

Инструкция по быстрому запуску СКДПУ НТ Шлюз доступа



Данная инструкция предназначена для администраторов, проводящих первоначальную настройку СКДПУ НТ Шлюз доступа 7 и выше.

Далее в тексте СКДПУ НТ Шлюз доступа для упрощения обозначается как "СКДПУ".

1. Подготовка к проведению работ
 - 1.1. Подключение СКДПУ в исполнении ПАК
 - 1.2. Подключение СКДПУ в исполнении VA
2. Порядок запуска и первоначальной настройки
3. Настройка системы в веб-интерфейсе
 - 3.1. Первичный вход
 - 3.2. Настройка шифрования
4. Системные настройки устройства
 - 4.1. Замена пароля администратора
 - 4.2. Настройка сети
 - 4.3. Настройка подсистемы точного времени
 - 4.4. Настройка подсистемы оповещений
 - 4.5. Подстройка параметров конфигурации для оптимальной работы.
 - 4.6. Завершение первоначальной настройки.
5. Настройка минимальной необходимой политики доступов
6. Соединение через СКДПУ
 - 6.1. Подключение по протоколу RDP
 - 6.2. Подключение по протоколу SSH
7. Аудит сессий пользователей
8. Подключение внешних каталогов пользователей
 - 8.1. Настройки Active Directory для авторизации исполнителей
9. Устранение возможных проблем
 - 9.1. Пароль пользователя admin устарел
 - 9.2. Восстановление пароля учетной записи wabadmin
 - 9.3. Восстановления начального состояния системы

1. Подготовка к проведению работ

Чтобы провести настройки, необходимо подготовить следующие параметры:

- IP адрес, маска подсети и шлюз для настройки на виртуальной машине. Если требуется включение нескольких интерфейсов – подготовить настройки и для них.
- адреса серверов NTP, DNS.
- при наличии источника централизованной авторизации (Active Directory, LDAP и т.п) подготовить адрес и учетные данные для подключения. При использовании Active Directory желательно иметь возможность создать в структуре AD 2-3 группы (Security – Global Distribution) для подключения пользователей с привязкой к группам
- адрес и учетные данные сервера SMTP для отправки уведомлений.
- При необходимости настраивать межсетевые экраны, роутинг и систему виртуализации необходимо обрести соответствующие права или контакты необходимых специалистов.
- Подготовить таблицу с адресами, протоколами доступа и учетными данными на тестовых целевых серверах.
- Подготовить АРМ администратора (обычно это Windows 7, 10. Можно и Linux), где будут доступны современный браузер, ssh и RDP клиенты, почтовый клиент для приема оповещений.

1.1. Подключение СКДПУ в исполнении ПАК

Для подключения СКДПУ в исполнении ПАК к инфраструктуре объекта необходимо:

1. Распаковать ПАК из транспортной тары.
2. Подключить ПАК к сети электропитания.
3. Подключить к разъемам ПАК необходимые периферийные устройства (монитор, клавиатура)
4. Подключить сетевой интерфейс в необходимый коммутатор посредством сетевого кабеля.
5. Подготовить АРМ администратора (обычно это Windows 7-10 или Linux), где будут доступны современный браузер, ssh и RDP клиенты, почтовый клиент для приема оповещений.

1.2. Подключение СКДПУ в исполнении VA

Для подключения СКДПУ в исполнении VA к виртуальной инфраструктуре объекта необходимо:

1. Требуется подготовить целевой сервер системы виртуализации, выделив на нем необходимые ресурсы в зависимости от предполагаемой нагрузки. В минимальной конфигурации параметры следующие: 3-4 ядра, 4-6 Гб RAM, 80 Гб диска, 1 сетевой интерфейс.
2. Скачать и сохранить готовую виртуальную машину по предоставленной ссылке.
3. Импортировать предоставленную виртуальную машину в систему виртуализации.
4. Подключить виртуальный сетевой интерфейс в необходимый виртуальный коммутатор.
5. Подготовить APM администратора (обычно это Windows 7-10 или Linux), где будут доступны современный браузер, ssh и RDP клиенты, почтовый клиент для приема оповещений.

2. Порядок запуска и первоначальной настройки



Данный пункт идентичен для каждого из вариантов исполнения СКДПУ.

Запустить ПАК/виртуальную машину.

1. После подключения к консоли дожидаться приглашения операционной системы.

```
WARNING: Access to this system is restricted to duly authorized users only.  
Any attempt to access this system without authorization or fraudulently  
remaining within such system will be prosecuted in accordance with the law.  
Any authorized user is hereby informed and acknowledges that his/her actions  
may be recorded, retained and audited.  
skdpu login: _
```

2. Ввести логин **wabadmin** и пароль **IQAZ2wsx** и при запросе **integrity level** указать **63**

```
WARNING: Access to this system is restricted to duly authorized users only.  
Any attempt to access this system without authorization or fraudulently  
remaining within such system will be prosecuted in accordance with the law.  
Any authorized user is hereby informed and acknowledges that his/her actions  
may be recorded, retained and audited.  
skdpu login: wabadmin  
Password:  
Integrity level: 63  
Last login: Fri Dec 29 15:40:48 MSK 2023 on tty1  
wabadmin@skdpu:~$ _
```

3. Получить права суперпользователя:

- выполнить команду **super** и ввести пароль **IQAZ2wsx**
- выполнить команду **sudo -i** и снова ввести пароль **IQAZ2wsx**

```
WARNING: Access to this system is restricted to duly authorized users only.
Any attempt to access this system without authorization or fraudulently
remaining within such system will be prosecuted in accordance with the law.
Any authorized user is hereby informed and acknowledges that his/her actions
may be recorded, retained and audited.
skdpu login: wabadmin
Password:
Integrity level: 63
Last login: Fri Dec 29 15:40:48 MSK 2023 on tty1
wabadmin@skdpu:~$ sudo
[sudo] password for wabsuper:
wabsuper@skdpu:/home/wabadmin$ sudo -i
[sudo] password for wabsuper:
root@skdpu:~#
```

4. Настроить сетевой интерфейс в файле /etc/network/interfaces

- открыть файл `/etc/network/interfaces` с помощью текстового редактора (например, nano или vim)

```
[root@skdpu:~# nano /etc/network/interfaces
```

Пример конфигурационного файла для **динамической** IP-адресации:

```
GNU nano 2.7.4 File: /etc/network/interfaces

auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp
```

Пример конфигурационного файла для **статической** IP-адресации:

```
GNU nano 2.7.4 File: /etc/network/interfaces

auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
    address 10.0.128.100
    netmask 255.255.0.0
    gateway 10.0.0.1
```

5. Ввести команду `systemctl restart networking` для перезапуска сетевой службы.

```
[root@skdpu:~# systemctl restart networking
```

6. Ввести команду `ifconfig` для проверки сетевых настроек.

```
root@skdpu:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.128.100 netmask 255.255.0.0 broadcast 10.0.255.255
    ether 00:50:56:96:0d:86 txqueuelen 1000 (Ethernet)
    RX packets 319 bytes 20707 (20.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 21 bytes 1688 (1.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 7722 bytes 974244 (951.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7722 bytes 974244 (951.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

7. После перезагрузки системы проверить SSH-соединение к консоли СКДПУ при помощи команды `ssh wabadmin@<ip-адрес хоста> -p 2242`

```
C:\Users\Администратор>ssh wabadmin@10.0.128.100 -p 2242
The authenticity of host '[10.0.128.100]:2242 ([10.0.128.100]:2242)' can't be established.
ECDSA key fingerprint is SHA256: [REDACTED]
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.0.128.100]:2242' (ECDSA) to the list of known hosts.
wabadmin@10.0.128.100's password:
Last login: Mon Jan  8 21:13:28 2024 from 172.16.136.246
wabadmin@skdpu:~$
```

8. Проверить доступность web-интерфейса, перейдя по IP-адресу хоста СКДПУ в браузере АРМ администратора (см. следующий пункт).

3. Настройка системы в веб-интерфейсе

3.1. Первичный вход

Пройдите по ссылке <https://<ip хоста СКДПУ>>

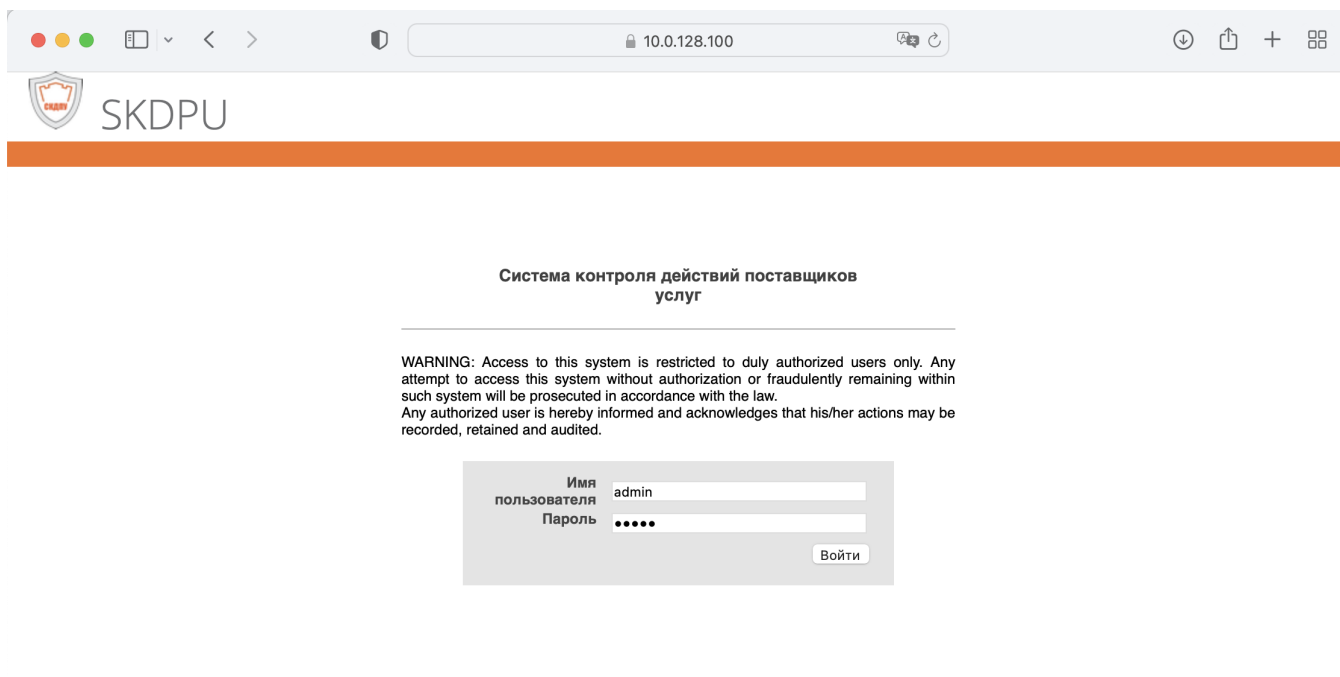


Параметры доступа по умолчанию

Логин – *admin*

Пароль – *admin*

Откроется интерфейс первичной инициализации устройства.

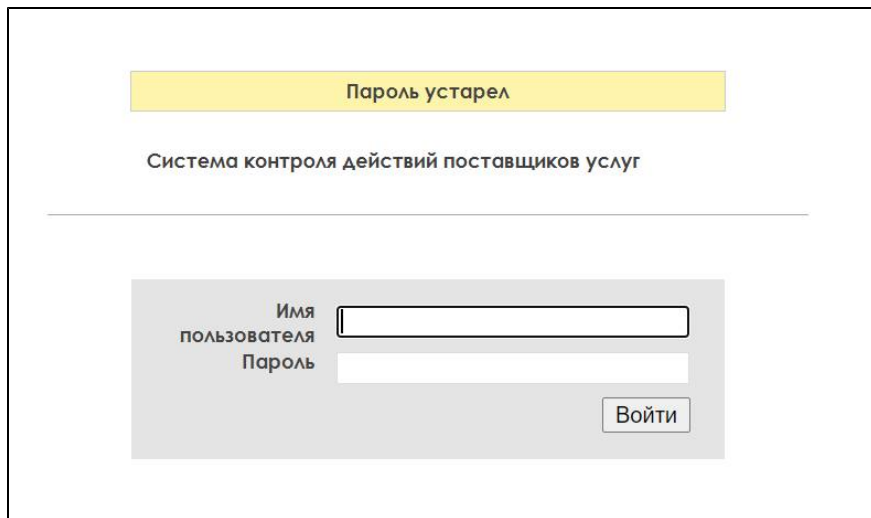


Система контроля действий поставщиков услуг

WARNING: Access to this system is restricted to duly authorized users only. Any attempt to access this system without authorization or fraudulently remaining within such system will be prosecuted in accordance with the law. Any authorized user is hereby informed and acknowledges that his/her actions may be recorded, retained and audited.

Имя пользователя: admin
Пароль:
Войти

Если этого не произошло, а появилось предупреждение "Пароль устарел", необходимо выполнить рекомендации раздела **"Устранение возможных проблем"** данной инструкции.



Пароль устарел

Система контроля действий поставщиков услуг

Имя пользователя:
Пароль:
Войти

3.2. Настройка шифрования

Настройка данного параметра обеспечивает повышенный уровень защищенности данной системы, препятствующий восстановлению и доступу к данным в случае несанкционированного доступа к резервным копиям, а также к самой ВМ системы.



В случае утери ранее введенной **Passphrase** восстановление и доступ к БД системы будет невозможен!

В демо-зонах шифрование диска рекомендуется не применять, поэтому выберите пункт **No, i don't need...** и нажмите **Send**.

В случае если данный параметр является требованием безопасности – введите **Passphrase** и нажмите **Send**.


SKDPU

admin (eth0)
Bastion Super Administrator

Configuration **Encryption**

Configuration
Encryption

The page you requested is unavailable, you must configure encryption

Encryption on SKDPU

The SKDPU encryption feature secures sensitive data (target account passwords, etc...) by using a strong cryptographic algorithm. The algorithm relies on a confidential encryption key unique to your SKDPU.

The definition of a passphrase involves a more complex access to SKDPU and raises the protection of your data as no malicious user who does not know the passphrase can access your product. Moreover, at each system reboot, connections using SKDPU proxies will not be usable as long as the passphrase is not entered by an administrator in the Web administration interface and only a subset of administration tasks would be authorized.

After the encryption initialization phase, we recommend you to back up SKDPU at least once to keep a copy of the encryption key in a safe place. If you do not perform this action, you would be at risk of not being able to access your data on remote storage if the key is lost.

Need first initialization

Please enter a passphrase to protect your system.
(This passphrase will be prompted to unlock your system after each reboot.)

Passphrase:

Passphrase confirmation:

No, I do not need a passphrase protection: ☒

Send

С этого момента активируется демо-лицензия и будет доступен полный функционал системы в течение 30 дней, для 5 сессий и 15 устройств.

При необходимости обратитесь за расширенной демо-лицензией по email support@it-bastion.com.

Далее, необходимо установить системные настройки устройства (см. следующий пункт)

4. Системные настройки устройства

4.1. Замена пароля администратора

В разделе **My Preferences** укажите email администратора, необходимый язык интерфейса и примените настройки.



SKDPU

admin (eth0)
 Bastion Super Administrator
 

My Preferences
 

My Preferences
 My Authorizations
 Audit
 Users
 Resources
 Password Management
 Session Management
 Authorizations
 Configuration
 System
 Import/Export

Profile

User name *: admin

Display name: Bastion Super Administrator

Preferred language *: Русский 

Email *: delfinaz02@icloud.com

User's preferred language
User's email

Apply

SKDPU password

Current password *:

New password *:

Password policy: at least 8 characters, at least 1 upper case letters, at least 1 lower case letters, at least 1 digits, at least 1 special characters, different from the last 4 passwords, different from the user name

Apply

Далее, смените пароль с дефолтного на подходящий для администратора. Система не даст сохранить слабый пароль.



SKDPU

admin (eth0)
 Bastion Super Administrator
 

Мои настройки
 

Мои настройки
 Мои авторизации
 Аудит
 Пользователи
 Ресурсы
 Управление паролями
Плагины изменения паролей
 Политики замены паролей
 Управление сессиями
 Авторизации
 Конфигурация
 Система
 Импорт/Экспорт

 Обновлены настройки пользователя 'admin'

Профиль

Имя пользователя *: admin

Видимое имя: Bastion Super Administrator

Предпочитаемый язык *: Русский 

Емейл *: delfinaz02@icloud.com

Предпочитаемый язык
email пользователя

Применить

Пароль SKDPU

Текущий пароль *:

Новый пароль *:

Политика паролей: минимум 8 символов, минимум 1 больших букв, как минимум 1 букв нижнего регистра, минимум 1 цифр, минимум 1 специальных символов, не совпадать с 4 крайними паролями, отличаться от имени пользователя

Применить

При необходимости, Вы можете изменить локальную политику паролей СКДПУ в разделе **Configuration → Local Password Policy**



SKDPU

admin (eth0)
 Bastion Super Administrator



Конфигурация

Локальная политика паролей




Мои настройки

Мои авторизации

Аудит

Пользователи

Ресурсы

Управление паролями

Управление сессиями

Авторизации

Конфигурация

Периоды времени

Внешние авторизации

Домены LDAP/AD

Уведомления

Локальная политика паролей

Сообщения соединения

X509 параметры

Настройки

API ключи

Лицензия

Шифрование

Собственный аудит

Система

Импорт/Экспорт

Редактировать политику паролей: default

Устаревание пароля * : 365
в днях. 0 означает - не устаревает.

Показывать предупреждение пользователю * : 20
в днях. 0 означает - не предупреждать.

Минимальная длина пароля * : 8

Макс. число ошибок авторизации для пользователя * : 5
0 означает без ограничений

Минимальное число букв нижнего регистра * : 1

Минимальное число спец-символов * : 1

Минимальное число больших букв * : 1

Минимальное число цифр * : 1

Число ранее действовавших паролей для контроля * : 4
между 0 и 15, 0 значит не отклонять

Имя пользователя и пароль могут совпадать * : ☐

Словарь запрещенных паролей :

файл не выбран

одно слово на строку

RSA
 ED25519
 ECDSA NIST p256
 ECDSA NIST p384
 ECDSA NIST p521

Разрешенные алгоритмы публичных ключей SSH :

Удерживайте CTRL для выбора нескольких значений

Минимальная длина ключа RSA * : 4096

Отменить

Применить

4.2. Настройка сети

В разделе **Система** → **Сеть** проверьте настройки сетевых интерфейсов.

Сетевая конфигурация для **динамической** IP-адресации:



SKDPU

admin (eth0)
Bastion Super Administrator

Система **Сеть**


Мои настройки

Мои авторизации

Аудит

Пользователи

Ресурсы

Управление паролями

Управление сессиями

Авторизации

Конфигурация

Система

Статус

Сеть

Сервис времени

Удаленное хранилище

Интеграция с SIEM

SNMP

Почтовый сервер

Управление сервисами

Syslog

Отчет по запуску

Резервные копии

Импорт/Экспорт

Сетевая конфигурация

Имя			
Имя хоста	alicia		
URL / Уведомления			
Доменное имя (FQDN)			
Полное имя домена (FQDN) для использования в уведомлениях (синхронизировано с другой нодой когда HA включен).			
Интерфейсы			
Имя интерфейса	DHCP	IP адрес	Маска сети
☒ eth0	Да		
Интерфейсы VLAN			
Физические интерфейсы	Метки VLAN	Адрес	Маска сети
eth0			
Виртуальные интерфейсы			
Физические интерфейсы	Имя	Адрес	Маска сети
eth0			
Маршруты			
Исходящий интерфейс по умолчанию	Шлюз		
Имя интерфейса	Сеть	Маска сети	Шлюз
eth0			
/etc/hosts			
Имя хоста	IP		
alicia	127.0.1.1		
localhost	127.0.0.1		
DNS			
Доменное имя			
Поиск			
Список серверов			
	172.16.30.54		
	8.8.8.8		
	172.16.30.55		

Применить

Сетевая конфигурация для **статической** IP-адресации:



SKDPU

admin (eth0)
Bastion Super Administrator



Система

Сеть

Мои настройки

Мои авторизации

Аудит

Пользователи

Ресурсы

Управление паролями

Управление сессиями

Авторизации

Конфигурация

Система

Статус

Сеть

Сервис времени

Удаленное хранилище

Интеграция с SIEM

SNMP

Почтовый сервер

Управление сервисами

Syslog

Отчет по запуску

Резервные копии

Импорт/Экспорт

Сетевая конфигурация

Имя

Имя хоста

URL / Уведомления

Доменное имя (FQDN)

Полное имя домена (FQDN) для использования в уведомлениях (синхронизировано с другой нодой когда HA включен).

Интерфейсы

Имя интерфейса ☐ DHCP

IP адрес

Маска сети

Интерфейсы VLAN

Физические интерфейсы

Метки VLAN

Адрес

Маска сети

Виртуальные интерфейсы

Физические интерфейсы

Имя

Адрес

Маска сети

Маршруты

Исходящий интерфейс по умолчанию

Шлюз

Имя интерфейса

Сеть

Маска сети

Шлюз

/etc/hosts

Имя хоста

IP

alicia 10.0.128.100

localhost 127.0.0.1

DNS

Доменное имя

Поиск

Список серверов

172.16.30.54

8.8.8.8

172.16.30.55

4.3. Настройка подсистемы точного времени

Рекомендуется указать действующий сервер точного времени для устройства в разделе **Система** → **Сервис времени**, т. к. от актуальности настроек времени будет зависеть стабильная работа смежных систем, например, передача логов во внешние SIEM-системы.



SKDPU

admin (eth0)
 Bastion Super Administrator



Система

Сервис времени




Мои настройки

Мои авторизации

Аудит

Пользователи

Ресурсы

Управление паролями

Управление сессиями

Авторизации

Конфигурация

Система

Статус

Сеть

Сервис времени

Удаленное хранилище

Интеграция с SIEM

SNMP

Почтовый сервер

Управление сервисами

Syslog

Отчет по запуску

Резервные копии

Импорт/Экспорт

Настройки времени

Таймзона:

Europe/Moscow

Статус:

Включено

Сервера NTP

✓ 172.16.30.55
+
−

Применить

4.4. Настройка подсистемы оповещений

В разделе **Система** → **Почтовый сервер** укажите настройки почтовой подсистемы. Здесь же можно отправить тестовое сообщение для проверки.

В настройках в СКДПУ 7 присутствует так же строка хэш сертификата. При использовании зашифрованного соединения с сервером почты, для того что бы сверять сертификат система запоминает его хэш. Для получения хэша есть кнопка **"Проверить сертификат"**. После связи и авторизации на целевом сервере система записывает себе данные сертификата.



Не нужно пытаться в ручную прописать контрольную сумму сертификата - это неверные данные. Если система по какой-то причине не получила хэш сертификата, проверьте корректность указанных параметров почтового сервера и данные авторизации на нем. В случае использования символического имени – проверьте, настроен ли DNS.



SKDPU

admin (eth0)
Bastion Super Administrator


Система Почтовый сервер
1 ?

Мои настройки

Мои авторизации

Аудит

Пользователи

Ресурсы

Управление паролями

Управление сессиями

Авторизации

Конфигурация

Система

Статус

Сеть

Сервис времени

Удаленное хранилище

Интеграция с SIEM

SNMP

Почтовый сервер

Управление сервисами

Syslog

Отчет по запуску

Резервные копии

Импорт/Экспорт

Настройка почтового сервиса

Протокол * :
 Метод авторизации * :
 Сервер * :
 Порт * :
 Email Постмастера * :
 Имя отправителя * :
 Хэш сертификата :
 Адрес отправителя * :
 Пользователь :
 Пароль :
 Адреса получателя для проверки :

SMTPS
 Automatic
 smtp.yandex.ru
 465
 support@it-bastion.com
 it-bastion
 15:9C:6B:17:B7:B0:B9:BA:E0:21:D8:A3:80:1E:44:7E:A9:B9:F6:07:58:A9:E0:20:C9:02:16:B4:C3:F7:60:12
 support@it-bastion.com
 support@it-bastion.com

 example@example.com

Адреса получателя надо разделять ";"

Проверить сертификат
Проверка
Отменить
Применить

4.5. Подстройка параметров конфигурации для оптимальной работы.

В разделе **Конфигурация** → **Настройки** выберите раздел **RDP proxy**. В секции [video] переключите значения в 0.

[video]

Smart video cropping : ☒ 0
☐ 1
☐ 2

0: Disabled. When replaying the session video, the content of the RDP viewer matches the size of the client's desktop
 1: When replaying the session video, the content of the RDP viewer is restricted to the greatest area covered by the application during session
 2: When replaying the session video, the content of the RDP viewer is fully covered by the size of the greatest application window during session
 Option [default: 0]

[remote_program]

Allow resize hosted desktop : ☒

Boolean [default: True]

Отменить
Применить

Если Вы работаете на компьютере с операционной системой MacOS, необходимо в этом же разделе в секции [client] установить значение "Enable new pointer update"

[client]

Tls fallback legacy :

☐

Fallback to RDP Legacy Encryption if client does not support TLS.
Boolean [default: False]

Tls support :

☒

Boolean [default: True]

Tls min level :

2

Minimal incoming TLS level 0=no restriction (TLSv1.0), 1=TLSv1.1, 2=TLSv1.2
Integer ≥ 0 [default: 2]

Enable suppress output :

☒

Boolean [default: True]

Ssl cipher list :

HIGH:!ADH:!3DES:!SHA

[Not configured]: Compatible with more RDP clients (less secure)
HIGH:!ADH:!3DES: Compatible only with MS Windows 7 client or more recent (moderately secure)
HIGH:!ADH:!3DES:!SHA: Compatible only with MS Server Windows 2008 R2 client or more recent (more secure)
String [default: "HIGH:!ADH:!3DES:!SHA"]

Show target user in f12 message :

☐

Boolean [default: False]

Enable new pointer update :

☒

Boolean [default: False]

Bogus ios glyph support level :

☒

Boolean [default: True]

Bogus number of fastpath input event :

☐ 0
☒ 1
☐ 2

0: disabled
1: pause key only
2: all input events
Option [default: 1]

Bogus pointer xormask padding :

☐

Boolean [default: False]

В разделе **Конфигурация** → **Настройки** выберите раздел **GUI**. Укажите оптимальное разрешение для окон RDP клиента. В версии 7 можно задать несколько доступных разрешений экрана.


SKDPU

admin (eth0)
Bastion Super Administrator

Конфигурация

Настройки

Мои настройки

Мои авторизации

Аудит

Пользователи

Ресурсы

Управление паролями

Управление сессиями

Авторизации

Конфигурация

Периоды времени

Внешние авторизации

Домены LDAP/AD

Уведомления

Локальная политика паролей

Сообщения соединения

X509 параметры

Настройки

API ключи

Лицензия

Шифрование

Собственный аудит

Конфигурация: GUI

☒ Подсказка по опциям
☐ Сложные настройки

[main]

Session timeout :

900

Session timeout (in seconds).
Integer ≥ 300 [default: 900]

Session cookie age :

900

Cookie age (in seconds).
Integer ≥ 300 [default: 900]

New local account notification :

☒

Send a notification email to the user when a new local account is created.
Boolean [default: True]

Rdp resolutions :

800x600,1024x768*,1280x1024,1600x1200,1920x1080,fullscreen,multimonitor,custom

List of pre-defined RDP resolutions; if a resolution ends with a "*" (star), it is used as default resolution.
Format: comma-separated list of values with format: WxH where W=width and H=height.
Special values allowed: "fullscreen" for fullscreen session, "multimonitor" to support multiple monitor session, "custom" to let the user choose another resolution.
String [default: "800x600,1024x768",1280x1024,1600x1200,1920x1080,fullscreen,multimonitor,custom"]

Rdp color bpp :

☐ 8
☒ 16
☐ 24
☐ 32

Default RDP color depth (bits per pixel).
Option [default: 16]

Если Вы работаете на компьютере с операционной системой MacOS, потребуется в этом же разделе для параметра "Rdp other os filetype" выставить значение "rdp" для просмотра сессий RDP

Rdp connection links:

☐ standard
☐ otp
☒ both

The links displayed for RDP connections on page "My authorizations":
- standard: connection with password
- otp: one-time password (direct access)
- both: display both links
Option [default: both]

Ssh connection links:

☐ standard
☐ otp
☒ both

The links displayed for SSH/RLOGIN/TELNET connections on page "My authorizations":
- standard: connection with password
- otp: one-time password (direct access)
- both: display both links
Option [default: both]

Rdp windows filetype:

☒ rdp
☐ rdesktop
☐ xfreerdp
☐ remmina

Downloadable file type on Windows platform for RDP sessions.
Option [default: rdp]

Rdp other os filetype:

☒ rdp
☐ rdesktop
☐ xfreerdp
☐ remmina

Downloadable file type on other platforms for RDP sessions.
Option [default: rdesktop]

Rdp remote app mode:

☒

Use Remote Application mode with MSTSC client.
This is used only for connections to applications.
Boolean [default: True]

Rdp enable sessions split:

☒

Create distinct session for each user application
Boolean [default: True]

Ssh windows filetype:

☒ wallix-putty
☐ Xshell
☐ ssh

Downloadable file type on Windows platform for SSH sessions.
Option [default: wallix-putty]

Ssh other os filetype:

☐ wallix-putty
☒ ssh

Downloadable file type on other platforms for SSH sessions.
Option [default: ssh]

Connection file fqdn standard:

If set, force Bastion FQDN in RDP/SSH files downloaded on page "My authorizations" (standard mode: no OTP).
If not set, the HTTP_HOST received in request is used.
String

Connection file fqdn otp:

If set, force Bastion FQDN in RDP/SSH files downloaded on page "My authorizations" (OTP).
If not set, the HTTP_HOST received in request is used.
String

Ssh session record timestamp:

☐

Add timestamp in SSH session record (text).
Boolean [default: False]

Self authorizations last connection: date

☒

Display the date in column Last connection on page My Authorizations / Sessions.
In case of latency period due to large volume of sessions, disable the option to improve page load performance.
Boolean [default: True]

Отменить

Применить

Настройка разрешения экрана при подключении к сессии производится в разделе Мои авторизации → Сессии во вкладке "Настройки".

Мои настройки

Мои авторизации

Сессии

Пароли

Аудит

Пользователи

Ресурсы

Управление паролями

Управление сессиями

Авторизации

Конфигурация

Система

Импорт/Экспорт

Мои авторизации

Сессии

Настройки

Разрешение: 1024x768

Глубина цвета (бит):

Показать 10 записей

Протоколы

Цель

Имя авторизации

0 - 0 / 0

Запросы подтверждения

Показать элементы 10

Отменить

Цель

Начало

Длительность

Тикет

Кворум

Статус

Ответы

0 - 0 / 0

admin (eth0)

Bastion Super Administrator

RDP: 1024x768, 32 bpp

800x600

✓ 1024x768

1280x1024

1600x1200

1920x1080

Полный экран

Все мониторы

свой

Поиск:

Подтверждения

В разделе **Управление сессиями** → **Параметры соединения** → **RDP** переключите в секции **[session_probe]** параметры **"On launch failure"** и **"On keepalive timeout"** на 0

[session_probe]

Enable session probe:

☒

Boolean [default: True]

Use smart launcher:

☒

Minimum supported server : Windows Server 2008.
Clipboard redirection should be remain enabled on Terminal Server.
Boolean [default: True]

On launch failure:

0 1 2

Behavior on failure to launch Session Probe.
0: ignore failure and continue.
1: disconnect user.
2: reconnect without Session Probe.
Option [default: 1]

Start launch timeout timer only after:
logon

☒

Minimum supported server : Windows Server 2008.
Boolean [default: True]

On keepalive timeout:

0 1 2

0: ignore and continue
1: disconnect user
2: freeze connection and wait
Option [default: 1]

End disconnected session:

☐

End automatically a disconnected session.
Session Probe must be enabled to use this feature.
Boolean [default: False]

Public session:

☐

If enabled, disconnected session can be recovered by a different primary user.
Boolean [default: False]

Outbound connection monitoring:
rules

Comma-separated rules (Ex.: \$deny:192.168.0.0/24:*,\$allow:host.domain.net:3389,\$allow:192.168.0.110:*)
(Ex. for backwards compatibility only: 10.1.0.0/16:22)
Session Probe must be enabled to use this feature.
String

Если позволяют политики безопасности в контуре инфраструктуры, можно выключить строгий контроль TLS-сертификатов в RDP-сессиях. Для этого в разделе **Управление сессиями** → **Параметры соединения** → **RDP** переключите в секции **[server_cert]** параметр **"Server cert check"** на 3. Это позволит избежать ошибки подключения и невозможности установить сессию в случае, если на стороне контролируемого целевого устройства изменился сертификат.

Страница 15

[server_cert]

Server cert store:
☒

Keep known server certificates on WAB
Boolean [default: True]

Server cert check:
☐ 0
☐ 1
☐ 2
☒ 3

Behavior of certificates check.
0: fails if certificates doesn't match or miss.
1: fails if certificate doesn't match, succeed if no known certificate.
2: succeed if certificates exists (not checked), fails if missing.
3: always succeed.
System errors like FS access rights issues or certificate decode are always check errors leading to connection rejection.
Option [default: 1]

4.6. Завершение первоначальной настройки.

На данном шаге, СКДПУ НТ Шлюз доступа готов к работе. Рекомендуется сделать снимок (snapshot) в рамках системы виртуализации и продолжать настройки в части политики.

При необходимости возможно сменить пароли для системных пользователей wabadmin, wabsuper в консоли системы – от root с помощью команд passwd wabadmin, passwd wabsuper.

Рекомендуется новые пароли записать и сохранить в сейф – они потребуются для эксплуатации системы в дальнейшем и восстанавливать их нетривиально.

ВАЖНО. Все пароли системы по умолчанию чувствительны к перебору и блокируются после 5 попыток

5. Настройка минимальной необходимой политики доступов

Добавление пользователей, устройств, групп и авторизаций.

В разделе **Пользователи** → **Аккаунты** создать пользователя с правами администратора (WAB_administrator). Авторизация "local" уже выбрана по умолчанию, поэтому нужно задать новому пользователю пароль в разделе **"Локальная авторизация"**.



Примечание

Здесь и далее примером дополнительной учётной записи с правами администратора используется **adm.alicia**


SKDPU

admin (eth0)
Bastion Super Administrator

Пользователи
Аккаунты

Мои настройки
Мои авторизации
Аудит
Пользователи
Аккаунты
Группы
Профили
Ресурсы
Управление паролями
Управление сессиями
Авторизации
Конфигурация

Редактировать пользователя

Имя пользователя *: adm.alicia

Видимое имя: Admin Alicia

Адрес отправителя *: support@it-bastion.com
email пользователя

GPG ключ:

Выбрать файл
файл не выбран

Предпочитаемый язык *: Русский
Предпочитаемый язык

Профиль *: WAB_administrator

Выключено:
☐

- Конфигурация
- Система
- Импорт/Экспорт

Выключено: ☐

Дата:
YYYY-MM-DD hh:mm
Группы:
Группы пользователя

Доступно Группы

Выбрано Группы

Сервера:
Список источников авторизации для проверки пароля
резервного копирования *

Доступно Аутентификация

Выбрано авторизаций

Локальная авторизация

Пароль:

Политика паролей: минимум 8 символов, минимум 1 больших букв, как минимум 1 букв нижнего регистра, минимум 1 цифр, минимум 1 специальных символов, не совпадать с 4 крайними паролями, отличаться от имени пользователя

Требовать смены пароля:

Загрузить публичный ключ: файл не выбран

Или вставить публичный ключ:

Ограничения по IP:

В разделе **Пользователи** → **Группы** создать группу, например **"Local_skdpu_users"**, и добавить в нее пользователей **admin**, **adm.alicia**


SKDPU

admin (eth0)
 Bastion Super Administrator

Пользователи

Группы

Мои настройки

Мои авторизации

Аудит

Пользователи

Аккаунты

Группы

Профили

Ресурсы

Управление паролями

Управление сессиями

Авторизации

Конфигурация

Система

Импорт/Экспорт

Добавить группу пользователей

Имя группы *: Local_skdpu_users
 Описание :

Периоды : allthetime
 времени :

Пользователи

Доступно Пользователи

⌵ Выбрать все

Выбрано Пользователи

adm.alicia
 admin

⌵ Удалить все

Действие Правила Подпротокол
 kill SSH_SHELL_SESSION / X11_SESSION

Отменить

Применить

В разделе **Ресурсы** → **Устройства** необходимо добавить профиль соединения с RDP хостом.

Указать **адрес** Вашего хоста RDP, в локальные домены занести строку **"local"**, выбрать протокол **RDP** и применить настройки устройства


SKDPU

admin (eth0)
Bastion Super Administrator

Ресурсы **Устройства**

Мои настройки
Мои авторизации
Аудит
Пользователи
Ресурсы
Домены
Устройства
Приложения
Аккаунты
Кластеры
Группы
Плагин хранения паролей
Политики выборки
Управление паролями
Управление сессиями
Авторизации
Конфигурация
Система
Импорт/Экспорт

Создать устройство

Устройство

Название * :

Алиас :

Хост устройства * :

Описание :

Локальные домены :

Название * :

local

Сервисы

Создать сервис от одного из протоколов:

VNC RDP RLOGIN TELNET SSH RAWTCP

RDP имя сервиса * : Порт * :

Свойства прокси: ☒ RDP_CLIPBOARD_UP ☒ RDP_CLIPBOARD_DOWN ☒ RDP_CLIPBOARD_FILE ☒ RDP_PRINTER ☒ RDP_COM_PORT ☒ RDP_DRIVE ☒ RDP_SMARTCARD ☒ RDP_AUDIO_OUTPUT

политика соединений * :

глобальные домены:

Удалить: ☐

Отменить Применить

Далее можно добавить учетную запись для соединения с целевым сервером и повышения прав исполнителя


SKDPU

admin (eth0)
Bastion Super Administrator

Ресурсы **Устройства**

Мои настройки
Мои авторизации
Аудит
Пользователи
Ресурсы
Домены
Устройства
Приложения
Аккаунты
Кластеры
Группы
Плагин хранения паролей
Политики выборки
Управление паролями
Управление сессиями
Авторизации
Конфигурация
Система
Импорт/Экспорт

Данные сохранены

Редактировать это устройство

Имя устройства : WindowsServer

Алиас : --

Хост устройства : 10.0.128.81

Описание : --

Локальные домены : local

Сервисы RDP :

RDP / 3389

RDP_CLIPBOARD_UP / 3389

RDP_CLIPBOARD_DOWN / 3389

RDP_PRINTER / 3389

RDP_COM_PORT / 3389

RDP_DRIVE / 3389

RDP_SMARTCARD / 3389

RDP_CLIPBOARD_FILE / 3389

RDP_AUDIO_OUTPUT / 3389

Учетные записи устройств

+ Добавить учетную запись

Связанные учетки

управление ассоциациями

Сертификаты на устройстве

Внесите данные **учетной записи целевого устройства** и сохраните. Обычно добавляют **административные** УЗ, чтобы не выдавать на руки исполнителям пароли от них.


SKDPU

admin (eth0)
Bastion Super Administrator

Ресурсы

Устройства

Мои настройки

Мои авторизации

Аудит

Пользователи

Ресурсы

Домены

Устройства

Приложения

Аккаунты

Кластеры

Группы

Плагины хранения паролей

Политики выборки

Управление паролями

Управление сессиями

Авторизации

Конфигурация

Система

Импорт/Экспорт

Редактировать учетку Администратор

Вернуться к сводной справке по устройству: WindowsServer

Тип аккаунта * : Устройство

Устройство : WindowsServer

Локальный домен : local

Название * : Администратор

Логин * : скопировать из имени ☒

Администратор

Описание :

Пароль :

.....

.....

Закрытый ключ SSH :

Сгенерировать закрытый ключ

--- Выберите ---

Закачать закрытый ключ SSH:

Выбрать файл

файл не выбран

Автозамена пароля :

☐

Снимите выделение чтобы полностью отключить замену паролей для этой УЗ

Автозамена ключа SSH :

☐

Снимите выделение чтобы полностью отключить замену ключей SSH для этой УЗ

Политика вскрытия :

default

Добавить/Удалить связь с ресурсом

Доступные ресурсы

Q

Выбрать все

Выбранные ресурсы

Q

Выбрать и кликнуть

WindowsServer:RDP

Удалить все

Отменить

Применить

Добавленная учетная запись должна выглядеть следующим образом

Учетные записи устройств

+ Добавить учетную запись

Показать элементы 10

Поиск:

	Имя аккаунта	Домен	Описание
☐	Администратор	local	

1 - 1 / 1

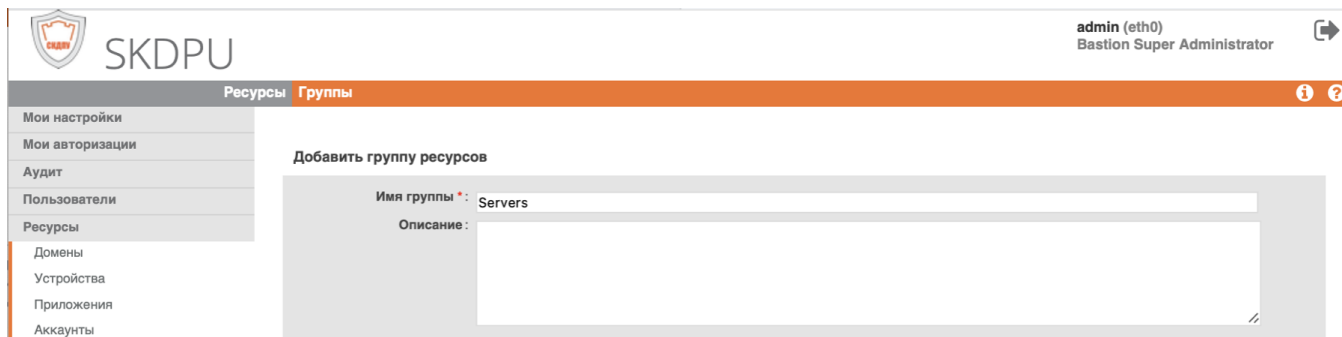
Система поддерживает 3 варианта доступа к системе:

- При входе по сохраненной УЗ (по учетной записи управления сессиями и учётке сценария) целевой вход будет от пользователя Администратор@local в нашем примере (предполагается, что такая УЗ на целевой системе есть).
- При входе через маппинг аккаунтов вход будет от УЗ, с которой пользователь вошел на СКДПУ (admin или adm.alicia в нашем примере, предполагается, что такие УЗ присутствуют в целевой системе).

Страница 20

- При **интерактивном входе** СКДПУ используется последовательная авторизация при условии, что пользователь знает УЗ локального пользователя СКДПУ и, в нашем случае, УЗ AD Windows Server. *СКДПУ будет записывать все действия при таком входе.

В разделе **Ресурсы** → **Группы** добавим группу ресурсов **"Servers"**.



SKDPU admin (eth0) Bastion Super Administrator

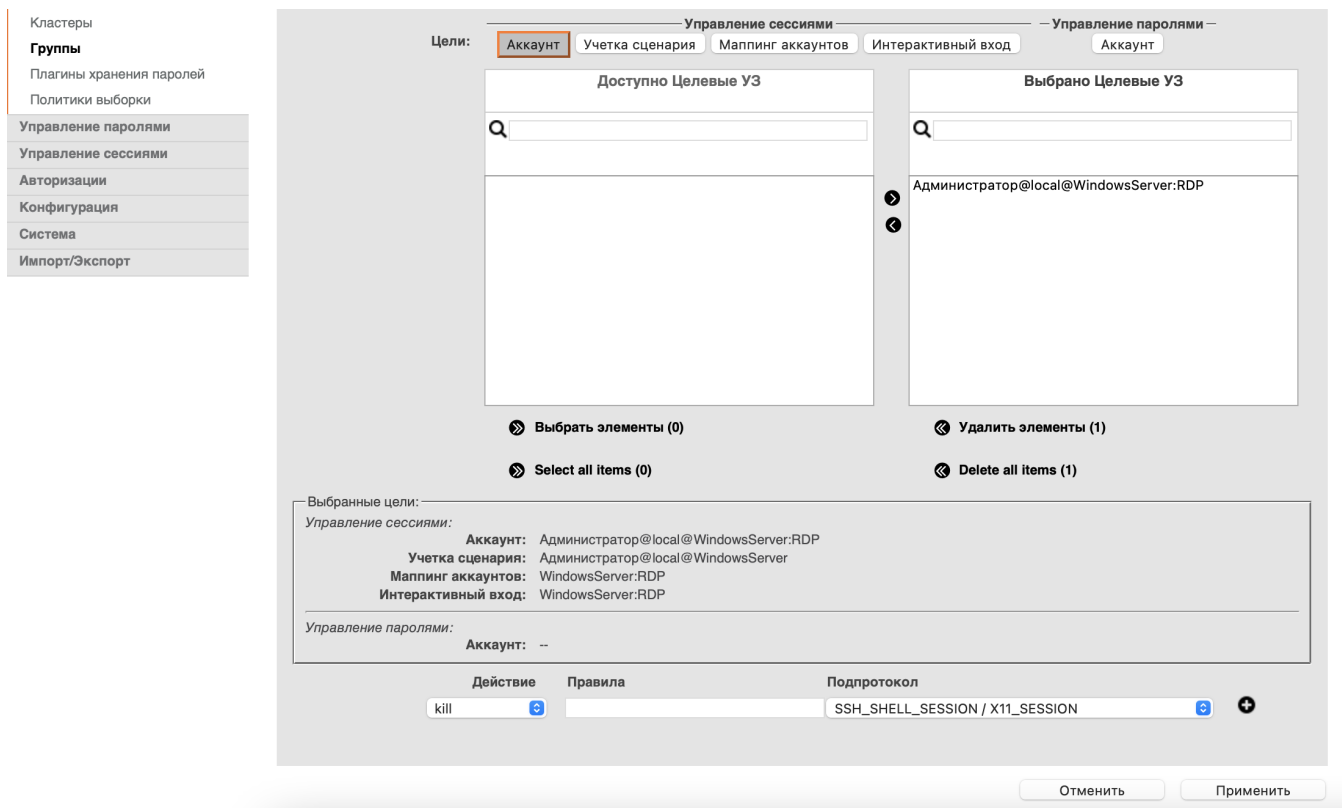
Ресурсы Группы

Добавить группу ресурсов

Имя группы *: Servers

Описание:

Добавить **разрешения** использовать ресурс. Можно добавить любое сочетание вариантов доступа к системе для каждого хоста.



Классеры Группы

Плагин хранения паролей Политики выборки

Управление паролями Управление сессиями Авторизации Конфигурация Система Импорт/Экспорт

Цели: Аккаунт Учетка сценария Маппинг аккаунтов Интерактивный вход Аккаунт

Доступно Целевые УЗ

Выбрано Целевые УЗ

Администратор@local@WindowsServer:RDP

Выбрать элементы (0) Удалить элементы (1)

Select all items (0) Delete all items (1)

Выбранные цели:

Управление сессиями:

Аккаунт: Администратор@local@WindowsServer:RDP

Учетка сценария: Администратор@local@WindowsServer

Маппинг аккаунтов: WindowsServer:RDP

Интерактивный вход: WindowsServer:RDP

Управление паролями:

Аккаунт: --

Действие Правила Подпротокол

kill SSH_SHELL_SESSION / X11_SESSION

Отменить Применить

Добавим их все и сохраним группу ресурсов.



SKDPU

admin (eth0)
Bastion Super Administrator


Ресурсы Группы



Мои настройки

Мои авторизации

Аудит

Пользователи

Ресурсы

Домены

Устройства

Приложения

Аккаунты

Кластеры

Группы

Плагины хранения паролей

Политики выборки

Управление паролями

Управление сессиями

Авторизации

Конфигурация

Система

Импорт/Экспорт

✎ Редактировать эту группу

Информация

Имя группы : Servers

Описание : --

Учетная запись управления : Администратор@local@WindowsServer:RDP
сессиями

Учетка сценария : --

Маппинг аккаунтов : WindowsServer:RDP

Интерактивный вход : WindowsServer:RDP

Учетка управления паролями : --


Добавление хоста SSH идентично принципам добавления хоста RDP, описанным в предыдущих пунктах.

В разделе **Авторизации** → **Управление авторизациями** добавим правило "Local_auth", разрешающее группе пользователей "Local_skdp_users" использовать ресурсы из группы "Servers" и все необходимые **протоколы и подпротоколы**. Также необходимо включить **запись сессий**.

Управление авторизациями

Мои настройки

Мои авторизации

Аудит

Пользователи

Ресурсы

Управление паролями

Управление сессиями

Авторизации

Управление авторизациями

Мои разрешения

История моих разрешений

Конфигурация

Система

Импорт/Экспорт

admin (eth0)

Bastion Super Administrator

Добавить авторизацию

Группа пользователей *

Local_skdp_users

Целевые группы УЗ *

Servers

Имя *

Local_auth

Описание :

Критичные цели :

☐

Разрешить сеансы :

☒

Протоколы :

Подпротоколы *

Доступно Протоколы/Подпротоколы

Q

Выбрать и кликнуть

RAWTCPIP

RDP

RDP_CLIPBOARD_UP

RDP_CLIPBOARD_DOWN

RDP_PRINTER

RDP_COM_PORT

RDP_DRIVE

RDP_SMARTCARD

RDP_CLIPBOARD_FILE

RDP_AUDIO_OUTPUT

RLOGIN

SSH_SHELL_SESSION

SSH_REMOTE_COMMAND

Выбрать все

Удалить все

Включить запись сессий :

☒

Включить извлечение пароля :

☐

Включение рабочего процесса утверждения :

☐

Отменить

Применить

Авторизация "Local_auth" для группы "Local_skdp_users" должна выглядеть следующим образом

Управление авторизациями

Мои настройки

Мои авторизации

Аудит

Пользователи

Ресурсы

Управление паролями

Управление сессиями

Авторизации

Управление авторизациями

Мои разрешения

История моих разрешений

Конфигурация

Система

Импорт/Экспорт

admin (eth0)

Bastion Super Administrator

Добавить авторизацию

Показать элементы 10

Поиск:

	Группа пользователей	Целевые группы УЗ	Имя	Протокол	Критичные цели	Включить запись сессий	Сессии	Выборка паролей	Подтверждения
☐	Local_skdp_users	Servers	Local_auth	RAWTCPIP, RDP, RLOGIN, TELNET, SSH, VNC	-	✓	✓	-	-

1 - 1 / 1

Если все сделано правильно, то в разделе **Мои авторизации** → **Сессии** будет представлен список доступных данному пользователю целевых ресурсов:


SKDPU

admin (eth0)
 Bastion Super Administrator

Мои авторизации
Сессии
?

Сессии

Пароли

Аудит

Пользователи

Ресурсы

Управление паролями

Управление сессиями

Авторизации

Конфигурация

Система

Импорт/Экспорт

Настройки
RDP: 1024x768, 16 bpp

Показать 10 записей
Поиск:

Протоколы	Цель	Имя авторизации	Описание уч. записи	Описание ресурса	Периоды времени	Крайнее соединение	Подтверждения
RDP	admin@WindowsServer:RDP	Local_auth	--	--	allthetime	--	
RDP	WindowsServer:RDP [interactive login]	Local_auth	--	--	allthetime	--	
RDP	Администратор@local@WindowsServer:RDP	Local_auth	--	--	allthetime	--	

1 - 3 / 3

Запросы подтверждения
Поиск:

Показать элементы 10
Поиск:

Отменить
Цель
Начало
Длительность
Тикет
Кворум
Статус
Ответы

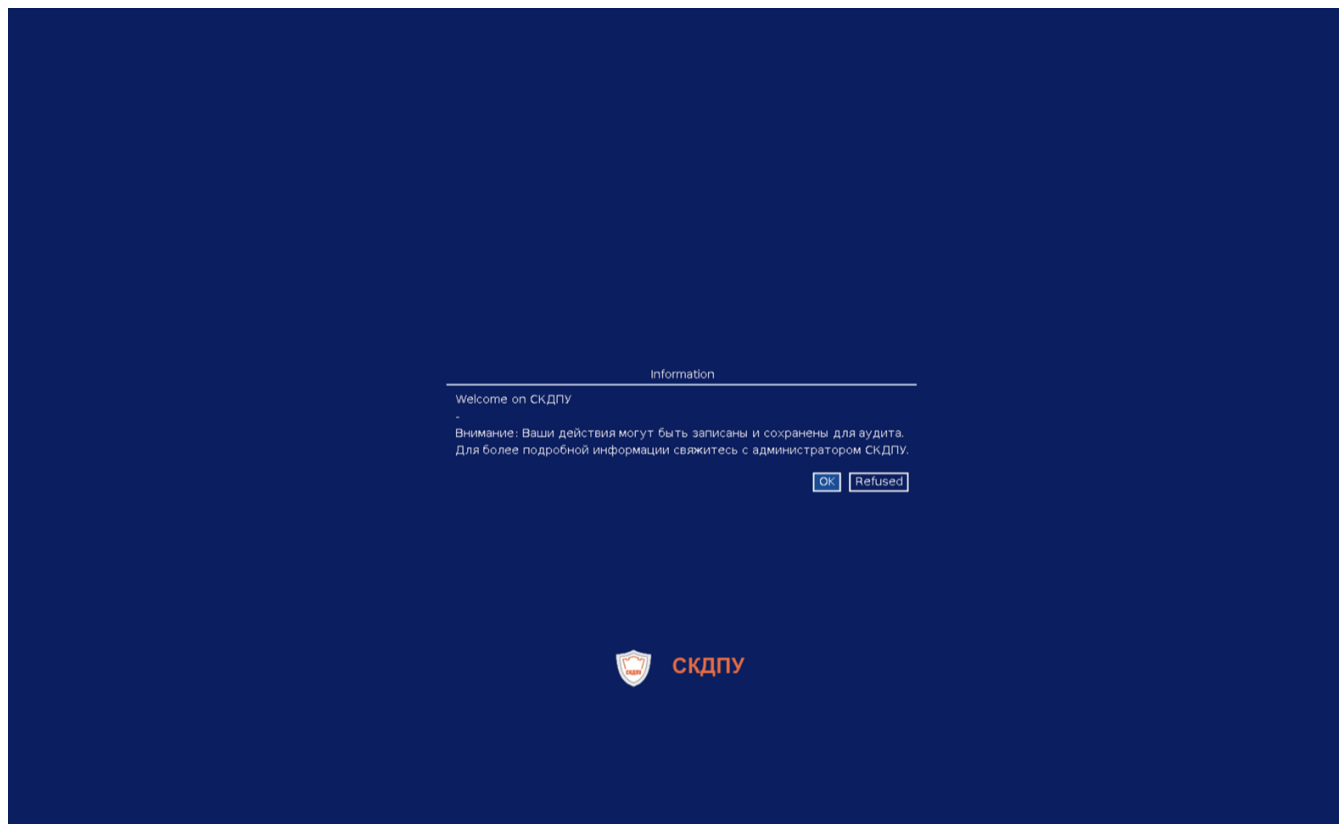
0 - 0 / 0

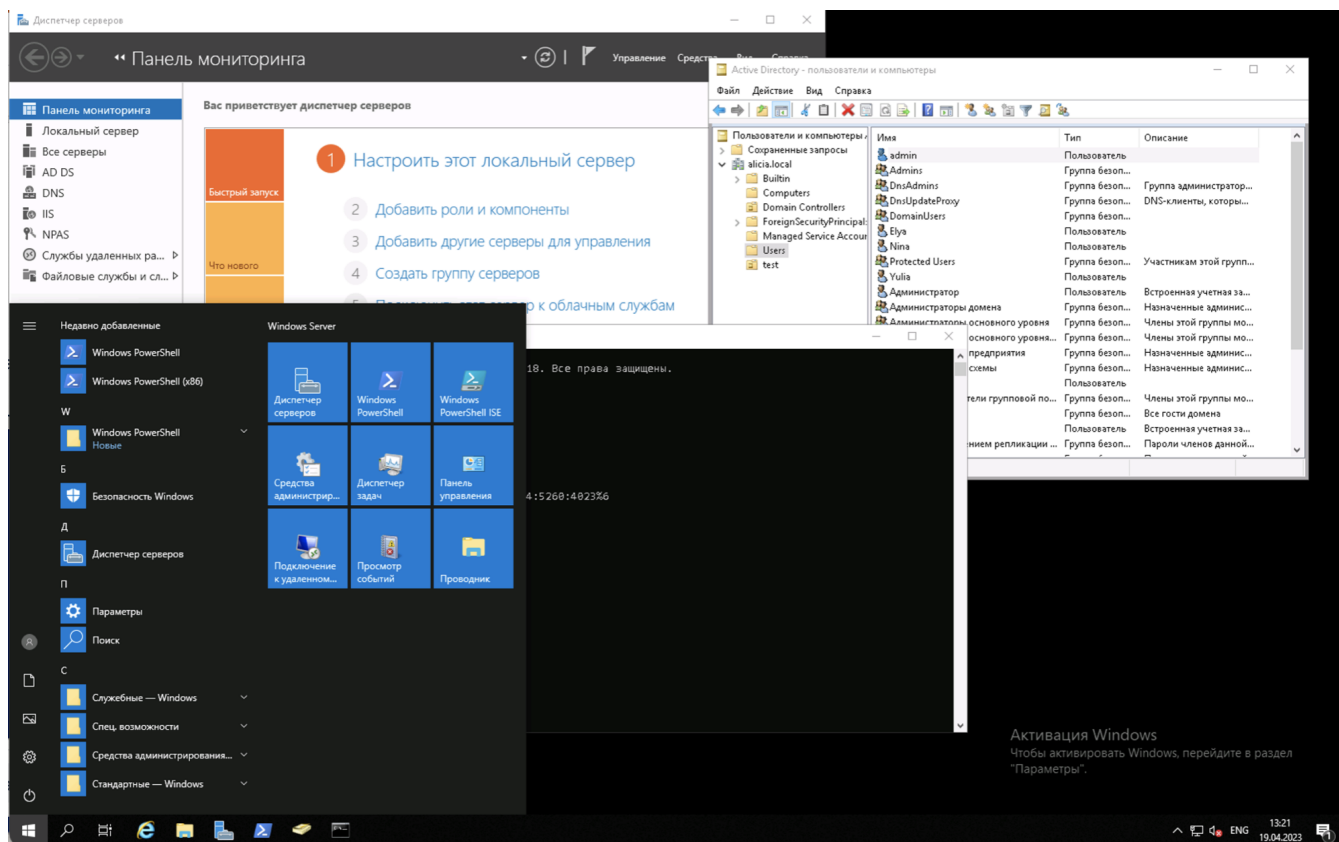
6. Соединение через СКДПУ

6.1. Подключение по протоколу RDP

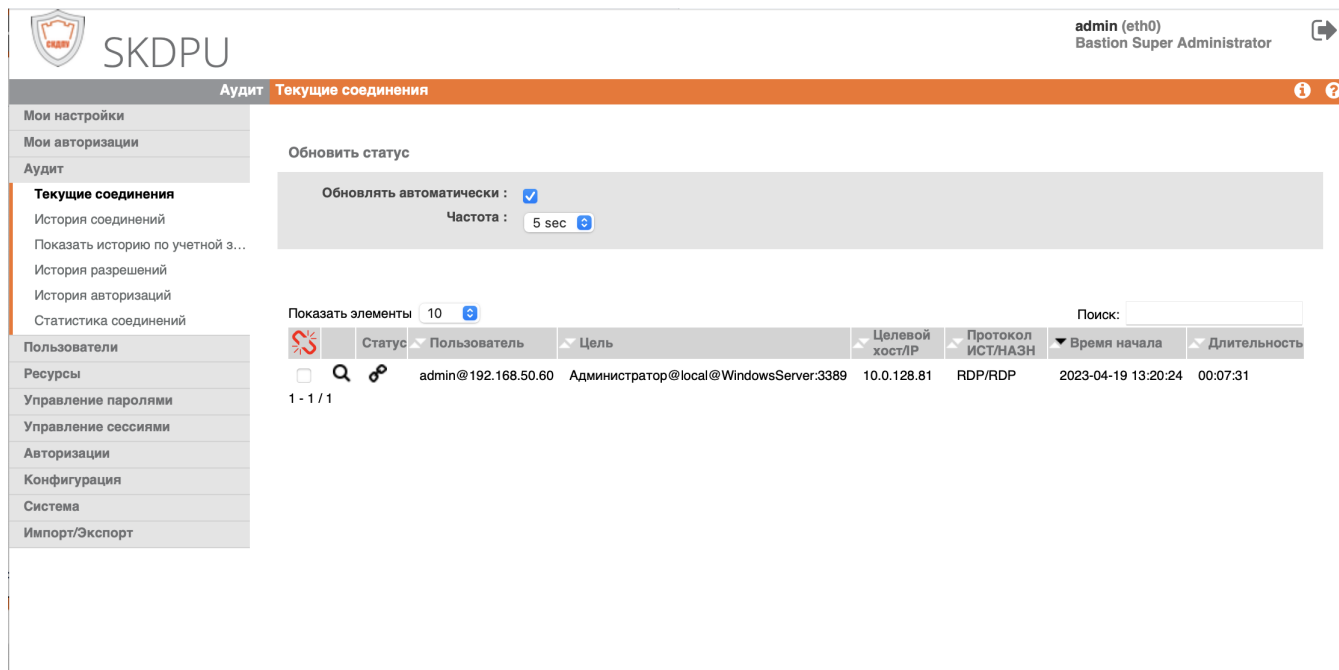
6.1.1. Подключение из интерфейса системы

Выберите в разделе **Мои авторизации** → **Сессии** вариант входа с сохраненной УЗ - Администратор@local@WindowsServer:RDP, скачайте и запустите ярлык запуска *mstsc* (либо Microsoft Remote Desktop на MacOS).

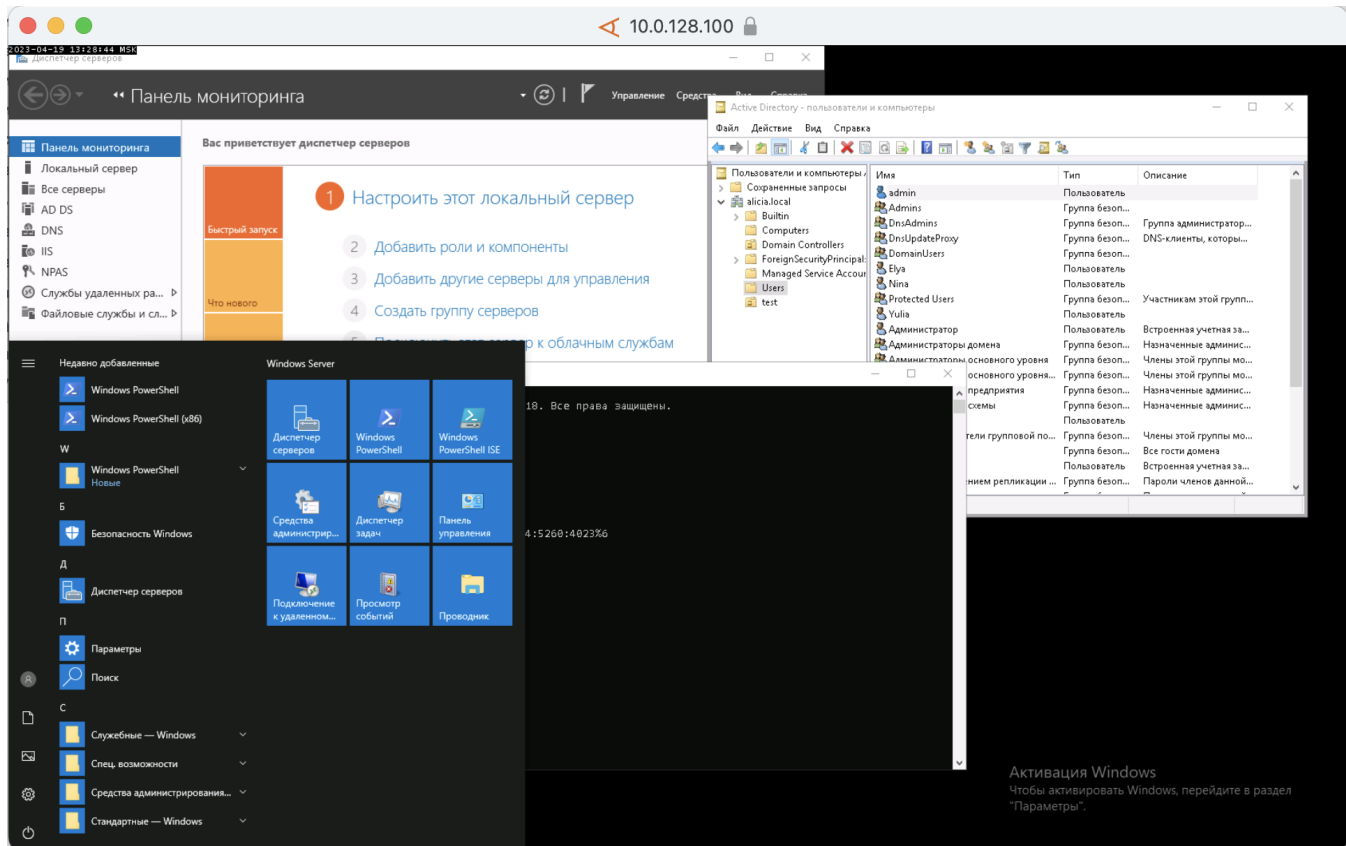




Пока сессия открыта, в разделе **Аудит → Текущие соединения** доступны сведения о происходящем.



Система позволяет оперативно наблюдать происходящее в рамках сессии по клику на

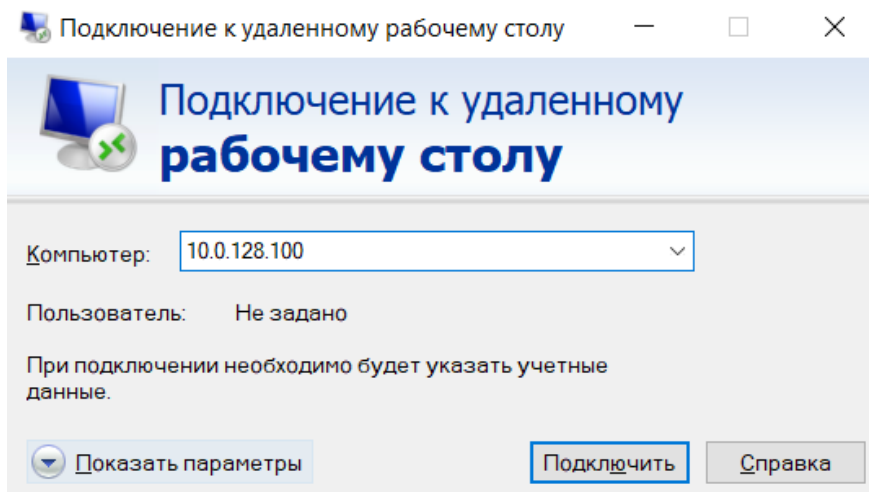


Закройте сессию.

6.1.2. Подключение при помощи клиента удаленного доступа mstsc или Microsoft Remote Desktop

Вход на систему можно осуществить и без входа в веб-интерфейс, например, можно запустить клиент напрямую на адрес СКДПУ и выбрать нужную целевую систему после авторизации:

Вход через mstsc:



В нашем случае, вход будет осуществляться при помощи Microsoft Remote Desktop

Add PC

PC name:

User account:

General | Display | Devices & Audio | Folders

Friendly name:

Group:

Gateway:

☒ Bypass for local addresses

☒ Reconnect if the connection is dropped

☐ Connect to an admin session

☐ Swap mouse buttons

Cancel

Add

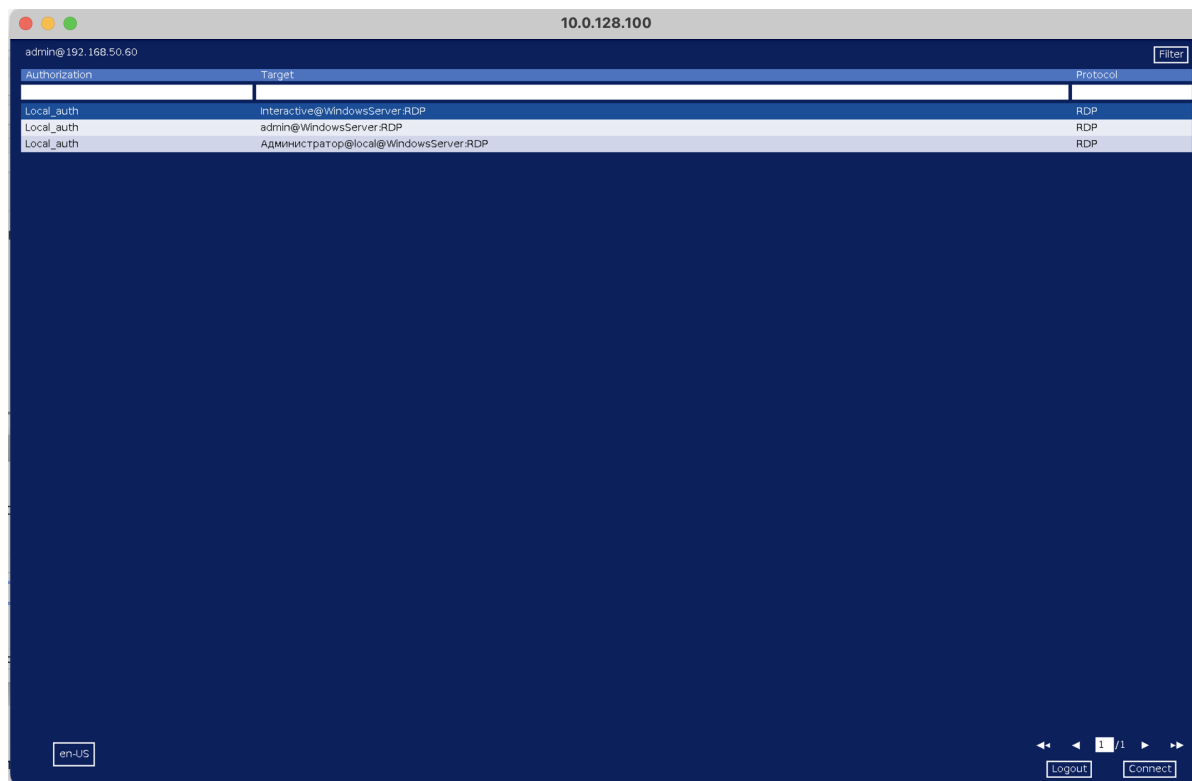
Conn
10.0.1
Conf

Enter Your User Account
This user account will be used to connect to 10.0.128.100 (remote PC).
Username:
Password:
☐ Show password

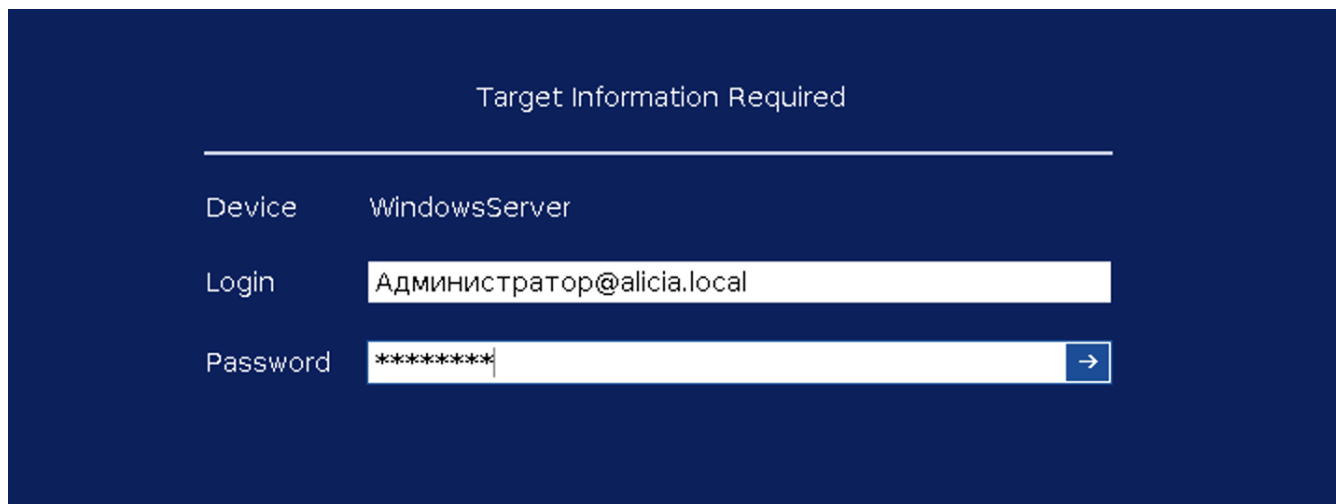
Cancel

Continue

После авторизации система выдаст меню доступных вариантов подключения по протоколам RDP или VNC для данного пользователя



Подключение к УЗ "Администратор" при помощи интерактивного входа реализуется так:



The screenshot shows a 'Target Information Required' form on a dark blue background. The form has three input fields:

- Device:** A text field containing 'WindowsServer'.
- Login:** A text field containing 'Администратор@alicia.local'.
- Password:** A text field containing '*****' with a blue arrow button to its right.

Протестируйте остальные варианты входа на целевое устройства.

6.2. Подключение по протоколу SSH

Такой же механизм работает и для SSH подключений.

Для того, чтобы открывать соединения с SSH системами из веб-интерфейса, необходимо установить клиента WABPutty, который идет в поставке системы. Ссылка на него появляется при добавлении первой целевой системы с протоколом ssh.

Мои настройки

Мои авторизации

Сессии

Пароли

Аудит

Пользователи

Ресурсы

Управление паролями

admin (eth0)
Bastion Super Administrator

Мои авторизации

Сессии

Настройки

Показать 10 записей

Поиск:

Протоколы	Цель	Имя авторизации	Описание уч. записи	Описание ресурса	Периоды времени	Крайний соеди
SSH	admin@astra17:SSH	astra17	--	--	allthetime	--

7. Аудит сессий пользователей

В разделе **Аудит** → **История соединений** доступен список обработанных системой сессий администрирования.

Мои настройки

Мои авторизации

Аудит

Текущие соединения

История соединений

Показать историю по учетной за...

История разрешений

История авторизаций

Статистика соединений

admin (eth0)
Bastion Super Administrator

Аудит

История соединений

Показать элементы 10

Поиск:

Пользователь	Цель	Целевой хост/IP	Протокол ИС/Т/НАШ	Время начала	Время окончания	Длительность	Размер	Результат
admin@192.168.50.60	Администратор@local@WindowsServer:3389	10.0.128.81	RDP/RDP	2023-04-19 13:41:38	2023-04-19 13:42:11	00:00:33	373.3 КБ	✓
admin@192.168.50.60	admin@WindowsServer:3389	10.0.128.81	RDP/RDP	2023-04-19 13:40:21	2023-04-19 13:41:22	00:01:01	280.0 КБ	✓
admin@192.168.50.60	Interactive@WindowsServer:3389 (Администратор@alicia.local)	10.0.128.81	RDP/RDP	2023-04-19 13:38:32	2023-04-19 13:39:53	00:01:20	1.1 МБ	✓
admin@192.168.50.60	Interactive@WindowsServer:3389 (Администратор@local)	10.0.128.81	RDP/RDP	2023-04-19 13:37:37	2023-04-19 13:38:01	00:00:23	--	✓
admin@192.168.50.60	Interactive@WindowsServer:3389 (Администратор@ALICIA)	10.0.128.81	RDP/RDP	2023-04-19 13:34:59	2023-04-19 13:36:53	00:01:53	--	✓
admin@192.168.50.60	Администратор@local@WindowsServer:3389	10.0.128.81	RDP/RDP	2023-04-19 13:20:24	2023-04-19 13:31:11	00:10:46	896.5 КБ	✓

Подробнее Вы можете изучить информацию о сессии , кликнув на

В данном диалоге, доступны мета-данные о сессии, видео-поток, который можно полностью скачать,

SKDPU

admin (eth0)
Bastion Super Administrator

Аудит История соединений

Мои настройки
Мои авторизации
Аудит
Текущие соединения
История соединений
Показать историю по учетной за...
История разрешений
История авторизаций
Статистика соединений
Пользователи
Ресурсы
Управление паролями
Управление сессиями
Авторизации
Конфигурация
Система
Импорт/Экспорт

Информация сессий

Имя пользователя : admin@192.168.50.60
Цель : Администратор@local@WindowsServer:3389
Целевой хост/IP : 10.0.128.81
Протокол ИСТ/НАЗН : RDP/RDP
Время начала : 2023-04-19 13:41:38
Время окончания : 2023-04-19 13:42:11
Длительность : 0:00:33.158689
Разрешение : 1680x1050
Результат : Success
Описание : --

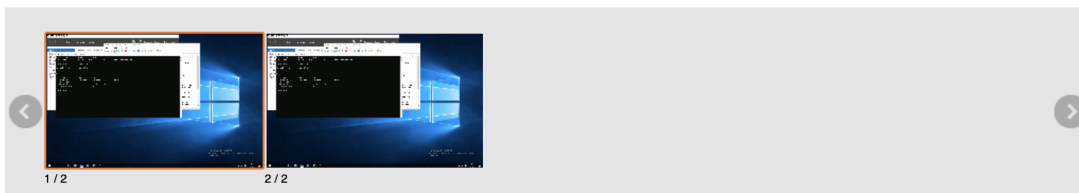
Просмотрщик RDP

Постоянное проигрывание

а также оглавление в виде ключевых кадров и список сохраненных системой событий, которые исполнил пользователь, работавший в рамках сессии.

Полная запись: [Создать](#)

Список снимков экрана



Данные сессий

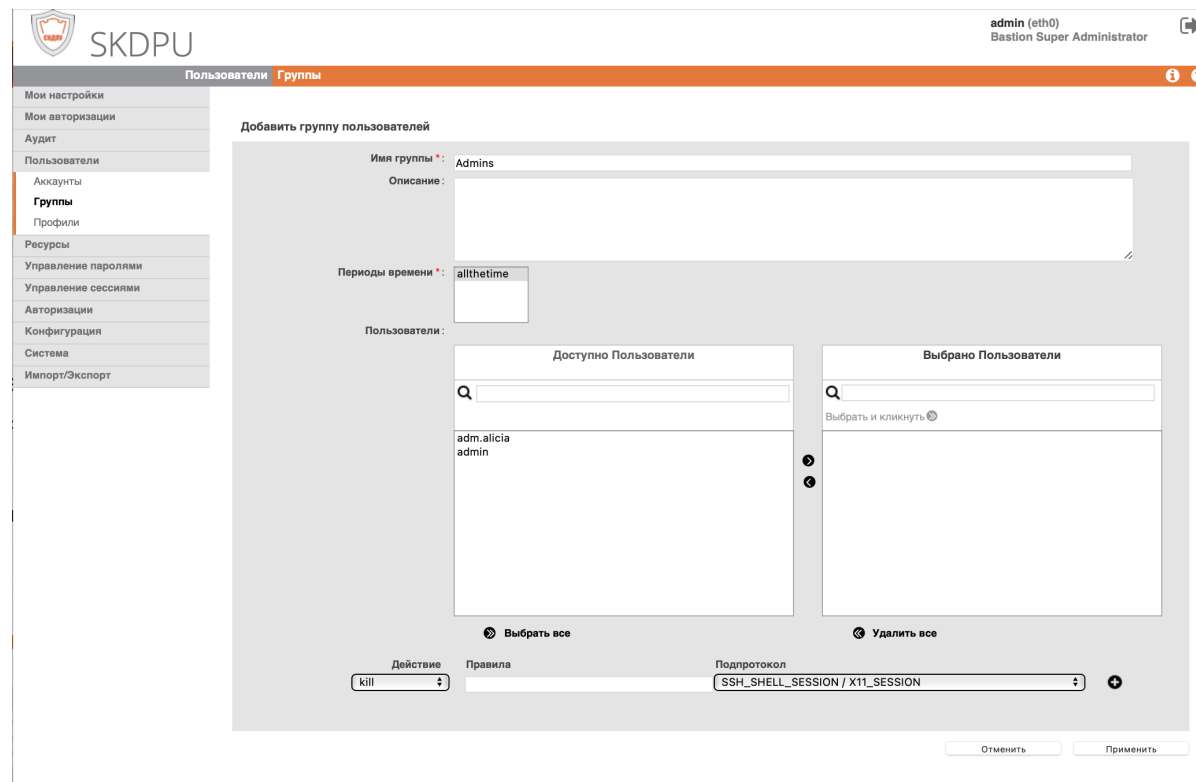
Индекс	Дата время	Действие	Поиск:
1	2023-04-19 13:41:38	Beginning	
	2023-04-19 13:41:43	type="NEW_PROCESS" command_line="C:\Windows\system32\TSTheme.exe -Embedding"	
	2023-04-19 13:41:43	type="COMPLETED_PROCESS" command_line="C:\Windows\system32\TSTheme.exe -Embedding"	
	2023-04-19 13:41:43	type="NEW_PROCESS" command_line="\"C:\Windows\system32\backgroundTaskHost.exe\" - ServerName:App.AppXv783p9dgsc3mek8m05c3tj95wa9p858.mca"	
	2023-04-19 13:41:43	type="COMPLETED_PROCESS" command_line="\"C:\Windows\system32\backgroundTaskHost.exe\" - ServerName:App.AppXv783p9dgsc3mek8m05c3tj95wa9p858.mca"	
	2023-04-19 13:41:43	type="NEW_PROCESS" command_line="C:\Windows\system32\TSTheme.exe -Embedding"	
	2023-04-19 13:41:43	type="NEW_PROCESS" command_line="rdpclip.exe"	
	2023-04-19 13:41:44	type="COMPLETED_PROCESS" command_line="rdpclip.exe"	

1 - 16 / 16

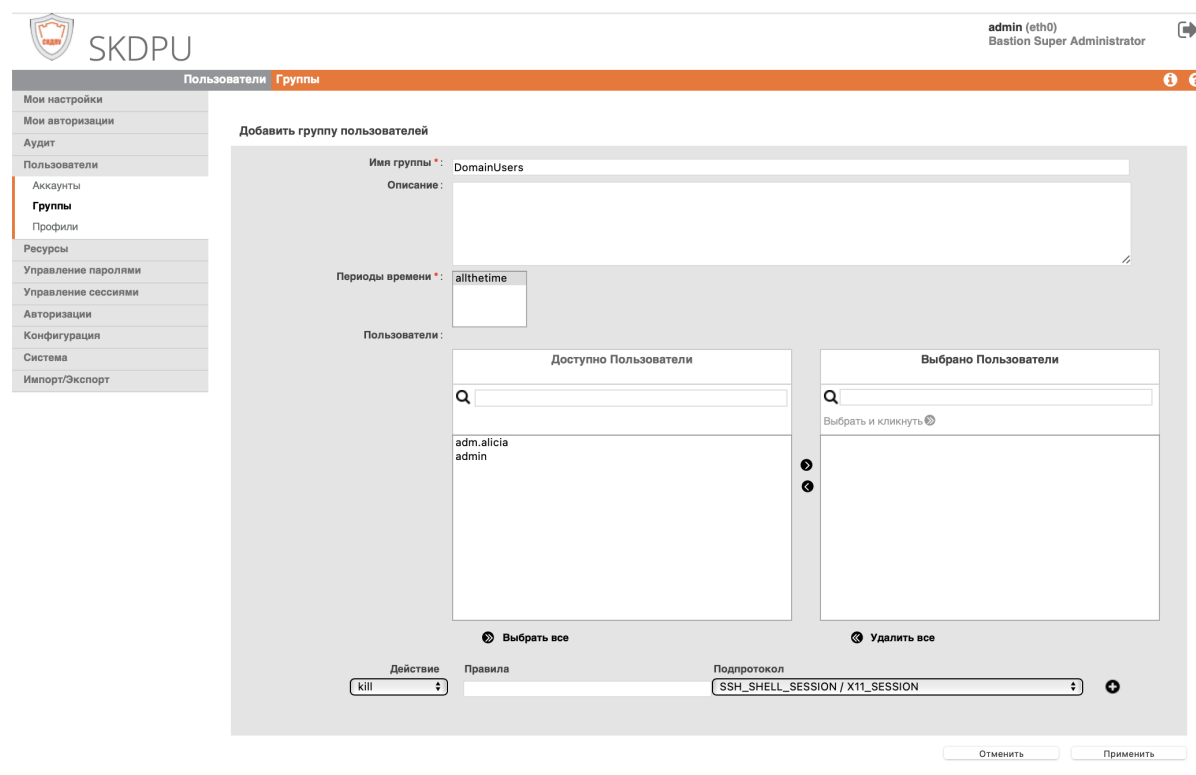
8. Подключение внешних каталогов пользователей

8.1. Настройки Active Directory для авторизации исполнителей

Добавим новые группы Admins и Domain Users в разделе **Пользователи** → **Группы**.



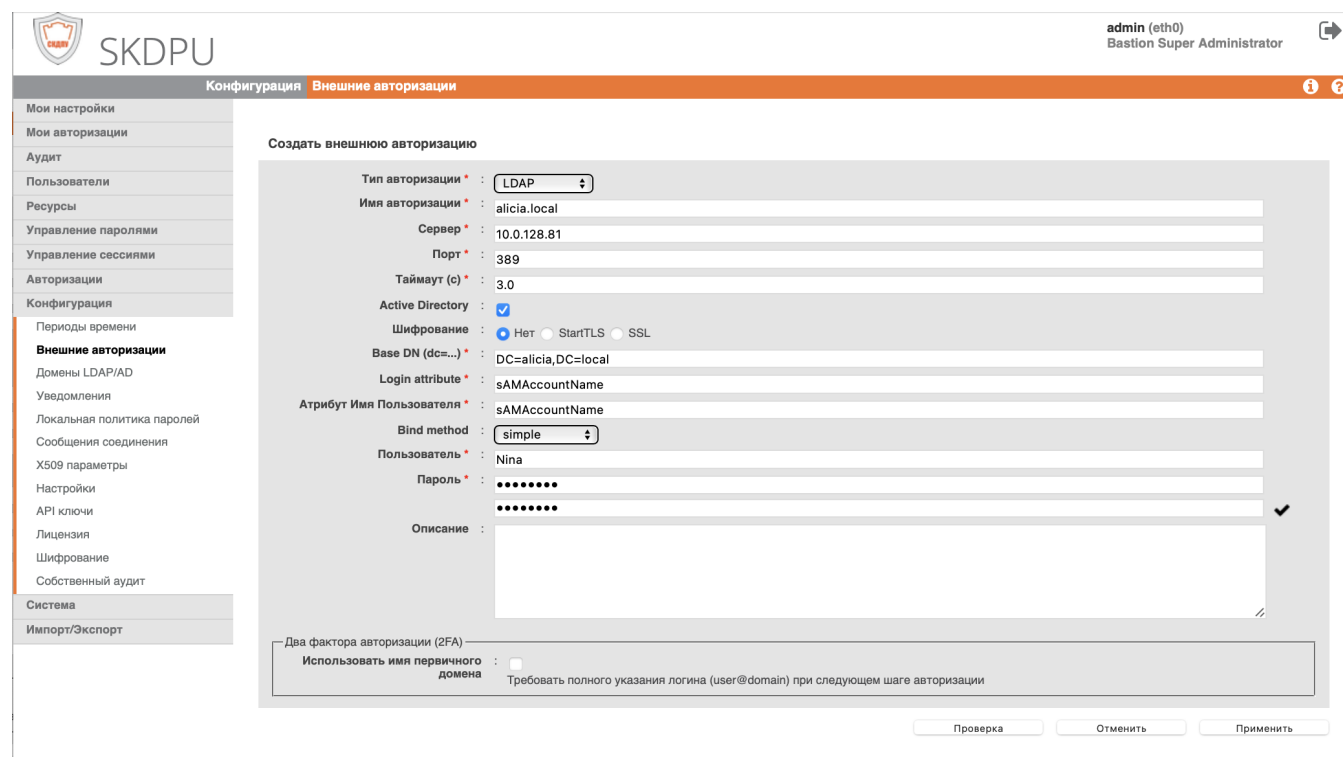
The screenshot shows the SKDPU web interface. The top navigation bar includes the SKDPU logo, the user 'admin (eth0) Bastion Super Administrator', and a help icon. The left sidebar contains a menu with items like 'Мои настройки', 'Мои авторизации', 'Аудит', 'Пользователи', 'Аккаунты', 'Группы' (highlighted), 'Профили', 'Ресурсы', 'Управление паролями', 'Управление сессиями', 'Авторизации', 'Конфигурация', 'Система', and 'Импорт/Экспорт'. The main content area is titled 'Добавить группу пользователей' (Add user group). It contains a form with the following fields: 'Имя группы' (Group name) set to 'Admins', 'Описание' (Description) as a text area, 'Периоды времени' (Time periods) set to 'allthetime', and 'Пользователи' (Users) as a list of users. Below the user list are two buttons: 'Выбрать все' (Select all) and 'Удалить все' (Delete all). At the bottom, there are dropdowns for 'Действие' (Action) set to 'kill', 'Правила' (Rules), and 'Подпротокол' (Subprotocol) set to 'SSH_SHELL_SESSION / X11_SESSION'. There are also 'Отменить' (Cancel) and 'Применить' (Apply) buttons.



The screenshot shows the SKDPU web interface with the 'Add Group' form for 'DomainUsers'. The interface is identical to the previous one, but the 'Имя группы' (Group name) is now 'DomainUsers'. The 'Пользователи' (Users) list still shows 'adm.alicia' and 'admin'. The 'Действие' (Action) dropdown is still set to 'kill', and the 'Подпротокол' (Subprotocol) is still 'SSH_SHELL_SESSION / X11_SESSION'. The 'Отменить' (Cancel) and 'Применить' (Apply) buttons are at the bottom.

В разделе **Конфигурация → Внешние авторизации** нужно добавить профиль LDAP сервера для работы с AD.

ВАЖНО! Пользователь AD должен обладать достаточными для чтения списка пользователей домена правами, при этом не рекомендуется добавлять самого Администратора домена для авторизации LDAP.



The screenshot shows the SKDPU configuration interface. The left sidebar contains a menu with options like 'Мои настройки', 'Мои авторизации', 'Аудит', 'Пользователи', 'Ресурсы', 'Управление паролями', 'Управление сессиями', 'Авторизации', 'Конфигурация', 'Периоды времени', 'Внешние авторизации', 'Домены LDAP/AD', 'Уведомления', 'Локальная политика паролей', 'Сообщения соединения', 'X509 параметры', 'Настройки', 'API ключи', 'Лицензия', 'Шифрование', 'Собственный аудит', 'Система', and 'Импорт/Экспорт'. The main area is titled 'Создать внешнюю авторизацию' and contains the following fields:

- Тип авторизации: LDAP
- Имя авторизации: alicia.local
- Сервер: 10.0.128.81
- Порт: 389
- Таймаут (с): 3.0
- Active Directory: ☒
- Шифрование: ☒ Нет ☐ StartTLS ☐ SSL
- Base DN (dc=...): DC=alicia,DC=local
- Login attribute: sAMAccountName
- Атрибут Имя Пользователя: sAMAccountName
- Bind method: simple
- Пользователь: Nina
- Пароль: (masked with dots)
- Описание: (empty text area)

At the bottom, there is a section for 'Два фактора авторизации (2FA)' with a checkbox 'Использовать имя первичного домена' and a note: 'Требовать полного указания логина (user@domain) при следующем шаге авторизации'. The bottom right has buttons for 'Проверка', 'Отменить', and 'Применить'.

Далее, в разделе **Конфигурация → Домены LDAP/AD** создаем профиль домена и используем в его настройке только что созданный профиль LDAP сервера

SKDPU

admin (eth0)
Bastion Super Administrator

КонфигурацияДомены LDAP/AD

Мои настройки
Мои авторизации
Аудит
Пользователи
Ресурсы
Управление паролями
Управление сессиями
Авторизация
Конфигурация

Периоды времени
Внешние авторизации
Домены LDAP/AD
Уведомления
Локальная политика паролей
Сообщения соединения
X509 параметры
Настройки
API ключи
Лицензия
Шифрование
Собственный аудит

Система
Импорт/Экспорт

Редактировать домены LDAP/AD: alicia.local

Описание :

Домен по умолчанию:

☒

Имя домена LDAP/AD *:

ALICIA

X509 authentication:

☐

If this option is selected, users can only authenticate on the domain through X509 authentication method.

Доменное имя для совпадения с SAN :
эмейлом

Only for X509 authentication with an AD server.

X509 matching condition:

Condition to match an LDAP domain with the X509 certificate (only for X509 authentication with an LDAP server)
E.g.: \$(issuer_o)=Organisation || \$(issuer_cn)=CommonName && \$(subject_ou)=OrganisationalUnit Operator && (AND) has precedence over operator || (OR)
Values are case sensitive whereas variables are not.
Available variables: issuer(_c,_l,o_ou,_sn,st_email), subject(_c,_l,i,o_ou,_sn,st_email_uid), mail(_o...N), msupn(_o...N), dns(_o...N)

Директория *:

Доступные директории

QActive Dir ↓

Выбранные директории

Q

Выбрать и кликнуть ⌕

alicia.local

>
<

⌕ Выбрать все

⌘ Удалить все

Вторичная авторизация:

Доступно Вторичных авторизаций

Q

Выбрано Вторичных авторизаций

Q

Выбрать и кликнуть ⌕

>
<

⌕ Выбрать все

⌘ Удалить все

Добавим соотнесение LDAP авторизации. Для созданных групп СКДПУ (в нашем примере, DomainUsers и Admins) укажем атрибуты (CN, OU, DC) групп LDAP Windows Server, которые мы хотим связать с локальными в СКДПУ, и сохраним созданный профиль.

Атрибут группы:

memberOf

Атрибут DN:

displayName

Атрибут E-mail:

mail

Атрибут языка:

preferredLanguage

Язык по умолчанию *:

Русский

Default email domain *:

icloud.com

X509 LDAP search filter:

LDAP search filter (only for X509 authentication with an LDAP server)
Expressed in LDAP filter syntax. Any variables listed below field "X509 matching condition" can be used.

Соотношение LDAP авторизации

Группа пользователей *

Адmins

Профиль *

WAB_administrator

Группа LDAP *

DomainUsers

DomainUsers

approver

CN=DomainUsers,CN=Users,DC=alicia,DC=local

Адmins

WAB_administrator

CN=Адmins,CN=Users,DC=alicia,DC=local

☐

Адmins

WAB_administrator

Группа по умолчанию для пользователей без группы в этом домене

Следующий обязательный шаг – задать соотношение доменных групп с локальными группами СКДПУ.

В разделе **Авторизации** → **Управление авторизациями** добавляем правила с использованием групп Admins и DomainUsers.


SKDPU

Управление авторизациями

- Мои настройки
- Мои авторизации
- Аудит
- Пользователи
- Ресурсы
- Управление паролями
- Управление сессиями
- Авторизации
- Управление авторизациями**
- Мои разрешения
- История моих разрешений
- Конфигурация
- Система
- Импорт/Экспорт

admin (eth0)
Bastion Super Administrator


Добавить авторизацию

Группа пользователей *:

Целевые группы УЗ *:

Имя *: domain_admins

Описание:

Критичные цели: ☐

Разрешить сеансы: ☒

Протоколы/Подпротоколы *:

Доступно Протоколы/Подпротоколы

⌕ Выбрать все

Выбрано Протоколы/Подпротоколы

Выбрать и кликнуть

- RAWTCP/IP
- ⌕ RDP
- ⌕ RDP_CLIPBOARD_UP
- RDP_CLIPBOARD_DOWN
- RDP_PRINTER
- RDP_COM_PORT
- RDP_DRIVE
- RDP_SMARTCARD
- RDP_CLIPBOARD_FILE
- RDP_AUDIO_OUTPUT
- RLOGIN
- SSH_SHELL_SESSION
- SSH_REMOTE_COMMAND

⌕ Удалить все

Включить запись сессий: ☒

Включить извлечение пароля: ☐

Включение рабочего процесса утверждения: ☐

Отменить
Применить

Управление авторизациями

Мои настройки

Мои авторизации

Аудит

Пользователи

Ресурсы

Управление паролями

Управление сессиями

Авторизации

Управление авторизациями

Мои разрешения

История моих разрешений

Конфигурация

Система

Импорт/Экспорт

admin (eth0)

Bastion Super Administrator

Добавить авторизацию

Группа пользователей *

DomainUsers

Целевые группы УЗ *

Servers

Имя *

domain_users

Описание

Критичные цели

Разрешить сеансы

✓

Протоколы/Подпротоколы *

Доступно Протоколы/Подпротоколы

Q

Выбрать и кликнуть

RAWTCPIP

1

RDP

2

RDP_CLIPBOARD_UP

3

RDP_CLIPBOARD_DOWN

4

RDP_PRINTER

5

RDP_COM_PORT

6

RDP_DRIVE

7

RDP_SMARTCARD

8

RDP_CLIPBOARD_FILE

9

RDP_AUDIO_OUTPUT

10

RLOGIN

11

SSH_SHELL_SESSION

12

SSH_REMOTE_COMMAND

Выборить все

Удалить все

Включить запись сессий

✓

Включить извлечение пароля

Включение рабочего процесса утверждения

Отменить

Применить

Теперь авторизации должны выглядеть следующим образом

Управление авторизациями

Мои настройки

Мои авторизации

Аудит

Пользователи

Ресурсы

Управление паролями

Управление сессиями

Авторизации

Управление авторизациями

Мои разрешения

История моих разрешений

Конфигурация

Система

Импорт/Экспорт

admin (eth0)

Bastion Super Administrator

Данные сохранены

Добавить авторизацию

Показать элементы

10

Поиск:

	Группа пользователей	Целевые группы УЗ	Имя	Протокол	Критичные цели	Включить запись сессий	Сессии	Выборка паролей	Подтверждения
☐	Admins	Servers	domain_admins	RAWTCPIP, RDP, RLOGIN, TELNET, SSH, VNC	—	✓	✓	—	—
☐	DomainUsers	Servers	domain_users	RAWTCPIP, RDP, RLOGIN, TELNET, SSH, VNC	—	✓	✓	—	—
☐	Local_skdp_users	Servers	Local_auth	RAWTCPIP, RDP, RLOGIN, TELNET, SSH, VNC	—	✓	✓	—	—

1 - 3 / 3

Сохраняем настройки. Если мы все указали правильно, в разделе **Пользователи** → **Аккаунты** появится возможность переключения между локальными учетными записями и пользователями домена. Для доменных пользователей, входящих в ранее указанные доменные группы, должны указываться локальные группы СКДПУ, с которыми выполнено соотнесение. Если это не так, то возможными причинами могут быть ошибки в настройках – недоступный хост домена, некорректные учетные данные учётной записи для чтения списка пользователей домена, не созданы соответствующие группы, некорректно настроенное соотнесение доменных и локальных групп и т.п.

Страница 35


SKDPU

admin (eth0)
Bastion Super Administrator

Пользователи **Аккаунты**

Мои настройки
Мои авторизации
Аудит
Пользователи
Аккаунты
Группы
Профили
Ресурсы
Управление паролями
Управление сессиями
Авторизации
Конфигурация
Система
Импорт/Экспорт

Показать пользователей домена :

Показать элементы

Логин	Видимое имя	Группы	Крайнее соединение
Elya	Elya	DomainUsers	--
Yulia	Yulia	DomainUsers	--
Администратор		Admins	--
Nina	Nina	Admins	--

1 - 4 / 4

Поиск:

Допустимые профили пользователей описаны в разделе **Пользователи** → **Профили**, там же можно создать свои профили с удобными ограничениями и разрешениями.


SKDPU

admin (eth0)
Bastion Super Administrator

Пользователи **Профили**

Мои настройки
Мои авторизации
Аудит
Пользователи
Аккаунты
Группы
Профили
Ресурсы
Управление паролями
Управление сессиями
Авторизации
Конфигурация
Система
Импорт/Экспорт

+ Добавить профиль

Показать элементы

Имя профиля

Ограничения по IP

approver

auditor

operation_administrator

system_administrator

user

WAB_administrator

1 - 6 / 6

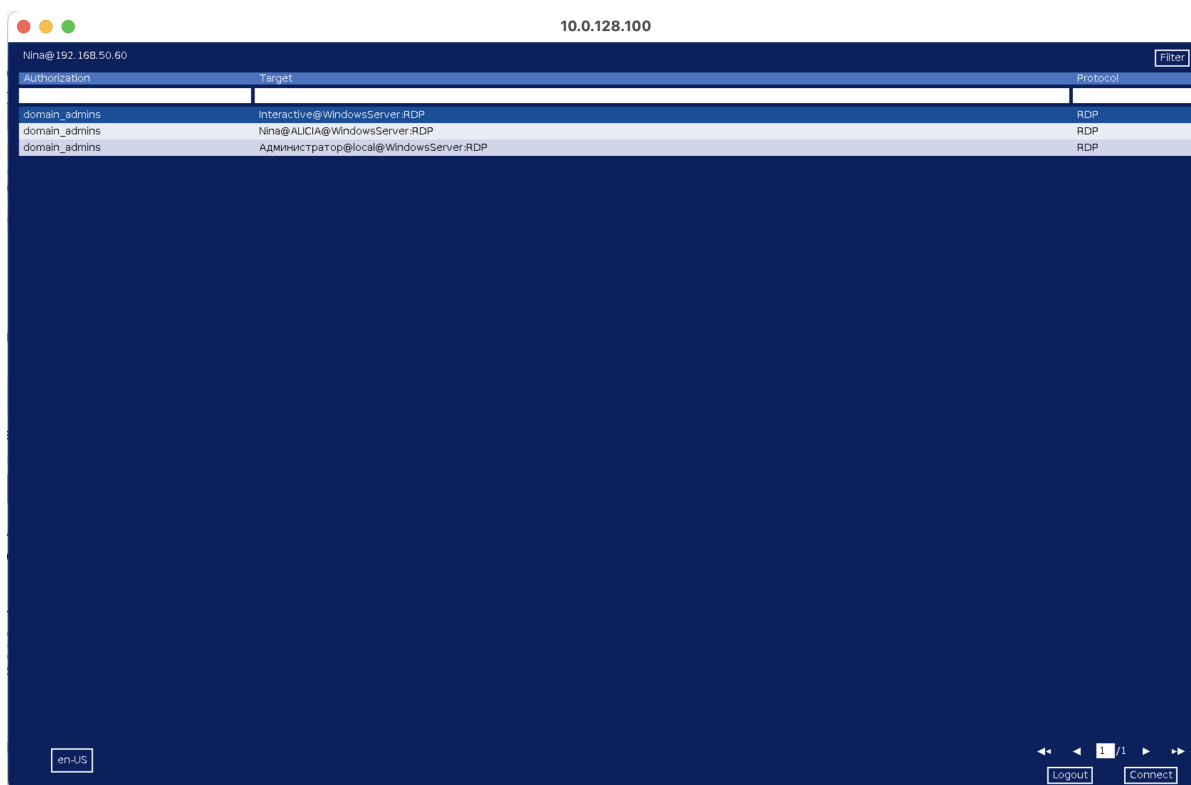
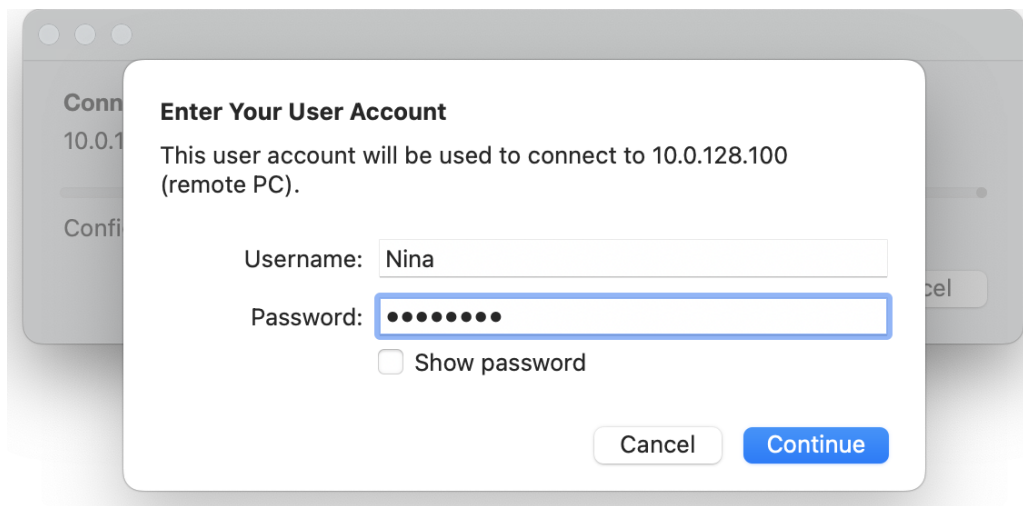
Поиск:

И сможете войти как доменный пользователь как на веб-интерфейс, так и залогиниться непосредственно в клиенте при соединении с СКДПУ.



Логин можно указывать и как DOMAIN\user, и как user@domain.name. Во многом это зависит от сервера домена

Если при создании домена LDAP указывался параметр "Домен по умолчанию", то можно зайти в СКДПУ под пользователем в формате <user> без указания домена



9. Устранение возможных проблем

9.1. Пароль пользователя admin устарел

Для того, чтобы сбросить пароль учетной записи admin требуется:

1. Войти по ssh на систему по порту 2242
2. Повысить привилегии до пользователя root командами

```
super
Password: !QAZ2wsx
sudo -i
Password: !QAZ2wsx
```

3. Ввести команду для сброса пароля:

```
/opt/wab/bin/WABRestoreDefaultAdmin
```

После этого пароль станет стандартным:

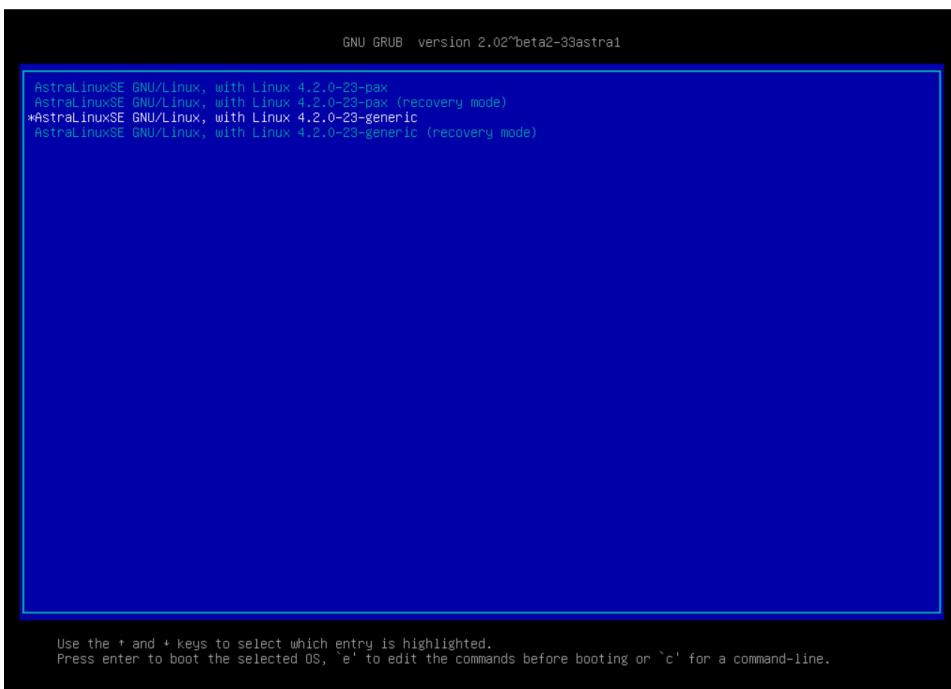
Логин -- **admin**

Пароль -- **admin**

9.2. Восстановление пароля учетной записи wabadmin

В случае, если при попытке авторизации учетной записи wabadmin возникают ошибки ("Login incorrect", "Access denied", "Password incorrect") или пароль данной учетной записи был утерян, для возобновления доступа к консоли устройства необходимо произвести восстановление пароля. Для этого нужно загрузиться в single mode:

1. Перезагрузить сервер командой **reboot** сервер, дождаться экрана загрузчика GRUB;



2. Войти в режим редактирования нажатием клавиши "e";
3. Выбрать строку, которая начинается со слова linux или kernel;
4. Удалить из нее слова **quiet** и **splash** и дописать в конец

```
single init=/bin/bash
```

5. Нажать Ctrl+X. Произойдет перезагрузка системы, после которой она будет загружена под управлением учетной записи **root**.
6. Войти в консоль, ввести следующие команды:

```
mount -a
pam_tally --user wabadmin --reset
pam_tally2 --user wabadmin --reset
```

7. Перезагрузить устройство командой **reboot**.
8. После перезагрузки попробовать войти под учетной записью **wabadmin** (пароль: **!QAZ2wsx**).
9. Чтобы получить права суперпользователя, после авторизации ввести следующие команды:

```
super
Password: !QAZ2wsx
sudo -i
Password: !QAZ2wsx
```

10. Если авторизация все ещё невозможна, повторить шаги 1-5.
11. После загрузки системы ввести следующие команды:

```
mount -a
parsec_pam del
passwd wabadmin ( )
parsec_pam add
```

12. Перезагрузить устройство командой `reboot` и повторить шаги 8-9.

9.3. Восстановления начального состояния системы

Возможны ситуации, когда требуется восстановить начальное состояние системы, для этого необходимо войти в консоль и выполнить следующие команды:

```
/etc/init.d/wab-gui stop
/etc/init.d/wabcore stop
/etc/init.d/wabengine stop
/etc/init.d/postgresql restart
WABSqlInit -f -y
reboot
```