

Аутентификация пользователя на терминальном сервере по сертификату

При выключенном Kerberos на десктоп-клиенте

В этом разделе описано, как настроить аутентификацию пользователя на терминальном сервере по сертификату при выключенном Kerberos на десктоп-клиенте.

Linux

Для повышения безопасности подключения пользователей к терминальным серверам настройте аутентификацию по сертификату. Это можно сделать тремя способами:

Способ 1. Через условный блок, используя один порт для подключения

1. Для этого после установки терминального агента в конце файла `/etc/ssh/sshd_config` (ПЕД ОС, AstraLinux, Debian, OpenSUSE)/ `/etc/openssh/sshd_config` (ALT Linux) добавьте строки:

```
TrustedUserCAKeys /etc/termit-agent/termit-ssh-ca.pub
AuthenticationMethods publickey,password
Match User ИМЯ_АДМИНИСТРАТОРА_СИСТЕМЫ
    AuthenticationMethods password publickey
```

Таким образом обычным пользователям разрешается заходить только с использованием временных сертификатов, подписанных доверенным ключом. При этом администратор системы может подключаться с использованием пароля или ключа, как и до внесения изменений.

2. Перезагрузите sshd с помощью команды:

```
sudo systemctl restart sshd
```

Способ 2. Через условный блок, используя два порта (для пользователей и администратора)

1. Для этого после установки терминального агента в файле `/etc/ssh/sshd_config` (ПЕД ОС, AstraLinux, Debian, OpenSUSE)/ `/etc/openssh/sshd_config` (ALT Linux) раскомментируйте строку с указанием порта, если она ранее не была изменена (Смотрите [Ручное изменение портов в файле конфигурации шлюза и агента](#)).

2. Ниже добавьте похожую строку с указанием произвольного порта, по которому сможет подключаться только администратор системы:

```
Port 22
Port 2222
```

Где:

- **Port 22** — порт для пользователей;
- **Port 2222** — порт для администратора.

3. В том же файле в конце добавьте строки:

```
Match LocalPort 22
    TrustedUserCAKeys /etc/termite-agent/termite-ssh-ca.pub
    AuthenticationMethods publickey,password
Match LocalPort 2222, User ИМЯ_АДМИНИСТРАТОРА_СИСТЕМЫ
    AuthenticationMethods password publickey
```

Таким образом обычным пользователям разрешается заходить только с использованием временных сертификатов, подписанных доверенным ключом, но только через порт 22. При этом администратор системы может подключаться с использованием пароля или ключа, как и до внесения изменений, но только через порт 2222.

4. Перезагрузите sshd с помощью команды:

```
sudo systemctl restart sshd
```

BASH |



На системах с SELinux (например РЕД ОС) могут возникнуть проблемы при использовании нового порта для SSH. Чтобы разрешить сервису SSH использовать новый порт, выполните команду:

```
sudo semanage port -a -t ssh_port_t -p tcp 2222
```

BASH |

Способ 3. Через дублирование ssh-сервиса

1. Создайте копии конфигурационного файла с помощью команды:

- i. Для РЕД ОС, AstraLinux, Debian, OpenSUSE:

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config_crt_pwd
```

BASH |

- ii. Для ALT Linux:

```
sudo cp /etc/openssh/sshd_config /etc/openssh/sshd_config_crt_pwd
```

BASH |

2. В новом конфигурационном файле измените строку с портом на любой другой:

```
Port 2222
```

3. Создайте новый сервис sshd через копирование конфигурации существующего сервиса с помощью команды:

```
sudo cp /usr/lib/systemd/system/sshd.service  
/usr/lib/systemd/system/sshd_crt_pwd.service
```

BASH | 

4. Измените строку ExecStart (укажите путь до нового конфигурационного файла sshd_config_crt_pwd) в скопированном файле:

i. Для РЕД ОС, AstraLinux, Debian, OpenSUSE:

```
ExecStart=/usr/sbin/sshd -D -f /etc/ssh/sshd_config_crt_pwd
```

ii. Для ALT Linux:

```
ExecStart=/usr/sbin/sshd -D -f /etc/openssh/sshd_config_crt_pwd
```

5. Запустите и добавьте в автозагрузку новый сервис с помощью команды:

```
sudo systemctl enable --now sshd_crt_pwd.service
```

BASH | 



На системах с SELinux (например РЕД ОС) могут возникнуть проблемы при использовании нового порта для SSH. Чтобы разрешить сервису SSH использовать новый порт, выполните команду:

```
sudo semanage port -a -t ssh_port_t -p tcp 2222
```

BASH | 

6. Добавьте в конце конфигурационного файла первого экземпляра ssh-сервиса /etc/ssh/sshd_config /etc/openssh/sshd_config (ALT Linux):

i. Для РЕД ОС, AstraLinux, Debian, OpenSUSE:

```
AllowUsers ИМЯ_АДМИНИСТРАТОРА_СИСТЕМЫ
```

ii. Для ALT Linux:

```
AllowUsers ИМЯ_АДМИНИСТРАТОРА_СИСТЕМЫ
```

Таким образом по порту 22 сможет подключаться только администратор системы.

7. Добавьте в конце конфигурационного файла первого экземпляра ssh-сервиса /etc/ssh/sshd_config_crt_pwd :

i. Для РЕД ОС, AstraLinux, Debian, OpenSUSE:

```
TrustedUserCAKeys /etc/termit-agent/termit-ssh-ca.pub  
AuthenticationMethods publickey,password
```

ii. Для ALT Linux:

```
TrustedUserCAKeys /etc/termit-agent/termit-ssh-ca.pub  
AuthenticationMethods publickey,password
```

Таким образом по 2222 порту смогут подключаться остальные пользователи, которые предоставят сертификат, подписанный доверенным ключом.

8. Перезапустите сервисы с помощью команды:

```
sudo systemctl restart sshd && sudo systemctl restart sshd_crt_pwd
```

BASH |

Windows



На TC Windows необходимо скачать и установить [OpenSSH версии v9.5.0.0p1-Beta](#).

Для повышения безопасности подключения пользователей к терминальным серверам настройте аутентификацию по сертификату. Для этого после установки терминального агента:

1. Настройте терминальный агент в конфигурационном файле

C:\ProgramData\ssh\sshd_config. Для этого:

a. В файле конфигурации измените параметр **Port**:

```
Port 13389
```

b. Перезагрузите sshd с помощью команды:

```
Restart-Service sshd -Force
```

Подробнее смотрите [в разделе](#).

2. Настройте ssh. Это можно сделать двумя способами:

Способ 1. Через условный блок, используя один порт для подключения

1. Откройте конфигурационный файл SSH (C:\ProgramData\ssh\sshd_config) и перед строками:

```
Match Group administrators
    AuthorizedKeysFile __PROGRAMDATA__/ssh/administrators_authorized_keys
```

добавьте:

```
casignaturealgorithms ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-
nistp384,ecdsa-sha2-nistp521,sk-ssh-ed25519@openssh.com,sk-ecdsa-sha2-
nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256,ssh-rsa

PubkeyAcceptedAlgorithms=ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-
nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-
v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,sk-ssh-ed25519-
cert-v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,rsa-sha2-
512-cert-v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-
ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ssh-
ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-
sha2-256,ssh-rsa-cert-v01@openssh.com,ssh-rsa

TrustedUserCAKeys "C:\Program Files\TermitAgent\config\termit-ssh-ca.pub"

AuthenticationMethods publickey

Match User ИМЯ_АДМИНИСТРАТОРА_СИСТЕМЫ
    AuthenticationMethods password publickey
```

Таким образом обычным пользователям разрешается заходить только с использованием временных сертификатов, подписанных доверенным ключом. При этом администратор системы может подключаться с использованием пароля или ключа, как и до внесения изменений.

2. Перезагрузите sshd с помощью команды:

```
Restart-Service sshd -Force
```

Способ 2. Через условный блок, используя два порта (для пользователей и администратора)

1. В конфигурационном файле SSH (C:\ProgramData\ssh\sshd_config) добавьте похожую строку с указанием произвольного порта, по которому сможет подключаться только администратор системы:

```
Port 2222
```

Где:

- **Port 2222** — порт для администратора.

2. В том же файле перед строками:

```
Match Group administrators
    AuthorizedKeysFile __PROGRAMDATA__/ssh/administrators_authorized_keys
```

Добавьте:

```
Match LocalPort 13389
    ciphersuitealgorithms ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-
nistp384,ecdsa-sha2-nistp521,sk-ssh-ed25519@openssh.com,sk-ecdsa-sha2-
nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256,ssh-rsa

    PubkeyAcceptedAlgorithms=ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-
nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-
v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,sk-ssh-ed25519-
cert-v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,rsa-sha2-
512-cert-v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-
ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ssh-
ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-
sha2-256,ssh-rsa-cert-v01@openssh.com,ssh-rsa

    TrustedUserCAKeys "C:\Program Files\TermitAgent\config\termit-ssh-
ca.pub"

    AuthenticationMethods publickey

Match LocalPort 2222, User ИМЯ_АДМИНИСТРАТОРА_СИСТЕМЫ
    AuthenticationMethods password publickey
```

3. Перезагрузите sshd с помощью команды:

```
Restart-Service sshd -Force
```



Чтобы разрешить сервису SSH использовать новый порт, требуется открыть входящее подключение. Для этого выполните команду:

```
New-NetFirewallRule -DisplayName "SSH Range" -Direction Inbound -Protocol TCP
-LocalPort 13389,2222 -Action Allow
```

4. В файле конфигурации агента "C:\Program Files\TermitAgent\config" измените параметр **TERMIT_AGENT_RDP_PARAMS**:

```
TERMIT_AGENT_RDP_PARAMS={"rdp0verSshPort": 13389}
```

5. Перезапустите агент с помощью команды

```
Restart-Service termit-agent -Force
```



При включенном Kerberos на десктоп-клиенте

В этом разделе описано, как настроить аутентификацию пользователя на терминальном сервере по сертификату при включенном Kerberos на десктоп-клиенте.

Linux

Для повышения безопасности подключения пользователей к терминальным серверам настройте аутентификацию по сертификату. Это можно сделать тремя способами:

Способ 1. Через условный блок, используя один порт для подключения

1. Для этого после установки терминального агента в конце файла `/etc/ssh/sshd_config` (ПЕД ОС, AstraLinux, Debian, OpenSUSE)/ `/etc/openssh/sshd_config` (ALT Linux) добавьте строки:

```
TrustedUserCAKeys /etc/termit-agent/termit-ssh-ca.pub
AuthenticationMethods publickey
Match User ИМЯ_АДМИНИСТРАТОРА_СИСТЕМЫ
    AuthenticationMethods password publickey
```



Таким образом обычным пользователям разрешается заходить только с использованием временных сертификатов, подписанных доверенным ключом. При этом администратор системы может подключаться с использованием пароля или ключа, как и до внесения изменений.

2. Перезагрузите sshd с помощью команды:

```
sudo systemctl restart sshd
```



Способ 2. Через условный блок, используя два порта (для пользователей и администратора)

1. Для этого после установки терминального агента в файле `/etc/ssh/sshd_config` (ПЕД ОС, AstraLinux, Debian, OpenSUSE)/ `/etc/openssh/sshd_config` (ALT Linux) раскомментируйте строку с указанием порта, если она ранее не была изменена (Смотрите [Ручное изменение портов в файле конфигурации шлюза и агента](#)).
2. Ниже добавьте похожую строку с указанием произвольного порта, по которому сможет подключаться только администратор системы:

```
Port 22
Port 2222
```

Где:

- **Port 22** — порт для пользователей;
- **Port 2222** — порт для администратора.

3. В том же файле в конце добавьте строки:

```
Match LocalPort 22
    TrustedUserCAKeys /etc/termit-agent/termit-ssh-ca.pub
    AuthenticationMethods publickey
Match LocalPort 2222, User ИМЯ_АДМИНИСТРАТОРА_СИСТЕМЫ
    AuthenticationMethods password publickey
```

Таким образом обычным пользователям разрешается заходить только с использованием временных сертификатов, подписанных доверенным ключом, но только через порт 22. При этом администратор системы может подключаться с использованием пароля или ключа, как и до внесения изменений, но только через порт 2222.

4. Перезагрузите sshd с помощью команды:

```
sudo systemctl restart sshd
```



На системах с SELinux (например РЕД ОС) могут возникнуть проблемы при использовании нового порта для SSH. Чтобы разрешить сервису SSH использовать новый порт, выполните команду:

```
sudo semanage port -a -t ssh_port_t -p tcp 2222
```

Способ 3. Через дублирование ssh-сервиса

1. Создайте копии конфигурационного файла с помощью команды:

i. Для РЕД ОС, AstraLinux, Debian, OpenSUSE:

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.crt_pwd
```

ii. Для ALT Linux:

```
sudo cp /etc/openssh/sshd_config /etc/openssh/sshd_config.crt_pwd
```

2. В новом конфигурационном файле измените строку с портом на любой другой:

Port 2222

3. Создайте новый сервис sshd через копирование конфигурации существующего сервиса с помощью команды:

```
sudo cp /usr/lib/systemd/system/sshd.service  
/usr/lib/systemd/system/sshd_crt_pwd.service
```

BASH |

4. Измените строку ExecStart (укажите путь до нового конфигурационного файла sshd_config_crt_pwd) в скопированном файле:

- i. Для РЕД ОС, AstraLinux, Debian, OpenSUSE:

```
ExecStart=/usr/sbin/sshd -D -f /etc/ssh/sshd_config_crt_pwd
```

- ii. Для ALT Linux:

```
ExecStart=/usr/sbin/sshd -D -f /etc/openssh/sshd_config_crt_pwd
```

5. Запустите и добавьте в автозагрузку новый сервис с помощью команды:

```
sudo systemctl enable --now sshd_crt_pwd.service
```

BASH |



На системах с SELinux (например РЕД ОС) могут возникнуть проблемы при использовании нового порта для SSH. Чтобы разрешить сервису SSH использовать новый порт, выполните команду:

```
sudo semanage port -a -t ssh_port_t -p tcp 2222
```

BASH |

6. Добавьте в конце конфигурационного файла первого экземпляра ssh-сервиса /etc/ssh/sshd_config /etc/openssh/sshd_config (ALT Linux):

- i. Для РЕД ОС, AstraLinux, Debian, OpenSUSE:

```
AllowUsers ИМЯ_АДМИНИСТРАТОРА_СИСТЕМЫ
```

- ii. Для ALT Linux:

```
AllowUsers ИМЯ_АДМИНИСТРАТОРА_СИСТЕМЫ
```

Таким образом по порту 22 сможет подключаться только администратор системы.

7. Добавьте в конце конфигурационного файла первого экземпляра ssh-сервиса /etc/ssh/sshd_config_crt_pwd :

- i. Для РЕД ОС, AstraLinux, Debian, OpenSUSE:

```
TrustedUserCAKeys /etc/termit-agent/termit-ssh-ca.pub  
AuthenticationMethods publickey
```

ii. Для ALT Linux:

```
TrustedUserCAKeys /etc/termit-agent/termit-ssh-ca.pub  
AuthenticationMethods publickey
```

Таким образом по 2222 порту смогут подключаться остальные пользователи, которые предоставят сертификат, подписанный доверенным ключом.

8. Перезапустите сервисы с помощью команды:

```
sudo systemctl restart sshd && sudo systemctl restart sshd_crt_pwd
```

BASH |

Windows



Внутренние пользователи осуществляют подключение к серверу по стандартному RDP-порту 3389, в то время как внешние пользователи подключаются через защищённый туннель, использующий порт 13389.

Для повышения безопасности подключения пользователей к терминальным серверам настройте аутентификацию по сертификату. Для этого после установки терминального агента выполните настройки из раздела .

Установка балансировщика нагрузки

В этом разделе приведены инструкции по созданию балансировщика нагрузки с высокой доступностью, используя HAProxy и Keepalived. Эти инструменты помогут вам разработать отказоустойчивую архитектуру: она обеспечит минимальное время простоя и повысит производительность системы.

Если вы планируете конфигурацию с одним брокером, то пропустите установку балансировщика нагрузки и перейдите к [установке брокера](#).



В текущей реализации поддерживается только TCP-балансировка нагрузки, то есть балансировщик должен работать в режиме SSL Passthrough.

Например, SSL Bridging на порту 443 для связи десктоп-клиент - брокер. При этом внутренний трафик связи брокер - агент должен передаваться в режиме SSL Passthrough.

Ниже приведены инструкции по установке и настройке HAProxy и Keepalived. При использовании другого балансировщика нагрузки убедитесь, что он поддерживает и настроен на работу в режимах, описанных выше.

Перейти к:

- [Установке и настройке HAProxy](#)
- [Установке и настройке Keepalived](#)

Установка брокера

В этом разделе описаны шаги по установке и первичной настройке сервера с ролью брокер, входящего в состав STD «Термит».



Не поддерживается развертывание БД и брокера на одном сервере.

РЕД ОС

Перед установкой брокера выполните шаги 1-2 по установке Docker, Docker Compose или перейдите к шагу 3 (установочный скрипт выполнит шаги 1-2, запрашивая подтверждение):



Для установки компонентов необходимы настроенные репозитории.

1. Чтобы установить Docker, Docker Compose, выполните команду:

```
sudo dnf install docker-ce docker-ce-cli docker-compose
```

BASH |

2. Чтобы установленные компоненты добавить в автозагрузку, выполните команду:

```
sudo systemctl enable docker --now
```

BASH |

3. Скопируйте дистрибутив на сервер.

4. Распакуйте архив с помощью команды:

```
unzip termit-2.*.*-*.zip
```

BASH |

5. При необходимости назначьте права на запуск скрипта с помощью команды:

```
sudo chmod +x ./install.sh
```

BASH |

6. Запустите скрипт:

```
sudo ./install.sh install
```

BASH |

7. Введите пароль администратора системы.

8. Укажите имя узла брокера. Имя может быть любым.

9. Появится сообщение:

```
«What do you want to do? (1/2)
1. Install first node of a new cluster
2. Add a new node to existing cluster
Enter 1 or 2»
```

Укажите «1».

10. Введите FQDN адрес брокера (инсталляция «Standalone») или балансировщика (инсталляция «High Availability» (HA)), например «broker.example.com». Портал будет доступен по этому адресу.

11. Появится сообщение:

```
Do you want to connect to an existing database or create a new one? (1/2)

1. Connect to an existing database
2. Create new database

Enter 1 or 2?
```

a. Если вы хотите подключиться к существующей базе данных (БД), то:

- i. Укажите «1».
- ii. Укажите имя хоста БД, например «db.example.com».
- iii. Укажите порт «5432».
- iv. Укажите имя БД, например «example».
- v. Укажите имя пользователя БД, например «termit».
- vi. Введите пароль для БД.

b. Если вы хотите создать новую базу данных (БД), то:

- i. Укажите «2».
- ii. Укажите имя хоста БД, например «db.example.com».
- iii. Укажите порт «5432».
- iv. Укажите имя новой БД.
- v. Укажите имя пользователя БД, например «termit».
- vi. Введите пароль для БД.

Установка брокера занимает около двух минут. Во время запуска отображается ключ шифрования БД, который необходимо сохранить. Этот ключ нужен для установки дополнительных брокеров.

```
----PLEASE SAVE YOUR ENCRYPTION KEY----
d0b6f362e51a1549480180432e224474756af0c
```

Для подтверждения успешной операции в браузере, в адресной строке, введите адрес брокера `https://broker.example.com`. В появившемся окне аутентификации укажите логин «tadm» и пароль «admin» от учетной записи по умолчанию.



- Если брокер установился с ошибкой, то проверьте логи в контейнерах: «config-service» и «broker-client» с помощью команды:

```
sudo docker logs %ID_Контейнера%
```

BASH |

- В случае переустановки брокера выполните шаги [по деинсталляции](#).
- Подробнее о настройках компонентов операционной системы [можно прочесть на официальном сайте Astra Linux](#).

Astra Linux

Перед установкой брокера выполните шаги 1-2 по установке Docker, Docker Compose или перейдите к шагу 3 (установочный скрипт выполнит шаги 1-2, запрашивая подтверждение):



Для установки компонентов необходимы настроенные репозитории.

1. Чтобы установить Docker, Docker Compose, выполните команду:

```
sudo apt install docker.io docker-compose
```

BASH |

2. Чтобы установленные компоненты добавить в автозагрузку, выполните команду:

```
sudo systemctl start docker
```

BASH |

3. Скопируйте дистрибутив на сервер.

4. Распакуйте архив с помощью команды:

```
unzip termit-2.*.*-*.zip
```

BASH |

5. При необходимости назначьте права на запуск скрипта с помощью команды:

```
sudo chmod +x ./install.sh
```

BASH |

6. Запустите скрипт:

```
sudo ./install.sh install
```

BASH |

7. Введите пароль администратора системы.

8. Укажите имя узла брокера. Имя может быть любым.

9. Появится сообщение:

```
«What do you want to do? (1/2)
1. Install first node of a new cluster
2. Add a new node to existing cluster
Enter 1 or 2»
```

Укажите «1».

10. Введите FQDN адрес брокера (инсталляция «Standalone») или балансировщика (инсталляция «HA»), например «broker.example.com». Портал будет доступен по этому адресу.

11. Появится сообщение:

```
Do you want to connect to an existing database or create a new one? (1/2)

1. Connect to an existing database
2. Create new database

Enter 1 or 2?
```

a. Если вы хотите подключиться к существующей базе данных (БД), то:

- i. Укажите «1».
- ii. Укажите имя хоста БД, например «db.example.com».
- iii. Укажите порт «5432».
- iv. Укажите имя БД, например «example».
- v. Укажите имя пользователя БД, например «termit».
- vi. Введите пароль для БД.

b. Если вы хотите создать новую базу данных (БД), то:

- i. Укажите «2».
- ii. Укажите имя хоста БД, например «db.example.com».
- iii. Укажите порт «5432».
- iv. Укажите имя новой БД.
- v. Укажите имя пользователя БД, например «termit».
- vi. Введите пароль для БД.

Установка брокера занимает около двух минут. Во время запуска отображается ключ шифрования БД, который необходимо сохранить. Этот ключ нужен для установки дополнительных брокеров.

----PLEASE SAVE YOUR ENCRYPTION KEY----
d0b6f362e51a1549480180432e224474756af0c

Для подтверждения успешной операции в браузере, в адресной строке, введите адрес брокера `https://broker.example.com`. В появившемся окне аутентификации укажите логин «tadm» и пароль «admin» от учетной записи по умолчанию.



- Если брокер установился с ошибкой, то проверьте логи в контейнерах: «config-service» и «broker-client» с помощью команды:

```
sudo docker logs %ID_Контейнера%
```

BASH |

- В случае переустановки брокера выполните шаги [по деинсталляции](#).
- Подробнее о настройках компонентов операционной системы [можно прочесть на официальном сайте Astra Linux](#).

Debian

Перед установкой брокера выполните шаги 1-2 по установке Docker, Docker Compose или перейдите к шагу 3 (установочный скрипт выполнит шаги 1-2, запрашивая подтверждение):



Для установки компонентов необходимы настроенные репозитории.

1. Чтобы установить Docker, Docker Compose, выполните команду:

```
sudo apt install docker.io docker-compose
```

BASH |

2. Чтобы установленные компоненты добавить в автозагрузку, выполните команду:

```
sudo systemctl enable docker --now
```

BASH |

3. Распакуйте архив с помощью команды:

```
unzip termit-2.*.*-*.zip
```

BASH |

4. Запустите установку с помощью команды:

```
sudo ./install.sh install
```

BASH |

5. Введите пароль администратора системы.
6. Укажите имя узла брокера. Имя может быть любым.
7. Появится сообщение:

«What do you want to do? (1/2)
1. Install first node of a new cluster
2. Add a new node to existing cluster
Enter 1 or 2»

Укажите «1».

8. Введите FQDN адрес брокера (инсталляция «Standalone») или балансировщика (инсталляция «HA»), например «broker.example.com». Портал будет доступен по этому адресу.

9. Появится сообщение:

Do you want to connect to an existing database or create a new one? (1/2)

1. Connect to an existing database
2. Create new database

Enter 1 or 2?

a. Если вы хотите подключиться к существующей базе данных (БД), то:

- i. Укажите «1».
- ii. Укажите имя хоста БД, например «db.example.com».
- iii. Укажите порт «5432».
- iv. Укажите имя БД, например «example».
- v. Укажите имя пользователя БД, например «termit».
- vi. Введите пароль для БД.

b. Если вы хотите создать новую базу данных (БД), то:

- i. Укажите «2».
- ii. Укажите имя хоста БД, например «db.example.com».
- iii. Укажите порт «5432».
- iv. Укажите имя новой БД.
- v. Укажите имя пользователя БД, например «termit».
- vi. Введите пароль для БД.

Установка брокера занимает около двух минут. Во время запуска отображается ключ шифрования БД, который необходимо сохранить. Этот ключ нужен для установки дополнительных брокеров.

----PLEASE SAVE YOUR ENCRYPTION KEY----
d0b6f362e51a1549480180432e224474756af0c

Для подтверждения успешной операции в браузере, в адресной строке, введите адрес брокера `https://broker.example.com`. В появившемся окне аутентификации укажите логин «tadm» и пароль «admin» от учетной записи по умолчанию.

ALT Linux

Перед установкой брокера выполните шаги 1-2 по установке Docker, Docker Compose или перейдите к шагу 3 (установочный скрипт выполнит шаги 1-2, запрашивая подтверждение):



Для установки компонентов необходимы настроенные репозитории.

1. Чтобы установить Docker, Docker Compose, выполните команду:

```
sudo apt-get install docker-ce docker-compose
```

BASH |



а. Проверьте, установлен ли Docker Compose v2 в качестве плагина с помощью команды:

```
docker compose version
```



Если вывод команды содержит версию Docker Compose, значит, у вас установлен плагин. (Не путайте с `docker-compose --version`).

б. Для плагина Docker Compose v2 создайте символическую ссылку для корректной работы установочного скрипта:

```
sudo ln -s /usr/lib/docker/cli-plugins/docker-compose  
/usr/local/bin/docker-compose
```



2. Чтобы установленные компоненты добавить в автозагрузку, выполните команду:

```
sudo systemctl enable docker --now
```

BASH |

3. Распакуйте архив с помощью команды:

```
unzip ./termit-2.1*.*-*.zip
```

BASH |

4. Запустите установку с помощью команды:

```
sudo ./install.sh install
```

BASH |

5. Введите пароль администратора системы.

6. Укажите имя узла брокера. Имя может быть любым.

7. Появится сообщение:

```
«What do you want to do? (1/2)
1. Install first node of a new cluster
2. Add a new node to existing cluster
Enter 1 or 2»
```

Укажите «1».

8. Введите FQDN адрес брокера (инсталляция «Standalone») или балансировщика (инсталляция «HA»), например «broker.example.com». Портал будет доступен по этому адресу.

9. Появится сообщение:

```
Do you want to connect to an existing database or create a new one? (1/2)

1. Connect to an existing database
2. Create new database

Enter 1 or 2?
```

a. Если вы хотите подключиться к существующей базе данных (БД), то:

- i. Укажите «1».
- ii. Укажите имя хоста БД, например «db.example.com».
- iii. Укажите порт «5432».
- iv. Укажите имя БД, например «example».
- v. Укажите имя пользователя БД, например «termit».
- vi. Введите пароль для БД.

b. Если вы хотите создать новую базу данных (БД), то:

- i. Укажите «2».
- ii. Укажите имя хоста БД, например «db.example.com».
- iii. Укажите порт «5432».
- iv. Укажите имя новой БД.
- v. Укажите имя пользователя БД, например «termit».
- vi. Введите пароль для БД.

Установка брокера занимает около двух минут. Во время запуска отображается ключ шифрования БД, который необходимо сохранить. Этот ключ нужен для установки дополнительных брокеров.

```
----PLEASE SAVE YOUR ENCRYPTION KEY----
d0b6f362e51a1549480180432e224474756af0c
```

Для подтверждения успешной операции в браузере, в адресной строке, введите адрес брокера `https://broker.example.com`. В появившемся окне аутентификации укажите логин «tadm» и пароль «admin» от учетной записи по умолчанию.



- Если брокер установился с ошибкой, то проверьте логи в контейнерах: «config-service» и «broker-client» с помощью команды:

```
sudo docker logs %ID_Контейнера%
```

BASH |

- В случае переустановки брокера выполните шаги [по деинсталляции](#).
- Подробнее о настройках компонентов операционной системы [можно прочесть на официальном сайте Astra Linux](#).

OpenSUSE

Перед установкой брокера выполните шаги 1-2 по установке Docker, Docker Compose или перейдите к шагу 3 (установочный скрипт выполнит шаги 1-2, запрашивая подтверждение):



Для установки компонентов необходимы настроенные репозитории.

1. Чтобы установить Docker, Docker Compose, выполните команду:

```
sudo zypper install docker docker-compose docker-compose-switch
```

BASH |

2. Чтобы установленные компоненты добавить в автозагрузку, выполните команду:

```
sudo systemctl enable docker --now
```

BASH |

3. Скопируйте дистрибутив на сервер.

4. Распакуйте архив с помощью команды:

```
unzip ./termit-2.1*.*-*.zip
```

BASH |

5. При необходимости назначьте права на запуск скрипта с помощью команды:

```
sudo chmod +x ./install.sh
```

BASH |

6. Запустите скрипт:

```
sudo ./install.sh install
```

BASH |

7. Введите пароль администратора системы.

8. Укажите имя узла брокера. Имя может быть любым.

9. Появится сообщение:

```
«What do you want to do? (1/2)
1. Install first node of a new cluster
2. Add a new node to existing cluster
Enter 1 or 2»
```

Укажите «1».

10. Введите FQDN адрес брокера (инсталляция «Standalone») или балансировщика (инсталляция «HA»), например «broker.example.com». Портал будет доступен по этому адресу.

11. Появится сообщение:

```
Do you want to connect to an existing database or create a new one? (1/2)

1. Connect to an existing database
2. Create new database

Enter 1 or 2?
```

a. Если вы хотите подключиться к существующей базе данных (БД), то:

- i. Укажите «1».
- ii. Укажите имя хоста БД, например «db.example.com».
- iii. Укажите порт «5432».
- iv. Укажите имя БД, например «example».
- v. Укажите имя пользователя БД, например «termit».
- vi. Введите пароль для БД.

b. Если вы хотите создать новую базу данных (БД), то:

- i. Укажите «2».
- ii. Укажите имя хоста БД, например «db.example.com».
- iii. Укажите порт «5432».
- iv. Укажите имя новой БД.
- v. Укажите имя пользователя БД, например «termit».
- vi. Введите пароль для БД.

Установка брокера занимает около двух минут. Во время запуска отображается ключ шифрования БД, который необходимо сохранить. Этот ключ нужен для установки дополнительных брокеров.

----PLEASE SAVE YOUR ENCRYPTION KEY----
d0b6f362e51a1549480180432e224474756af0c

Для подтверждения успешной операции в браузере, в адресной строке, введите адрес брокера <https://broker.example.com>. В появившемся окне аутентификации укажите логин «tadm» и пароль «admin» от учетной записи по умолчанию.



- Если брокер установился с ошибкой, то проверьте логи в контейнерах: «config-service» и «broker-client» с помощью команды:

```
sudo docker logs %ID_Контейнера%
```

BASH |

- В случае переустановки брокера выполните шаги [по деинсталляции](#).
- Подробнее о настройках компонентов операционной системы [можно прочесть на официальном сайте Astra Linux](#).

Установка сертификата на десктоп-клиент

Для успешного подключения к СТД «Термит» необходимо, чтобы используемый корневой сертификат был добавлен в список доверенных на десктоп-клиенте.

Windows

1. Запустите сертификат двойным нажатием на него и выберите опцию **Установить сертификат**.
2. Выберите опцию **Текущий пользователь**:



При работе с правами администратора установка возможна в хранилище сертификатов компьютера (для всех пользователей).

3. Выберите опцию **Поместить все сертификаты в следующие хранилище**, нажмите **Обзор** и выберите **Доверенные корневые центры сертификации**.



При наличии промежуточного центра сертификации повторите шаги выше, выбрав хранилище **Промежуточные центры сертификации** на шаге 3.

4. Перезапустите браузер и проверьте доверие сертификату, открыв адрес брокера.

РЕД ОС

1. Скопируйте файл корневого сертификата в каталог `/etc/pki/ca-trust/source/anchors/` с помощью команды:

```
sudo cp %Путь_к_сертификату% /etc/pki/ca-trust/source/anchors/
```

BASH |

Где: **%Путь_к_сертификату%** — полный путь к файлу сертификата в формате PEM.

2. Чтобы применить изменения, выполните команды:

```
sudo update-ca-trust force-enable  
sudo update-ca-trust extract
```

BASH |

3. Перезапустите браузер и проверьте доверие сертификату, открыв адрес брокера.



Для систем Linux иногда необходима дополнительная ручная конфигурация хранилищ браузеров Firefox и Chrome\Chromium:

Chrome\Chromium

1. Перейдите в меню **Настройки > Конфиденциальность и безопасность > Безопасность > Настроить сертификаты** и перейдите на вкладку **Центры сертификации**.
2. Добавьте необходимый сертификат или цепочку сертификатов с помощью кнопки **Импорт**.
3. Укажите необходимый уровень доверия.

Firefox

1. Перейдите в **Настройки > Приватность и защита > Защита > Сертификаты > Просмотр сертификатов**.
2. Добавьте необходимый сертификат или цепочку сертификатов с помощью кнопки **Импорт**.
3. Укажите необходимый уровень доверия.

Astra Linux



Сертификат должен быть в формате **CRT**.

Если формат сертификата отличается, необходимо выполнить его конвертацию используя утилиту `openssl`, например:

- Если сертификат имеет кодировку DER :

```
openssl x509 -inform DER -in %Исходный_Сертификат% -out  
%Конечный_Сертификат%
```



- Если исходный сертификат имеет кодировку PEM :

```
openssl x509 -inform PEM -in %Исходный_Сертификат% -out  
%Конечный_Сертификат%
```



Где:

- **%Исходный_Сертификат%** — путь к исходному сертификату «certificate.cer».
- **%Конечный_Сертификат%** — путь к конечному сертификату, например «certificate.crt».

1. Скопируйте полученные выше сертификаты в каталог `/usr/local/share/ca-certificates` с помощью команды:

```
sudo cp %Путь_к_сертификату% /usr/local/share/ca-certificates
```



Где: **%Путь_к_сертификату%** — полный путь к файлу сертификата.

2. Чтобы применить изменения, выполните команду:

```
sudo update-ca-certificates
```

3. Перезапустите браузер и проверьте доверие сертификату, открыв адрес брокера.



Для систем Linux иногда необходима дополнительная ручная конфигурация хранилищ браузеров Firefox и Chrome\Chromium:

Chrome\Chromium

1. Перейдите в меню **Настройки > Конфиденциальность и безопасность > Безопасность > Настроить сертификаты** и перейдите на вкладку **Центры сертификации**.
2. Добавьте необходимый сертификат или цепочку сертификатов с помощью кнопки **Импорт**.
3. Укажите необходимый уровень доверия.

Firefox

1. Перейдите в **Настройки > Приватность и защита > Защита > Сертификаты > Просмотр сертификатов**.
2. Добавьте необходимый сертификат или цепочку сертификатов с помощью кнопки **Импорт**.
3. Укажите необходимый уровень доверия.

ALT Linux

Подробнее об установке сертификата можно прочесть [на официальном сайте](#).

1. Скопируйте корневой сертификат в хранилище сертификатов с помощью команды ниже. Сертификат должен быть в формате **.CRT**.

```
sudo cp %путь_к_сертификату% /etc/pki/ca-trust/source/anchors/
```

2. Обновите хранилище сертификатов с помощью команды:

```
sudo update-ca-trust
```

Для систем Linux иногда необходима дополнительная ручная конфигурация хранилищ браузеров Firefox и Chrome\Chromium:

Chrome\Chromium

1. Перейдите в меню **Настройки > Конфиденциальность и безопасность > Безопасность > Настроить сертификаты** и перейдите на вкладку **Центры сертификации**.
2. Добавьте необходимый сертификат или цепочку сертификатов с помощью кнопки **Импорт**.
3. Укажите необходимый уровень доверия.

Firefox

1. Перейдите в **Настройки > Приватность и защита > Защита > Сертификаты > Просмотр сертификатов**.
2. Добавьте необходимый сертификат или цепочку сертификатов с помощью кнопки **Импорт**.
3. Укажите необходимый уровень доверия.

OpenSUSE

1. Скопируйте файл корневого сертификата в каталог `/etc/pki/trust/anchors` с помощью команды:

```
sudo cp %Путь_к_сертификату% /etc/pki/trust/anchors
```

Где: **%Путь_к_сертификату%** — полный путь к файлу сертификата в формате PEM.

2. Обновите хранилище сертификатов с помощью команды:

```
sudo update-ca-certificates
```

3. Перезапустите браузер и проверьте доверие сертификату, открыв адрес брокера.



Для систем Linux иногда необходима дополнительная ручная конфигурация хранилищ браузеров Firefox и Chrome\Chromium:

Chrome\Chromium

1. Перейдите в меню **Настройки > Конфиденциальность и безопасность > Безопасность > Настроить сертификаты** и перейдите на вкладку **Центры сертификации**.
2. Добавьте необходимый сертификат или цепочку сертификатов с помощью кнопки **Импорт**.
3. Укажите необходимый уровень доверия.

Firefox

1. Перейдите в **Настройки > Приватность и защита > Защита > Сертификаты > Просмотр сертификатов**.
2. Добавьте необходимый сертификат или цепочку сертификатов с помощью кнопки **Импорт**.
3. Укажите необходимый уровень доверия.

MacOS

1. Запустите сертификат двойным нажатием на него, сертификат будет добавлен в приложение **Связка ключей**.
2. Найдите в приложении добавленный сертификат или цепочку сертификатов.
3. Укажите необходимый уровень доверия.

Установка десктоп-клиента

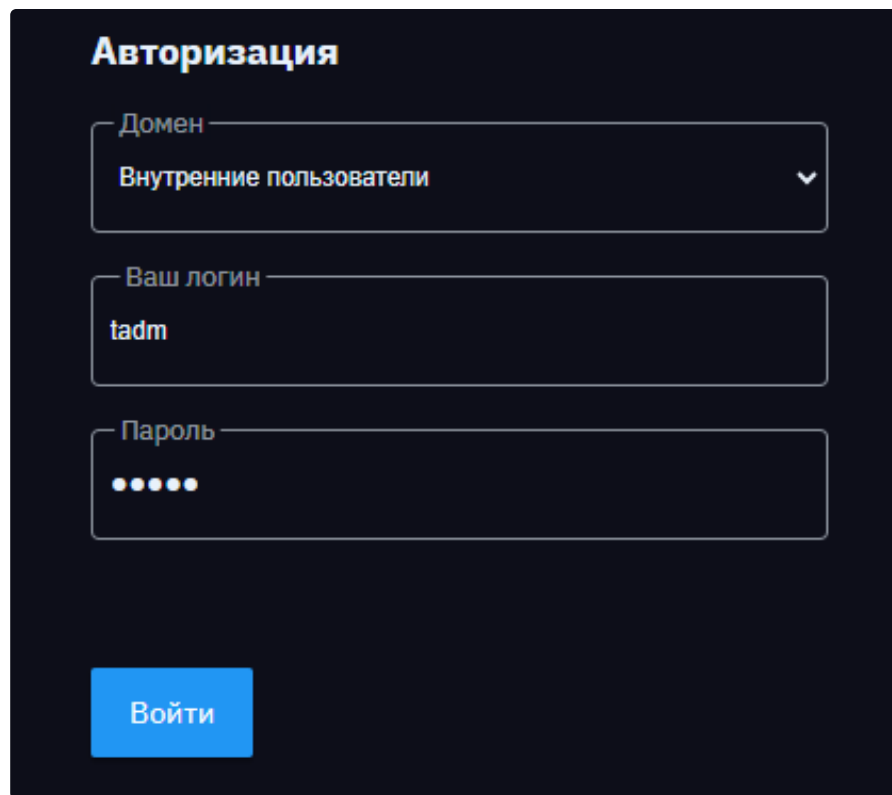
Чтобы установить десктоп-клиент:

1. В адресной строке браузера введите адрес брокера, например `https://broker.example.com`.
2. Выберите источник авторизации:
 - **Авто**. Система автоматически выберет LDAP-каталог из списка доступных каталогов или внутренних пользователей.
 - **Внутренние пользователи**. Вход будет выполнен под учетной записью локального администратора «tadm».
 - **Имя LDAP-каталога**, отображаемое полное имя которого было задано при добавлении в систему, например «ldap123».
3. Для входа под учетной записью локального администратора системы укажите в поле ввода:
 - **Ваш логин** — «tadm».
 - **Пароль** — пароль по умолчанию «admin».



Пользователь входит под доменной учетной записью. Атрибут для имени пользователя указан в настройках LDAP раздел тип LDAP в графе «Атрибут, используемый для поиска пользователя».

4. Нажмите [**Войти**].



Авторизация

Домен
Внутренние пользователи

Ваш логин
tadm

Пароль
•••••

Войти

После успешного входа в систему откроется интерфейс портала администрирования.

5. В левом меню выберите раздел **Скачать клиент**.
6. Выберите операционную систему и установите десктоп-клиент.

Windows

1. Перейдите на вкладку **Windows**.
2. Скачайте **Десктоп-клиент для Windows 7/8.1** или **Десктоп-клиент для Windows 10/11** и установите его.

Также можно установить десктоп-клиент в «тихом» режиме. Информация о ходе выполнения отображаться не будет. Для установки в таком режиме добавьте параметр `/S`. Пример: `"%путь до exe файла%\termiт-desktop-2...exe" /S`.

MacOS

1. Перейдите на вкладку **MAC OS**.
2. Скачайте **Десктоп-клиент для Mac OS** и выполните шаги по установке.
3. Скачайте XQuartz и выполните шаги по установке.
4. Скачайте и установите приложение Microsoft Remote Desktop из App Store.

При подключении к сессии на терминальном сервере Windows будет открыто приложение Microsoft Remote Desktop и окно для ввода пароля. После ввода пароля

запустится сессия. Во время сессии завершать работу приложения Microsoft Remote Desktop нельзя, так как это приведет к отключению от сессии.



Перед запуском десктоп-клиента в настройках необходимо разрешить использование СТД «Термит». Для этого выберите в меню **Apple > Системные настройки**, затем в боковом меню нажмите **Конфиденциальность и безопасность**, прокрутите вниз до параметра **Разрешить использование приложений, загруженных из:** и выберите **App Store и от подтвержденных разработчиков**.

Linux

Astra Linux



Десктоп-клиент поддерживает только FreeRDP версии 2 (freerdp2). При установке десктоп-клиента пакет `freerdp2` будет установлен автоматически.

1. Перейдите на вкладку **Linux**.
2. Скачайте **Десктоп-клиент для Linux deb**.
3. Установите клиент Термит:

```
sudo apt install ./termit-desktop-2.*.deb
```

BASH |

Где:

`./termit-desktop-2.*.deb` — название файла.



Установка в ЗПС

1. Перед установкой поместите публичный (открытый) ключ, скачанный с брокера по пути `https://broker.example.com/dist/termit_astra.key`, в директорию `/etc/digisig/keys` с помощью команды:

```
sudo cp %Путь_к_Открытому_Ключу% /etc/digisig/keys
```

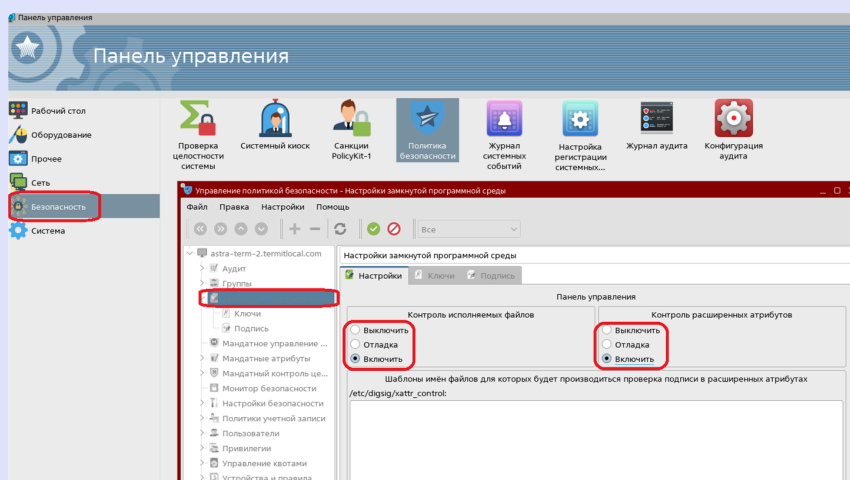
BASH |

2. Обновите ключи с помощью команды:

```
sudo update-initramfs -u -k all
```

BASH |

3. Перезагрузите ПК.
4. Включите режим замкнутой программной среды (ЗПС), если не был включен ранее:



5. Установите десктоп-клиент в обычном режиме.

При отображении «Ошибка сегментирования» ключ не может быть считан.

РЕД ОС

Десктоп-клиент поддерживает только FreeRDP версии 2 (freerdp2). При установке десктоп-клиента пакет `freerdp2` будет установлен автоматически.

1. Перейдите на вкладку **Linux**.
2. Скачайте **Десктоп-клиент для Linux rpm** и выполните шаги по установке.
3. Обновите репозиторий с помощью команды:

```
sudo dnf update
```

BASH |

4. Установите десктоп-клиент:

```
sudo dnf install ./termit-desktop-2.*.rpm
```

BASH |

Где:

`./termit-desktop-2.*.rpm` — название файла.

ALT Linux



Десктоп-клиент поддерживает только FreeRDP версии 2 (freerdp2). При установке десктоп-клиента пакет `freerdp2` будет установлен автоматически.

1. Перейдите на вкладку **Linux**.
2. Скачайте **Десктоп-клиент для Linux rpm**.
3. Обновите репозиторий с помощью команды:

```
sudo apt-get update
```

BASH |

4. Установите десктоп-клиент:

```
sudo apt-get install ./termit-desktop-2.*.rpm
```

BASH |

5. Для корректного запуска десктоп-клиента установите бит `setuid`:

```
sudo chmod 4755 /opt/Термит/chrome-sandbox
```

BASH |