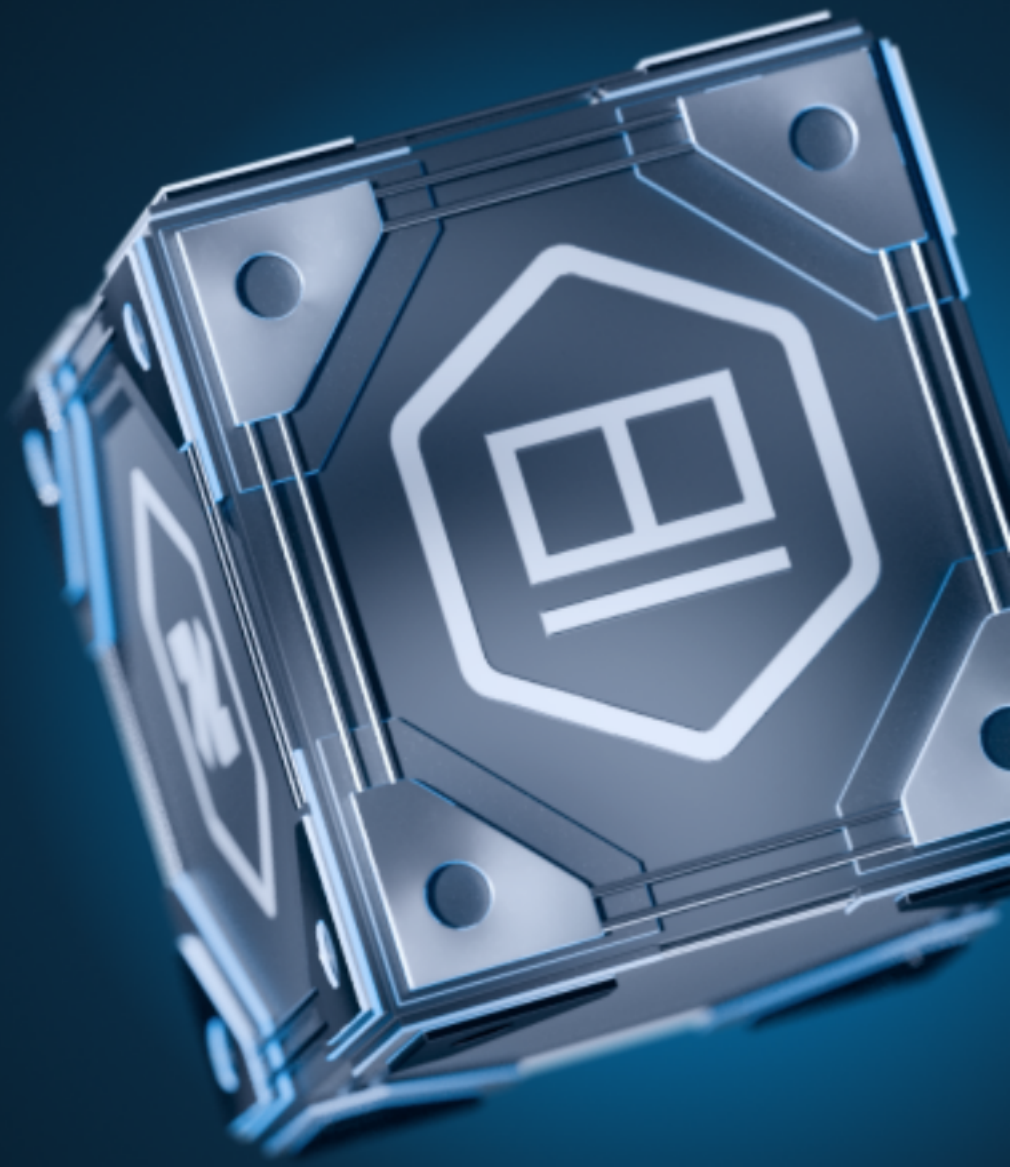
TERMIDESK VDI



Руководство администратора

Установка и настройка «Агрегатора»

СЛЕТ.10001-01 90 08

Версия 7.0.2. Выпуск от 15.09.2026

Оглавление

ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ . . . 3
АГРЕГАТОР. ОБЩИЕ СВЕДЕНИЯ . . . 4
АГРЕГАТОР. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ . . . 7
АГРЕГАТОР. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ . . . 11
Подготовка среды функционирования для «Агрегатора» . . . 11
ОС Astra Linux Special Edition . . . 11
Проверка работоспособности после установки «Агрегатора» . . . 35
АГРЕГАТОР. НАСТРОЙКА АГРЕГАЦИИ РЕСУРСОВ . . . 36
АГРЕГАТОР. ДОМЕНЫ АУТЕНТИФИКАЦИИ . . . 37
Добавление доменов аутентификации в «Агрегаторе» . . . 37
Действия над группами в домене аутентификации в «Агрегаторе» . . . 66
Действия над пользователями в домене аутентификации в «Агрегаторе» . . . 68
Просмотр данных о пользователе домена аутентификации в «Агрегаторе» . . . 70
Действия над атрибутами в домене аутентификации в «Агрегаторе» . . . 71
АГРЕГАТОР. ФЕРМЫ ПОСТАВЩИКОВ РЕСУРСОВ . . . 73
АГРЕГАТОР. УЗЛЫ ФЕРМ ПОСТАВЩИКОВ РЕСУРСОВ . . . 78
АГРЕГАТОР. САЙТЫ . . . 82
АГРЕГАТОР. ШАБЛОНЫ ТЕХОБСЛУЖИВАНИЯ . . . 93
АГРЕГАТОР. ШЛЮЗЫ . . . 95
АГРЕГАТОР. ТЕГИ . . . 97
АГРЕГАТОР. КОНСОЛЬ УПРАВЛЕНИЯ ФЕРМАМИ . . . 100
АГРЕГАТОР. НАЗНАЧЕНИЕ СЛУЖЕБНЫХ ФУНКЦИЙ АДМИНИСТРАТОРАМ . . . 105
АГРЕГАТОР. НАСТРОЙКИ . . . 108
Конфигурационные файлы «Агрегатора» . . . 108
Общие системные настройки «Агрегатора» . . . 146
Системные настройки безопасности «Агрегатора» . . . 149
АГРЕГАТОР. СИСТЕМА АУДИТА . . . 151
Системные настройки аудита «Агрегатора» . . . 151
Описание шаблонов событий аудита «Агрегатора» . . . 152
Формат `CEF` в «Агрегаторе» . . . 164
АГРЕГАТОР. ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ . . . 166
Утилита `termidesk-vdi-manage` в «Агрегаторе» . . . 166
Утилита `termidesk-config` в «Агрегаторе» . . . 169
Утилита `scramble` в «Агрегаторе» . . . 175
АГРЕГАТОР. ГРАФИЧЕСКИЙ ИНТЕРФЕЙС . . . 178
Доступ к веб-интерфейсу «Агрегатора» . . . 178
Типы веб-интерфейса «Агрегатора» . . . 178
Работа с основными функциями веб-интерфейса «Агрегатора» . . . 178
АГРЕГАТОР. ЖУРНАЛИРОВАНИЕ . . . 182
Системные настройки журналирования «Агрегатора» . . . 182
Настройка уровня журналирования «Агрегатора» . . . 182
Журналы «Агрегатора» . . . 183
Просмотр журналов в «Агрегаторе» . . . 183
ТЕРМИНЫ . . . 187
СОКРАЩЕНИЯ . . . 188

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, ВРМ) 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 1. 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

CPU, шт	RAM, ГБ	HDD, ГБ	Сеть, Мбит/с
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 «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)			

CPU, шт	RAM, ГБ	HDD, ГБ	Сеть, Мбит/с
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.

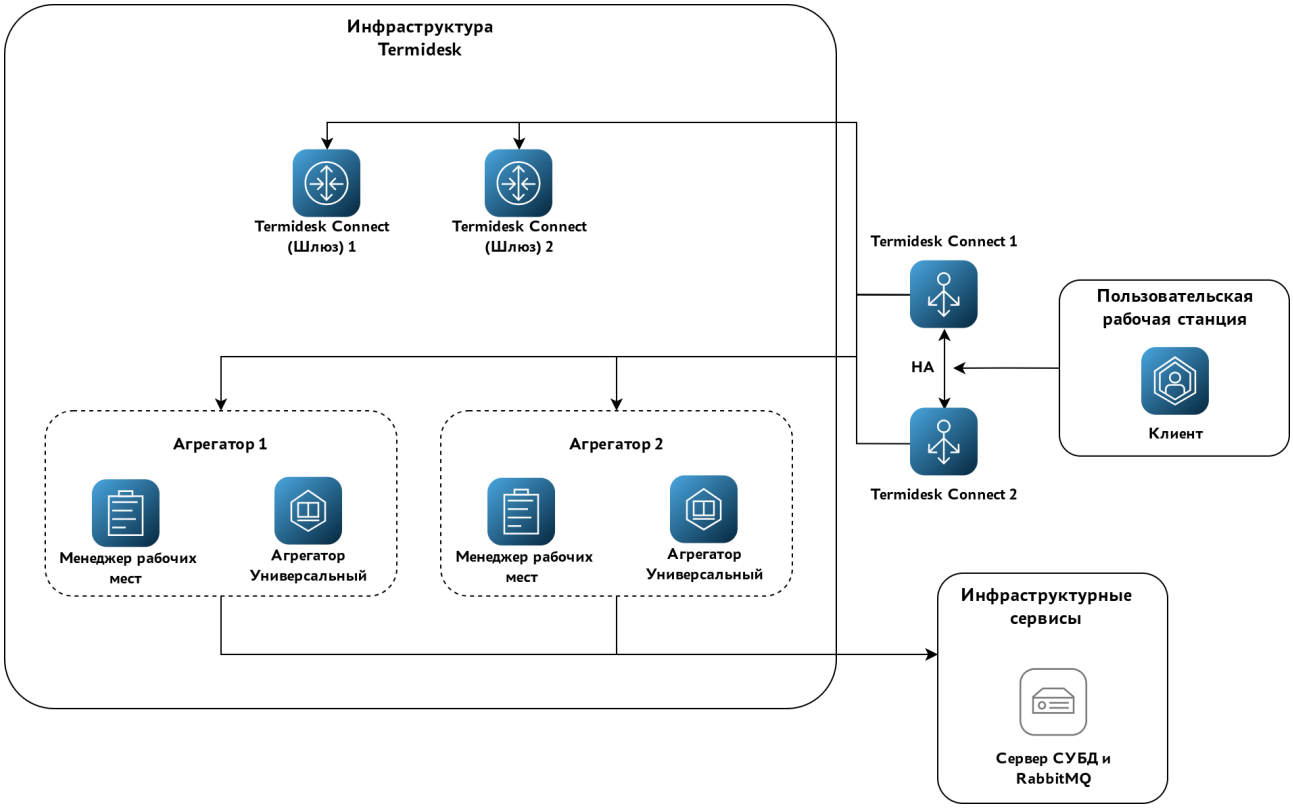


Рисунок 1. Схема минимальной распределенной установки

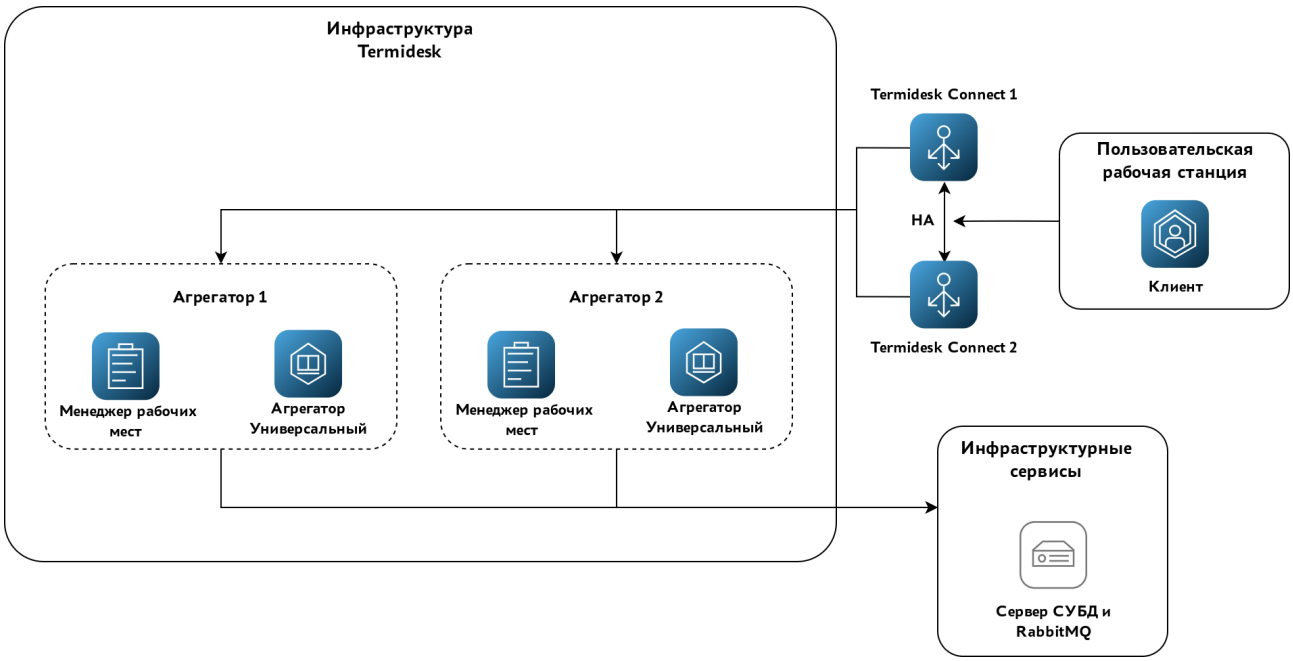


Рисунок 2. Схема минимальной распределенной установки при наличии лицензии Termidesk Connect

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

Таблица 3. 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.

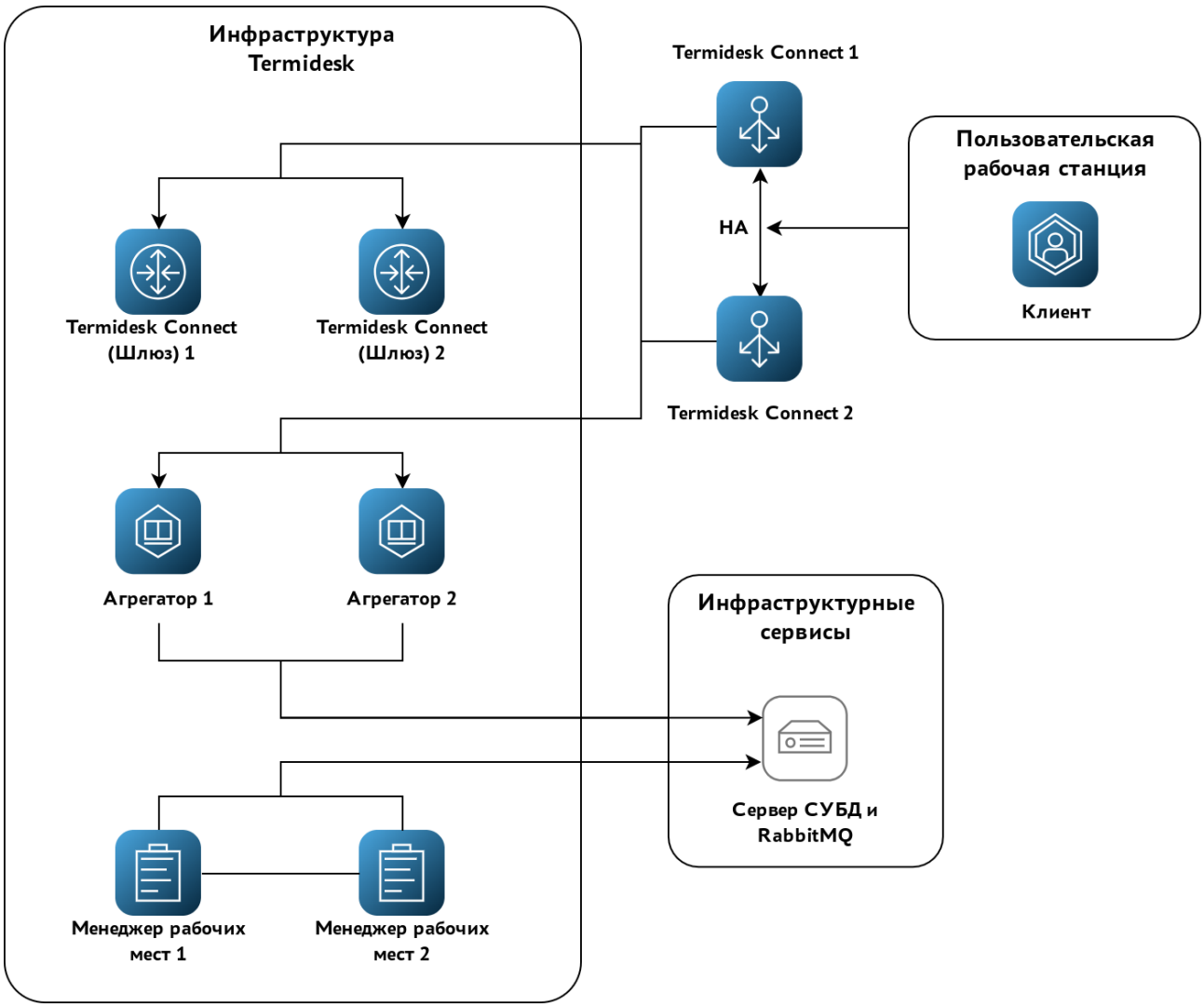


Рисунок 3. Схема стандартной распределенной установки

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 4. 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.

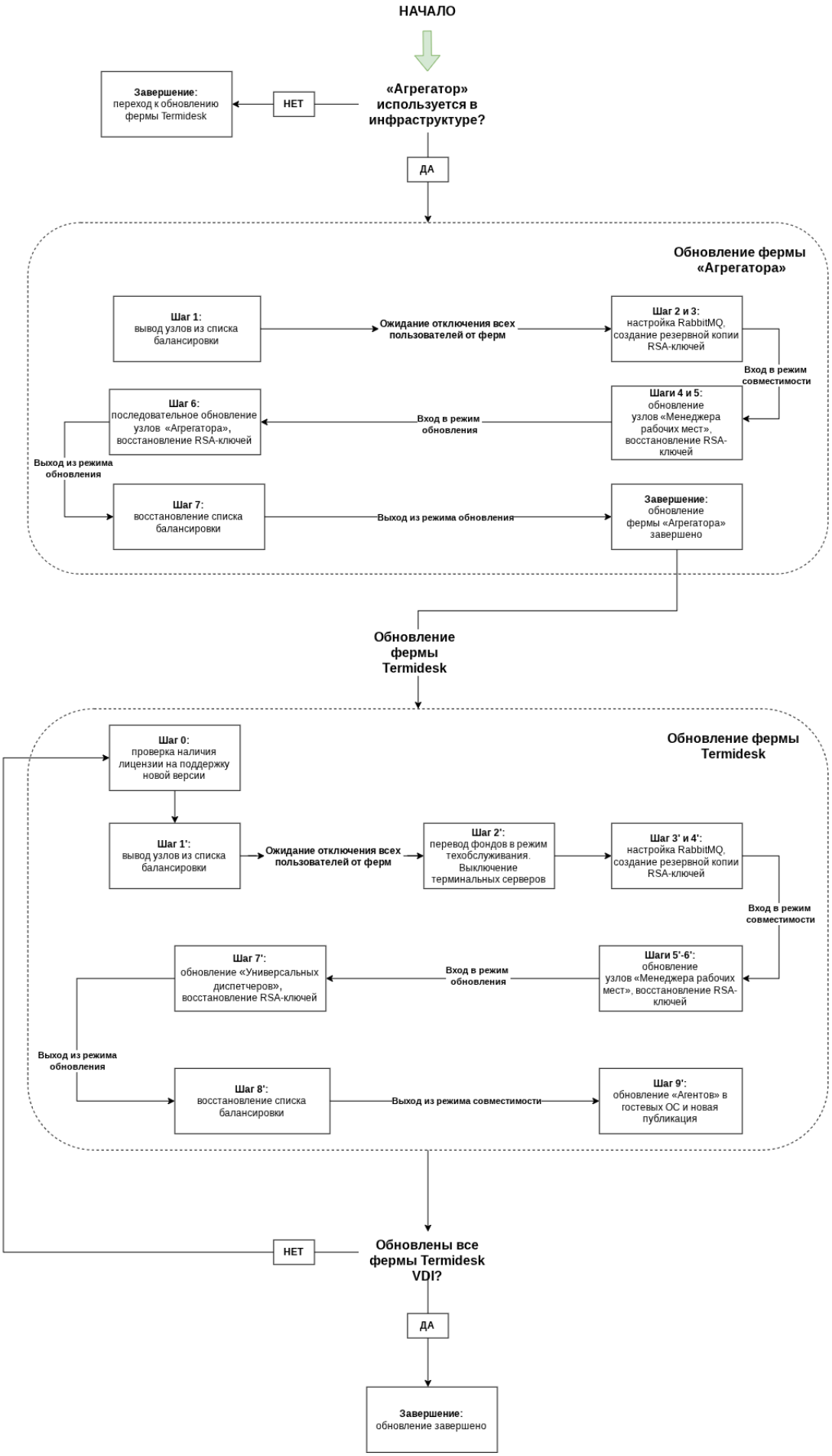


Рисунок 4. Последовательность обновления распределенной конфигурации

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 5. 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 6. 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
«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)

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 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
«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

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

«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.

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/»

«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»);

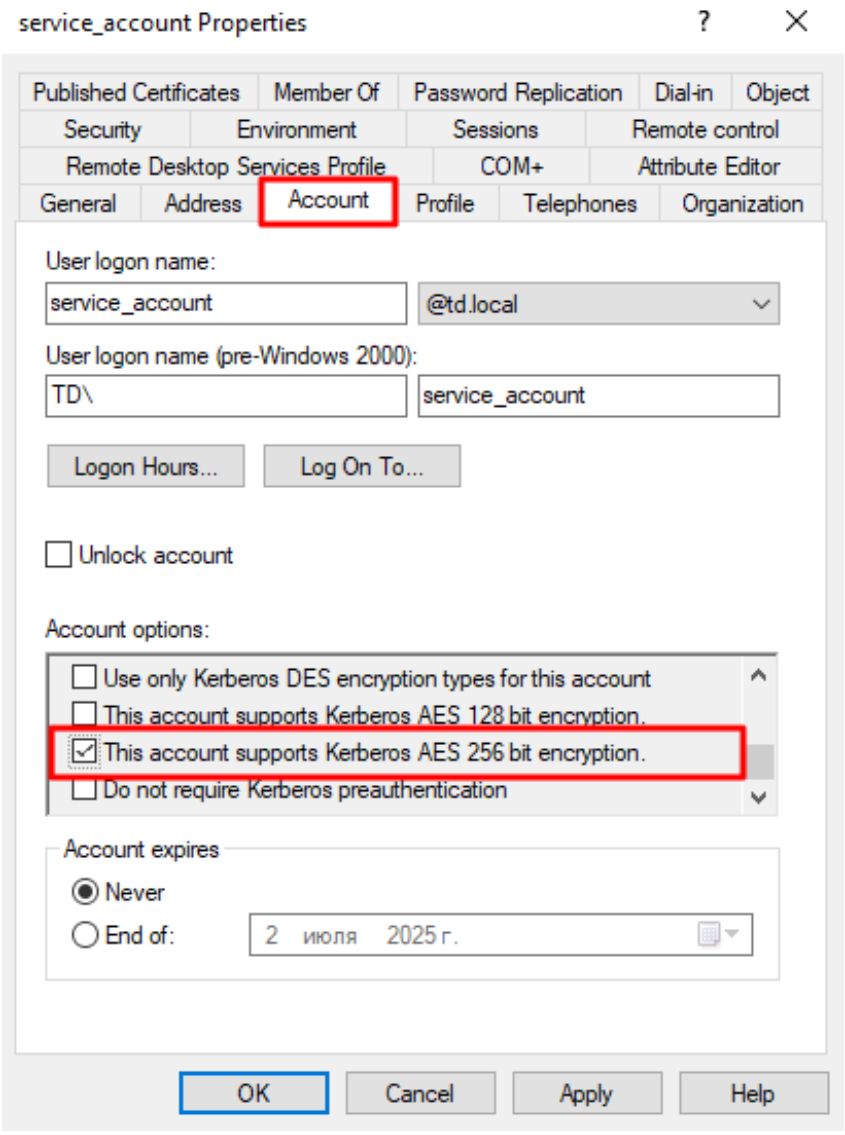


Рисунок 5. Активация параметра «This account supports Kerberos AES 256 bit encryption»

- 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»);

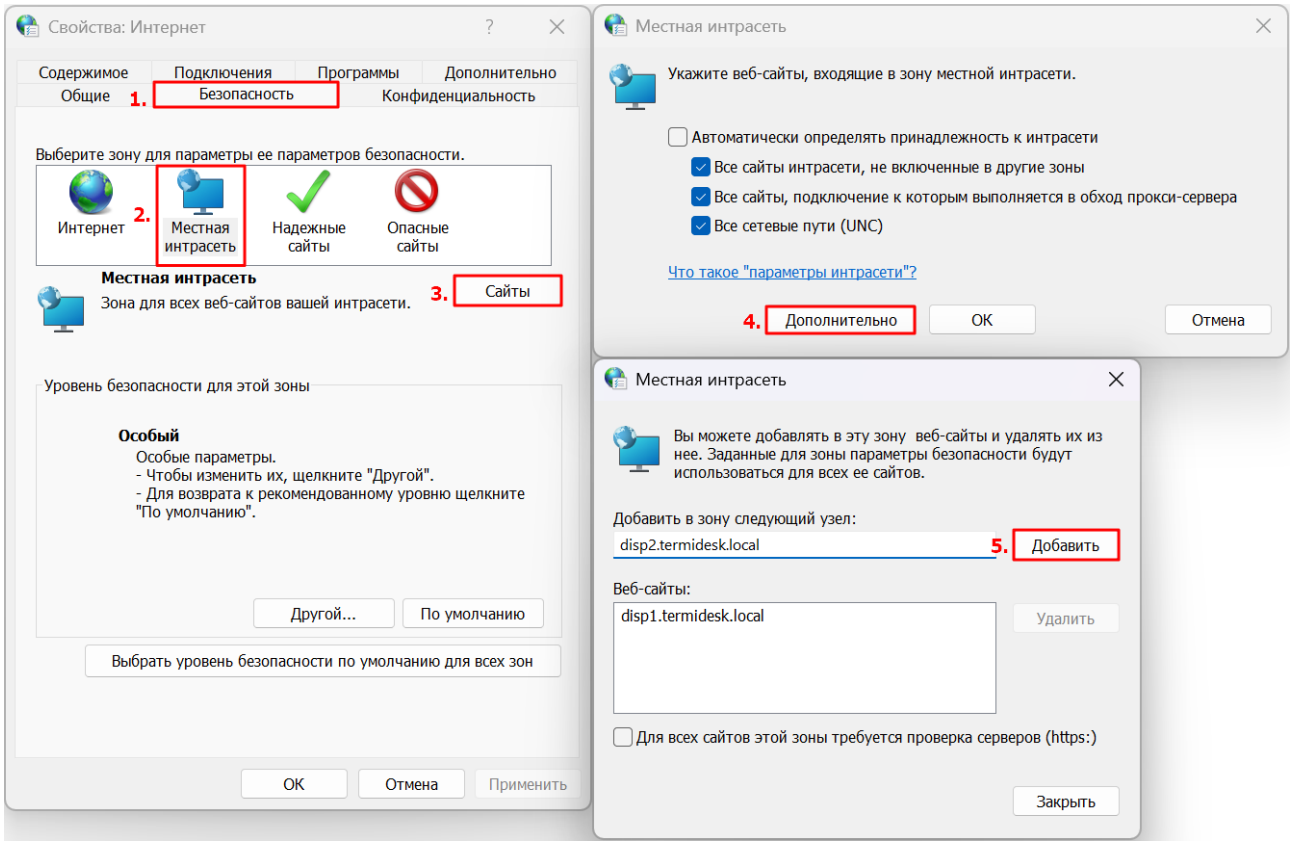


Рисунок 6. Добавление FQDN компонента «Универсальный диспетчер» в зону «Местная интрасеть»

- 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 7. 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 8. 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 9. 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 10. 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 11. 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 12. 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 13. 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 14. 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 15. 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 16. 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 17. 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
«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 18. 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
«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»

Параметр	Описание
«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
«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 19. 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 20. Данные для добавления узла Termidesk VDI

Параметр	Описание
«Название»	Текстовое наименование добавляемого узла
«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»

Параметр	Описание
«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 21. 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
«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 22. 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»

Параметр	Описание
«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»
«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**

Параметр	Описание
«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
«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

Параметр	Описание
«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
«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

Параметр	Описание
«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»
«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

Параметр	Описание
«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
«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

Параметр	Описание
«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»
«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

Параметр	Описание
«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»
«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 23. 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 24. 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

Параметр	Описание
«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**)
«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 25. 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 26. 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 27. Параметры списка шлюзов

Параметр	Описание
«Название»	Текстовое наименование шлюза
«URL»	Адрес шлюза, обеспечивающего формирование и поддержание соединения
«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 28. Данные для добавления шлюза

Параметр	Описание
«Название»	Текстовое наименование добавляемого шлюза
«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 29. 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 30. 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 31. 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 32. 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

Параметр	Описание
«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 33. Параметры списка сессий

Параметр	Описание
«Дата и время»	Дата и время входа пользователя на РМ
«Пользователь»	Имя пользователя, которому было выдано РМ

Параметр	Описание
«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 34. 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

Параметр	Описание
«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
«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).

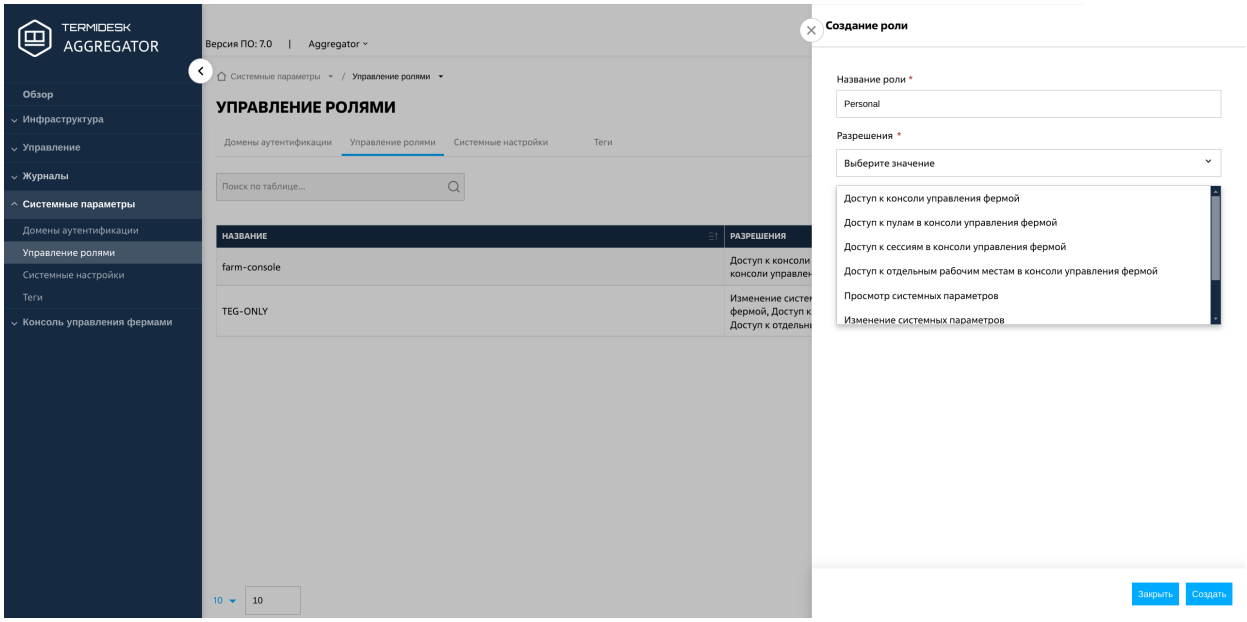


Рисунок 7. Окно назначения пользовательских разрешений

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 35. 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).

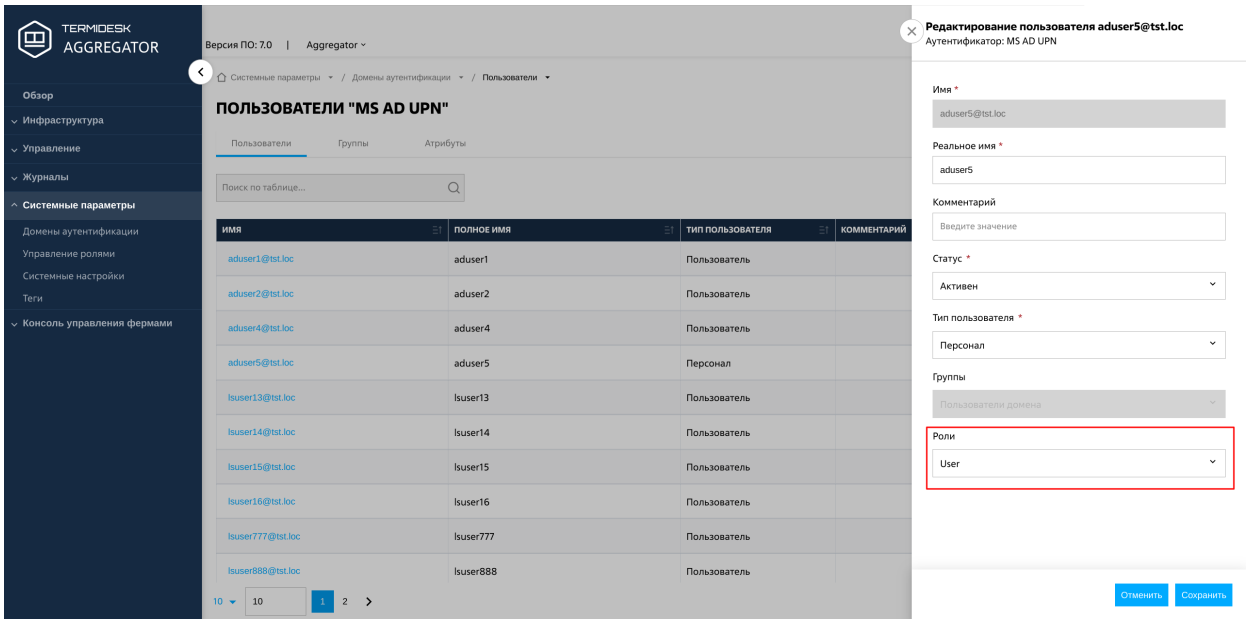


Рисунок 8. Окно назначения пользовательских ролей

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 36. 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		

Параметр	Значение по умолчанию	Описание
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		
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		

Параметр	Значение по умолчанию	Описание
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		
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		

Параметр	Значение по умолчанию	Описание
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
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

Параметр	Значение по умолчанию	Описание
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 устаревших 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 37. 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 38. 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 39. 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 40. 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 41. 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»

Параметр	Описание
«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»
«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 42. 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 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 43. Список типов и шаблонов регистрируемых событий аудита

Событие	Состав регистрируемой информации	Шаблон регистрации события
Базовый класс событий		

Событие	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 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 44. 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
`tdsk_auth list`	Вывод списка доменов аутентификации. Подкоманда `list` принимает аргумент `--output json` для вывода списка в формате JSON

Параметр	Описание
`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).

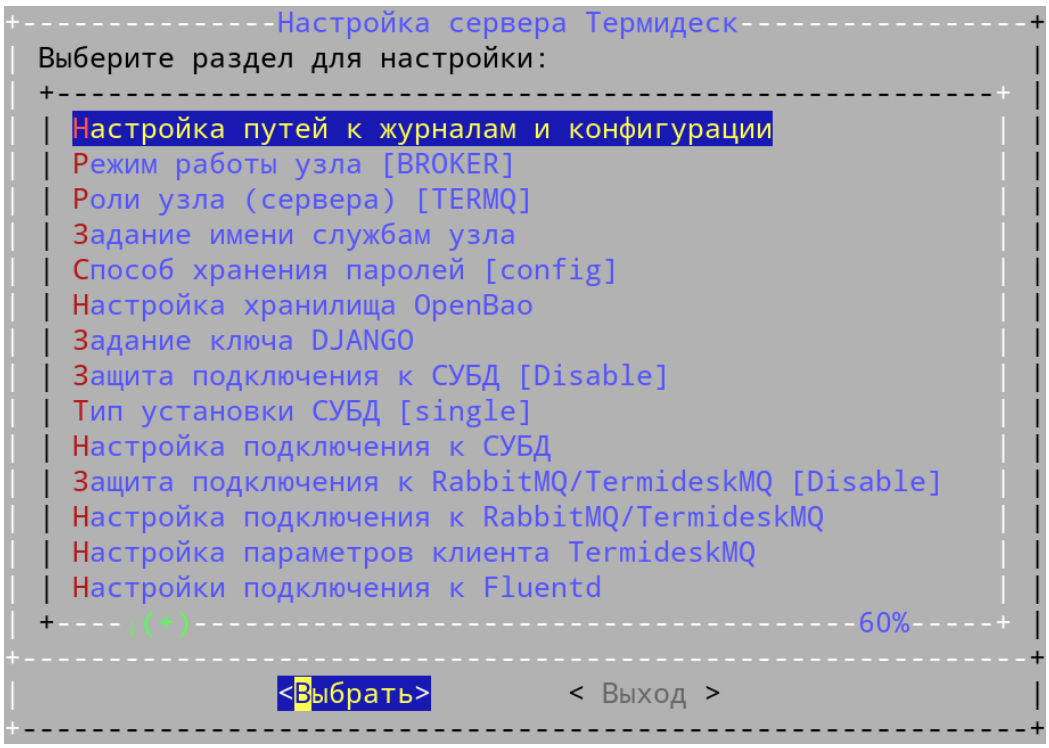


Рисунок 9. Интерфейс утилиты termidesk-config

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 45. 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).

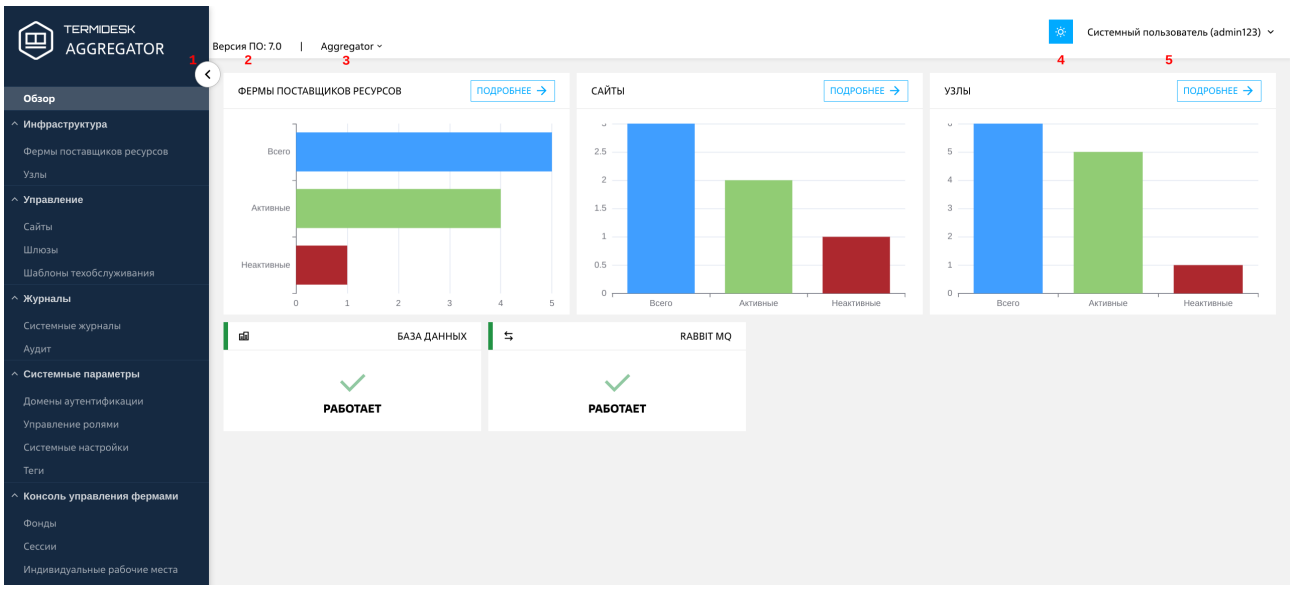


Рисунок 10. Системная панель в графическом интерфейсе управления Termidesk

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.

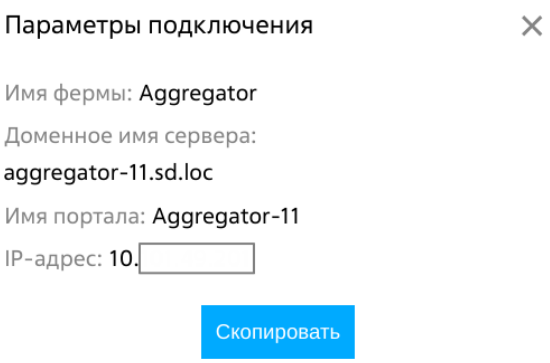


Рисунок 11. Окно сведений о параметрах текущего подключения

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».

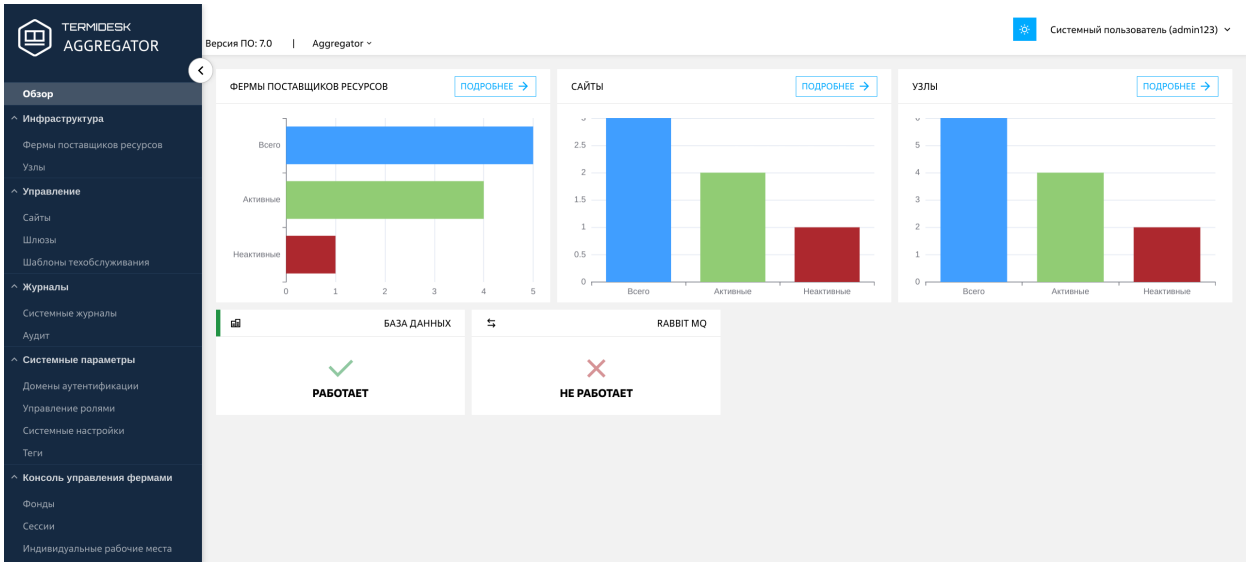


Рисунок 12. Окно функции «Обзор» в графическом интерфейсе управления «Агрегатора»

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 46. Системные настройки журналирования

Параметр	Описание
«Логирование Syslog»	Перенаправление потока событий мониторинга на отдельный syslog-сервер
«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).

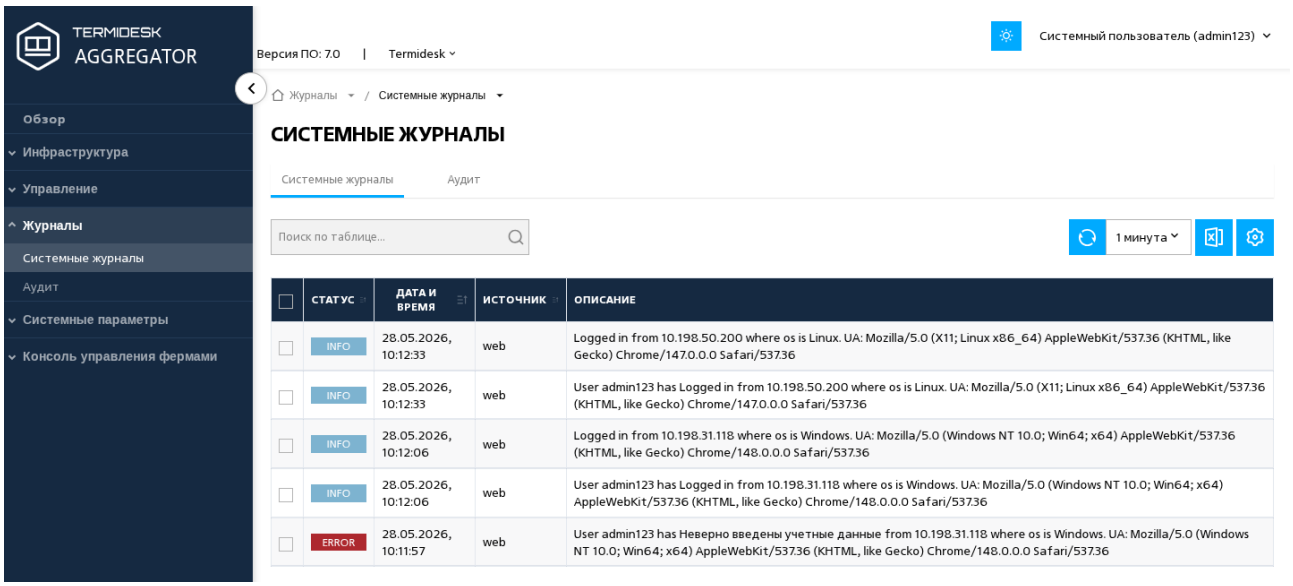


Рисунок 13. Отображение общего журнала событий

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».

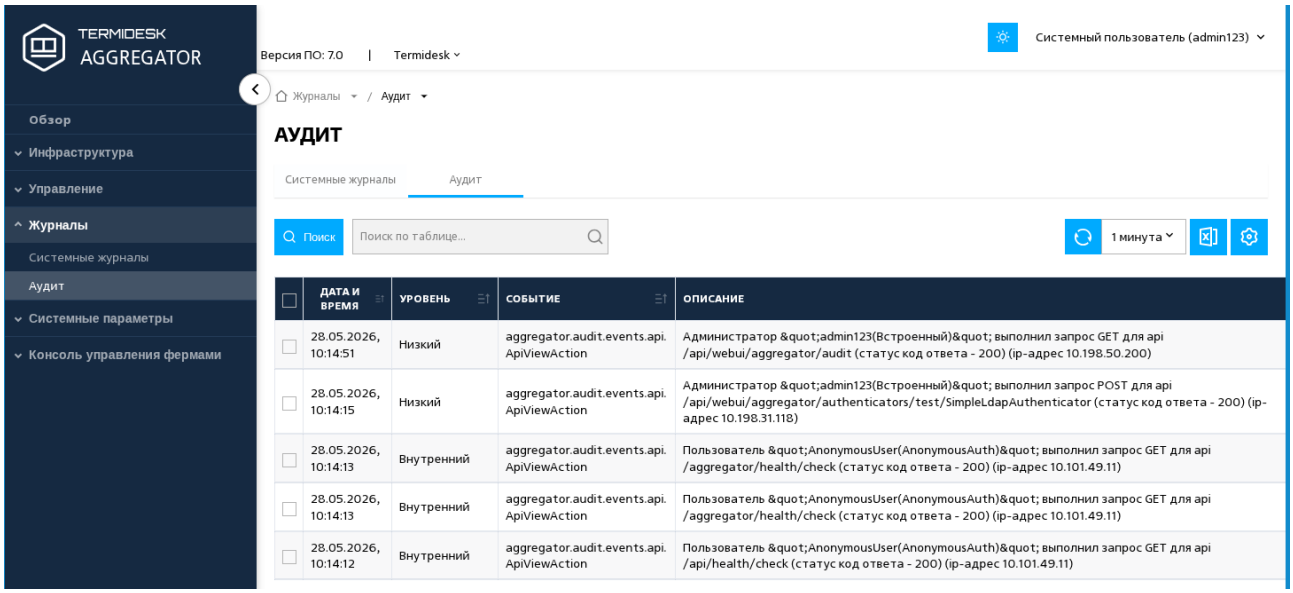


Рисунок 14. Отображение журнала аудита

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

UVEON



© 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