports/gui	GET	Возвращает описание для графического интерфейса
/api/webui/server/servicespools/{servicespool_uuid}/users	GET	Возвращает список пользователей фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/users	POST	Добавляет пользователя в фонд РМ

URL-команда	Тип	Описание
/api/webui/server/servicespools/{servicespool_uuid}/users/{uuid}	DELETE	Удаляет пользователя из фонда РМ
/api/webui/server/servicespools/{servicespool_uuid}/users/gui	GET	Возвращает описание для графического интерфейса
/api/webui/server/servicespools/{uuid}	GET	Возвращает фонд РМ
/api/webui/server/servicespools/{uuid}	PUT	Обновляет фонд РМ
/api/webui/server/servicespools/{uuid}	DELETE	Удаляет фонд РМ
/api/webui/server/servicespools/{uuid}/log	GET	Возвращает журнал фонда РМ
/api/webui/server/servicespools/{uuid}/maintenance	PATCH	Переводит фонд РМ в режим техобслуживания и возвращает из него
/api/webui/server/servicespools/gui	GET	Возвращает описание для графического интерфейса
/api/webui/server/servicespools/types	GET	Возвращает список доступных типов для фондов РМ

Команды, связанные с группами РМ

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с группами РМ).

Таблица 359. Перечень URL-команд, связанных с группами РМ

URL-команда	Тип	Описание
/api/webui/server/spgroups	GET	Возвращает список групп
/api/webui/server/spgroups	POST	Создает группу
/api/webui/server/spgroups/{uuid}	GET	Возвращает группу с идентификатором {uuid}
/api/webui/server/spgroups/{uuid}	PUT	Обновляет группу
/api/webui/server/spgroups/{uuid}	DELETE	Удаляет группу
/api/webui/server/spgroups/gui	GET	Возвращает описание для графического интерфейса

Команды, связанные с сессиями пользователей

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с сессиями пользователей).

Таблица 360. Перечень URL-команд, связанных с сессиями пользователей

URL-команда	Тип	Описание
/api/webui/server/spsessions	GET	Возвращает список активных сессий пользователей

URL-команда	Тип	Описание
/api/webui/server/spsessions/{uuid}	GET	Возвращает активную сессию пользователя. Пример запроса конкретной сессии через утилиту curl: `curl -X 'GET' \ 'https://disp.termidesk.local/api/webui/draft/spsessions?owner__iexact=user' \ -H 'accept: application/json' \ -H 'X-Auth-Token: 7bjqtodywjd69dkpdta9ncqprifkr3pu'` где: disp.termidesk.local - IP-адрес или FQDN узла с «Универсальным диспетчером»; user - пользователь; X-Auth-Token - токен, использующийся для аутентификации запросов
/api/webui/server/spsessions/{uuid}/disconnect	PATCH	Сбрасывает активную сессию пользователя
/api/webui/server/spsessions/{uuid}/logoff	PATCH	Останавливает активную сессию пользователя
/api/webui/server/spsessions/{uuid}/metrics	GET	Получает метрики компонента «Агент виуртуальных рабочиих мест»
/api/webui/server/spsessions/{uuid}/policies	GET	Возвращает политики сессии пользователя
/api/webui/server/spsessions/{uuid}/raconnect	PATCH	Генерирует уникальный URL для подключения к «Удаленному помощнику»

/api/webui/server/spsessions/message	POST	Отправляет сообщение в пользовательскую сессию. Параметры для заполнения в запросе:
		
		• title - заголовок сообщения;
		• message - текст сообщения;
		• level - уровень важности. Может быть:
		  - informational - информационное сообщение. Для пользователя отобразится сообщение с уровнем важности «informational»;
		  - warning - предупреждение. Для пользователя отобразится сообщение с уровнем важности «warning»;
		  - error - ошибка. Для пользователя отобразится сообщение с уровнем важности «error»;
		• confirmation - требование подтверждения о прочтении;
		• uuids - перечень уникальных идентификаторов сессий пользователя, в которые отправится сообщение

/api/webui/server/spsessions/message-stats/{group_id}	GET	Возвращает результат отправки сообщения

Команды, связанные с тегами

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с тегами).

Таблица 361. Перечень URL-команд, связанных с тегами

URL-команда	Тип	Описание
`/api/webui/server/tags`	GET	Возвращает список тегов
`/api/webui/server/tags`	POST	Создает тег
`/api/webui/server/tags/{id}`	GET	Возвращает тег
`/api/webui/server/tags/{id}`	PUT	Обновляет тег
`/api/webui/server/tags/{id}`	DELETE	Удаляет тег
`/api/webui/server/tags/export`	GET	Формирует файл экспорта тегов
`/api/webui/server/tags/export`	POST	Получает файл экспорта тегов

Команды, связанные с системными параметрами

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с системными параметрами).

Таблица 362. Перечень URL-команд, связанных с системными параметрами

URL-команда	Тип	Описание
`/api/webui/server/tconfig`	GET	Возвращает список системных параметров
`/api/webui/server/tconfig`	PUT	Сохраняет параметры конфигурации

Команды, связанные с протоколом доставки TERA

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с TERA).

Таблица 363. Перечень URL-команд, связанных с TERA

URL-команда	Тип	Описание
`/api/webui/server/tera/{transport_uuid}/group-channels`	GET	Возвращает список каналов приоритизации для протокола доставки TERA
`/api/webui/server/tera/{transport_uuid}/group-channels/bulk_update`	PATCH	Обновляет список каналов приоритизации для протокола доставки TERA

Команды, связанные с терминальными серверами

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с терминальными серверами).

Таблица 364. Перечень URL-команд, связанных с терминальными серверами

URL-команда	Тип	Описание
`/api/webui/server/terminals`	GET	Возвращает список терминальных серверов
`/api/webui/server/terminals/{uuid}`	GET	Возвращает терминальный сервер с идентификатором `{uuid}`
`/api/webui/server/terminals/{uuid}/metrics`	GET	Возвращает метрики терминального сервера с идентификатором `{uuid}`

Команды, связанные с протоколами доставки

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с протоколами доставки).

Таблица 365. Перечень URL-команд, связанных с протоколами доставки

URL-команда	Тип	Описание
/api/webui/server/transports	GET	Возвращает список протоколов доставки
/api/webui/server/transports	POST	Создает протокол доставки
/api/webui/server/transports/{uuid}	GET	Возвращает протокол доставки
/api/webui/server/transports/{uuid}	PUT	Обновляет протокол доставки
/api/webui/server/transports/{uuid}	DELETE	Удаляет протокол доставки
/api/webui/server/transports/export	GET	Формирует файл экспорта протоколов доставки
/api/webui/server/transports/export	POST	Получает файл экспорта протоколов доставки
/api/webui/server/transports/gui/{transport_type}	GET	Возвращает описание для графического интерфейса
/api/webui/server/transports/test/{transport_type}	POST	Тестирует параметры протокола доставки
/api/webui/server/transports/types	GET	Возвращает список типов протоколов доставки

Команды, связанные с управлением РМ

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с управлением РМ).

Таблица 366. Перечень URL-команд, связанных с управлением РМ

URL-команда	Тип	Описание
/api/webui/server/userservices/bulk/bulk-assign	PATCH	Назначает пользователей на РМ
/api/webui/server/userservices/bulk/bulk-destroy	PATCH	Удаляет РМ
/api/webui/server/userservices/bulk/bulk-machine-state	PATCH	Управляет состоянием РМ
/api/webui/server/userservices/bulk/bulk-refresh	PATCH	Восстанавливает РМ

Команды, связанные с работой мастеров фонда РМ

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с работой мастеров).

Таблица 367. Перечень URL-команд, связанных с работой мастеров

URL-команда	Тип	Описание
/api/webui/server/wizards	GET	Возвращает список мастеров
/api/webui/server/wizards/{uuid}	DELETE	Удаляет мастер с идентификатором {uuid}
/api/webui/server/wizards/{uuid}/finish	PATCH	Создает объект после валидации собранных данных. Удаляет мастер из временного хранилища
/api/webui/server/wizards/{uuid}/step/{step}	PATCH	Обрабатывает данные для указанного шага мастера
/api/webui/server/wizards/{uuid}/step/{step}/gui	GET	Возвращает спецификацию действий и полей
/api/webui/server/wizards/types	GET	Возвращает список доступных типов мастеров

Команды, связанные со списком РМ

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных со списком РМ).

Таблица 368. Перечень URL-команд, связанных со списком РМ

URL-команда	Тип	Описание
`/api/webui/server/workplaces`	GET	Возвращает список РМ
`/api/webui/server/workplaces/{id}/tags`	PATCH	Редактирует список тегов РМ

Доступные команды модуля «wsproxy»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «wsproxy»).

Версия API `/api/wsproxy/v1.1` удалена.

Таблица 369. Перечень URL-команд модуля «wsproxy»

URL-команда	Тип	Описание

`/api/wsproxy/v7.0/verify/{token}`	POST	Валидация токена шлюза для подключения к компоненту «Универсальный диспетчер» с поддержкой информации по протоколу TCP или UDP.
		
		В запросе передается дополнительное поле `proto` с указанием значения протокола, по умолчанию TCP:
		
		`HTTP 200`
		`{`
		`"host": "192.0.2.1",`
		`"port": 6195,`
		`"ssl_target": true,`
		`"proto": "tcp"`
		`}`

«АГРЕГАТОР»

Начало работы с REST API портала «Агрегатор»

Получение токена для доступа к REST API портала «Агрегатор»

Перед использованием REST API нужно получить токен, который необходимо подставлять во все последующие запросы, кроме запросов `health`. Для получения токена нужно авторизоваться в Termidesk VDI, для этого:

- выполнить запрос «https://aggr.termidesk.local/api/auth/v7.0/authenticators»;
- запомнить значения параметров `authUuid`, `authSmallName`, `auth`;
- выполнить запрос, подставив соответствующие значения параметров, полученных ранее:
  - либо с использованием утилиты `curl`. Пример (в поле `authId` подставляется значение из `authUuid`):

```
curl -X 'POST' \
  'https://aggr.termidesk.local/api/auth/v7.0/login' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -d '{
  "username": "admin123",
  "password": "admin123",
  "auth": "Встроенный",
  "authId": "a6ec7be4-93d1-4473-8471-6dfc8f734d78",
  "authSmallName": "builtin"
}'
```

- либо с использованием интерфейса Swagger, предоставляющего электронный справочник по командам.

В приведенных командах `aggr.termidesk.local` - сетевой адрес или полное доменное имя узла с порталом «Агрегатор» Termidesk VDI.

Для запросов проверки состояния сервера `/aggregator/health` используется токен, определенный в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` в значении параметра `HEALTH_CHECK_ACCESS_KEY`.

Формат запроса к `/health/check` выглядит следующим образом:

```
curl -X 'GET' \
'https://aggr.termidesk.local/aggregator/health/check' \
-H 'accept: application/json' \
-H 'Authorization: Token
072bfec46ac7c42078bb41ff5f6d1ae201006f0824fb4b2bb8ab8befacb01058'
```

где:

`Token 072…` - токен, определенный в параметра `HEALTH_CHECK_ACCESS_KEY` файла `/etc/opt/termidesk-vdi/termidesk.conf`.

Для форматированного вывода рекомендуется:

- установить пакет `jq`:

```
sudo apt install jq
```

- выполнить запрос, добавив в конец команды `|jq`. Пример:

```
curl -X 'GET' \
'https://aggr.termidesk.local/aggregator/health/check' \
-H 'accept: application/json' \
-H 'Authorization: Token
```

```
072bfec46ac7c42078bb41ff5f6d1ae201006f0824fb4b2bb8ab8befacb01058' | jq
```

В случае, если запрос завершится ошибкой вида «curl: (60) SSL: no alternative certificate subject name matches target host name... curl failed to verify the legitimacy... », нужно дополнить запрос флагом `--insecure`, который отключит проверку валидности сертификатов:

Выполнение запроса без использования проверки SSL допустимо только на тестовых стендах. Для исправления ошибки в производственной среде необходимо установить на сервер с порталом «Агрегатор» валидные сертификаты.

```
curl -X 'GET' \
'https://aggr.termidesk.local/aggregator/health/check' \
-H 'accept: application/json' \
-H 'Authorization: Token
072bfec46ac7c42078bb41ff5f6d1ae201006f0824fb4b2bb8ab8befacb01058' --insecure | jq
```

Формат URL-команд портала «Агрегатор»

Общий вид команд реализован следующим образом:

`/aggregator/api/<module>/<ver>/aggregator/<name>/`

где:

`<module>` - наименование модуля, реализованного в REST API;

`<ver>` - версия;

`<name>` - наименование элемента (эндпоинта). После наименования элемента также могут быть включены уникальные номера объектов и наименования других элементов.

Пример команды через `curl`:

```
curl -X 'GET' \
  'https://aggr.termidesk.local/api/discover/' \
  -H 'accept: application/json' \
  -H 'X-Auth-Token: izycb3z47wwziibprg183t4ep2ti0tar'
```

В REST API реализовано следующее логическое разделение на модули в части портала «Агрегатор»:

- «auth» - модуль для аутентификации пользователей веб-интерфейса;
- «client» - модуль взаимодействия с компонентом «Клиент»;
- «discover» - используется для отображения списка модулей API, предоставляемого сервером (команда `/api/discover/`);
- «health» - модуль проверок состояния;
- «userinfo» - модуль получения информации о пользователе;
- «webui» - модуль управления функциями, доступными через веб-интерфейс.

Список отображаемых модулей зависит от типа портала, который был выбран при установке:

- «Агрегатор администратора»: доступны «auth», «discover», «health», «userinfo», «webui»;
- «Агрегатор пользователя»: «auth», «discover», «health», «client», «userinfo»;
- «Агрегатор администратора» и «Агрегатор пользователя»: доступны все модули.

Электронный справочник по командам портала «Агрегатор»

Полная информация о параметрах и командах REST API доступна при вводе URL-команды `https://aggr.termidesk.local/aggregator/docs/`, где `aggr.termidesk.local` - сетевой адрес или полное доменное имя узла с порталом «Агрегатор» Termidesk VDI.

Для получения доступа пользователь должен быть аутентифицирован на портале «Агрегатор администратора» в этой же сессии веб-браузера. Доступ предоставляется после авторизации в веб-интерфейсе портала «Агрегатор».

Пример использования:

- нажать экранную кнопку **[Try it out]** в пространстве команд какого-либо модуля для составления запроса (см. рисунок Расположение экранных кнопок для получения доступа к формированию запроса);
- отправить запрос на выполнение экранной кнопкой **[Execute]** (см. рисунок Расположение экранной кнопки для формирования запроса). После нажатия будет отображена также команда для запроса через `curl`.

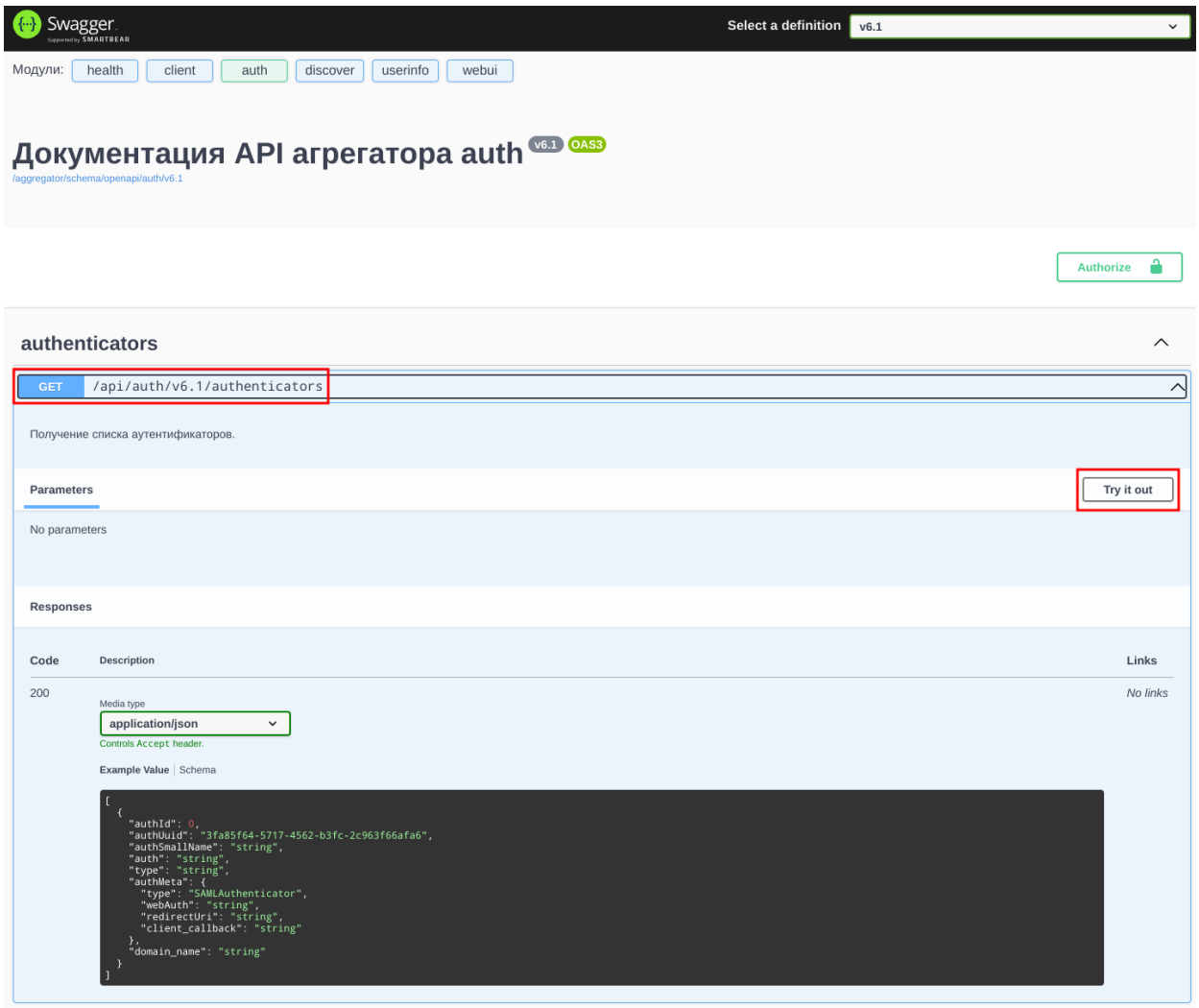


Рисунок 220. Расположение экранных кнопок для получения доступа к формированию запроса

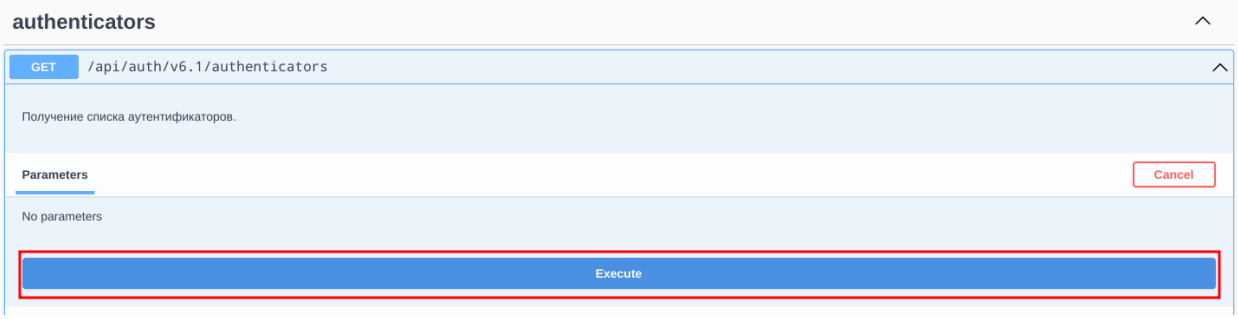


Рисунок 221. Расположение экранной кнопки для формирования запроса

Команды портала «Агрегатор»

Доступные команды модуля «auth» портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «auth» портала «Агрегатор»).

Таблица 370. Перечень URL-команд модуля «auth» портала «Агрегатор»

URL-команда	Тип	Описание
`/api/auth/v7.0/authenticators`	GET	Возвращает список доменов аутентификации

URL-команда	Тип	Описание
/api/auth/v7.0/authenticators/{auth_uuid}/pkinit/finalize	PATCH	Завершает аутентификацию Kerberos PKINIT
/api/auth/v7.0/authenticators/{auth_uuid}/pkinit/login	PATCH	Инициализирует аутентификацию Kerberos PKINIT и получает данные на подпись
/api/auth/v7.0/authenticators/{auth_uuid}/pkinit/raw	PATCH	Прямой запрос на сервер Kerberos PKINIT с подписанным сертификатом
/api/auth/v7.0/jwtauth	POST	Авторизация «Агрегатора» на «Универсальном диспетчере». В ответ на подписанный «Агрегатором» токен «Универсальный диспетчер» возвращает сеансовый ключ (токен)
/api/auth/v7.0/login	POST	Аутентификация пользователя на базе аутентификатора, логина и пароля. При отправке запроса необходимо обязательно указать один из параметров: • «authId»; • «auth»; • «authSmallName»
/api/auth/v7.0/login/2fa	POST	Двухфакторная аутентификация пользователя на базе аутентификатора, логина и пароля. При отправке запроса необходимо обязательно указать один из параметров: • «authId»; • «auth»; • «authSmallName»
/api/auth/v7.0/logout	POST	Прекращение действие токена/сессии пользователя. Токен аутентификации должен передаваться в заголовке X-Auth-Token
/api/auth/v7.0/settings	GET	Получение глобальных настроек сервера

Доступные команды модуля «client» портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «client» портала «Агрегатор»).

Таблица 371. Перечень URL-команд модуля «client» портала «Агрегатор»

URL-команда	Тип	Описание
/aggregator/api/client/v7.0/{site_uri}/connectionInfo/{id}	GET	API для выдачи параметров подключения компоненту «Клиент» для протоколов RDP и SPICE от «Универсального диспетчера»
/aggregator/api/client/v7.0/{site_uri}/preconnectionInfo/{id}	GET	API для выдачи параметров подключения компоненту «Клиент» для протоколов RDP и SPICE от «Универсального диспетчера». Компонент «Клиент» использует метод для проверки готовности сервиса к подключению и уточнения используемого протокола. По полученным данным принимает решение: завершить неудачное подключение, подождать и повторить, подключаться новым/старым методом
/aggregator/api/client/v7.0/{site_uri}/reconnect/	POST	Обновляет ссылку для переподключения к сессии РМ

URL-команда	Тип	Описание
`/aggregator/api/client/v7.0/{site_uri}/servicesList/`	GET	Получение и сравнение списка доменов аутентификации из базы данных (БД) и от «Универсального диспетчера», а также получение связанного списка сервисов, если получены совпадающие короткие наименования доменов аутентификации (одинаковые метки доменов)

Доступные команды модуля «discover» портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «discover» портала «Агрегатор»).

Таблица 372. Перечень URL-команд модуля «discover» портала «Агрегатор»

URL-команда	Тип	Описание
`/api/discover/`	GET	Возвращает список модулей API, предоставляемых «Агрегатором»

Доступные команды модуля «health» портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «health» портала «Агрегатор»).

Таблица 373. Перечень URL-команд модуля «health» портала «Агрегатор»

URL-команда	Тип	Описание

/aggregator/health/check	GET	Проверка состояния сервера. Собираются общие показатели и набор числовых метрик.
		
		Для авторизации при обращении к запросу используется токен, определенный в переменной HEALTH_CHECK_ACCESS_KEY конфигурационного файла /etc/opt/termidesk-vdi/termidesk.conf.
		
		Оценка состояния должна производиться в инициаторе запроса на основе набора правил и пороговых значений с учетом конкретной конфигурации системы.
		
		Для разных конфигураций системы один и тот же показатель в абсолютном выражении может соответствовать состоянию и «PASS», и «FAIL».
		
		Формат запроса:
		
		`curl --insecure -v -s -X 'GET' \`
		`  'https://$\{hostname}:$\{health_port}/aggregator/health/check' \`
		`  -H 'accept: application/json' \`
		`  -H 'Authorization: Token $\{health_check_access_key}'`
		
		где:
		
		--insecure - отключение проверки валидности сертификатов. Выполнение запроса без использования проверки SSL допустимо только на тестовых стендах. В производственной среде необходимо установить валидные сертификаты;
		
		${hostname} - сетевой адрес или полное доменное имя узла;
		
		${health_port} - порт для запросов проверки состояния;
		
		${health_check_access_key} - токен, определенный в переменной HEALTH_CHECK_ACCESS_KEY файла /etc/opt/termidesk-vdi/termidesk.conf.
		
		Пример возвращаемого списка приведен после таблицы

URL-команда	Тип	Описание
/aggregator/health/metrics	GET	Возвращает список метрик сервера. Для авторизации при обращении к запросу используется токен, определенный в переменной METRICS_ACCESS_KEY конфигурационного файла /etc/opt/termidesk-vdi/termidesk.conf. Формат запроса: `curl --insecure -v -s -X 'GET' \ 'https://$\{hostname}:$\{health_port}/aggregator/health/metrics' \ -H 'accept: application/json' \ -H 'Authorization: Token $\{metrics_access_key}'` где: --insecure - отключение проверки валидности сертификатов. Выполнение запроса без использования проверки SSL допустимо только на тестовых стендах. В производственной среде необходимо установить валидные сертификаты; ${hostname} - сетевой адрес или полное доменное имя узла; ${health_port} - порт для запросов проверки состояния; ${metrics_access_key} - токен, определенный в переменной METRICS_ACCESS_KEY файла /etc/opt/termidesk-vdi/termidesk.conf. Информацию по всем возвращаемым значениям можно получить в документации библиотеки psutil на сайте: https://psutil.readthedocs.io/en/latest. Вид возвращаемого списка метрик приведен после таблицы

Пример возвращаемого списка для /aggregator/health/check:

```
{"version":"5.1","description":"termidesk-aggregator","status":"pass","checks":
    {
    "celery:connectionTest":

[{"componentId":"celery(common)","componentType":"component","status":"pass"},

{"componentId":"celery@test(worker)","componentType":"component","status":"pass"}],
    "database:responseTime":

[{"componentId":"default","componentType":"datastore","observedValue":0.00040602684
020996094,"observedUnit":"s","status":"pass"}],
    "messages_broker:connectionTest":

[{"componentId":"amqp://termidesk:**@localhost:5672/termidesk","componentType":"com
ponent","status":"pass"}],
    "fluentd:connectionTest":[],
    "sites:connectionTest":
        [{"componentId":"site2","componentType":"component","status":"pass"},
```

```
            {"componentId":"stal","componentType":"component","status":"pass"},
            {"componentId":"test-
site","componentType":"component","status":"pass"},
            {"componentId":"site1-1","componentType":"component","status":"pass"},
            {"componentId":"site99","componentType":"component","status":"pass"}
        ]}
}
```

Вид возвращаемого списка метрик:

```
# Версия портала «Агрегатор»
version_info{version="5.1"} 1.0
# Версия ОС
system_info{machine="x86_64",os="Linux 6.1.90-1-generic",version="#astra3+ci20 SMP
PREEMPT_DYNAMIC Mon Jul 22 14:15:46 UTC 2024"} 1.0
# Период в секундах, в течение которого система функционирует без проблем
uptime_seconds 66686.97834658623
# Общая загрузка процессора в процентах
cpu_total_percent 4.8
# Общее использование физической памяти в процентах
virtual_memory_total_percent 40.5
# Количество операций чтения с диска
disk_read_count 68201.0
# Количество операций записи на диск
disk_write_count 729848.0
# Число прочитанных с диска байт
disk_read_bytes 2.094142464e+09
# Число записанных на диск байт
disk_write_bytes 7.54249728e+09
# Общий размер физической памяти в байтах
virtual_memory_total_bytes 4.117311488e+09
# Размер доступной физической памяти в байтах
virtual_memory_available_bytes 2.447736832e+09
# Размер используемой физической памяти в байтах
virtual_memory_used_bytes 1.303724032e+09
# Размер свободной физической памяти в байтах
virtual_memory_free_bytes 3.78679296e+08
# Общий размер диска в байтах
disk_total_bytes 1.5742214144e+010
# Используемый размер диска в байтах
disk_used_bytes 1.4512279552e+010
# Свободный размер диска в байтах
disk_free_bytes 4.07957504e+08
# Количество авторизованных пользователей в портале «Агрегатор пользователя»
user_session_count 1.0
# Количество авторизованных администраторов в портале «Агрегатор администратора»
admin_session_count 11.0
# Количество доменов аутентификации
```

```
auth_domain_count 4.0
# Количество ферм поставщиков ресурсов
# TYPE farms_count gauge
farms_count 4.0
# Количество узлов
servers_count 4.0
# Количество сайтов
sites_count 4.0
```

Доступные команды модуля «userinfo» портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «userinfo» портала «Агрегатор»).

Таблица 374. Перечень URL-команд модуля «userinfo» портала «Агрегатор»

URL-команда	Тип	Описание
/api/userinfo/themes	GET	Получение параметров брендирования
/api/userinfo/themes	PUT	Обновление параметров брендирования
/api/userinfo	GET	Получение информации о пользователе

Доступные команды модуля «webui» портала «Агрегатор»

Команды, связанные с объектами инфраструктуры

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с объектами инфраструктуры портала «Агрегатор»).

Таблица 375. Перечень URL-команд, связанных с объектами инфраструктуры портала «Агрегатор»

URL-команда	Тип	Описание
/api/webui/aggregator/appnodes/portals	GET	Возвращает список объектов инфраструктуры («Порталов»)
/api/webui/aggregator/appnodes/portals/{uuid}	DELETE	Удаляет объект инфраструктуры («Порталов»)
/api/webui/aggregator/appnodes/portals/{uuid}/metrics	PATCH	Возвращает список метрик объектов инфраструктуры («Порталов»)
/api/webui/aggregator/appnodes/portals/{uuid}/tags	PATCH	Возвращает список тегов объектов инфраструктуры («Порталов»)
/api/webui/aggregator/appnodes/portals/export	GET	Формирует файл экспорта объектов инфраструктуры («Порталов»)
/api/webui/aggregator/appnodes/portals/export	POST	Получает файл экспорта объектов инфраструктуры («Порталов»)

Команды, связанные с событиями аудита портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с событиями аудита портала «Агрегатор»).

Таблица 376. Перечень URL-команд, связанных с событиями аудита портала «Агрегатор»

URL-команда	Тип	Описание
/api/webui/aggregator/audit	GET	Возвращает список событий аудита
/api/webui/aggregator/audit/export	GET	Формирует файл экспорта событий аудита
/api/webui/aggregator/audit/export	POST	Получает файл экспорта событий аудита

Команды, связанные с доменами аутентификации портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с доменами аутентификации портала «Агрегатор»).

Таблица 377. Перечень URL-команд, связанных с доменами аутентификации портала «Агрегатор»

URL-команда	Тип	Описание
/api/webui/aggregator/authenticators	GET	Возвращает список доменов аутентификации, добавленных на портал «Агрегатор»
/api/webui/aggregator/authenticators	POST	Создает домен аутентификации
/api/webui/aggregator/authenticators/{auth_uuid}/groups	GET	Возвращает список групп домена аутентификации
/api/webui/aggregator/authenticators/{auth_uuid}/groups	POST	Создает группу домена аутентификации
/api/webui/aggregator/authenticators/{auth_uuid}/groups/{uuid}	GET	Возвращает группу с идентификатором {uuid} домена аутентификации с идентификатором {auth_uuid}
/api/webui/aggregator/authenticators/{auth_uuid}/groups/{uuid}	PUT	Обновляет группу с идентификатором {uuid} домена аутентификации с идентификатором {auth_uuid}
/api/webui/aggregator/authenticators/{auth_uuid}/groups/{uuid}	PATCH	Обновляет группу с идентификатором {uuid} домена аутентификации с идентификатором {auth_uuid}
/api/webui/aggregator/authenticators/{auth_uuid}/groups/{uuid}	DELETE	Удаляет группу с идентификатором {uuid} домена аутентификации с идентификатором {auth_uuid}
/api/webui/aggregator/authenticators/{auth_uuid}/groups/bulk_destroy	POST	Удаляет все группы домена аутентификации с идентификатором {auth_uuid}
/api/webui/aggregator/authenticators/{auth_uuid}/groups/external	GET	Возвращает список групп из службы каталогов для домена аутентификации с идентификатором {auth_uuid}
/api/webui/aggregator/authenticators/{auth_uuid}/users	GET	Возвращает список пользователей домена аутентификации
/api/webui/aggregator/authenticators/{auth_uuid}/users	POST	Создает пользователя домена аутентификации
/api/webui/aggregator/authenticators/{auth_uuid}/users/{uuid}	GET	Возвращает пользователя с идентификатором {uuid} домена аутентификации с идентификатором {auth_uuid}
/api/webui/aggregator/authenticators/{auth_uuid}/users/{uuid}	PUT	Обновляет пользователя с идентификатором {uuid} домена аутентификации с идентификатором {auth_uuid}
/api/webui/aggregator/authenticators/{auth_uuid}/users/{uuid}	PATCH	Обновляет пользователя с идентификатором {uuid} домена аутентификации с идентификатором {auth_uuid}
/api/webui/aggregator/authenticators/{auth_uuid}/users/{uuid}	DELETE	Удаляет пользователя с идентификатором {uuid} домена аутентификации с идентификатором {auth_uuid}
/api/webui/aggregator/authenticators/{auth_uuid}/users/bulk_destroy	POST	Удаляет всех пользователей домена аутентификации с идентификатором {auth_uuid}

URL-команда	Тип	Описание
/api/webui/aggregator/authenticators/{uuid}	GET	Возвращает домен аутентификации с идентификатором {uuid}
/api/webui/aggregator/authenticators/{uuid}	PUT	Обновляет домен аутентификации с идентификатором {uuid}
/api/webui/aggregator/authenticators/{uuid}	PATCH	Обновляет домен аутентификации с идентификатором {uuid}
/api/webui/aggregator/authenticators/{uuid}	DELETE	Удаляет домен аутентификации с идентификатором {uuid}
/api/webui/aggregator/authenticators/{uuid}/attribute	PATCH	Добавить, изменить или удалить атрибут домена для сохранения в учетной записи пользователя
/api/webui/aggregator/authenticators/bulk_destroy	POST	Удаляет домены аутентификации
/api/webui/aggregator/authenticators/gui/{data_type}	GET	Возвращает описание для графического интерфейса домена аутентификации с типом {data_type}
/api/webui/aggregator/authenticators/test_params/{type}	POST	Тестирует параметры домена аутентификации
/api/webui/aggregator/authenticators/test/{type}	POST	Тестирует параметры домена аутентификации
/api/webui/aggregator/authenticators/types	GET	Возвращает список доступных типов доменов аутентификации

Команды, связанные с парметрами подключения к порталу «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с панелью мониторинга портала «Агрегатор»).

Таблица 378. Перечень URL-команд, связанных с панелью мониторинга портала «Агрегатор»

URL-команда	Тип	Описание
/api/webui/aggregator/node-info	GET	Возвращает информацию о сервере

Команды, связанные с панелью мониторинга портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с панелью мониторинга портала «Агрегатор»).

Таблица 379. Перечень URL-команд, связанных с панелью мониторинга портала «Агрегатор»

URL-команда	Тип	Описание
/api/webui/aggregator/dashboard/admin	GET	Просмотр списка объектов панели мониторинга для «Агрегатора администратора»
/api/webui/aggregator/dashboard/user/{site_uri}	GET	Просмотр списка объектов панели мониторинга для «Агрегатора пользователя»

Команды, связанные с узлами «Универсального диспетчера» портала

«Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу [ПеречеьURLкомандсвязанныхсузламиУниверсальногодиспетчерапорталаАгрегато]).

Таблица 380. Перечень URL-команд, связанных с узлами «Универсального диспетчера»

портала «Агрегатор»

URL-команда	Тип	Описание
/api/webui/aggregator/dispatchers	GET	Возвращает список узлов «Универсального диспетчера», добавленных на портал «Агрегатор»
/api/webui/aggregator/dispatchers	POST	Добавляет узел «Универсального диспетчера»
/api/webui/aggregator/dispatchers/{id}	GET	Возвращает узел «Универсального диспетчера» с идентификатором {id}
/api/webui/aggregator/dispatchers/{id}	PUT	Обновляет узел «Универсального диспетчера» с идентификатором {id}
/api/webui/aggregator/dispatchers/{id}	PATCH	Обновляет узел «Универсального диспетчера» с идентификатором {id}
/api/webui/aggregator/dispatchers/{id}	DELETE	Удаляет узел «Универсального диспетчера» с идентификатором {id}
/api/webui/aggregator/dispatchers/bulk_destroy	POST	Удаляет все узлы «Универсального диспетчера»

Команды, связанные с фермами поставщиков ресурсов портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с фермами поставщиков ресурсов портала «Агрегатор»).

Таблица 381. Перечень URL-команд, связанных с фермами поставщиков ресурсов портала «Агрегатор»

URL-команда	Тип	Описание
/api/webui/aggregator/farms	GET	Возвращает список ферм поставщиков ресурсов, добавленных на портал «Агрегатор»
/api/webui/aggregator/farms	POST	Создает ферму поставщиков ресурсов
/api/webui/aggregator/farms/{id}	GET	Возвращает ферму поставщиков ресурсов с идентификатором {id}
/api/webui/aggregator/farms/{id}	PUT	Обновляет ферму поставщиков ресурсов с идентификатором {id}
/api/webui/aggregator/farms/{id}	PATCH	Обновляет ферму поставщиков ресурсов с идентификатором {id}
/api/webui/aggregator/farms/{id}	DELETE	Удаляет ферму поставщиков ресурсов с идентификатором {id}
/api/webui/aggregator/farms/{id}/dispatchers	GET	Возвращает список узлов «Универсального диспетчера» для фермы с идентификатором {id}
/api/webui/aggregator/farms/{id}/tags	GET	Возвращает список тегов с узлов «Универсального диспетчера» для фермы с идентификатором {id}
/api/webui/aggregator/farms/bulk_destroy	POST	Удаляет все фермы поставщиков ресурсов

Команды, связанные с изображениями портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с изображением портала «Агрегатор»).

Таблица 382. Перечень URL-команд, связанных с изображением портала «Агрегатор»

URL-команда	Тип	Описание
/api/webui/aggregator/gallery/images/srvimg/{image_id}	GET	Возвращает изображение по идентификатору, либо для протокола доставки, либо установленное по умолчанию
/api/webui/aggregator/gallery/images/transicon/{image_id}	GET	Возвращает изображение для протокола доставки

Команды, связанные со шлюзами портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных со шлюзами портала «Агрегатор»).

Таблица 383. Перечень URL-команд, связанных со шлюзами портала «Агрегатор»

URL-команда	Тип	Описание
/api/webui/aggregator/gateways	GET	Возвращает список объектов («Шлюзов»), добавленных на портал «Агрегатор»
/api/webui/aggregator/gateways	POST	Создает объект («Шлюз»)
/api/webui/aggregator/gateways/{id}	GET	Возвращает объект («Шлюз») с идентификатором {id}
/api/webui/aggregator/gateways/{id}	PUT	Обновляет объект («Шлюз») с идентификатором {id}
/api/webui/aggregator/gateways/{id}	PATCH	Обновляет объект («Шлюз») с идентификатором {id}
/api/webui/aggregator/gateways/{id}	DELETE	Удаляет объект («Шлюз») с идентификатором {id}
/api/webui/aggregator/gateways/bulk_destroy	PATCH	Удаляет все объекты («Шлюзы»)

Команды, связанные с шаблонами техобслуживания

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с шаблонами техобслуживания).

Таблица 384. Перечень URL-команд, связанных с шаблонами техобслуживания

URL-команда	Тип	Описание
/api/webui/aggregator/maintenance	GET	Возвращает список шаблонов техобслуживания, добавленных на портал «Агрегатор»
/api/webui/aggregator/maintenance	POST	Создает шаблон техобслуживания
/api/webui/aggregator/maintenance/{id}	GET	Возвращает шаблон техобслуживания с идентификатором {id}
/api/webui/aggregator/maintenance/{id}	PUT	Обновляет шаблон техобслуживания с идентификатором {id}
/api/webui/aggregator/maintenance/{id}	PATCH	Обновляет шаблон техобслуживания с идентификатором {id}
/api/webui/aggregator/maintenance/{id}	DELETE	Удаляет шаблон техобслуживания с идентификатором {id}
/api/webui/aggregator/maintenance/bulk_destroy	PATCH	Удаляет шаблоны техобслуживания

Команды, связанные с функциями мониторинга портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень

URL-команд, связанных с функциями мониторинга портала «Агрегатор»).

Таблица 385. Перечень URL-команд, связанных с функциями мониторинга портала «Агрегатор»

URL-команда	Тип	Описание
/api/webui/aggregator/monitoring	GET	Просмотр всех записей журнала в виде списка
/api/webui/aggregator/monitoring	POST	Добавляет запись в журнал
/api/webui/aggregator/monitoring/{id}	GET	Просмотр записи журнала с идентификатором {id}
/api/webui/aggregator/monitoring/{id}	PUT	Обновляет запись журнала с идентификатором {id}
/api/webui/aggregator/monitoring/{id}	PATCH	Обновляет запись журнала с идентификатором {id}
/api/webui/aggregator/monitoring/{id}	DELETE	Удаляет запись журнала с идентификатором {id}
/api/webui/aggregator/monitoring/bulk_destroy	PATCH	Удаляет все записи журнала
/api/webui/aggregator/monitoring/export	GET	Формирует файл экспорта событий журнала
/api/webui/aggregator/monitoring/export	POST	Получает файл экспорта событий журнала

Команды, связанные с группами пользователей

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с группами пользователей портала «Агрегатор»).

Таблица 386. Перечень URL-команд, связанных с группами пользователей портала «Агрегатор»

URL-команда	Тип	Описание
/api/webui/aggregator/priority_groups	GET	Возвращает список групп, добавленных на портал «Агрегатор»
/api/webui/aggregator/priority_groups	POST	Создает группу
/api/webui/aggregator/priority_groups/{id}	GET	Возвращает группу с идентификатором {id}
/api/webui/aggregator/priority_groups/{id}	PUT	Обновляет группу с идентификатором {id}
/api/webui/aggregator/priority_groups/{id}	PATCH	Обновляет группу с идентификатором {id}
/api/webui/aggregator/priority_groups/{id}	DELETE	Удаляет группу с идентификатором {id}

Команды, связанные с управлением полномочиями (ролями) портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с управлением полномочиями (ролями) портала «Агрегатор»).

Таблица 387. Перечень URL-команд, связанных с управлением полномочиями (ролями) портала «Агрегатор»

URL-команда	Тип	Описание
/api/webui/aggregator/rbac	GET	Возвращает список ролей, добавленных на портал «Агрегатор»
/api/webui/aggregator/rbac	POST	Создает роль
/api/webui/aggregator/rbac/{id}	GET	Возвращает роль с идентификатором {id}

URL-команда	Тип	Описание
/api/webui/aggregator/rbac/{id}	PUT	Обновляет роль с идентификатором {id}
/api/webui/aggregator/rbac/{id}	PATCH	Обновляет роль с идентификатором {id}
/api/webui/aggregator/rbac/{id}	DELETE	Удаляет роль с идентификатором {id}
/api/webui/aggregator/rbac/permissions	GET	Возвращает список доступных пользовательских разрешений

Команды, связанные с объединенными наборами ресурсов сайтов портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с объединенными наборами ресурсов сайтов портала «Агрегатор»).

Таблица 388. Перечень URL-команд, связанных с объединенными наборами ресурсов сайтов портала «Агрегатор»

URL-команда	Тип	Описание
/api/webui/aggregator/rules	GET	Возвращает список объединенных наборов ресурсов, добавленных на портал «Агрегатор»
/api/webui/aggregator/rules	POST	Добавляет объединенный набор ресурсов
/api/webui/aggregator/rules/{id}	GET	Возвращает объединенный набор ресурсов с идентификатором {id}
/api/webui/aggregator/rules/{id}	PUT	Обновляет объединенный набор ресурсов с идентификатором {id}
/api/webui/aggregator/rules/{id}	PATCH	Обновляет объединенный набор ресурсов с идентификатором {id}
/api/webui/aggregator/rules/{id}	DELETE	Удаляет объединенный набор ресурсов с идентификатором {id}

Команды, связанные с фондами РМ портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с фондами РМ портала «Агрегатор»).

Таблица 389. Перечень URL-команд, связанных с фондами РМ портала «Агрегатор»

URL-команда	Тип	Описание
/api/webui/aggregator/servicespools	GET	Возвращает список фондов РМ, добавленных на портал «Агрегатор»
/api/webui/aggregator/servicespools/{id}/maintenance/{servicepool_uuid}	PATCH	Управляет режимом техобслуживания фонда РМ
/api/webui/aggregator/servicespools/{id}/update/{servicepool_uuid}	PUT	Обновляет фонд РМ
/api/webui/aggregator/servicespools/{service_pool_uuid}/policies	GET	Возвращает список политик для фонда РМ с идентификатором {service_pool_uuid}, полученного от «Универсального диспетчера»

Команды, связанные с сайтами портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу [ПереченьURLкомандсвязанныхссайтамипорталаАгрегато]).

Таблица 390. Перечень URL-команд, связанных с сайтами портала «Агрегатор»

URL-команда	Тип	Описание
/api/webui/aggregator/sites	GET	Возвращает список сайтов, добавленных на портал «Агрегатор»
/api/webui/aggregator/sites	POST	Добавляет сайт
/api/webui/aggregator/sites/{id}	GET	Возвращает сайт с идентификатором {id}
/api/webui/aggregator/sites/{id}	PUT	Обновляет сайт с идентификатором {id}
/api/webui/aggregator/sites/{id}	PATCH	Обновляет сайт с идентификатором {id}
/api/webui/aggregator/sites/{id}	DELETE	Удаляет сайт с идентификатором {id}
/api/webui/aggregator/sites/{id}/farms	GET	Способ предоставления всех ферм сайта с идентификатором {id}
/api/webui/aggregator/sites/{id}/rules	GET	Способ предоставления всех правил (объединенных наборов ресурсов) сайта с идентификатором {id}
/api/webui/aggregator/sites/bulk_destroy	POST	Удаляет все сайты
/api/webui/aggregator/sites/users-groups-from-domains	GET	Способ получения пользователей и групп доменов аутентификации, доступных для добавления на сайт

Команды, связанные с сессиями пользователей РМ портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с сессиями пользователей РМ портала «Агрегатор»).

Таблица 391. Перечень URL-команд, связанных с сессиями пользователей РМ портала «Агрегатор»

URL-команда	Тип	Описание
/api/webui/aggregator/spsessions	GET	Возвращает список активных сессий пользователей РМ
/api/webui/aggregator/spsessions/{id}/disconnect/{session_uuid}	PATCH	Отключает активную сессию пользователя РМ
/api/webui/aggregator/spsessions/{id}/logoff/{session_uuid}	PATCH	Завершает активную сессию пользователя РМ
/api/webui/aggregator/spsessions/{id}/raconnect/{session_uuid}	PATCH	Генерация уникального URL для подключения к «Удаленному помощнику»

Команды, связанные с тегами портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с тегами).

Таблица 392. Перечень URL-команд, связанных с тегами

URL-команда	Тип	Описание
/api/webui/aggregator/tags	GET	Возвращает список тегов
/api/webui/aggregator/tags	POST	Создает тег
/api/webui/aggregator/tags/{id}	GET	Возвращает тег
/api/webui/aggregator/tags/{id}	PUT	Обновляет тег
/api/webui/aggregator/tags/{id}	PATCH	Управляет тегами
/api/webui/aggregator/tags/{id}	DELETE	Удаляет тег
/api/webui/aggregator/tags/export	GET	Формирует файл экспорта тегов

URL-команда	Тип	Описание
/api/webui/aggregator/tags/export	POST	Получает файл экспорта тегов

Команды, связанные с системными параметрами портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с системными параметрами портала «Агрегатор»).

Таблица 393. Перечень URL-команд, связанных с системными параметрами портала «Агрегатор»

URL-команда	Тип	Описание
/api/webui/aggregator/tconfig	GET	Возвращает список системных параметров
/api/webui/aggregator/tconfig	PUT	Сохраняет параметры конфигурации

Команды, связанные с управлением РМ портала «Агрегатор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с управлением РМ портала «Агрегатор»).

Таблица 394. Перечень URL-команд, связанных с управлением РМ портала «Агрегатор»

URL-команда	Тип	Описание
/api/webui/aggregator/workplaces	GET	Возвращает список РМ
/api/webui/aggregator/workplaces/{id}/assign/{servicespool_uuid}/{workplace_uuid}	PATCH	Назначает владельца РМ
/api/webui/aggregator/workplaces/{id}/delete/{servicespool_uuid}/{workplace_uuid}	DELETE	Удаляет РМ
/api/webui/aggregator/workplaces/{id}/machine/{servicespool_uuid}/{workplace_uuid}	PATCH	Управление состоянием РМ (ВМ)
/api/webui/aggregator/workplaces/{id}/maintenance/{servicespool_uuid}/{workplace_uuid}	PATCH	Управление режимом техобслуживания РМ
/api/webui/aggregator/workplaces/{id}/message/{servicespool_uuid}	POST	Отправляет сообщение в РМ
/api/webui/aggregator/workplaces/{id}/refresh/{servicespool_uuid}/{workplace_uuid}	PATCH	Возвращает ВМ на базовый снапшот
/api/webui/aggregator/workplaces/{id}/tags/{workplace_uuid}	PATCH	Редактирует список тегов РМ

«ШЛЮЗ»

Начало работы с REST API компонента «Шлюз»

Описание относится к компоненту «Шлюз», реализованного пакетом termidesk-gateway.

Формат URL-команд для компонента «Шлюз»

Общий вид URL-команд реализован следующим образом:

```
/api/<module>/<command>
```

где:

`<module>` - наименование модуля, реализованного в REST API. В текущей версии для компонента «Шлюз» доступен модуль `health`;

`<command>` - наименование команды. В текущей версии для компонента «Шлюз» доступна команда `metrics`.

Пример запроса через `curl`:

```
curl -X 'GET' \
  'http://gateway.termidesk.local:8102/api/health/metrics' \
  -H 'accept: application/json' \
  -H 'Authorization: Token 270c1e6a4cd013a382498'
```

где:

`gateway.termidesk.local` - сетевой адрес или полное доменное имя узла компонента «Шлюз»;

`8102` - порт доступа к API компонента «Шлюз»;

`270c1e6a4cd013a382498` - токен, определенный в параметре `token: ${metricsaccesskey}` конфигурационного файла «Шлюза» `/etc/termidesk/gateway.yaml`.

Если «Шлюз» настроен на использование SSL-сертификатов, то в запросе `curl` нужно указывать соответствующий протокол для подключения: вместо `http` использовать `https`.

Команды компонента «Шлюз»

Описание относится к компоненту «Шлюз», реализованного пакетом `termidesk-gateway`.

Доступные команды модуля «health» компонента «Шлюз»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «health»).

Таблица 395. Перечень URL-команд модуля «health»

URL-команда	Тип	Описание

/api/health	GET	Проверка состояния компонента.
		
		Формат запроса:
		
		`curl -X 'GET' \`
		`  'http://$\{hostname}:$\{health_port}/api/health' \`
		`  -H 'accept: application/json' \`
		`  -H 'Authorization: Token $\{health_check_access_key}'`
		
		где:
		
		${hostname} - сетевой адрес или полное доменное имя узла компонента «Шлюза»;
		
		${health_port} - порт для запросов проверки состояния, для компонента «Шлюз» - 8102. Порт определен в параметре listen: ${mgtServerIP:0.0.0.0}:${mgtServerPort:8102} конфигурационного файла «Шлюза» /etc/termidesk/gateway.yaml;
		
		${health_check_access_key} - токен, определенный в параметре token: ${healthcheckaccesskey} конфигурационного файла «Шлюза» /etc/termidesk/gateway.yaml.
		
		Формат запроса, если «Шлюз» настроен для работы по защищенному соединению:
		
		`curl --insecure -v -s -X 'GET' \`
		`  'https://$\{hostname}:$\{health_port}/api/health' \`
		`  -H 'accept: application/json' \`
		`  -H 'Authorization: Token $\{health_check_access_key}'`
		
		Ключ --insecure используется для отключения проверки валидности сертификатов. Выполнение запроса без использования проверки SSL допустимо только на тестовых стендах. В производственной среде необходимо установить валидные сертификаты.
		
		Вид возвращаемого списка:
		
		`{`
		`  "status": "pass",`
		`  "version": "0.7.0.24295",`
		`  "output": "",`
		`  "description": "Termidesk Gateway"`
		`}`

URL-команда	Тип	Описание

/api/health/metrics	GET	Возвращает список метрик узла компонента.
		
		Формат запроса:
		
		`curl -X 'GET' \`
		`  'http://$\{hostname}:$\{health_port}/api/health/metrics' \`
		`  -H 'accept: application/json' \`
		`  -H 'Authorization: Token $\{metrics_access_key}'`
		
		где:
		
		${hostname} - сетевой адрес или полное доменное имя узла компонента «Шлюза»;
		
		${health_port} - порт для запросов проверки состояния, для компонента «Шлюз» - 8102. Порт определен в параметре listen: ${mgtServerIP:0.0.0.0}:${mgtServerPort:8102} конфигурационного файла «Шлюза» /etc/termidesk/gateway.yaml;
		
		${metrics_access_key} - токен, определенный в параметре token: ${metricsaccesskey} конфигурационного файла «Шлюза» /etc/termidesk/gateway.yaml.
		
		Информацию по всем возвращаемым значениям можно получить в документации библиотеки psutil на сайте: https://psutil.readthedocs.io/en/latest.
		
		Вид возвращаемого списка метрик приведен после таблицы

Вид возвращаемого списка метрик:

```
# Версия компонента (Шлюза)
version_info{version="0.7.0.24295"} 1.0
# Версия ОС
system_info{comp_name="gateway.termidesk.local",machine="x86_64",os_name="Linux
6.1.90-1-generic",version="#astra3+ci20 SMP PREEMPT_DYNAMIC Mon Jul 22 14:15:46 UTC
2024"} 1.0
# Общая загрузка процессора в процентах
cpu_total_percent 0.1
# Общий размер физической памяти в байтах
virtual_memory_total_bytes 4107214848
# Размер доступной физической памяти в байтах
virtual_memory_available_bytes 3748093952
# Размер используемой физической памяти в байтах
virtual_memory_used_bytes 153673728
# Размер свободной физической памяти в байтах
virtual_memory_free_bytes 3794550784
# Период в секундах, в течение которого система функционирует без проблем
uptime_seconds 20652
# Общий размер диска в байтах
disk_total_bytes 15791431680
# Используемый размер диска в байтах
```

```
disk_used_bytes 4137959424
# Свободный размер диска в байтах
disk_free_bytes 10828980224
# Количество операций чтения с диска
disk_read_count 3877
# Количество операций записи на диск
disk_write_count 2899
# Число прочитанных с диска байт
disk_read_bytes 138545152
# Число записанных на диск байт
disk_write_bytes 138545152
# Информация о Шлюзе и его состоянии
gateway_info{version="0.7.0.24295", status="A"} 1.0
# Далее следует информация о сетевых метриках
# Общее количество сессий на Шлюзе
gateway_current_total_sessions 0
# Текущий входящий трафик по каждому интерфейсу в отдельности, Мбит/с
throughput_if_rx{type="lo"} 0.0
throughput_if_rx{type="eth0"} 0.005
# Текущий исходящий трафик по каждому интерфейсу в отдельности, Мбит/с
throughput_if_tx{type="lo"} 0.0
throughput_if_tx{type="eth0"} 0.0
# Общий объём входящего трафика по всем интерфейсам с момента старта Шлюза, в
байтах
bytes_if_rx{type="lo"} 0
bytes_if_rx{type="eth0"} 7033268
# Общий объём исходящего трафика по всем интерфейсам с момента старта Шлюза, в
байтах
bytes_if_tx{type="lo"} 0
bytes_if_tx{type="eth0"} 141252
```

«АГЕНТ ВИРТУАЛЬНОГО РАБОЧЕГО МЕСТА»

Начало работы с REST API компонента «Агент виртуального рабочего места»

Формат URL-команд для компонента «Агент виртуального рабочего места»

Общий вид URL-команд реализован следующим образом:

`/<uuid>/<module>/<command>`,

где:

`<uuid>` - случайное значение, генерируемое компонентом «Агент виртуального рабочего места»;

`<module>` - наименование модуля, реализованного в REST API. В текущей версии для компонента «Агент виртуального рабочего места» доступен модуль `health`;

`<command>` - наименование команды. В текущей версии для компонента «Агент виртуального рабочего места» доступна команда `metrics`.

Пример запроса через `curl`:

```
curl -k
https://agent.termidesk.local:43969/97jbI6HiRePIbYowVnsYGZyBZp4UJz29PEkzG29nEyuNmIT
E/health/metrics
```

где:

`agent.termidesk.local` - сетевой адрес или полное доменное имя узла компонента «Агент виртуального рабочего места»;

`43969` - порт компонента «Агент виртуального рабочего места»;

`97jbI6Hi…` - случайное значение, генерируемое компонентом «Агент виртуального рабочего места».

Значение порта и случайного значения можно получить из журнала работы компонента «Клиент», оно будет храниться в строке вида: «https://agent.termidesk.local:43969/HN4PlWm0wc8ZyPndsczqvXkpbDsXu44ITrdIE4WC0mLnp68W/sso_login».

В приведенном примере случайное значение - «HN4PlWm0wc8ZyPndsczqvXkpbDsXu44ITrdIE4WC0mLnp68W», значение порта - «43969».

Команды компонента «Агент виртуального рабочего места»

Доступные команды модуля «health» компонента «Агент виртуального рабочего места»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «health»).

Таблица 396. Перечень URL-команд модуля «health»

URL-команда	Тип	Описание

/health/check	GET	Проверка состояния компонента.
		
		Формат запроса:
		
		`curl -k -X 'GET' \`
		`  'https://$\{hostname}:$\{health_port}/$\{uuid}/health/check' \`
		`  -H 'accept: application/json'`
		
		где:
		
		${hostname} - сетевой адрес или полное доменное имя узла компонента «Агент виртуального рабочего места»;
		
		${port} - порт компонента «Агент виртуального рабочего места». Значение порта можно получить из журнала работы компонента «Клиент»;
		
		${uuid} - случайное значение, генерируемое компонентом «Агент виртуального рабочего места». Значение можно получить из журнала работы компонента «Клиент».
		
		Вид возвращаемого списка:
		
		`{`
		`  "status": "pass",`
		`  "version": "5.1.0.24177",`
		`  "output": "",`
		`  "description": "Termidesk Agent"`
		`}`

URL-команда	Тип	Описание
/health/metrics	-	Возвращает список метрик узла компонента. По умолчанию получение/обновление метрик происходит с интервалом в 3 секунды, однако через REST API получить метрики можно в любой момент. При этом интервал получения и обновления метрик можно изменить через переменную окружения TDSK_METRIC_INTERVAL на узле компонента «Агент виртуального рабочего места». Формат запроса: `curl -k https://$\{hostname}:$\{port}/$\{uuid}/health/metrics` где: ${hostname} - сетевой адрес или полное доменное имя узла компонента «Агент виртуального рабочего места»; ${port} - порт компонента «Агент виртуального рабочего места». Значение порта можно получить из журнала работы компонента «Клиент»; ${uuid} - случайное значение, генерируемое компонентом «Агент виртуального рабочего места». Значение можно получить из журнала работы компонента «Клиент». Информацию по всем возвращаемым значениям можно получить в документации библиотеки psutil на сайте: https://psutil.readthedocs.io/en/latest. Вид возвращаемого списка метрик приведен после таблицы

Вид возвращаемого списка метрик:

```
# Версия компонента «Агент виртуального рабочего места»
version_info{version="5.1.0.24176"} 1.0
# Версия ОС
system_info{comp_name="17sls-a17o-001",machine="x86_64",os_name="Linux 5.10.176-1-
hardened",version="#astra1 SMP Thu Mar 30 16:11:58 UTC 2023"} 1.0
# Общая загрузка процессора в процентах
cpu_total_percent 0.8
# Общий размер физической памяти в байтах
virtual_memory_total_bytes 2074025984
# Размер доступной физической памяти в байтах
virtual_memory_available_bytes 1323507712
# Размер используемой физической памяти в байтах
virtual_memory_used_bytes 550551552
# Размер свободной физической памяти в байтах
virtual_memory_free_bytes 80166912
# Период в секундах, в течение которого система функционирует без проблем
uptime_seconds 77650
# Общий размер диска в байтах
disk_total_bytes 15742214144
# Используемый размер диска в байтах
disk_used_bytes 12199178240
```

```
# Свободный размер диска в байтах
disk_free_bytes 2721058816
# Количество операций чтения с диска
disk_read_count 48247
# Количество операций записи на диск
disk_write_count 49692
# Число прочитанных с диска байт
disk_read_bytes 1661751296
# Число записанных на диск байт
disk_write_bytes 1661751296
# Информация о состоянии компонента «Агент виртуального рабочего места». A -
активен, I - простаивает/неактивен
agent_info{version="5.1.0.24176", status="A"} 1.0
# Состояние сессии - активна (A), отключена (D), ошибка (E), бездействует или
неактивна (I)
sessions_info{1="I"} 1.0
```

«СЕССИОННЫЙ АГЕНТ»

Начало работы с REST API компонента «Сессионный агент»

Формат URL-команд для компонента «Сессионный агент»

Общий вид команд реализован следующим образом:

`/<module>/<command>`

где:

`<module>` - наименование модуля, реализованного в REST API. В текущей версии доступен модуль `health`;

`<command>` - наименование команды для выполнения.

Пример команды через `curl`:

> Пример команды приведен для обращения по протоколу HTTP. Для использования протокола HTTPS компонент «Сессионный агент» должен быть настроен соответствующим образом, а именно: пути к сертификату и ключу должны быть указаны в конфигурационном файле «Сессионного агента», параметру `USE_HTTPS` должно быть присвоено значение `True`.

```
curl -X 'GET' \
  'http://agent.termidesk.local:31000/health/metrics' \
  -H 'accept: application/json' \
  -H 'Authorization: Token
HjXcGpVu8bSPEoq4NQ0qo0KpdfwoEbuTbElG3J7uSFr2aK3oPtNqlnw4VEARS2HY'
```

где:

`agent.termidesk.local` - сетевой адрес или полное доменное имя узла компонента

«Сессионный агент»;

31000 - порт для запросов проверки состояния, для компонента «Сессионный агент» - 31000;

Authorization: Token - токен, определенный в параметре METRICS_ACCESS_KEY конфигурационного файла «Сессионного агента»: /etc/opt/termidesk-session-agent/session_agent.ini (для ОС Astra Linux Special Edition (Server)) или %ProgramData%\UVEON\Termidesk Session Agent\session_agent.ini (для ОС Microsoft Windows Server).

Команды компонента «Сессионный агент»

Доступные команды модуля «health» компонента «Сессионный агент»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «health»).

Таблица 397. Перечень URL-команд модуля «health»

URL-команда	Тип	Описание

/health/check	GET	Проверка состояния компонента.
		
		Формат запроса:
		
		`curl -X 'GET' \`
		`  'http://$\{hostname}:$\{health_port}/health/check' \`
		`  -H 'accept: application/json' \`
		`  -H 'Authorization: Token $\{health_check_access_key}'`
		
		где:
		
		${hostname} - сетевой адрес или полное доменное имя узла компонента «Сессионный агент»;
		
		${health_port} - порт для запросов проверки состояния, для компонента «Сессионный агент» - 31000;
		
		${health_check_access_key} - токен, определенный в параметре HEALTH_CHECK_ACCESS_KEY конфигурационного файла «Сессионного агента».
		
		Сразу после установки токен HEALTH_CHECK_ACCESS_KEY имеет значение None (не задано), в этом случае проверка токена не производится и запрос можно выполнять без конструкции Authorization: Token.
		
		Вид возвращаемого списка:
		
		`{`
		`  "status": "pass",`
		`  "version": "5.0.0.24118",`
		`  "output": "",`
		`  "description": "termidesk-session-agent"`
		`}`

URL-команда	Тип	Описание

/health/metrics	GET	Возвращает список метрик узла компонента.
		
		Формат запроса:
		
		`curl -X 'GET' \`
		`  'http://$\{hostname}:$\{health_port}/health/metrics' \`
		`  -H 'accept: application/json' \`
		`  -H 'Authorization: Token $\{metrics_access_key}'`
		
		где:
		
		${hostname} - сетевой адрес или полное доменное имя узла компонента «Сессионный агент»;
		
		${health_port} - порт для запросов проверки состояния, для компонента «Сессионный агент» - 31000;
		
		${metrics_access_key} - токен, определенный в параметре METRICS_ACCESS_KEY конфигурационного файла «Сессионного агента».
		
		Сразу после установки токен METRICS_ACCESS_KEY имеет значение None (не задано), в этом случае проверка токена не производится и запрос можно выполнять без конструкции Authorization: Token.
		
		Информацию по всем возвращаемым значениям можно получить в документации библиотеки psutil на сайте: https://psutil.readthedocs.io/en/latest.
		
		Вид возвращаемого списка метрик приведен после таблицы

Вид возвращаемого списка метрик:

```
# Версия компонента
version_info{version="5.0.24152"} 1.0
# Версия ОС
system_info{machine="x86_64",os="Linux 5.15.0-33-generic",version="#astra2+ci96 SMP
Fri Oct 28 18:23:37 UTC 2022"} 1.0
# Общая загрузка процессора в процентах
cpu_total_percent 4.0
# Общее использование физической памяти в процентах
virtual_memory_total_percent 70.3
# Общий размер физической памяти в байтах
virtual_memory_total_bytes 2.070183936e+09
# Размер доступной физической памяти в байтах
virtual_memory_available_bytes 6.1464576e+08
# Размер используемой физической памяти в байтах
virtual_memory_used_bytes 1.26932992e+09
# Размер свободной физической памяти в байтах
virtual_memory_free_bytes 3.23608576e+08
# Общий размер диска в байтах
disk_total_bytes 1.9994066944e+010
# Используемый размер диска в байтах
```

```
disk_used_bytes 1.005756416e+010
# Свободный размер диска в байтах
disk_free_bytes 8.897261568e+09
# Период в секундах, в течение которого система функционирует без проблем
uptime_seconds 2.256339795133114e+06
# Количество операций чтения с диска
disk_read_count 271249.0
# Количество операций записи на диск
disk_write_count 865272.0
# Число прочитанных с диска байт
disk_read_bytes 7.215997952e+09
# Число записанных на диск байт
disk_write_bytes 9.192820736e+09
# Состояние сессии - активна (A), бездействует или любое другое состояние (I)
sessions_info 1.0
```

«ОРКЕСТРАТОР»

Начало работы с REST API компонента «Оркестратор»

Формат URL-команд для компонента «Оркестратор»

Общий вид команд реализован следующим образом:

`/api/<ver>/<module>`

где:

`<ver>` - версия API;

`<module>` - наименование модуля, реализованного в REST API.

Пример команды через curl:

```
curl -X 'GET' \
  'https://orchestrator.termidesk.local/api/draft/orc/health/' \
  -H 'accept: application/json' \
  -H 'X-ORC-TOKEN-APP:
HjXcGpVu8bSPEoq4NQ0qo0KpdfwoEbuTbElG3J7uSFr2aK3oPtNqlnw4VEARS2HY'
```

где:

`orchestrator.termidesk.local` - сетевой адрес или полное доменное имя узла компонента «Оркестратор» Termidesk VDI;

`X-ORC-TOKEN-APP` - токен аутентификации компонента «Оркестратор» в поставщике ресурсов OpenStack. Значение токена уникально и время его жизни ограничено.

Электронный справочник по командам REST API компонента «Оркестратор»

Полная информация о параметрах и командах REST API доступна при вводе URL-команды `https://orchestrator.termidesk.local/api/docs/`, где `orchestrator.termidesk.local` - сетевой адрес или полное доменное имя узла компонента «Оркестратор» Termidesk VDI.

Команды компонента «Оркестратор»

Доступные команды модуля «health» компонента «Оркестратор»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с проверкой состояния Termidesk VDI).

Таблица 398. Перечень URL-команд, связанных с проверкой состояния Termidesk VDI

URL-команда	Тип	Описание
`api/draft/health`	GET	Проверка состояния Termidesk
`api/draft/orc/health`	GET	Проверка состояния компонента «Оркестратор» Termidesk

Доступные команды модуля «infra»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с управлением инфраструктурой Termidesk VDI).

Таблица 399. Перечень URL-команд, связанных с управлением инфраструктурой Termidesk VDI

URL-команда	Тип	Описание
`api/draft/infra`	POST	Создание ВМ для поставщика ресурсов OpenStack
`api/draft/configure_infra`	POST	Подготовка среды функционирования Termidesk VDI на ВМ
`api/draft/install_termidesk`	POST	Установка программного комплекса Termidesk VDI на ВМ

Доступные команды для управления компонентом «Универсальный диспетчер»

Команды, связанные с управлением доменами аутентификации

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с управлением доменами аутентификации).

Таблица 400. Перечень URL-команд, связанных с управлением доменами аутентификации

URL-команда	Тип	Описание
`/api/draft/auth`	POST	Добавление домена аутентификации
`/api/draft/auth/types`	GET	Возвращение списка типов доменов аутентификации
`/api/draft/auth`	GET	Возвращение списка доменов аутентификации
`/api/draft/auth/<id>/groups`	GET	Возвращение списка групп пользователей домена аутентификации
`/api/draft/auth/<id>/groups`	POST	Добавление группы домена аутентификации

URL-команда	Тип	Описание
/api/draft/auth/<id>/users	GET	Возвращение списка пользователей домена аутентификации
/api/draft/auth/<id>/users	POST	Добавление пользователя домена аутентификации
/api/draft/auth/<id>/users/<user>/pools	GET	Возвращение списка фондов РМ, назначенных пользователю
/api/draft/auth/<id>/users/<user>/vms	GET	Возвращение списка РМ, назначенных пользователю

Команды, связанные с управлением поставщиками ресурсов

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с управлением поставщиками ресурсов).

Таблица 401. Перечень URL-команд, связанных с управлением поставщиками ресурсов

URL-команда	Тип	Описание
/api/draft/providers	POST	Добавление поставщика ресурсов
/api/draft/providers/overview	GET	Возвращение списка поставщиков ресурсов
/api/draft/providers/<id>/services/overview	GET	Возвращение списка шаблонов РМ
/api/draft/providers/<id>/services/types	GET	Возвращение списка типов шаблонов ВМ
/api/draft/providers/<uid>/services/gui/<type>	GET	Возвращение описания графического интерфейса шаблонов РМ

Команды, связанные с управлением шаблонами ВМ

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с управлением шаблонами ВМ).

Таблица 402. Перечень URL-команд, связанных с управлением шаблонами ВМ

URL-команда	Тип	Описание
/api/draft/providers/<uuid>/services	POST	Создание шаблона РМ
/api/draft/providers/<prov>/services/<id>	GET	Возвращение информации о шаблоне РМ

Команды, связанные с управлением параметрами гостевых ОС

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с управлением параметрами гостевых ОС).

Таблица 403. Перечень URL-команд, связанных с управлением параметрами гостевых ОС

URL-команда	Тип	Описание
/api/draft/osmanagers	POST	Добавление параметра управления гостевой ОС

Команды, связанные с управлением протоколами доставки

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с управлением протоколами доставки).

Таблица 404. Перечень URL-команд, связанных с управлением протоколами доставки

URL-команда	Тип	Описание
/api/draft/transports	POST	Добавление протокола доставки
/api/draft/transports/types	GET	Возвращение списка типов протоколов доставки
/api/draft/transports/overview	GET	Возвращение списка протоколов доставки

Команды, связанные с управлением фондами рабочих мест

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с управлением фондами РМ).

Таблица 405. Перечень URL-команд, связанных с управлением фондами РМ

URL-команда	Тип	Описание
/api/draft/pools	GET	Возвращение списка фондов РМ
/api/draft/pools	POST	Добавление фонда РМ
/api/draft/pools/<id>	GET	Возвращение информации о фонде РМ
/api/draft/pools/<id>/vms	GET	Возвращение списка назначенных РМ
/api/draft/pools/<id>/cache	GET	Возвращение списка РМ, находящихся в кеше
/api/draft/pools/<id>/groups	POST	Добавление группы в фонд РМ
/api/draft/pools/<id>/transports	POST	Добавление протокола доставки в фонд РМ
/api/draft/pools/gui	GET	Возвращение описания графического интерфейса фонда РМ
/api/draft/pools/<id>/groups/overview	GET	Возвращение списка групп фонда РМ
/api/draft/pools/<id>/transports/overview	GET	Возвращение списка протоколов доставки фонда РМ

Команды, связанные с аудитом и мониторингом Termidesk

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с аудитом и мониторингом Termidesk VDI).

Таблица 406. Перечень URL-команд, связанных с аудитом и мониторингом Termidesk VDI

URL-команда	Тип	Описание
/api/draft/monitoring	GET	Возвращение списка операций
/api/draft/audit	GET	Возвращение списка событий аудита

Команды, связанные с управлением сессиями

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с управлением сессиями).

Таблица 407. Перечень URL-команд, связанных с управлением сессиями

URL-команда	Тип	Описание
/api/draft/sessions	GET	Возвращение списка активных сессий пользователей

URL-команда	Тип	Описание
/api/draft/sessions/<session>/logoff	PATCH	Останов активной сессии пользователя

Команды, связанные с запросами о данных ВМ

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд, связанных с запросами о данных ВМ).

Таблица 408. Перечень URL-команд, связанных с запросами о данных ВМ

URL-команда	Тип	Описание
/api/draft/util/resources	GET	Возвращение списка ВМ поставщика ресурсов OpenStack
/api/draft/util/images	GET	Возвращение списка образов ВМ поставщика ресурсов OpenStack

«УДАЛЕННЫЙ ПОМОЩНИК»

Начало работы с REST API компонента «Удаленный помощник»

Формат URL-команд для компонента «Удаленный помощник»

Общий вид команд реализован следующим образом:

/api/<module>

где:

<module> - наименование модуля, реализованного в REST API.

Список модулей API, предоставляемого компонентом, может быть получен URL-командой /api/discover/.

Пример команды через curl:

```
curl -X 'GET' \
  'https://assistant.termidesk.local/api/discover/' \
  -H 'accept: application/json' \
  -H 'X-CSRFToken:
HjXcGpVu8bSPEoq4NQ0qo0KpdfwoEbuTbElG3J7uSFr2aK3oPtNqlnw4VEARS2HY'
```

где:

assistant.termidesk.local - сетевой адрес или полное доменное имя узла компонента «Удаленный помощник» Termidesk VDI;

X-CSRFToken - уникальный идентификатор запроса, генерируемый Django. Значение токена уникально и время его жизни ограничено.

Электронный справочник по командам REST API компонента «Удаленный помощник»

Полная информация о параметрах и командах REST API доступна при вводе URL-команды

https://assistant.termidesk.local/assistant/api/docs/, где assistant.termidesk.local - сетевой адрес или полное доменное имя узла компонента «Удаленный помощник» Termidesk VDI.

Команды компонента «Удаленный помощник»

Доступные команды модуля «settings»

Доступные администратору URL-команды перечислены в таблице (см. таблицу Перечень URL-команд модуля «settings»).

Команда /assistant/api/{session_id}/settings объявлена устаревшей.

Таблица 409. Перечень URL-команд модуля «settings»

URL-команда	Тип	Описание
/assistant/{session_id}/settings	GET	Получение информации о сессии. Пример запроса через утилиту curl: `curl --insecure -X 'GET' 'https://assistant.termidesk.local/assistant/2345/settings -H 'accept: application/json'` где: --insecure - отключение проверки валидности сертификатов. Выполнение запроса без использования проверки SSL допустимо только на тестовых стендах. В производственной среде необходимо установить валидные сертификаты; 2345 - идентификатор сессии; assistant.termidesk.local - сетевой адрес или полное доменное имя узла серверной части компонента «Удаленный помощник» Termidesk
/assistant/api/{session_id}/settings	GET	Получение информации о сессии
/assistant/api	PUT	Создание сессии и возврат относительной ссылки на подключение

ТЕРМИНЫ

Компонент «Агент»

Самостоятельный компонент, отвечающий за контролируемую доставку РМ, взаимодействие с «Универсальным диспетчером» и «Менеджером рабочих мест». Собирательное название для следующих компонентов Termidesk VDI:

- «Агент виртуального рабочего места»;
- «Агент узла виртуализации»;
- «Сессионный агент»;
- «Видеоагент»;
- «Агент виртуальных смарт-карт».

Компонент «Агент виртуального рабочего места»

Компонент Termidesk VDI. Устанавливается в гостевую ОС при подготовке базового виртуального РМ (ВРМ). Выполняет взаимодействие с «Универсальным диспетчером», конфигурирует ВРМ, фиксирует действия пользователя, реализует передачу управляющих сообщений

Компонент «Сессионный агент»

Компонент Termidesk VDI. Устанавливается на терминальный сервер (MS RDS/STAL), активирует возможность множественного доступа пользователей к удаленным рабочим столам и приложениям

Виртуальное рабочее место

Развернутая на ВМ ОС с установленным «Агентом виртуального рабочего места» и необходимым прикладным ПО. Подключение к ВРМ происходит через протоколы удаленного доступа

Рабочее место

Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа. Под рабочими местами подразумеваются как ВРМ, так и терминальный доступ или доступ к опубликованным на сервере терминалов приложениям

Гостевая ОС

ОС, функционирующая на ВМ

Группы рабочих мест

Функциональное объединение множества фондов РМ по определенному признаку

Домен аутентификации

Способ проверки субъектов и их полномочий

Компонент «Менеджер рабочих мест»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за взаимодействие с поставщиком ресурсов и управления жизненным циклом РМ, включая создание, настройку, запуск, отключение и удаление. Является обработчиком фоновых задач. Устанавливается из пакета `termidesk-vdi`. Наименование служб после установки: `termidesk-celery-beat.service` и `termidesk-celery-worker.service`

Компонент «Оркестратор»

Компонент Termidesk VDI. Самостоятельный компонент, отвечающий за согласованную работу всех компонентов программного комплекса при децентрализованном развертывании, для нужд отказоустойчивости и комплексирования с облачными службами

Поставщик ресурсов

ОС, платформа виртуализации или терминальный сервер (MS RDS/STAL), предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов РМ

Протокол доставки

Поддерживаемый в Termidesk VDI протокол удаленного доступа к РМ

Компонент «Универсальный диспетчер»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им РМ и контроля доставки РМ. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-vdi.service`

Фонд рабочих мест

Совокупность подготовленных РМ для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей

Компонент «Шлюз»

Компонент Termidesk VDI. Самостоятельный компонент, отвечающий за туннелирование протоколов доставки, использующих транспортный протокол TCP. Устанавливается из пакета `termidesk-gateway`. Наименование службы после установки: `termidesk-gateway.service`

Портал администратора

Предоставляет веб-интерфейс для управления Termidesk VDI и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API

Портал пользователя

Предоставляет пользовательский веб-интерфейс Termidesk VDI (без доступа к функциям управления) и интерфейс swagger для доступа к ограниченному списку модулей документации по командам REST API

Портал универсальный

Предоставляет функции обоих вариантов - и «Портала администратора», и «Портала пользователя». При этом активируется доступ ко всем модулям документации по командам REST API, предоставляемым интерфейсом Swagger

Ключ

Применяется в контексте файла, не опции в команде. Последовательность псевдослучайных чисел, сгенерированная особым образом

Сертификат

Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу

СОКРАЩЕНИЯ

БД	База данных
ВМ	Виртуальная машина
ВРМ	Виртуальное рабочее место
ОС	Операционная система
ПО	Программное обеспечение
РМ	Рабочее место
API	Application Programming Interface (интерфейс прикладного программирования)
FQDN	Fully Qualified Domain Name (полностью определенное имя домена)
HTML	Hypertext Markup Language (язык гипертекстовой разметки)
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста)
HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
ID	Identification Data (идентификатор)

IP	Internet Protocol (межсетевой протокол)
PKINIT	Public Key Cryptography for Initial Authentication (механизм Kerberos, позволяющий использовать сертификаты X.509)
RDP	Remote Desktop Protocol (протокол удаленного рабочего стола)
RDS	Remote Desktop Services (службы удаленного рабочего стола Microsoft)
REST	Representational State Transfer (программная архитектура, определяющая условия работы API)
SPICE	Simple Protocol for Independent Computing Environments (простой протокол для независимой вычислительной среды)
SSL	Secure Sockets Layer (криптографический протокол)
STAL	Terminal Server Astra Linux (компонент «Сервер терминалов Astra Linux»)
TCP	Transmission Control Protocol (протокол управления передачей)
UDP	User Datagram Protocol (протокол пользовательских датаграмм)
URL	Uniform Resource Locator (унифицированный указатель ресурса)
UUID	Universally Unique Identifier (уникальный идентификатор)

СЛЕТ.10001-01 91 02. ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ. КОМПОНЕНТ «УДАЛЕННЫЙ ПОМОЩНИК»

ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ

Назначение документа

Настоящий документ является инструкцией по использованию компонента «Удаленный помощник» программного комплекса «Диспетчер подключений виртуальных рабочих мест Термидеск» (далее - Termidesk VDI, Termidesk VDI). Документ предназначен для администраторов системы и сети.

В документе приведено назначение, установка и использование компонента «Удаленный помощник».

Типографские соглашения

Приняты следующие типографские соглашения:

- `моноширинный шрифт` – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk VDI, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

УДАЛЕННЫЙ ПОМОЩНИК. ОБЩИЕ СВЕДЕНИЯ

Назначение компонента «Удаленный помощник»

Компонент «Удаленный помощник» (далее - Удаленный помощник) входит в состав Termidesk VDI.

Удаленный помощник предоставляет администратору или специалисту технической поддержки экран узла пользователя через сеанс удаленного подключения и обеспечивает передачу голосовой информации для взаимодействия с пользователем.

Удаленный помощник состоит из серверной и клиентской частей. Серверная часть устанавливается на узел консультирующего специалиста, а клиентская часть на узел пользователя.

Требования к программному и аппаратному обеспечению

Для установки серверной части Удаленного помощника минимальные аппаратные и программные требования узла должны соответствовать следующим:

- оперативная память, не менее 4 ГБ;
- свободное дисковое пространство, не менее 1 ГБ;
- сетевое соединение, не менее 100 Мбит/с.

Серверная часть Удаленного помощника устанавливается на операционную систему (ОС):

- Astra Linux Special Edition 1.8 (1.7.1, 1.7.2, 1.7.3, 1.7.4, 1.7.5, 1.7.6, 1.7.7, 1.7.7, 1.7.9);
- Astra Linux Special Edition 1.8 (1.8.1, 1.8.2, 1.8.3, 1.8.4).

Для установки клиентской части Удаленного помощника минимальные аппаратные требования узла должны соответствовать следующим:

- процессор архитектуры Intel x86 с разрядностью 64 бит;
- оперативная память, не менее 1 ГБ;
- свободное дисковое пространство, не менее 200 МБ;
- сетевое соединение, не менее 100 Мбит/с.

Клиентская часть Удаленного помощника устанавливается на ОС:

- Astra Linux Special Edition 1.8 (1.7.1, 1.7.2, 1.7.3, 1.7.4, 1.7.5, 1.7.6, 1.7.7, 1.7.7, 1.7.9);
- Astra Linux Special Edition 1.8 (1.8.1, 1.8.2, 1.8.3, 1.8.4, 1.8.5, 1.8.6);
- Microsoft Windows 10 1809 LTS;
- Microsoft Windows 11 LTSC 2024.

УДАЛЕННЫЙ ПОМОЩНИК. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ

Получение пакетов установки в ОС Astra Linux Special Edition

Дистрибутив представлен бинарным файлом пакета ПО в `deb`-формате. Установка в ОС Astra Linux Special Edition производится из локального репозитория, распространяемого в формате `iso`-образа.

Получить `iso`-образ можно двумя способами:

- заполнив запрос через сайт Termidesk VDI: https://termidesk.ru/support/#request-support;
- через личный кабинет:https://lk.astra.ru/.

Для подключения локального репозитория Termidesk VDI на узле, где предполагается установка, нужно:

- скопировать в домашний каталог пользователя образ диска `termidesk-<версия>.iso`;
- подключить образ диска к файловой системе в каталог `/mnt`:

```
sudo mount -o loop termidesk-<версия>.iso /mnt
```

где:

`-o loop` - параметры для привязки петлевого устройства (`/dev/loop`) к файлу `termidesk-<версия>.iso`, устройство затем монтируется в указанный каталог `/mnt`;

- скопировать содержимое каталога `repos` подключенного образа диска в каталог `/var` локальной файловой системы:

```
sudo cp -Rp /mnt/repos /var
```

где:

`-Rp` - ключ для рекурсивного копирования подкаталогов и файлов с сохранением исходных свойств;

- отключить подключенный ранее образ диска от узла:

```
sudo umount /mnt
```

- установить пакет `lsb-release`:

```
sudo apt install -y lsb-release
```

- добавить локальный репозиторий Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list` через командный интерпретатор `sh`:
  - выяснить установленную версию ОС:

    ```
    sudo cat /etc/astra_version
    ```

  - определить актуальное имя каталога с пакетами в `/var/repos`;
  - указать в файле конфигурации APT корректное (фактическое) имя каталога:

    ```
    sudo sh -c 'echo "deb file:/var/repos/astra 1.8_x86-64 non-free" >
    /etc/apt/sources.list.d/termidesk_local.list'
    ```

    где:

    `-c` - ключ для чтения команд из вводимой строки (стандартный ввод);

    `echo` - команда вывода текста, совместно с символом «>» используется для перенаправления строки в файл;

    `deb file:/var/repos/astra 1.8_x86-64 non-free` - добавляемый репозиторий с вложенной командой получения версии ОС;

    Приведенный пример команды актуален для установки основных компонентов Termidesk, пакеты которых расположены в каталоге `1.8_x86-64`.

- для корректной установки компонентов TERA потребуется корректно подключить дополнительные репозитории и настроить их приоритет:
  - для версий ОС Astra Linux Special Edition меньше или равных 1.7.6, а также для версий 1.8.X:
    - подключить два репозитория:

      ```
      sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
      non-free" > /etc/apt/sources.list.d/termidesk_local.list'
      sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
      ```

```
/dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

- добавить повышенный приоритет для репозитория с требуемой версией ОС (значение `$(cat /etc/astra_version)` может подходить не для всех репозиториев, т.к. версия может указываться без точек - в этом случае нужно вручную указать корректную версию):

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000
EOF"
```

- для версий ОС Astra Linux Special Edition 1.7.7 и 1.7.8:
  - подключить три репозитория:

```
sudo sh -c 'echo "deb file:/var/repos/astra 1.7.6 non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
/dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

  - настроить два приоритета:

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=1.7.6
Pin-Priority: 950

Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000

EOF"
```

- выполнить поиск ключа репозитория Termidesk VDI `GPG-KEY-PUBLIC` и добавить его:

```
sudo cat /var/repos/astra/GPG-KEY-PUBLIC | sudo gpg --dearmour -o
/etc/apt/trusted.gpg.d/termidesk.gpg
```

- убедиться, что ключ `release@uveon.ru` был успешно добавлен:

```
apt-key list
```

В случае, если ключ не отображен в выводе команды, необходимо убедиться, что ключ `GPG-KEY-PUBLIC` существует:

```
cat /var/repos/astra/GPG-KEY-PUBLIC
```

Если ключ все же существует, следует проверить правильность выполнения шагов по добавлению репозитория Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list`.

При успешном выполнении всех шагов команда выведет содержимое ключа в формате Base64.

В зависимости от используемой версии ОС команды добавления ключа репозитория Termidesk VDI могут отличаться. Если для ОС Astra Linux Special Edition 1.8 ключ репозитория был добавлен командой, применимой к другой версии ОС, то для исправления нужно:

- узнать идентификатор добавленного ключа репозитория:

```
apt-key list
```

- удалить ключ:

```
apt-key --keyring /etc/apt/trusted.gpg del 4E1632CC
```

где `4E1632CC` - последние 8 символов идентификатора ключа;

- вновь добавить ключ репозитория.

- обновить данные пакетного менеджера:

```
sudo apt update
```

- проверить настройку приоритетов репозиториев:

```
apt-cache policy
```

Команду `sudo apt update` необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.

УДАЛЕННЫЙ ПОМОЩНИК. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ

ОС Astra Linux Special Edition

Установка, обновление, удаление серверной части в Astra Linux Special Edition

Установка серверной части в ОС Astra Linux Special Edition

Не рекомендуется устанавливать серверную часть Удаленного помощника на узел с установленным компонентом «Универсальный диспетчер», поскольку оба компонента вносят изменения в конфигурацию веб-сервера apache.

Для установки серверной части Удаленного помощника:

- для ОС Astra Linux Special Edition версии 1.7.4 и 1.7.5 обновить пакет `libastraevents`:

```
sudo apt install --only-upgrade libastraevents
```

- подключить локальный репозиторий Termidesk VDI;
- выполнить:

```
sudo apt install termidesk-assistant-server
```

Установка будет выполнена в каталог `/opt/termidesk/share/assistant`. После установки настройки веб-сервера apache доступны в конфигурационном файле `/etc/apache2/sites-available/termidesk-assistant.conf`.

Установку также можно выполнить из `deb`-пакета без подключения репозитория:

```
sudo apt install <путь_к_пакету_termidesk-assistant-server>
```

- в окне «Настройки сервера» оставить значения по умолчанию или при необходимости изменить значения:
  - «Каталог конфигурации»: каталог хранения конфигурационного файла. Значение по умолчанию: `/etc/opt/termidesk-assistant`;
  - «Каталог журналов сервера»: каталог хранения журналов для непривилегированного пользователя. Значение по умолчанию: `/var/log/termidesk/assistant`.

Окно «Настройки сервера» будет показано единожды, если конфигурационный файл `assistant.conf` отсутствует в системе.

Предпочтительные значения в расширенных настройках будут подставлены автоматически. Если настройки были изменены, то значения подставятся с учетом их приоритета:

- в первую очередь подставляются значения из переменных окружения. Все ранее заданные значения конфигурационного файла игнорируются;
- если переменные окружения не заданы, то подставляются значения из конфигурационного файла;
- если ничего из пунктов выше не задано, то применяются значения по умолчанию.

После установки изменить настройки можно через указание переменных

окружения в файле /etc/default/termidesk-assistant-server.

Для «тихой» установки без отображения дополнительных окон следует назначить переменные окружения TDSK_SETUP_NONINTERACTIVE, TDSK_CONFIG_DIR, TDSK_LOG_SRV_DIR и передать их в команду установки:

```
sudo TDSK_SETUP_NONINTERACTIVE=1 TDSK_CONFIG_DIR=<путь_к_каталогу>
TDSK_LOG_SRV_DIR=<путь_к_каталогу> apt install termidesk-assistant-server
```

Где:

- TDSK_SETUP_NONINTERACTIVE=1 - переменная, указывающая запуск в режиме «тихой» установки;
- TDSK_CONFIG_DIR=<путь_к_каталогу> - переменная, указывающая путь к каталогу с конфигурационным файлом assistant.conf. Например, TDSK_CONFIG_DIR=/etc/termidesk-test;
- TDSK_LOG_SRV_DIR=<путь_к_каталогу> - переменная, указывающая путь к каталогу хранения журналов для непривилегированного пользователя.

Далее необходимо скорректировать файл конфигурации веб-сервера /etc/apache2/apache2.conf. Для этого найти и раскомментировать строку с параметром AstraMode, далее присвоить данному параметру значение off, точно соблюдая отступы и пробелы в файле:

```
# Astra security mode
#
AstraMode off
```

Затем перезапустить веб-сервер:

```
sudo systemctl restart apache2
```

И выполнить активацию HTTPS-сервера командами:

```
sudo a2ensite default-ssl
sudo systemctl reload apache2
```

Выполнять команды по активации нужно только в случае, если на данном узле ранее не был настроен HTTPS-сервер.

После установки серверной части автоматически запускается и добавляется в автозагрузку ОС служба termidesk-assistant-server.

Проверка состояния службы производится командой:

```
sudo systemctl status termidesk-assistant-server
```

Строка Active отображает состояние сервиса, где статус active (running) означает

успешный запуск.

При необходимости ручного перезапуска службы выполнить:

```
sudo systemctl restart termidesk-assistant-server
```

Строка `Active` отображает состояние сервиса, где статус `active (running)` означает успешный запуск.

Обновление серверной части в ОС Astra Linux Special Edition

Обновление серверной части Удаленного помощника производится установкой новой версии поверх предыдущей.

Удаление серверной части в ОС Astra Linux Special Edition

Для удаления серверной части Удаленного помощника из среды ОС Astra Linux Special Edition выполнить:

```
sudo apt purge termidesk-assistant-server
```

Установка, обновление, удаление клиентской части в Astra Linux Special Edition

Установка клиентской части в ОС Astra Linux Special Edition

Для установки клиентской части Удаленного помощника:

- подключить локальный репозиторий Termidesk VDI;
- выполнить:

```
sudo apt install termidesk-assistant-client
```

> Установку также можно выполнить из `deb`-пакета без подключения репозитория:
>
> ```
> sudo apt install <путь_к_пакету_termidesk-assistant-client>
> ```

- в окне «Расширенные настройки» оставить значения по умолчанию или при необходимости изменить значения:
  - «Каталог журналов пользователя»: каталог хранения журналов для непривилегированного пользователя. Значение по умолчанию: `~./config/UVEON/logs`;
  - «Каталог настроек»: каталог хранения конфигурационного файла. Значение по умолчанию: `/etc/termidesk/assistant`.

> Окно «Расширенные настройки» будет показано единожды, если конфигурационный файл `client.conf` отсутствует в системе.
>
> Предпочтительные значения в расширенных настройках будут

подставлены автоматически. Если настройки были изменены, то значения подставятся с учетом их приоритета:

- в первую очередь подставляются значения из переменных окружения. Все ранее заданные значения конфигурационного файла игнорируются;
- если переменные окружения не заданы, то подставляются значения из конфигурационного файла;
- если ничего из пунктов выше не задано, то применяются значения по умолчанию.

После установки изменить настройки можно через указание переменных окружения в файле `/etc/default/termidesk-assistant-client`.

Для «тихой» установки без отображения дополнительных окон следует назначить переменные окружения `TDSK_SETUP_NONINTERACTIVE`, `TDSK_CONFIG_DIR`, `TDSK_LOG_USER_DIR` и передать их в команду установки:

```
sudo TDSK_SETUP_NONINTERACTIVE=1 TDSK_CONFIG_DIR=<путь_к_каталогу>
TDSK_LOG_USER_DIR=<путь_к_каталогу> apt install termidesk-assistant-client
```

Где:

- `TDSK_SETUP_NONINTERACTIVE=1` - переменная, указывающая запуск в режиме «тихой» установки;
- `TDSK_CONFIG_DIR=<путь_к_каталогу>` - переменная, указывающая путь к каталогу с конфигурационным файлом `client.cfg`. Например, `TDSK_CONFIG_DIR=/etc/termidesk-test`;
- `TDSK_LOG_USER_DIR=<путь_к_каталогу>` - переменная, указывающая путь к каталогу хранения журналов для непривилегированного пользователя.

После установки клиентской части в ОС станет доступно графическое приложение «Termidesk Assistant» для подключения к серверной части Удаленного помощника. Для доступа к графическому приложению следует открыть меню «Звезда», выбрать пункт «Утилиты» и в выпадающем меню щелкнуть левой кнопкой мыши по строке «Termidesk Assistant».

Обновление клиентской части в ОС Astra Linux Special Edition

Обновление клиентской части Удаленного помощника производится установкой новой версии поверх предыдущей.

Удаление клиентской части в ОС Astra Linux Special Edition

Для удаления клиентской части Удаленного помощника из среды ОС Astra Linux Special Edition выполнить:

```
sudo apt purge termidesk-assistant-client
```

Установка в режиме ЗПС

Замкнутая программная среда (ЗПС) является средством повышения безопасности ОС путем контроля целостности (неизменности) файлов.

Механизм контроля реализован в виде невыгружаемого модуля ядра ОС Astra Linux Special

Edition (модуль digsig_verif), выполняющего проверку электронной цифровой подписи файлов (ЭЦП).

Перед установкой компонентов Termidesk VDI необходимо установить пакет termidesk-digsig-keys, для этого:

- подключить репозиторий Termidesk VDI или получить отдельный пакет termidesk-digsig-keys из репозитория;
- выполнить установку с использованием репозитория:

```
sudo apt -y install termidesk-digsig-keys
```

- либо выполнить установку из deb-пакета:

```
sudo apt install -y /home/user/termidesk-digsig-keys-XXXXXX_amd64.deb
```

где:

-y - ключ для пропуска подтверждения установки;

/home/user/termidesk-digsig-keys-XXXXXX_amd64.deb - расположение пакета termidesk-digsig-keys-XXXXXX_amd64.deb.

- перезагрузить ОС:

```
sudo reboot
```

- выполнить установку компонента Termidesk VDI.

Для ЗПС может быть активирован режим проверки встроенной ЭЦП в расширенных атрибутах (DIGSIG_XATTR_MODE). В этом случае потребуется подписать файлы, которые будут проходить проверку, имеющимися в организации ключами. Информация о процессе подписи и активации механизма проверки встроенной ЭЦП в расширенных атрибутах приведена в справочном центре Astra Linux: https://wiki.astralinux.ru/pages/viewpage.action?pageId=41190634.

Другие ОС Linux

Установка, обновление, удаление клиентской части в других ОС Linux

Установка клиентской части в других ОС Linux

Для установки клиентской части Удаленного помощника:

- выполнить:

```
sudo apt install <путь_к_пакету_termidesk-assistant-client>
```

В зависимости от дистрибутива ОС Linux команда установки может отличаться от приведенной. Например, при использовании пакетного

менеджера yum следует использовать команду:

```
sudo yum install <путь_к_пакету_termidesk-assistant-client>
```

- в окне «Расширенные настройки» оставить значения по умолчанию или при необходимости изменить значения:
  - «Каталог журналов пользователя»: каталог хранения журналов для непривилегированного пользователя. Значение по умолчанию: `~./config/UVEON/logs`;
  - «Каталог настроек»: каталог хранения конфигурационного файла. Значение по умолчанию: `/etc/termidesk/assistant`.

Окно «Расширенные настройки» будет показано единожды, если конфигурационный файл `client.conf` отсутствует в системе.

Предпочтительные значения в расширенных настройках будут подставлены автоматически. Если настройки были изменены, то значения подставятся с учетом их приоритета:

- в первую очередь подставляются значения из переменных окружения. Все ранее заданные значения конфигурационного файла игнорируются;
- если переменные окружения не заданы, то подставляются значения из конфигурационного файла;
- если ничего из пунктов выше не задано, то применяются значения по умолчанию.

После установки изменить настройки можно через указание переменных окружения в файле `/etc/default/termidesk-assistant-client`.

Для «тихой» установки без отображения дополнительных окон следует назначить переменные окружения `TDSK_SETUP_NONINTERACTIVE`, `TDSK_CONFIG_DIR`, `TDSK_LOG_USER_DIR` и передать их в команду установки:

```
sudo TDSK_SETUP_NONINTERACTIVE=1 TDSK_CONFIG_DIR=<путь_к_каталогу>
TDSK_LOG_USER_DIR=<путь_к_каталогу> apt install termidesk-assistant-client
```

Где:

- `TDSK_SETUP_NONINTERACTIVE=1` - переменная, указывающая запуск в режиме «тихой» установки;
- `TDSK_CONFIG_DIR=<путь_к_каталогу>` - переменная, указывающая путь к каталогу с конфигурационным файлом `client.cfg`. Например, `TDSK_CONFIG_DIR=/etc/termidesk-test`;
- `TDSK_LOG_USER_DIR=<путь_к_каталогу>` - переменная, указывающая путь к каталогу хранения журналов для непривилегированного пользователя.

После установки клиентской части в ОС станет доступно графическое приложение «Termidesk Assistant» для подключения к серверной части Удаленного помощника. Для доступа к графическому приложению следует открыть меню рабочего стола ОС и найти приложение «Termidesk Assistant».

При использовании графического сервера Wayland в ОС подключение к серверной части Удаленного помощника не происходит. Следует

использовать другой графический сервер.

Обновление клиентской части в других ОС Linux

Обновление клиентской части Удаленного помощника производится установкой новой версии поверх предыдущей.

Удаление клиентской части в других ОС Linux

Для удаления клиентской части Удаленного помощника выполнить:

```
sudo apt purge termidesk-assistant-client
```

В зависимости от дистрибутива ОС Linux команда удаления может отличаться от приведенной. Например, при использовании пакетного менеджера yum следует использовать команду:

```
sudo yum remove termidesk-assistant-client
```

ОС Microsoft Windows

Установка, обновление, удаление клиентской части в ОС Microsoft Windows

Установка клиентской части в ОС Microsoft Windows

Клиентская часть для ОС Microsoft Windows распространяется в виде установочного `msi` -файла.

Получить установочный файл можно из образа диска `termidesk-vdi.XXXXX.iso`, где `XXXXX` - версия сборки, распаковав его как обычный архив в нужный каталог.

Установочный файл `termidesk-assistant-client_XXXXX_x64.msi` будет располагаться по пути «repos - windows - windows_x86_64».

Для установки на пользовательскую рабочую станцию нужно:

- запустить установочный файл, в окне приветствия мастера установки нажать экранную кнопку **[Далее]**;
- ознакомиться с лицензионным соглашением. Для принятия условий лицензионного соглашения и продолжения установки следует отметить поле «Я принимаю условия лицензионного соглашения» и нажать экранную кнопку **[Далее]** (см. рисунок Лицензионное соглашение «Termidesk Assistant»);

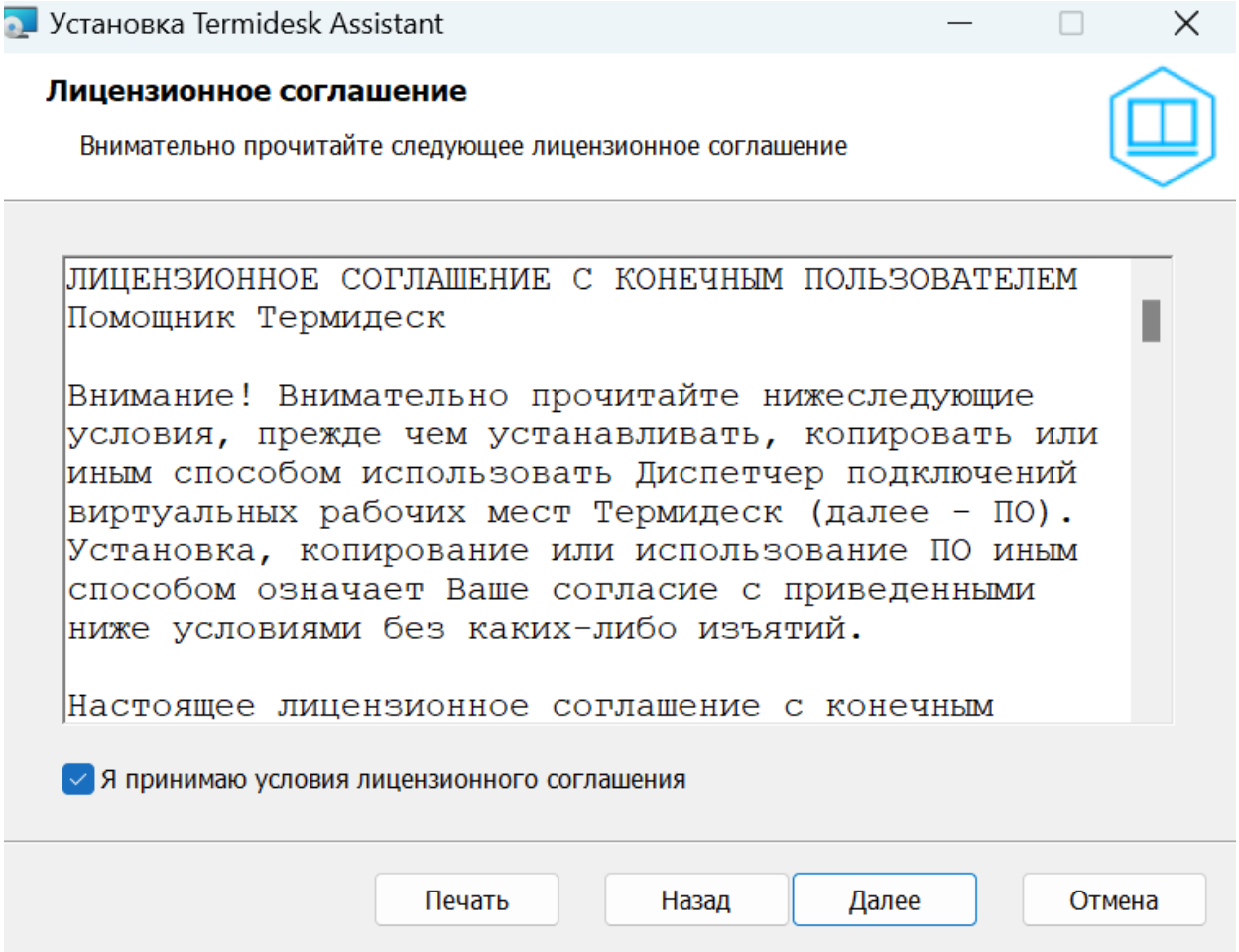


Рисунок 222. Лицензионное соглашение «Termidesk Assistant»

- для установки приложения «Termidesk Assistant» в каталог по умолчанию следует нажать экранную кнопку **[Далее]**. Для смены каталога установки приложения нажать экранную кнопку **[Изменить]** (см. рисунок Выбор каталога для установки приложения «Termidesk Assistant»);

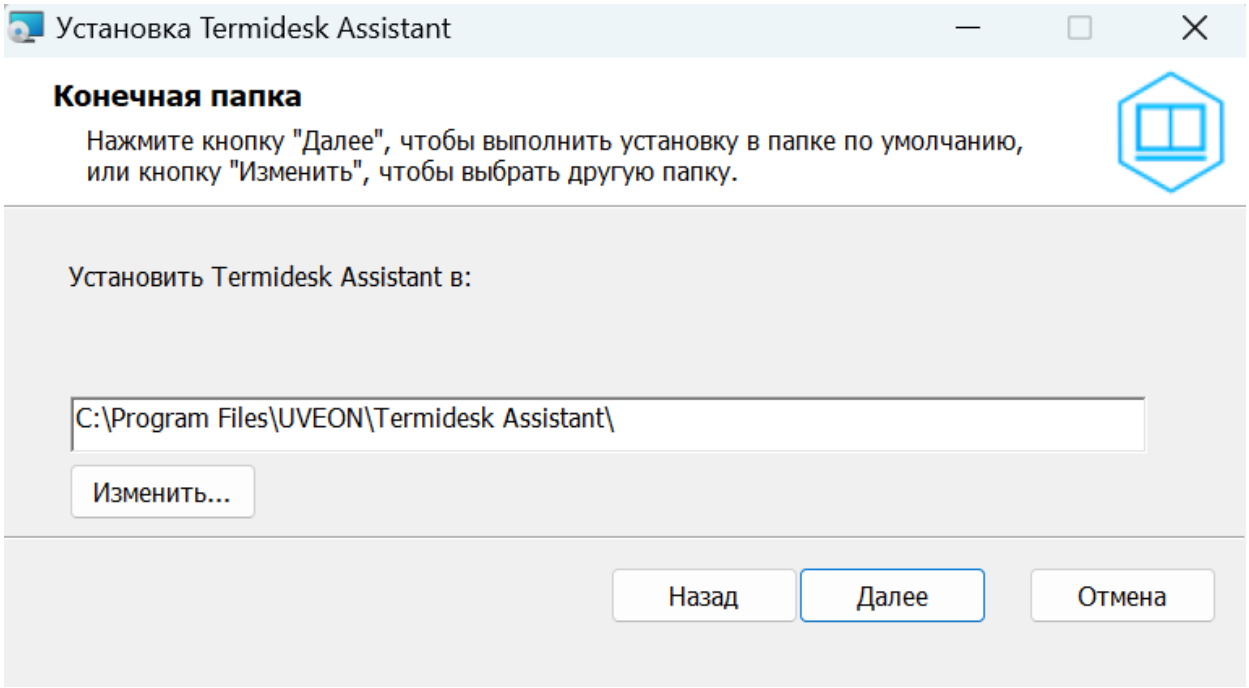


Рисунок 223. Выбор каталога для установки приложения «Termidesk Assistant»

- нажать экранную кнопку **[Установить]** для запуска процесса на установки (см. рисунок Запуск процесса установки приложения «Termidesk Assistant»). Для успешной установки необходимо разрешить внесение изменений при появлении соответствующего окна уведомления;

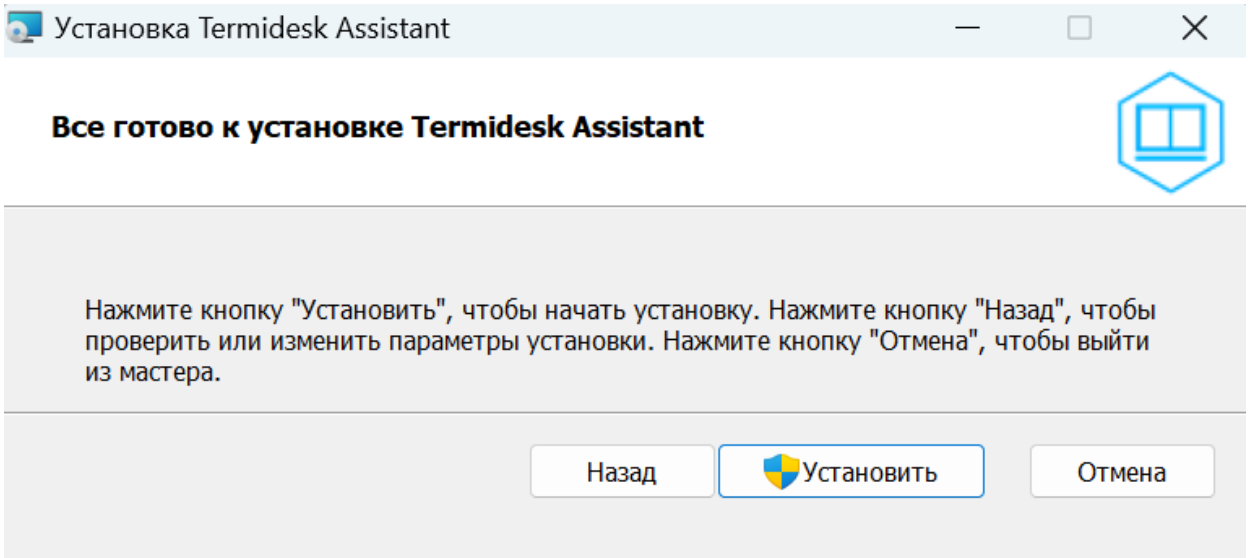


Рисунок 224. Запуск процесса установки приложения «Termidesk Assistant»

- дождаться завершения выполнения операции, нажать экранную кнопку **[Готово]** для выхода мастера установки (см. рисунок Выход из мастера установки приложения «Termidesk Assistant»).

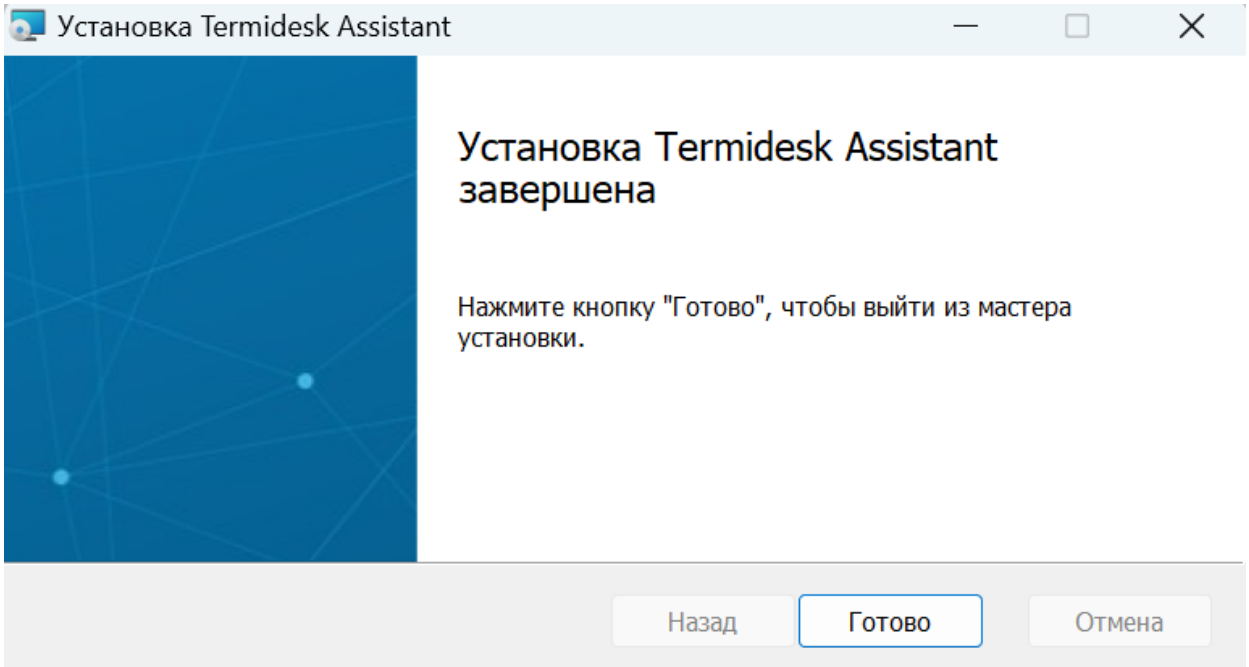


Рисунок 225. Выход из мастера установки приложения «Termidesk Assistant»

После установки клиентской части в ОС станет доступно графическое приложение «Termidesk Assistant» для подключения к серверной части Удаленного помощника.

Обновление клиентской части в ОС Microsoft Windows

Обновление клиентской части Удаленного помощника производится установкой новой версии поверх предыдущей.

Восстановление работоспособности клиентской части в ОС Microsoft Windows

В установочном файле `termidesk-assistant-client_XXXXX_x64.msi` предусмотрена возможность исправления ошибок, возникших при установке или использовании клиентской части Удаленного помощника. Исправление ошибок выполняется путем восстановления отсутствующих и поврежденных файлов, ярлыков и записей реестра.

Для восстановления работоспособности клиентской части Удаленного помощника нужно:

- запустить установочный файл, в окне приветствия мастера установки нажать экранную кнопку **[Далее]**;
- нажать экранную кнопку **[Восстановить]**. Далее необходимо подтвердить восстановление и дождаться завершения операции. Для успешного восстановления необходимо разрешить внесение изменений при появлении соответствующего окна уведомления.

Удаление клиентской части в ОС Microsoft Windows

Удаление клиентской части Удаленного помощника выполняется одним из способов:

- для удаления с использованием стандартных средств ОС Microsoft Windows:
  - открыть меню «Пуск», перейти в «Панель управления - Программы - Удаление программы», выбрать «Termidesk Assistant» и нажать на экранную кнопку **[Удалить]**. Далее необходимо подтвердить удаление и дождаться завершения операции;
- для удаления с использованием установочного файла `termidesk-assistant-client_XXXXX_x64.msi`:
  - запустить установочный файл, нажать экранную кнопку **[Удалить]** и дождаться завершения операции. Для успешного удаления необходимо разрешить внесение изменений при появлении соответствующего окна уведомления.

УДАЛЕННЫЙ ПОМОЩНИК. НАСТРОЙКИ

Конфигурационные файлы «Удаленного помощника»

Конфигурационные файлы серверной части

Конфигурационный файл серверной части

Параметры конфигурирования серверной части Удаленного помощника могут быть заданы:

- в конфигурационном файле `/etc/opt/termidesk-assistant/assistant.conf`. После установки конфигурационный файл не существует, поэтому его нужно предварительно создать. Если файл не существует, параметры в нем закомментированы или какие-то из параметров не указаны, то будут использоваться значения по умолчанию, указанные в таблице (см. таблицу Параметры конфигурационного файла серверной части Удаленного помощника). Для переопределения значений по умолчанию нужно раскомментировать нужный параметр;
- через переменную окружения, заданную в файле `/etc/default/termidesk-assistant-server`. Переменная окружения имеет более высокий приоритет, чем параметры, заданные через конфигурационный файл.

Пример файла `/etc/opt/termidesk-assistant/assistant.conf` с изначально закомментированными параметрами:

```
# STUN_SERVER_URL1="stun:stun.services.mozilla.com"
```

```
# STUN_SERVER_URL2="stun:stun.l.google.com:19302"
# STUN_SERVER_URL3=""
# WEBRTC_MOUSE_CURSOR=Yes
# BROWSER_MOUSE_CURSOR=Yes
# MEMCACHE_HOST1="127.0.0.1:11211"
# REDIS_HOST1=""
# AUDIT_SYSLOG_HOST1="127.0.0.1:514"
# AUDIT_SYSLOG_PROTO="UDP"
# AUDIT_SYSLOG_FACILITY="syslog"
# AUDIT_MAX_MESSAGE_LENGTH=1024
# AUDIT_QUEUE_SIZE=1000
# AUDIT_TLS_CERT_PATH=
# AUDIT_TLS_KEY_PATH=
# AUDIT_TLS_CA_PATH=
# AUTH_IP_LIST=["0.0.0.0/0"]
# AUTH_TOKEN_LIST=['Значение1', 'Значение2']
# AUDIO_ENABLE=Yes
# CAMERA_ENABLE=Yes
# MEDIA_ROOT = "/opt/termidesk/share/assistant/var/media"
# LOG_DIR=/var/log/termidesk/assistant
```

Описание параметров конфигурационного файла серверной части приведено в таблице (см. таблицу Параметры конфигурационного файла серверной части Удаленного помощника).

Таблица 410. Параметры конфигурационного файла серверной части Удаленного помощника

Параметр	Значение по умолчанию	Описание
STUN_SERVER_URL1	stun:stun.services.mozilla.com	Менять параметр не рекомендуется. IP-адрес или FQDN сервера STUN. Используется для возможности установки сеанса связи через внешнюю сеть. Можно задать несколько адресов, но не более трех
STUN_SERVER_URL2	stun:stun.l.google.com:19302	Менять параметр не рекомендуется. IP-адрес или FQDN сервера STUN. Используется для возможности установки сеанса связи через внешнюю сеть. Можно задать несколько адресов, но не более трех

Параметр	Значение по умолчанию	Описание
WEBRTC_MOUSE_CURSOR	Yes	Управление поведением курсора мыши при подключении к экрану пользователя. Возможные значения: • Yes - включить отображение курсора как экрана пользовательской ОС, так и локальной ОС; • No - выключить отображение локального курсора в области отображения экрана пользовательской ОС
BROWSER_MOUSE_CURSOR	Yes	Менять параметр не рекомендуется. Управление поведением курсора мыши из гостевой ОС в браузер. Возможные значения: • Yes - включить отображение курсора в браузере; • No - выключить отображение курсора в браузере
MEMCACHE_HOST1	127.0.0.1:11211	Менять параметр не рекомендуется. IP-адрес или FQDN сервера memcache и порт. Можно задать только один сервер
REDIS_HOST1	Не задано	IP-адрес или FQDN сервера Redis и порт. Можно задать только один сервер. Если IP-адрес и порт не заданы, сервер Redis не используется. Примеры: • REDIS_HOST1="127.0.0.1:6379" - сервер redis задан и используется; • REDIS_HOST1="" - сервер redis не используется
AUDIT_ENABLE	No	Управление отправкой сообщений на сервер syslog. Возможные значения: • Yes - отправка сообщений включена; • No - отправка сообщений отключена
AUDIT_SYSLOG_HOST1	127.0.0.1:514	IP-адрес или FQDN сервера syslog и порт. Если параметр не задан, сообщения не будут отправлены. Можно задать только один сервер

Параметр	Значение по умолчанию	Описание
AUDIT_SYSLOG_PROTO	UDP	Протокол подключения к серверу syslog. Возможные значения: • TLS. Для использования защищенного соединения по протоколу TLS нужно также задать параметры AUDIT_TLS_CERT_PATH, AUDIT_TLS_KEY_PATH и AUDIT_TLS_CA_PATH. Если указанные параметры не заданы, то подключение работать будет, но без защитного преобразования; • TCP; • UDP
AUDIT_SYSLOG_FACILITY	syslog	Категория сообщений syslog. Возможные значения: • auth; • authpriv; • cron; • daemon; • ftp; • kern; • lpr; • mail; • news; • syslog; • user; • uucp; • local0; • local1; • local2; • local3; • local4; • local5; • local6; • local
AUDIT_MAX_MESSAGE_LENGTH	1024	Максимальная длина сообщений аудита
AUDIT_QUEUE_SIZE	1000	Длина очереди сообщений

Параметр	Значение по умолчанию	Описание
AUDIT_TLS_CERT_PATH	Не задано	Путь к файлу сертификата для соединения TLS. Параметр должен быть задан, если в параметре AUDIT_SYSLOG_PROTO задано значение TLS. Файл сертификата должен быть скопирован в каталог /opt/termidesk/share/assistant/django_termidesk_assistant/. Параметр не имеет значения по умолчанию. Пример: AUDIT_TLS_CERT_PATH='/opt/termidesk/share/assistant/django_termidesk_assistant/ssl-cert-snakeoil.pem' или AUDIT_TLS_CERT_PATH="/opt/termidesk/share/assistant/django_termidesk_assistant/ssl-cert-snakeoil.pem"
AUDIT_TLS_KEY_PATH	Не задано	Путь к файлу ключа для соединения TLS. Параметр должен быть задан, если используется параметр AUDIT_TLS_CERT_PATH. Ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению: openssl rsa -in <путь_к_файлу_ключа>.key -out <путь_сохранения_преобразованного_ключа>.key Файл ключа должен быть скопирован в каталог /opt/termidesk/share/assistant/django_termidesk_assistant/. Параметр не имеет значения по умолчанию. Пример: AUDIT_TLS_KEY_PATH='/opt/termidesk/share/assistant/django_termidesk_assistant/ssl-cert-snakeoil.key' или AUDIT_TLS_KEY_PATH="/opt/termidesk/share/assistant/django_termidesk_assistant/ssl-cert-snakeoil.key"

Параметр	Значение по умолчанию	Описание
AUDIT_TLS_CA_PATH	Не задано	Путь к корневому сертификату, на котором выпущен сертификат, указанный в параметре AUDIT_TLS_CERT_PATH. Файл корневого сертификата должен быть скопирован в каталог /opt/termidesk/share/assistant/django_termidesk_assistant/. Используется для проверки подлинности указанного в параметре AUDIT_TLS_CERT_PATH сертификата. Параметр не имеет значения по умолчанию. Пример: AUDIT_TLS_CA_PATH='/opt/termidesk/share/assistant/django_termidesk_assistant/ssl-cert-ca.crt' или `AUDIT_TLS_CA_PATH="/opt/termidesk/share/assistant/django_termidesk_assistant/ssl-cert-ca.crt"
AUTH_IP_LIST	0.0.0.0/0	Список сетей, из которых доступно создание сессии с серверной частью Удаленного помощника. По умолчанию инициировать создание сессии можно из любых сетей. Если подключение инициируется через «Портал администратора» Termidesk VDI, то в списке должны быть заданы: • IP-адрес «Портала администратора» Termidesk VDI; • IP-адрес РМ, к которому производится подключение. Если подключение инициируется вручную, не через «Портал администратора» Termidesk VDI, то ограничение списка сетей, заданное в этом параметре, игнорируется. Поддерживается задание списка сетей в следующих форматах: • IP-адрес; • IP-адрес в формате CIDR. Пример: AUTH_IP_LIST=[192.0.2.10, 198.51.100.0/24]

Параметр	Значение по умолчанию	Описание

AUTH_TOKEN_LIST	Не задано	Значение мастер-ключа «Портала администратора» Termidesk VDI. Используется для авторизации запросов на создание сессии при подключении через «Портала администратора» Termidesk VDI.
		
		Этот тип авторизации имеет более высокий приоритет, чем авторизация по IP-адресам (параметр AUTH_IP_LIST).
		
		После задания параметра потребуется перезагрузка службы termidesk-assistant-server.
		
		Значение можно получить, перейдя в «Портале администратора» по пути «Системные параметры - Системные настройки - Безопасность» и скопировав значение параметра «Мастер-ключ».
		
		Особенности функционирования:
		
		• если параметр используется (не закомментирован), то:
		  - при подключении через «Портала администратора» Termidesk VDI в запросе к серверной части Удаленного помощника будет передан токен (заголовок X-TDSK-TOKEN), содержащий преобразованное значение мастер-ключа;
		  - серверная часть Удаленного помощника выполнит обратное преобразование значения для получения мастер-ключа и затем сравнит его с тем, что задано в этом параметре;
		  - если полученное значение окажется отличным от того, что задано в параметре, то сессия не создастся и пользователю будет отображена ошибка 401;
		• если параметр не используется (закомментирован), то проверка значений серверной частью Удаленного помощника не производится. При подключении через «Портала администратора» Termidesk VDI серверная часть Удаленного помощника создаст сессию без авторизации по токенам.
		
		Длина строки получаемого токена (преобразованного значения мастер-ключа) ограничена 1024 байтами.
		
		Пример:
		
		AUTH_TOKEN_LIST=['123456789', 'masterkey']

Параметр	Значение по умолчанию	Описание
AUDIO_ENABLE	Yes	Управление передачей звука при подключении к пользователю. Если подключение выполняется через «Портал администратора» Termidesk VDI, то настройки с сервера Termidesk VDI, заданные через политики фонда рабочих мест, приоритетнее, чем настройка, заданная в этом параметре. Если подключения выполняется через REST API, то настройки, переданные в запросе, приоритетнее, чем настройка, заданная в этом параметре. Возможные значения: • Yes - передача звука включена; • No - передача звука отключена
CAMERA_ENABLE	Yes	Управление передачей веб-камеры при подключении к пользователю. Если подключение выполняется через «Портал администратора» Termidesk VDI, то настройки с сервера Termidesk VDI, заданные через политики фонда рабочих мест, приоритетнее, чем настройка, заданная в этом параметре. Если подключения выполняется через REST API, то настройки, переданные в запросе, приоритетнее, чем настройка, заданная в этом параметре. Возможные значения: • Yes - передача веб-камеры включена; • No - передача веб-камеры отключена
MEDIA_ROOT	/opt/termidesk/share/assistant/var/media	Каталог для хранения файлов

LOG_DIR	/var/log/termidesk/assistant	Каталог хранения журналов серверной части Удаленного помощника.
		
		Для записи журналов в новый каталог он должен быть предварительно создан:
		
		`sudo mkdir <путь_к_каталогу>`
		`sudo chown termidesk-assistant:termidesk-assistant <путь_к_каталогу>`

Файл /etc/default/termidesk-assistant-server

Одним из параметров службы termidesk-assistant-server является аргумент EnvironmentFile, задающий путь к дополнительным аргументам запуска, перечисленным в файле /etc/default/termidesk-assistant-server.

Файл /etc/default/termidesk-assistant-server:

- является необязательным и может отсутствовать в ОС;
- если он существует, то происходит его построчное чтение в формате `<ключ>=<значение>` и в запускаемый процесс добавляются переменные окружения, которые указаны в этом файле (см. подраздел **Переменные окружения**).

Конфигурационные файлы клиентской части

Конфигурационный файл клиентской части

Параметры конфигурирования клиентской части Удаленного помощника могут быть заданы:

- для ОС Linux:
  - в конфигурационном файле `/etc/termidesk/assistant/client.conf`;
  - через переменную окружения, заданную в файле `/etc/default/termidesk-assistant-client`;
- для ОС Microsoft Windows:
  - в конфигурационном файле `C:\ProgramData\UVEON\Termidesk Assistant.ini`. При отсутствии данного файла используется файл `C:\Users\<Пользователь>\AppData\Roaming\UVEON\Termidesk Assistant.ini`;
  - через переменную окружения (см. подраздел **Переменные окружения**).

Переменная окружения имеет более высокий приоритет, чем параметры, заданные через конфигурационный файл. После установки конфигурационный файл не существует, поэтому его нужно предварительно создать. Если файл не существует, параметры в нем закомментированы или какие-то из параметров не указаны, то будут использоваться значения по умолчанию, указанные в таблице (см. таблицу Параметры конфигурационного файла клиентской части Удаленного помощника).

Пример содержимого конфигурационного файла клиентской части:

```
LOG_DIR=~/.config/UVEON/logs
```

Описание параметров конфигурационного файла клиентской части приведено в таблице (см. таблицу Параметры конфигурационного файла клиентской части Удаленного помощника).

Таблица 411. Параметры конфигурационного файла клиентской части Удаленного помощника

Параметр	Значение по умолчанию	Описание

`LOG_DIR`	Для ОС Linux: `~/.config/UVEON/logs`
	
	Для ОС Microsoft Windows: `C:/Users/<Пользователь>/AppData/Roaming/UVEON/logs`
		Каталог хранения журналов клиентской части Удаленного помощника.
		
		Для записи журналов в новый каталог он должен быть предварительно создан:
		
		`sudo mkdir <путь_к_каталогу>`
		`sudo chown $USER:$USER <путь_к_каталогу>`

Файл `/etc/default/termidesk-assistant-client`

Одним из параметров службы `termidesk-assistant-client` является аргумент `EnvironmentFile`, задающий путь к дополнительным аргументам запуска, перечисленным в файле `/etc/default/termidesk-assistant-client`.

Файл `/etc/default/termidesk-assistant-client`:

- является необязательным и может отсутствовать в ОС;
- если он существует, то происходит его построчное чтение в формате `<ключ>=<значение>` и в запускаемый процесс добавляются переменные окружения, которые указаны в этом файле (см. подраздел **Переменные окружения**).

Переменные окружения «Удаленного помощника»

Переменные окружения клиентской части

Перечень переменных окружения, используемых клиентской частью Удаленного помощника, приведена в таблице (см. таблицу Перечень переменных окружения клиентской части Удаленного помощника).

Переменные окружения имеют более высокий приоритет над конфигурацией Удаленного помощника, чем конфигурационный файл.

Для задания переменных окружения:

- в ОС Linux должен использоваться файл `/etc/default/termidesk-assistant-client` (см. подраздел **Конфигурационные файлы**);
- в ОС Microsoft Windows нужно:
  - нажать клавиши **<Win+R>**, в окне «Выполнить» ввести `sysdm.cpl` и нажать экранную кнопку **[OK]**;
  - в окне «Свойства системы» во вкладке «Дополнительно» нажать экранную кнопку **[Переменные среды]**;
  - в окне «Переменные среды» нажать экранную кнопку **[Создать]**, задать имя и значение переменной, затем нажать экранную кнопку **[OK]**.

Таблица 412. Перечень переменных окружения клиентской части Удаленного помощника

Переменная окружения	Значение по умолчанию	Описание

TDSK_CONFIG_DIR	Для ОС Linux: /etc/termidesk/assistant.
	
	Для ОС Microsoft Windows: C:\ProgramData\Uveon
		Задает место хранения файлов конфигурации клиентской части Удаленного помощника.
		
		Пример: администратор хочет изменить место хранения файла конфигурирования.
		
		Для этого ему нужно:
		
		• создать файл client.cfg с настройками или скопировать существующий из /etc/termidesk/assistant;
		• поместить client.cfg в нужный каталог. Каталог должен обладать свойствами:
		  - права доступа: rwxr-xr-x (в восьмеричной записи - 755);
		  - владелец и группа: root:root;
		• создать файл /etc/default/termidesk-assistant-client. Указать в нем каталог, откуда будет считан конфигурационный файл. Пример:
		
		`TDSK_CONFIG_DIR=/etc/termidesk`
		
		• перезапустить приложение клиентской части Удаленного помощника

TDSK_LOG_USER_DIR	Для ОС Linux: ~/.config/UVEON/logs.
	
	Для ОС Microsoft Windows: C:\Users\<Пользователь>\AppData\Roaming\UVEON\logs
		Каталог хранения журналов клиентской части Удаленного помощника (для непривилегированного пользователя).
		
		Для записи журналов в новый каталог он должен быть предварительно создан:
		
		`sudo mkdir <путь_к_каталогу>`
		`sudo chmod 700 <путь_к_каталогу>`

TDSK_SETUP_NONINTERACTIVE	Не задано	«Тихий» режим установки. Возможные значения: • 1 - активировать режим. Используется при необходимости установки без отображения дополнительных окон

Переменные окружения серверной части

Перечень переменных окружения, используемых серверной частью Удаленного помощника, приведена в на таблице (см. таблицу Перечень переменных окружения серверной части Удаленного помощника).

Переменные окружения имеют более высокий приоритет над конфигурацией Удаленного помощника, чем конфигурационный файл.

Для задания переменных окружения в ОС Linux должен использоваться файл `/etc/default/termidesk-assistant-server`.

Таблица 413. Перечень переменных окружения серверной части Удаленного помощника

Переменная окружения	Значение по умолчанию	Описание

`TDSK_LOG_SRV_DIR`	`/var/log/termidesk/assistant`	Каталог хранения журналов серверной части Удаленного помощника.
		
		Для записи журналов в новый каталог он должен быть предварительно создан:
		
		`sudo mkdir <путь_к_каталогу>`
		`sudo chown termidesk-assistant:termidesk-assistant <путь_к_каталогу>`

`TDSK_CONFIG_DIR`	`/etc/opt/termidesk-assistant`	Задает место хранения файлов конфигурации серверной части Удаленного помощника.
		
		Пример: администратор хочет изменить место хранения файла конфигурирования.
		
		Для этого ему нужно:
		
		• создать файл `server.cfg` с настройками или скопировать существующий из `/etc/opt/termidesk-assistant/`;
		• поместить `server.cfg` в нужный каталог. Каталог должен обладать свойствами:
		  - права доступа: `rwxr-xr-x` (в восьмеричной записи - `755`);
		  - владелец и группа: `root:root`;
		• создать файл `/etc/default/termidesk-assistant-server`. Указать в нем каталог, откуда будет считан конфигурационный файл. Пример:
		
		`TDSK_CONFIG_DIR=/etc/opt/termidesk`
		
		• перезапустить серверную часть Удаленного помощника:
		
		`sudo systemctl restart termidesk-assistant-server`

`TDSK_SETUP_NONINTERACTIVE`	`Не задано`	«Тихий» режим установки. Возможные значения: • `1` - активировать режим. Используется при необходимости установки без отображения дополнительных окон

Количество одновременных подключений к серверу «Удаленного помощника»

В веб-сервере apache есть ограничение на количество одновременных подключений, задаваемых в параметре `MaxRequestWorkers` конфигурационного файла `/etc/apache2/mods-available/mpm_event.conf`. По умолчанию поддерживается 150 одновременных подключений.

Чтобы увеличить количество одновременных подключений, нужно:

- изменить значение параметра `MaxRequestWorkers` конфигурационного файла `/etc/apache2/mods-available/mpm_event.conf` на нужное, например, `200`:

```
# event MPM
# StartServers: initial number of server processes to start
# MinSpareThreads: minimum number of worker threads which are kept spare
# MaxSpareThreads: maximum number of worker threads which are kept spare
# ThreadsPerChild: constant number of worker threads in each server process
# MaxRequestWorkers: maximum number of worker threads
# MaxConnectionsPerChild: maximum number of requests a server process serves
<IfModule mpm_event_module>
        StartServers                     2
        MinSpareThreads          25
        MaxSpareThreads          75
        ThreadLimit                      64
        ThreadsPerChild          25
        MaxRequestWorkers         200
        MaxConnectionsPerChild   0
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

- перезапустить веб-сервер apache:

```
sudo systemctl restart apache2
```

Управление поведением курсора

Поведением курсора при подключении к экрану пользователя можно управлять:

- включить отображение курсора как экрана пользовательской ОС, так и локальной ОС;
- выключить отображение курсора локальной ОС в области экрана пользовательской ОС.

Поведение курсора настраивается через параметр `WEBRTC_MOUSE_CURSOR` (см. подраздел **Конфигурационные файлы серверной части**).

Замена SSL-сертификата веб-сервера для «Удаленного помощника»

Для доступа к веб-интерфейсу по протоколу HTTPS на этапе установки веб-сервера автоматически генерируется самоподписанный сертификат и закрытый ключ к нему. В некоторых случаях может понадобиться заменить эти сертификаты на другие.

Для замены SSL-сертификатов необходимо:

- получить новый сертификат и ключ к нему;
- поместить новый сертификат формата `.pem` в каталог `/etc/ssl/certs/`:

```
sudo cp <путь_к_сертификату> /etc/ssl/certs/
```

- поместить новый ключ формата `.key` в каталог `/etc/ssl/private/`:

```
sudo cp <путь_к_ключу> /etc/ssl/private/
```

Если сертификат и ключ находятся в PKCS12-контейнере (файл формата `.pfx`), необходимо сначала сконвертировать их в нужный формат:

```
openssl pkcs12 -in <путь_к_pfx-контейнеру> -out <путь_к_создаваемому_файлу.pem>
-nodes
openssl pkcs12 -in <путь_к_pfx-контейнеру> -nocerts -nodes  -out
<путь_к_создаваемому_файлу.key>
openssl rsa -in <путь_к_созданному_файлу_ключа.key> -out
<путь_сохранения_преобразованного_ключа.key>
```

- отредактировать файл `/etc/apache2/sites-available/default-ssl.conf`, заменив путь к сертификату и ключу для параметров `SSLCertificateFile` и `SSLCertificateKeyFile` на новые:

```
SSLEngine on
SSLCertificateFile      /etc/ssl/certs/new_cert.pem
SSLCertificateKeyFile /etc/ssl/private/new_key.key
```

- перезапустить веб-сервер:

```
sudo systemctl restart apache2
```

Взаимодействие с серверной частью «Удаленного помощника» по REST API

Для активации возможности взаимодействия клиентской части с серверной частью Удаленного помощника по REST API предусмотрен технологический компонент `termidesk_assistant_api`, представляющий собой библиотеку для Python, устанавливаемую на узел с клиентской частью.

Для установки `termidesk-assistant-api` в ОС Astra Linux Special Edition нужно:

- открыть программу «Терминал Fly» и получить доступ к интерфейсу командной строки;
- установить пакет виртуальной среды для Python `python3-venv` командой:

```
sudo apt -y install python3-venv
```

- создать виртуальное окружение, например, `my_venv`, командой:

```
python -m venv my_venv
```

Для разных версий Python могут использоваться разные команды для установки виртуального окружения и его использования.

- активировать виртуальное окружение `my_venv` командой:

```
source my_venv/bin/activate
```

- установить библиотеку `termidesk_assistant_api-<версия>.tar.gz`:

```
pip install <путь_к_termidesk_assistant_api-<версия>.tar.gz>
```

Для установки `termidesk-assistant-api` в ОС Microsoft Windows нужно:

- установить Python для ОС Microsoft Windows, предварительно загрузив установщик (доступ: https://www.python.org/downloads/windows/);
- запустить интерфейс командной строки от имени администратора;
- создать виртуальное окружение, например, `my_venv`, командой:

```
python -m venv my_venv
```

- активировать виртуальное окружение `my_venv` командой:

```
source my_venv/bin/activate
```

- установить библиотеку `termidesk_assistant_api-<версия>.tar.gz`:

```
pip install <путь_к_termidesk_assistant_api-<версия>.tar.gz>
```

Для начала работы с библиотекой `termidesk_assistant_api` нужно:

- переключиться на интерпретатор Python:

```
python
```

Для ОС Microsoft Windows команда переключения будет аналогичной.

- выполнить импорт установленной библиотеки:

```
>>> from termidesk_assistant_api import rest
```

Примеры запросов REST API в Python, которые могут быть использованы:

- получение версии серверной части Удаленного помощника:

```
example = rest.Client(url="\https://192.0.2.1/assistant")
print(example.version())
```

- установка места хранения файла журнала (обязательно для ОС Microsoft Windows):

```
example = rest.Client(url="\https://192.0.2.1/assistant")
example.init_logging("C:\\logs\\log.log")
```

- получение JSON-структуры с информацией о серверной части:

```
example = rest.Client(url="https://192.0.2.1/assistant")
print(example.discovery())
```

- получение версии Удаленного помощника и создание сессии:

```
example = rest.Client(url="https://192.0.2.1/assistant")
print(example.version())  # получение версии
print(example.session.create().session_id) # создание сессии и возврат ее ID
```

В приведенных примерах использованы следующие параметры:

- `192.0.2.1` - IP-адрес узла с установленной серверной частью Удаленного помощника;
- `C:\\logs\\log.log` - путь к файлу, который будет использоваться как журнал.

Отправка событий на сервер syslog для «Удаленного помощника»

События серверной части Удаленного помощника могут быть отправлены на сервер syslog (удаленный или локальный).

Отправка событий настраивается через параметры `AUDIT_ENABLE`, `AUDIT_SYSLOG_HOST`, `AUDIT_SYSLOG_PORT`, `AUDIT_SYSLOG_PROTO`, `AUDIT_SYSLOG_FACILITY` (см. подраздел **Конфигурационные файлы серверной части**).

УДАЛЕННЫЙ ПОМОЩНИК. ПОДКЛЮЧЕНИЕ И ОТКЛЮЧЕНИЕ

Подключение к удаленному рабочему столу

Подключиться к удаленному рабочему столу (экрану) пользовательской рабочей станции можно одним из способов:

- через компонент «Универсальный диспетчер»;
- через веб-браузер. Для этого в адресной строке нужно ввести URL-адрес: https://IP-address/assistant, где IP-address - IP-адрес узла с установленной серверной частью Удаленного помощника. Пример подключения приведен на рисунке (см. рисунок Пример ввода параметров подключения в браузере).

Перед подключением через веб-браузер рекомендуется убедиться в разрешении правил брандмауэра и добавить их при необходимости:

```
sudo firewall-cmd --zone=public --add-service=http --permanent
sudo firewall-cmd --zone=public --add-service=https --permanent
```

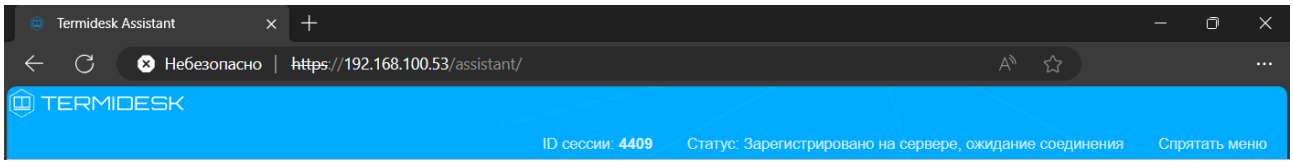


Рисунок 226. Пример ввода параметров подключения в браузере

Администратор или специалист технической поддержки, оказывающий консультацию, должен передать значение параметра «ID сессии», а также URL-адрес для подключения пользователю.

Администратор может передать URL для подключения, содержащий идентификатор сессии, например: https://192.0.2.1/assistant/1010. Пользователь может открыть подключение как из графического приложения «Termidesk Assistant», так и через интерфейс командной строки, указав полученный URL (см. подраздел **Удаленный помощник. Интерфейс командной строки**).

В этом случае подключение будет установлено после его на подтверждения (см. рисунок Подтверждение демонстрации экрана) в диалоговом окне со стороны пользователя.

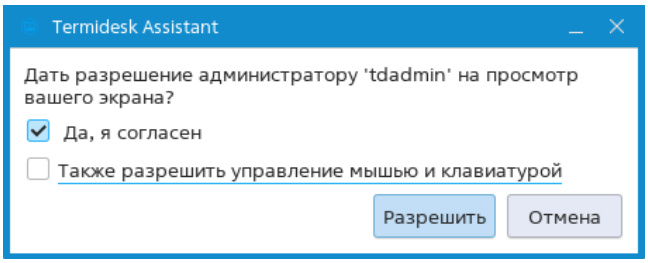


Рисунок 227. Подтверждение демонстрации экрана

При подключении администратора через веб-интерфейс «Универсального диспетчера»:

- возможность управления параметром «Также разрешить управление мышью и клавиатурой» зависит от значения политики «Режим подключения администратора в Удалённом Помощнике»;
- если фонду РМ назначена политика «Согласие пользователя для подключения администратора в Удалённом Помощнике» - «Не требуется»:
  - администратор подключается без подтверждения пользователя;
  - администратору доступно управление клавиатурой и указателем мыши независимо от значения политики «Режим подключения администратора в Удалённом Помощнике»;

- запрос на подключение пользователю не отображается;
- информация о подключении администратора отображается в трее.

При этом, если в пользовательской рабочей станции уже есть запущенный экземпляр графического приложения «Termidesk Assistant», то перед появлением диалога подтверждения в системном трее появится всплывающее сообщение (см. рисунок Уведомление о подключении). Пользователю нужно нажать левой кнопкой мыши на уведомление для отображения диалога подтверждения, если этого не сделать или нажать на иконку «Крестик» - диалог подтверждения подключения показан не будет.

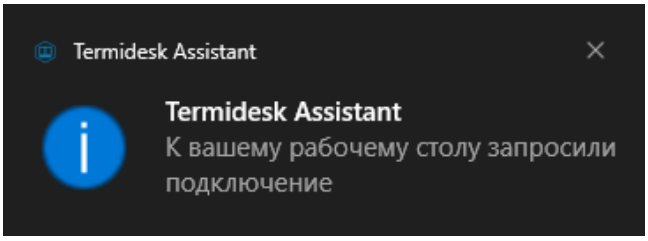


Рисунок 228. Уведомление о подключении

При подключении без использования командной строки пользователь на своей рабочей станции должен открыть графическое приложение «Termidesk Assistant», перейдя в меню «Звезда», пункт «Утилиты».

При попытке одновременного запуска нескольких экземпляров приложения «Termidesk Assistant» будет отображено уже активное приложение.

В приложении «Termidesk Assistant» пользователю нужно (см. рисунок Пример ввода параметров в клиентском приложении Удаленного помощника):

- заполнить поля:
  - «URL сервера» - IP-адрес узла с установленной серверной частью Удаленного помощника;
  - «Идентификатор сессии» - идентификатор сессии, полученный из веб-интерфейса серверной части Удаленного помощника;
- затем нажать экранную кнопку **[Подключиться]**.

Если администратор подключается к сессии через компонент «Универсальный диспетчер», то поля будут заполнены автоматически.

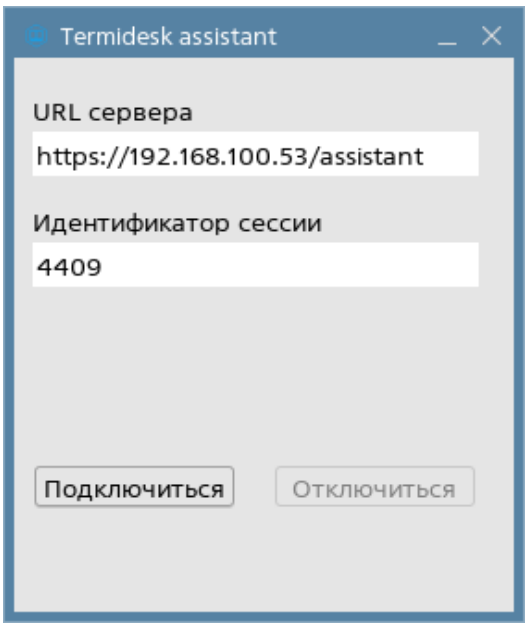


Рисунок 229. Пример ввода параметров в клиентском приложении Удаленного помощника

После нажатия на экранную кнопку **[Подключиться]** производится подключение к серверной части Удаленного помощника. Администратор или специалист технической поддержки должен в браузере нажать экранную кнопку **[Разрешить]** (см. рисунок Уведомление о необходимости предоставления доступа к веб-камере и микрофону) на уведомлении о необходимости доступа к микрофону и веб-камере.

Уведомление не будет отражено, если администратор подключается через веб-интерфейс «Универсального диспетчера» и политиками фонда запрещено использование аудиосвязи и веб-камеры.

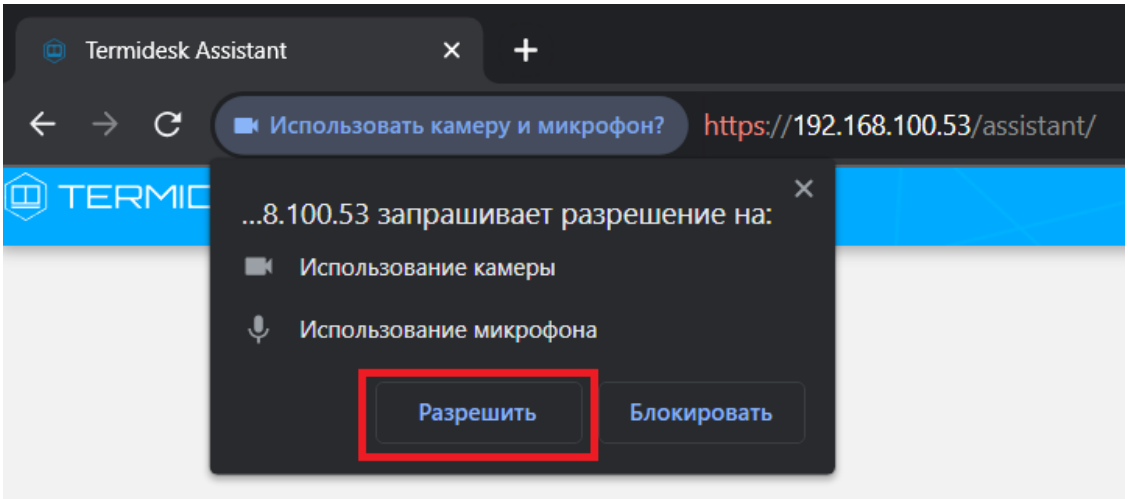


Рисунок 230. Уведомление о необходимости предоставления доступа к веб-камере и микрофону

Завершение демонстрации рабочего стола

Для завершения демонстрации рабочего стола (экрана) пользовательской рабочей станции пользователю следует нажать экранную кнопку **[Disconnect]** в приложении «Termidesk Assistant».

После этого в браузере администратора или специалиста технической поддержки появится оповещение о перезагрузке страницы (см. рисунок Оповещение администратора при завершении сессии).

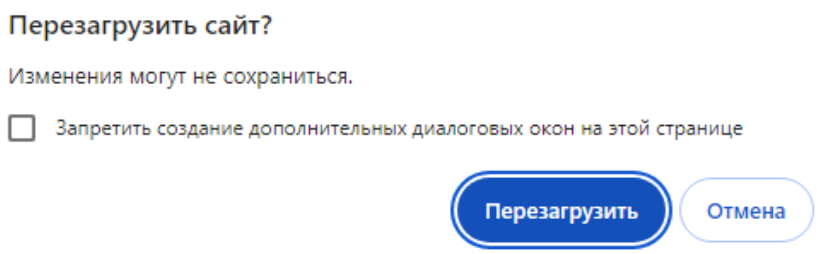


Рисунок 231. Оповещение администратора при завершении сессии

Возможности при подключении

Перенаправление устройств

Перенаправление устройств выполняется при подключении к серверной части Удаленного помощника через веб-браузер по протоколу HTTPS.

Меню выбора устройств отображается в левом верхнем углу веб-интерфейса после установления соединения клиентской части с серверной частью. Для перенаправления микрофона и камеры нужно выбрать соответствующие устройства в раскрывающемся списке и нажать экранную кнопку **[начать стрим]** (см. рисунок Выбор перенаправляемых устройств). В случае, если перенаправление устройств в браузере было запрещено, сразу будет открыто окно трансляции экрана, без отображения меню выбора устройств.

При подключении по протоколу HTTP нужно также нажать экранную кнопку **[начать стрим]**, меню выбора устройств при этом может быть не отображено.

Рисунок 232. Выбор перенаправляемых устройств

Удаленное управление

При подключении к удаленному рабочему столу администратору (специалисту технической поддержки) доступно управление ОС пользовательской рабочей станции с использованием следующих функций:

- управление мышью;
- выбор и отправка комбинаций клавиш. Для отправки комбинации клавиш необходимо выбрать нужную комбинацию и подтвердить ее отправку экранной кнопкой, указанной на рисунке (см. рисунок Удаленное управление пользовательской рабочей станцией).

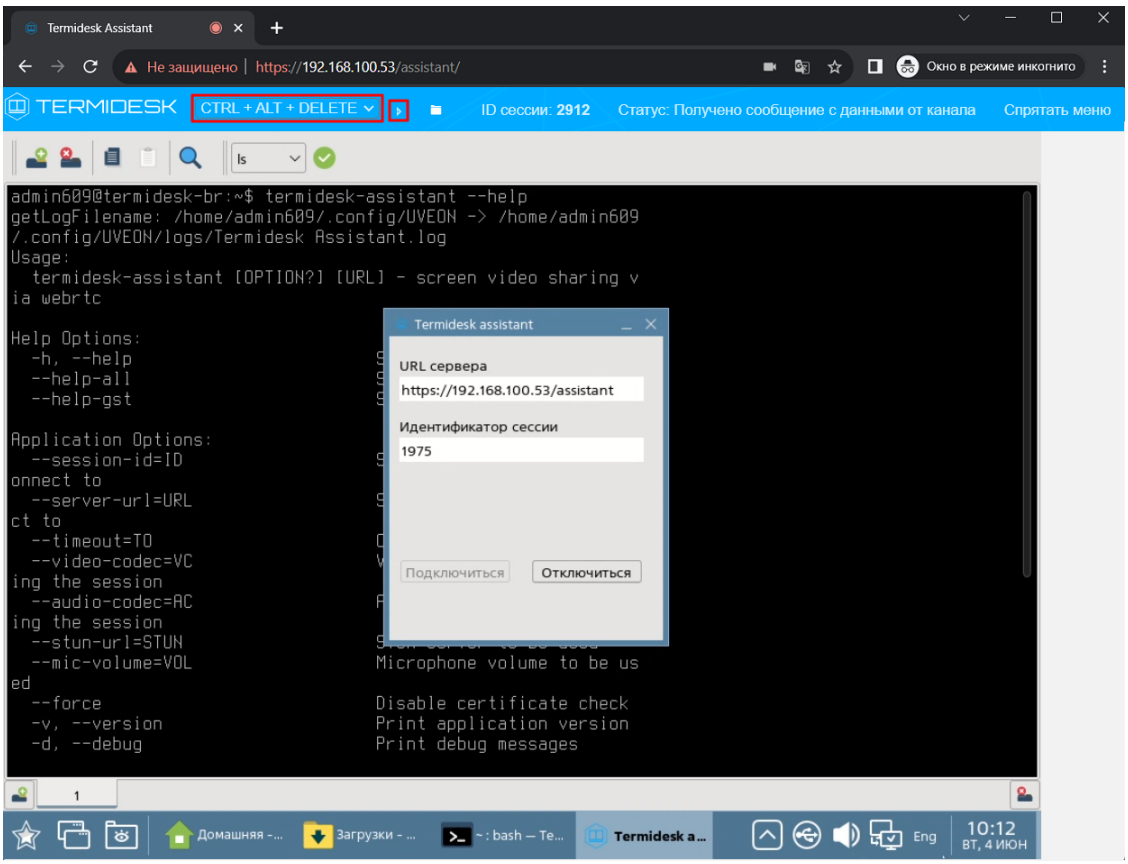


Рисунок 233. Удаленное управление пользовательской рабочей станцией

УДАЛЕННЫЙ ПОМОЩНИК. ГРАФИЧЕСКИЙ ИНТЕРФЕЙС

Работа с основными функциями веб-интерфейса серверной части

Графический интерфейс серверной части Удаленного помощника представлен веб-интерфейсом, доступным при переходе в браузер и вводе URL-адреса в формате: `https://IP-address/assistant`, где `IP-address` - IP-адрес узла с установленной серверной частью Удаленного помощника.

Сразу после подключения пользователя по указанному URL-адресу в правом верхнем углу вкладки отобразится следующая информация (см. рисунок Веб-интерфейс серверной части удаленного помощника):

- «Нет видеовхода» - выбор перенаправляемой камеры;
- «Нет аудиовхода» - выбор перенаправляемого микрофона;

> Для отображения списка устройств в пунктах «Нет видеовхода» и «Нет аудиовхода» необходимо, чтобы у браузера было разрешение на их перенаправление. Обычно разрешение запрашивается в виде всплывающего окна «Использовать камеру и микрофон?». Доступ к камере и микрофону также можно разрешить в настройках браузера.

- «Начать стрим» - начать трансляцию экрана пользователя;
- «Ярлыки клавиатуры» - выбор сочетаний клавиш для перенаправления в пользовательскую рабочую станцию;
- пиктограмма запуска - подтверждение выбора комбинации клавиш и их перенаправление;
- пиктограмма папки - открывает файловый менеджер для передачи файлов на

серверную часть Удаленного помощника;

- «ID сессии» - идентификатор подключения;
- «Статус» - статус подключения;
- «Спрятать меню» - сокрытие меню подключений. Используется для того, чтобы не перекрывать отображение рабочего стола.

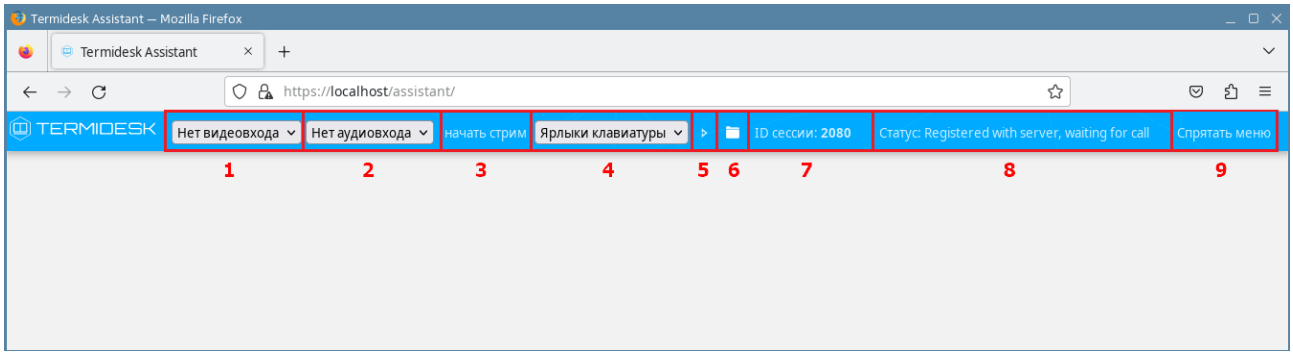


Рисунок 234. Веб-интерфейс серверной части удаленного помощника

Работа с основными функциями графического интерфейса клиентской части

Графический интерфейс клиентской части Удаленного помощника представлен интерфейсом приложения «Termidesk Assistant».

В приложении «Termidesk Assistant» доступны следующие поля и экранные кнопки (см. рисунок Графический интерфейс клиентской части удаленного помощника):

- «URL сервера» - URL для подключения к серверной части Удаленного помощника, должен быть передан администратором или специалистом технической поддержки;
- «Идентификатор сессии» - идентификатор сессии, должен быть передан администратором или специалистом технической поддержки;
- **[Подключиться]** - экранная кнопка для инициирования трансляции экрана;
- **[Отключиться]** - экранная кнопка для прекращения трансляции экрана. Становится доступна после начала трансляции.

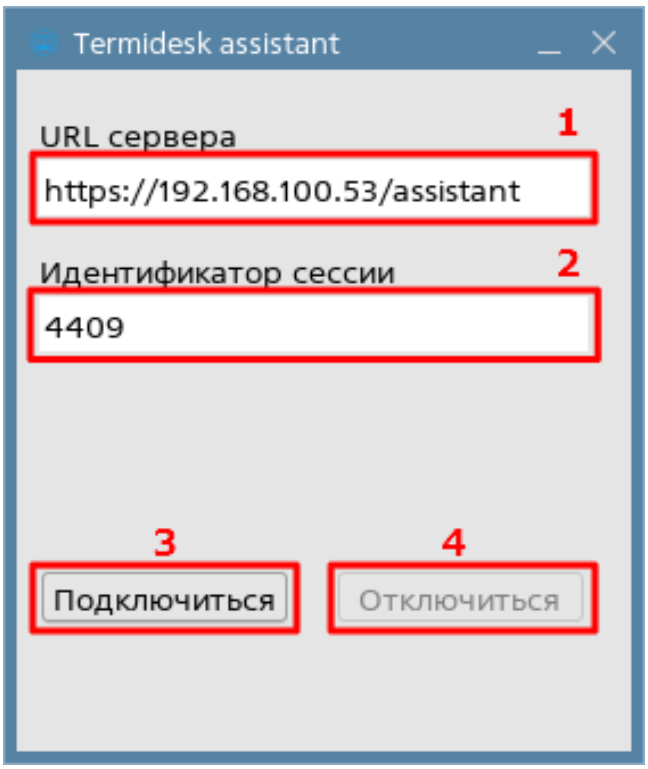


Рисунок 235. Графический интерфейс клиентской части удаленного помощника

После открытия приложения оно автоматически становится доступно из системного трея.

При нажатии правой кнопкой мыши на иконку в системном трее будет доступен выбор функций:

- «Показать» - отображение окна приложения, если оно ранее было скрыто, на рабочем столе и в меню «Пуск»/«Звезда»;
- «Скрыть» - сокрытие окна приложения с рабочего стола и из меню «Пуск»/«Звезда»;
- «Выход» - завершение работы приложения с подтверждением действия.

Окно приложения можно поместить поверх других окон, если нажать левой кнопкой мыши на иконку «Termidesk Assistant» в системном трее.

УДАЛЕННЫЙ ПОМОЩНИК. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

Интерфейс командной строки клиентской части

Параметры запуска клиента Удаленного помощника могут быть переопределены аргументами командной строки.

Для получения краткой информации по доступным аргументам командной строки следует вызвать приложение `termidesk-assistant` с аргументом `--help`:

```
termidesk-assistant --help
```

Для получения полной информации по доступным аргументам командной строки следует вызвать приложение `termidesk-assistant` с аргументом `--help-all`:

```
termidesk-assistant --help-all
```

Чтобы посмотреть доступные аргументы, относящиеся только к GStreamer (обработчик потоковой информации), следует вызвать приложение termidesk-assistant с аргументом --help-gst:

```
termidesk-assistant --help-gst
```

Список доступных аргументов приведен в таблице.

Таблица 414. Список аргументов командной строки для клиентской части Удаленного помощника

Параметр	Переменная окружения	Описание	Значение по умолчанию
Не задано	Не задано	URL с указанием идентификатора сессии для подключения к серверу с установленной серверной частью Удаленного помощника. Параметр может быть передан пользователю или другому приложению для подключения. Пример использования из интерфейса командной строки в ОС Linux: termidesk-assistant https://192.0.2.1/assistant/1010 Пример использования из интерфейса командной строки в ОС Microsoft Windows: "C:\Program Files\UVEON\Termidesk Assistant\bin\termidesk-assistant.exe" https://192.0.2.1/assistant/1010 где: 192.0.2.1 - IP-адрес узла с серверной частью Удаленного помощника; 1010 - идентификатор сессии. Вместо https могут использоваться также: http, trdas, tdra (зарезервированное расширение URL-схем для работы с компонентами Termidesk VDI)	Не задано
--session-id	TDSK_SESSION_ID	Идентификатор сессии	Не задано
--server-url	TDSK_VDI_URL	Адрес сервера с установленной серверной частью Удаленного помощника	Не задано
--timeout	TDSK_TIMEOUT	Время ожидания подключения к серверу	60
--video-codec	TDSK_VIDEO_CODEC	Используемый видеокодек	VP8
--audio-codec	TDSK_AUDIO_CODEC	Используемый аудиокодек	OPUS
--stun-url	TDSK_STUN_URL	Адрес сервера STUN. Используется для возможности установки сеанса связи с сервером Удаленного помощника через внешнюю сеть	stun://stun.l.google.com:19302
--mic-volume	Не задано	Громкость микрофона (в процентах)	100

Параметр	Переменная окружения	Описание	Значение по умолчанию
--force	Не задано	Параметр для отключения проверки сертификата. При вызове этого параметра проверка сертификата при подключении не производится	Не задано
--version	Не задано	Вывод версии приложения	Не задано
--debug	TDSK_DEBUG	Вывод подробной информации о параметрах Удаленного помощника, его работе и взаимодействии с сервером	Не задано

Интерфейс командной строки серверной части

Серверная часть Удаленного помощника не поддерживает интерфейс командной строки.

УДАЛЕННЫЙ ПОМОЩНИК. ЖУРНАЛИРОВАНИЕ

Журналы работы Удаленного помощника ведутся:

- для серверной части:
  - в файле /var/log/termidesk/assistant/signalling.log;
  - в файле /var/log/termidesk/assistant/browser.log;
- для клиентской части:
  - ОС Microsoft Windows: в файле C:\Users\<user>\AppData\Roaming\UVEON\logs\Termidesk Assistant.log;
  - ОС Linux: в файле /home/<user>/.config/UVEON/logs/Termidesk Assistant.log.

Каталог хранения файлов журналов может быть изменен на этапе установки или через задание переменной окружения в файле:

- для серверной части: /etc/default/termidesk-assistant-server;
- для клиентской части:
  - в ОС Linux: /etc/default/termidesk-assistant-client;
  - в ОС Microsoft Windows каталог хранения файлов журналов задается через переменную окружения TDSK_LOG_USER_DIR.

УДАЛЕННЫЙ ПОМОЩНИК. НЕШТАТНЫЕ СИТУАЦИИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

Возможные неисправности при работе с Удаленным помощником и способы их устранения приведены в таблице (см. таблицу Перечень возможных нештатных ситуация и способов их устранения).

Таблица 415. Перечень возможных нештатных ситуация и способов их устранения

Индикация	Описание	Возможное решение
Клиентская часть Удаленного помощника зависает, а затем некорректно завершает свою работу	Если при активной трансляции экрана узла пользователя обновить страницу в веб-браузере, то клиентская часть некорректно завершает свою работу	Рекомендуется установить новейшие версии клиентской и серверной части Удаленного помощника

Индикация	Описание	Возможное решение
Нет подключения к экрану узла пользователя после обновления страницы в веб-браузере	Если после завершения сессии или обновления страницы в веб-браузере попытаться вновь организовать подключение к экрану узла пользователя, то подключение не устанавливается	Рекомендуется установить новейшие версии клиентской и серверной части Удаленного помощника
Ошибка: «Could not open playback device»	Ошибка возникает при запуске клиентской части Удаленного помощника от суперпользователя ОС	Для исправления ошибки следует выполнить команду: `sudo modprobe snd-aloop`
В окне веб-браузера отображается только основной монитор, подключенный к узлу пользователя	При многомониторной конфигурации узла пользователя в веб-браузере открывается только окно основного монитора пользователя	Это ожидаемое поведение, т.к. клиентская часть Удаленного помощника работает только с одним, основным монитором
В окне веб-браузера неактивна часть экрана узла пользователя	Часть экрана узла пользователя становится неактивной при отображении в окне веб-браузера: при прокрутке страницы к нижней части отображаемого экрана курсор мыши перемещается выше	Для разрешения ситуации следует выполнить масштабирование окна веб-браузера: поместить курсор к панели управления серверной части Удаленного помощника и воспользоваться колесиком мыши
В окне веб-браузера наблюдается задвоение курсоров, нарушена синхронизация координат курсора	После подключения к экрану пользовательской рабочей станции в окне веб-браузера нарушается синхронизация координат курсора, на экране отображаются два курсора	После подключения администратора к экрану пользовательской рабочей станции пользователю не допускается изменять режим или размер окна ПО Termidesk Viewer. Изменение размеров окна ПО Termidesk Viewer не изменяет координатную сетку курсора, что приводит к задвоению курсоров

ТЕРМИНЫ

Ключ Применяется в контексте файла, не опции в команде. Последовательность псевдослучайных чисел, сгенерированная особым образом

Сертификат Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу

СОКРАЩЕНИЯ

ЗПС Замкнутая программная среда

ОС Операционная система

ПО Программное обеспечение

ЭЦП Электронная цифровая подпись

API Application Programming Interface (интерфейс прикладного программирования)

FQDN Fully Qualified Domain Name (полностью определенное имя домена)

HTTPS Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)

ID Identification Data (идентификатор)

IP Internet Protocol (межсетевой протокол)

JSON JavaScript Object Notation (стандартный текстовый формат для структурированных данных)

REST Representational State Transfer (программная архитектура, определяющая условия работы API)

STUN Session Traversal Utilities for NAT (сетевой протокол, который позволяет определить внешний IP-адрес и другие параметры)

TCP Transmission Control Protocol (протокол управления передачей)

TLS Transport Layer Security (протокол защиты транспортного уровня)

URL Uniform Resource Locator (унифицированный указатель ресурса)

СЛЕТ.10001-01 91 03. ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ. КОМПОНЕНТ «ВИРТУАЛЬНЫЙ МОДУЛЬ TERMIDESK» (ВМТ)

ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ

Назначение документа

Настоящий документ является инструкцией по использованию компонента «Виртуальный модуль Termidesk» программного комплекса «Диспетчер подключений виртуальных рабочих мест Термидеск» (далее - Termidesk VDI, Termidesk VDI). Документ предназначен для администраторов системы и сети.

В документе приведено назначение, настройка и использование компонента «Виртуальный модуль Termidesk». Для того чтобы получить информацию по доступным действиям в веб-интерфейсе Termidesk VDI, необходимо обратиться к документам СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса» и СЛЕТ.10001-01 90 03 «Руководство администратора. Графический интерфейс управления программным комплексом».

Типографские соглашения

Приняты следующие типографские соглашения:

- `моноширинный шрифт` – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk VDI, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

ВМТ. ОБЩИЕ СВЕДЕНИЯ

Назначение компонента «Виртуальный модуль Termidesk»

Компонент «Виртуальный модуль Termidesk» (далее - ВМТ) представляет собой образ виртуальной машины (ВМ) (или диска ВМ) с предварительно установленной и настроенной операционной системой (ОС) и набором программного обеспечения (ПО), необходимого для эксплуатации Termidesk VDI.

ВМТ предоставляет фиксированный набор функций для быстрого развертывания и использования Termidesk VDI с выполнением минимума действий по его настройке, что существенно упрощает ввод в эксплуатацию программного комплекса. Каждый экземпляр ВМТ может быть установлен с различным набором функций Termidesk VDI.

Состав ВМТ:

- ОС Astra Linux Special Edition 1.8.1;
- программные пакеты из состава подключенного в ВМТ репозитория Termidesk VDI:
  - `termidesk-vdi`;

  - termidesk-gateway;
  - termidesk-digsig-keys;
  - termidesk-assistant-server;
- система управления базами данных (СУБД) PostgreSQL версии 15;
- брокер сообщений RabbitMQ;
- веб-сервер Apache;
- служба ведения журналов syslog-ng;
- инструмент обеспечения высокой доступности узлов и служб keepalived;
- инструмент организации списка сетей ipset.

При первичной настройке ВМТ выбирается один из двух режимов защищенности ОС Astra Linux Special Edition: «Базовый» («Орел») или «Усиленный» («Воронеж»). Режим защищенности определяет, какие механизмы безопасности ОС будут активированы. Для режима «Базовый» специальные механизмы безопасности ОС не активируются.

Для режима «Усиленный» активируются следующие специальные механизмы безопасности ОС Astra Linux Special Edition:

- режим замкнутой программной среды (astra-digsig-control);
- механизм контроля целостности в ядре (astra-mic-control);
- режим мандатного контроля целостности файловой системы (set-fs-ilev);
- режим безопасного удаления файлов (astra-secdel-control);
- блокировка загрузки неиспользуемых модулей ядра (astra-modban-lock);
- отключение отображения меню загрузчика GRUB (astra-nobootmenu-control).

ВМТ распространяется в следующих форматах:

- для гипервизоров QEMU/KVM:
  - диск termidesk-virtual-appliance_<версия>_kvm.qcow2;
- для платформы виртуализации VMware:
  - пакет открытого виртуального устройства, представленный файлом termidesk-virtual-appliance_<версия>_vmware.ova.

В образе ВМТ используются разные наборы инструментов гостевой ОС для указанных платформ.

ВМТ. ПОЛУЧЕНИЕ ОБРАЗОВ

ВМТ можно получить двумя способами:

- заполнив форму запроса на сайте Termidesk VDI: https://termidesk.ru/support/#request-support;
- через личный кабинет: https://lk-new.astralinux.ru/.

ВМТ. УСТАНОВКА И ОБНОВЛЕНИЕ

Установка ВМТ

Порядок развертывания ВМТ

ВМТ может быть установлен в следующих режимах:

- «Ферма» - используется для установки узлов фермы Termidesk VDI;
- «Агрегатор» - используется для установки портала «Агрегатор»;
- «База данных» - используется для установки узла с СУБД. Узел может содержать несколько баз данных (БД).

Ферма - логическое объединение узлов, взаимодействующих с одной БД.

Для режима «Ферма»используются три основных типа установки:

- «Комплексная» - используется для быстрой установки узла фермы с полным набором компонентов Termidesk VDI. Этот тип применяется для ознакомления с функционалом Termidesk VDI в тестовой среде;
- «Рекомендованная» - используется для установки узла фермы с минимальным набором компонентов («Менеджер рабочих мест» и «Универсальный диспетчер»), необходимых для функционирования Termidesk VDI. Для установки требуется подключение к СУБД. Этот тип обычно применяется для установки фермы в распределенном варианте;
- «Произвольная» - используется для установки отдельных компонентов Termidesk VDI («Менеджер рабочих мест», «Универсальный диспетчер», «Шлюз») или инфраструктурных компонентов (брокер сообщений RabbitMQ), исходя из потребности в них. Этот тип обычно применяется для расширения узлов существующей фермы.

Общий порядок развертывания ВМТ определяется сценариями использования, приведенными в таблице (см. таблицу Сценарии использования ВМТ).

Таблица 416. Сценарии использования ВМТ

Сценарий	Установка
Комплексная установка узла фермы для ознакомления с функционалом Termidesk VDI	Последовательность установки: 1) выбрать режим «Ферма»; 2) выбрать тип установки «Комплексная»
Установка фермы в стандартном распределенном варианте	Последовательность установки: 1) установить первый узел ВМТ с режимом «База данных»; 2) установить второй узел ВМТ с режимом «Ферма». Выбрать тип установки «Рекомендованная». Выбрать пункт «Менеджер рабочих мест». После установки выполнить экспорт ключей; 3) установить третий узел ВМТ с режимом «Ферма». Выбрать тип установки «Рекомендованная». Выбрать пункт «Диспетчер». Выполнить импорт ключей с узла, установленного на шаге 2); 4) (опционально) установить четвертый узел ВМТ с режимом «Ферма». Выбрать тип установки «Произвольная». Выбрать пункт «Шлюз». Привязать узел к существующей ферме (будет соответствующий запрос в диалоговом окне), выполнить импорт ключей с узла, установленного на шаге 2)

Сценарий	Установка
Установка фермы в распределенном варианте с расширенным количеством узлов	Последовательность установки: 1) установить первый узел ВМТ с режимом «База данных»; 2) установить второй узел ВМТ с режимом «Ферма». Выбрать тип установки «Произвольная». Выбрать пункт «RabbitMQ». Не привязывать узел к существующей ферме (будет соответствующий запрос в диалоговом окне); 3) установить третий узел ВМТ с режимом «Ферма». Выбрать тип установки «Произвольная». Выбрать пункт «Celeryman». Не привязывать узел к существующей ферме (будет соответствующий запрос в диалоговом окне). После установки выполнить экспорт ключей; 4) установить четвертый узел ВМТ с режимом «Ферма». Выбрать тип установки «Произвольная». Выбрать пункт «Celeryman». Привязать узел к существующей ферме (будет соответствующий запрос в диалоговом окне), выполнить импорт ключей с узла, установленного на шаге 3); 5) установить пятый узел ВМТ с режимом «Ферма». Выбрать тип установки «Произвольный». Выбрать пункт «Диспетчер». Привязать узел к существующей ферме (будет соответствующий запрос в диалоговом окне), выполнить импорт ключей с узла, установленного на шаге 3); 6) установить шестой узел ВМТ с режимом «Ферма». Выбрать тип установки «Произвольный». Выбрать пункт «Диспетчер». Привязать узел к существующей ферме (будет соответствующий запрос в диалоговом окне), выполнить импорт ключей с узла, установленного на шаге 3); 7) (опционально, если планируется использование «Шлюза» Termidesk VDI) установить седьмой и восьмой узлы ВМТ с режимом «Ферма». Выбрать вариант установки «Произвольная». Выбрать пункт «Шлюз». Привязать узел к существующей ферме (будет соответствующий запрос в диалоговом окне), выполнить импорт ключей с узла, установленного на шаге 3)

Сценарий	Установка
Установка портала «Агрегатор»	Последовательность установки (ферма Termidesk VDI должна быть предварительно развернута в одном из вариантов, представленных выше): 1) установить первый узел ВМТ с режимом «База данных»; 2) установить второй узел ВМТ с режимом «Агрегатор»; 3) (опционально, если планируется использование «Шлюза» Termidesk VDI) установить третий узел ВМТ с режимом «Ферма». Выбрать тип установки «Произвольная». Выбрать пункт «Шлюз». Не привязывать узел к существующей ферме (будет соответствующий запрос в диалоговом окне)

Базовые настройки ВМТ

Для первичной настройки ВМТ нужно выполнить следующее:

- ознакомиться с лицензионным соглашением и нажать экранную кнопку **[OK]** (см. рисунок Лицензионное соглашение);

Переключение между пунктами меню выполняется клавишей **<TAB>**. Подтверждение выбора выполняется клавишами **<ENTER>** или **<SPACE>**.

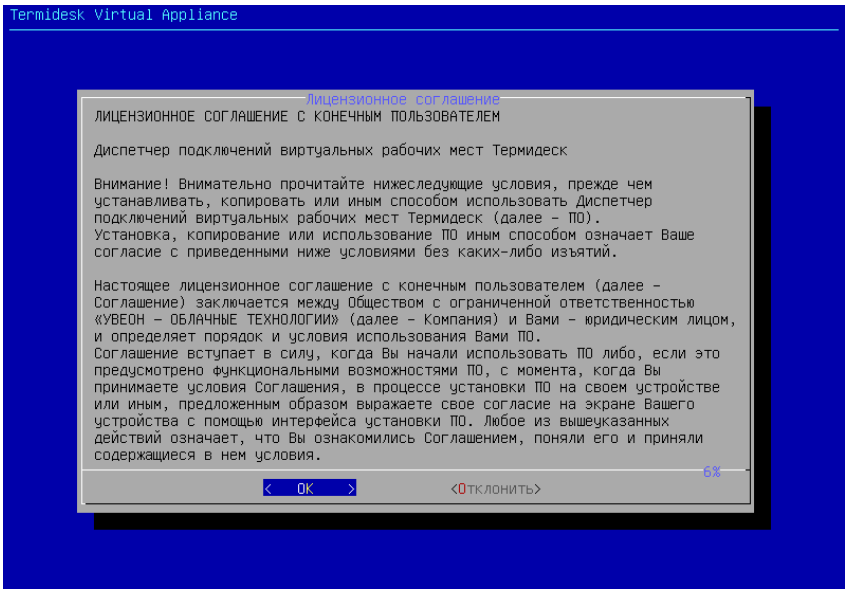


Рисунок 236. Лицензионное соглашение

- выбрать режим защищенности ОС (см. рисунок Выбор режима защищенности ОС). Режим защищенности определяет, какие механизмы безопасности ОС будут активированы. Для режима «basic» («Базовый») специальные механизмы безопасности ОС не активируются;

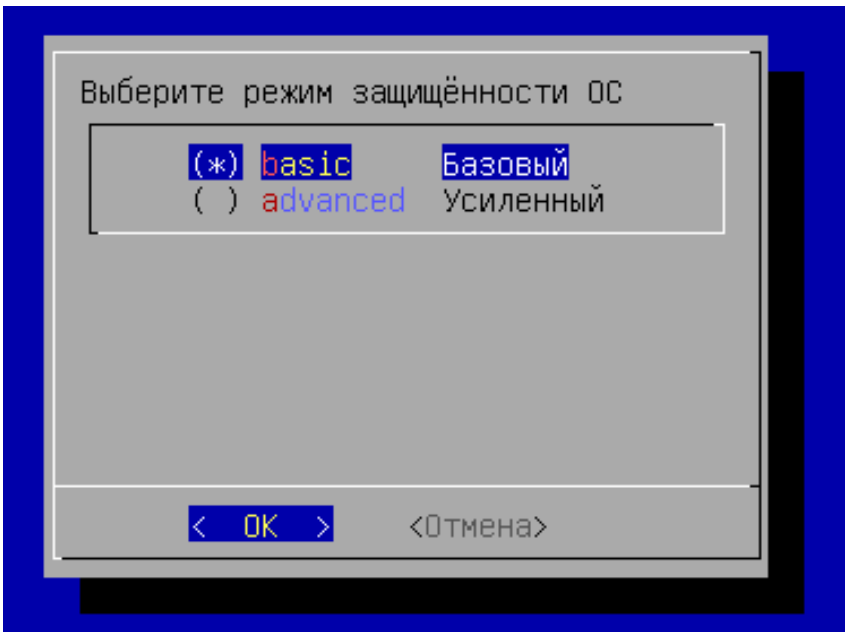


Рисунок 237. Выбор режима защищенности ОС

- согласиться с перезапуском системы для применения режима защищенности ОС;
- после перезапуска системы будет показано информационное сообщение (см. рисунок Сообщение о настроенном режиме защищенности) о настроенном режиме защищенности ОС и активированных механизмах (см. рисунок Информационное сообщение об активированных механизмах безопасности на примере режима «Базовый»);

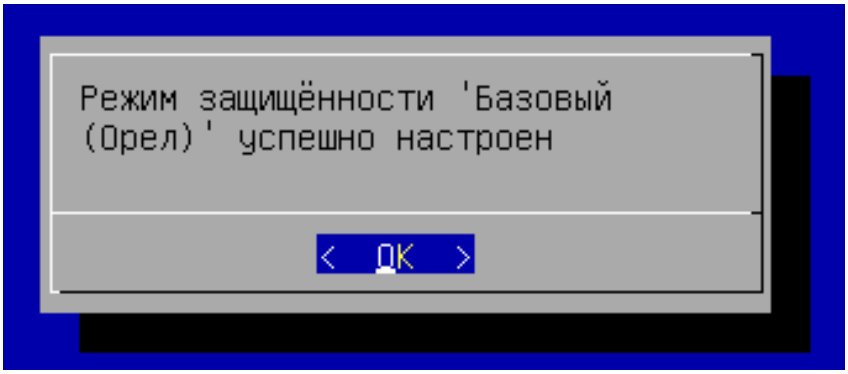


Рисунок 238. Сообщение о настроенном режиме защищенности

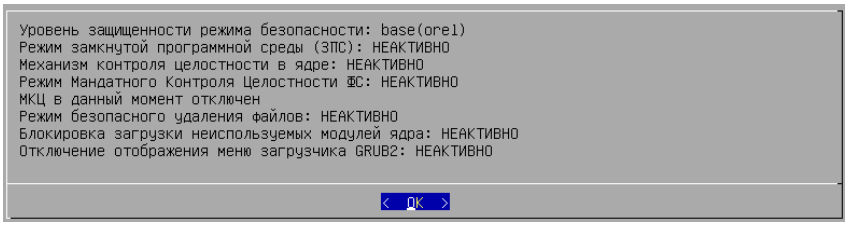


Рисунок 239. Информационное сообщение об активированных механизмах безопасности на примере режима «Базовый»

- заполнить имя хоста (hostname), которое будет использоваться для идентификации устройства в сети (см. рисунок Ввод имени хоста). Необходимо учесть, что указанный hostname, в свою очередь, должен являться полным доменным именем (FQDN), если ВМТ используется в домене. Указанный hostname будет использован для настройки веб-сервера apache;

Необходимо учесть, что при использовании указанного имени в других

подключениях требуется, чтобы в сетевой инфраструктуре имена хостов могли разрешаться в IP-адреса (должен быть настроен DNS-сервер).

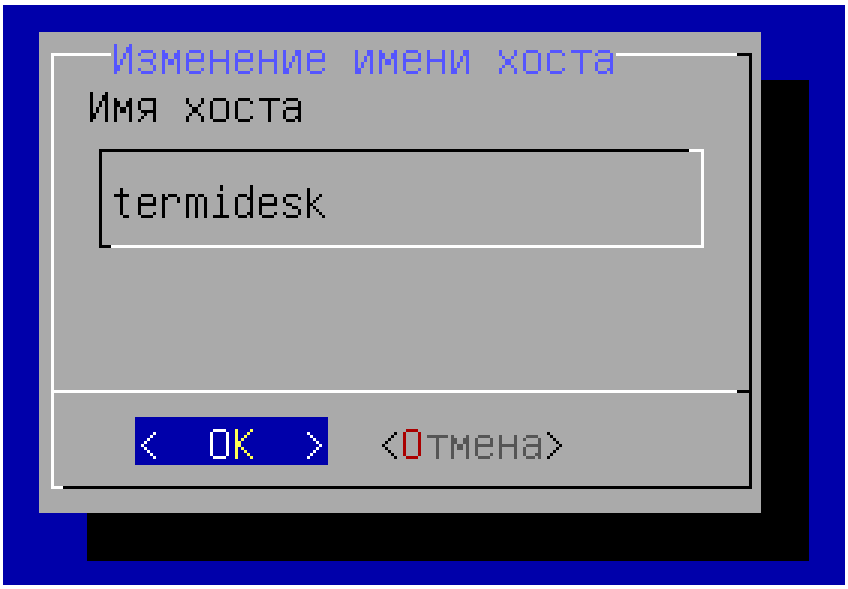


Рисунок 240. Ввод имени хоста

- после применения настройки будет показано информационное сообщение (см. рисунок Информационное сообщение об успешном изменении имени хоста);

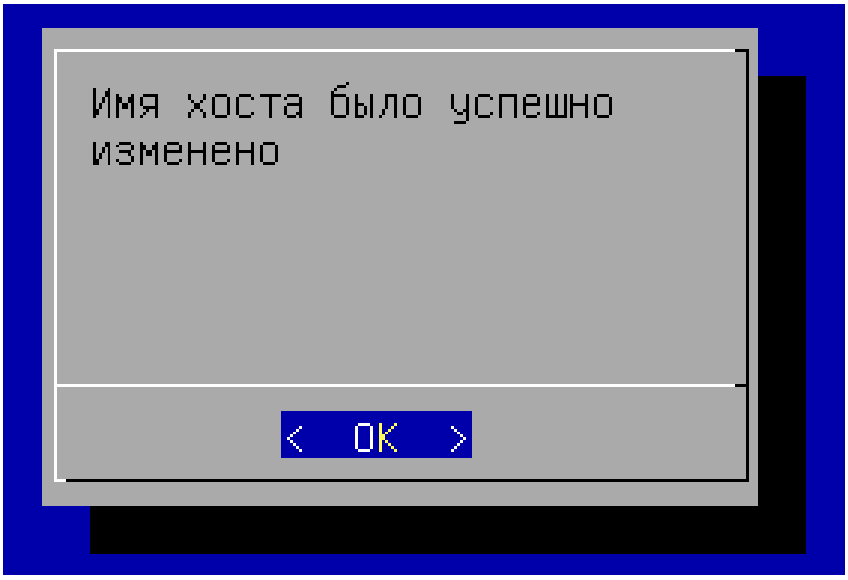


Рисунок 241. Информационное сообщение об успешном изменении имени хоста

- выбрать сетевые интерфейсы при помощи клавиши **<SPACE>** (см. рисунок Выбор сетевого интерфейса);

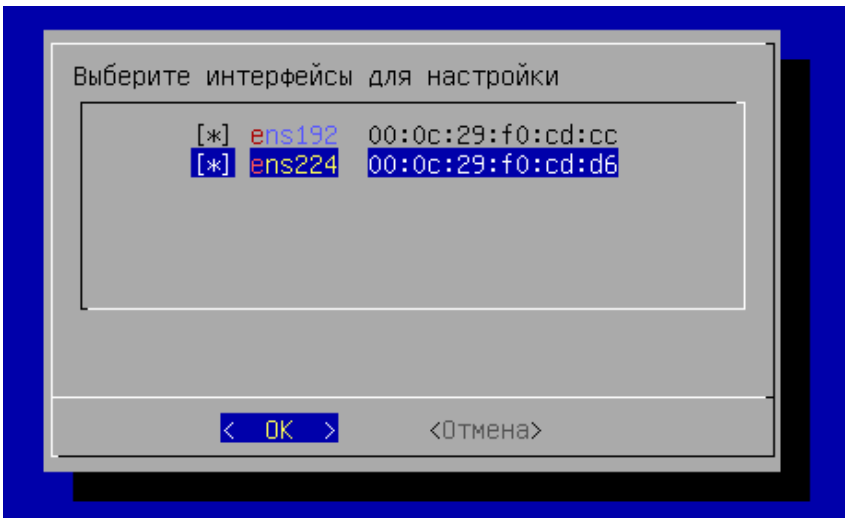


Рисунок 242. Выбор сетевого интерфейса

- далее указать сетевые настройки: IP-адрес, маску сети, IP-адрес шлюза и IP-адреса DNS-серверов, выполняющих разрешение сетевых имен в IP-адреса. Настройки следует выполнить для каждого интерфейса. По умолчанию предложено задать статические настройки (см. рисунок Задание статических сетевых настроек), однако при помощи клавиши **<TAB>** можно перейти к меню «DHCP», нажать клавишу <ENTER> и получить сетевые параметры от DHCP-сервера;

Все указанные IP-адреса должны быть заменены на актуальные, соответствующие схеме адресации, принятой в инфраструктуре организации.

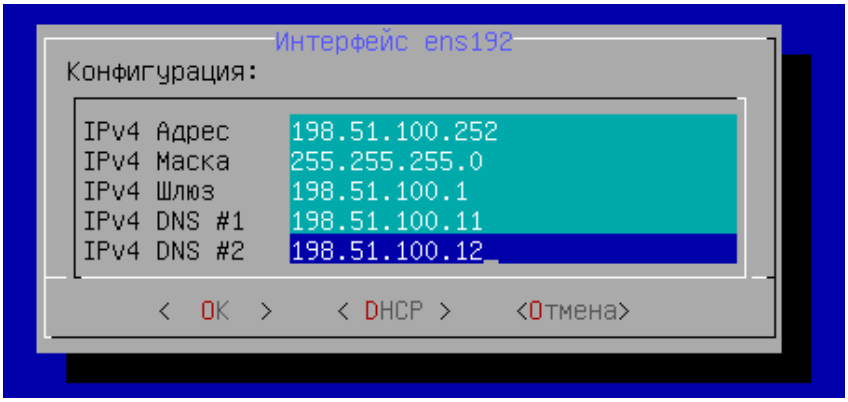


Рисунок 243. Задание статических сетевых настроек

- изучить заданные параметры и подтвердить изменение сетевых настроек, нажав экранную кнопку **[Да]** (см. рисунок Подтверждение сетевых настроек);

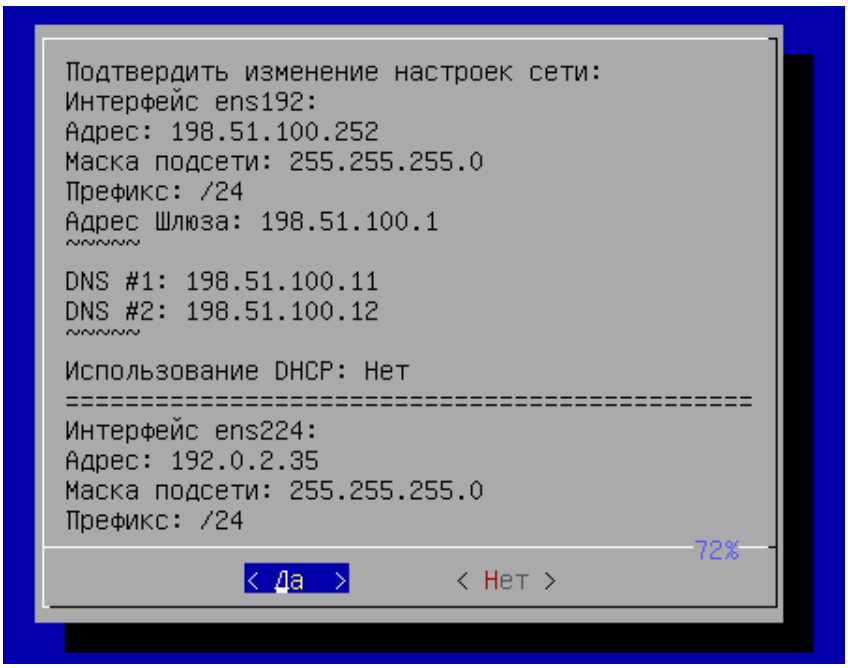


Рисунок 244. Подтверждение сетевых настроек

- после применения настроек будет показано информационное сообщение (см. рисунок Информационное сообщение об успешной конфигурации сетевых интерфейсов).

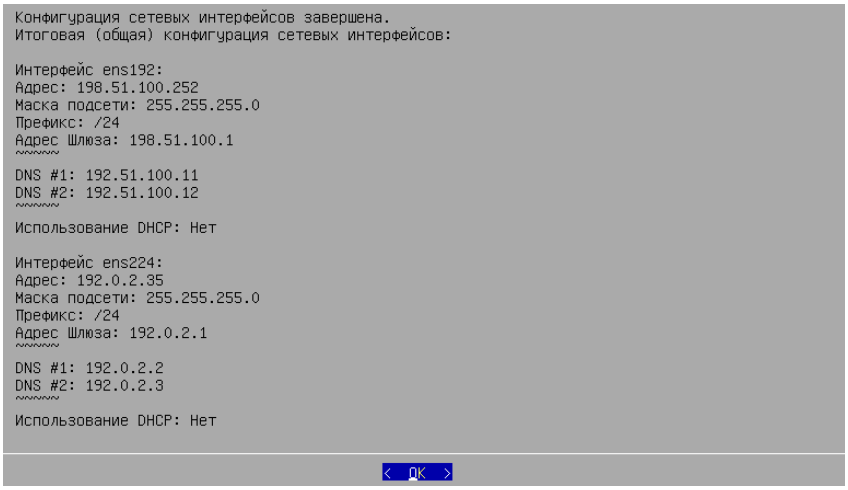


Рисунок 245. Информационное сообщение об успешной конфигурации сетевых интерфейсов

Комплексная установка

Комплексная установка позволяет быстро установить и настроить на узле все необходимые компоненты Termidesk VDI.

Комплексную установку рекомендуется использовать только для ознакомления в тестовой среде.

В процессе установки нужно:

- выполнить базовую настройку ВМТ;
- выбрать режим установки «Ферма» (см. рисунок Выбор режима установки):

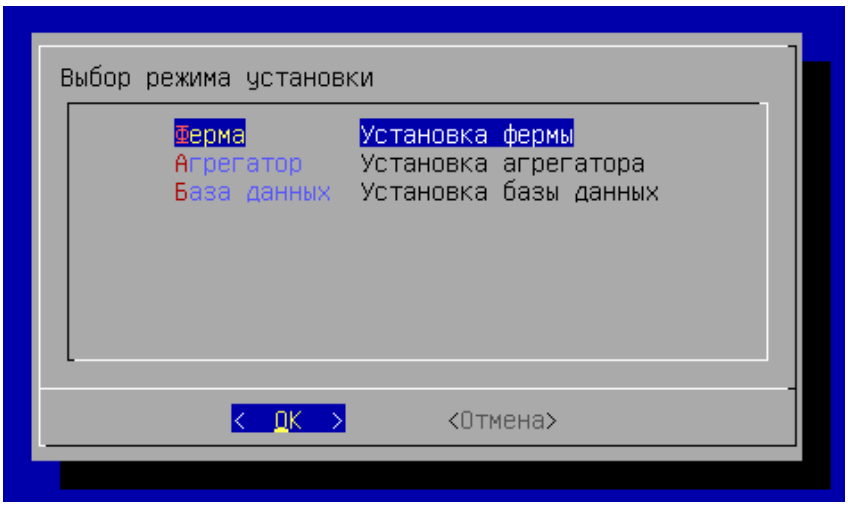


Рисунок 246. Выбор режима установки

- далее выбрать тип установки в режиме фермы «Комплексная» (см. рисунок Выбор комплексного типа установки в режиме фермы);

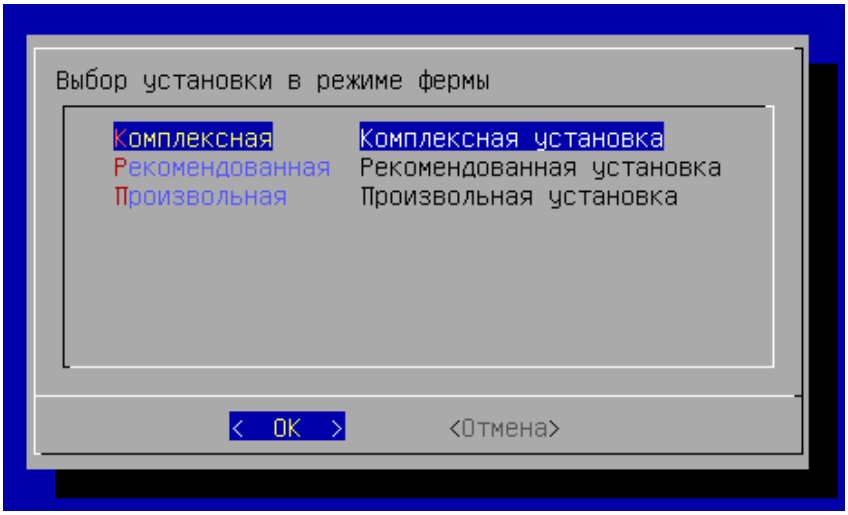


Рисунок 247. Выбор комплексного типа установки в режиме фермы

- далее задать уникальное имя узла для его идентификации (см. рисунок Настройка уникального имени узла). Это требуется для однозначной идентификации узлов, в частности, узлов «Агрегатора» во время балансировки подключений к ним;

Рисунок 248. Настройка уникального имени узла

После выполнения шагов по комплексной установке фермы произойдет переход в окно управления ВМТ (см. рисунок Окно управления ВМТ). Службы Termidesk VDI будут автоматически активированы, перезагрузка не требуется. IP-адрес, отображаемый в

главном окне ВМТ, соответствует IP-адресу первого настроенного интерфейса.

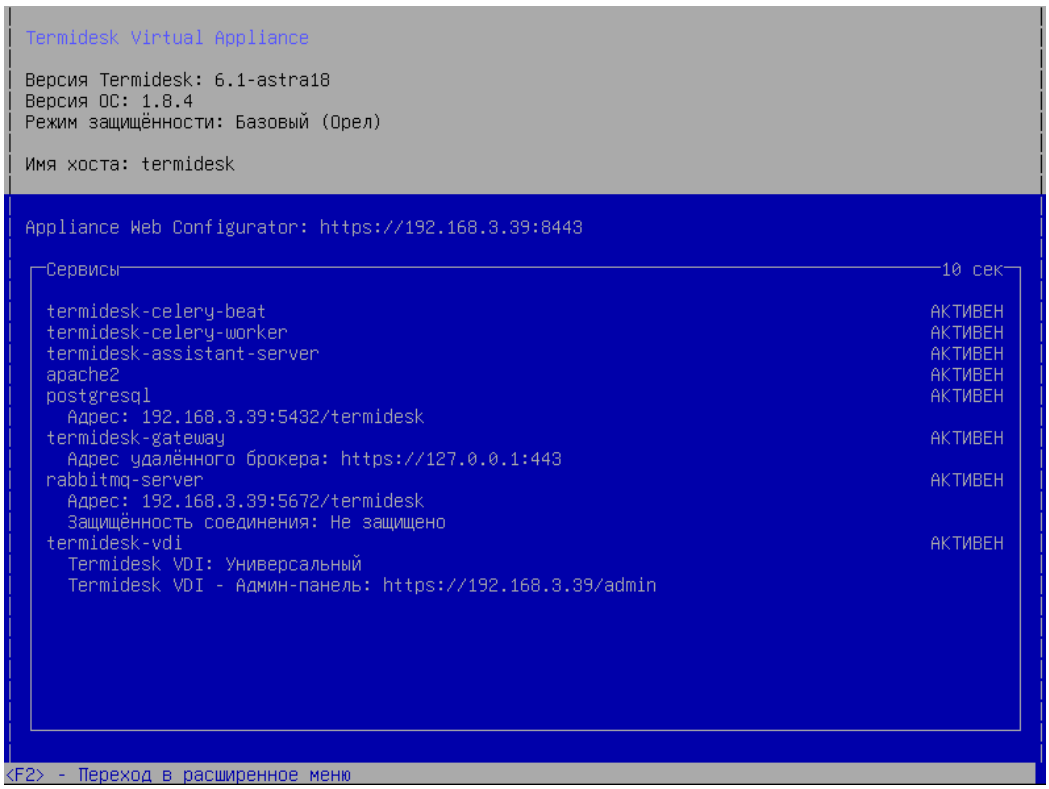


Рисунок 249. Окно управления ВМТ

После установки на узле будут установлены следующие компоненты:

- «Универсальный диспетчер» с ролями «Портал администратора» и «Портал пользователя». После установки будет запущена служба `termidesk-vdi`;
- «Менеджер рабочих мест». После установки будут запущены службы `termidesk-celery-beat`, `termidesk-celery-worker`;
- серверная часть компонента «Удаленный помощник». После установки будет запущена служба `termidesk-assistant-server`;
- веб-сервер Apache;
- СУБД PostgreSQL, настройка БД будет выполнена автоматически. Для подключения к БД используются стандартные параметры:
  - наименование БД - `termidesk`;
  - имя пользователя для подключения к БД - `termidesk`;
  - пароль для подключения к БД - `ksedimret`;
  - номер порта, используемого для соединения с сервером СУБД - `5432`;
- «Шлюз». После установки будет запущена служба `termidesk-gateway`;
- брокер сообщений RabbitMQ. После установки будет запущена служба `rabbitmq-server`. Для подключения к RabbitMQ используются стандартные параметры:
  - номер порта, используемого для соединения с RabbitMQ - `5672`;
  - виртуальный узел, к которому будет производиться подключение - `termidesk`;
  - имя пользователя для подключения - `termidesk`;
  - пароль для подключения - `ksedimret`.

Рекомендованная установка

Рекомендованная установка позволяет создать узел фермы с минимальным набором компонентов для функционирования Termidesk VDI.

В процессе установки нужно:

- выполнить базовую настройку ВМТ;
- выбрать режим установки «Ферма» (см. рисунок Выбор режима установки):

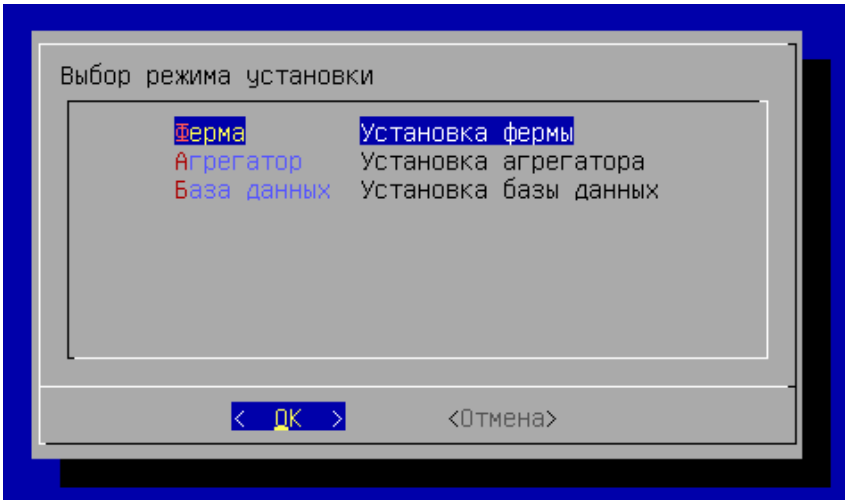


Рисунок 250. Выбор режима установки

- далее выбрать тип установки «Рекомендованная» (см. рисунок Выбор рекомендованного типа установки в режиме фермы);

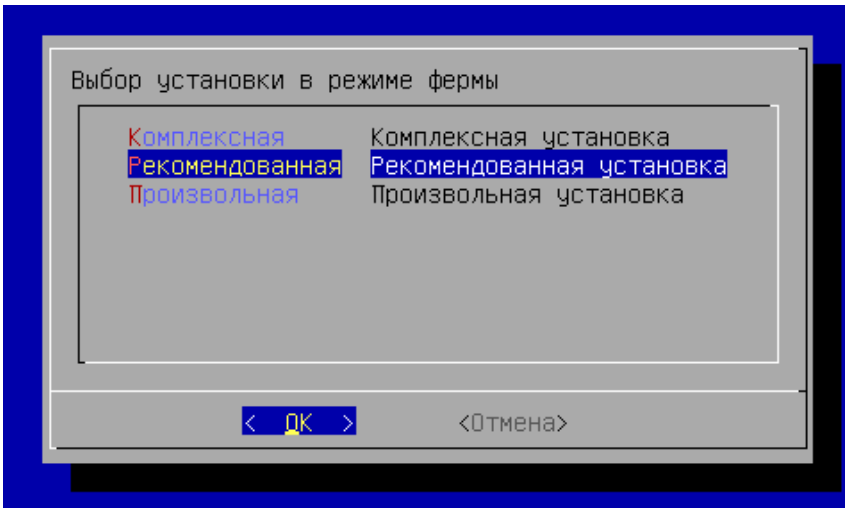


Рисунок 251. Выбор рекомендованного типа установки в режиме фермы

- в окне «Выбор установки в режиме фермы (рекомендованная)» следует выбрать компонент, который будет установлен на узел (см. рисунок Выбор компонента для установки).

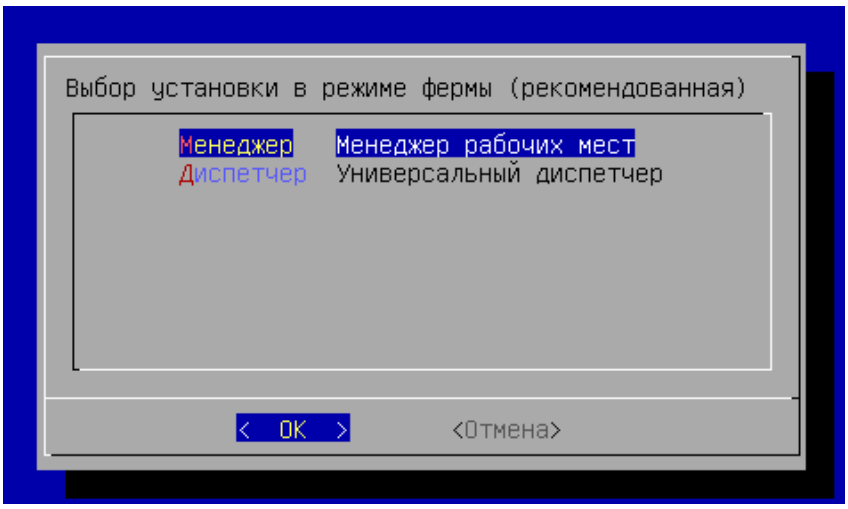


Рисунок 252. Выбор компонента для установки

В зависимости от выбранного варианта дальнейшие действия по настройке будут отличаться.

Если был выбран пункт «Менеджер», далее нужно выполнить:

- настроить параметры подключения к СУБД (см. рисунок Ввод параметров подключения к СУБД):

> Все указанные IP-адреса должны быть заменены на актуальные, соответствующие схеме адресации, принятой в инфраструктуре организации.
>
> Следует учесть, что в БД должны отсутствовать записи (необходимо использовать чистую БД). Также узел не должен использовать экземпляры БД, предназначенные для других компонентов Termidesk VDI (портала «Агрегатор»).

  - «Имя пользователя»: имя пользователя для подключения к БД (`termidesk`, значение по умолчанию при установке БД из состава ВМТ);
  - «Пароль»: пароль для подключения к БД (`ksedimret`, значение по умолчанию при установке БД из состава ВМТ);
  - «Хост»: IP-адрес или FQDN узла с установленной СУБД;
  - «Порт»: номер порта, используемого для соединения с сервером СУБД (стандартный порт `5432`);
  - «База данных»: наименование БД (`termidesk`, значение по умолчанию при установке БД из состава ВМТ);

> Если указанная БД не существует, но у пользователя есть права на ее создание, то будет отображен запрос «Подключение к базе данных прошло успешно, однако, база данных <имя> не существует. Желаете создать?». Следует ответить **<Да>**, если новая БД действительно нужна.

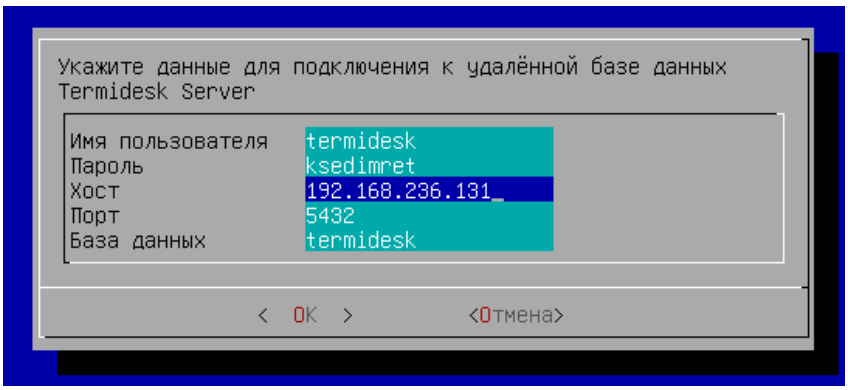


Рисунок 253. Ввод параметров подключения к СУБД

- убедиться, что подключение успешно выполнено, результат отобразится в информационном окне (см. рисунок Информационное сообщение о результате подключения к БД):

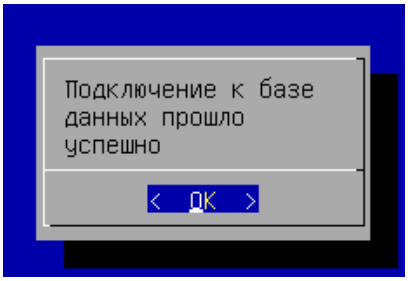


Рисунок 254. Информационное сообщение о результате подключения к БД

- указать протокол (см. рисунок Выбор протокола для подключения к БД), используемый для подключения к БД. При выборе значения «Disabled» защищенное соединение при подключении к БД использоваться не будет;

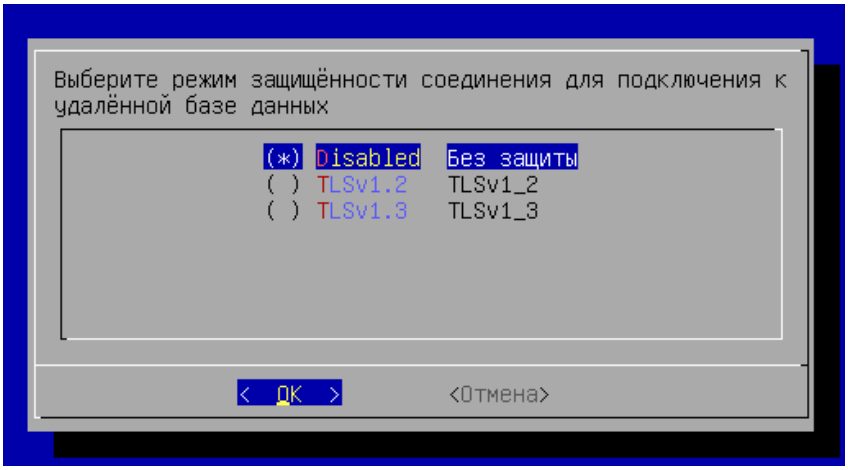


Рисунок 255. Выбор протокола для подключения к БД

- задать параметры для подключения к RabbitMQ (см. рисунок Параметры для подключения к RabbitMQ):
  - «Имя пользователя»: имя пользователя для подключения к RabbitMQ, по умолчанию `termidesk`;
  - «Пароль»: пароль для подключения к RabbitMQ, по умолчанию `ksedimret`;
  - «Хост»: указывается адрес установленного ранее «Менеджера рабочих мест», т.к. в режиме рекомендованной установки RabbitMQ устанавливается на одном узле с ним;
  - «Порт»: по умолчанию `5672`;

- «Очередь»: по умолчанию `termidesk`;

Перед продолжением установки необходимо удостовериться, что заданы правильные параметры подключения к RabbitMQ! В противном случае поменять параметры можно будет только подключившись по протоколу SSH к узлу.

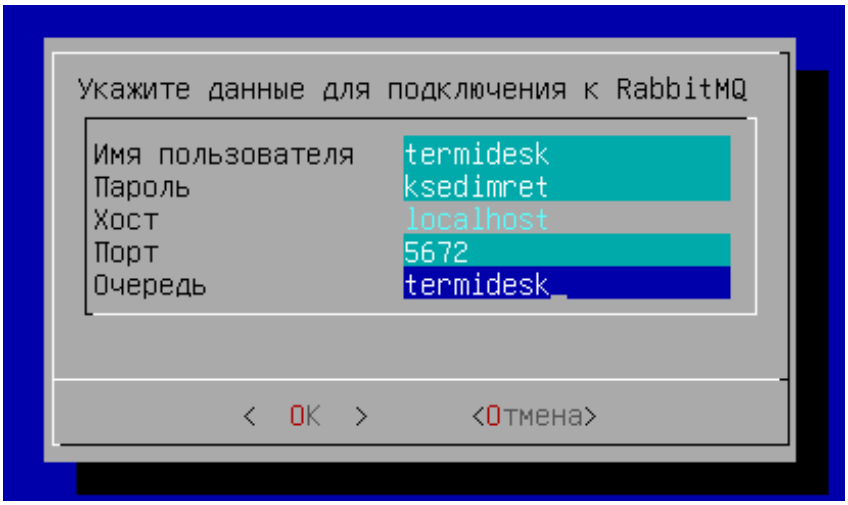


Рисунок 256. Параметры для подключения к RabbitMQ

- выбрать протокол, используемый для подключения к RabbitMQ (см. рисунок Выбор протокола для подключения к RabbitMQ). При выборе значения «Disabled» защищенное соединение при подключении к RabbitMQ использоваться не будет;

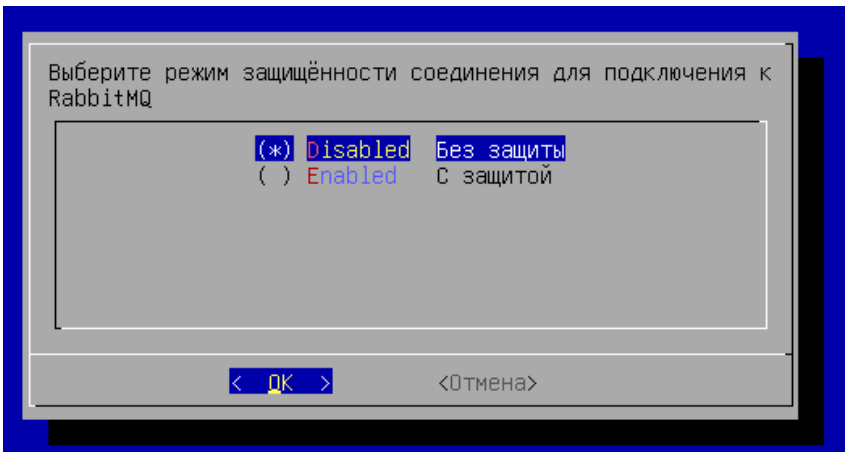


Рисунок 257. Выбор протокола для подключения к RabbitMQ

- задать уникальное имя узла для его идентификации (см. рисунок Указание уникального имени узла). Это требуется для однозначной идентификации узлов, в частности, узлов «Агрегатора» во время балансировки подключений к ним;

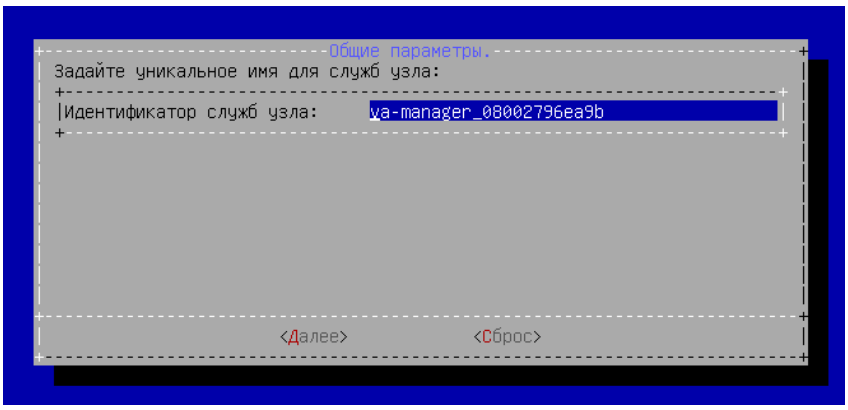


Рисунок 258. Указание уникального имени узла

- убедиться, что после установки произошел переход в окно управления ВМТ (см. рисунок Окно управления ВМТ с установленным компонентом «Менеджер рабочих мест»). Службы Termidesk VDI будут автоматически активированы, перезагрузка не требуется. IP-адрес, отображаемый в главном окне ВМТ, соответствует IP-адресу первого настроенного интерфейса.

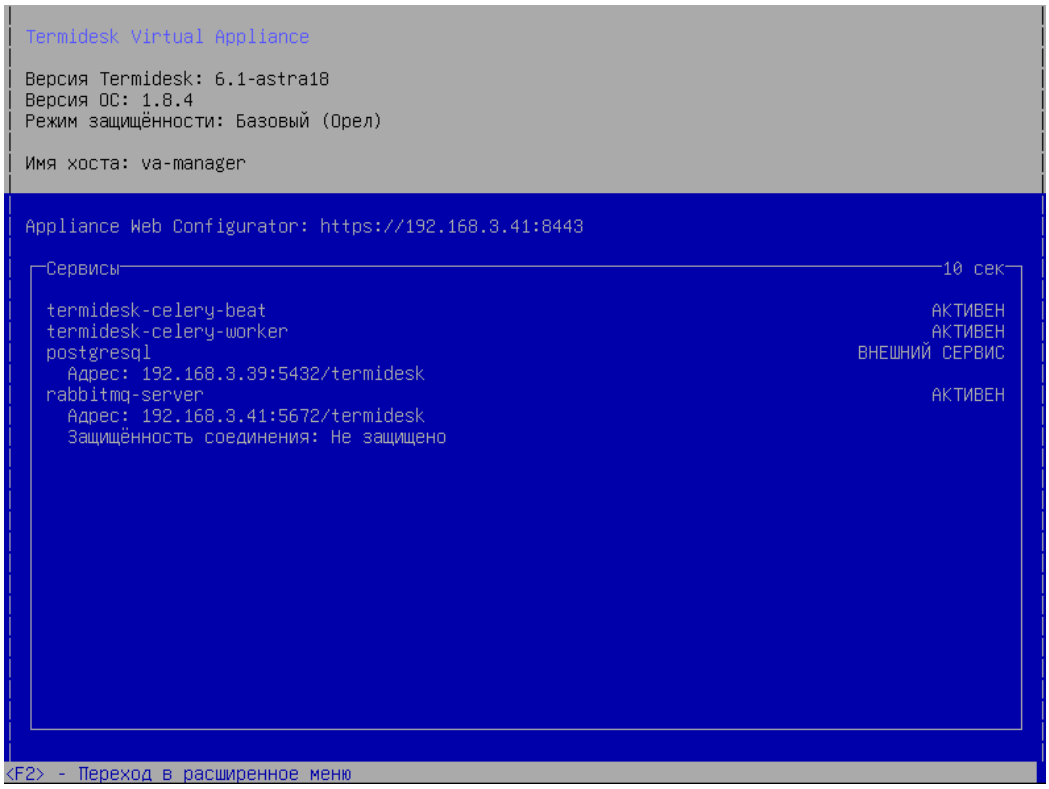


Рисунок 259. Окно управления ВМТ с установленным компонентом «Менеджер рабочих мест»

После установки на узле будут установлены:

- компонент «Менеджер рабочих мест», будут запущены службы `termidesk-celery-beat`,`termidesk-celery-worker`;
- брокер сообщений RabbitMQ, будет запущена служба `rabbitmq-server`.

Если был выбран пункт «Диспетчер», далее нужно выполнить:

- экспортировать конфигурацию с узла компонента «Менеджер рабочих мест» (см. подраздел **Экспорт параметров Termidesk VDI**);

- ввести данные для импортирования ключей (см. рисунок Импортирование ключей с узла компонента «Менеджер рабочих мест»):
  - «IP Адрес Mastera»: IP-адрес или FQDN узла с установленным компонентом «Менеджер рабочих мест»;
  - «Временный пароль»: временный пароль, созданный на узле компонента «Менеджер рабочих мест» при экспорте ключей;
  - «Секретное слово»: секретная фраза, заданная администратором при экспорте ключей с узла компонента «Менеджер рабочих мест»;

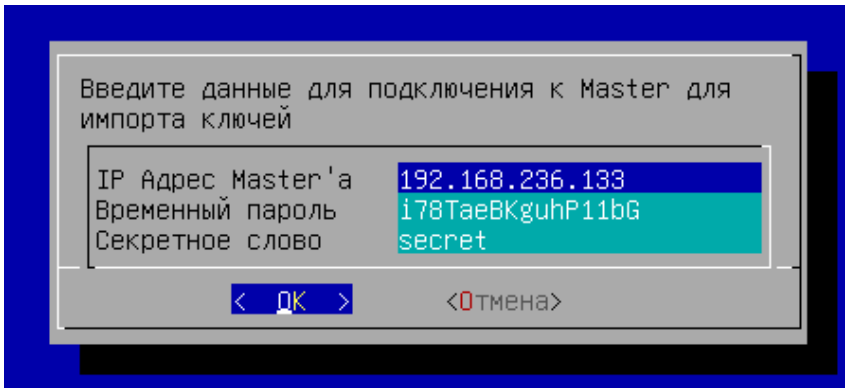


Рисунок 260. Импортирование ключей с узла компонента «Менеджер рабочих мест»

- убедиться, что конфигурация была успешно применена, результат конфигурации узла отобразится в информационном окне (см. рисунок Информационное сообщение о результате конфигурации узла):

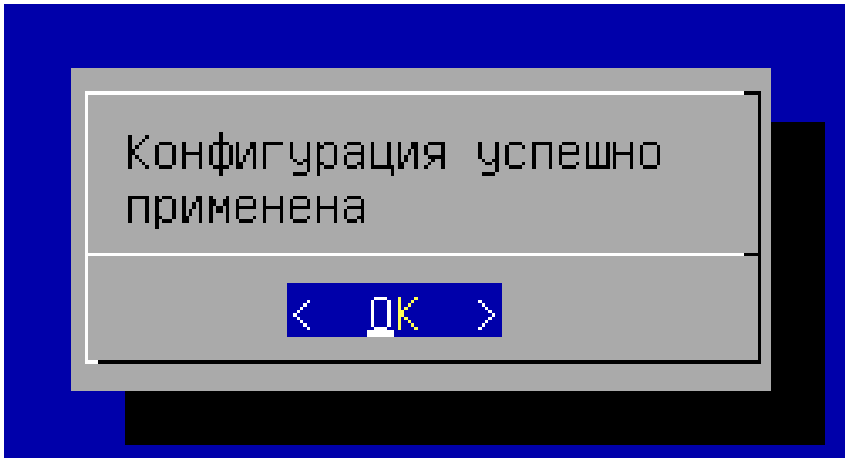


Рисунок 261. Информационное сообщение о результате конфигурации узла

- задать параметры для подключения к СУБД и RabbitMQ (см. рисунок Параметры для подключения к RabbitMQ) аналогично тому, как для узла компонента «Менеджер рабочих мест»;
- выбрать тип портала, который будет установлен для компонента «Универсальный диспетчер» (см. рисунок Выбор типа портала, с которым будет установлен компонент «Универсальный диспетчер»):
  - «Universal» - будет активирован «Портал универсальный», совмещающий в себе функции «Портала администратора» и «Портала пользователя»;
  - «User» - будет активирован «Портал пользователя», предоставляющий пользовательский интерфейс Termidesk VDI и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API;
  - «Admin» - будет активирован «Портал администратора», предоставляющий интерфейс управления Termidesk VDI и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API;

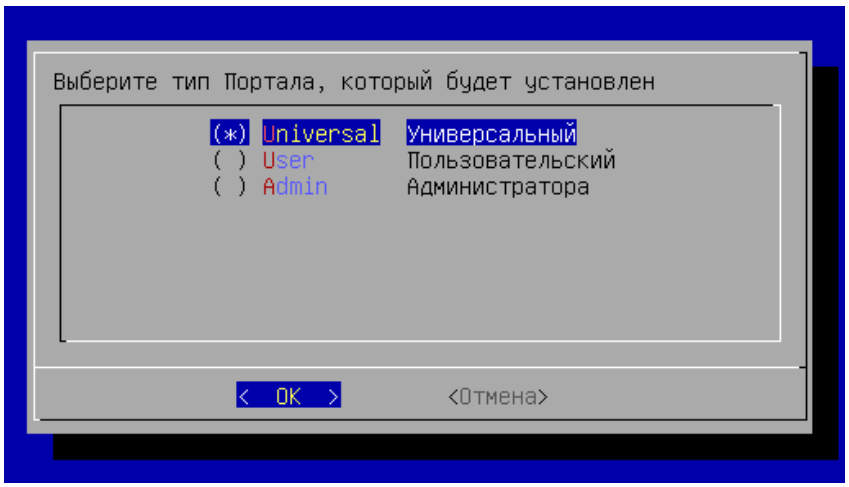


Рисунок 262. Выбор типа портала, с которым будет установлен компонент «Универсальный диспетчер»

- задать уникальное имя узла для его идентификации (см. рисунок Указание уникального имени узла). Это требуется для однозначной идентификации узлов, в частности, узлов «Агрегатора» во время балансировки подключений к ним;

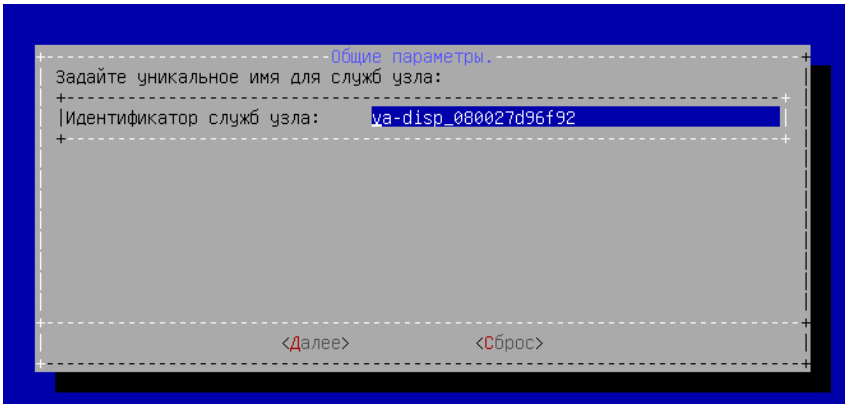


Рисунок 263. Указание уникального имени узла

- убедиться, что после установки произошел переход в окно управления ВМТ (см. рисунок Окно управления ВМТ с установленным компонентом «Универсальный диспетчер»). Службы Termidesk VDI будут автоматически активированы, перезагрузка не требуется. IP-адрес, отображаемый в главном окне ВМТ, соответствует IP-адресу первого настроенного интерфейса.

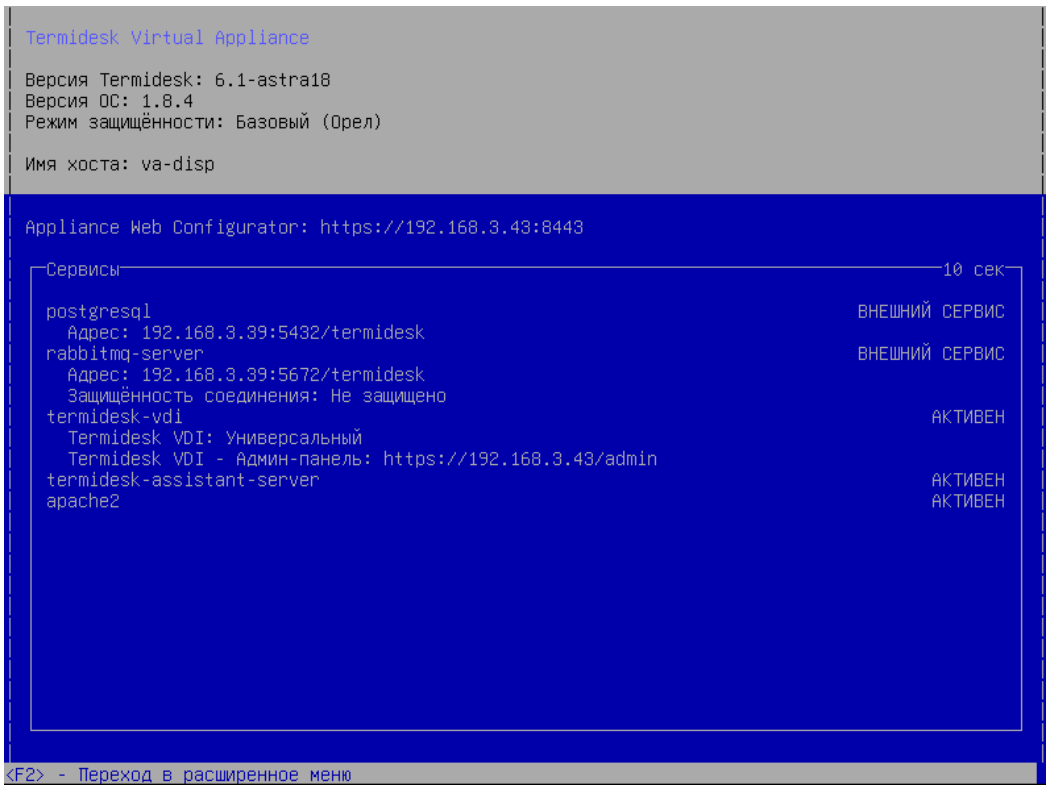


Рисунок 264. Окно управления ВМТ с установленным компонентом «Универсальный диспетчер»

После установки «Универсального диспетчера» будет запущены службы `termidesk-vdi` и `apache2`. Если были выбраны «Портал универсальный» и «Портал администратора», то будет установлена серверная часть компонента «Удаленный помощник».

Произвольная установка

Произвольная установка позволяет создать узел с отдельным компонентом Termidesk VDI или инфраструктурным компонентом.

В процессе установки нужно:

- выполнить базовую настройку ВМТ;
- выбрать режим установки «Ферма»;
- далее выбрать тип установки «Произвольная»;
- в окне «Выбор установки в режиме фермы (произвольная)» следует выбрать компонент, который будет установлен на узел (см. рисунок Выбор компонента для установки).

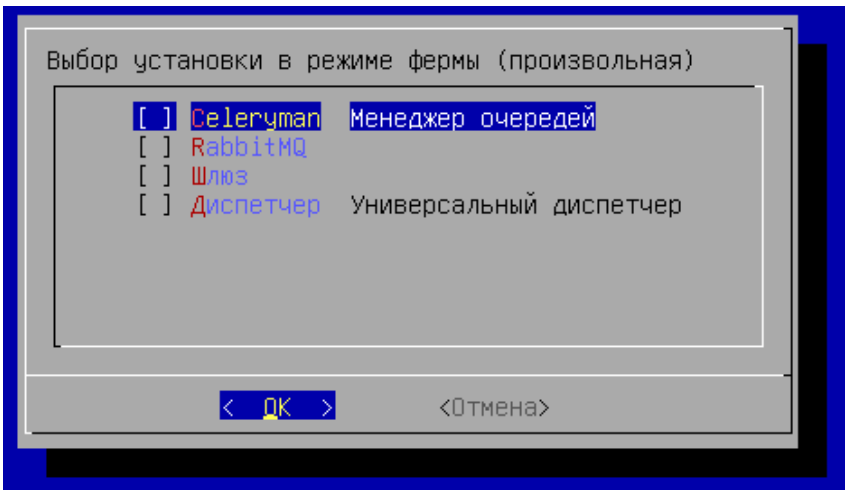


Рисунок 265. Выбор компонента для установки

В зависимости от выбранного варианта дальнейшие действия по настройке будут отличаться.

Если был выбран пункт «Celeryman», далее нужно выполнить:

- настроить параметры подключения к СУБД:
  - «Имя пользователя»: имя пользователя для подключения к БД (`termidesk`, значение по умолчанию при установке БД из состава ВМТ);
  - «Пароль»: пароль для подключения к БД (`ksedimret`, значение по умолчанию при установке БД из состава ВМТ);
  - «Хост»: IP-адрес или FQDN узла с установленной СУБД;
  - «Порт»: номер порта, используемого для соединения с сервером СУБД (стандартный порт `5432`);
  - «База данных»: наименование БД (`termidesk`, значение по умолчанию при установке БД из состава ВМТ);

Если указанная БД не существует, но у пользователя есть права на ее создание, то будет отображен запрос «Подключение к базе данных прошло успешно, однако, база данных <имя> не существует. Желаете создать?». Следует ответить **<Да>**, если новая БД действительно нужна.

- убедиться, что подключение успешно выполнено, результат отобразится в информационном окне;
- указать протокол, используемый для подключения к БД. При выборе значения «Disabled» защищенное соединение при подключении к БД использоваться не будет;
- задать параметры для подключения к RabbitMQ:
  - «Имя пользователя»: имя пользователя для подключения к RabbitMQ, по умолчанию `termidesk`;
  - «Пароль»: пароль для подключения к RabbitMQ, по умолчанию `ksedimret`;
  - «Хост»: IP-адрес или FQDN узла с установленным RabbitMQ;
  - «Порт»: по умолчанию `5672`;
  - «Очередь»: по умолчанию `termidesk`;

Перед продолжением установки необходимо удостовериться, что заданы правильные параметры подключения к RabbitMQ! В противном случае поменять параметры можно будет только подключившись по протоколу

SSH к узлу.

- выбрать протокол, используемый для подключения к RabbitMQ. При выборе значения «Disabled» защищенное соединение при подключении к RabbitMQ использоваться не будет;
- задать уникальное имя узла для его идентификации. Это требуется дляоднозначной идентификации узлов, в частности, узлов «Агрегатора» во время балансировки подключений к ним.

После установки на узле будут запущены службы `termidesk-celery-beat`, `termidesk-celery-worker`.

Если был выбран пункт «RabbitMQ», далее нужно выполнить:

- задать параметры RabbitMQ:
  - «Имя пользователя»: имя пользователя RabbitMQ;
  - «Пароль»: пароль подключения к RabbitMQ;
  - «Хост»: localhost (значение неизменяемое);
  - «Порт»: порт подключения к RabbitMQ;
  - «Очередь»: имя очереди;
- выбрать тип подключения, который будет настроен для RabbitMQ:
  - «Disabled» - защищенное соединение не будет настроено;
  - «Enabled» - будет автоматически настроено защищенное соединение по протоколу TLS 1.2.

На узле будет установлен брокер сообщений RabbitMQ, будет запущена служба `rabbitmq-server`.

Если был выбран пункт «Шлюз», далее нужно выполнить:

- ввести адрес узла «Универсальный диспетчер» или адрес балансировщика (если он используется) для подключения к нему. Указание порта для подключения является опциональным;
- задать параметры для подключения к RabbitMQ:
  - «Имя пользователя»: имя пользователя для подключения к RabbitMQ, по умолчанию `termidesk`;
  - «Пароль»: пароль для подключения к RabbitMQ, по умолчанию `ksedimret`;
  - «Хост»: IP-адрес или FQDN узла с установленным RabbitMQ;
  - «Порт»: по умолчанию `5672`;
  - «Очередь»: по умолчанию `termidesk`;

Перед продолжением установки необходимо удостовериться, что заданы правильные параметры подключения к RabbitMQ! В противном случае поменять параметры можно будет только подключившись по протоколу SSH к узлу.

- выбрать протокол, используемый для подключения к RabbitMQ. При выборе значения «Disabled» защищенное соединение при подключении к RabbitMQ использоваться не будет.

На узле будет установлен компонент «Шлюз», будет запущена служба

termidesk-gateway.

Компонент «Шлюз» из состава ВМТ рекомендуется использовать только для ознакомления в тестовой среде.

Если был выбран пункт «Диспетчер», далее нужно выполнить:

- настроить параметры подключения к СУБД:
  - «Имя пользователя»: имя пользователя для подключения к БД (termidesk, значение по умолчанию при установке БД из состава ВМТ);
  - «Пароль»: пароль для подключения к БД (ksedimret, значение по умолчанию при установке БД из состава ВМТ);
  - «Хост»: IP-адрес или FQDN узла с установленной СУБД;
  - «Порт»: номер порта, используемого для соединения с сервером СУБД (стандартный порт 5432);
  - «База данных»: наименование БД (termidesk, значение по умолчанию при установке БД из состава ВМТ);

Если указанная БД не существует, но у пользователя есть права на ее создание, то будет отображен запрос «Подключение к базе данных прошло успешно, однако, база данных <имя> не существует. Желаете создать?». Следует ответить **<Да>**, если новая БД действительно нужна.

- убедиться, что подключение успешно выполнено, результат отобразится в информационном окне;
- указать протокол, используемый для подключения к БД. При выборе значения «Disabled» защищенное соединение при подключении к БД использоваться не будет;
- задать параметры для подключения к RabbitMQ:
  - «Имя пользователя»: имя пользователя для подключения к RabbitMQ, по умолчанию termidesk;
  - «Пароль»: пароль для подключения к RabbitMQ, по умолчанию ksedimret;
  - «Хост»: IP-адрес или FQDN узла с установленным RabbitMQ;
  - «Порт»: по умолчанию 5672;
  - «Очередь»: по умолчанию termidesk;

Перед продолжением установки необходимо удостовериться, что заданы правильные параметры подключения к RabbitMQ! В противном случае поменять параметры можно будет только подключившись по протоколу SSH к узлу.

- выбрать протокол, используемый для подключения к RabbitMQ. При выборе значения «Disabled» защищенное соединение при подключении к RabbitMQ использоваться не будет.
- выбрать тип портала, который будет установлен для компонента «Универсальный диспетчер»:
  - «Universal» - будет активирован «Портал универсальный», совмещающий в себе функции «Портала администратора» и «Портала пользователя»;
  - «User» - будет активирован «Портал пользователя», предоставляющий пользовательский интерфейс Termidesk VDI и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API;
  - «Admin» - будет активирован «Портал администратора», предоставляющий

интерфейс управления Termidesk VDI и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API.

- задать уникальное имя узла для его идентификации. Это требуется для однозначной идентификации узлов, в частности, узлов «Агрегатора» во время балансировки подключений к ним.

После установки «Универсального диспетчера» будет запущены службы `termidesk-vdi` и `apache2`. Если были выбраны «Портал универсальный» и «Портал администратора», то будет установлена серверная часть компонента «Удаленный помощник».

Установка в режиме «Агрегатор»

Установка в режиме «Агрегатор» позволяет установить на узле портал «Агрегатор» с набором компонентов, необходимых для его функционирования.

В процессе установки нужно:

- выполнить базовую настройку ВМТ;
- выбрать режим установки «Агрегатор»;
- настроить параметры подключения к СУБД «Агрегатора»:
  - «Имя пользователя»: имя пользователя для подключения к БД (`termidesk`, значение по умолчанию при установке БД из состава ВМТ);
  - «Пароль»: пароль для подключения к БД (`ksedimret`, значение по умолчанию при установке БД из состава ВМТ);
  - «Хост»: IP-адрес или FQDN узла с установленной СУБД;
  - «Порт»: номер порта, используемого для соединения с сервером СУБД (стандартный порт `5432`);
  - «База данных»: наименование БД (`termidesk`, значение по умолчанию при установке БД из состава ВМТ);

Если указанная БД не существует, но у пользователя есть права на ее создание, то будет отображен запрос «Подключение к базе данных прошло успешно, однако, база данных <имя> не существует. Желаете создать?». Следует ответить **<Да>**, если новая БД действительно нужна.

- убедиться, что подключение успешно выполнено, результат отобразится в информационном окне;
- указать протокол, используемый для подключения к БД. При выборе значения «Disabled» защищенное соединение при подключении к БД использоваться не будет;
- задать параметры для подключения к RabbitMQ фермы Termidesk VDI:
  - «Имя пользователя»: имя пользователя для подключения к RabbitMQ, по умолчанию `termidesk`;
  - «Пароль»: пароль для подключения к RabbitMQ, по умолчанию `ksedimret`;
  - «Хост»: IP-адрес или FQDN узла с установленным RabbitMQ;
  - «Порт»: по умолчанию `5672`;
  - «Очередь»: по умолчанию `termidesk`;

Перед продолжением установки необходимо удостовериться, что заданы правильные параметры подключения к RabbitMQ! В противном случае поменять параметры можно будет только подключившись по протоколу

SSH к узлу.

- выбрать протокол, используемый для подключения к RabbitMQ. При выборе значения «Disabled» защищенное соединение при подключении к RabbitMQ использоваться не будет.
- выбрать тип веб-интерфейса, который будет установлен для «Агрегатора»:
  - «Universal» - будет активирован «Портал универсальный», совмещающий в себе функции «Агрегатора администратора» и «Агрегатора пользователя»;
  - «User» - будет активирован «Агрегатор пользователя», веб-интерфейс для получения ресурсов, предоставляемых «Агрегатором»;
  - «Admin» - будет активирован «Агрегатор администратора», веб-интерфейс управления «Агрегатором».

После установки будут запущены службы `termidesk-vdi`, `apache2` и `rabbitmq-server`.

- задать уникальное имя узла для его идентификации. Это требуется для однозначной идентификации узлов, в частности, узлов «Агрегатора» во время балансировки подключений к ним.

Установка в режиме «База данных»

Установка в режиме «База данных» позволяет установить и настроить на узле СУБД PostgreSQL, которая будет использоваться компонентами Termidesk VDI.

В процессе установки нужно:

- выполнить базовую настройку ВМТ;
- выбрать режим установки «База данных»;
- задать параметры для подключения к СУБД:
  - «Имя пользователя»: имя пользователя для подключения к БД, по умолчанию `termidesk`;
  - «Пароль»: пароль для подключения к БД, по умолчанию `ksedimret`;
  - «Хост»: установка СУБД в режиме «База данных» выполняется локально на текущем узле;
  - «Порт»: номер порта, используемого для соединения с сервером СУБД (стандартный порт `5432`);
  - «База данных»: наименование БД, по умолчанию `termidesk`;
- настроить права на создание новых БД пользователем:
  - выбрать **<Да>**, для выдачи пользователю разрешения на создание новых БД;
  - выбрать **<Нет>**, для отказа в выдаче разрешения;

Если пользователю выданы права на создание БД, при установке компонентов Termidesk VDI из состава ВМТ можно указать несуществующую БД. В этом случае отобразится запрос: «Подключение к базе данных прошло успешно, однако база данных <имя> не существует. Желаете создать?». Для создания новой БД следует выбрать **<Да>**, после чего ее можно будет использовать при установке компонента.

- после установки СУБД PostgreSQL будет запущена служба `postgresql`.

Проверка работоспособности

ВМТ работоспособен, если после установки отобразилось главное меню ВМТ, а также при переходе по адресу https://<IP-адрес_ВМТ>:8443/ отобразилась страница авторизации веб-интерфейса ВМТ (см. рисунок Страница авторизации веб-интерфейса VA).

Для доступа к веб-интерфейсу ВМТ после установки необходимо использовать следующие данные:

- логин: `admin`;
- пароль: `admin`.

При трех подряд неудачных попытках авторизации доступ к веб-интерфейсу блокируется на 60 секунд.

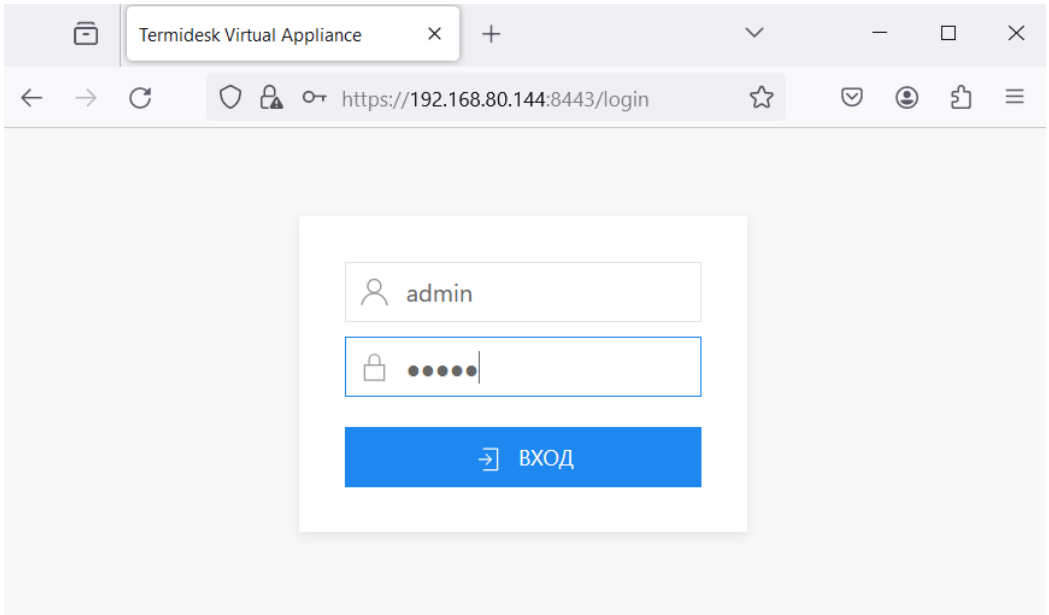


Рисунок 266. Страница авторизации веб-интерфейса VA

Обновление ВМТ

Обновление фермы Termidesk VDI для комплексной конфигурации установки

Общая концепция обновления фермы Termidesk VDI для комплексной конфигурации установки

Описание применимо к ферме Termidesk VDI, установленной в комплексной конфигурации через ВМТ. Общая последовательность действий приведена на рисунке (см. рисунок Обновление комплексной конфигурации фермы Termidesk VDI).

Перед обновлением требуется удалить через «Портал администратора» Termidesk VDI:

- фонды и шаблоны, созданные ранее для поставщика ресурсов «Static IP Machines»;
- шаблоны РМ «Статичная ВМ» (для всех поставщиков ресурсов, ранее имевших эти шаблоны) и ассоциированные с ними фонды;
- шаблоны, созданные ранее для поставщика ресурсов VMmanager. Если шаблоны не были удалены перед обновлением, то после него необходимо отредактировать существующие шаблоны и корректно

задать значения новых параметров.

Обновление должно осуществляться с соблюдением условия: после начала процедуры обновления запрещается производить любые операции с объектами на «Порталах» с предыдущими версиями Termidesk VDI.

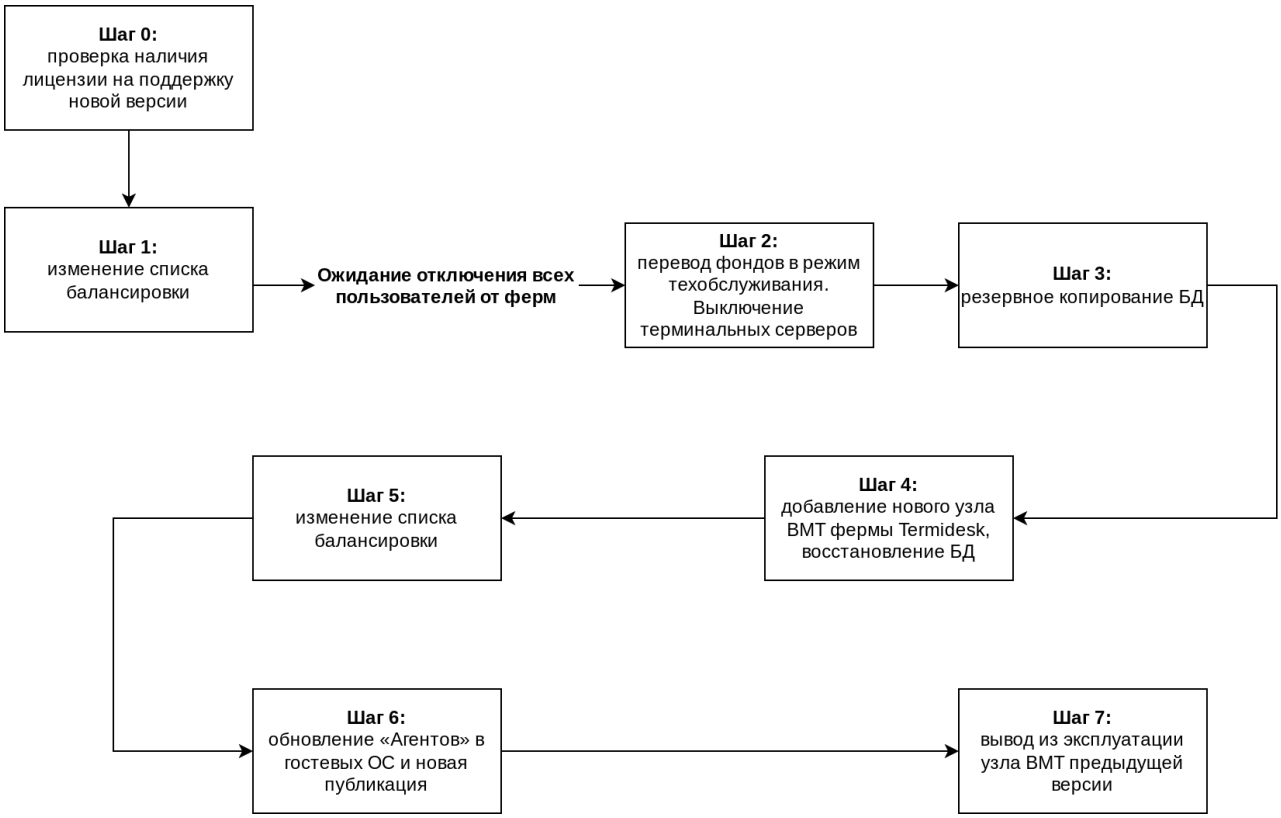


Рисунок 267. Обновление комплексной конфигурации фермы Termidesk VDI

При обновлении добавляются новые узлы. Поскольку любой новый узел имеет свой IP-адрес (или FQDN), то в этом случае нужно учесть, что все компоненты «Агента» должны получить новый адрес для регистрации в Termidesk VDI. Потребуется настроить «Агенты» на взаимодействие с новым узлом «Универсального диспетчера». Например, для удобства можно использовать:

- технологию балансировки виртуальных IP-адресов;
- alias-записи в DNS совместно с циклическим перебором (DNS Round Robin).

Последовательность обновления фермы Termidesk VDI, установленной в комплексной конфигурации:

Обновление выполняется с приостановкой обслуживания пользователей!Требуется заранее спланировать временной промежуток приостановки обслуживания.

Шаг 0. Проверить наличие лицензии на поддержку новой версии Termidesk VDI.

Шаг 1. На всех балансировщиках нагрузки, отвечающих за распределение подключений, из списка балансировки вывести узлы ВМТ.

Шаг 2. Все пользователи должны отключиться от фондов РМ. Нужно дождаться завершения работы пользователей. Затем:

- через веб-интерфейс «Портал администратора» перевести все фонды РМ в режим техобслуживания;
- выключить все терминальные серверы, которые были подключены в Termidesk VDI как поставщики ресурсов.

Шаг 3. Выполнить резервное копирование БД.

Шаг 4. Добавить узел ВМТ новой версии с комплексной установкой фермы Termidesk VDI. Убедиться, в наличии резервной копии БД старого узла ВМТ, затем перенести резервную копию БД на новый узел ВМТ.

Шаг 5. Изменить список балансировки, заменив адреса узлов ВМТ на новые. Проверить доступность графического интерфейса Termidesk VDI сначала обращением на IP-адрес каждого из «Универсальных диспетчеров», затем обращением на IP-адрес балансировщика нагрузки.

Шаг 6. После выполнения обновления узлов:

- обновить компоненты в гостевых ОС РМ (в базовом ВРМ - «золотом образе» или в ОС терминального сервера) в соответствии с документацией на них:
  - «Агент виртуального рабочего места»;
  - «Агент виртуальных смарт-карт»;
  - «Видеоагент»;
  - «Сессионный агент»;
  - STAL (если используется);
  - TERA (если используется);
- выполнить новую публикацию в фондах РМ, если публикация применима к ним (для фондов с терминальными серверами публикация не выполняется).

Шаг 7. Выключение узла ВМТ предыдущей версии.

Шаг 1. Изменение конфигурации балансировщика нагрузки

На балансировщике нагрузки открыть и отредактировать файл конфигурации, в котором перечисляются узлы ВМТ для балансировки:

- вывести все узлы ВМТ из балансировки;
- сохранить файл;
- перезагрузить службу балансировщика нагрузки.

Выполнить действия на всех балансировщиках нагрузки.

Шаг 2. Перевод фондов в режим техобслуживания

Для продолжения обновления нужно дождаться отключения пользователей от фондов рабочих мест.

Затем:

- через веб-интерфейс «Портал администратора» Termidesk VDI перевести **все** фонды в режим техобслуживания. Для этого перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Техобслуживание]** с выбором из выпадающего списка значения «Включить». Подтвердить включение режима;
- выключить каждый узел терминального сервера, который подключен к Termidesk VDI как поставщик ресурсов.

Шаг 3. Резервное копирование БД

Для резервного копирования БД нужно:

- удаленно подключиться узлу ВМТ (см. подраздел **Удаленное подключение к ВМТ**);
- выполнить резервное копирование БД (см. подраздел **Резервное копирование и восстановление БД**);
- сохранить резервную копию на внешнем носителе информации.

Шаг 4. Добавление нового узла ВМТ

Обновление фермы Termidesk VDI приводит к изменению UUID узла, что требует восстановления лицензии. Восстановить лицензию можно одним из способов:

- заполнить запрос на сайте Termidesk VDI: https://termidesk.ru/demonstration/ и выбрать пункт «Ключ активации»;
- подключить диск нового узла к старому узлу и настроить загрузку с этого диска;
- заменить UUID нового узла на UUID старого узла.

Для добавления узла нужно:

- добавить ВМ для загрузки ВМТ;
- выполнить базовые настройки ВМТ;
- выполнить установку узла фермы в режиме установки «Комплексная»;
- выполнить восстановление БД. Для этого:
  - остановить службы Termidesk VDI:

    ```
    sudo systemctl stop termidesk-vdi termidesk-gateway termidesk-celery-beat
    termidesk-celery-worker
    ```

  - переключиться на пользователя `postgres`:

    ```
    sudo su postgres
    ```

  - запустить терминальный клиент СУБД PostgreSQL:

    ```
    psql
    ```

  - удалить БД нового узла ВМТ:

    Перед выполнением операции необходимо убедиться, что удаляется БД, установленная на новом узле ВМТ.

    ```
    postgres=# DROP DATABASE termidesk;
    ```

  - создать пустую БД `termidesk` на новом узле ВМТ:

```
postgres=# CREATE DATABASE termidesk LC_COLLATE 'ru_RU.utf8' LC_CTYPE
'ru_RU.utf8' TEMPLATE template0;
```

- сделать пользователя `termidesk` владельцем БД `termidesk`, тем самым предоставив ему все возможные права:

```
postgres=# ALTER DATABASE termidesk OWNER TO termidesk;
```

- выйти из интерактивного интерфейса терминального клиента СУБД PostgreSQL:

```
postgres=# \q
```

- выйти из сеанса пользователя `postgres`:

```
exit
```

- выполнить восстановление БД (см. подраздел **Резервное копирование и восстановление БД**);
- затем привести структуру БД в соответствие актуальной версии Termidesk VDI:

```
sudo /opt/termidesk/sbin/termidesk-vdi-manage migrate
```

- после установки проверить доступность веб-порталов Termidesk VDI через веб-браузер.

Шаг 5. Изменение конфигурации балансировщика нагрузки

На балансировщике нагрузки открыть и отредактировать файл конфигурации, в котором перечисляются узлы ВМТ для балансировки:

- заменить адреса узлов ВМТ предыдущих версий Termidesk VDI на адреса новых узлов ВМТ;
- сохранить файл;
- перезагрузить службу балансировщика нагрузки.

Выполнить действия на всех балансировщиках нагрузки.

Выполнить проверку доступности веб-порталов Termidesk VDI через веб-браузер сначала обращением на IP-адрес каждого из «Универсальных диспетчеров» (например, на «Портал администратора»), затем обращением на IP-адрес балансировщика нагрузки.

Шаг 6. Обновление компонентов в ОС рабочих мест и новая публикация

После выполнения всех шагов:

- обновляются компоненты в ОС РМ (в базовом ВРМ - «золотом образе» или в ОС терминального сервера) в соответствии с документацией на них:
  - «Агент виртуального рабочего места»;

- «Агент виртуальных смарт-карт»;
- «Видеоагент»;
- «Сессионный агент»;
- STAL (если используется);
- TERA (если используется);

- выполняется новая публикация в фондах РМ, если публикация применима к ним.

Для фондов с терминальными серверами публикация не выполняется: достаточно того, чтобы узел с терминальным сервером был включен.

Обновление комплексной конфигурации фермы Termidesk VDI с переходом на распределенную

Общая концепция обновления фермы Termidesk VDI с переходом в распределенную конфигурацию

Описание применимо к ферме Termidesk VDI, установленной первоначально в комплексной конфигурации ВМТ. Общая последовательность действий приведена на рисунке (см. рисунок Обновление фермы Termidesk VDI с переходом в распределенную конфигурацию).

Перед обновлением требуется удалить через «Портал администратора» Termidesk VDI:

- фонды и шаблоны, созданные ранее для поставщика ресурсов «Static IP Machines»;
- шаблоны РМ «Статичная ВМ» (для всех поставщиков ресурсов, ранее имевших эти шаблоны) и ассоциированные с ними фонды;
- шаблоны, созданные ранее для поставщика ресурсов VMmanager. Если шаблоны не были удалены перед обновлением, то после него необходимо отредактировать существующие шаблоны и корректно задать значения новых параметров.

Во время обновления распределенной конфигурации установки:

- изменение политик нужно проводить после обновления всех узлов Termidesk VDI;
- изменение системных параметров нужно проводить после обновления всех узлов Termidesk VDI.

Обновление должно осуществляться с соблюдением условия: после начала процедуры обновления запрещается производить любые операции с объектами на «Порталах» с предыдущими версиями Termidesk VDI.

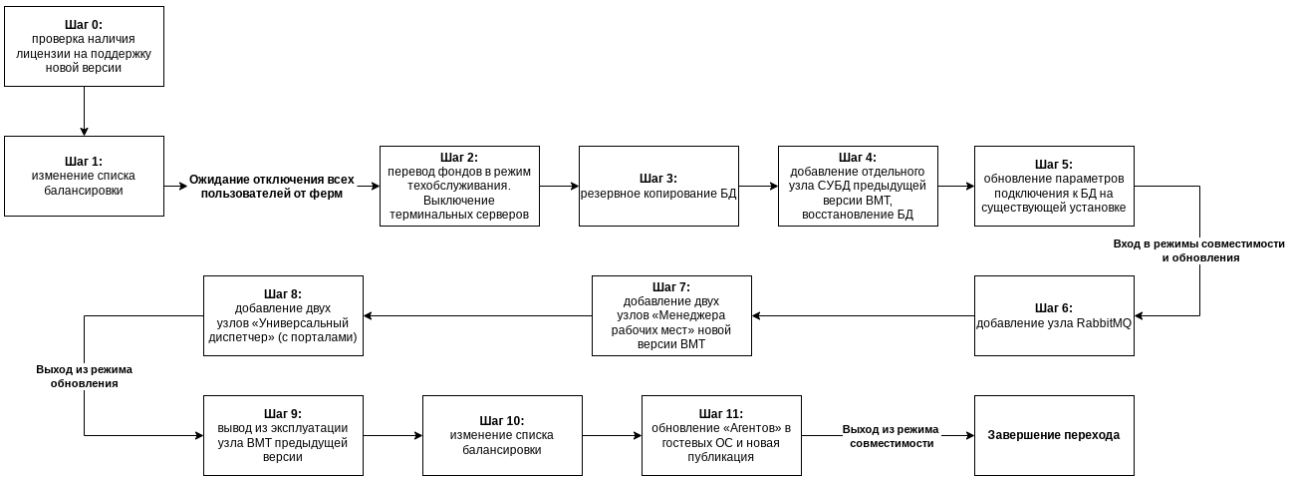


Рисунок 268. Обновление фермы Termidesk VDI с переходом в распределенную конфигурацию

На схеме:

- режим совместимости - режим, характеризующийся отличием в версиях между любыми компонентами фермы Termidesk VDI;
- режим обновления - режим, характеризующийся наличием не обновленных «Универсальных диспетчеров» при уже обновленных записях БД. Становится ограничен в действиях «Портал администратора». Ферма Termidesk VDI при этом должна работать с теми записями БД, которые есть на момент входа в этот режим.

При обновлении добавляются новые узлы. Поскольку любой новый узел имеет свой IP-адрес (или FQDN), то в этом случае нужно учесть, что все компоненты «Агента» должны получить новый адрес для регистрации в Termidesk VDI. Потребуется настроить «Агенты» на взаимодействие с новым узлом «Универсального диспетчера». Например, для удобства можно использовать:

- технологию балансировки виртуальных IP-адресов;
- alias-записи в DNS совместно с циклическим перебором (DNS Round Robin).

Последовательность обновления фермы Termidesk VDI, установленной в распределенной отказоустойчивой конфигурации:

Обновление выполняется с приостановкой обслуживания пользователей! Требуется заранее спланировать временной промежуток приостановки обслуживания.

Для обновления потребуется выполнить миграцию локальной БД на отдельный узел СУБД.

Шаг 0. Проверить наличие лицензии на поддержку новой версии Termidesk VDI.

Шаг 1. На всех балансировщиках нагрузки, отвечающих за распределение подключений, из списка балансировки вывести узлы ВМТ.

Шаг 2. Все пользователи должны отключиться от фондов РМ. Нужно дождаться завершения работы пользователей. Затем:

- через веб-интерфейс «Портал администратора» перевести все фонды РМ в режим техобслуживания;

- выключить все терминальные серверы, которые были подключены в Termidesk VDI как поставщики ресурсов.

Шаг 3. Выполнить резервное копирование БД.

Шаг 4. Добавить узел ВМТ предыдущей версии с СУБД. Выполнить восстановление БД из резервной копии.

Шаг 5. На существующем узле ВМТ, установленным в комплексном режиме, изменить параметры подключения к БД.

Шаг 6. Добавить узел ВМТ новой версии с компонентом RabbitMQ.

Шаг 7. Добавить два узла ВМТ новой версии с компонентом «Менеджер рабочих мест» («Менеджера очередей»).

Шаг 8. Добавить два узла ВМТ новой версии с компонентом «Универсальный диспетчер» с установкой порталов: «Портал администратора», «Портал пользователя» или «Портал универсальный». Тип портала выбирается исходя из потребностей в нем.

Шаг 9. Выключение узла ВМТ предыдущей версии.

Шаг 10. Изменить список балансировки, заменив адреса узлов ВМТ на новые. Проверить доступность графического интерфейса Termidesk VDI сначала обращением на IP-адрес каждого из «Универсальных диспетчеров», затем обращением на IP-адрес балансировщика нагрузки.

Шаг 11. После выполнения обновления узлов:

- обновить компоненты в гостевых ОС РМ (в базовом ВРМ - «золотом образе» или в ОС терминального сервера) в соответствии с документацией на них:
  - «Агент виртуального рабочего места»;
  - «Агент виртуальных смарт-карт»;
  - «Видеоагент»;
  - «Сессионный агент»;
  - STAL (если используется);
  - TERA (если используется);
- выполнить новую публикацию в фондах РМ, если публикация применима к ним (для фондов с терминальными серверами публикация не выполняется).

После выполнения всех шагов убедиться, что ферма находится в работоспособном состоянии, пользователи могут подключиться к рабочим местам.

Шаг 1. Редактирование конфигурации балансировки

На балансировщике нагрузки открыть и отредактировать файл конфигурации, в котором перечисляются узлы ВМТ для балансировки:

- вывести все узлы ВМТ из балансировки;
- сохранить файл;
- перезагрузить службу балансировщика нагрузки.

Выполнить действия на всех балансировщиках нагрузки.

Шаг 2. Перевод фондов в режим техобслуживания, отключение пользователей

Для продолжения обновления нужно дождаться отключения пользователей от фондов рабочих мест.

Затем:

- через веб-интерфейс «Портал администратора» Termidesk VDI перевести **все** фонды в режим техобслуживания. Для этого перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Техобслуживание]** с выбором из выпадающего списка значения «Включить». Подтвердить включение режима;
- выключить каждый узел терминального сервера, который подключен к Termidesk VDI как поставщик ресурсов.

Шаг 3. Резервное копирование

Для резервного копирования БД нужно:

- удаленно подключиться узлу ВМТ (см. подраздел **Удаленное подключение к ВМТ**);
- выполнить резервное копирование БД (см. подраздел **Резервное копирование и восстановление БД**);
- сохранить резервную копию на внешнем носителе информации.

Шаг 4. Добавление нового узла ВМТ с СУБД

Выполняется добавление узла с существующей (не новой) версией ВМТ. Для добавления узла нужно:

- добавить ВМ для загрузки ВМТ;
- выполнить базовые настройки ВМТ ;
- выполнить установку узла в режиме установки «База данных»;
- выполнить восстановление БД.

Шаг 5. Изменение параметров подключения к БД

На существующем узле ВМТ, установленным в комплексном режиме, изменить параметры подключения к БД:

- выполнить удаленное подключение к узлу;
- отредактировать конфигурационный файл `/etc/opt/termidesk-vdi/termidesk.conf`, задав актуальные значения параметрам:
  - `DBHOST` - IP-адрес или FQDN узла с СУБД;
  - `DBPORT` - порт соединения с сервером БД, по умолчанию `5432`;
  - `DBNAME` - имя БД, по умолчанию termidesk;
  - `DBUSER` - имя пользователя для подключения к БД, по умолчанию `termidesk`;
  - `DBPASS` - пароль для подключения к БД, по умолчанию `ksedimret`;
- сохранить файл;
- перезапустить службу `termidesk-vdi`:

```
sudo systemctl restart termidesk-vdi
```

Выполнить проверку доступности веб-порталов Termidesk VDI.

Шаг 6. Добавление узла ВМТ - RabbitMQ

Для добавления узла нужно:

- добавить ВМ для загрузки ВМТ;
- выполнить базовые настройки ВМТ;
- выполнить установку узла фермы в режиме установки «Произвольная». В процессе установки выбрать «RabbitMQ».

Шаг 7. Добавление двух узлов ВМТ - «Менеджер рабочих мест»

Для добавления первого узла нужно:

- добавить ВМ для загрузки ВМТ;
- выполнить базовые настройки ВМТ;
- выполнить установку узла фермы в режиме установки «Произвольная». В процессе установки выбрать «Celeryman». Не привязывать узел к существующей ферме (будет соответствующий запрос в диалоговом окне);
- после установки выполнить экспорт ключей (см. подраздел **Экспорт параметров Termidesk VDI**).

Записи в БД, которая используется фермой Termidesk VDI, будут обновлены с добавлением первого узла ВМТ с «Менеджером рабочих мест».

Ключи, экспортированные на этом шаге, будут импортироваться для последующих добавленных узлов.

Для добавления второго узла нужно:

- добавить ВМ для загрузки ВМТ;
- выполнить базовые настройки ВМТ;
- выполнить установку узла фермы в режиме установки «Произвольная». В процессе установки выбрать «Celeryman». Привязать узел к существующей ферме (будет соответствующий запрос в диалоговом окне);
- после установки выполнить импорт ключей (см. подраздел **Импорт параметров Termidesk VDI**).

Шаг 8. Добавление узлов ВМТ - «Универсальный диспетчер»

Для добавления первого узла нужно:

- добавить ВМ для загрузки ВМТ;
- выполнить базовые настройки ВМТ;
- выполнить установку узла фермы в режиме установки «Произвольная». В процессе установки выбрать «Диспетчер» и один из предложенных типов портала. Тип портала выбирается исходя из потребностей в нем. Привязать узел к существующей ферме (будет соответствующий запрос в диалоговом окне);
- после установки выполнить импорт ключей (см. подраздел **Импорт параметров Termidesk VDI**);
- после установки проверить доступность веб-порталов Termidesk VDI через веб-браузер.

Добавление второго узла «Универсального диспетчера» выполняется аналогично.

Шаг 9. Выключение узла ВМТ предыдущей версии

Выключить узел ВМТ с комплексной установкой предыдущей версии.

Шаг 10. Изменение конфигурации балансировки

На балансировщике нагрузки открыть и отредактировать файл конфигурации, в котором перечисляются узлы ВМТ для балансировки:

- заменить адреса узлов ВМТ предыдущих версий Termidesk VDI на адреса новых узлов ВМТ;
- сохранить файл;
- перезагрузить службу балансировщика нагрузки.

Выполнить действия на всех балансировщиках нагрузки.

Выполнить проверку доступности веб-порталов Termidesk VDI через веб-браузер сначала обращением на IP-адрес каждого из «Универсальных диспетчеров» (например, на «Портал администратора»), затем обращением на IP-адрес балансировщика нагрузки.

Шаг 11. Обновление компонентов в ОС рабочих мест, новая публикация

После выполнения всех шагов:

- обновляются компоненты в ОС РМ (в базовом ВРМ - «золотом образе» или в ОС терминального сервера) в соответствии с документацией на них:
  - «Агент виртуального рабочего места»;
  - «Агент виртуальных смарт-карт»;
  - «Видеоагент»;
  - «Сессионный агент»;
  - STAL (если используется);
  - TERA (если используется);
- выполняется новая публикация в фондах РМ, если публикация применима к ним.

Для фондов с терминальными серверами публикация не выполняется: достаточно того, чтобы узел с терминальным сервером был включен.

Обновление фермы Termidesk VDI для распределенной конфигурации установки

Общая концепция обновления фермы Termidesk VDI для распределенной конфигурации установки

Описание применимо к ферме Termidesk VDI, установленной в распределенной конфигурации ВМТ. Общая последовательность действий приведена на рисунке (см. рисунок Обновление распределенной конфигурации фермы Termidesk).

Перед обновлением требуется удалить через «Портал администратора» Termidesk VDI:

- фонды и шаблоны, созданные ранее для поставщика ресурсов «Static IP Machines»;
- шаблоны РМ «Статичная ВМ» (для всех поставщиков ресурсов, ранее имевших эти шаблоны) и ассоциированные с ними фонды;
- шаблоны, созданные ранее для поставщика ресурсов VMmanager. Если

шаблоны не были удалены перед обновлением, то после него необходимо отредактировать существующие шаблоны и корректно задать значения новых параметров.

Во время обновления распределенной конфигурации установки:

- изменение политик нужно проводить после обновления всех узлов Termidesk VDI;
- изменение системных параметров нужно проводить после обновления всех узлов Termidesk VDI.

Обновление должно осуществляться с соблюдением условия: после начала процедуры обновления запрещается производить любые операции с объектами на «Порталах» с предыдущими версиями Termidesk VDI.

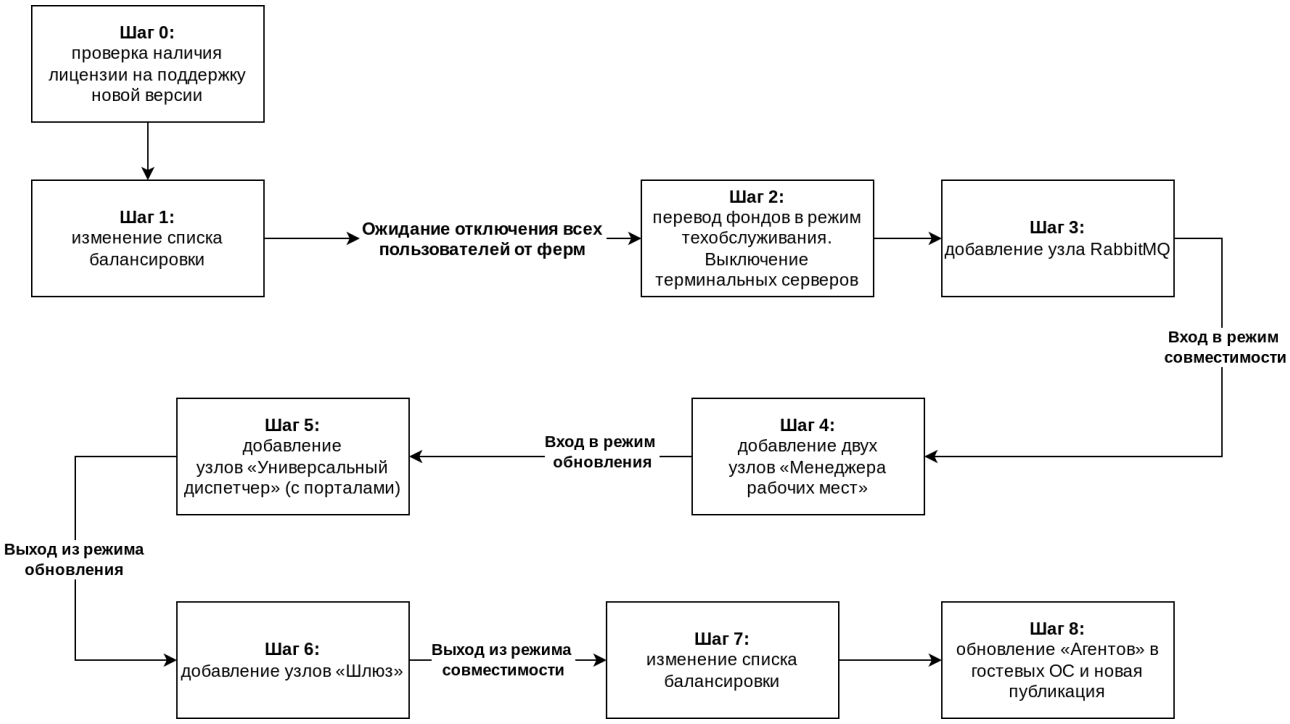


Рисунок 269. Обновление распределенной конфигурации фермы Termidesk

На схеме:

- режим совместимости - режим, характеризующийся отличием в версиях между любыми компонентами фермы Termidesk VDI;
- режим обновления - режим, характеризующийся наличием не обновленных «Универсальных диспетчеров» при уже обновленных записях БД. Становится ограничен в действиях «Портал администратора». Ферма Termidesk VDI при этом должна работать с теми записями БД, которые есть на момент входа в этот режим.

При обновлении добавляются новые узлы. Поскольку любой новый узел имеет свой IP-адрес (или FQDN), то в этом случае нужно учесть, что все компоненты «Агента» должны получить новый адрес для регистрации в Termidesk VDI. Потребуется настроить «Агенты» на взаимодействие с новым узлом «Универсального диспетчера». Например, для удобства можно использовать:

- технологию балансировки виртуальных IP-адресов;
- alias-записи в DNS совместно с циклическим перебором (DNS Round Robin).

> Обновление выполняется с приостановкой обслуживания пользователей! Требуется заранее спланировать временной промежуток приостановки обслуживания.
>
> Обновление узла ВМТ с СУБД не производится: узел остается тем же. Записи в БД будут обновлены с добавлением первого узла ВМТ с компонентом «Менеджер рабочих мест».

Последовательность обновления фермы Termidesk VDI, установленной в распределенной отказоустойчивой конфигурации:

Шаг 0. Проверить наличие лицензии на поддержку новой версии Termidesk VDI.

Шаг 1. На всех балансировщиках нагрузки, отвечающих за распределение подключений, из списка балансировки вывести узлы ВМТ.

Шаг 2. Все пользователи должны отключиться от фондов РМ. Нужно дождаться завершения работы пользователей. Затем:

- через веб-интерфейс «Портал администратора» перевести все фонды РМ в режим техобслуживания;
- выключить все терминальные серверы, которые были подключены в Termidesk VDI как поставщики ресурсов.

Шаг 3. Добавить узел ВМТ новой версии с компонентом RabbitMQ.

Шаг 4. Добавить два узла ВМТ новой версии с компонентом «Менеджер рабочих мест» («Менеджера очередей»).

Шаг 5. Добавить узлы ВМТ новой версии с компонентом «Универсальный диспетчер» с установкой порталов: «Портал администратора», «Портал пользователя» или «Портал универсальный». Тип портала выбирается исходя из потребностей в нем.

Шаг 6. Добавить узел ВМТ с компонентом «Шлюз».

Шаг 7. Изменить список балансировки, заменив адреса узлов ВМТ на новые. Проверить доступность графического интерфейса Termidesk VDI сначала обращением на IP-адрес каждого из «Универсальных диспетчеров», затем обращением на IP-адрес балансировщика нагрузки.

Шаг 8. После завершения предыдущих шагов:

- обновляются компоненты в гостевых ОС РМ (в «золотых образах»):
  - «Агент виртуального рабочего места». В настройках «Агент виртуального рабочего места» нужно указать новый адрес узла для подключения;
  - «Агент виртуальных смарт-карт»;
  - «Видеоагент»;
  - «Сессионный агент»;
  - STAL (если используется);
  - TERA (если используется);
- выполняется новая публикация в фондах РМ, если публикация применима к ним (для фондов с терминальными серверами публикация не выполняется).

Шаг 1. Редактирование конфигурации балансировщика нагрузки

На балансировщике нагрузки открыть и отредактировать файл конфигурации, в котором перечисляются узлы ВМТ для балансировки:

- вывести все узлы ВМТ из балансировки;
- сохранить файл;
- перезагрузить службу балансировщика нагрузки.

Выполнить действия на всех балансировщиках нагрузки.

Шаг 2. Перевод фондов в режим техобслуживания и отключение пользователей

Для продолжения обновления нужно дождаться отключения пользователей от фондов рабочих мест.

Затем:

- через веб-интерфейс «Портал администратора» Termidesk VDI перевести **все** фонды в режим техобслуживания. Для этого перейти «Рабочие места - Фонды» и нажать экранную кнопку **[Техобслуживание]** с выбором из выпадающего списка значения «Включить». Подтвердить включение режима;
- выключить каждый узел терминального сервера, который подключен к Termidesk VDI как поставщик ресурсов.

Шаг 3. Добавление узла ВМТ с RabbitMQ

Для добавления узла нужно:

- добавить ВМ для загрузки ВМТ;
- выполнить базовые настройки ВМТ;
- выполнить установку узла фермы в режиме установки «Произвольная». В процессе установки выбрать «RabbitMQ».

Шаг 4. Добавление двух узлов ВМТ с «Менеджером рабочих мест»

Для добавления первого узла нужно:

- добавить ВМ для загрузки ВМТ;
- выполнить базовые настройки ВМТ;
- выполнить установку узла фермы в режиме установки «Произвольная». В процессе установки выбрать «Celeryman». Не привязывать узел к существующей ферме (будет соответствующий запрос в диалоговом окне);
- после установки выполнить экспорт ключей (см. подраздел **Экспорт параметров Termidesk VDI**).

Записи в БД, которая используется фермой Termidesk VDI, будут обновлены с добавлением первого узла ВМТ с «Менеджером рабочих мест».

Ключи, экспортированные на этом шаге, будут импортироваться для последующих добавленных узлов.

Для добавления второго узла нужно:

- добавить ВМ для загрузки ВМТ;
- выполнить базовые настройки ВМТ;
- выполнить установку узла фермы в режиме установки «Произвольная». В процессе установки выбрать «Celeryman». Привязать узел к существующей ферме (будет соответствующий запрос в диалоговом окне);
- после установки выполнить импорт ключей (см. подраздел **Импорт параметров**

Termidesk VDI).

Шаг 5. Добавление узлов ВМТ с «Универсальным диспетчером»

Для добавления первого узла нужно:

- добавить ВМ для загрузки ВМТ;
- выполнить базовые настройки ВМТ;
- выполнить установку узла фермы в режиме установки «Произвольная». В процессе установки выбрать «Диспетчер» и один из предложенных типов портала. Тип портала выбирается исходя из потребностей в нем. Привязать узел к существующей ферме (будет соответствующий запрос в диалоговом окне);
- после установки выполнить импорт ключей (см. подраздел **Импорт параметров Termidesk VDI**);
- после установки проверить доступность веб-порталов Termidesk VDI через веб-браузер.

После установки первого узла «Универсального диспетчера» и обновления БД (происходит на Шаге 4) узлы предыдущей версии Termidesk VDI можно выводить из состава фермы Termidesk VDI.

Добавление последующих узлов «Универсального диспетчера» выполняется аналогично.

Шаг 6. Добавление узлов ВМТ со «Шлюзом»

Для добавления узла нужно:

- добавить ВМ для загрузки ВМТ;
- выполнить базовые настройки ВМТ;
- выполнить установку узла фермы в режиме установки «Произвольная». В процессе установки выбрать «Шлюз». Привязать узел к существующей ферме (будет соответствующий запрос в диалоговом окне);
- после установки выполнить импорт ключей (см. подраздел **Импорт параметров Termidesk VDI**).

Шаг 7. Изменение конфигурации балансировщика нагрузки

На балансировщике нагрузки открыть и отредактировать файл конфигурации, в котором перечисляются узлы ВМТ для балансировки:

- заменить адреса узлов ВМТ предыдущих версий Termidesk VDI на адреса новых узлов ВМТ;
- сохранить файл;
- перезагрузить службу балансировщика нагрузки.

Выполнить действия на всех балансировщиках нагрузки.

Выполнить проверку доступности веб-порталов Termidesk VDI через веб-браузер сначала обращением на IP-адрес каждого из «Универсальных диспетчеров» (например, на «Портал администратора»), затем обращением на IP-адрес балансировщика нагрузки.

Шаг 8. Обновление компонентов в ОС рабочих мест

После выполнения всех шагов:

- «Агент виртуального рабочего места»;

- «Агент виртуальных смарт-карт»;
- «Видеоагент»;
- «Сессионный агент»;
- STAL (если используется);
- TERA (если используется);

- выполняется новая публикация в фондах РМ, если публикация применима к ним.

Для фондов с терминальными серверами публикация не выполняется: достаточно того, чтобы узел с терминальным сервером был включен.

ВМТ. ДЕЙСТВИЯ В ГЛАВНОМ МЕНЮ

Изменение настроек сети

Для изменения настроек сети нужно в главном меню ВМТ нажать клавишу **<F2>**, ввести текущий пароль администратора (по умолчанию после установки - `admin`). Будет выполнен переход в меню расширенных настроек (см. рисунок Меню расширенных настроек VA).

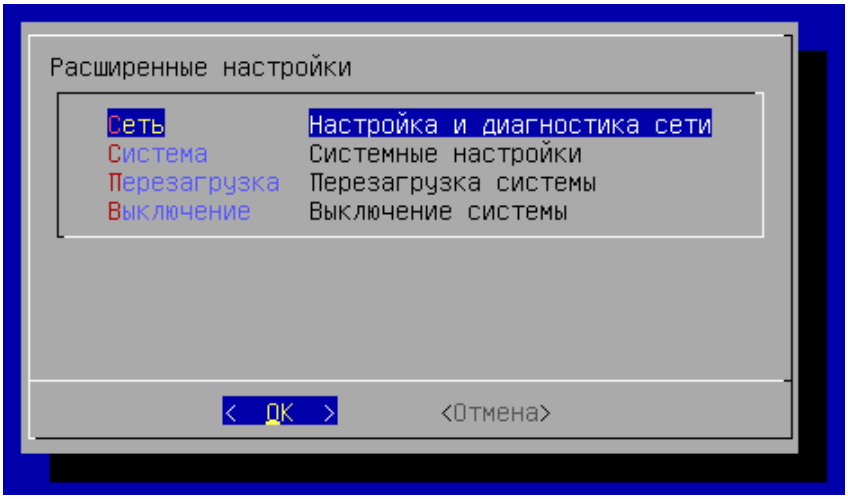


Рисунок 270. Меню расширенных настроек VA

В меню настроек выбрать пункт «Сеть», затем «Настройка» (см. рисунок Переход к конфигурации сети). Далее действия не будут отличаться от процесса первичного конфигурирования сетевых параметров.

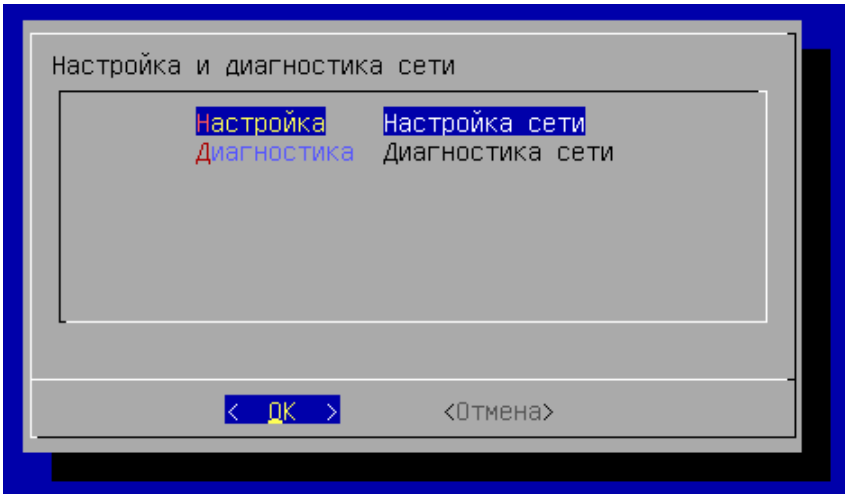


Рисунок 271. Переход к конфигурации сети

Диагностика сети

Для диагностики сети нужно перейти в меню расширенных настроек, нажав клавишу **<F2>** в главном меню ВМТ, ввести текущий пароль администратора (по умолчанию после установки - `admin`). Далее выбрать пункт «Сеть», затем «Диагностика».

Ввести имя или IP-адрес узла, подключение к которому нужно проверить (см. рисунок Окно диагностики сети). ВМТ выполнит команду `ping` до указанного узла.

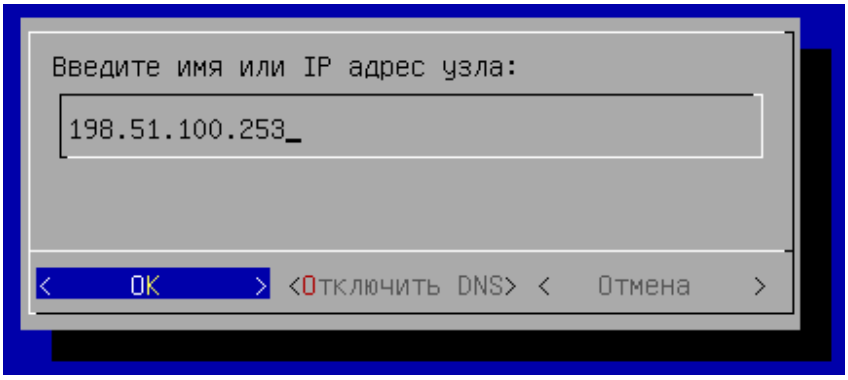


Рисунок 272. Окно диагностики сети

Результат диагностики сети будет показан в окне (см. рисунок Результат диагностики сети).

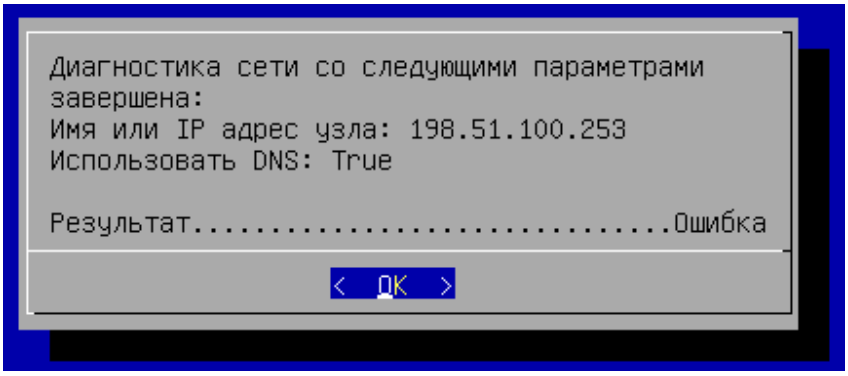


Рисунок 273. Результат диагностики сети

Изменение имени узла ВМТ

Для изменения имени узла нужно в главном меню ВМТ нажать клавишу **<F2>**, ввести текущий пароль администратора (по умолчанию после установки - `admin`). Далее выбрать пункт «Система», затем «Имя хоста».

В появившемся окне (см. рисунок Редактирование имени узла ВМТ) задать новое имя узла ВМТ и нажать экранную кнопку **[OK]**, дождаться применения изменений. Новое имя узла будет отображено в главном меню ВМТ.

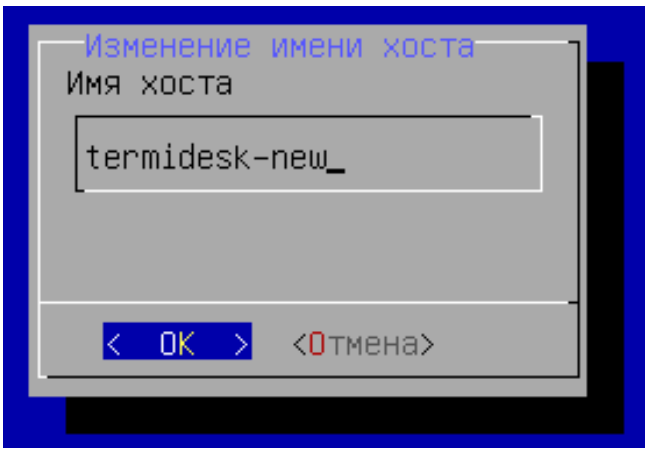


Рисунок 274. Редактирование имени узла ВМТ

Смена пароля администратора ВМТ

После установки ВМТ по умолчанию используется логин `admin` с паролем `admin` для доступа к веб-интерфейсу Termidesk VDI и ряду функций управления.

Для смены пароля нужно:

- в главном меню ВМТ нажать клавишу **<F2>**, ввести текущий пароль администратора (по умолчанию после установки - `admin`);
- далее выбрать пункт «Система», затем «Пароль»;
- в появившемся окне (см. рисунок Ввод текущего пароля администратора) ввести текущий пароль (после установки пароль по умолчанию - `admin`) и нажать экранную кнопку **[OK]**;
- затем ввести новый пароль (см. рисунок Ввод нового пароля администратора), переключиться на строку «Повтор пароля» при помощи клавиши **<↓>** (**<СТРЕЛКА ВНИЗ>**) и повторить ввод пароля. Подтвердить данные, нажав экранную кнопку **[OK]**.

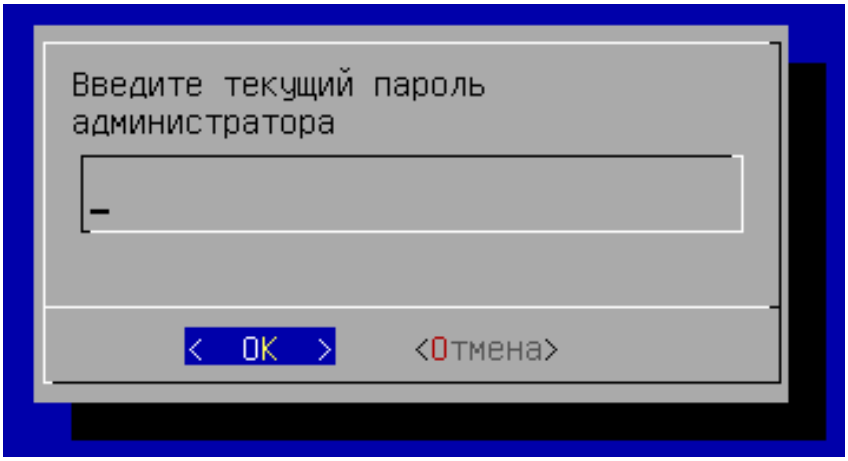


Рисунок 275. Ввод текущего пароля администратора

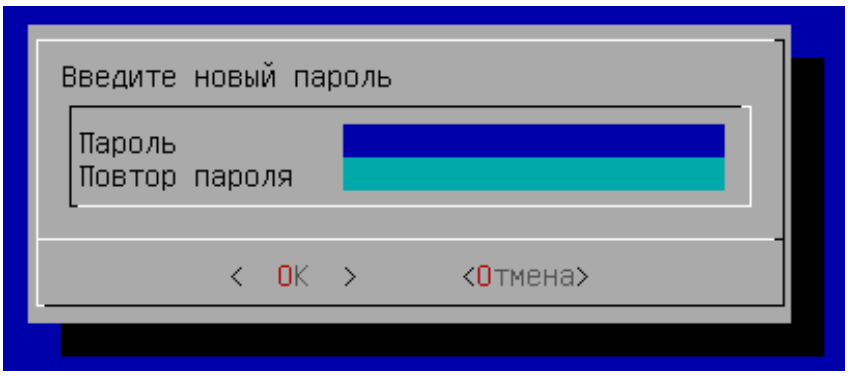


Рисунок 276. Ввод нового пароля администратора

Синхронизация параметров между ВМТ

Экспорт параметров Termidesk VDI

Параметры DJANGO_SECRET_KEY и HEALTH_CHECK_ACCESS_KEY используются в Termidesk VDI для проверок пересылаемых между компонентами данных и состояния API. При распределенной установке эти параметры должны быть одинаковыми на всех узлах ВМТ.

Для передачи конфигураций и параметров ВМТ использует механизм ETCD и сетевые порты 2379, 2380 (протоколы TCP/UDP).

Синхронизация указанных параметров не подразумевает синхронизацию учетных данных для подключения RabbitMQ.

Список параметров Termidesk VDI, синхронизируемых через экспорт и импорт:

- DJANGO_SECRET_KEY;
- HEALTH_CHECK_ACCESS_KEY;
- файлы ключей из каталога /etc/opt/termidesk-vdi/wsproxy;
- CRYPTO_RSA_KEY (файл ключа из каталога /etc/opt/termidesk-vdi/);
- файл /var/lib/rabbitmq/.erlang.cookie.

Для экспорта параметров с ноды ВМТ нужно:

- в главном меню ВМТ нажать клавишу **<F2>**, ввести текущий пароль администратора (по умолчанию после установки - admin);
- далее выбрать пункт «Система», затем «Синхронизация»;
- в появившемся окне выбрать «Экспорт ключей» (см. рисунок Переход к экспорту ключей);

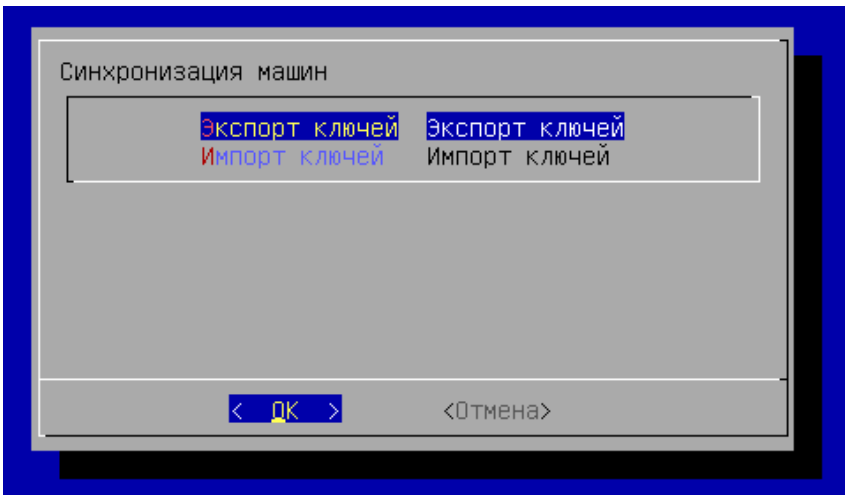


Рисунок 277. Переход к экспорту ключей

- задать секретное слово, которое будет использоваться при импорте ключей на другую ноду ВМТ (см. рисунок Создание секретного слова);

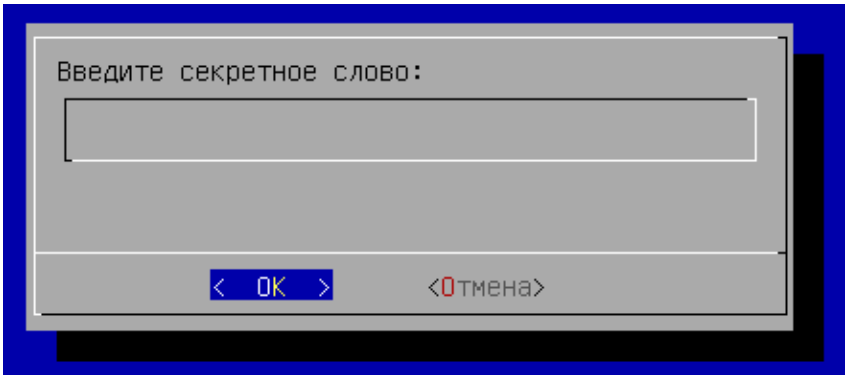


Рисунок 278. Создание секретного слова

- запомнить сгенерированный временный пароль для синхронизации (см. рисунок Параметры для синхронизации между нодами), который будет использоваться при импорте ключей на другую ноду ВМТ.

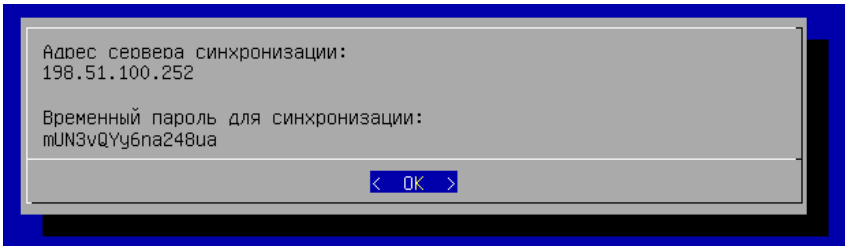


Рисунок 279. Параметры для синхронизации между нодами

Импорт параметров Termidesk VDI

Для импорта параметров на ноду ВМТ нужно:

- в главном меню ВМТ нажать клавишу **<F2>**, ввести текущий пароль администратора (по умолчанию после установки - `admin`);
- далее выбрать пункт «Система», затем «Синхронизация»;
- в появившемся окне выбрать «Импорт ключей» (см. рисунок Переход к импорту ключей);

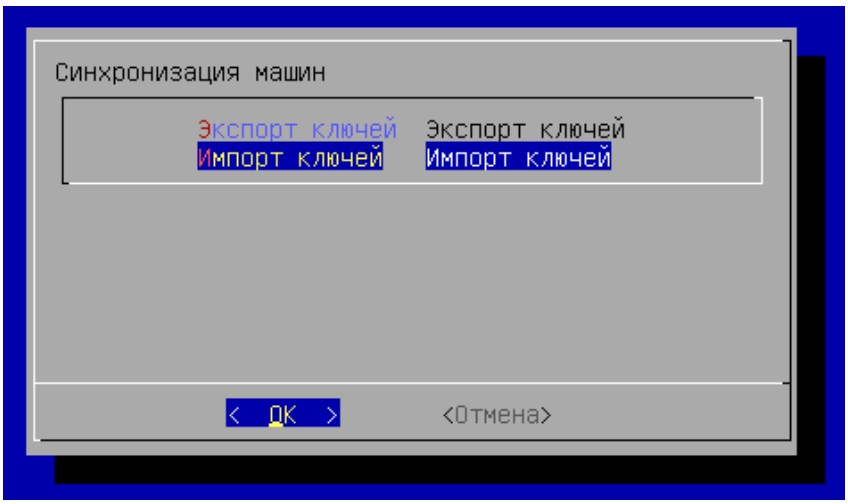


Рисунок 280. Переход к импорту ключей

- ввести параметры синхронизации, полученные при экспорте ключей с другой ноды (см. рисунок Ввод параметров синхронизации). Нажать экранную кнопку **[OK]** и дождаться сообщения об успешном применении конфигурации.

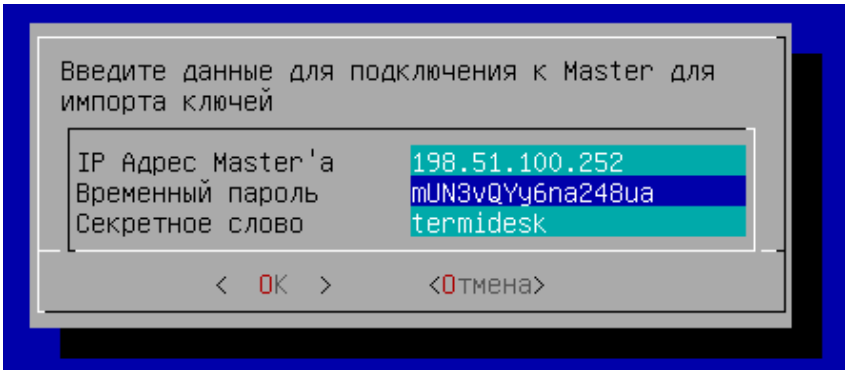


Рисунок 281. Ввод параметров синхронизации

ВМТ. НАСТРОЙКИ

Резервное копирование и восстановление БД для ВМТ

Резервное копирование БД

Резервное копирование БД, созданной СУБД PostgreSQL можно выполнить утилитой `pg_dump`:

```
pg_dump -d <наименование_БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь> -W
--format=t > <имя_файла_для_сохранения_БД.tar>
```

Где:

`-d <наименование_БД>` - имя БД. При стандартных настройках используется имя `termidesk`;

`-h <IP-адрес_хоста>` - IP-адрес узла, где расположена БД. Если БД устанавливалась локально, нужно указать `localhost`;

`-p <порт>` - порт для подключения к БД. При стандартных настройках используется `5432`;

-U <пользователь> - имя пользователя для подключения. При стандартных настройках используется имя termideskdb;

-W - запрос пароля для подключения к БД. При стандартных настройках при появлении запроса нужно указать ksedimret;

--format=t - ключ для экспорта БД в формате tar;

<имя_файла_для_сохранения_БД.tar> - имя и формат файла (tar) для сохранения БД;

Если указанная команда не помогла, то сделать резервную копию вторым способом:

- на узле с СУБД PostgreSQL переключиться на пользователя postgres:

```
sudo su postgres
```

- выполнить резервное копирование БД:

```
pg_dump -d <наименование_БД> > <имя_файла_для_сохранения_БД.sql>
```

где:

-d <наименование_БД> - имя БД. При стандартных настройках используется имя termidesk;

<имя_файла_для_сохранения_БД.sql> - имя и формат файла (sql) для сохранения БД.

Восстановление БД из резервной копии

Восстановление БД из резервной копии выполняется командой:

```
pg_restore -d <наименование БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь> -W
--format=t <файл_копии_БД.tar>
```

где:

-d <наименование БД> - имя БД. При стандартных настройках используется имя termidesk;

-h <IP-адрес_хоста> - IP-адрес узла, где расположена БД. Если используется локальная БД, нужно указать localhost;

-p <порт> - порт для подключения к БД. При стандартных настройках используется 5432;

-U <пользователь> - имя пользователя для подключения. При стандартных настройках используется имя termideskdb;

-W - запрос пароля для подключения к БД. При стандартных настройках при появлении запроса нужно указать ksedimret;

--format=t <файл_копии_БД.tar> - ключ для восстановления БД из резервной копии в формате tar.

Если резервная копия сохранена в файле формата .sql, нужно:

- переключиться на пользователя `postgres`:

```
sudo su postgres
```

- восстановить БД из резервной копии:

```
psql -d <наименование_БД> -f <имя_файла_для_сохранения_БД.sql>
```

Удаленное подключение к ВМТ

Для расширенной настройки ВМТ может использоваться удаленное подключение по протоколу SSH к ВМ, на которой он предварительно установлен.

По умолчанию удаленное подключение по протоколу SSH включено. Для управления режимом включения и отключения SSH нужно:

- в главном меню ВМТ нажать клавишу **<F2>**, ввести текущий пароль администратора (по умолчанию после установки - `admin`);
- далее выбрать пункт «Сеть», затем «SSH»;
- выбрать нужный вариант: «on» (включение) или «off» (выключение) и нажать экранную кнопку **[OK]**. После выбора режима настройки применятся автоматически и сразу.

Данные по умолчанию для подключения:

- логин: `admin`;
- пароль: `admin`. В случае, если пароль был изменен через меню ВМТ, то при подключении нужно использовать измененный пароль.

Сертификат, используемый для удаленного подключения, генерируется при первом запуске ВМТ. Таким образом для каждого экземпляра ВМТ будет использоваться индивидуальный сертификат.

ВМТ. ВЕБ-ИНТЕРФЕЙС

Обзор доступных функций веб-интерфейса ВМТ

Доступ к веб-интерфейсу управления ВМТ осуществляется из веб-браузера по протоколу HTTPS с указанием URL-адреса подключения: https://<IP-адрес_ВМТ>:8443/.

При трех подряд неудачных попытках авторизации доступ к веб-интерфейсу блокируется на 60 секунд.

Веб-интерфейс ВМТ позволяет администратору выполнить ряд задач по настройке и управлению ВМТ, а именно:

- проверить состояние служб ВМТ и выполнить их останов, запуск и перезапуск;
- сформировать и выгрузить журналы работы ВМТ;
- заменить используемые сертификаты.

Сразу после аутентификации администратору доступна панель, содержащая список основных функций:

- «Обзор» - предоставляет информацию об основных параметрах, характеризующих ВМТ (см. рисунок Отображение функции «Обзор»), таких, как:
  - версия установленной ОС;
  - время доступности ВМТ, информация об активных пользователях системы (доступна при нажатии ссылки «<количество> users» в блоке «Время доступности системы»), полученная утилитой `w`;
  - назначенные IP-адреса;
  - версия Termidesk VDI;
  - список установленных ролей;
  - графики использования процессора («CPU Usage») и памяти («Memory Usage»).
- «Службы» - предоставляет информацию о состоянии служб ВМТ, позволяет управлять ими;
- «Сертификат» - предоставляет информацию об установленном сертификате, а также позволяет заменить его на другой;
- «Дата и время» - позволяет выполнить настройку даты и времени, добавить информацию о NTP-серверах;
- «Журналы» - позволяет сформировать общий архив с файлами журналов ВМТ и выгрузить его.

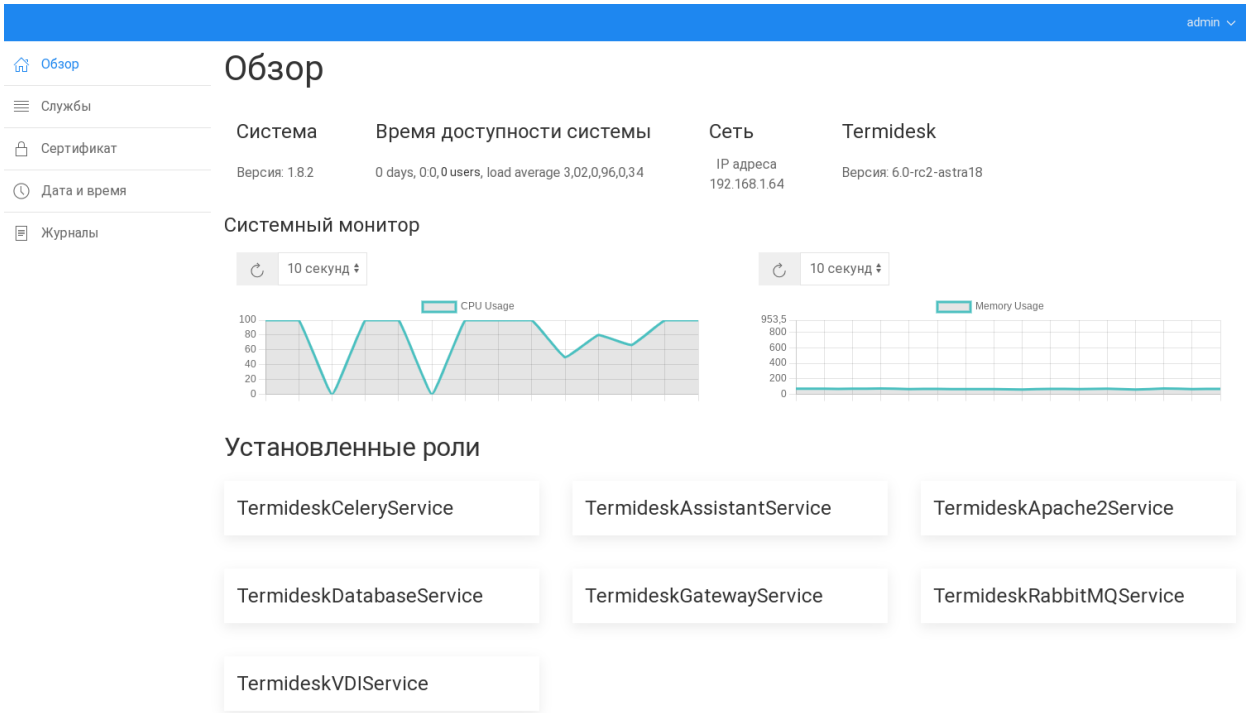


Рисунок 282. Отображение функции «Обзор»

Управление состоянием служб ВМТ

Для просмотра состояния служб, критичных для ВМТ, необходимо перейти в функцию «Службы» веб-интерфейса ВМТ.

Список служб, отображаемый на странице, зависит от перечня ролей (или роли), выбранных при первичной настройке ВМТ. Список может быть отсортирован по столбцам «Служба», «Загружено», «Состояние», «Подробности».

Для управления состоянием службы нужно выбрать строку с наименованием службы (за раз можно выбрать только одну) и воспользоваться экранными кнопками **[Запустить]**, **[Остановить]** или **[Перезапустить]**, в зависимости от действия, которое нужно

произвести над службой.

Список обновится после того, как выбранная ранее служба изменила свое состояние после выполненного действия, не ожидая обновления по таймеру (по умолчанию 10 секунд). Для принудительного обновления статусов можно воспользоваться экранной кнопкой, приведенной на рисунке (см. рисунок Отображение функции «Службы»).

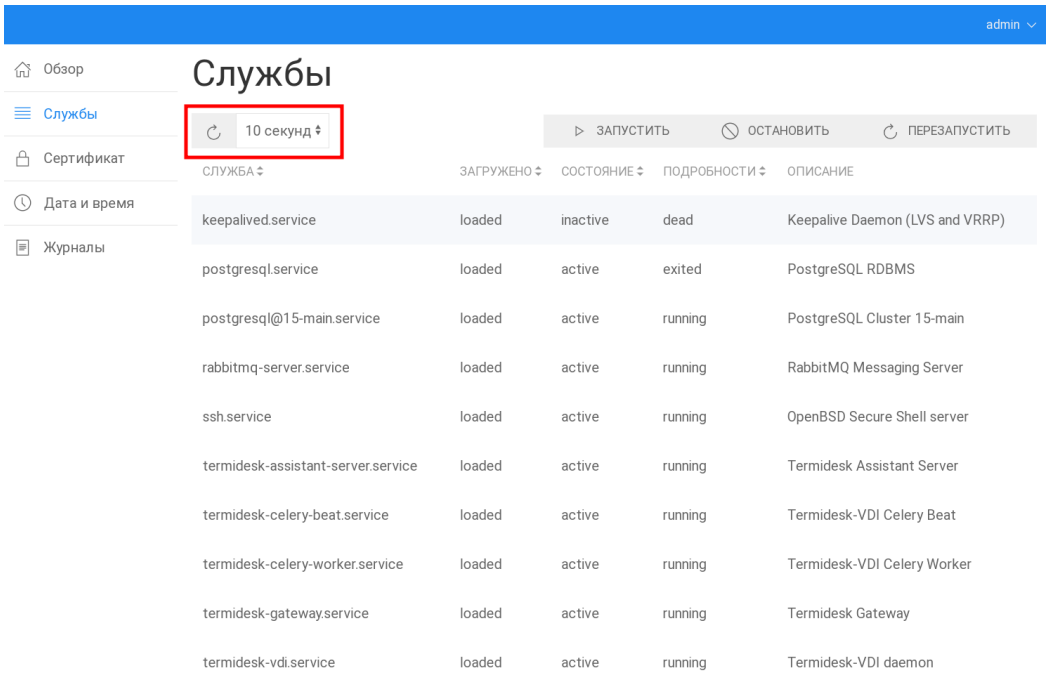


Рисунок 283. Отображение функции «Службы»

Формирование и выгрузка журнала ВМТ

Для формирования архива с файлами журналов и конфигурации нужно перейти в функцию «Журналы» веб-интерфейса ВМТ и нажать экранную кнопку,отмеченную на рисунке (см. рисунок Отображение функции «Журналы»).

Будет сформирован архив формата `.tar.gz` с именем `TDVAlogs_<временная_метка>.tar.gz`, в который будут помещены файлы из каталогов `/var/log/` и конфигурационные файлы `/etc/opt/termidesk-vdi/termidesk.conf`, `/etc/rabbitmq/defifnitions.json`, `/etc/keepalived/keepalived.conf`.

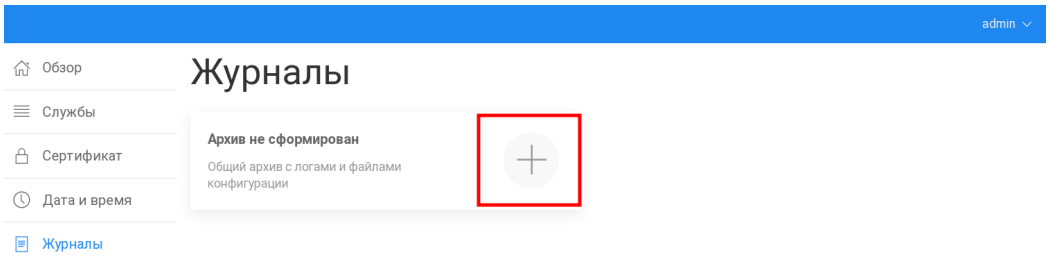


Рисунок 284. Отображение функции «Журналы»

По завершении формирования архива станут доступны следующие действия (см. рисунок Доступные действия с архивом):

- скачать сформированный архив;
- обновить архив. Новый архив перезапишет предыдущий без подтверждения. До окончания формирования нового архива предыдущий не удалится;

- удалить архив. После применения этого действия архив будет удален, строка с его наименованием и размером исчезнет.

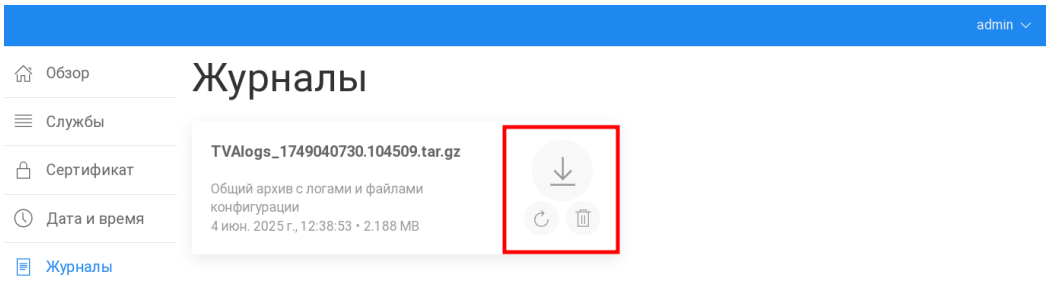


Рисунок 285. Доступные действия с архивом

Просмотр и замена сертификата через веб-интерфейс ВМТ

Для доступа к веб-интерфейсу Termidesk VDI по протоколу HTTPS, а также для других подключений, требующих защищенного соединения, на этапе первичной настройки сгенерировался самоподписанный сертификат.

Для просмотра текущего сертификата, установленного в ВМТ, нужно перейти в функцию «Сертификат» веб-интерфейса ВМТ, затем нажать экранную кнопку **[Подробнее]**. В отдельном окне будет отображено подробное описание созданного или загруженного на ВМТ сертификата (см. рисунок Отображение подробного описания сертификата).

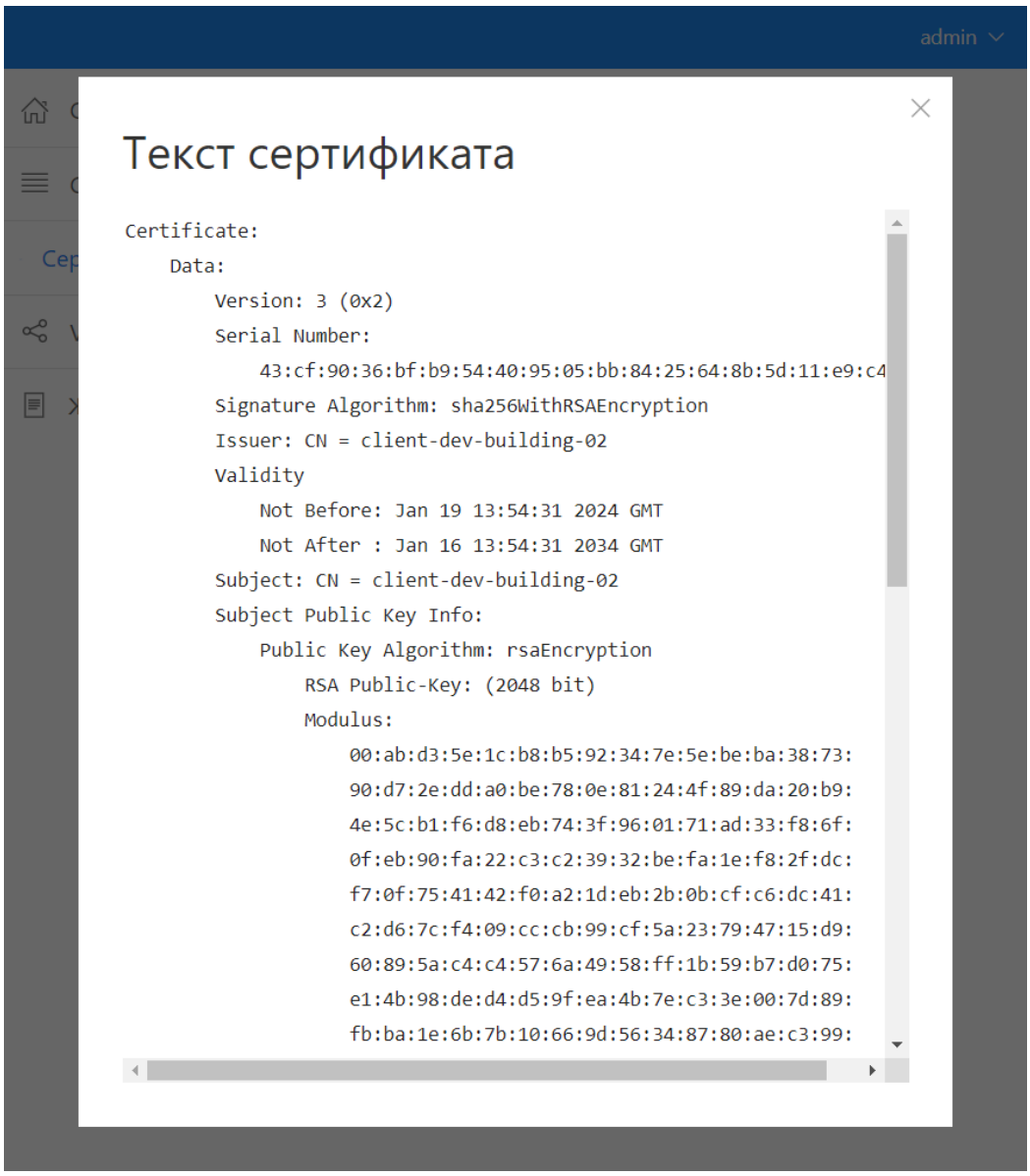


Рисунок 286. Отображение подробного описания сертификата

Для замены текущего сертификата на новый нужно:

- в функции «Сертификат» нажать экранную кнопку **[Изменить]**;
- в открывшейся форме (см. рисунок Замена сертификата через веб-интерфейс ВМТ) выбрать:
  - файл нового сертификата. Поддерживаются форматы: `.pfx`, `.pem`, `.crt`, `.cer`;
  - файл закрытого ключа. Поддерживаются форматы: `.pem`, `.key`;
  - файл проверки цепочки сертификатов (необязательно). Поддерживаются форматы: `.pfx`, `.pem`, `.crt`, `.cer`.

> В случае, если выбранный файл защищен паролем, то при попытке его загрузить в веб-браузере появится всплывающее окно ввода пароля. Необходимо ввести пароль и нажать экранную кнопку **[OK]**.

- после загрузки файлов параметры нового сертификата отобразятся рядом с параметрами текущего сертификата. Для отображения полного описания сертификата нужно нажать экранную кнопку **[Подробнее]**. Для применения изменений нужно нажать экранную кнопку **[Применить]**.

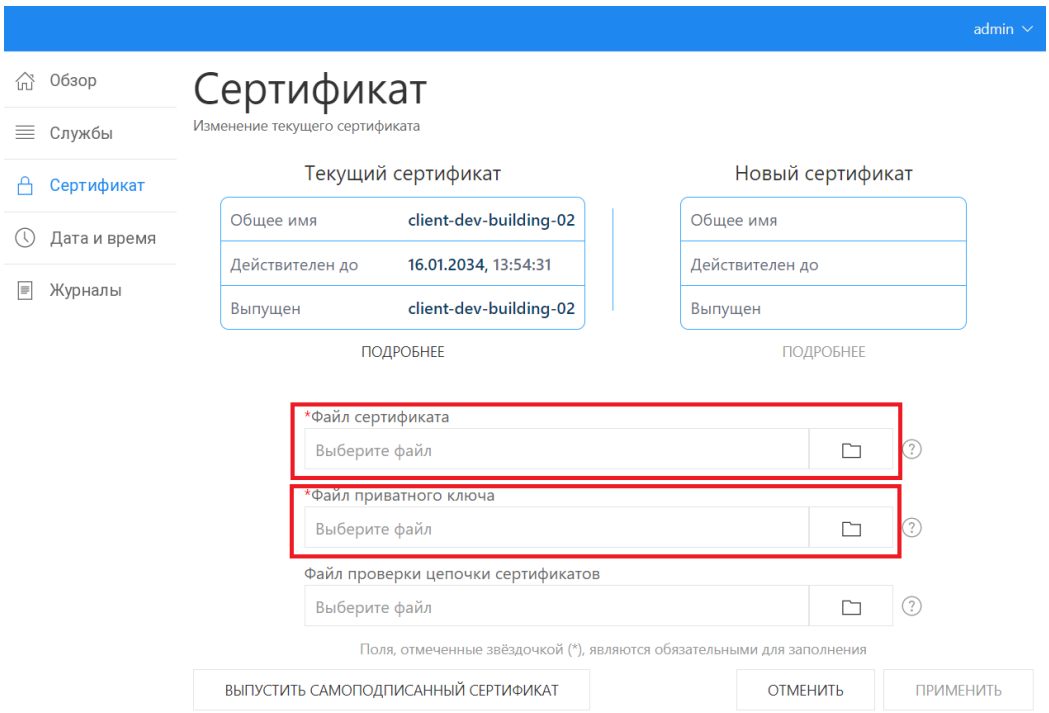


Рисунок 287. Замена сертификата через веб-интерфейс ВМТ

Для замены текущего сертификата на новый самоподписанный нужно:

- в функции «Сертификат» нажать экранную кнопку **[Изменить]**;
- в открывшейся форме нажать экранную кнопку **[Выпустить самоподписанный сертификат]**;
- задать общее имя (Common Name, CN) и дату, до которой будет действителен сертификат (см. рисунок Выпуск самоподписанного сертификата);

Новое общее имя (CN) должно отличаться от предыдущего.

- нажать экранную кнопку **[Сгенерировать]**;
- закрыть окно выпуска и нажать экранную кнопку **[Применить]**.

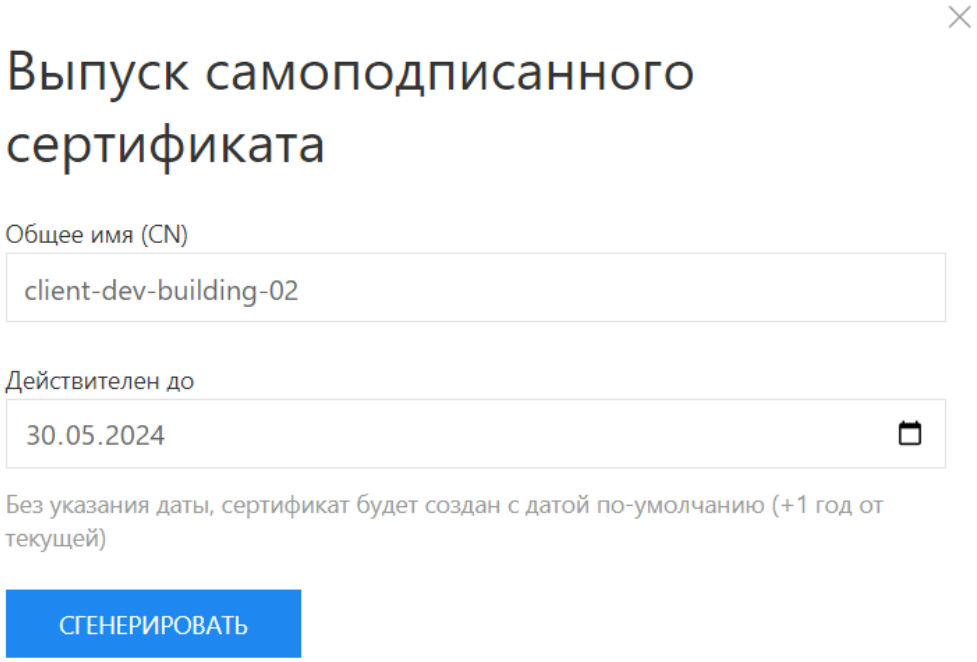


Рисунок 288. Выпуск самоподписанного сертификата

Новый сертификат отобразится в функции «Сертификат» после обновления страницы.

Управление датой и временем на ВМТ

Для просмотра текущего времени и даты следует перейти в функцию «Дата и время» веб-интерфейса ВМТ.

Для более подробного просмотра установленных значений даты и времени нужно воспользоваться экранной кнопкой **[Подробный просмотр]**, которая отобразит вывод команды `timedatectl`.

Для изменения даты и времени:

- нажать экранную кнопку **[Изменить]** в функции «Дата и время» веб-интерфейса ВМТ;
- на открывшейся странице вновь нажать экранную кнопку **[Изменить]** для поля «Текущее время» (см. рисунок Изменение даты и времени узла ВМТ);
- задать нужные значения и нажать экранную кнопку **[Выбрать]** (см. рисунок Выбор новых значений даты и времени);
- нажать экранную кнопку **[Применить]**.

Для сброса значений используется экранная кнопка **[Очистить]**, восстанавливающая значения, которые были актуальны в момент перехода на страницу, если не была активирована экранная кнопка **[Применить]**.

После активации экранной кнопки **[Применить]** сброс значений не действует.

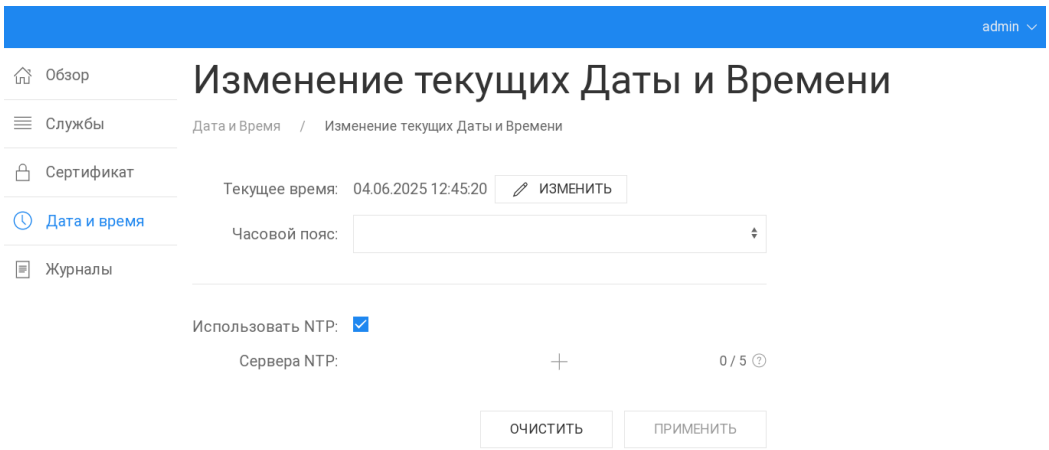


Рисунок 289. Изменение даты и времени узла ВМТ

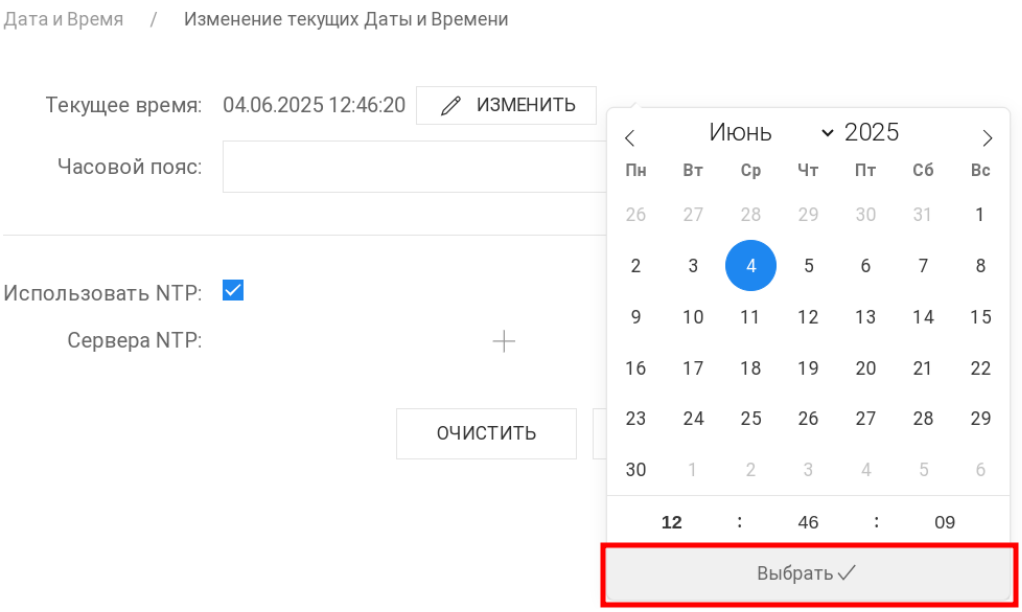


Рисунок 290. Выбор новых значений даты и времени

ВМТ поддерживает задание NTP-сервера для автоматического получения даты и времени, для этого нужно:

- нажать экранную кнопку **[Изменить]** в функции «Дата и время» веб-интерфейса ВМТ;
- воспользоваться экранной кнопкой **[+]** (см. рисунок Добавление NTP-сервера) и ввести IP-адрес или FQDN сервера. Поддерживается добавление до пяти (включительно) NTP-серверов. Если сервер недоступен, будет выведено соответствующее на сообщение (см. рисунок Сообщение о недоступности NTP-сервера);
- нажать экранную кнопку **[Применить]**.

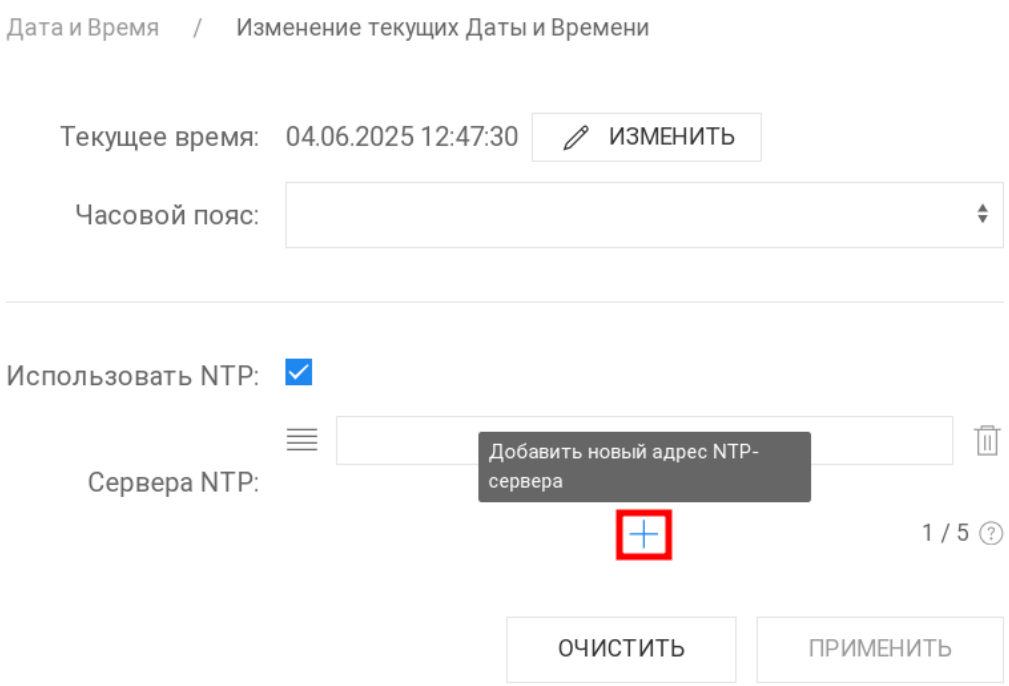


Рисунок 291. Добавление NTP-сервера

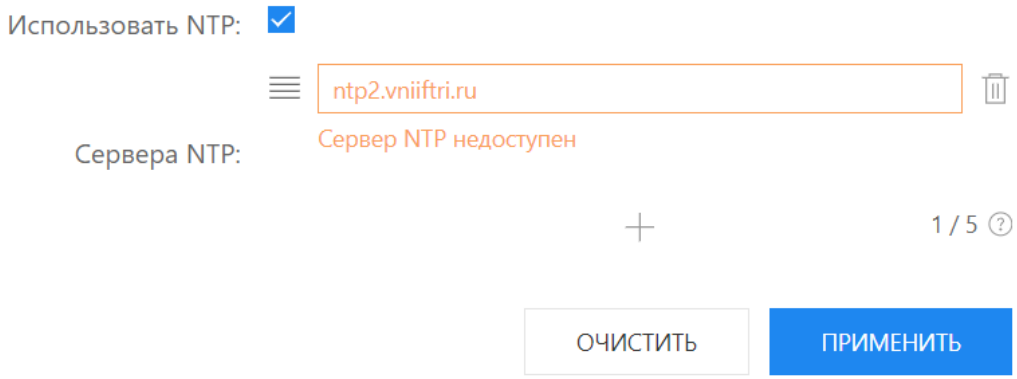


Рисунок 292. Сообщение о недоступности NTP-сервера

ВМТ. ЗАВЕРШЕНИЕ РАБОТЫ

Для завершения работы ВМТ и выключения ВМ следует:

- перейти в меню расширенных настроек, нажав клавишу **<F2>** в главном меню ВМТ;
- выбрать пункт «Выключение»;
- подтвердить действие, нажав экранную кнопку **[Да]** (см. рисунок Подтверждение выключения ВМТ).

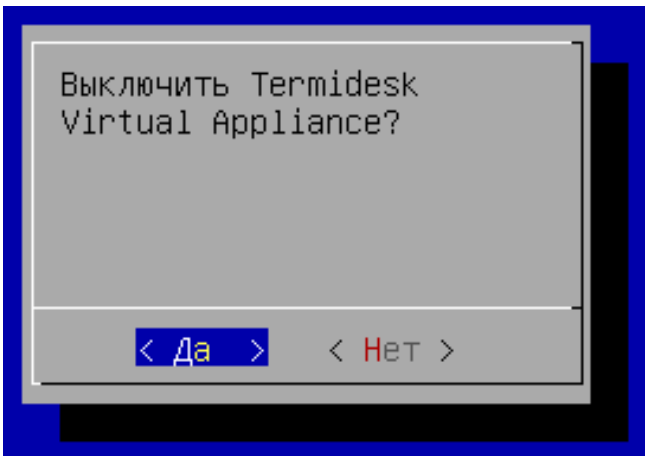


Рисунок 293. Подтверждение выключения ВМТ

ТЕРМИНЫ

Агрегатор администратора

Веб-интерфейс управления порталом «Агрегатор»

Агрегатор пользователя

Веб-интерфейс пользователя для получения ресурсов, предоставляемых порталом «Агрегатор»

Виртуальное рабочее место

Развернутая на ВМ ОС с установленным «Агентом виртуального рабочего места» и необходимым прикладным ПО. Подключение к ВРМ происходит при помощи протоколов удаленного доступа

Рабочее место

Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа. Под РМ подразумеваются как ВРМ, так и терминальный доступ или доступ к опубликованным на сервере терминалов приложениям

Гостевая ОС

ОС, функционирующая на ВМ

Компонент «Менеджер рабочих мест»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за взаимодействие с поставщиком ресурсов и управления жизненным циклом РМ, включая создание, настройку, запуск, отключение и удаление. Является обработчиком фоновых задач. Устанавливается из пакета `termidesk-vdi`. Наименование служб после установки: `termidesk-celery-beat.service` и `termidesk-celery-worker.service`

Поставщик ресурсов

ОС, платформа виртуализации или терминальный сервер, предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов РМ

Протокол доставки

Поддерживаемый в Termidesk VDI протокол удаленного доступа к РМ

Компонент «Универсальный диспетчер»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им РМ и контроля доставки РМ. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки:

`termidesk-vdi.service`

Компонент «Шлюз»

Самостоятельный компонент, отвечающий за туннелирование протоколов доставки, использующих транспортный протокол TCP. Устанавливается из пакета `termidesk-gateway`. Наименование службы после установки: `termidesk-gateway.service`

Портал «Агрегатор»

Роль компонента «Универсальный диспетчер», доступная при установке Termidesk VDI. Является единой точкой входа для получения ресурсов пользователями, предоставляет им объединенный список приложений и РМ с ферм Termidesk

Портал администратора

Предоставляет веб-интерфейс для управления Termidesk VDI и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API

Портал пользователя

Предоставляет пользовательский веб-интерфейс Termidesk VDI (без доступа к функциям управления) и интерфейс Swagger для доступа к ограниченному списку модулей документации по командам REST API

Портал универсальный

Предоставляет функции обоих вариантов порталов, как пользовательского, так и административного

Ключ

Последовательность псевдослучайных чисел, сгенерированная особым образом

Сертификат

Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу

Ферма

Логическое объединение узлов, взаимодействующих с одной БД

СОКРАЩЕНИЯ

БД	База данных
ВМ	Виртуальная машина
ВМТ	Виртуальный модуль Termidesk
ВРМ	Виртуальное рабочее место
ОС	Операционная система
ПО	Программное обеспечение
РМ	Рабочее место
СУБД	Система управления базами данных
API	Application Programming Interface (интерфейс прикладного программирования)
CN	Common Name (общее имя)
CPU	Central Processing Unit (центральный процессор)

DHCP Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста)

DNS Domain Name System (система доменных имен)

FQDN Fully Qualified Domain Name (полностью определенное имя домена)

GRUB GRand Unified Bootloader (загрузчик ОС)

HTTP HyperText Transfer Protocol (протокол передачи гипертекста)

HTTPS Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)

IP Internet Protocol (межсетевой протокол)

KVM Kernel-based Virtual Machine (программное решение, обеспечивающее виртуализацию в среде Linux на платформе, которая поддерживает аппаратную виртуализацию на базе Intel VT (Virtualization Technology) либо AMD SVM (SecureVirtual Machine))

NTP Network Time Protocol (протокол сетевого времени)

OVA Open Virtual Appliance (открытое виртуальное устройство)

OVF Open Virtualization Format (формат открытой виртуализации)

QEMU Quick Emulator (средства эмуляции аппаратного обеспечения)

REST Representational State Transfer (программная архитектура, определяющая условия работы API)

SSH Secure Shell Protocol (протокол защищенной передачи информации)

SSL Secure Sockets Layer (криптографический протокол)

TCP Transmission Control Protocol (протокол управления передачей)

UUID Unique User Identifier (уникальный идентификатор пользователя)

VDI Virtual Desktop Infarsticture (инфраструктура виртуальных рабочих столов)

VRRP Virtual Redundancy Routing Protocol (сетевой протокол виртуального резервирования маршрутизаторов, предназначенный для увеличения доступности)

СЛЕТ.10001-01 91 04. ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ. КОМПОНЕНТ TERMIDESK LIVE

ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ

Назначение документа

Настоящий документ является инструкцией по использованию компонента Termidesk Live программного комплекса «Диспетчер подключений виртуальных рабочих мест Термидеск» (далее - Termidesk VDI, Termidesk VDI). Документ предназначен для администраторов системы.

В документе приведено назначение, настройка и использование Termidesk Live. Для того чтобы получить информацию по доступным действиям в компоненте «Клиент», входящем в Termidesk Live, необходимо обратиться к документу СЛЕТ.10001-01 92 01 «Руководство пользователя. Установка и эксплуатация компонента «Клиент».

Типографские соглашения

Приняты следующие типографские соглашения:

- `моноширинный шрифт` – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk VDI, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

TERMIDESK LIVE. ОБЩИЕ СВЕДЕНИЯ

Компонент Termidesk Live переведён в режим ограниченной поддержки: обновления не выпускаются. Совместимость гарантируется с Termidesk VDI версии не выше 5.0.

Назначение компонента Termidesk Live

Компонент Termidesk Live (далее - Termidesk Live) представляет собой загрузочный образ операционной системы (ОС) с предустановленным компонентом «Клиент» (далее - Клиент) из состава программного комплекса «Диспетчер подключений виртуальных рабочих мест Termidesk» (далее - Termidesk VDI, Termidesk VDI).

Termidesk Live предназначен для работы сразу после загрузки, не требует установки на жесткий диск и поддерживает два режима:

- загрузка с подготовленного USB-носителя;
- загрузка по сети, с использованием технологии PXE-загрузки.

Termidesk Live распространяется в форматах:

- iso-образ, использующийся для загрузки с подготовленного USB-накопителя;
- каталог initrd (с файлами initrd, vmlinuz), использующийся для PXE-загрузки по сети.

Требования к аппаратному обеспечению

Минимальные аппаратные требования должны соответствовать следующим:

- для версии 5.6 с 32-битной архитектурой:
  - оперативная память, не менее 640 МБ;
  - процессор, частота не менее 512 МГц;
- для версии 6.2 с 64-битной архитектурой:
  - оперативная память, не менее 1024 МБ;
  - процессор, частота не менее 1 ГГц.

TERMIDESK LIVE. ПОЛУЧЕНИЕ ОБРАЗОВ

Образ Termidesk Live размещен в Интернет-репозитории Termidesk VDI: https://repos.termidesk.ru/Addons/Live/.

Доступны следующие версии Termidesk Live:

- версия 5.6 для 32-битной архитектуры содержит образ, используемый для физических машин (tonk-1200);
- версия 6.2 для 64-битной архитектуры содержит образ, используемый для физических машин (tonk-1200). Поддерживается загрузка спецификации UEFI.

TERMIDESK LIVE. ПОДГОТОВКА К РАБОТЕ

Подготовка к загрузке с USB-носителя

Подготовка к загрузке с USB-носителя в ОС Astra Linux Special Edition

Для подготовки загрузочного USB-носителя рекомендуется использовать встроенную в ОС утилиту fly-admin-iso («Запись ISO образа на USB носитель»).

После запуска утилиты (см. рисунок Последовательность шагов при работе с утилитой fly-admin-iso):

> USB-носитель будет отформатирован, убедитесь, что на нем нет важных данных. Не прерывайте монтирование образа на USB-накопитель, так как возможен его выход из строя.

1. Указать USB-носитель, на который будет записан образ, выбрав пункт «Записать на:».
2. Указать загруженный ранее образ thinstation.iso, выбрав пункт «Образ ISO».
3. Начать запись образа, выбрав пункт «Запись».

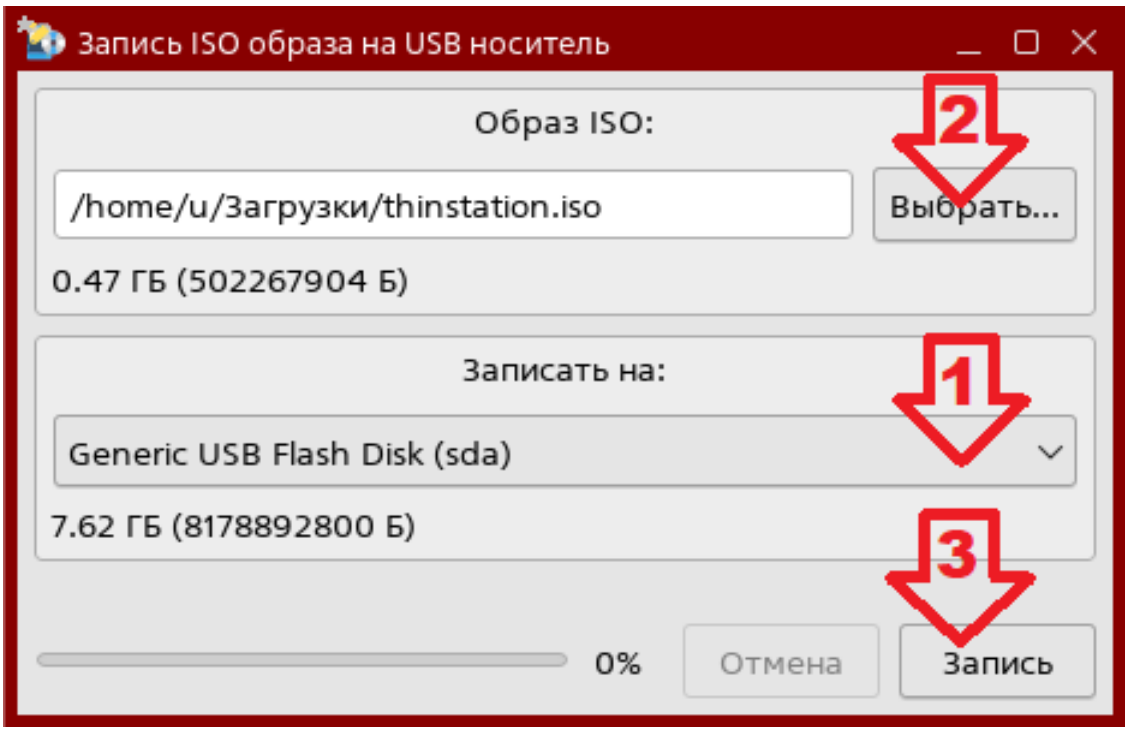


Рисунок 294. Последовательность шагов при работе с утилитой `fly-admin-iso`

Подготовка к загрузке с USB-носителя в других ОС Linux

Для подготовки загрузочного USB-носителя в ОС Linux может использоваться поставляемый с образом Termidesk Live исполняемый файл `iso2usb.sh`. Этот способ подойдет только для записи образа версии 6.2 для 64-битной архитектуры.

Для записи образа на USB-носитель:

- разархивировать полученный `thinstation.iso` в предпочитаемый каталог для получения доступа к файлу `iso2usb.sh`;
- задать файлу `iso2usb.sh` флаг для запуска:

```
sudo chmod +x <путь_к_iso2usb.sh>
```

- узнать путь к USB-носителю, выполнив команду вывода списка дисков:

```
sudo fdisk -l
```

- выполнить запись `iso`-образа на USB-носитель командой:

```
sudo <путь_к_iso2usb.sh> /dev/sdX <путь_к_thinstation.iso>
```

где:

`/dev/sdX` - путь к USB-носителю, полученный через команду `fdisk`;

- дождаться завершения записи.

Подготовка к загрузке с USB-носителя в ОС Microsoft Windows

Подготовка загрузочного USB-носителя может выполняться через утилиты `etcher` или `rufus`. Рекомендуется использовать утилиту `rufus`, поставляемую в образе `thinstation.iso`.

Для подготовки загрузочного USB-носителя через утилиту `etcher` нужно (см. рисунок Последовательность шагов при работе с etcher):

> USB-носитель будет отформатирован, убедитесь, что на нем нет важных данных. Не прерывайте монтирование образа на USB-накопитель, так как возможен его выход из строя.

1. Указать загруженный ранее образ `thinstation.iso`, выбрав пункт «Flash from file».
2. Указать USB-носитель, на который будет записан образ, выбрав пункт «Select target».
3. Начать запись образа, выбрав пункт «Flash!».

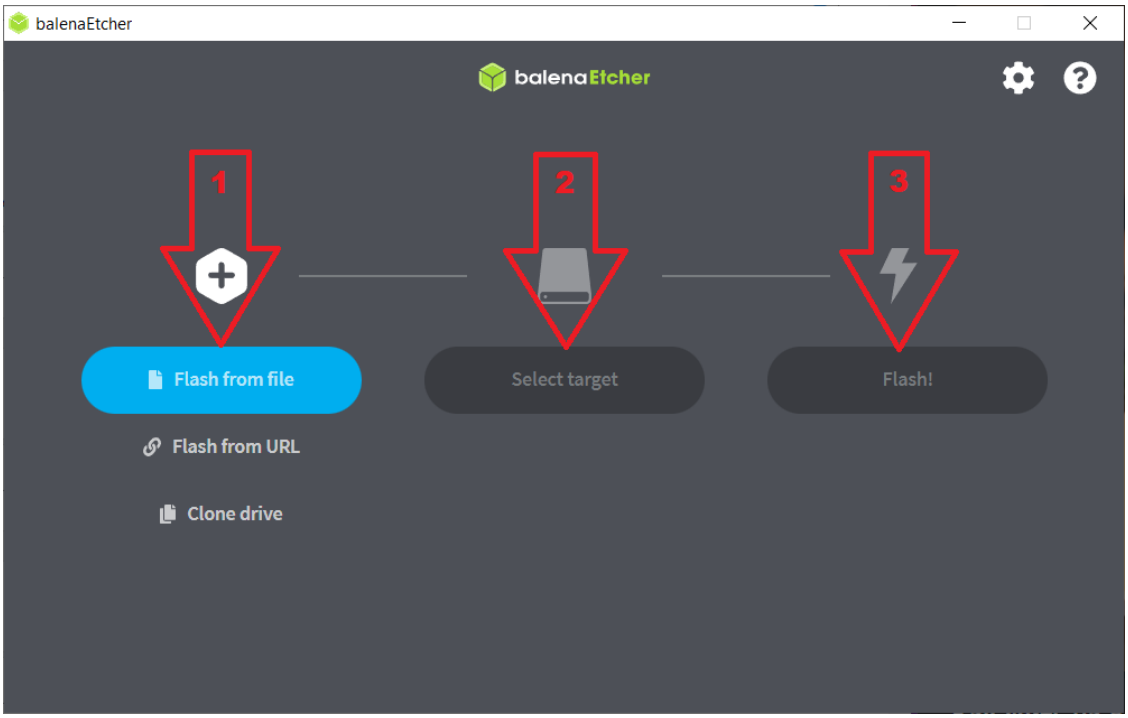


Рисунок 295. Последовательность шагов при работе с etcher

При успешном завершении записи образа в интерфейсе утилиты `etcher` появится сообщение «Flash Completed!». USB-носитель готов к дальнейшему использованию. Утилиту `etcher` можно закрыть, а USB-носитель извлечь из пользовательской рабочей станции.

> Если после записи через утилиту `etcher` загрузка с USB-носителя не происходит, необходимо переподготовить его утилитой `rufus`, как описано далее.

Для подготовки загрузочного USB-носителя через утилиту `rufus` нужно сначала разархивировать образ `thinstation.iso` любым доступным архиватором и открыть утилиту из каталога `\thinstation-efi\rufus`.Затем:

> USB-носитель будет отформатирован, убедитесь, что на нем нет важных данных. Не прерывайте монтирование образа на USB-накопитель, так как возможен его выход из строя.

1. Указать USB-носитель, на который будет записан образ, выбрав его в пункте «Device».
2. Нажать экранную кнопку **[SELECT]** и выбрать образ `thinstation.iso`. Убедиться, что параметру «Partition Scheme» присвоилось значение «MBR», параметру «Target system» - «BIOS or UEFI», параметру «Volume label» - «ThinStation»;
3. Начать запись образа, нажав экранную кнопку **[START]** (см. рисунок Последовательность шагов при работе с rufus.

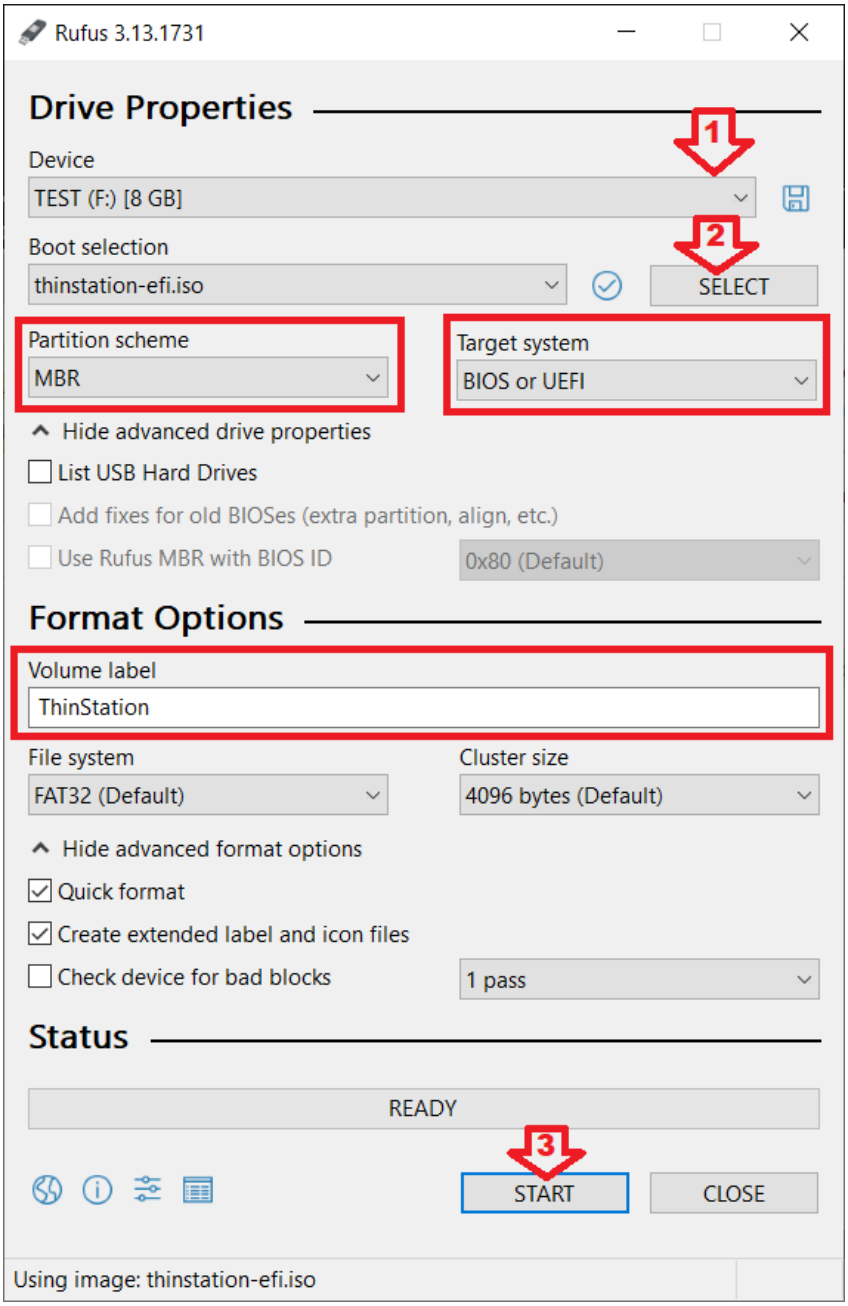


Рисунок 296. Последовательность шагов при работе с rufus

На запрос «ISOHybrid image detected» выбрать вариант «Write in ISO Image mode (Recommended)» (см. рисунок Выбор режима записи).

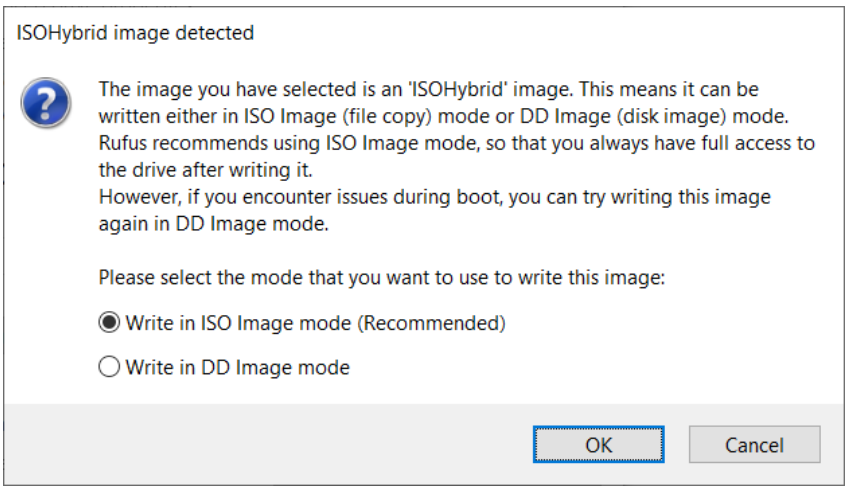


Рисунок 297. Выбор режима записи

Подтвердить уничтожение данных на носителе (см. рисунок Подтверждение уничтожения данных на носителе) и дождаться успешного окончания записи образа (см. рисунок Сигнализация об успешной записи образа).

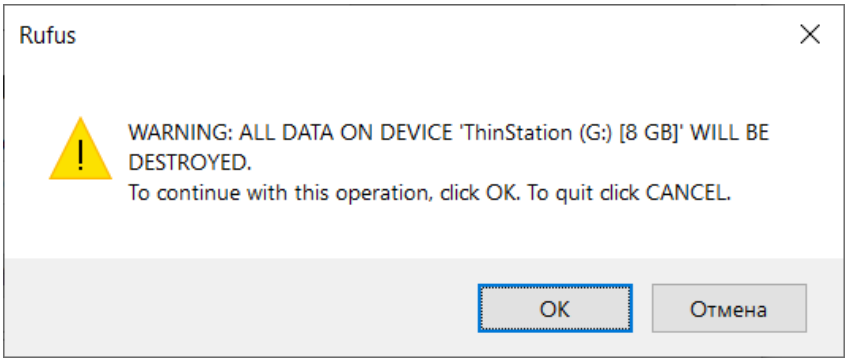


Рисунок 298. Подтверждение уничтожения данных на носителе

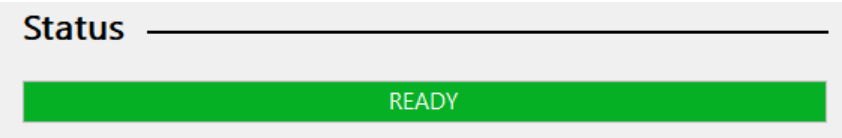


Рисунок 299. Сигнализация об успешной записи образа

Подготовка к PXE-загрузке по сети

Для PXE-загрузки по сети должно выполняться следующее:

- все целевые устройства (компьютер, тонкий клиент и др.) должны находиться в одной локальной сети (в одном широковещательном домене);
- в этой сети должны быть:
  - настроенный DHCP-сервер, выдающий клиентским компьютерам не только сетевые IP-адреса, но и другие сетевые параметры (в частности, IP-адрес TFTP-сервера, с которого будет загружаться Termidesk Live);
  - настроенный TFTP-сервер, с которого можно загрузить установочные данные и файлы для первичной загрузки;
  - настроенные разделяемые сетевые ресурсы, из которых можно загружать пакеты.

Порядок работы:

- целевое устройство подключается к сети и запрашивает IP-адрес, передавая в запросе

информацию о собственной конфигурации;

- DHCP-сервер назначает целевому устройству IP-адрес и вместе с назначенным адресом передает ему дополнительные сетевые параметры, в том числе IP-адрес TFTP-сервера с необходимыми файлами сценариев загрузки Termidesk Live;
- целевое устройство подключается к TFTP-серверу и загружает файлы со сценариями загрузки Termidesk Live.

Подробно о том, как подготовить инфраструктуру PXE на ОС Astra Linux, можно узнать в справочном центре Astra Linux: https://wiki.astralinux.ru/pages/viewpage.action?pageId=263031254.

Пример подготовки TFTP-сервера на ОС Windows

Подготовка сервера будет осуществляться утилитой `tftpd` (доступ по ссылке: `https://bitbucket.org/phjounin/tftpd64/downloads/`). Для установки используется файл `Tftpd64-4.64-setup.exe`.

Все указанные IP-адреса должны быть заменены на актуальные, соответствующие схеме адресации, принятой в инфраструктуре организации.

После установки утилиты необходимо:

- создать в файловой системе каталог, который будет использоваться для хранения загрузочных файлов (в примере используется `F:\tftpboot`);
- скачать загрузчик `syslinux` (доступ по ссылке: `https://mirrors.edge.kernel.org/pub/linux/utils/boot/syslinux/syslinux-6.03.zip`) в `zip`-формате и разархивировать. Скопировать в каталог `F:\tftpboot` файлы:
  - `\syslinux-6.03\bios\core\pxelinux.0`;
  - `\syslinux-6.03\bios\com32\elflink\ldlinux\ldlinux.c32`;
- создать файл `default` следующего содержания:

```
TIMEOUT 0
DEFAULT default
LABEL default
KERNEL ::vmlinuz
APPEND initrd=::initrd splash=silent,theme:default load_ramdisk=1
ramdisk_blocksize=4096 root=/dev/ram0 ramdisk_size=786432 console=tty1
vt.global_cursor_default=0 quiet loglevel=3 LM=3
```

- создать каталог `F:\tftpboot\pxelinux.cfg` и скопировать в него файл `default`;
- скопировать в каталог `F:\tftpboot\` ранее загруженные файлы Termidesk Live: `initrd`, `vmlinuz`;
- открыть утилиту `tftpd` и перейти в пункт «Settings - TFTP». Задать параметры (см. рисунок Настройки TFTP-сервера):
  - «Base Directory» - корневая директория, в которой находятся файлы загрузки;
  - «TFTP Security» - управление уровнем TFTP-безопасности. Стандартный уровень - чтение и запись файлов доступны только в корневой директории;
  - «Timeout (seconds)» - таймаут передачи в секундах;
  - «Max Retransmit» - максимальное количество попыток повторной передачи;

- «Tftp port» - используемый порт. Следует изменить, если сервер расположен за межсетевым экраном;
- «PXE Compatibility» - управление PXE-совместимостью;
- «Show Progress bar» - управление индикацией для каждой передачи данных;
- «Translate Unix files names» - управление преобразованием имен файлов в Unix-подобные;
- «Bind TFTP to this address» - адрес, с которым будет ассоциирован TFTP-сервер;
- «Allow '\' As virtual root» - управление чтением файлов из корневой директории;

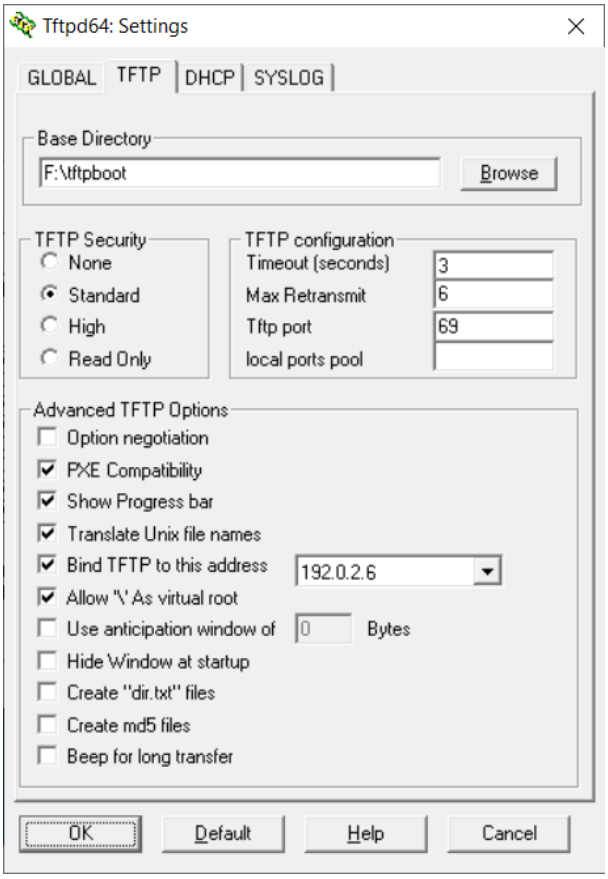


Рисунок 300. Настройки TFTP-сервера

- перейти в пункт «DHCP». Задать параметры для DHCP-сервера (см. рисунок Настройки DHCP-сервера утилиты tftpd):
  - option 1 (согласно указаниюIANA) - «Mask» - маска подсети;
  - option 3 - «Def. router» - IP-адрес маршрутизатора;
  - option 6 - «DNS Servers» - IP-адрес DNS-сервера;
  - option 15 - «Domain Name» - доменное имя;
  - option 42 - «NTP server» - IP-адрес NTP-сервера. В примере не использовался;
  - option 44 - «WINS server» - IP-адрес WINS-сервера;
  - option 120 - «SIP server» - IP-адрес SIP-сервера. В примере не использовался;
  - «IP pool start address» - начальный IP-адрес пула;
  - «Size of pool» - размер пула;
  - «Lease (minutes)» - время аренды IP-адреса;
  - «Boot File» - расположение файла `pxelinux.0` с учетом указанной корневой директории;

- «Ping address before assignation» - управление проверкой адреса перед назначением;
- «Persistant leases» - управление сохранением информации об аренде IP-адреса;
- «Bind DHCP to this address» - адрес, с которым будет ассоциирован DHCP-сервер;

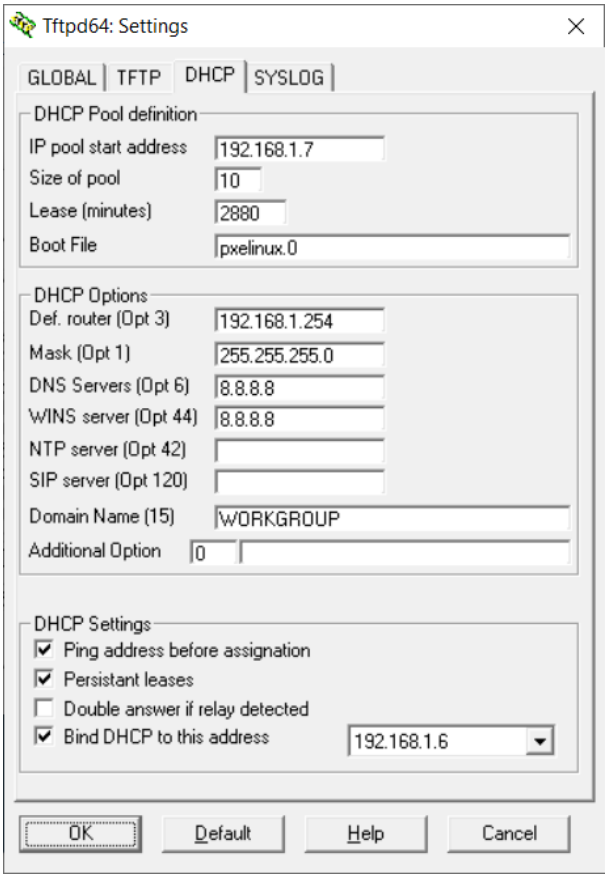


Рисунок 301. Настройки DHCP-сервера утилиты tftpd

- в главном окне проверить, что параметры «Current Directory» и «Server interfaces» соответствуют ранее на выбранным (см. рисунок Отображение заданных параметров в главном окне утилиты tftpd).

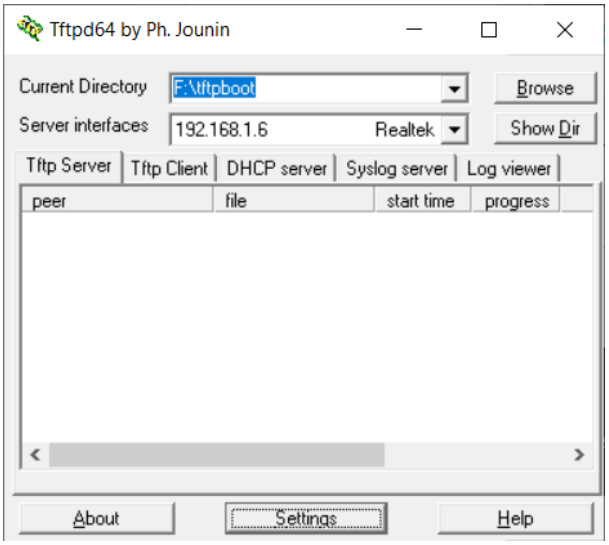


Рисунок 302. Отображение заданных параметров в главном окне утилиты tftpd

TERMIDESK LIVE. НАСТРОЙКИ

Добавление приложений в Termidesk Live

Общие сведения

Termidesk Live поддерживает добавление приложений в ОС посредством файловой системы overlay, при этом первоначальный образ Termidesk Live не меняется. Приложения, необходимые пользователю для работы, добавляются на этапе загрузки образа через опрос NFS-сервера, который должен функционировать в сетевой инфраструктуре.

Для добавления приложений должно выполняться следующее:

- все целевые устройства (компьютер, тонкий клиент и др.) должны находиться в одной локальной сети (в одном широковещательном домене);
- в этой сети должны быть:
  - настроенный DHCP-сервер, выдающий клиентским компьютерам не только сетевые IP-адреса, но и другие сетевые параметры, в частности, IP-адрес NFS-сервера и опцию «appimage». Настройка опции «appimage» приведена ниже;

> Работа функционала проверена с программными DHCP-серверами. С аппаратными комплексами DHCP-серверов работа функционала будет затруднена, поскольку в большинстве случаев такие DHCP-серверы поддерживают только назначение IP-адресов и не поддерживают передачу других сетевых параметров.

  - настроенный NFS-сервер, на котором выполнены дополнительные действия, приведенные ниже;
  - разделяемые сетевые ресурсы NFS-сервера, используемые для хранения приложений. Настройка сетевых ресурсов приведена ниже.

Порядок работы:

- целевое устройство с образом Termidesk Live подключается к сети и запрашивает IP-адрес, передавая в запросе информацию о собственной конфигурации;
- DHCP-сервер назначает целевому устройству IP-адрес и вместе с назначенным адресом передает ему дополнительные сетевые параметры, в том числе IP-адрес NFS-сервера и значение опции «appimage»;

> Образ Termidesk Live поставляется с уже настроенным функционалом поддержки получения IP-адреса от DHCP-сервера.
>
> Если целевое устройство с образом Termidesk Live имеет два и более сетевых интерфейса с автоматическим получением параметров от DHCP-сервера, для поиска NFS-сервера будет использоваться первый интерфейс.
>
> В текущей версии Termidesk Live не предусмотрена парольная или какая-либо иная аутентификация при монтировании каталога с NFS-сервера.

- целевое устройство с образом Termidesk Live подключается к указанному в опции «appimage» NFS-серверу и каталогу и монтирует его в ОС Termidesk Live;
- после завершения загрузки Termidesk Live приложения, которые были размещены в каталоге на NFS-сервере, отображаются на рабочем столе ОС Termidesk Live.

Дополнительная настройка существующего DHCP-сервера

Дополнительная настройка существующего DHCP-сервера сводится к редактированию конфигурационного файла `dhcpd.conf`, а именно:

- в файле обязательно должна быть указана опция `appimage` с кодом `155` и значением `text`:

> Получение опции `appimage` с кодом `155` и значением `text` предопределено в образе Termidesk Live, использование других значений опции не предусмотрено.

```
option appimage code 155 = text;
```

- в файле обязательно должен быть указан NFS-сервер, например:

```
host nfs-server { hardware ethernet 08:00:27:be:4a:f0; fixed-address 192.0.2.1; }
```

- в файле обязательно присвоить опции `appimage` путь к каталогу на NFS-сервере, из которого Termidesk Live будет получать приложения:

```
option appimage "192.0.2.1:111:2049:/nfs";
```

Где:

`192.0.2.1` - IP-адрес NFS-сервера;

`111` - порт регистрации удаленных вызовов процедур (RPC);

`2049` - порт для подключения к NFS-серверу;

`/nfs` - путь к каталогу на NFS-сервере для монтирования.

Пример файла `dhcpd.conf`:

> Приведен только пример файла! Настройки DHCP-сервера и IP-адреса должны быть заменены на актуальные, используемые согласно схеме адресации, принятой в инфраструктуре организации.

```
option appimage code 155 = text;
subnet 192.0.2.0 netmask 255.255.255.0 {
    host nfs-server { hardware ethernet 08:00:27:be:4a:f0; fixed-address 192.0.2.1;
}
    option routers 192.0.2.2;
    option subnet-mask 255.255.255.0;
    range 192.0.2.10 192.0.2.255;
    default-lease-time 600;
    max-lease-time 1800;
    option appimage "192.0.2.1:111:2049:/nfs";
    option domain-name-servers 8.8.8.8, 8.8.4.4;
```

```
}
```

Дополнительная настройка существующего NFS-сервера

Дополнительная настройка существующего NFS-сервера сводится к:

- созданию обязательного каталога, указанного в опции `appimage`, в котором будут размещаться приложения (`/nfs`):

```
sudo mkdir /nfs
```

- созданию подкаталога `appimage` в указанном каталоге (`/nfs/appimage`) для хранения файлов разрешения `.AppImage`:

```
sudo mkdir /nfs/appimage
```

- созданию подкаталога `menu` в указанном каталоге (`/nfs/menu`) для хранения конфигурационных файлов:

```
sudo mkdir /nfs/menu
```

- созданию подкаталога `images` в каталоге `appimage` (`/nfs/appimage/images`) для хранения изображений (иконок) приложений:

```
sudo mkdir /nfs/appimage/images
```

После создания каталогов они должны быть наполнены соответствующим образом:

- в корень каталога `/nfs/appimage` необходимо поместить непосредственно приложения в формате `.AppImage`;

Файлам `.AppImage` обязательно нужно добавить флаг исполнения:

```
sudo chmod +x /nfs/appimage/*.AppImage
```

- в каталог `/nfs/appimage/images` необходимо поместить изображения;
- в каталог `/nfs/menu` необходимо поместить конфигурационные файлы, соответствующие `.AppImage`, содержащие описание размещения приложения на рабочем столе Termidesk Live. Пример конфигурационного файла `/nfs/menu/Application`:

```
needs="x11"; title="Application"; icon="/nfs/appimage/images/Application.png";
command="/nfs/appimage/Application-x86_64.AppImage";
```

Создание приложений формата AppImage

Для создания приложений формата .AppImage может использоваться исполняемый файл appimage-builder.sh. Преобразование приложений должно выполняться на любом узле, отличном от Termidesk Live и на котором возможно разрешение зависимостей, приведенных ниже.

Действия для подготовки к использованию appimage-builder.sh:

> Все перечисленные в этом подразделе действия должны выполняться на ОС, отличной от ОС Astra Linux Special Edition, например: Alpine Linux, Debian.

- скачать утилиту appimagetool: https://github.com/AppImage/appimagetool/releases. Поместить в любую директорию, например, /home/user/;
- скачать среду выполнения runtime: https://github.com/AppImage/type2-runtime/releases. Поместить в любую директорию, например, /home/user/;
- установить пакеты rpm2cpio и cpio;
- установить пакет binutils;
- назначить флаг исполнения для загруженных утилит appimagetool-x86_64.AppImage и runtime-x86_64:

```
chmod +x /home/user/appimagetool-x86_64.AppImage /home/user/runtime-x86_64
```

- создать каталог appimage-builder:

```
mkdir /home/user/appimage-builder
```

- скопировать в него файл appimage-builder.sh и сделать его исполняемым:

```
chmod +x /home/user/appimage-builder/appimage-builder.sh
```

- создать каталог приложения apps с подкаталогом наименования приложения (в примерах используется icaclient):

```
mkdir -p /home/user/appimage-builder/apps/icaclient
```

- создать в каталоге /home/user/appimage-builder/apps/icaclient файл sources и внести в него все зависимости приложения, пример:

```
http://security.debian.org/debian-
security/pool/updates/main/w/webkit2gtk/libwebkit2gtk-4.0-37_2.42.5-
1~deb12u1_amd64.deb
http://security.debian.org/debian-
security/pool/updates/main/w/webkit2gtk/libjavascriptcoregtk-4.0-18_2.42.5-
1~deb12u1_amd64.deb
http://ftp.ru.debian.org/debian/pool/main/i/icu/libicu72_72.1-3_amd64.deb
```

```
http://ftp.ru.debian.org/debian/pool/main/g/gst-plugins-bad1.0/libgstreamer-
plugins-bad1.0-0_1.22.0-4+deb12u5_amd64.deb
http://ftp.ru.debian.org/debian/pool/main/libj/libjpeg-turbo/libjpeg62-turbo_2.1.5-
2_amd64.deb
http://ftp.ru.debian.org/debian/pool/main/liba/libavif/libavif15_0.11.1-1_amd64.deb
http://ftp.ru.debian.org/debian/pool/main/libm/libmanette/libmanette-0.2-0_0.2.6-
3+b1_amd64.deb
http://ftp.ru.debian.org/debian/pool/main/d/dav1d/libdav1d6_1.0.0-2_amd64.deb
http://ftp.ru.debian.org/debian/pool/main/libg/libgav1/libgav1-1_0.18.0-
1+b1_amd64.deb
http://ftp.ru.debian.org/debian/pool/main/r/rust-rav1e/librav1e0_0.5.1-6_amd64.deb
http://ftp.ru.debian.org/debian/pool/main/s/svt-av1/libsvtav1enc1_1.4.1+dfsg-
1_amd64.deb
http://ftp.ru.debian.org/debian/pool/main/a/aom/libaom3_3.6.0-1_amd64.deb
http://ftp.ru.debian.org/debian/pool/main/liby/libyuv/libyuv0_0.0~git20230123.b2528
b0-1_amd64.deb
http://ftp.ru.debian.org/debian/pool/main/a/abseil/libabsl20220623_20220623.1-
1_amd64.deb
http://ftp.ru.debian.org/debian/pool/main/g/gcc-12/libstdc++6_12.2.0-14_amd64.deb
http://ftp.ru.debian.org/debian/pool/main/g/glib2.0/libglib2.0-0_2.74.6-2_amd64.deb
http://ftp.ru.debian.org/debian/pool/main/libs/libselinux/libselinux1_3.4-
1+b6_amd64.deb
http://ftp.ru.debian.org/debian/pool/main/libf/libffi/libffi8_3.4.4-1_amd64.deb
http://ftp.ru.debian.org/debian/pool/main/g/gstreamer1.0/libgstreamer1.0-0_1.22.0-
2_amd64.deb
http://ftp.ru.debian.org/debian/pool/main/g/gst-plugins-base1.0/libgstreamer-
plugins-base1.0-0_1.22.0-3+deb12u1_amd64.deb
http://ftp.ru.debian.org/debian/pool/main/g/gst-plugins-base1.0/libgstreamer-gl1.0-
0_1.22.0-3+deb12u1_amd64.deb
```

- в каталоге приложения (в примере - `icaclient`) создать подкаталог `files`:

```
mkdir /home/user/appimage-builder/apps/icaclient/files
```

- поместить в подкаталог `files` файлы для запуска `.AppImage`, а именно:
  - изображение приложения в формате `.png`;
  - конфигурационный файл формата `.desktop`, содержащий информацию о запуске приложения, пример:

    ```
    [Desktop Entry]
    Version=1.0
    Type=Application
    Name=Citrix Workspace
    Icon=receiver
    Categories=Network;
    Exec=opt/Citrix/ICAClient/selfservice --icaroot opt/Citrix/ICAClient
    ```

- исполняемый файл AppRun, содержащий основную команду запуска приложения, пример:

```
#!/bin/sh

export LD_LIBRARY_PATH="lib/x86_64-linux-
gnu;lib;lib64;usr/lib;usr/lib/x86_64-linux-gnu;"

readlink_file() {
    next_path=$1
    i=0
    while [ "$i" != 10 ] && [ "x$next_path" != "x$path" ]; do
        path=$next_path
        next_path=$(readlink "$path" || echo $path)
        ((++i))
    done
    echo "$path"
}

basedir() {
    file=$(readlink -f "$1") || $(readlink_file "$1")
    echo $(cd "$(dirname "$file")" && pwd -P)
}

cd "$(basedir "$0")" && LD_PRELOAD=usr/lib/x86_64-linux-gnu/libgmodule-
2.0.so.0 opt/Citrix/ICAClient/selfservice --icaroot opt/Citrix/ICAClient
```

Если приложение необходимо модифицировать, применить к нему патч, то это возможно сделать, создав исполняемый файл build.sh.

Build.sh должен содержать в себе необходимые инструкции по модификации и должен быть скопирован в каталог приложения, в примерах это /home/user/appimage-builder/icaclient.

- убедиться, что структура каталога приложения (в примере - icaclient) соответствует следующей:

```
appimage-builder/icaclient
 ├──── build.sh (необязательный файл)
 ├──── files
 │     ├──── AppRun
 │     ├──── icaclient.desktop
 │     └──── icaclient.png
 └──── sources
```

После выполнения всех перечисленных действий по подготовке среды выполнения можно перейти к формированию файлов .AppImage:

- перейти в каталог appimage-builder:

```
cd /home/user/appimage-builder/
```

- запустить исполняемый файл appimage-builder.sh, указав приложение, для которого необходимо сформировать .AppImage (в примере - icaclient), и инструменты сборки:

```
./appimage-builder.sh --appimage-tool /home/user/appimage-builder/appimagetool-
x86_64.AppImage --appimage-runtime /home/user/appimage-builder/runtime-x86_64
icaclient
```

Если среда выполнения была подготовлена правильно, то appimage-builder.sh автоматически создаст каталог AppImages в домашнем каталоге пользователя и поместит в него после сборки файлы .AppImage и журнал сборки. В качестве временного каталога используется /tmp/.

Список всех параметров, поддерживаемых исполняемым файлом appimage-builder.sh, приведен в на таблице (см. таблицу Список параметров для appimage-builder.sh).

Таблица 417. Список параметров для appimage-builder.sh

Параметр	Описание
--help	Вызов справки appimage-builder.sh
--version	Вывод текущей версии appimage-builder.sh
--appimage-tool	Путь к инструменту сборки appimagetool
--appimage -runtime	Путь к инструменту среды выполнения runtime
--input-path	Каталог с файлами исходных пакетов (AppRun, .desktop, .png)
--output-path	Каталог для сохранения собранных файлов .AppImage
--cache-path	Каталог с загруженными пакетами зависимостей. Задание параметра избавляет от необходимости повторной загрузки пакетов, указанных в sources
--log-path	Каталог для сохранения журнала сборки

TERMIDESK LIVE. РАБОТА С ОБРАЗОМ

Загрузка в ОС Termidesk Live

Загрузка с USB-носителя

Для начала работы с Termidesk Live и загрузки с подготовленного ранее загрузочного USB-носителя:

- установить USB-носитель в USB-порт целевого устройства (компьютер, тонкий клиент и др.), которое должно быть загружено с Termidesk Live;
- включить целевое устройство;
- на этапе включения до загрузки ОС нажать клавиши **<F11>** или **<F12>** для перехода в меню выбора загрузочного устройства в базовой системе ввода-вывода (BIOS);
- выбрать подготовленный USB-носитель;
- дождаться загрузки ОС (см. рисунок Экран загрузки Termidesk Live) и отображения рабочего стола (см. рисунок Рабочий стол Termidesk Live).

Рисунок 303. Экран загрузки Termidesk Live

Рисунок 304. Рабочий стол Termidesk Live

Загрузка по сети

Для загрузки Termidesk Live по сети нужно подготовить целевое устройство, настроив в

BIOS/UEFI загрузку по сети.

Начало работы в ОС Termidesk Live

После загрузки в ОС нужно открыть компонент «Клиент» (ярлык программы «Termidesk Client»), расположенный на рабочем столе.

По умолчанию для работы с конфигурацией Termidesk Live используются учетные записи:

- `root` с паролем `root`;
- `tsuser` с паролем `tsuser`.

TERMIDESK LIVE. ЗАВЕРШЕНИЕ РАБОТЫ

Для завершения работы с Termidesk Live и выключения устройства необходимо:

- в панели управления ОС перейти «Applications - Session»;
- выбрать пункт «Shut Down» (см. рисунок Пункт меню для выключения устройства).

После завершения работы с Termidesk Live прогресс, сделанный за сеанс, не будет сохранен!

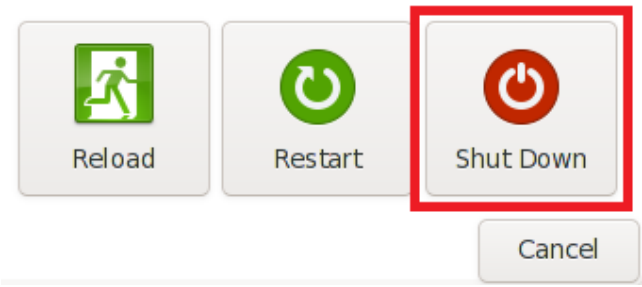


Рисунок 305. Пункт меню для выключения устройства

TERMIDESK LIVE. НЕШТАТНЫЕ СИТУАЦИИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

Возможные неисправности при работе с Клиентом и способы их устранения приведены в таблице (см. таблицу Перечень возможных нештатных ситуаций и способов их устранения).

Таблица 418. Перечень возможных нештатных ситуаций и способов их устранения

Индикация	Описание	Возможное решение
Ошибка: «Не задан транспорт подключения»	Ошибка появляется при попытке получить РМ	Необходимо обратиться к администратору. Администратору необходимо добавить протоколы доставки в фонд РМ

Индикация	Описание	Возможное решение
Ошибка: «Number of service reached MAX for service poll»	Ошибка появляется при запросе РМ	Необходимо обратиться к администратору. Ошибка значит, что достигнуто максимальное количество РМ. Администратору необходимо либо перейти в фонд и принудительно завершить сессию, либо увеличить в фонде максимальное количество РМ
Ошибка: «INTERNAL ERROR: cannot create temporary directory!»	Ошибка появляется при входе в гостевую ОС Microsoft Windows	Необходимо обратиться к администратору. Возможные причины ошибки: • нет прав на каталог профиля пользователя (локальный/сетевой); • профиль не успел создаться в момент запуска компонента «Агент виртуального рабочего места». Администратору необходимо в гостевой ОС РМ перейти в «Управление компьютером - Службы и приложения - Службы - Termidesk Agent Daemon» и в свойствах службы на вкладке «Общие» установить «Тип запуска - Автоматически (отложенный запуск)»
Ошибка: «Прокси-сервер запретил подключение»	Ошибка появляется при подключении к фонду РМ	Необходимо обратиться к администратору. Необходимо настроить прокси-сервер на уровне ОС пользовательской рабочей станции

Индикация	Описание	Возможное решение
Статус «Подготовка рабочего места» висит неограниченно долго	При попытке подключиться к РМ по протоколу RDP (напрямую или через компонент «Шлюз») появляется статус «Подключение к рабочему месту», который потом сменяется на «Подготовка рабочего места» и отображается неограниченно долго	Необходимо обратиться к администратору. Ситуация возникает, если порт РМ недоступен: при запросе подключения к РМ по протоколу RDP перед выдачей подключения «Универсальный диспетчер» проводит проверку доступности порта затребованного протокола на целевом IP-адресе. Администратору необходимо в настройках фильтра трафика разрешить подключение из сегмента сети с инфраструктурой Termidesk VDI для узлов с компонентами «Универсальный диспетчер» в сегмент сети, где находятся РМ, на порт RDP 3389
Ошибка: «Не удалось установить соединение с сервером»	Ошибка появляется при попытке получить РМ	Необходимо выбрать корректный протокол доставки (SPICE) или обратиться к администратору. Ошибка сообщает, что ПО для визуализации РМ не смогло подключиться к платформе виртуализации. Отказ подключения происходит со стороны SPICE-сервера гипервизора. Причиной могут быть: • неправильный протокол доставки; • виртуальная машина (ВМ) выключается и отключает видеокарту; • проблемы с межсетевым экраном; • завис процесс `qemu` ВМ
Ошибка: «VMwareLinkedDeployment object has no attribute 'getConsoleConnection'»	Ошибка появляется при попытке получить РМ	Необходимо обратиться к администратору. С поставщиком ресурсов VMware vSphere необходимо использовать протокол RDP для РМ. Протокол SPICE не поддерживается данным поставщиком

Индикация	Описание	Возможное решение

Гостевая ОС Astra Linux не производит автоматическое масштабирование экрана	При подключении к РМ не происходит автоматическое масштабирование экрана	В гостевой ОС РМ открыть программу «Терминал fly» и выполнить следующее:
		• получить название активного монитора:
		`xrandr --listactivemonitors`
		• выполнить команду:
		`xrandr --output $MONITOR --auto`
		где `$MONITOR` - название активного монитора, полученное предыдущей командой.
		Если действия не привели к желаемому результату, необходимо обратиться к администратору для проверки настроек масштабирования в гостевой ОС РМ

При попытке соединения к терминальному серверу или опубликованному на нем приложению соединение не устанавливается	При подключении к терминальному серверу соединение не устанавливается. При подключении к опубликованному приложению вместо приложения - черный фон. Ошибка может возникнуть при подключении к «Серверу терминалов Astra Linux» (STAL) или MS RDS	Необходимо обратиться к администратору. Для устранения проблемы необходимо в графическом интерфейсе управления Termidesk VDI перейти «Рабочие места - Фонды», выбрать фонд РМ и задать ему политику «Аутентификация на уровне сети (RDP)»: • «TLS» или «RDP» для STAL; • «NLA» для MS RDS
Ошибка: «Фонд находится в режиме техобслуживания, подключение к рабочему месту временно недоступно»	Ошибка появляется при попытке получить РМ	Необходимо обратиться к администратору. Выбранный фонд находится в режиме техобслуживания. Чтобы фонд вновь был доступен для подключения, администратор должен отключить этот режим

Индикация	Описание	Возможное решение
Ошибка: «Ошибка сервера»	Ошибка появляется при попытке подключения к терминальному серверу STAL	Необходимо обратиться к администратору. Администратору необходимо подключиться к серверу с установленным STAL и проверить значение параметра `allowed_users` в файле `/etc/X11/Xwrapper.config`. Этот параметр должен соответствовать: `allowed_users=anybody`
Ошибка: «Этот сеанс будет прекращен из-за ошибки протокола. Попробуйте подключиться заново к удаленному компьютеру»	Ошибка появляется при попытке подключиться к терминальному серверу STAL через стандартную утилиту Windows `mstsc`	Необходимо обратиться к администратору. Администратор должен проверить значение политики «Глубина цвета (RDP)» в «Портале администратора» компонента «Универсальный диспетчер»: значение политики должно быть «32 бит»

Ошибка:
 	
«Сервис cups не запущен или работает некорректно»
	Ошибка появляется при нажатии на экранную кнопку **[Перенаправление принтеров]** в интерфейсе ПО Termidesk Viewer	Необходимо обратиться к администратору.
		Администратор должен:
		
		• проверить состояние службы `termidesk-cupsd`:
		
		`sudo systemctl status termidesk-cupsd`
		
		• если служба неактивна, то активировать ее:
		
		`sudo systemctl start termidesk-cupsd`
		
		• если служба не найдена или рекомендации не помогли, то переустановить компонент «Агент виртуальных рабочих мест»

Индикация	Описание	Возможное решение
Ошибка: «Достигнуто максимально допустимое количество подключений, разрешённое лицензией. Пожалуйста, обратитесь к администратору» или «Maximum allowed number of licensed connections has been reached. Please contact your adminstrator»	Ошибка появляется при запросе РМ	Необходимо обратиться к администратору. Ошибка значит, что достигнуто максимальное количество подключений, определенное лицензией. Администратору необходимо либо принудительно завершить сессии, либо получить и внести лицензию на большее количество подключений
Ошибка: «Не удалось авторизовать пользователя на фермах ресурсов» или «JWTAuthenticationError: Failed to get token from Server»	Ошибка появляется при попытке подключиться к РМ через веб-бразуер или через Клиент	Необходимо обратиться к администратору. Администратор должен: • убедиться, что для параметра `AGGREGATOR_JWT_SSL_KEY` в конфигурационном файле «Агрегатора» задан правильный путь к корректному файлу закрытого ключа; • убедиться, что для параметра `AGGREGATOR_JWT_SSL_CERT` в конфигурационном файле «Универсального диспетчера», использующегося в ферме, задан правильный путь к корректному файлу сертификата

Индикация	Описание	Возможное решение
Ошибка: «Неправильный формат имени пользователя. Имя пользователя должно соответствовать формату sAMAccountName» или «Неправильный формат имени пользователя. Имя пользователя должно соответствовать формату UPN»	Ошибка появляется при попытке авторизоваться в Клиенте или в «Портале пользователя»	Ошибка означает, что для авторизации в домене аутентификации используется неверный формат имени пользователя: • если ошибка относится к формату «sAMAccountName», то логин пользователя следует указывать в формате «UserPrincipalName» (UPN), с доменной частью. Например: user@local; • если ошибка относится к формату UPN, то логин пользователя следует указывать в формате «sAMAccountName». Например: user. Если ошибка воспроизводится, следует обратиться к администратору. Администратор должен проверить, что в домене аутентификации установлено правильное значение для параметра «Формат имени пользователя для аутентификации»

Индикация	Описание	Возможное решение
Ошибка: «В данный момент создание новой сессии невозможно из-за удаления предыдущей. Попробуйте через несколько минут. Если проблема повторится, обратитесь к администратору»	Ошибка появляется при попытке подключиться к терминальному серверу	Ошибка означает, что предыдущая сессия в данный момент удаляется. Следует подождать некоторое время, затем снова подключиться к терминальному серверу. Если ошибка воспроизводится, следует обратиться к администратору. Администратор должен проверить: • доступность поставщика ресурсов экранной кнопкой **[Тест]** в «Портале администратора». Для этого нужно перейти «Инфраструктура - Поставщики ресурсов», выбрать наименование поставщика ресурсов и нажать экранную кнопку **[Изменить]**; • работоспособность службы компонента «Сессионный агент» на терминальном сервере; • работоспособность служб STAL, если используется терминальный сервер с этим компонентом
Индикация: «Администратор запретил доступ клиенту с этого IP адреса»	При подключении пользователя к Termidesk VDI отображается фонд, к которому невозможно подключиться. При этом при наведении мыши на фонд появляется сообщение «Администратор запретил доступ клиенту с этого IP адреса»	Индикация означает, что администратор запретил доступ к фонду с этого IP-адреса, но разрешил его отображение. Если доступ к фонду необходим, следует обратиться к администратору. Администратор должен: • добавить соответствующую сеть в настройках фонда; • проверить правильность значения параметра «Доступ из связанных сетей» в свойствах фонда; • проверить правильность значения параметра «Скрывать недоступные ресурсы» в «Портале администратора»

Индикация	Описание	Возможное решение
При работе с файлами и их сохранении возникают ошибки записи. При работе в офисных пакетах (например, LibreOffice) появляется ошибка: «Невозможно создать файл блокировки ...»	При подключении пользователя к РМ по протоколу TERA и работе с перенаправленным каталогом наблюдаются ошибки записи файлов при попытке их сохранения и при работе с ними в офисных пакетах (например, LibreOffice)	Для исправления ситуации нужно отредактировать файл `~/.davfs2/davfs2_termidesk.conf`, добавив строку: Для редактирования файла требуется повышение привилегий пользователя (`sudo`). `use_locks 0`
Не перенаправляется микрофон при подключении по протоколу RDP к ВРМ с гостевой ОС Microsoft Windows	При подключении по протоколу RDP к ВРМ с гостевой ОС Microsoft Windows с пользовательской рабочей станции, на которой микрофон отсутствует или отключен, соединение устанавливается корректно. Однако последующее подключение микрофона во время активного сеанса в ПО Termidesk Viewer не приводит к его перенаправлению в ВРМ	Для исправления ситуации нужно завершить текущий сеанс и повторно подключиться к ВРМ после подключения микрофона к пользовательской рабочей станции
Ошибка: «Не удалось установить доверительные отношения между этой рабочей станцией и основным доменом»	Ошибка появляется при попытке авторизоваться в гостевой ОС РМ	Необходимо обратиться к администратору. Администратор должен убедиться, что для РМ используются параметры гостевых ОС Windows с доменом MS AD
Ошибка: «Удаленный рабочий стол не готов. Повторите попытку позже»	Ошибка появляется при попытке получить РМ	Ошибка означает, что РМ еще не готово (не перешло в статус «Действительный») или не получен ответ от «Агента виртуального рабочего места». Необходимо дождаться подготовки РМ и повторно подключиться через некоторое время. Если ошибка сохранилась: • необходимо обратиться к администратору; • администатор должен убедиться в правильности настройки «Агента виртуального рабочего места»

Индикация	Описание	Возможное решение

Ошибка:
 	
«Ошибка подключения: Termidesk Agent не отвечает — возможно, он не установлен или не запущен на выбранном ВРМ»
	Ошибка появляется при попытке подключиться к назначенному РМ	Необходимо обратиться к администратору.
		Администратор должен:
		
		• проверить состояние службы `termidesk-agent`:
		
		`sudo systemctl status termidesk-agent`
		
		• убедиться в правильности настройки «Агента виртуального рабочего места»;
		• перезапустить службу `termidesk-agent`:
		
		`sudo systemctl restart termidesk-agent`
		
		• если служба не найдена или рекомендации не помогли, то переустановить компонент «Агент виртуальных рабочих мест»

После переподключения к сессии РМ или при разрыве сетевого соединения с РМ перенаправление каталога на сервер терминалов MS RDS становится недоступным	При активном использовании перенаправленного каталога (например, при копировании данных) переподключение к сессии РМ либо разрыв сетевого соединения с РМ приводит к нарушению работы механизма перенаправления. После восстановления соединения перенаправление каталога на сервер терминалов MS RDS для текущего пользователя становится недоступным: каталог не перенаправляется либо доступ к ранее перенаправленному каталогу отсутствует	Для исправления ситуации нужно выполнить выход из гостевой ОС РМ и повторно переподключиться к сессии РМ

ТЕРМИНЫ

Поставщик ресурсов

ОС, платформа виртуализации или терминальный сервер (MS RDS/STAL), предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов РМ

Протокол доставки

Поддерживаемый в Termidesk VDI протокол удаленного доступа к РМ

Компонент «Универсальный диспетчер»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им РМ и контроля доставки

РМ

Фонд рабочих мест

Совокупность подготовленных РМ для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей

Компонент «Шлюз»

Самостоятельный компонент, отвечающий за туннелирование протоколов доставки, использующих транспортный протокол TCP

Компонент «Сервер терминалов Astra Linux»

Компонент Termidesk VDI. Также: STAL. Обеспечивает подключение пользовательских рабочих станций к рабочим местам с ОС Astra Linux Special Edition через сеанс удаленного терминала

СОКРАЩЕНИЯ

ОС	Операционная система
РМ	Рабочее место
BIOS	Basic Input-Output system (базовая система ввода-вывода)
DHCP	Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста)
IP	Internet Protocol (межсетевой протокол)
ISO	International Organization for Standardization (Международная организация по стандартизации)
MBR	Master Boot Record (главная загрузочная запись)
NFS	Network File System (сетевая файловая система)
NTP	Network Time Protocol (протокол сетевого времени)
PXE	Preboot eXecution Environment (среда для загрузки компьютера с помощью сетевой карты без использования локальных носителей данных)
RDP	Remote Desktop Protocol (протокол удаленного рабочего стола)
RDS	Remote Desktop Services (службы удаленного рабочего стола Microsoft)
RPC	Remote Procedure Call (удаленный вызов процедур)
SIP	Session Initiation Protocol (протокол инициализации сеанса связи)
STAL	Terminal Server Astra Linux (сервер терминалов Astra Linux)
TCP	Transmission Control Protocol (протокол управления передачей)
TFTP	Trivial File Transfer Protocol (простой протокол передачи файлов)
UEFI	Unified Extensible Firmware Interface (унифицированный расширяемый микропрограммный интерфейс)
USB	Universal Serial Bus (последовательный интерфейс для подключения периферийных устройств)

WINS Windows Internet Name Service (служба сопоставления NetBIOS-имён компьютеров с IP-адресами узлов)

© ООО «Увеон»

Телефон: +7 495 975 19 75
8 800 222 07 00

Электронная почта для связи: info@uveon.ru

Отдел продаж: info@astralinux.ru
Техподдержка: termidesk@astralinux.ru

Сайт: https://termidesk.ru/

Главный офис 119571, г. Москва,
Ленинский проспект, д. 119А