TERMIDESK

Вариант лицензирования «TermideskTerminal»

РУКОВОДСТВО АДМИНИСТРАТОРА

СЛЕТ.10001-02 90 05

Версия 5.0. Выпуск от мая 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». 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»

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

1.3 . Требования к программному и аппаратному обеспечению

Для установки Шлюза минимальные аппаратные требования узла должны соответствовать следующим:

- процессор архитектуры Intel x86 с разрядностью 64 бит;
- оперативная память, не менее 4 ГБ;
- свободное дисковое пространство, не менее 1 ГБ;
- сетевое соединение, не менее 100 Мбит/с.

В среде функционирования Шлюза должна быть предварительно установлена операционная система (ОС) Astra Linux Special Edition версии 1.7 (и выше).

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

Для установки Шлюза необходимо:

- остановить и отключить службу Шлюза `termidesk-wsproxy`, если он ранее использовался:

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

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

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

Для обслуживания API-запросов по состоянию Шлюза необходимо после установки Шлюза задать параметр `urlCheckToken`.
Для регистрации Шлюза в системе управления и мониторинга Termidesk и отслеживания его актуального статуса из портала администратора Termidesk, необходимо после установки Шлюза задать параметры `coordinatorUrl`, `coordinatorUser`, `coordinatorPass` (см. подраздел **Параметры конфигурирования компонента**).

Зависимости пакета `termidesk-gateway`:

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

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
```

Начиная с Termidesk версии 5.0 изменился API-запрос валидации токена Шлюза `termidesk-gateway` для подключения к компоненту «Универсальный диспетчер».
При обновлении компонента «Универсальный диспетчер» и/или Шлюза `termidesk-gateway` на версию из состава программного комплекса 5.X нужно вручную обновить параметр `urlCheckToken` (см. подраздел **Параметры конфигурирования компонента**) на значение `https://<IP-адрес>/api/wsproxy/v1.1/verify` для корректной работы переключения между протоколами TCP и UDP.

2.2 . Удаление Шлюза

Для удаления Шлюза `termidesk-gateway` нужно:

- удалить без подтверждения `termidesk-gateway`:

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

- очистить оставшиеся зависимости и конфигурации:

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

2.3 . Обновление Шлюза

Обновление Шлюза `termidesk-gateway` выполняется процедурой установки новой версии. При обновлении `termidesk-gateway` файл `/lib/systemd/system/termidesk-gateway.service` будет перезаписан. Конфигурационный файл Шлюза `/etc/termidesk/termidesk-gateway.conf` будет заменен файлом `/etc/termidesk/gateway.yaml`.

> Начиная с Termidesk версии 5.0 изменился API-запрос валидации токена Шлюза `termidesk-gateway` для подключения к компоненту «Универсальный диспетчер».
> При обновлении компонента «Универсальный диспетчер» и/или Шлюза `termidesk-gateway` на версию из состава программного комплекса 5.X нужно вручную обновить параметр `urlCheckToken` (см. подраздел **Параметры конфигурирования компонента**) на значение `https://<IP-адрес>/api/wsproxy/v1.1/verify` для корректной работы переключения между протоколами TCP и UDP.

При обновлении распределенной конфигурации необходимо учесть, что если ранее на узлах со Шлюзом был установлен `termidesk-gateway`, необходимо сначала обновить эти узлы, и только потом - узлы компонента «Универсальный диспетчер» и узлы компонента «Менеджер рабочих мест».

3 . НАСТРОЙКА КОМПОНЕНТА

3.1 . Общие сведения по настройке и функционированию Шлюза

Для проверки состояния службы Шлюза используется команда:

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

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 изменение в конфигурационный файл `termidesk-gateway.yaml` (см. подраздел **Параметры конфигурирования компонента**).

На новой установке Шлюза `termidesk-gateway` механизм взаимодействия веб-сервера со Шлюзом удален.
Однако если ранее на узле был установлен Шлюз `termidesk-wsproxy` и конфигурация веб-сервера была сохранена, то взаимодействие выглядит следующим образом:

- запросы на подключения принимает веб-сервер `apache` по портам 80 или 443;
- веб-сервер `apache` перенаправляет запросы Шлюзу на указанные IP-адрес на порт;
- далее Шлюз направляет запросы либо на поставщик ресурсов, либо в виртуальную машину.

3.2 . Регистрация компонента в системе управления и мониторинга Termidesk

Для централизованного управления объектами инфраструктуры в веб-интерфейсе Termidesk реализована система управления и мониторинга состояния компонентов.
Регистрация компонента в системе происходит через подключение к серверу RabbitMQ, который хранит информацию об узле компонента и передает ее компоненту «Менеджер рабочих мест» (`termidesk-taskman`). Для регистрации Шлюза в системе необходимо задать обязательные параметры `coordinatorUrl`, `coordinatorUser`, `coordinatorPass` (см. подраздел **Параметры конфигурирования компонента**).
Если параметр `coordinatorUrl` задан, то после запуска Шлюз инициирует подключение к серверу RabbitMQ. Все запросы к серверу RabbitMQ ожидают ответа в течение времени, заданного в параметре `coordinatorTimeout`, по истечении которого фиксируется ошибка подключения. При успешном подключении Шлюз передает свой статус с URL проверки состояния (`healthcheck`) в

формате JSON и периодически обновляет его. Таймаут обновления статуса задается в параметре `coordinatorRefreshTime`.

3.3 . Параметры конфигурирования компонента

Параметры конфигурирования Шлюза задаются в конфигурационном файле `/etc/termidesk/gateway.yaml`.

> При обновлении компонента «Универсальный диспетчер» и/или Шлюза `termidesk-gateway` на версию из состава программного комплекса 5.X вместо значения `https://127.0.0.1/api/wsproxy/v1/verify` для параметра `urlCheckToken` нужно использовать значение `https://127.0.0.1/api/wsproxy/v1.1/verify`.

Для задания параметров конфигурирования Шлюза из файла необходимо:

- отредактировать файл `gateway.yaml`, указав необходимые значения для параметров. Пример приведен в файле `/etc/termidesk/gateway.yaml.example`:

```
# Объявляем переменную для SSL (потом ее используем в качестве ссылки)
_val0: &sslprof0                                # Шаблон для SSL
  key: "/etc/key"                               # SSL Key file name (default "")
  cert: "/etc/cert"                             # SSL Cert file name (default "")
  ca: "/etc/ca"                                 # SSL CA file name (default "")
  passphrase: "phrase"                          # SSL PassPhrase (default "")
  dhparams: "/etc/dhparams"                     # SSL DhParams file name (default
"")
  ciphers: "ciphers"                            # SSL Cipher (default "")

# Gateway серверы (это список, по умолчанию он пустой)
gwservers:
- listen: "127.0.0.1:9200"                      # IP + port, для IPv6
"[::1]:80" (default ~)
  ssl: *sslprof0                                # SSL настройки (default {})
  websocket:                                    # Настройка WebSocket
    pingtimeout: 35                             # Время пинга «Клиента» в секундах,
диапазон [0, 100000], если 0, то пинги отключены (default 30)
  checktoken:                                   # Настройка проверки токенов
    url: "http://127.0.0.1:80/api/verify"       # URL для проверки (default "http://
127.0.0.1:8080/api/wsproxy/v1/verify")
  # ...  Другие шлюзы

# MGT сервер
mgtserver:
  listen: "127.0.0.1:8181"                      # IP + port, для IPv6
"[::1]:80" (default ~)
  path: /api/health                             # Path для запроса информации (default
"/api/health")
  token: "abcde12345"                           # Токен валидации (default "")
  ssl: *sslprof0                                # SSL настройки (default {})

# RabbitMQ клиент
```

```
rabbitmq:
  url: "amqp://USER:PASS@localhost/"        # URL, где USER и PASS - это необязательные поля (default ~)
  user: "user"                              # user - пользователь, если задан, то изменяет url.USER (default "")
  pass: "pass"                              # RabbitMQ pass - пароль, если задан, то изменяет url.PASS (default "")
  timeout: 40                               # RabbitMQ timeout(sec), диапазон [1, 60] (default 10)
  refreshtime: 80                           # Период (sec) обновления информация на сервере RabbitMQ, диапазон [10, 100'000] (default 60)
  single: true                              # Если true - то данные передаются до первого подтверждения,
                                            # если false - то данные передаются по циклу (бесконечно) (default false)
  exchange: "exchange"                      # RabbitMQ exchange (default "")
  routingkey: "routingkey"                  # RabbitMQ routing key (default "termidesk_appnode")

loglevel:                                   # Логирование сообщений
  info: true                                # Уровень INFO (default true)
  debug: true                               # Уровень DEBUG (default false)
```

- выполнить перезагрузку службы:

```
:~$ systemctl restart termidesk-gateway.service
```

Для получения информации по доступным аргументам командной строки нужно выполнить команду:

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

Параметры, используемые в файле `/etc/termidesk/gateway.yaml` после установки приведены в таблице (см. Таблица 1).

Задание параметров может производиться и переменными окружения в формате: `${ENV}` или `${ENV:DEFAULT}`, где `DEFAULT` - значение для подстановки, если указанная переменная окружения не найдена.

Например, если нужно задать через переменные окружения адрес `IP_ADDR` и порт прослушивания службы `PORT`, то в конфигурационном файле `/etc/termidesk/gateway.yaml` можно изменить значение следующим образом:

```
listen: ${IP_ADDR}:${PORT:8000}
```

Либо эти значения можно задать напрямую в файле, без использования переменных окружения, тогда запись изменится к виду:

```
listen: "127.0.0.1:8181"
```

Таблица 1 – Доступные переменные Шлюза

Параметр	Описание
Секция `val0: &sslprof0`	

`key: ${sslKey}`	Путь к файлу ключа для соединения SSL. Параметр не имеет значения по умолчанию.
	При использовании сертификатов и ключей на файлы `.key` и `.pem` необходимо выдать права на чтение командой `chmod 644`:
	`:~$ sudo chmod 644 /etc/termidesk/ssl-cert-snakeoil.key`
	`:~$ sudo chmod 644 /etc/termidesk/ssl-cert-snakeoil.pem`

`cert: ${sslCert}`	Путь к файлу сертификата для соединения SSL. Параметр не имеет значения по умолчанию
`ca: ${sslCa}`	Путь к корневому сертификату, на котором выпущен сертификат, указанный в параметре `cert`. Параметр не имеет значения по умолчанию. Используется для проверки подлинности указанного в параметре `cert` сертификата
`passphrase: ${sslPassPhrase}`	Парольная фраза для соединения SSL. Параметр не имеет значения по умолчанию
`dhparams: ${sslDhParams}`	Путь к файлу с ключами Диффи-Хеллмана для соединения SSL. Параметр не имеет значения по умолчанию
`ciphers: ${sslCiphers}`	Используемый алгоритм преобразований для соединения SSL. Параметр не имеет значения по умолчанию
Секция `gwservers:`	
`listen: ${wsServerIP:0.0.0.0}:${wsServerPort:5099}`	Назначение параметров узла Шлюза: ▪ `wsServerIP` - адрес прослушивания входящих подключений. При распределенной установке указывается 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). При комплексной установке Termidesk указывается `127.0.0.1`; ▪ `wsServerPort` - порт прослушивания службы для входящих подключений. Значения по умолчанию: ▪ `wsServerIP:0.0.0.0`; ▪ `wsServerPort:5099` Для протокола SSL нужно использовать параметры `wssServerPort` и `wssServerPort`, но в этом случае будет использоваться порт 10000: `wsServerPort:10000`
`websocket:` `pingtimeout: ${wsIdleTimeout:30}`	Таймаут соединения (в секундах) к компоненту «Клиент» Termidesk. Может принимать значения в интервале с 8 до 960, а также 0 (отключен). Значение по умолчанию: `30`

Параметр	Описание
checktoken: url: ${urlCheckToken:https:// 127.0.0.1/api/wsproxy/v1/verify}	Назначение IP-адреса или FQDN компонента «Универсальный диспетчер» для обслуживания API-запросов по состоянию Шлюза. При обновлении компонента «Универсальный диспетчер» и/или Шлюза `termidesk-gateway` на версию из состава программного комплекса 5.X нужно использовать значение: `urlCheckToken:https://127.0.0.1/api/wsproxy/v1.1/verify`. Если программный комплекс Termidesk установлен в распределенном варианте, следует изменить значение `127.0.0.1` на внешний IP-адрес или FQDN балансировщика нагрузки. Значение по умолчанию: `urlCheckToken:https://127.0.0.1/api/wsproxy/v1/verify`
Секция `mgtserver:`	
`listen: ${mgtServerIP:127.0.0.1}:${mgtServerPort:8102}`	Задание параметров для подключения к API Шлюза: ▪ `mgtServerIP` - IP-адрес 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; ▪ `mgtServerPort` - порт доступа к API Шлюза. Значения по умолчанию: ▪ `mgtServerIP:127.0.0.1`; ▪ `mgtServerPort:8102`. Запрос со значениями по умолчанию успешно выполнится только с узла, на котором установлен Шлюз: `:~$ wget http://localhost:8102/api/health`
`path: ${healthCheckURL:/api/health}`	Адрес для запросов проверки состояния Шлюза. Значение по умолчанию: `healthCheckURL:/api/health`
`token: ${healthCheckAccessKey}`	Задание ключа доступа для аутентификации запросов к API Шлюза. Параметр не имеет значения по умолчанию. 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)
`ssl: *sslprof0`	Настройка SSL
Секция `rabbitmq:`	

Параметр	Описание
`url: ${coordinatorUrl}`	URL, содержащий IP-адрес (или FQDN) и порт (по умолчанию `5672`) для подключения к серверу RabbitMQ, а также очередь - `termidesk`. Параметр не имеет значения по умолчанию. Используемый формат: `amqp(s)://USER:PASS@<IP-адрес>:<порт>/termidesk`. `USER` и `PASS` необязательные параметры, они могут быть заданы в параметрах `coordinatorPass` и `coordinatorPass`. Пример: `coordinatorUrl:ampq://termidesk:ksedimret@disp.termidesk.local:5672/termidesk`. На данный момент поддерживается задание только одного URL для подключения к серверу RabbitMQ. Подключение может использоваться как незащищенное (в этом случае указывается `amqp`), так и защищенное (`amqps`). В случае, если RabbitMQ установлен на том же узле (локально), нужно указать: `coordinatorUrl:amqp://127.0.0.1:5672/termidesk`
`user: ${coordinatorUser}`	Имя пользователя для подключения к серверу RabbitMQ. Параметр не имеет значения по умолчанию. Если параметр задан, то он меняет значение USER в параметре `coordinatorUrl`. При стандартной установке компонента «Универсальный диспетчер» строго по документации в части настроек файла `/etc/rabbitmq/definitions.json` используется `coordinatorUser:termidesk`
`pass: ${coordinatorPass}`	Пароль для подключения серверу RabbitMQ. Параметр не имеет значения по умолчанию. При стандартной установке компонента «Универсальный диспетчер» строго по документации в части настроек файла `/etc/rabbitmq/definitions.json` используется `coordinatorPass:ksedimret`
`timeout: ${coordinatorTimeout}`	Интервал (в секундах) ожидания ответа от сервера RabbitMQ. Параметр не имеет значения по умолчанию
`refreshtime: ${coordinatorRefreshTime}`	Интервал (в секундах) обновления (переопубликации) регистрационной информации (URL и другие данные) Шлюза. Параметр не имеет значения по умолчанию. Значение «0» отключает автоматическую отправку состояния Шлюза на сервер RabbitMQ
`single: ${coordinatorSingle:true}`	Способ передачи данных. Параметр принимает значения: ▪ `true` - данные передаются до первого подтверждения; ▪ `false` - данные передаются по циклу (бесконечно). Значение по умолчанию: `coordinatorSingle:true`
`exchange: ${coordinatorExchange}`	Координатор маршрутизации сообщений, определенный в RabbitMQ. Отвечает за маршрутизацию сообщений в разные очереди. Параметр не имеет значения по умолчанию
`routingkey: ${coordinatorRoutingKey}`	Ключ маршрутизации RabbitMQ, используется для маршрутизации задачи в очереди. Параметр не имеет значения по умолчанию
Секция `loglevel:`	
`info: ${logInfo:true}`	Активация режима журналирования уровня INFO
`debug: ${logDebug:false}`	Активация подробного режима журналирования уровня DEBUG

Пример команды проверки состояния компонента через утилиту `curl` для 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"
```

3.4 . Журналирование

Для просмотра журнала Шлюза `termidesk-gateway` можно выполнить:

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

или:

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

4 . ПРИНЯТЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин	Определение
Балансировщик нагрузки	Самостоятельный компонент, отвечающий за распределение нагрузки на множество «Универсальных диспетчеров» и «Шлюзов»
Виртуальное рабочее место	Также: ВРМ. Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа
Гостевая ОС	ОС, функционирующая на ВМ
Компонент «Менеджер рабочих мест»	Компонент Termidesk. Отделяемый компонент программного комплекса, отвечающий за взаимодействие с поставщиком ресурсов и управления жизненным циклом ВРМ, включая создание, настройку, запуск, отключение и удаление. Является обработчиком фоновых задач. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-taskman.service`
Поставщик ресурсов	ОС, платформа виртуализации или терминальный сервер (MS RDS/STAL), предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов ВРМ
Протокол доставки	Поддерживаемый в Termidesk протокол удаленного доступа к ВРМ
Компонент «Универсальный диспетчер»	Компонент Termidesk. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им ВРМ и контроля доставки ВРМ. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-vdi.service`
Компонент «Шлюз»	Компонент Termidesk. Самостоятельный компонент, отвечающий за туннелирование протоколов доставки, использующих транспортный протокол TCP. В более старой реализации устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-wsproxy.service`. В новой реализации устанавливается из пакета `termidesk-gateway`, поддержка старой реализации удалена, начиная с Termidesk версии 5.0. Наименование службы после установки: `termidesk-gateway.service`.
Ключ	Применяется в контексте файла, не опции в команде. Последовательность псевдослучайных чисел, сгенерированная особым образом
Сертификат	Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу

5 . 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»

UVEON
Unified Virtualization
Experience, Opportunities, Now

119571, г. Москва, Ленинский проспект,
д. 119А, помещ. 9Н
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