TERMIDESK

РУКОВОДСТВО АДМИНИСТРАТОРА

СЛЕТ.10001-01 90 06

Версия 6.0. Выпуск от июня 2025

Настройка компонента «Оркестратор»

ОГЛАВЛЕНИЕ

1 . ОБЩИЕ СВЕДЕНИЯ 3
1.1 . О документе 3
1.2 . Назначение компонента «Оркестратор» 3
1.3 . Требования к программному и аппаратному обеспечению 3
1.4 . Типографские соглашения 4
2 . УСТАНОВКА И УДАЛЕНИЕ КОМПОНЕНТА 5
2.1 . Настройки среды функционирования 5
2.2 . Получение пакетов установки в ОС Astra Linux Special Edition 5
2.3 . Установка Оркестратора 7
2.4 . Удаление Оркестратора 8
2.5 . Обновление Оркестратора 8
2.6 . Постановка Оркестратора на контроль целостности 8
3 . НАСТРОЙКА КОМПОНЕНТА 10
3.1 . Настройка сервера apache2 10
3.2 . Настройка Оркестратора 10
3.3 . Проверка заданных настроек 12
3.4 . Запуск служб 12
3.5 . Журналирование 13
4 . ПРИНЯТЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 14
5 . ПЕРЕЧЕНЬ СОКРАЩЕНИЙ 15

1 . ОБЩИЕ СВЕДЕНИЯ

1.1 . О документе

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

В этом руководстве приведено назначение, установка и настройка компонента «Оркестратор». 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 «Оркестратор»

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

Оркестратор отвечает за согласованную работу всех компонентов Termidesk при децентрализованном развертывании в целях отказоустойчивости и комплексирования с облачными службами.

Оркестратор построен по архитектуре «Клиент - Сервер», выступая по отношению к облачным службам как в роли клиента, так и в роли сервера. Оркестратор также является API-шлюзом: управляющие запросы, пришедшие из облачной инфраструктуры, транслируются (транзитом) в запросы к Termidesk, а ответы (включая ошибки) возвращаются в облачную инфраструктуру.

1.3 . Требования к программному и аппаратному обеспечению

Для установки Оркестратора 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.

Среда функционирования Оркестратора должна соответствовать следующим требованиям:

- должна быть установлена операционная система (ОС) Astra Linux Special Edition версии 1.7 и выше;
- должен быть установлен Python 3.7.3 из состава ОС;
- должен быть доступен API компонента Keystone из состава OpenStack для проверки токена приложения;

- должен быть доступен API компонента «Универсальный диспетчер».

1.4 . Типографские соглашения

Приняты следующие типографские соглашения:

- моноширинный шрифт – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, 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 . Настройки среды функционирования

Узлу, на который будет установлен Оркестратор, необходимо присвоить имя (hostname) при помощи команды:

```
sudo hostname orchestrator.test.lan
```

где orchestrator.test.lan - назначаемое узлу имя.

Для того, чтобы после перезагрузки ОС назначенное имя сохранилось, необходимо внести его в файл /etc/hosts.

Пример файла /etc/hosts с указанием полного и короткого имени узла:

```
127.0.0.1       localhost
192.0.2.35   orchestrator.test.lan orchestrator
```

где 192.0.2.35 - IP-адрес сервера с установленным Оркестратором. Пример IP-адреса приведен в соответствии с RFC 5737, он должен быть заменен на актуальный, используемый согласно схеме адресации, принятой в инфраструктуре организации.

2.2 . Получение пакетов установки в ОС Astra Linux Special Edition

Дистрибутив представлен бинарным файлом пакета 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:

- 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`:

```
1 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 - `1.8_x86-64`;

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

```
sudo cat /var/repos/astra/GPG-KEY-PUBLIC | sudo gpg --dearmour -o /etc/apt/trusted.gpg.d/termidesk.gpg
```

- убедиться, что ключ `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.
В зависимости от используемой версии ОС команды добавления ключа репозитория Termidesk могут отличаться. Если для ОС Astra Linux Special Edition 1.8 ключ репозитория был добавлен командой, применимой к другой версии ОС, то для исправления нужно:

- узнать идентификатор добавленного ключа репозитория:

```
apt-key list
```

- удалить ключ:

```
apt-key --keyring /etc/apt/trusted.gpg del 4E1632CC
```

где `4E1632CC` - последние 8 символов идентификатора ключа;

- вновь добавить ключ репозитория.

- 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.

2.3 . Установка Оркестратора

Перед установкой необходимо подключить локальный репозиторий Termidesk, как приведено в подразделе **Получение пакетов установки в ОС Astra Linux Special Edition**.
Установка Оркестратора выполняется командой:

```
sudo apt install termidesk-orchestrator
```

Установку можно также выполнить из deb-пакета, не подключая локальный репозиторий:

```
sudo apt install /home/user/termidesk-orchestrator_XXX-astra17_amd64.deb
```

где `/home/user/termidesk-orchestrator_XXX-astra17_amd64.deb` - путь к deb пакету.

В процессе установки необходимо принять лицензионное соглашение, доступное в псевдографическом интерфейсе. Для виспользования псевдографического интерфейса должен быть установлен пакет `dialog`.

Дополнительно установятся следующие пакеты (зависимости):

- apache2;
- ssl-cert;
- memcached;
- openssl;
- libcurl3-nss;
- libcairo2;
- gettext;
- python3-click;
- python3-distutils.

2.4 . Удаление Оркестратора

Удаление Оркестратора из среды ОС Astra Linux Special Edition 1.7 выполняется командой:

```
sudo aptitude purge -y termidesk-orchestrator
```

где:

`-y` - ключ для пропуска подтверждения удаления.

После удаления необходимо очистить оставшиеся зависимости и конфигурации:

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

Команда полностью удалит оставшиеся настройки и зависимости уже удаленных пакетов.

2.5 . Обновление Оркестратора

Обновление Оркестратора выполняется установкой новой версии поверх предыдущей.

2.6 . Постановка Оркестратора на контроль целостности

После установки и настройки Оркестратора необходимо поставить его на контроль целостности.

Для контроля целостности используются встроенные в ОС Astra Linux Special Edition программные средства на основе `Another File Integrity Checker`, представленного пакетом `afick`.

Настройка регламентного контроля целостности выполняется в конфигурационном файле `/etc/afick.conf`.

> Настройку следует производить только после окончательного внедрения компонента, поскольку с файлов конфигурации и исполняемых файлов будут сняты эталонные контрольные суммы.

Для постановки на контроль целостности Оркестратора необходимо добавить в конфигурационный файл `/etc/afick.conf` следующие строки:

```
/etc/default/termidesk-orchestrator PARSEC
/etc/opt/termidesk-orchestrator  PARSEC
/opt/termidesk  PARSEC
/usr/lib/systemd/system/termidesk-orchestrator.service  PARSEC
/usr/share/doc/termidesk-orchestrator  PARSEC
/var/opt/termidesk-ochestrator  PARSEC

#Репозиторий Termidesk
/var/repos/ PARSEC
```

Для снятия эталонных значений контрольных сумм используется команда:

```
afick -i
```

Для проверки соответствия контрольных сумм эталонным значениям автоматически создаются задания в системном планировщике заданий `cron`.

Для ручной проверки соответствия контрольных сумм используется команда:

```
afick -k
```

> В случае отсутствия по какой-либо причине исполняемых фалов `*.pyc`, они будут повторно сгенерированы при перезапуске сервера Python. В этом случае нужно повторно проинициализировать средство регламентного контроля целостности `afick`.

3 . НАСТРОЙКА КОМПОНЕНТА

3.1 . Настройка сервера apache2

Вместе с Оркестратором будет установлен сервер apache2, если он не был установлен ранее.

После установки Оркестратора необходимо скорректировать файл конфигурации веб-сервера `/etc/apache2/apache2.conf`. Для этого следует найти и раскомментировать строку с параметром `AstraMode`, далее присвоить данному параметру значение `off`, точно соблюдая отступы и пробелы в файле.

Пример:

```
# Astra security mode.
#
AstraMode off
```

После перезапустить веб-сервер:

```
sudo systemctl restart apache2
```

3.2 . Настройка Оркестратора

Для настройки Оркестратора нужно отредактировать разделы `Termidesk params` и `OpenStack params` в файле `/opt/termidesk/share/termidesk-orchestrator/src/config/orc_config.py`.

При первой установке этот конфигурационный файл отсутствует. Его можно скопировать из шаблона `/opt/termidesk/share/termidesk-orchestrator/src/config/orc_config.py.dist`, для этого:

- перейти в каталог с конфигурационными файлами:

```
cd /opt/termidesk/share/termidesk-orchestrator/src/config
```

- переключиться на пользователя `termidesk`:

```
sudo -u termidesk bash
```

- скопировать шаблон в новый файл:

```
cp orc_config.py.dist orc_config.py
```

- выйти из окружения пользователя `termidesk` :

```
exit
```

Параметры внутри разделов конфигурационного файла `/opt/termidesk/share/termidesk-orchestrator/src/config/orc_config.py` имеют следующую структуру:

```
ВНУТРЕННЯЯ_ПЕРЕМЕННАЯ = os.getenv("ПЕРЕМЕННАЯ_ОКРУЖЕНИЯ", "ЗНАЧЕНИЕ_ВВОДИМОЕ_ВРУЧНУЮ")
```

где:

`ПЕРЕМЕННАЯ_ОКРУЖЕНИЯ` - наименование переменной окружения, назначенной через команду `export`. Если переменная в окружении не задана, она добавится с указанным значением;

`ЗНАЧЕНИЕ_ВВОДИМОЕ_ВРУЧНУЮ` - новое значение переменной.

Пример файла `/opt/termidesk/share/termidesk-orchestrator/src/config/orc_config.py`:

```
# Termidesk params
TERMIDESK_HOST = os.getenv("TSRV_HOST", '')
TERMIDESK_PORT = os.getenv("TERMIDESK_PORT", "")
TERMIDESK_USERNAME = os.getenv("TSRV_USERNAME", '')
TERMIDESK_PASSWORD = os.getenv("TSRV_PASSWORD", '')
#Termidesk auth domain ID: authSmallName
 TERMIDESK_AUTH = os.getenv("TSRV_AUTH", '')
TERMIDESK_AUTH_URL = os.getenv('TSRV_AUTH_URI', '/api/auth/draft/legacy/login')

# OpenStack params
# The name of application credentials
APP_CREDENTIALS_NAME = os.getenv("APP_CREDENTIALS_NAME", "")
# The secret for application credentials
APP_CREDENTIALS_SECRET = os.getenv("APP_CREDENTIALS_SECRET", "")
# The user name for application credentials
APP_CREDENTIALS_USER_NAME = os.getenv("APP_CREDENTIALS_USER_NAME", "")
# The name of user domain for application credentials
APP_CREDENTIALS_USER_DOMAIN = os.getenv("APP_CREDENTIALS_USER_DOMAIN", "")
# The url of application credentials authentication. Example: http://0.0.0.0/identity/v3/auth/tokens
OPENSTACK_AUTH_URL = os.getenv("OPENSTACK_AUTH_URL", "")
```

Список доступных параметров конфигурационного файла приведен в таблице (см. Таблица 1).

Таблица 1 – Описание параметров конфигурационного файла Оркестратора

Параметр	Назначение	Значение по умолчанию
Параметры компонента «Универсальный диспетчер» (секция `Termidesk params`)		
`TERMIDESK_HOST`	FQDN или IP-адрес компонента «Универсальный диспетчер»	Не задано
`TERMIDESK_PORT`	Номер порта компонента «Универсальный диспетчер» (как правило, 80 или 443)	Не задано
`TERMIDESK_USERNAME`	Имя пользователя с правами администратора в компоненте «Универсальный диспетчер»	Не задано
`TERMIDESK_PASSWORD`	Пароль пользователя с правами администратора в компоненте «Универсальный диспетчер»	Не задано

TERMIDESK_AUTH	Идентификатор домена аутентификации (authSmallName, метка) в компоненте «Универсальный диспетчер», в который входит пользователь TERMIDESK_USERNAME	Не задано
TERMIDESK_AUTH_URL	Данный URL используется для проверки состояния (health check) компонента «Универсальный диспетчер». Если страница доступна (получен ответ: HTTP_200_OK), то считается, что компонент «Универсальный диспетчер» функционирует правильно	'/api/auth/draft/legacy/login'
Параметры для проверки пароля приложений OpenStack (секция OpenStack params)		
APP_CREDENTIALS_NAME	Имя приложения для подключения к OpenStack	Не задано
APP_CREDENTIALS_SECRET	Ключ-пароль для подключения к OpenStack. Может быть задан или автоматически сгенерирован при создании доступа для приложения. Отображается в интерфейсе OpenStack только один раз, и, в случае утери, требует перегенерации	Не задано
APP_CREDENTIALS_USER_NAME	Имя пользователя, предоставляющего доступ приложению. Уровень пользователя должен быть не ниже «member». Возможные варианты уровня: «member», «admin»,«owner»	Не задано
APP_CREDENTIALS_USER_DOMAIN	Имя (не идентификатор) домена OpenStack, в который входит пользователь APP_CREDENTIALS_USER_NAME	Не задано
OPENSTACK_AUTH_URL	URL компонента Identity, располагается в OpenStack по пути «Проект - Доступ к API - Identity»	Не задано

3.3 . Проверка заданных настроек

Для проверки корректности заданных настроек применяется исполняемый файл /opt/termidesk/share/termidesk-orchestrator/src/self_check.py.

Для его использования нужно выполнить команды:

```
cd /opt/termidesk/share/termidesk-orchestrator/src/
python3 self_check.py
```

Если во время проверки возникает ошибка, подробную информацию о ней можно найти в файле /tmp/termidesk_self_check_crash.log. Файл журнала перезаписывается при каждом запуске проверок.

3.4 . Запуск служб

Запуск служб осуществляется после задания настроек и проверки их корректности.

Добавить в автоматический запуск службу Оркестратора:

```
sudo systemctl enable termidesk-orchestrator.service
```

Затем запустить службу:

```
sudo systemctl start termidesk-orchestrator.service
```

3.5 . Журналирование

Журнал работы Оркестратора расположен в файле `/var/log/termidesk/orchestrator.log`.

4 . ПРИНЯТЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин	Определение
Балансировщик нагрузки	Самостоятельный компонент, отвечающий за распределение нагрузки на множество «Универсальных диспетчеров» и «Шлюзов»
Домен аутентификации	Способ проверки субъектов и их полномочий
Компонент «Оркестратор»	Компонент Termidesk. Самостоятельный компонент, отвечающий за согласованную работу всех компонентов программного комплекса при децентрализованном развертывании, для нужд отказоустойчивости и комплексирования с облачными службами
Компонент «Универсальный диспетчер»	Компонент Termidesk. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение и контроль доставки им рабочих мест. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-vdi.service`
Ключ	Последовательность псевдослучайных чисел, сгенерированная особым образом
Сертификат	Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу

5 . ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Пояснение
ОС	Операционная система
ПО	Программное обеспечение
API	Application Programming Interface (интерфейс прикладного программирования)
FQDN	Fully Qualified Domain Name (полностью определенное имя домена)
HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
IP	Internet Protocol (межсетевой протокол)
RFC	Request for Comments (рабочее предложение Интернет)
URL	Uniform Resource Locator (унифицированный указатель ресурса)

UVEON
Unified Virtualization
Experience, Opportunities, Now

© ООО «УВЕОН»

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