TERMIDESK

РУКОВОДСТВО АДМИНИСТРАТОРА

СЛЕТ.10001-01 90 05

Версия 4.3. Выпуск от ноября 2023

Настройка компонента «Шлюз»

ОГЛАВЛЕНИЕ

1 . ОБЩИЕ СВЕДЕНИЯ

1.1 . О документе

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

В этом руководстве приведено назначение, установка и настройка компонента «Шлюз». Для того, чтобы получить информацию о месте компонента в программном комплексе, необходимо обратиться ко второй части руководства администратора - СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

1.2 . Назначение компонента «Шлюз»

Компонент «Шлюз» (далее - Шлюз) входит в состав Termidesk.

Шлюз отвечает за туннелирование протоколов доставки, использующих транспортный протокол TCP, обеспечивая отделение инфраструктуры виртуальных рабочих мест (BPM), находящихся во внутренней локальной сети, от внешних локальных сетей или глобальных сетей.

Шлюз является отделяемым компонентом Termidesk и может устанавливаться как совместно с компонентами «Универсальный диспетчер», «Менеджер рабочих мест», так и отдельно при необходимости обеспечить распределенную конфигурацию.

Место Шлюза в архитектуре Termidesk представлено в документе СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

> ⚠ В экспериментальном режиме добавлена возможность использования нового Шлюза `termidesk-gateway`. Информация об установке приведена в подразделе **Установка Шлюза**. Информация о настройке приведена в подразделе **Параметры конфигурирования компонента**.

1.3 . Требования к программному и аппаратному обеспечению

Требования к аппаратному и программному обеспечению соответствуют требованиям к Termidesk, приведенным в документе СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса».

1.4 . Типографские соглашения

В настоящем документе приняты следующие типографские соглашения:

- моноширинный шрифт – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), путей перемещения, строк комментариев,

различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;

- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

2 . УСТАНОВКА И УДАЛЕНИЕ КОМПОНЕНТА

2.1 . Получение пакетов установки в ОС Astra Linux Special Edition

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

Получить iso-образ можно двумя способами:

- заполнив запрос через сайт Termidesk: `https://termidesk.ru/support/#request-support`;
- через личный кабинет: `https://lk-new.astralinux.ru/`.

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

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

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

где:

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

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

```
:~$ sudo cp -Rp /mnt/repos /var
```

где:

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

- отключить подключенный ранее образ диска от узла:

```
:~$ sudo umount /mnt
```

- установить пакет `lsb-release`:

```
:~$ sudo apt install -y lsb-release
```

где:

`-y` - ключ для пропуска подтверждения установки;

- добавить локальный репозиторий Termidesk (`/var/repos/astra`) в файл `/etc/apt/sources.list.d/termidesk_local.list` через командный интерпретатор `sh`:

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

где:

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

`echo` - команда вывода текста, совместно с символом «>» используется для перенаправления строки `deb file:/var/repos/astra $(lsb_release -cs) non-free` в файл `/etc/apt/sources.list.d/termidesk_local.list`;

`deb file:/var/repos/astra $(lsb_release -cs) non-free` - добавляемый репозиторий, вложенная команда `$(lsb_release -cs)` подставляет версию - `1.7_x86-64`;

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

```
:~$ cat /var/repos/astra/GPG-KEY-PUBLIC | sudo apt-key add -
```

- убедиться, что ключ с `uid` «`release@uveon.ru`» был успешно добавлен:

```
:~$ apt-key list
```

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

```
:~$ cat /var/repos/astra/GPG-KEY-PUBLIC
```

Если ключ все же существует, необходимо проверить правильность выполнения шагов по добавлению репозитория Termidesk в файл `/etc/apt/sources.list.d/termidesk_local.list`.
При успешном выполнении всех шагов команда выведет содержимое ключа в формате Base64.

- обновить данные пакетного менеджера:

```
:~$ sudo apt update
```

Данную команду (`sudo apt update`) необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.

2.2 . Установка Шлюза

Подготовка к установке и непосредственно установка Шлюза в разных конфигурациях Termidesk приведена в документе СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса».

Для экспериментального использования добавлен новый Шлюз `termidesk-gateway`, который в следующих версиях заменит существующий `termidesk-wsproxy`.

> ⚠ Использование нового Шлюза является экспериментальным, его установка рекомендуется только в ознакомительных целях!

Для установки нового Шлюза необходимо:

- остановить службу используемого Шлюза:

```
:~$ sudo systemctl stop termidesk-wsproxy
```

- отключить автоматический запуск службы:

```
:~$ sudo systemctl disable termidesk-wsproxy
```

- выполнить установку `termidesk-gateway` из подключенного репозитория Termidesk:

```
:~$ sudo apt install termidesk-gateway
```

Зависимости пакета `termidesk-gateway`:

- `libc6 (>= 2.14)`;
- `libgcc1 (>= 1:3.3.1)`;
- `libssl1.1 (>= 1.1.0)`;
- `libstdc++6 (>= 5.2)`;
- `libuv1 (>= 1.4.2)`;
- `zlib1g (>= 1:1.1.4)`.

Проверка состояния службы `termidesk-gateway` выполняется командой:

```
:~$ sudo systemctl status termidesk-gateway
```

Строка «`Active`» отображает состояние сервиса, где статус «`active (running)`» свидетельствует об успешном запуске `termidesk-gateway`.

Для просмотра установленной версии Шлюза `termidesk-gateway` нужно выполнить:

```
:~$ termidesk-gateway -v
```

2.3 . Удаление Шлюза

Действия по удалению Шлюза идентичны действиям по удалению Termidesk и приведены в документе СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса».

Для удаления нового Шлюза `termidesk-gateway` необходимо выполнить:

- удалить без подтверждения `termidesk-gateway`:

```
:~$ sudo aptitude purge -y termidesk-gateway
```

- очистить оставшиеся зависимости и конфигурации:

```
:~$ sudo aptitude purge ~c -y
```

Если после удаления нового Шлюза необходимо включить ранее использовавшуюся версию (`termidesk-wsproxy`), нужно:

- добавить службу `termidesk-wsproxy` в автозагрузку:

```
:~$ sudo systemctl enable termidesk-wsproxy
```

- выполнить запуск службы `termidesk-wsproxy`:

```
:~$ sudo systemctl start termidesk-wsproxy
```

2.4 . Обновление Шлюза

Действия по обновлению Шлюза идентичны действиям по обновлению Termidesk и приведены в документе СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса».

Обновление экспериментального прототипа нового Шлюза `termidesk-gateway` выполняется процедурой установки новой версии. При обновлении распределенной конфигурации необходимо учесть, что если ранее на узлах-шлюзах был установлен `termidesk-gateway`, необходимо сначала обновить эти узлы, и только потом - узлы-диспетчеры и узлы-менеджеры BPM.

3 . НАСТРОЙКА КОМПОНЕНТА

3.1 . Принципы настройки и функционирования компонента

Для работы Шлюза необходимо добавить в автозагрузку и запустить службу `termidesk-wsproxy` командами:

```
:~$ sudo systemctl enable termidesk-wsproxy
:~$ sudo systemctl start termidesk-wsproxy
```

При работе нового Шлюза необходимо использовать службу `termidesk-gateway`, предварительно остановив и отключив службу `termidesk-wsproxy`:

```
:~$ sudo systemctl stop termidesk-wsproxy
:~$ sudo systemctl disable termidesk-wsproxy
```

Здесь и далее `termidesk-wsproxy` - ранее установленный с Termidesk Шлюз, `termidesk-gateway` - экспериментальный новый Шлюз.

Шлюз может быть вынесен в демилитаризованную зону сетевой инфраструктуры предприятия.
Для работы подключения пользователей к BPM через Шлюз необходимо обеспечить доступность следующих сетевых портов:

- 80 (HTTP);
- 443 (HTTPS).

По умолчанию Шлюз прослушивает порт `TCP:5099` на интерфейсе `localhost (127.0.0.1)`. Для изменения порта прослушивания службы необходимо внести изменения в файлы запуска службы `termidesk-wsproxy` и конфигурации веб-сервера `apache`.
В случае экспериментального использования нового Шлюза эти параметры могут быть изменены через файл конфигурации (см. подраздел **Параметры конфигурирования компонента**).

Механизм взаимодействия веб-сервера `apache` и Шлюза выглядит следующим образом:

- запросы на подключения принимает веб-сервер `apache` по портам 80 или 443;
- веб-сервер `apache` перенаправляет запросы Шлюзу на указанный в параметре `WSPROXY_BIND_ADDRESS` IP-адрес на порт `WSPROXY_PORT` (см. подраздел **Параметры конфигурирования компонента**);
- далее Шлюз направляет запросы либо на поставщик ресурсов, либо в виртуальную машину.

3.2 . Параметры конфигурирования компонента

Параметры Шлюза задаются переменными, описанными в файле `/etc/opt/termidesk-vdi/termidesk.conf`, а также аргументами командной строки.

Перечень доступных переменных и аргументов приведен в таблице (см. Таблица 1).

⚠ Информация в таблице относится к ранее установленному с Termidesk Шлюзу `termidesk-wsproxy`.

Таблица 1 – Доступные переменные Шлюза

Наименование переменной	Значение по умолчанию	Описание	Аргумент командной строки
`WSPROXY_PORT`	`5099`	Порт прослушивания службы	Не задан
`WSPROXY_BIND_ADDRESS`	`127.0.0.1`	Адрес прослушивания службы. При распределенной установке необходимо использовать значение `0.0.0.0`, чтобы порт `5099` прослушивался не только `localhost`, если планируется принимать запросы на подключения с внешних систем (например, с балансировщиков нагрузки)	Не задан
`WSPROXY_HEALTH_CHECK_PORT`	`8101`	Порт веб-сервера для обслуживания API-запросов по состоянию Шлюза (`healthcheck`). По умолчанию переменная не используется (закомментирована)	Не задан
`WSPROXY_HEALTH_CHECK_CERT`	`/etc/opt/termidesk-vdi/wsproxy-healthcheck.pem`	Путь к сертификату (открытому ключу), который используется для защиты подключения API-запросов по состоянию Шлюза (`healthcheck`). По умолчанию переменная не используется (закомментирована) Примечание: сертификат - артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу	Не задан

Наименование переменной	Значение по умолчанию	Описание	Аргумент командной строки
WSPROXY_HEALTH_CHECK_KEY	/etc/opt/termidesk-vdi/wsproxy-healthcheck.key	Путь к закрытому ключу, который используется для защиты подключения API-запросов по состоянию Шлюза (healthcheck). По умолчанию переменная не используется (закомментирована) Примечание: ключ - последовательность псевдослучайных чисел, сгенерированная особым образом	Не задан

Наименование переменной	Значение по умолчанию	Описание	Аргумент командной строки
LOG_LEVEL	INFO	Аргумент командной строки применяется для изменения уровня логирования Шлюза. Изначально уровень логирования применяется из значения переменной LOG_LEVEL конфигурационного файла /etc/opt/termidesk-vdi/termidesk.conf. Для того чтобы применить уровень логирования из аргумента командной строки, необходимо отредактировать unit-файл службы Шлюза: ▪ открыть для редактирования файл /lib/systemd/system/termidesk-wsproxy.service ; ▪ найти строку, начинающуюся с ExecStart и добавить ключ --loglevel с нужным уровнем. Пример строки: ExecStart=/opt/termidesk/share/termidesk-vdi/venv/bin/python wsproxy.py --verification-key=/etc/opt/termidesk-vdi/wsproxy/id_rsa.pub --host=${WSPROXY_BIND_ADDRESS} --port=${WSPROXY_PORT} --loglevel=INFO Затем выполнить перезапуск конфигурации и службы: ▪ выполнить команду sudo systemctl daemon-reload; ▪ выполнить команду sudo systemctl restart termidesk-wsproxy.	--loglevel

⚠ Далее информация относится к новому (экспериментальному) Шлюзу termidesk-gateway.

Параметры конфигурирования нового Шлюза задаются из конфигурационного файла `/etc/termidesk/termidesk-gateway.conf`.

Для задания параметров конфигурирования нового Шлюза из файла необходимо:

- создать пустой файл `/etc/termidesk/ termidesk-gateway.conf`:

```
:~$ sudo touch /etc/termidesk/termidesk-gateway.conf
```

- отредактировать файл `termidesk-gateway.conf`, указав необходимые значения для параметров:

```
# Адреса, на которых принимать входящие подключения
wsServerIP=0.0.0.0
# Прослушиваемый порт для входящих подключений
wsServerPort=5099
# Адрес брокера, по которому будет осуществляться проверка пользовательских подключений в случае комплексной установки
# Если программный комплекс Termidesk установлен в распределенном варианте, вместо 127.0.0.1 следует указать адрес балансировщика
urlCheckToken=https://127.0.0.1/api/wsproxy/v1/verify
# Режим журналирования.
# gatewayLogMode=-l - включить отладку уровня INFO.
# gatewayLogMode=-d - включить отладку уровня DEBUG.
# Пустое значение параметра gatewayLogMode= - выключить отладку.
# gatewayLogMode=-l
```

- выполнить перезагрузку службы:

```
:~$ sudo systemctl restart termidesk-gateway
```

Доступные параметры, а также аргументы командной строки для нового Шлюза приведены в таблице (см. Таблица 2).

Для получения информации по доступным параметрам из интерфейса командной строки, необходимо выполнить команду:

```
:~$ termidesk-gateway --help
```

Таблица 2 – Доступные переменные нового Шлюза

Параметр конфигурационного файла	Значение по умолчанию после установки Шлюза	Описание	Аргумент командной строки
`wsServerPort`	`5099`	Порт прослушивания службы для входящих подключений	`--wsServerPort`

Параметр конфигурационного файла	Значение по умолчанию после установки Шлюза	Описание	Аргумент командной строки
`wsServerIP`	`127.0.0.1`	Адрес прослушивания входящих подключений при комплексной установке. При распределенной установке необходимо использовать значение `0.0.0.0`, чтобы порт `5099` прослушивался не только `localhost`, если планируется принимать запросы на подключения с внешних систем (например, с балансировщиков нагрузки)	`--wsServerIP`
Не задан	`10000`	Порт прослушивания службы для входящих подключений по протоколу SSL	`--wssServerPort`
Не задан	`127.0.0.1`	Адрес прослушивания входящих подключений по протоколу SSL при комплексной установке. При распределенной установке необходимо использовать значение `0.0.0.0`, чтобы порт прослушивался не только `localhost`, если планируется принимать запросы на подключения с внешних систем (например, с балансировщиков нагрузки)	`--wssServerIP`
Не задан	Нет	Путь к файлу ключа для соединения SSL	`--sslKey`
Не задан	Нет	Путь к файлу сертификата для соединения SSL	`--sslCert`
Не задан	Нет	Парольная фраза для соединения SSL	`--sslPassPhrase`
Не задан	Нет	Путь к файлу с ключами Диффи-Хеллмана для соединения SSL	`--sslDhParams`

Параметр конфигурационного файла	Значение по умолчанию после установки Шлюза	Описание	Аргумент командной строки
Не задан	Нет	Путь к корневому сертификату, на котором выпущен сертификат, указанный в параметре `sslCert`. Используется для проверки подлинности указанного в параметре `sslCert` сертификата	`--sslCa`
Не задан	Нет	Используемый алгоритм для преобразований для соединения SSL	`--sslCiphers`
`urlCheckToken`	`https://127.0.0.1/api/wsproxy/v1/verify`	IP-адрес или FQDN диспетчера Termidesk для обслуживания API-запросов по состоянию Шлюза в случае комплексной установки. Если программный комплекс Termidesk установлен в распределенном варианте, следует изменить значение `127.0.0.1` на IP-адрес или FQDN балансировщика	Не задан
Не задан	`30`	Интервал установки соединения (в секундах)	`--wsIdleTimeout`

Параметр конфигурационного файла	Значение по умолчанию после установки Шлюза	Описание	Аргумент командной строки

`gatewayLogMode`	Нет	Активация и переключение режима журналирования. Значение задается через файл `termidesk-gateway.conf`.
		При значении «`-d`» активируется подробный режим уровня DEBUG, при значении «`-l`» активируется менее подробный режим уровня INFO. Пустое значение параметра приводит к отключению режима журналирования.
		Активировать режим можно также через аргумент командной строки, для этого выполнить:
		`termidesk-gateway <значение>`
		Пример:
		`termidesk-gateway -l`
		Информация будет выводиться в интерфейс командной строки. Для прекращения вывода и отключения режима необходимо нажать сочетание клавиш **<Ctrl>+<C>**
			`-d`
			`-l`

3.3 . Журналирование

Журнал работы Шлюза расположен в файле `/var/log/termidesk/wsproxy.log`.

4 . ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Пояснение
BPM	Виртуальное рабочее место
API	Application Programming Interface (интерфейс прикладного программирования)
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста)
HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
IP	Internet Protocol (межсетевой протокол)
TCP	Transmission Control Protocol (протокол управления передачей данных)
Termidesk	Программный комплекс «Диспетчер подключений виртуальных рабочих мест Termidesk»

Адрес: 119571, г. Москва, Ленинский проспект, д. 119А, помещ. 9Н
Сайт: www.termidesk.ru
Телефон: +7 (495) 975-1-975

Общий e-mail: info@uveon.ru
Отдел продаж: sales@uveon.ru
Техническая поддержка: support@uveon.ru