TERMIDESK

Вариант лицензирования «TermideskTerminal»

РУКОВОДСТВО АДМИНИСТРАТОРА

СЛЕТ.10001-02 90 05

Версия 4.3.2. Выпуск от января 2024

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» (далее - Шлюз). Для того чтобы получить информацию о месте компонента в программном комплексе, необходимо обратиться ко второй части руководства администратора - СЛЕТ.10001-02 90 02 «Руководство администратора. Настройка программного комплекса».

1.2 . Назначение компонента «Шлюз»

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.10001-02 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.10001-02 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 . Установка Шлюза

Подготовка к установке и непосредственно установка Шлюза в разных конфигурациях Termidesk приведена в документе СЛЕТ.10001-02 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
```

2.2 . Удаление Шлюза

Действия по удалению Шлюза идентичны действиям по удалению Termidesk и приведены в документе СЛЕТ.10001-02 90 01 «Руководство администратора. Установка программного комплекса».

2.3 . Обновление Шлюза

Действия по обновлению Шлюза идентичны действиям по обновлению Termidesk и приведены в документе СЛЕТ.10001-02 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
`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 при условии определения переменных в файле /lib/systemd/system/termidesk-gateway.service.

⚠ При необходимости переопределить параметры запуска Шлюза через интерфейс командной строки, необходимо сначала остановить службу:

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

Помимо аргументов командной строки параметры запуска службы могут быть переопределены в unit-файле службы termidesk- gateway /lib/systemd/system/termidesk-gateway.service.

Пример файла /lib/systemd/system/termidesk-gateway.service:

```
1 [Unit]
2 Description=Termidesk Gateway
```

```
After=network.target
[Service]
Environment=wsServerIP=0.0.0.0
Environment=wsServerPort=5099
Environment=urlCheckToken=http: /127.0.0.1:8000/api/wsproxy/v1/verify
Environment=gatewayLogMode="-l"
Environment=wsIdleTimeout=30
Environment=mgtServerIP=0.0.0.0
Environment=mgtServerPort=8444
Environment=wssServerIP=0.0.0.0
Environment=wssServerPort=8443
Environment=sslKey=/etc/termidesk/ssl-cert-snakeoil.key
Environment=sslCert=/etc/termidesk/ssl-cert-snakeoil.pem
Environment=healthCheckAccessKey=a0e08d1b0e95dfea4f431d5849b934e09ac5067b
EnvironmentFile=-/etc/termidesk/termidesk-gateway.conf
Restart=on-failure
RestartSec=5
User=termidesk-gateway
Group=termidesk-gateway
ExecStart=/usr/bin/termidesk-gateway ${gatewayLogMode} \
-wsServerIP=${wsServerIP} -wsServerPort=${wsServerPort} \
-urlCheckToken=${urlCheckToken} -wsIdleTimeout=${wsIdleTimeout} \
-mgtServerIP=${mgtServerIP} -mgtServerPort=${mgtServerPort} \
-healthCheckAccessKey=${healthCheckAccessKey} \
-wssServerIP=${wssServerIP} \
-wssServerPort=${wssServerPort} \
-sslKey=/etc/termidesk/ssl-cert-snakeoil.key \
-sslCert=/etc/termidesk/ssl-cert-snakeoil.pem
[Install]
WantedBy=multi-user.target
```

Для задания параметров конфигурирования нового Шлюза из файла необходимо:

- создать каталог `/etc/termidesk/`, если его нет:

```
:~$ sudo mkdir /etc/termidesk/
```

- 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
# Интервал установки соединения (в секундах)
wsIdleTimeout=30
# Режим журналирования.
gatewayLogMode=-l - включить отладку уровня INFO.
# gatewayLogMode="-d" - включить отладку уровня DEBUG.
# Пустое значение параметра gatewayLogMode= - выключить отладку.
# Адрес для доступа к API
# Если нужно, чтобы доступ был у внешних систем, то вместо 127.0.0.1 следует указать 0.0.0.0
mgtServerIP=127.0.0.1
# Порт для доступа к API
mgtServerPort=8102
# Ключ доступа для аутентификации запросов к API. Указание значения ключа обязательно
# При задании ключа его размер должен составлять от 0 до 64 символа, должны использоваться символы в шестнадцатеричной системе (0-9, a-f)
healthCheckAccessKey=a0e08d1b0e95dfea4f431d5849b934e09ac5067b
```

- выполнить перезагрузку службы и модуля:

```
:~$ systemctl daemon-reload & systemctl restart termidesk-gateway.service
```

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

Наименование переменной	Значение по умолчанию	Описание	Аргумент командной строки
wsServerPort	5099	Порт прослушивания службы для входящих подключений	--wsServerPort
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 задано	10000	Порт прослушивания службы для входящих подключений по протоколу SSL	--wssServerPort

Наименование переменной	Значение по умолчанию	Описание	Аргумент командной строки
Не задано	`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 задано	Нет	Путь к файлу ключа для соединения SSL.
		Пример команды, в которой переопределены параметры запуска службы Шлюза, указаны пути к файлам ключа и сертификата и включен отладочный режим:
		`:~$ termidesk-gateway --wssServerIP=0.0.0.0 --wssServerPort=8443 --sslKey=/etc/ssl/private/ssl-cert-snakeoil.key --sslCert=/etc/ssl/certs/ssl-cert-snakeoil.pem --debug`
		При использовании сертификатов и ключей на файлы `.key` и `.pem` необходимо выдать права на чтение командой `chmod 644`:
		`:~$ sudo chmod 644 /etc/termidesk/ssl-cert-snakeoil.key`
		`:~$ sudo chmod 644 /etc/termidesk/ssl-cert-snakeoil.pem`
		И перезапустить `termidesk-gateway`:
		`:~$ sudo systemctl restart termidesk-gateway.service`
			`--sslKey`

Не задано	Нет	Путь к файлу сертификата для соединения SSL. Пример команды для переопределения параметра приведен выше	`--sslCert`
Не задано	Нет	Парольная фраза для соединения SSL	`--sslPassPhrase`
Не задано	Нет	Путь к файлу с ключами Диффи-Хеллмана для соединения SSL	`--sslDhParams`

Наименование переменной	Значение по умолчанию	Описание	Аргумент командной строки
Не задано	Нет	Путь к корневому сертификату, на котором выпущен сертификат, указанный в параметре `sslCert`. Используется для проверки подлинности указанного в параметре `sslCert` сертификата	`--sslCa`
Не задано	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 внешний IP-адрес или FQDN балансировщика	`--urlCheckToken`
Не задано	`30`	Интервал установки соединения (в секундах)	`--wsIdleTimeout`

`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`

Наименование переменной	Значение по умолчанию	Описание	Аргумент командной строки

mgtServerIP	127.0.0.1	Задание IP-адреса или FQDN доступа к API Шлюза. Код 200 в ответе на API-запрос свидетельствует о работоспособности Шлюза.
		При распределенной установке следует задать значение 0.0.0.0 для активации приема запросов с внешних систем.
		Запрос с параметрами по умолчанию успешно выполнится только с узла, на котором установлен Шлюз:
		`:~$ wget http://localhost:8102/api/health`
		Для того чтобы получить состояние Шлюза с другого узла, нужно задать параметру --mgtServerIP значение 0.0.0.0. Пример команды для запуска Шлюза с переопределенными параметрами:
		`:~$ termidesk-gateway --wsServerIP=0.0.0.0 --wsServerPort=5099 --urlCheckToken=http://<FQDN_Узла>/api/wsproxy/v1/verify --wsIdleTimeout=30 --mgtServerIP=0.0.0.0 --mgtServerPort=8102 --healthCheckAccessKey=6622b09199c62bcf9418ad846dd0e4bbdfc6ee4b`
		Значение также может быть переопределено через файл termidesk-gateway.conf
			--mgtServerIP

Наименование переменной	Значение по умолчанию	Описание	Аргумент командной строки
mgtServerPort	8102	Задание порта доступа к API Шлюза. По умолчанию используется порт 8102. Пример команды для переопределения параметров запуска Шлюза для доступа к API из внешних систем: :~$ termidesk-gateway --wsServerIP=0.0.0.0 --wsServerPort=5099 --urlCheckToken=http://<FQDN_Узла>/api/wsproxy/v1/verify --wsIdleTimeout=30 --mgtServerIP=0.0.0.0 --mgtServerPort=8102 --healthCheckAccessKey=6622b09199c62bcf9418ad846dd0e4bbdfc6ee4b Значение также может быть переопределено через файл termidesk-gateway.conf	--mgtServerPort
healthCheckAccessKey	a0e08d1b0e95dfea...	Задание ключа доступа для аутентификации запросов к API Шлюза. Пример команды для переопределения параметра приведен выше. Значение также может быть переопределено через файл termidesk-gateway.conf. При задании значения ключа следует руководствоваться правилом, что: ▪ размер ключа должен составлять от 0 до 64 символа; ▪ должны использоваться символы в шестнадцатеричной системе (0-9, a-f)	--healthCheckAccessKey
Не задан	Нет	Вывод версии Шлюза	--version

Пример команды проверки состояния компонента через утилиту `curl` для нового Шлюза `termidesk-gateway`:

```
:~$ curl -v -s -X 'GET' "${HOSTNAME}:8102/api/health" -H 'accept: application/json' -H "Authorization: Token ${HEALTH_CHECK_ACCESS_KEY}" --fail -w "\n%{http_code}\n"
```

3.3 . Журналирование

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

Для просмотра журнала нового Шлюза можно выполнить:

```
:~$ sudo journalctl -f -u termidesk-gateway.service
```

или:

```
:~$ sudo less /var/log/syslog
```

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: https://termidesk.ru
Телефон: +7 (495) 975-1-975

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