

Установка дополнительного ПО на терминальный сервер

Установите дополнительное ПО перед установкой агента на терминальный сервер.

РЕД ОС



Проверьте, что все терминальные серверы введены в домен. Подробнее в статье [Ввод РЕД ОС в домен](#).

1. В файле конфигурации `sshd (/etc/ssh/sshd_config)`, в параметре `X11Forwarding`, укажите значение «yes».
2. Чтобы установить X2Go server на терминальный сервер, выполните команду:

```
sudo dnf install x2goserver-xsession x2goserver-fmbindings x2goserver-common x2goserver x2goagent
```

BASH |

3. Чтобы избежать ошибки при монтировании сетевых дисков, установите пакет `cifs-utils` с помощью команды:

```
sudo dnf install cifs-utils
```

BASH |

4. Для корректного перенаправления смарт-карт на сервер установите утилиту `socat` с помощью команды:

```
sudo dnf install socat
```

5. Установите агент, используя скрипт, полученный при создании сервера.

Astra Linux



Проверьте, что все терминальные серверы введены в домен. Подробнее в статье [Ввод Astra Linux в домен](#).

1. В файле конфигурации `sshd (/etc/ssh/sshd_config)`, в параметре `X11Forwarding`, укажите значение «yes».

- В файле конфигурации `/etc/systemd/logind.conf`, в параметре `KillUserProcesses` задайте значение «no» для корректной работы переключения сессии и перезагрузите терминальный сервер.

```
[Login]
#NAutoVTs=6
#ReserveVT=6
KillUserProcesses=no
#KillOnlyUsers=
#KillExcludeUsers=root
```

- Установите компоненты X2Go сервера с помощью команды:

```
sudo apt install x2goserver-xsession x2goserver-fmbindings x2goserver-common
x2goserver-x2goagent
```

BASH |

- Чтобы избежать ошибки при монтировании сетевых дисков, установите пакет `cifs-utils` с помощью команды:

```
sudo apt install cifs-utils
```

BASH |

- Для корректного перенаправления смарт-карт на сервер установите утилиту `socat` с помощью команды:

```
sudo apt install socat
```

- Установите агент, используя скрипт, полученный при создании сервера.

Debian



Проверьте, что все терминальные серверы введены в домен. Подробнее в статье [Ввод Debian в домен](#).

- В файле конфигурации `sshd` (`/etc/ssh/sshd_config`), в параметре `X11Forwarding`, укажите значение «yes».

- Установите компоненты X2Go сервера с помощью команды:

```
sudo apt install x2goserver-xsession x2goserver-fmbindings x2goserver-common
x2goserver-x2goagent
```

BASH |

- Чтобы избежать ошибки при монтировании сетевых дисков, установите пакет `cifs-utils` с помощью команды:

```
sudo apt install cifs-utils
```

BASH |

- Для корректного перенаправления смарт-карт на сервер установите утилиту `socat` с помощью команды:

```
sudo apt install socat
```



5. Установите агент, используя скрипт, полученный при создании сервера.

ALT Linux



Проверьте, что все терминальные серверы введены в домен. Подробнее в статье [Ввод ALT Linux в домен](#).

1. В файле конфигурации `sshd (/etc/openssh/sshd_config)`, в параметре `X11Forwarding`, укажите значение «yes».
2. В файле конфигурации `/etc/systemd/logind.conf`, в параметре `KillUserProcesses` задайте значение «no» для корректной работы переподключения сессии и перезагрузите терминальный сервер.
3. Установите компоненты X2Go сервера с помощью команды:

```
sudo apt-get install x2goserver-xsession x2goserver-fmbindings x2goserver-x2goagent
```

BASH |

4. Добавьте X2Go в автозапуск с помощью команды:

```
sudo systemctl enable x2goserver --now
```

BASH |

5. Чтобы избежать ошибки при монтировании сетевых дисков, установите пакет `cifs-utils` с помощью команды:

```
sudo apt-get install cifs-utils
```

BASH |

6. Для корректного перенаправления смарт-карт на сервер установите утилиту `socat` с помощью команды:

```
sudo apt-get install socat
```



7. Установите агент, используя скрипт, полученный при создании сервера.

Windows

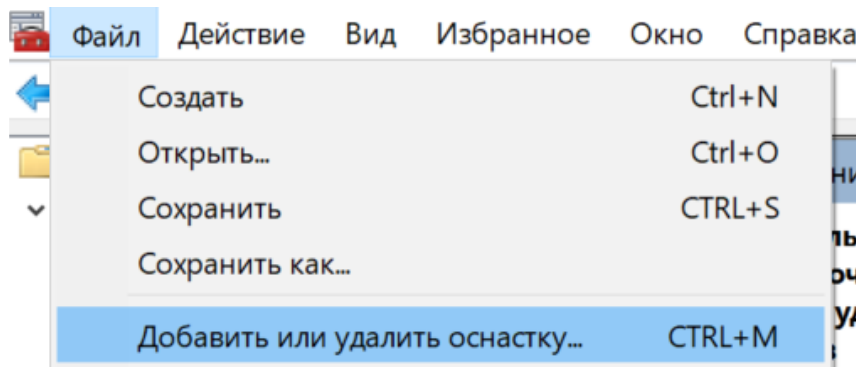


1. Для Windows Server 2012R2 и Windows Server 2016 (редакции ниже 1803) необходимо:
 - a. Установить утилиту curl.
 - b. Установочные файлы из архива `curl`, из каталога `bin`, разместить в системной директории `C:\Windows\system32`.
2. Проверьте, что все терминальные серверы введены в домен. Подробнее в статье Ввод Windows в домен.

1. Включите роль «Remote Desktop Session Host» («Узел сеансов удаленных рабочих столов»):
 - a. Откройте **Диспетчер серверов > Панель мониторинга**.
 - b. В правом верхнем углу нажмите [**Управление**].
 - c. Выберите **Добавить роли и компоненты**.
 - d. Нажмите [**Далее**].
 - e. На вкладке **Тип установки** оставьте по умолчанию опцию **Установка ролей и компонентов**.
 - f. Нажмите [**Далее**].
 - g. На вкладке **Выбор сервера** оставьте по умолчанию **Выберите сервер из пула серверов**.
 - h. Нажмите [**Далее**].
 - i. На вкладке **Роли сервера** включите опцию **Службы удаленных рабочих столов**.
 - j. Нажмите **Далее > Далее > Далее**.
 - k. На вкладке **Службы ролей** включите опцию **Remote Desktop Session Host (Узел сеансов удаленных рабочих столов)** и нажмите [**Добавить компоненты**].
 - l. Нажмите **Далее > Установить**.

После установки и добавления роли перезагрузите ВМ.

2. Включите политику «Разрешить удаленный запуск любых программ» и выключите политику «Ограничить пользователей служб удаленных рабочих столов одним сеансом служб удаленных рабочих столов»:
 - a. Откройте консоль MMC.
 - b. В левом верхнем углу нажмите [**Файл**] и выберите **Добавить или удалить оснастку**.

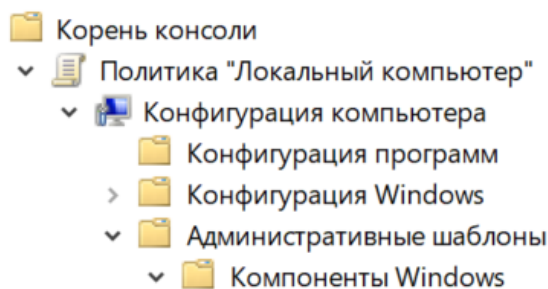


- c. В доступных оснастках выберите **Редактор объектов групповой политики**.
- d. В параметре **Объект групповой политики** оставьте по умолчанию **Локальный компьютер**.

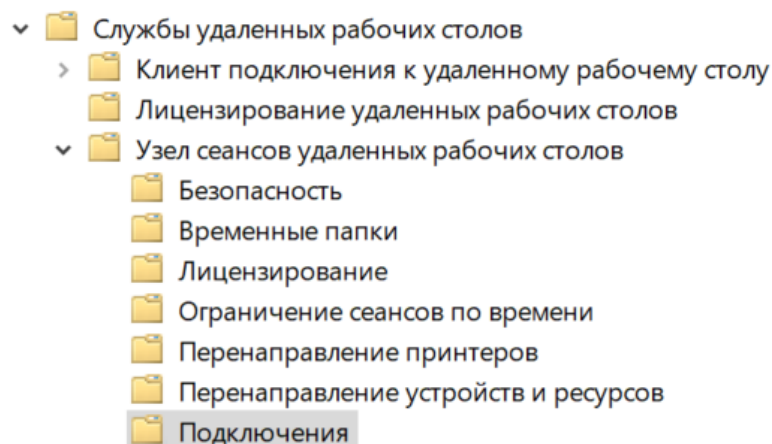


Параметры ниже могут быть настроены с использованием групповой политики или локальной.

- e. Нажмите **Готово** > **ОК**.
- f. Раскройте **Политика «Локальный компьютер»**.
- g. Раскройте **Конфигурация компьютера** > **Административные шаблоны** > **Компоненты Windows**.



- h. Выберите **Службы удаленных рабочих столов** > **Узел сеансов удаленных рабочих столов** > **Подключения**.



- i. Нажмите два раза левой кнопкой мыши на политику «Разрешить удаленный запуск любых программ».
- j. Активируйте опцию **Включено** и нажмите [**ОК**].

k. Нажмите два раза левой кнопкой мыши на политику «Ограничить пользователей служб удаленных рабочих столов одним сеансом служб удаленных рабочих столов».

l. Активируйте опцию **Отключено** и нажмите [**ОК**].

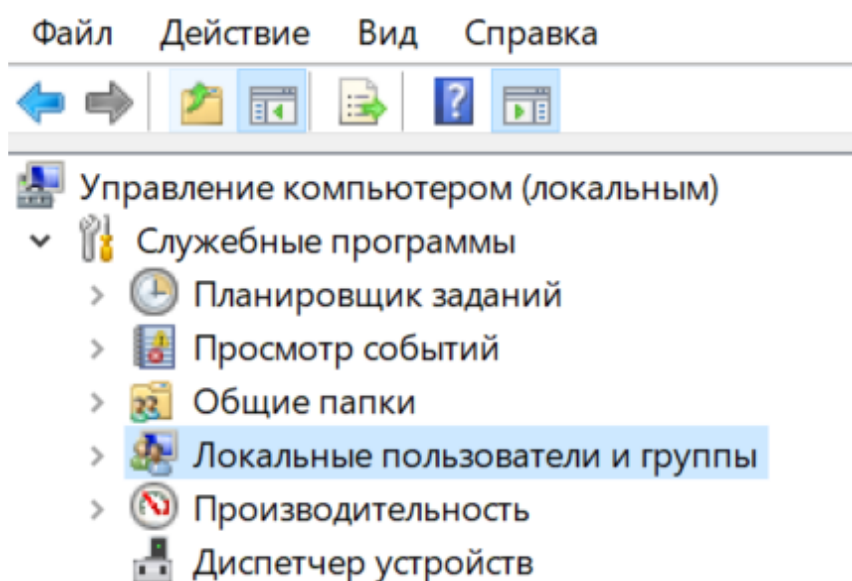
m. Откройте `cmd.exe` и примените политики с помощью команды `gpupdate /force` или перезагрузите сервер.

После успешной операции в выводе команды появится сообщение «Computer Policy update has completed successfully».

3. Настройте разрешение на подключение пользователей по RDP:

a. Удобным способом откройте **Управление компьютером**.

b. Выберите **Локальные пользователи и группы**.



c. Выберите **Группы > Пользователи удаленного рабочего стола**.

d. Двойным кликом мыши нажмите на [**Пользователи удаленного рабочего стола**].

e. Нажмите [**Добавить**].

f. В поле **Введите имена выбираемых объектов (примеры):** введите **Пользователи домена**.

g. Нажмите **ОК > ОК**.

4. Установите [Latest Microsoft Visual C++ Redistributable Version](#).

5. Установите агент, используя [скрипт](#), полученный при создании сервера. Установка должна выполняться с правами администратора.

OpenSUSE

В этой инструкции приведен пример установки пакета для X2Go, скачанного [по этой ссылке](#).



- В репозиториях OpenSUSE нет официального пакета для X2Go. Есть только экспериментальная версия, доступная [по ссылке](#).
- Проверьте, что все терминальные серверы введены в домен. Подробнее в статье [Ввод OpenSUSE в домен](#). Далее проверьте конфигурацию файла `sssd.conf`, находящийся по пути `sudo vim /etc/sss/sss.conf` и установите значение `False` в следующей строке:

```
use_fully_qualified_names = False
```

- Проверьте, что на всех терминальных серверах доступны порты. Подробнее в статье [Требования к развертыванию](#).

1. Добавьте репозиторий X2Go с помощью команды:

```
sudo zypper addrepo -f http://packages.x2go.org/opensuse/15.4/main  
x2go_repos
```

BASH |

2. Обновите репозиторий с помощью команды:

```
sudo zypper refresh
```

BASH |

3. Установите компоненты X2Go сервера с помощью команды:

```
sudo zypper install x2goserver
```

BASH |

4. Добавьте X2Go в автозапуск с помощью команды:

```
sudo systemctl enable x2goserver.service --now
```

BASH |

5. Проверьте статус службы x2goserver с помощью команды:

```
sudo systemctl status x2goserver.service
```

BASH |

Статус должен быть «Active»:

```
suse@suse-term-1:~> systemctl status x2goserver.service
● x2goserver.service - X2Go Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/x2goserver.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2024-02-02 06:48:33 EST; 49s ago
     Docs: man:x2goserver.conf(5)
    Main PID: 3298 (x2gocleansessio)
      Tasks: 1 (limit: 2323)
    CGroup: /system.slice/x2goserver.service
            └─ 3298 /usr/bin/perl /usr/sbin/x2gocleansessions
```

6. Чтобы избежать ошибки при монтировании сетевых дисков, установите пакет `cifs-utils` с помощью команды:

```
sudo zypper install cifs-utils
```

BASH |

7. Для корректного перенаправления смарт-карт на сервер установите утилиту `socat` с помощью команды:

```
sudo zypper install socat
```


8. Установите агент, используя скрипт, полученный при создании сервера, добавив в конце параметр `/etc/systemd/system/`.

Пример скрипта:

```
rm -f ./agent-installer && wget --no-check-certificate https://<FQDN  
брокера/балансировщика>/dist/agent-installer -O agent-installer && sudo  
chmod +x agent-installer && sudo ./agent-installer install https://<FQDN  
брокера/балансировщика> <секрет> /etc/systemd/system/
```

BASH | 

Последний параметр является опциональным и указывается в тех случаях, когда каталог `systemd` отсутствует в директории `/lib` (то есть не существует пути `/lib/systemd/system/`, необходимого для установки агента) и находится по другому пути. В случае OpenSUSE для доступа к каталогу `systemd` необходимо указывать путь `/etc/systemd/system/` в конце скрипта, иначе агент не будет установлен.

Пример:

[illegible]

Руководство по установке

В этом руководстве подробно описано, как системным администраторам установить систему терминального доступа «Термит» (СТД «Термит»). Это поможет избежать ошибок, ускорить процесс развертывания и обеспечить корректную работу системы после установки.

Руководство содержит информацию о необходимых компонентах, требованиях к системе, процессе установки, настройке параметров и других важных аспектах работы с системой.

Ссылки на разделы:

- [Подготовка окружения](#)
- [Настройка межсетевого экрана](#)
- [Базовая конфигурация базы данных](#)
- [Установка балансировщика нагрузки](#)
- [Установка брокера](#)
- [Установка второго и следующего брокера](#)
- [Установка дополнительного ПО на терминальный сервер](#)
- [Аутентификация пользователя на терминальном сервере по сертификату](#)
- [Установка шлюза удаленного доступа](#)
- [Установка десктоп-клиента](#)
- [Установка сертификата на десктоп-клиент](#)
- [Выпуск самоподписанного сертификата](#)
- [Обновление пакетов десктоп-клиента на РЕД ОС при установке в закрытом контуре](#)
- [Деинсталляция компонентов](#)



Деинсталляция компонентов

Деинсталляция компонентов СТД «Термит» включает в себя удаление:

- брокера;
- агента;
- клиента.



При необходимости удалите XQuartz и X2Go клиенты на MacOS.

Удаление брокера

Чтобы удалить брокер терминального сервера:

1. Перейдите в каталог, куда был распакован дистрибутив.
2. Запустите скрипт с параметром `uninstall` с помощью команды:

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

BASH |



При деинсталляции брокера база данных удаляется вручную. Повторное использование базы данных для новой инсталляции невозможно.

Удаление агента

Чтобы удалить агент:

1. На портале администрирования, в левом меню выберите раздел **Серверы**.
2. Наведите курсор на нужный сервер и нажмите на FQDN адрес сервера.
3. В правом верхнем углу нажмите [**Дополнительно**].
4. Выберите **Удалить агент**.
5. Скопируйте актуальную команду На портале администрирования или предложенную ниже:
 - Для Linux:

```
sudo ./agent-installer uninstall
```

BASH |

- Для Windows:

```
.\agent-installer.exe uninstall
```

BASH | 

6. Для Linux перейдите в каталог, где был запущен скрипт установки агента.

Для Windows (операция удаления может быть выполнена только с правами администратора) перейдите по пути `C:\Program Files\TermitAgent\`.

7. Выполните скопированную команду в терминале.

Агент удален на терминальном сервере.

Удаление десктоп-клиента

РЕД ОС

Чтобы удалить десктоп-клиент, введите команду:

```
sudo dnf remove termit-desktop
```

BASH | 

Astra Linux

Чтобы удалить десктоп-клиент, введите команду:

```
sudo apt remove termit-desktop
```

BASH | 

ALT Linux

Чтобы удалить десктоп-клиент, введите команду:

```
sudo apt-get remove termit-desktop
```

BASH | 

MacOS

Чтобы удалить десктоп-клиент:

1. Откройте **Finder**.
2. В боковом меню **Finder** нажмите на **Программы**.
3. Удалите десктоп-клиент.

Windows

Чтобы удалить десктоп-клиент:

1. Введите **Панель управления** в поле поиска на панели задач, а затем в списке результатов выберите **Панель управления**.
2. Перейдите в **Программы > Программы и компоненты**.
3. Удалите десктоп-клиент.

Также можно удалить десктоп-клиент в «тихом» режиме. Информация о ходе выполнения отображаться не будет. Для удаления в таком режиме добавьте параметр `/S` :

```
"C:\Program Files\termit-desktop\Uninstall Термит.exe" /S
```





Удаление разделов при повторной установке

1. Вопрос

Как произвести удаление разделов при повторной установке zVirt Node?

2. Ответ

2.1. Вариант 1

Развернуть категории и удалить все разделы через графический интерфейс.

2.2. Вариант 2

Перейти в другую консоль **ALT** + **F3** и выполнить команду:

```
wipefs -fa /путь-до-устройства
```



Перейти обратно в графическую консоль **ALT** + **F6** и продолжить установку.

Ошибка "The host CPU does not match the Cluster CPU Type and is running in a degraded mode" при добавлении хоста zVirt во вложенной виртуализации VMWare

1. Вопрос

При добавлении хоста zVirt (расположенного во вложенной виртуализации VMWare ESXi) в менеджере виртуализации zVirt возникает ошибка:

```
InstallFailed.  
The host CPU does not match the Cluster CPU Type and is running in a degraded mode. It is missing the following CPU flags: vmx, ssbd, md_clear, model_Westmere, aes, spec_ctrl. Please update the host CPU microcode or change the Cluster CPU Type.
```

2. Решение

Вопрос флагов внутри VM внутри VMWare - это проблема правильной настройки проброса флагов в vmware. Для исключения подобных ошибок необходимо подготовить VM (внутри VMWare).

1. Проверить наличие флагов **nx**, **vmx** командой

```
grep flags /proc/cpuinfo|head -n1|grep -Eo '(vmx|svm|nx)'
```

2. На используемых коммутаторах хостов ESXi разрешить следующие режимы работы:

- **Promiscuous mode**
- **MAC address changes**
- **Forged transmits**

3. Предоставит аппаратную виртуализацию для гостевой ОС. Для этого в свойствах VM, раздел CPU выбрать пункт: **Expose hardware assisted virtualization to the guest OS**.

▼ CPU	4 ▼	ⓘ
Cores per Socket	1 ▼ Sockets: 4	
CPU Hot Plug	<input type="checkbox"/> Enable CPU Hot Add	
Reservation	0 ▼ MHz ▼	
Limit	Unlimited ▼ MHz ▼	
Shares	Normal ▼ 4000	
CPUID Mask	Expose the NX/XD flag to guest ▼ Advanced...	
Hardware virtualization	<input checked="" type="checkbox"/> Expose hardware assisted virtualization to the guest OS	
Performance Counters	<input type="checkbox"/> Enable virtualized CPU performance counters	
I/O MMU	<input type="checkbox"/> Enabled	
> Memory	16 ▼ GB ▼	
> Hard disk 1	200 GB ▼	
> SCSI controller 0	VMware Paravirtual	