TERMIDESK

# РУКОВОДСТВО АДМИНИСТРАТОРА

СЛЕТ.10001-01 90 08

Версия 6.0. Выпуск от июня 2025

## Установка и настройка «Агрегатора»

# ОГЛАВЛЕНИЕ

1 . ОБЩИЕ СВЕДЕНИЯ ..... 6
1.1 . О документе ..... 6
1.2 . Назначение «Агрегатора» ..... 6
1.3 . Типографские соглашения ..... 6
2 . ТРЕБОВАНИЯ К СРЕДЕ ФУНКЦИОНИРОВАНИЯ ..... 8
2.1 . Требования к аппаратному обеспечению ..... 8
2.2 . Требования к программному обеспечению ..... 8
2.3 . Требования к синхронизации времени ..... 8
2.4 . Требования к службам DNS и DHCP ..... 8
2.5 . Требования к серверам каталогов ..... 8
3 . УСТАНОВКА И УДАЛЕНИЕ ..... 10
3.1 . Получение пакетов установки в ОС Astra Linux Special Edition ..... 10
3.2 . Подготовка среды функционирования ..... 12
3.3 . Установка «Агрегатора» ..... 12
3.3.1 . Неавтоматизированная установка «Агрегатора» ..... 12
3.3.2 . Автоматизированная установка «Агрегатора» ..... 13
3.3.3 . Проверка работоспособности после установки ..... 14
3.3.4 . Распределенная установка «Агрегатора» ..... 16
3.3.4.1 . Основные принципы распределенной установки ..... 16
3.3.4.2 . Установка и настройка СУБД PostgreSQL ..... 18
3.3.4.3 . Установка первого узла с «Агрегатором» ..... 19
3.3.4.4 . Установка «Шлюзов» ..... 19
3.3.4.5 . Установка «Менеджеров рабочих мест» ..... 20
3.3.4.6 . Установка балансировщиков ..... 21
3.3.4.7 . Действия после распределенной установки ..... 21
3.4 . Обновление «Агрегатора» ..... 21

3.4.1 . Комплексное обновление «Агрегатора» ....21
3.5 . Обновление для распределенной конфигурации установки «Агрегатора» .... 22
3.5.1 . Общая концепция обновления ....22
3.5.2 . Шаг 1. Редактирование конфигурации балансировщика нагрузки ....25
3.5.3 . Шаг 2. Установка и настройка RabbitMQ ....26
3.5.4 . Шаг 3. Резервное копирование RSA-ключей ....26
3.5.5 . Шаг 4. Обновление первого «Менеджера рабочих мест» ....26
3.5.6 . Шаг 5. Обновление второго «Менеджера рабочих мест» ....27
3.5.7 . Шаг 6. Обновление узлов «Агрегаторов» ....27
3.5.8 . Шаг 7. Восстановление конфигурации балансировщика нагрузки ....28
3.6 . Удаление «Агрегатора» .... 28
4 . ГРАФИЧЕСКИЙ ИНТЕРФЕЙС ....30
4.1 . Доступ к веб-интерфейсу .... 30
4.2 . Типы веб-интерфейса .... 30
4.3 . Основные функции веб-интерфейса .... 30
4.3.1 . Функция «Обзор» ....30
4.3.2 . Функция «Инфраструктура» ....31
4.3.3 . Функция «Управление» ....31
4.3.4 . Функция «Журналы» ....32
4.3.5 . Функция «Системные параметры» ....32
4.3.6 . Функция «Консоль управления фермами» ....32
5 . НАСТРОЙКА АГРЕГАЦИИ РЕСУРСОВ ....33
5.1 . Последовательность шагов для настройки агрегации ресурсов .... 33
6 . ДОМЕНЫ АУТЕНТИФИКАЦИИ ....34
6.1 . Общие сведения о доменах аутентификации .... 34
6.1.1 . Добавление аутентификации через MS AD (LDAP) ....35
6.1.2 . Перечень параметров для добавления домена аутентификации MS AD (LDAP) ....35
6.1.3 . Получение и добавление файла keytab для Kerberos-аутентификации ....39

6.1.4 . Настройка пользовательской рабочей станции для Kerberos-аутентификации ....41
6.2 . Добавление домена аутентификации OIDC .... 44
6.3 . Действия над группами в домене аутентификации .... 46
6.4 . Действия над пользователями в домене аутентификации.... 48
7 . ФЕРМЫ ПОСТАВЩИКОВ РЕСУРСОВ....51
7.1 . Общие сведения о фермах поставщиков ресурсов .... 51
7.2 . Добавление фермы поставщиков ресурсов .... 52
8 . УЗЛЫ....54
8.1 . Общие сведения об узлах .... 54
8.2 . Добавление узла Termidesk .... 55
9 . САЙТЫ ....57
9.1 . Общие сведения о сайтах .... 57
9.2 . Добавление сайта .... 58
9.3 . Добавление объединенного набора ресурсов.... 59
10 . ШАБЛОНЫ ТЕХОБСЛУЖИВАНИЯ ....60
10.1 . Общие сведения о шаблонах техобслуживания .... 60
10.2 . Добавление шаблона техобслуживания .... 61
11 . НАСТРОЙКА ПОДКЛЮЧЕНИЯ ПОЛЬЗОВАТЕЛЕЙ ЧЕРЕЗ ШЛЮЗ ....62
11.1 . Общие сведения по использованию шлюза .... 62
11.2 . Добавление шлюза .... 63
12 . СИСТЕМНЫЕ НАСТРОЙКИ....64
12.1 . Назначение служебных функций администраторам.... 64
12.2 . Параметры конфигурирования «Агрегатора» .... 66
12.3 . Утилиты интерфейса командной строки для настройки Агрегатора.... 79
12.3.1 . Утилита termidesk-config....79
13 . КОНСОЛЬ УПРАВЛЕНИЯ ФЕРМАМИ....84
13.1 . Общие сведения по управлению из консоли .... 84

13.2 . Управление фондами РМ ..... 84
13.3 . Управление сессиями ..... 85
13.4 . Управление индивидуальными рабочими местами ..... 86
14 . СИСТЕМА АУДИТА ..... 89
14.1 . Журналы ..... 89
14.2 . Настройка журналирования ..... 89
14.3 . Просмотр журналов ..... 89
14.3.1 . Просмотр системного журнала ..... 89
14.3.2 . Просмотр журнала аудита ..... 90
14.4 . Описание шаблонов событий аудита ..... 91
14.4.1 . Типы данных регистрируемой информации событий аудита ..... 91
14.4.2 . Типы и шаблоны регистрируемых событий аудита ..... 91
14.4.3 . Форматы регистрируемых событий аудита и их примеры ..... 96
15 . ХРАНЕНИЕ ЧУВСТВИТЕЛЬНОЙ ИНФОРМАЦИИ ..... 97
15.1 . Хранение чувствительной информации с выбранным способом хранения «hvac» ..... 97
16 . ПЕРЕЧЕНЬ ТЕРМИНОВ ..... 100
17 . ПЕРЕЧЕНЬ СОКРАЩЕНИЙ ..... 101

# 1 . ОБЩИЕ СВЕДЕНИЯ

## 1.1 . О документе

Настоящий документ является восьмой частью руководства администратора на программный комплекс «Диспетчер подключений виртуальных рабочих мест Termidesk» (далее - Termidesk). Документ определяет назначение, установку и настройку «Агрегатора» и предназначен для администраторов системы и сети.

## 1.2 . Назначение «Агрегатора»

«Агрегатор» - это тип роли, доступный при установке Termidesk. «Агрегатор» является единой точкой входа для получения ресурсов пользователями Termidesk и предоставляет им объединенный список приложений с нескольких установок Termidesk, с возможностью объединения одинаковых приложений или виртуальных рабочих мест (ВРМ).
«Агрегатор» должен быть установлен отдельно от узлов с ролями «Портал администратора», «Портал пользователя».
«Агрегатор» может быть установлен со следующими типами веб-интерфейса:

- «Агрегатор администратора» - веб-интерфейс управления «Агрегатором»;
- «Агрегатор пользователя» - веб-интерфейс пользователя для получения ресурсов, предоставляемых Агрегатором;
- «Агрегатор универсальный» - веб-интерфейс, предоставляющий функции обоих вариантов.

Функции «Агрегатора»:

- объединение установки основных узлов Termidesk в виде ферм поставщиков ресурсов;
- дедупликация (объединение, устранение дубликатов) приложений или ВРМ на фермах поставщиков ресурсов;
- создание единого списка ресурсов (приложений, ВРМ) для пользователя с нескольких ферм поставщиков ресурсов.

## 1.3 . 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 . ТРЕБОВАНИЯ К СРЕДЕ ФУНКЦИОНИРОВАНИЯ

## 2.1 . Требования к аппаратному обеспечению

Минимальные аппаратные требования узла должны соответствовать следующим:

- процессор архитектуры x86-64 (AMD, Intel), не менее 4 шт.;
- оперативная память, не менее 4 ГБ. Следует учесть, что для работы службы `termidesk-celery-worker` требуется, чтобы на каждое ядро процессора было выделено по 500 Мб оперативной памяти;
- свободное дисковое пространство, не менее 1 ГБ;
- сетевое соединение, не менее 100 Мбит/с.

## 2.2 . Требования к программному обеспечению

В среде функционирования должны быть предварительно установлены:

- ОС Astra Linux Special Edition версии 1.8 (минимальная версия - 1.8.1);
- СУБД PostgreSQL версии 15 из состава репозитория ОС Astra Linux Special Edition версии 1.8. Из внешних по отношению к ОС Astra Linux Special Edition версии 1.8 СУБД поддерживается СУБД PostgreSQL версии 12 и выше;
- брокер сообщений RabbitMQ из состава репозитория ОС Astra Linux Special Edition.

ОС Astra Linux Special Edition версии должна быть установлена из `iso`-образа, доступного в личном кабинете на портале Astra Linux: https://lk-new.astralinux.ru/. Работа Termidesk на преднастроенных образах ОС не гарантируется.

## 2.3 . Требования к синхронизации времени

В сетевой инфраструктуре должен быть настроен NTP-сервер, обеспечивающий синхронизацию времени для компонентов Termidesk.

## 2.4 . Требования к службам DNS и DHCP

В сетевой инфраструктуре должны быть развернуты и исправно функционировать службы доменных имен (DNS) и автоматического назначения сетевых параметров (DHCP) в необходимых сегментах сети.

## 2.5 . Требования к серверам каталогов

Серверы каталогов должны удовлетворять следующим требованиям:

- сервер каталогов должен размещаться в том же сегменте локальной сети, где развернут «Агрегатор». Если выполнение требования невозможно и сервер каталогов находится в другом сегменте, то необходимо обеспечить маршрутизацию между этими сегментами;

- при использовании Microsoft Active Directory Domain Service (далее - MS AD) необходимо создать сервисную учетную запись для взаимодействия Termidesk с контроллером домена (КД). Допускается использование учетной записи администратора домена;
- при использовании MS AD рекомендуется создавать отдельные организационные подразделения (OU) для пользователей рабочих мест (РМ) и для учетных записей типа «Компьютер» для самих РМ. Права на OU для компьютеров должны быть либо у созданной сервисной учетной записи, либо у отдельной созданной учетной записи, допускается также использовать учетную запись администратора домена.

# 3 . УСТАНОВКА И УДАЛЕНИЕ

## 3.1 . 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`:

```
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.

### 3.2 . Подготовка среды функционирования

Перед установкой «Агрегатора» должна быть предварительно подготовлена среда функционирования узла:

- установлена и настроена СУБД PostgreSQL;
- установлен и настроен брокер сообщений RabbitMQ.

Подготовка среды функционирования осуществляется аналогично разделу **Подготовка среды функционирования** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса».

Узел «Агрегатора» не должен использовать экземпляры БД и брокера сообщений RabbitMQ, предназначенные для других компонентов Termidesk. БД и брокер сообщений RabbitMQ могут быть установлены локально на узел «Агрегатора».

Для корректной регистрации событий подключения пользователя к ресурсу фермы Termidesk необходимо на всех узлах «Универсального диспетчера», ферма которого подключается к порталу «Агрегатор», перейти «Настройки - Системные параметры - Безопасность» и включить параметр «Использовать анонсируемый IP клиента».
В противном случае при подключении пользователей к ресурсам ферм Termidesk в журналах «Универсального диспетчера» будет отображен IP-адрес портала «Агрегатор», а не IP-адреса подключившихся пользователей.

### 3.3 . Установка «Агрегатора»

#### 3.3.1 . Неавтоматизированная установка «Агрегатора»

Перед установкой «Агрегатора» должна быть подготовлена среда функционирования (см. подраздел **Подготовка среды функционирования**).

Установка производится аналогично подразделу **Неавтоматизированная установка** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса».

Установка веб-порталов «Агрегатор администратора» и «Агрегатор пользователя» не предусмотрена в рамках лицензии Termidesk Terminal.

Установка веб-порталов «Агрегатор администратора» и/или «Агрегатор пользователя» должна производиться на узле, отличном от «Портала администратора» и/или «Портала пользователя» Termidesk.
Предполагается, что Агрегатор может быть настроен на работу с компонентом «Шлюз», устанавливаемого из пакета `termidesk-gateway`. Для установки или обновления «Шлюза» следует обратиться к подразделам **Установка Шлюза** и **Обновление Шлюза** документа СЛЕТ.10001-01 90 05 «Руководство администратора. Настройка компонента «Шлюз».

В процессе установки необходимо отметить следующие пункты:

Описание относится к комплексной установке: все указанные роли устанавливаются на одном узле.

- «Агрегатор администратора (AGGR_ADM)». После установки будет запущена служба `termidesk-vdi`;
- и (или) «Агрегатор пользователя (AGGR_USR)». После установки будет запущена служба `termidesk-vdi`;
- «Менеджер рабочих мест (CELERYMAN)». После установки будут запущены службы `termidesk-celery-beat`, `termidesk-celery-worker`.

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

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

Затем перезапустить веб-сервер:

```
sudo systemctl restart apache2
```

После установки параметры «Агрегатора» могут быть изменены через файл `/etc/opt/termidesk-vdi/termidesk.conf` (см. подраздел **Параметры конфигурирования «Агрегатора»**) или через утилиту `termidesk-config` (см. подраздел **Утилита termidesk-config**).

### 3.3.2 . Автоматизированная установка «Агрегатора»

Перед установкой «Агрегатора» должна быть подготовлена среда функционирования (см. подраздел **Подготовка среды функционирования**).

Для автоматизированной установки рекомендуется предварительно подготовить файл `/etc/opt/termidesk-vdi/termidesk.conf`, описание параметров которого приведено в подразделе **Параметры конфигурирования «Агрегатора»**, и затем выполнить:

```
sudo apt -y install termidesk-vdi
```

⚠ Перед установкой следует убедиться, что в БД отсутствуют записи (необходимо использовать чистую БД).

Пример файла `/etc/opt/termidesk-vdi/termidesk.conf` с установленными значениями имени пользователи и пароля по умолчанию, без использования защищенного подключения к БД и RabbitMQ (см. раздел **Подготовка среды функционирования**):

```
SECRETS_STORAGE_METHOD='config'
DB_CLUSTER_MODE='single'
DBHOST='localhost'
DBPORT='5432'
DBSSL='Disable'
DBNAME='termidesk'
DBUSER='termidesk'
DBPASS='ksedimret'
DBCERT=
DBKEY=
DBCHAIN=
DJANGO_SECRET_KEY='XejStbL6jtZ7DGTH02vJpw4vf1zTWM07RqWhwWGYKgs='
RABBITMQ_URL1='amqp://termidesk:ksedimret@localhost:5672/termidesk'
RABBITMQ_URL2=
RABBITMQ_URL3=
RABBITMQ_SSL='Disable'
LOG_LEVEL='INFO'
LOG_ADDRESS='/dev/log'
LOG_FACILITY='local3'
HEALTH_CHECK_ACCESS_KEY='270c1e6a4cd013a3824982458a26ec4dcac17f60f80a74098a62994f775351e2'
METRICS_ACCESS_KEY='2559773a3b1104064bbcb0b5315749a3783cb4f2fae6ee1925dc84ac0eef0f09'
NODE_ROLES='AGGR_ADM,AGGR_USR,CELERYMAN'
EULA_ACCEPTED='YES'
AGGREGATOR_ACCESS_TOKEN_TITLE='Termidesk JWT Title'
AGGREGATOR_JWT_SSL_KEY=
AGGREGATOR_ACCESS_TOKEN_TTL_SECONDS=600
```

После установки указанные в открытом виде пароли можно привести к преобразованным значениям через утилиту `/opt/termidesk/bin/scramble` (см. подраздел **Параметры конфигурирования «Агрегатора»**).

### 3.3.3 . Проверка работоспособности после установки

«Агрегатор» является работоспособным, если в результате перехода в веб-браузере по адресу https://localhost/ или https://127.0.0.1/ отобразилась страница входа (см. Рисунок 1) в веб-портал. Если страница сразу не отобразилась, следует подождать 10-15 секунд и обновить ее.

> После установки по умолчанию для доступа к порталу включено перенаправление на протокол HTTPS. При необходимости использования незащищенного протокола HTTP администратор должен изменить файл `/etc/apache2/sites-available/termidesk.conf`.

Указанные адреса используются в случае локальной установки. Если «Агрегатор» установлен на узле, отличном от того, на котором происходит проверка, необходимо вместо localhost или 127.0.0.1 использовать IP-адрес узла «Агрегатора».

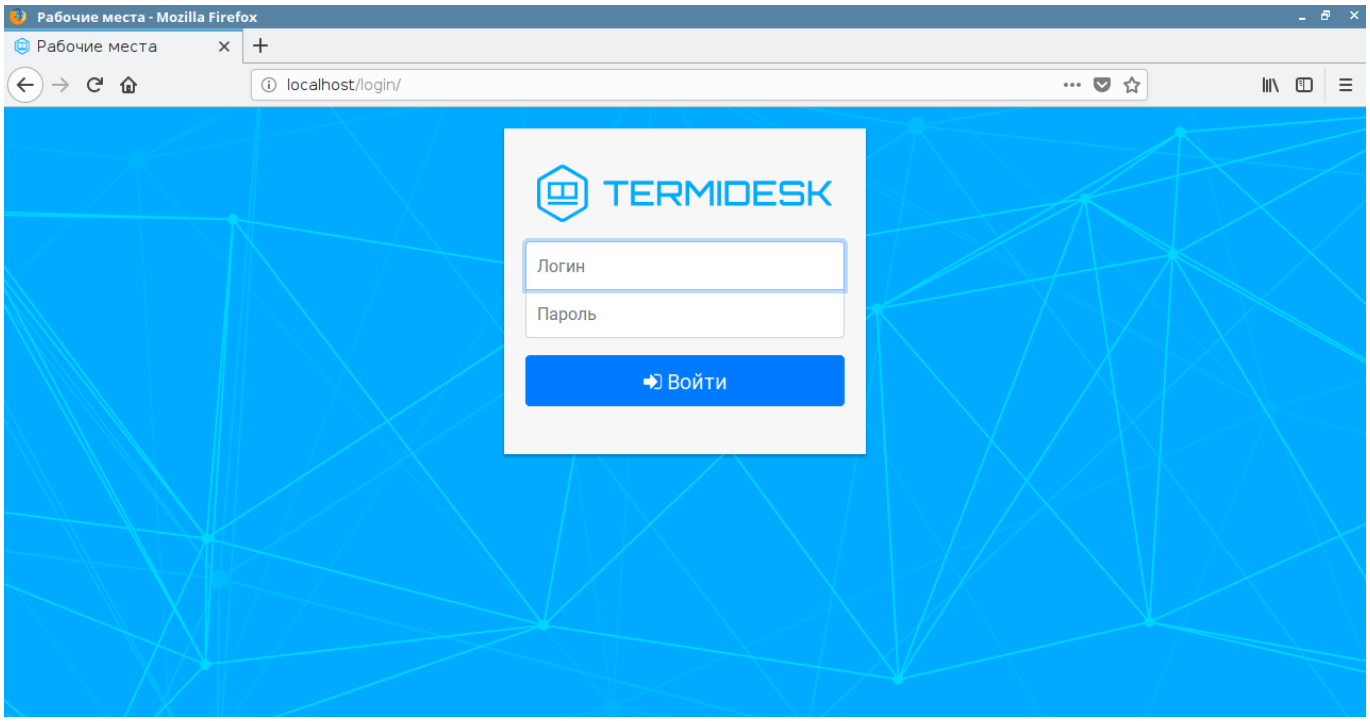



Рисунок 1 – Авторизация в веб-портале Агрегатора

По умолчанию после установки вход в веб-портал доступен только авторизованному пользователю ОС с ролью «Администратор»:

- пользователь ОС должен быть членом группы `astra-admin (1001)`
- для входа в полях «Логин» и «Пароль» необходимо указать идентификатор пользователя ОС и его пароль соответственно, а затем нажать экранную кнопку **[Войти]**.

Проверка добавления ключа от репозитория производителя в ОС выполняется командой:

```
apt-key list
```

Проверка состояния компонентов выполняется командами:

```
1  systemctl status termidesk-vdi.service
2  systemctl status termidesk-celery-beat.service
3  systemctl status termidesk-celery-worker.service
```

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

### 3.3.4 . Распределенная установка «Агрегатора»

#### 3.3.4.1 . Основные принципы распределенной установки

В Termidesk предусмотрена распределенная установка компонентов на отдельные серверы или ВМ.

> ⓘ Описание применимо к ферме «Агрегатора».

Установка компонентов Termidesk выполняется в среде функционирования ОС Astra Linux Special Edition.

В распределенном варианте устанавливаются:

- «Агрегатор» (служба `termidesk-vdi`);
- «Шлюз» (при необходимости, служба `termidesk-gateway`);
- «Менеджер рабочих мест» (службы `termidesk-celery-beat`, `termidesk-celery-worker`).

Перечень условий для распределенной установки:

- брокер сообщений RabbitMQ устанавливается на одном узле с СУБД (в общем случае этот компонент может устанавливаться на отдельный узел, но в рамках настоящей процедуры данный вариант не рассматривается);

> ⚠ При использовании внешней по отношению к Termidesk СУБД, следует установить брокер сообщений RabbitMQ на узел «Менеджера рабочих мест» или на отдельный узел.

- на всех узлах, предназначенных для установки компонентов, настроены статические IP-адреса;
- на всех узлах настроена синхронизация времени от единого источника.

Упрощенная общая схема при распределенной установке Termidesk приведена на рисунке (см. Рисунок 2).

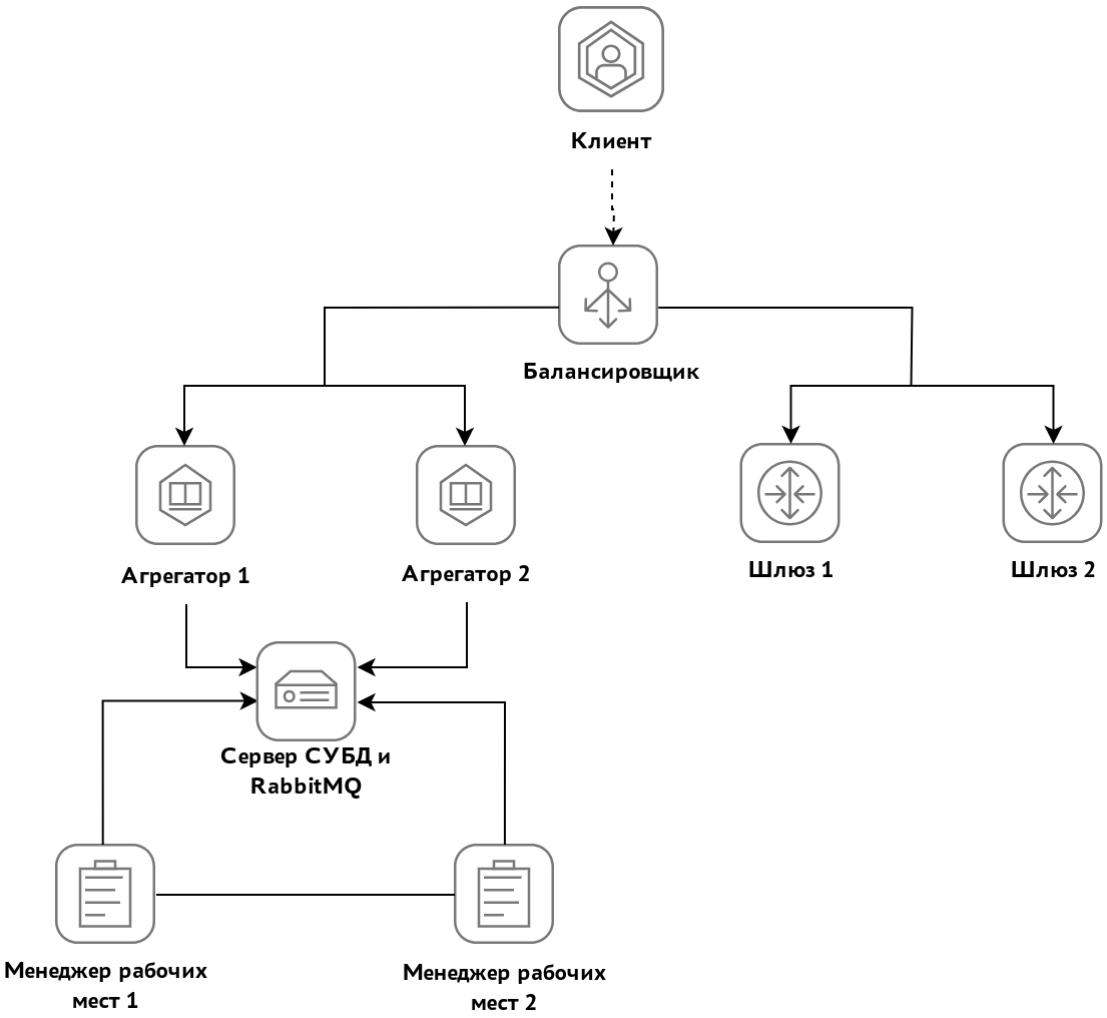



Рисунок 2 – Схема распределенной установки

Перечень обозначенных на схеме компонентов приведен в таблице (см. Таблица 1).

Таблица 1 – Перечень компонентов

| Компонент | FQDN | Подпись на схеме |
|---|---|---|
| «Агрегатор» №1 с ролью «Агрегатор универсальный» | `aggr1termidesk.local` | «Агрегатор 1» |
| «Агрегатор» №2 с ролью «Агрегатор универсальный» | `aggr2.termidesk.local` | «Агрегатор 2» |
| «Шлюз» №1 | `gw1.termidesk.local` | «Шлюз 1» |
| «Шлюз» №2 | `gw2.termidesk.local` | «Шлюз 2» |
| «Менеджер рабочих мест» №1 | `tsk1.termidesk.local` | «Менеджер рабочих мест 1» |
| «Менеджер рабочих мест» №2 | `tsk2.termidesk.local` | «Менеджер рабочих мест 2» |
| Балансировщик нагрузки (`nginx`) | `nginx.termidesk.local` | «Балансировщик» |
| База данных с брокером сообщений RabbitMQ | `db.termidesk.local` | «Сервер СУБД и RabbitMQ» |

Распределенная установка проводится в следующей последовательности:

1) на одном узле устанавливаются СУБД и RabbitMQ. При установке следует учесть, что в БД должны отсутствовать записи (необходимо использовать чистую БД);

2) устанавливается первый (эталонный) узел с «Агрегатором». При установке необходимо выбрать роль «Агрегатор универсальный». Роль активируется при одновременном выборе ролей «Агрегатор администратора» и «Агрегатор пользователя» в диалоговом окне псевдографического интерфейса инсталлятора;

> Настройки первого узла с «Агрегатором» будут использоваться как эталонные для других узлов.
> Параметры конфигурации находятся в файле `/etc/opt/termidesk-vdi/termidesk.conf`.
> Нужно скопировать каталог `/etc/opt/termidesk-vdi` вместе с его содержимым на другие узлы «Агрегатора» и «Менеджера рабочих мест».

3) устанавливаются остальные «Агрегаторы» с копированием файлов, указанных в п.2, с эталонного узла;

4) устанавливаются «Шлюзы», настраивается защищенное подключение к «Шлюзу», каталог `/etc/termidesk/` копируется с первого узла «Шлюза» на другие узлы с этим компонентом;

5) устанавливаются «Менеджеры рабочих мест» с копированием файлов, указанных в п.2, с эталонного узла.

Заключительным этапом устанавливаются и настраиваются балансировщики нагрузки на базе ОС Astra Linux Special Edition и `nginx`.

#### 3.3.4.2 . Установка и настройка СУБД PostgreSQL

Процесс установки брокера сообщений RabbitMQ не отличается от процесса, описанного в разделе **Подготовка среды функционирования**. Установка и настройка СУБД PostgreSQL осуществляется согласно выбранной версии.

Для завершения настройки нужно:

- отредактировать файл `/etc/rabbitmq/rabbitmq-env.conf`, приведя его к виду:

```
# Defaults to rabbit. This can be useful if you want to run more than one node
# per machine - RABBITMQ_NODENAME should be unique per erlang-node-and-machine
# combination. See the clustering on a single machine guide for details:
# http://www.rabbitmq.com/clustering.html#single-machine
#NODENAME=rabbit

# By default RabbitMQ will bind to all interfaces, on IPv4 and IPv6 if
# available. Set this if you only want to bind to one network interface or#
# address family.
NODE_IP_ADDRESS=0.0.0.0
# Defaults to 5672.
NODE_PORT=5672
```

- сохранить файл и перезапустить службу `rabbitmq-server`:

```
sudo systemctl restart rabbitmq-server
```

#### 3.3.4.3 . Установка первого узла с «Агрегатором»

Процесс установки первого узла с «Агрегатором» аналогичен комплексной установке, за исключением выбора только ролей «Агрегатор администратора» и «Агрегатор пользователя».

После установки передать каталог `/etc/opt/termidesk-vdi` на остальные узлы «Агрегатора» и «Менеджера рабочих мест»:

```
sudo scp -r /etc/opt/termidesk-vdi localuser@ipaddr_or_fqdn_host:/home/user/
```

где:

`-r` - ключ для рекурсивной (со вложенными каталогами) передачи;

`localuser` - имя пользователя целевого узла;

`ipaddr_or_fqdn_host` - IP-адрес или FQDN целевого узла;

`/home/user` - путь, куда будет скопирован каталог.

Перед началом установки остальных узлов «Универсальных диспетчеров» необходимо переместить скопированный ранее каталог `termidesk-vdi` в каталог `/etc/opt/`:

```
sudo mv /home/user/termidesk-vdi /etc/opt/
```

Установить второй узел с «Агрегатором» по аналогии с первым, не меняя параметры в диалогах подключения к СУБД и заполнения информации о подключении к RabbitMQ.

#### 3.3.4.4 . Установка «Шлюзов»

Установка «Шлюзов» выполняется из пакета `termidesk-gateway`.

> ⚠ Для установки «Шлюза» следует обратиться к подразделу **Установка Шлюза** документа СЛЕТ.10001-01 90 05 «Руководство администратора. Настройка компонента «Шлюз».

После завершения установки нужно:

- настроить защищенное подключение к «Шлюзу» согласно подразделу **Настройка защищенного подключения к Шлюзу** документа СЛЕТ.10001-01 90 05 «Руководство администратора. Настройка компонента «Шлюз»;
- привести файл `/etc/termidesk/gateway.yaml` к виду согласно подразделу **Параметры конфигурирования компонента** документа СЛЕТ.10001-01 90 05 «Руководство администратора. Настройка компонента «Шлюз». Задать актуальные значения IP-адресов (или FQDN) параметрам:
  - `url: ${urlCheckToken}` - для обслуживания API-запросов по валидации подключений, запрашиваемых «Универсальным диспетчером» через «Шлюз»;
  - `url: ${coordinatorUrl}` - для подключения к RabbitMQ;

- сохранить файл, а затем перезапустить службу:

```
sudo systemctl restart termidesk-gateway
```

После настройки нужно передать каталог `/etc/termidesk/` с первого узла «Шлюза» на другие узлы с этим компонентом:

```
sudo scp -r /etc/termidesk localuser@ipaddr_or_fqdn_host:/home/user/
```

где:

`-r` - ключ для рекурсивной (со вложенными каталогами) передачи;

`localuser` - имя пользователя целевого узла;

`ipaddr_or_fqdn_host` - IP-адрес или FQDN целевого узла;

`/home/user` - путь, куда будет скопирован каталог.

Перед началом установки остальных узлов «Шлюзов» необходимо:

- переместить скопированный ранее каталог `termidesk` в каталог `/etc/`:

```
sudo mv /home/user/termidesk /etc/
```

- назначить права по использованию ключа и сертификата пользователю `termidesk-gateway`:

```
sudo chown termidesk-gateway:termidesk-gateway /etc/termidesk/ssl-cert-snakeoil.*
```

- предоставить права на чтение ключа и сертификата:

```
1  sudo chmod 640 /etc/termidesk/ssl-cert-snakeoil.key
2  sudo chmod 644 /etc/termidesk/ssl-cert-snakeoil.pem
```

- перезапустить службу:

```
sudo systemctl restart termidesk-gateway
```

Установка второго узла «Шлюза» выполняется по аналогии с первым.

#### 3.3.4.5 . Установка «Менеджеров рабочих мест»

Установка «Менеджеров рабочих мест» производится на два узла, работающих в режиме `network failover`.

Установка компонента на первый узел проводится в следующей последовательности:

- перемещается скопированный ранее каталог `termidesk-vdi` в каталог `/etc/opt/`:

```
sudo mv /home/user/termidesk-vdi /etc/opt/
```

- редактируется файл `/etc/opt/termidesk-vdi/termidesk.conf`, параметру `NODE_ROLES` присваивается значение `CELERYMAN`;

- устанавливается пакет `termidesk-vdi`:

```
sudo apt -y install termidesk-vdi
```

где:

`-y` - ключ для пропуска подтверждения установки.

В результате установки пакета `termidesk-vdi` на узле будут запущены службы `termidesk-celery-beat`, `termidesk-celery-worker`.

Установка второго узла с «Менеджером рабочих мест» выполняется по аналогии с первым.

#### 3.3.4.6 . Установка балансировщиков

Балансировщики нагрузки необходимы для балансировки клиентских подключений к «Агрегаторам» и «Шлюзам», равномерного распределения нагрузки на них. Средой функционирования для балансировщиков нагрузки является ОС Astra Linux Special Edition.

Балансировщик nginx устанавливается командой:

```
sudo apt install -y nginx
```

где:

`-y` - ключ для пропуска подтверждения установки.

#### 3.3.4.7 . Действия после распределенной установки

Настройка балансировщика нагрузки приведена в подразделе Настройка балансировщика для работы с самоподписанными сертификатами документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

### 3.4 . Обновление «Агрегатора»

#### 3.4.1 . Комплексное обновление «Агрегатора»

Обновление должно осуществляться операцией установки поверх предыдущей версии. В противном случае, если ранее «Агрегатор» был удален без удаления БД, при повторной установке может возникнуть ряд ошибок.

> ⚠ Если в файлы запуска вручную были внесены какие-либо изменения, то эти изменения при обновлении не сохраняются.

Перед любым обновлением рекомендуется выполнить резервное копирование БД:

```
1  pg_dump -d <наименование БД> -h <IP-адрес_хоста> -p <порт> -U <пользователь> -W
   > <имя_файла_для_сохранения_БД.sql>
```

где:

`-d <наименование БД>` - имя БД. При стандартных настройках используется имя `termidesk`;

`-h <IP-адрес_хоста>` - IP-адрес узла, где расположена БД. Если БД устанавливалась локально, нужно указать `localhost`;

`-p <порт>` - порт для подключения к БД. При стандартных настройках используется `5432`;

`-U <пользователь>` - имя пользователя для подключения. При стандартных настройках используется имя `termidesk`;

`-W` - запрос пароля для подключения к БД. При стандартных настройках при появлении запроса нужно указать `ksedimret`;

`<имя_файла_для_сохранения_БД.sql>` - имя и формат файла (`sql`) для сохранения БД.

Для обновления «Агрегатора» нужно:

- остановить службы:

```
sudo systemctl stop termidesk-vdi termidesk-celery-beat termidesk-celery-worker
```

- подключить репозиторий Termidesk (см. подраздел **Получение пакетов установки**);
- выполнить обновление:

```
sudo apt install -y termidesk-vdi
```

где:

`-y` - ключ для пропуска подтверждения установки;

- в диалогах ввода параметров подключения к СУБД и RabbitMQ нажать экранную кнопку **[OK]**;
- в диалоге выбора ролей нужно нажать экранную кнопку **[OK]**;

Диалоги настройки параметров отображается в том случае, если ранее они не были заданы.

- если совместно с «Агрегатором» на том же узле используется компонент «Шлюз», необходимо выполнить его обновление:

```
sudo apt install -y termidesk-gateway
```

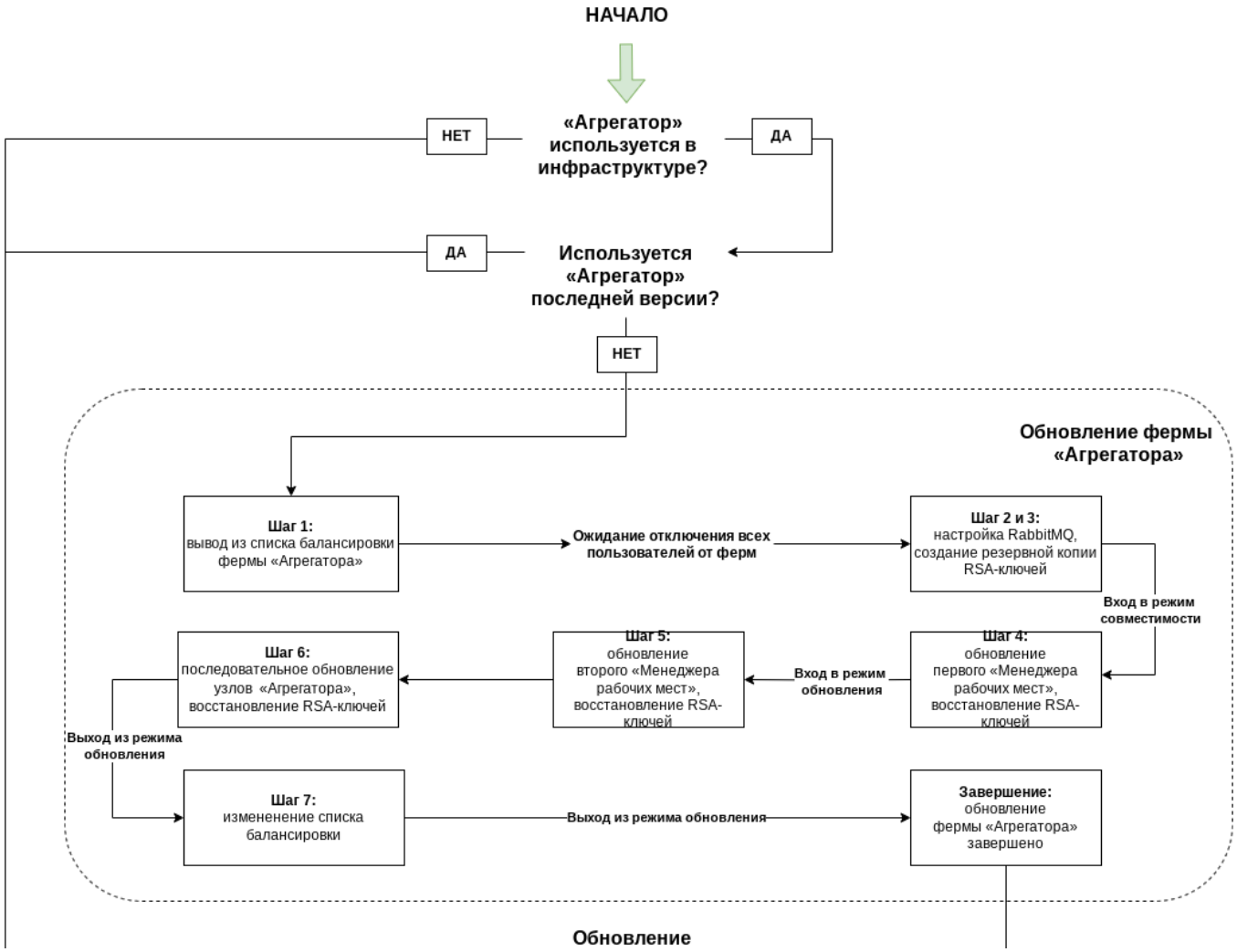
### 3.5 . Обновление для распределенной конфигурации установки «Агрегатора»

#### 3.5.1 . Общая концепция обновления

Описание применимо к ферме «Агрегатора», установленной в распределенной конфигурации. Общая последовательность действий приведена на рисунке (см. Рисунок 3).

Обновление должно осуществляться с соблюдением условий:

- если используется «Агрегатор», то процесс обновления зависит от его версии:
  - если установлен «Агрегатор» самой последней версии, то обновляется ферма поставщиков ресурсов (ферма Termidesk);
  - если установлен «Агрегатор» предыдущей версии, то ферма «Агрегатора» обновляется первой, и только потом обновляется ферма поставщиков ресурсов (ферма Termidesk);
- обновление выполняется последовательно, с установкой промежуточных версий релизов. Например, если сейчас установлена версия 5.1, то порядок обновления до 6.0 будет следующим: 5.1 - 5.1.1 - 6.0;
- обновление выполняется операцией установки поверх предыдущей версии. В противном случае, если ранее «Агрегатор» был удален без удаления БД, при повторной установке может возникнуть ряд ошибок;
- после начала процедуры обновления запрещается производить любые операции с объектами с предыдущими версиями «Агрегатора».



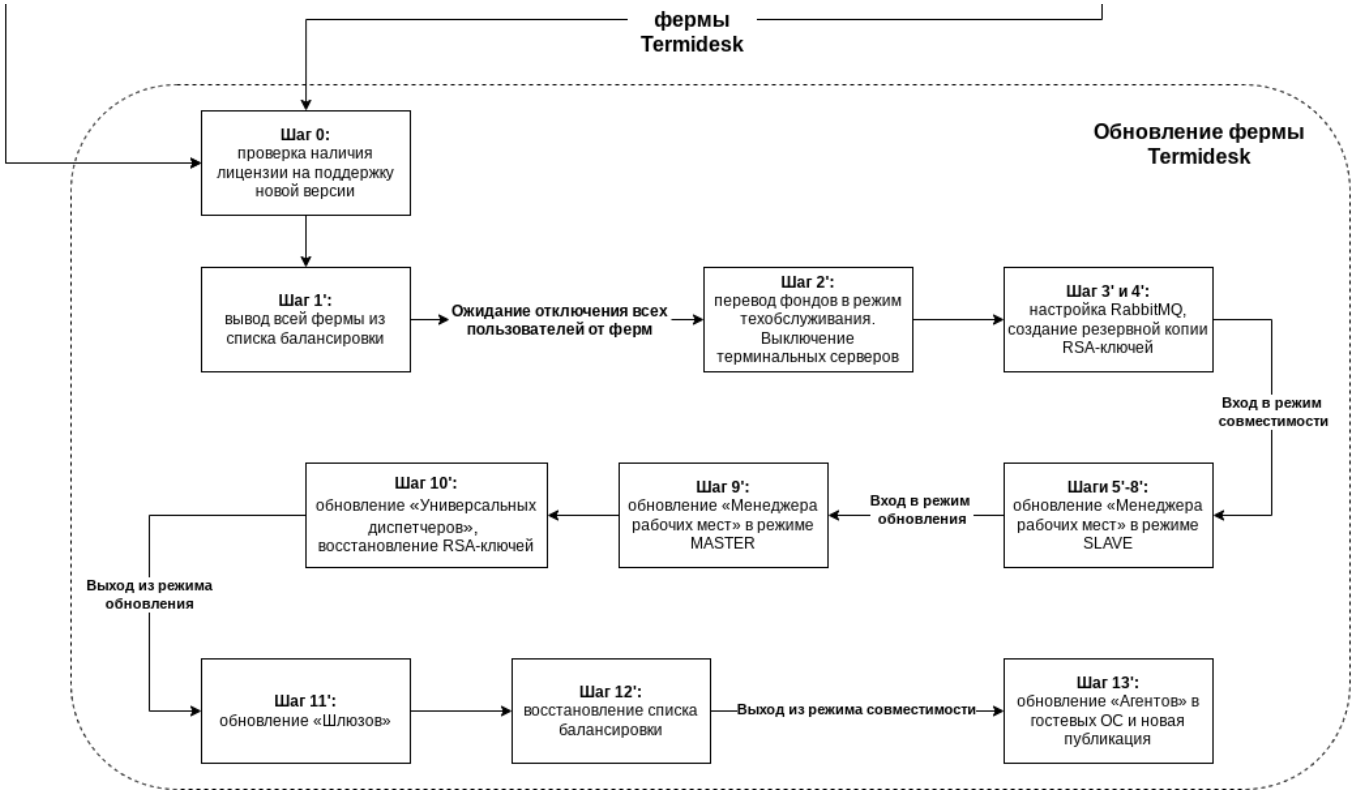



Рисунок 3 – Последовательность обновления распределенной конфигурации

На схеме:

- режим совместимости - режим, характеризующийся отличием в версиях между любыми компонентами фермы «Агрегатора»;
- режим обновления - режим, характеризующийся наличием не обновленных «Агрегаторов» при уже обновленных записях БД.

Последовательность обновления фермы «Агрегатора», установленной в распределенной отказоустойчивой конфигурации:

Шаг 1. На всех балансировщиках нагрузки, отвечающих за распределение подключений к «Агрегаторам», из списка балансировки исключается часть «Агрегаторов».

Шаг 2. На сервер с СУБД, либо на отдельно выделенный сервер, устанавливается и настраивается компонент RabbitMQ в случае, если ранее RabbitMQ не был установлен.

Шаг 3. Создается резервная копия RSA-ключей, расположенных в каталоге `/etc/opt/termidesk-vdi/wsproxy/`.

Шаг 4. Обновляется первый «Менеджер рабочих мест». Запуск служб выполняется автоматически. На обновленном «Менеджере рабочих мест» восстанавливаются RSA-ключи из резервной копии, созданной на **Шаге 3**. В этом процессе автоматически будут обновлены записи в БД.

Шаг 5. Обновляется второй «Менеджер рабочих мест». Запуск служб выполняется автоматически. На обновленном «Менеджере рабочих мест» восстанавливаются RSA-ключи из резервной копии, созданной на **Шаге 3**.

Шаг 6. Последовательно обновляются все узлы «Агрегатора» («Агрегатор администратора», «Агрегатор пользователя», «Агрегатор универсальный»). Запуск служб выполняется автоматически. На обновленных «Агрегаторах» восстанавливаются RSA-ключи из резервных копий, созданных на **Шаге 3**. Узлы перезагружается.

Шаг 7. На всех балансировщиках нагрузки список балансировки восстанавливается до исходного.

После обновления фермы «Агрегатора» выполняется обновление фермы Termidesk.

> ⚠ Описание обновления фермы Termidesk приведено в подразделе **Обновление для распределенной конфигурации установки** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса».

### 3.5.2 . Шаг 1. Редактирование конфигурации балансировщика нагрузки

На балансировщике нагрузки открыть и отредактировать файл `/etc/nginx/sites-available/sampledomain.ru.conf`.

В данном конфигурационном файле следует найти директиву `daas-upstream-nodes` с перечислением списка «Агрегаторов», закомментировать все узлы и сохранить файл.

Пример для списка балансировки:

> ⚠ Здесь и далее примеры IP-адресов приведены в соответствии с RFC 5737. Указанные IP-адреса должны быть заменены на актуальные, используемые согласно схеме адресации, принятой в инфраструктуре организации.

```
upstream daas-upstream-nodes {
 least_conn;
     server 192.0.2.33;
     server 192.0.2.34;
     server 192.0.2.35;
 }
```

Для исключения всех узлов файл приводится к виду:

```
upstream daas-upstream-nodes {
 least_conn;
     # server 192.0.2.33;
     # server 192.0.2.34;
     # server 192.0.2.35;
 }
```

После изменения файла перезапустить веб-сервер:

```
sudo systemctl restart nginx
```

### 3.5.3 . Шаг 2. Установка и настройка RabbitMQ

При отсутствии ранее установленного RabbitMQ выполняется его установка в соответствии с подразделами **Установка брокера сообщений RabbitMQ** и **Настройка брокера сообщений RabbitMQ** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Установка программного комплекса».

> ⚠ Ферма «Агрегатора» не должна использовать экземпляры БД и брокера сообщений RabbitMQ, предназначенные для фермы Termidesk.

### 3.5.4 . Шаг 3. Резервное копирование RSA-ключей

Выполнить резервное копирование RSA-ключей с одного из узлов «Агрегатора». Резервные копии ключей можно скопировать, например, на другой сетевой узел командой:

```
sudo scp -r /etc/opt/termidesk-vdi/wsproxy localuser@ipaddr_or_fqdn_host:/home/localuser/
```

где:

`-r` - ключ для рекурсивной (со вложенными каталогами) передачи;

`localuser` - имя пользователя целевого узла;

`ipaddr_or_fqdn_host` - IP-адрес или FQDN целевого узла;

`/home/user` - путь, куда будет скопирован каталог.

### 3.5.5 . Шаг 4. Обновление первого «Менеджера рабочих мест»

Перед запуском процедуры обновления нужно:

- отредактировать файл `/etc/opt/termidesk-vdi/termidesk.conf` и задать значение для параметра `METRICS_ACCESS_KEY`, если оно не задано;

> ⚠ При редактировании файла `/etc/opt/termidesk-vdi/termidesk.conf` рекомендуется использовать одинаковое значение параметра `METRICS_ACCESS_KEY` для всех «Менеджеров рабочих мест».

- остановить службы Termidesk:

```
sudo systemctl stop termidesk-celery-beat termidesk-celery-worker
```

- удалить кеш файла ответов `debconf` командами:

```
1 sudo rm -f /var/cache/debconf/config.dat
2 sudo rm -f /var/cache/debconf/config.dat-old
```

Для обновления «Менеджера рабочих мест»:

- обновить список пакетов и выполнить запуск файла установщика:

```
sudo apt update
sudo apt install termidesk-vdi
```

- в диалоговом окне псевдографического интерфейса инсталлятора выбирается роль «Менеджер рабочих мест».

После обновления выполнить копирование сохраненных на Шаге 3 (see page 26) RSA-ключей на узел с обновленным «Менеджером рабочих мест».

### 3.5.6 . Шаг 5. Обновление второго «Менеджера рабочих мест»

Обновление производится аналогично **Шагу 4** (see page 26).

### 3.5.7 . Шаг 6. Обновление узлов «Агрегаторов»

Перед запуском процедуры обновления нужно:

- отредактировать файл `/etc/opt/termidesk-vdi/termidesk.conf` и задать значение для параметра `METRICS_ACCESS_KEY`, если оно не задано;

> Корректировка файла `/etc/apache2/apache2.conf` при обновлении не производится.
> При редактировании файла `/etc/opt/termidesk-vdi/termidesk.conf` рекомендуется задать одинаковое значение параметра `METRICS_ACCESS_KEY` для всех узлов «Агрегатора».

- остановить службу Termidesk:

```
sudo systemctl stop termidesk-vdi
```

- удалить кеш файла ответов `debconf` командами:

```
sudo rm -f /var/cache/debconf/config.dat
sudo rm -f /var/cache/debconf/config.dat-old
```

где:

`-f` - ключ игнорирования несуществующих файлов.

Для обновления «Агрегатора»:

- обновить список пакетов и выполнить запуск файла установщика:

```
sudo apt update
sudo apt install termidesk-vdi
```

- в диалоговом окне псевдографического интерфейса инсталлятора выбирается роль «Агрегатор администратора» и/или «Агрегатор пользователя» в зависимости от ранее установленной роли.

После обновления:

- выполнить копирование сохраненных на **Шаге 3** (see page 26) RSA-ключей на узлы с обновленными «Агрегаторами»;
- перезагрузить узлы:

```
sudo reboot
```

После загрузки узла проверить состояние служб:

```
sudo systemctl -a | grep termidesk
```

где:

`-a` - ключ для вывода списка служб;

`grep` - утилита для поиска текста в выводе предыдущей команды.

Проверить доступность веб-порталов «Агрегатора» через веб-браузер.

### 3.5.8 . Шаг 7. Восстановление конфигурации балансировщика нагрузки

По завершении обновления **ВСЕХ** узлов «Агрегатора» список балансировки на **ВСЕХ** балансировщиках восстанавливается до исходного.

Ранее закомментированные строки нужно раскомментировать, затем выполнить перезагрузку службы `nginx` на каждом балансировщике:

```
sudo systemctl restart nginx
```

Выполнить проверку доступности веб-портала «Агрегатора» через веб-браузер сначала обращением на IP-адрес каждого из «Агрегаторов», затем обращением на IP-адрес балансировщика нагрузки.

## 3.6 . Удаление «Агрегатора»

Для удаления нужно:

- выполнить:

```
sudo aptitude purge -y termidesk-vdi
```

где:

`-y` - ключ для пропуска подтверждения удаления;

- очистить оставшиеся зависимости и конфигурации:

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

Команда полностью удалит оставшиеся настройки и зависимости уже удаленных пакетов.

Для удаления БД и роли пользователя следует выполнить следующие действия, строго соблюдая их последовательность:

- переключиться на пользователя `postgres` (через пользователя `root`):

```
sudo su postgres
```

- запустить терминальный клиент СУБД:

```
psql
```

- используя интерактивный интерфейс терминального клиента СУБД, удалить БД:

```
postgres=# DROP DATABASE termidesk;
```

- удалить роль пользователя БД:

```
postgres=# DROP ROLE termidesk;
```

- выйти из интерактивного интерфейса терминального клиента СУБД:

```
postgres=# \q
```

- выйти из сеанса пользователя `postgres`:

```
exit
```

- удалить оставшийся каталог с файлами, содержащими переменные для подключения к БД, сертификат и ключ:

```
sudo rm -R /etc/opt/termidesk-vdi
```

где:

`-R` - ключ для рекурсивного действия. Будут удалены все вложенные подкаталоги.

# 4 . ГРАФИЧЕСКИЙ ИНТЕРФЕЙС

## 4.1 . Доступ к веб-интерфейсу

Доступ веб-интерфейсу осуществляется из веб-браузера по протоколу HTTPS с указанием URL-адреса подключения.
Для подключения должны использоваться веб-браузеры с поддержкой спецификации W3C HTML5: Яндекс.Браузер версии 15.9 и выше, Google Chrome версии 46 и выше, Mozilla Firefox версии 41 и выше.
Минимально необходимое разрешение экрана монитора для работы с веб-интерфейсом - 1366x768 пикселей.

При наличии только домена аутентификации с типом «Встроенный» на странице подключения нужно заполнить экранные поля:

- «Логин» – идентификатор субъекта с ролью «Администратор»;
- «Пароль» – набор символов, подтверждающий назначение полномочий.

При последующих сеансах входа после добавления нового домена аутентификации добавится дополнительное экранное поле для выбора:

- «Домен аутентификации» – источник сведений о субъектах и их полномочиях.

## 4.2 . Типы веб-интерфейса

В «Агрегаторе» определены следующие типы веб-интерфейса:

- «Агрегатор администратора» - предоставляет интерфейс для управления объединенными ресурсами (фермами) Termidesk;
- «Агрегатор пользователя» - предоставляет пользовательский интерфейс «Агрегатора» без функций управления;
- «Агрегатор универсальный» - предоставляет функции обоих вариантов - «Агрегатор администратора» и «Агрегатор пользователя».

Доступный тип веб-интерфейса определяется на этапе установки.

## 4.3 . Основные функции веб-интерфейса

### 4.3.1 . Функция «Обзор»

При нажатии в левой части веб-интерфейса на функцию «Обзор» визуализируется краткое представление состояния основных параметров.
В графических блоках функции «Обзор» представлены следующие элементы (см. Рисунок 4):

- «Фермы поставщиков ресурсов» - суммарное число и состояние ферм поставщиков ресурсов, добавленных на «Агрегатор»;

- «Сайты» - суммарное число и состояние сайтов, созданных на «Агрегаторе»;
- «Узлы» - суммарное число и состояние узлов ферм поставщиков ресурсов, добавленных на «Агрегатор»;
- «База данных» - состояние БД, к которой подключен «Агрегатор»;
- «Rabbit MQ» - состояние брокера сообщений, к которому подключен «Агрегатор».

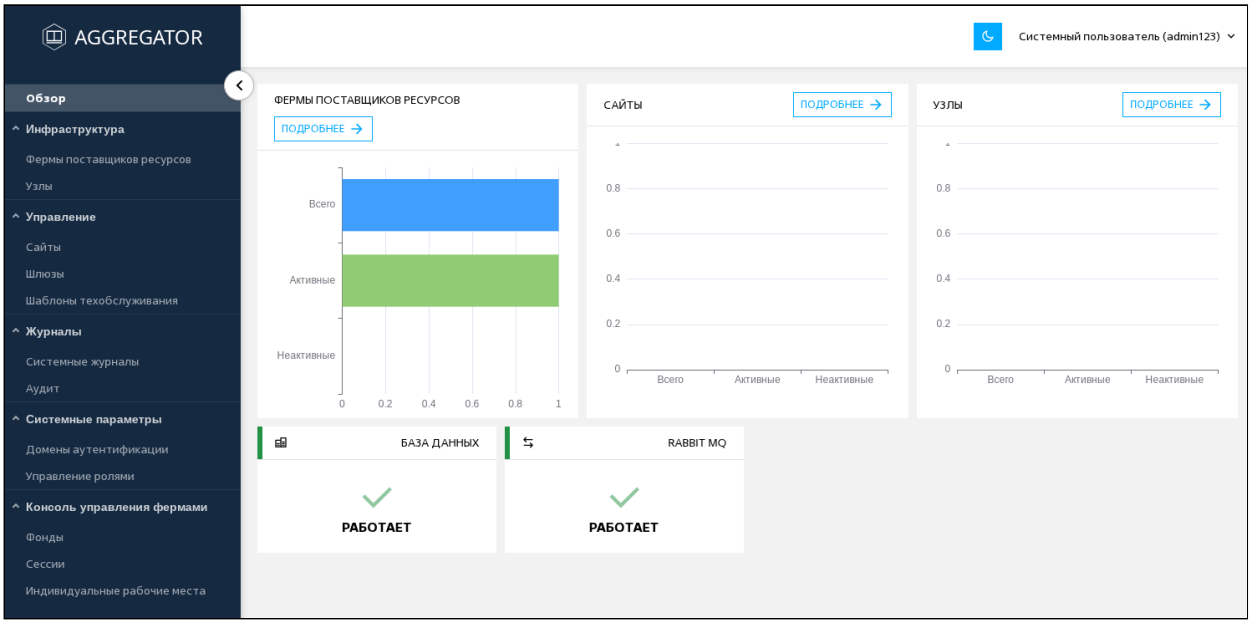



Рисунок 4 – Окно функции «Обзор» в графическом интерфейсе управления «Агрегатора»

### 4.3.2 . Функция «Инфраструктура»

При нажатии в левой части веб-интерфейса на функцию «Инфраструктура» открывается список, содержащий процедуры для настройки взаимодействия «Агрегатора» с фермами поставщиков ресурсов.

Функция «Инфраструктура» представлена следующими процедурами:

- «Фермы поставщиков ресурсов» - определяет настройку взаимодействия с фермами поставщиков ресурсов;
- «Узлы» - предоставляет список добавленных в ферму поставщиков ресурсов объектов типа «Узел».

### 4.3.3 . Функция «Управление»

При нажатии в левой части веб-интерфейса на функцию «Управление» открывается список, содержащий процедуры для формирования эргономичного представления списка ресурсов и дополнительной настройки взаимодействия «Агрегатора» с фермами поставщиков ресурсов.

Функция «Управление» представлена следующими процедурами:

- «Сайты» - определяет настройку размещения объединенных ресурсов для пользователей;

- «Шлюзы» - определяет настройку взаимодействия пользователей с ресурсами, предоставляемыми «Агрегатором», через компонент «Шлюз»;
- «Шаблоны тех. обслуживания» - определяет настройку текстов сообщений, отправляемых пользователю при попытке подключиться к сайту, находящемуся в режиме техобслуживания.

#### 4.3.4 . Функция «Журналы»

При нажатии в левой части веб-интерфейса на функцию «Журналы» открывается список процедур для просмотра событий субъектов доступа, а также событий функционирования «Агрегатора».

Функция «Журналы» представлена следующими процедурами:

- «Журналы» - позволяет просматривать события функционирования «Агрегатора»;
- «Аудит» - позволяет просматривать события аудита из веб-интерфейса «Агрегатора».

#### 4.3.5 . Функция «Системные параметры»

При нажатии в левой части веб-интерфейса на функцию «Системные параметры» открывается список процедур для настройки «Агрегатора».

Функция «Системные параметры» представлена следующими процедурами:

- «Домены аутентификации» - определяет настройку взаимодействия с источниками сведений о субъектах и их полномочиях;
- «Управление ролями» - определяет назначение служебных функций администраторам «Агрегатора».

#### 4.3.6 . Функция «Консоль управления фермами»

При нажатии в левой части веб-интерфейса на функцию «Консоль управления фермами» открывается список процедур для управления фондами, сессиями пользователей и рабочими местами, размещенными в фермах поставщиков ресурсов.

Функция «Консоль управления фермами» представлена следующими процедурами:

- «Фонды» - позволяет управлять фондами, размещенными в фермах поставщиков ресурсов;
- «Сессии» - позволяет управлять сессиями подключенных к фондам пользователей;
- «Индивидуальные рабочие места» - позволяет управлять рабочими местами фондов.

# 5 . НАСТРОЙКА АГРЕГАЦИИ РЕСУРСОВ

## 5.1 . Последовательность шагов для настройки агрегации ресурсов

Общая последовательность шагов выглядит следующим образом:

- подготовка сетевой инфраструктуры в соответствии с требованиями раздела **Требования к настройкам инфраструктуры**;
- установка «Агрегатора» в соответствии с подразделами **Подготовка среды функционирования** и **Установка Агрегатора**;
- переход в веб-портал «Агрегатор администратора»;
- добавление домена аутентификации в соответствии с подразделом **Домены аутентификации**;
- добавление групп домена аутентификации в соответствии с подразделом **Действия над группами в домене аутентификации**;
- добавление ферм поставщиков ресурсов в соответствии с подразделом **Добавление фермы поставщика ресурсов**;
- добавление узлов в соответствии с подразделом **Добавление узла Termidesk**;
- создание сайта в соответствии с подразделом **Добавление сайта**;
- создание объединенного набора ресурсов в соответствии с подразделом **Добавление объединенного набора ресурсов**.

После этого пользователю станет доступно подключение к «Агрегатору» через компонент «Клиент» для получения объединенного набора ресурсов.

# 6 . ДОМЕНЫ АУТЕНТИФИКАЦИИ

## 6.1 . Общие сведения о доменах аутентификации

Домен аутентификации - источник сведений о субъектах и их полномочиях.

> ⚠ Следует предусмотреть, что в целях безопасности учетная запись для биндинга (подключения) к домену не должна иметь прав на удаление или изменение объекта типа «пользователь».

Для отображения списка доменов аутентификации следует перейти «Системные параметры - Домены аутентификации». Основные параметры списка приведены в таблице (см. Таблица 2).

Таблица 2 – Параметры списка доменов аутентификации

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование домена аутентификации |
| «Приоритет» | Приоритет отображения в списке доменов аутентификации |
| «Название в системе» | Тип домена аутентификации |
| «Пользователи» | Количество пользователей домена аутентификации |
| «Комментарии» | Информационное сообщение, используемое для описания назначения протокола доставки |

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца.
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Для добавления домена аутентификации в веб-портале «Агрегатор администратора» следует перейти «Системные параметры - Домены аутентификации», затем нажать экранную кнопку **[Создать]**. Каждый домен аутентификации описывается перечнем параметров, требуемых для получения идентификаторов субъектов и информации о полномочиях.

Созданный домен аутентификации можно:

- редактировать, для этого нужно пометить домен аутентификации и нажать на экранную кнопку **[Изменить]**;
- удалить, для этого нужно пометить домен аутентификации и нажать на экранную кнопку **[Удалить]**.

### 6.1.1 . Добавление аутентификации через MS AD (LDAP)

### 6.1.2 . Перечень параметров для добавления домена аутентификации MS AD (LDAP)

Для добавления домена аутентификации следует перейти «Системные параметры - Домены аутентификации», а затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «MS Active Directory (LDAP)». Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 3). Для проверки и сохранения параметров конфигурации нужно нажать экранную кнопку **[Тест]**, затем **[Создать]**.

Таблица 3 – Данные для добавления аутентификации MS AD

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование домена аутентификации |
| «Комментарий» | Информационное сообщение, используемое для описания назначения домена аутентификации |
| «Приоритет» | Преимущество использования домена аутентификации при проверке субъекта и его полномочий |
| «Метка» | Информационное поле, используемое для идентификации объекта во внутренней структуре данных.<br>Параметр используется для поиска аналогичного домена «Универсального диспетчера», поэтому должен быть одинаковым как на портале «Агрегатор» (при его использовании), так и на «Универсальном диспетчере».<br>Поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание) |
| «Субъекты» | Выбор субъектов, для которых будет доступен домен аутентификации.<br>Возможные значения:<br>▪ «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»;<br>▪ «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»;<br>▪ «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»;<br>▪ «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала |
| «Сервер LDAP» | IP-адрес или доменное имя сервера службы каталогов, являющегося источником сведений о субъектах и их полномочиях |

| Параметр | Описание |
|---|---|
| «Порт» | TCP-порт, на котором запущена служба каталогов.<br>Возможные стандартные значения:<br>▪ «389» (по умолчанию). Используется, если доступ к службе каталогов осуществляется по протоколу LDAP;<br>▪ «636». Используется, если доступ к службе каталогов осуществляется по протоколу LDAPS;<br>▪ «3268». Альтернативный порт. Используется, если доступ к службе каталогов осуществляется по протоколу LDAP;<br>▪ «3269». Альтернативный порт. Используется, если доступ к службе каталогов осуществляется по протоколу LDAPS.<br>Для ускорения поиска пользователей в службе каталогов рекомендуется указывать альтернативный порт |
| «Использовать SSL» | Использовать защищенное соединение при взаимодействии со службой каталогов |
| «Путь к секретам» | Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «hvac».<br>Путь к аутентификационным данным учетной записи, расположенным в хранилище. Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**.<br>Пример: «hvac-kv://secret#termidesk-admin/msad/» |
| «Учетная запись» | Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config».<br>Учетная запись в формате Distinguished Name (DN) в домене MS AD (LDAP), используемая для подключения к службе каталогов.<br>Пример: «CN=admin,OU=user,DC=test,DC=desk» |
| «Пароль учетной записи» | Параметр доступен, если на этапе установки Termidesk был выбран способ хранения паролей «config».<br>Набор символов, подтверждающий полномочия объекта для подключения к службе каталогов |
| «Таймаут» | Время ожидания (в секундах) ответа от службы каталогов.<br>Значение по умолчанию: «10» |
| «Base DN» | Корень поиска в службе каталогов в формате DN. Параметру следует задавать значение, соответствующее записи верхнего уровня в иерархии службы каталогов (без указания OU).<br>Вводимое значение не должно содержать пробелов:<br>▪ в начале и конце строки;<br>▪ рядом с разделителями (запятыми);<br>▪ в элементах пути (например, «DC=company name,DC=de»).<br>Пример: «DC=test,DC=desk» |
| «Имя класса пользователя» | Атрибут класса пользователя в службе каталогов.<br>Для корректного заполнения данного поля необходимо указать значение «person» |

| Параметр | Описание |
|---|---|
| «Атрибут идентификатора пользователя» | Атрибут уникального имени или идентификатора пользователя в службе каталогов.<br>Для корректного заполнения данного поля необходимо указать:<br>▪ значение «name», если активирован параметр «Использовать PKINIT»;<br>Атрибут идентификатора пользователя задается с учетом того, какой шаблон использовался при выдаче сертификата пользователя. Например, значение «name» для механизма аутентификации Kerberos PKINIT указывается в том случае, если сертификат для подключения выдан на имя пользователя.<br>▪ значение «userPrincipalName», если в параметре «Формат имени пользователя для аутентификации» используется «userPrincipalName»;<br>▪ значение «SamAccountName» в остальных случаях |
| «Список атрибутов пользователя» | Список атрибутов, содержащий уникальные данные пользователя, разделенные запятыми.<br>Для корректного заполнения данного поля необходимо указать значение:<br>▪ «userPrincipalName», если в параметре «Формат имени пользователя для аутентификации» используется «userPrincipalName»;<br>▪ «name», если в параметре «Формат имени пользователя для аутентификации» используется «sAMAccountName» |
| «Формат имени пользователя для аутентификации» | Формат имени пользователя, заданный в службе каталогов.<br>Если на пользовательской рабочей станции установлен компонент «Клиент» версии, младше 6.0, то он будет поддерживать только формат «sAMAccountName».<br>Возможные значения:<br>▪ «sAMAccountName» (по умолчанию) - имя пользователя без доменной части;<br>▪ «userPrincipalName» - имя пользователя с доменной частью |
| «Имя атрибута группы» | Атрибут принадлежности к группе в службе каталогов.<br>Для корректного заполнения данного поля необходимо указать значение «group» |
| «Атрибут имени группы» | Атрибут идентификатора группы, к которой относится субъект в службе каталогов.<br>Для корректного заполнения данного поля необходимо указать:<br>▪ значение «distinguishedname», если включены параметры «Использовать рекурсивный поиск групп» или «Использовать обратный порядок проверки членства пользователей»;<br>▪ значение «name», если активирован параметр «Использовать PKINIT»;<br>Атрибут имени группы задается с учетом того, какой шаблон использовался при выдаче сертификата пользователя. Например, значение «name» для механизма аутентификации Kerberos PKINIT указывается в том случае, если сертификат для подключения выдан на имя пользователя.<br>▪ значение «cn» в остальных случаях.<br>Если используется значение «distinguishedname», то при добавлении группы в домен аутентификации по пути «Компоненты - Домены аутентификации - Наименование домена - Группы» нужно указывать длинные имена групп, например: «CN=RootGroup,CN=Users,DC=test,DC=desk». Если используется значение «cn», то нужно указывать короткие имена групп.<br>Если параметр «Атрибут имени группы» был изменен, то необходимо заново добавить группы, используя соответствующие имена групп: для «cn» - короткие имена, для «distinguishedname» - длинные имена |
| «Атрибут членства в группе» | Идентификатор группы для назначения полномочий субъекту.<br>Для корректного заполнения данного поля необходимо указать значение «member» |

| Параметр | Описание |
|---|---|
| «Атрибут групп для LDAP-запросов» | Атрибут, определяющий группы пользователя при запросах к службе каталогов.<br>Возможные значения: «objectClass», «objectCategory» |
| «Использовать рекурсивный поиск групп» | При запросе групп пользователя будут учтены его родительские группы, в которых он состоит неявно.<br>Если дополнительно включен параметр «Использовать обратный порядок проверки членства пользователей», то параметр «Использовать рекурсивный поиск групп» можно не включать.<br>Возможные значения:<br>▪ «Да» - использовать рекурсивный поиск;<br>▪ «Нет» (по умолчанию) - не использовать рекурсивный поиск |
| «Использовать обратный порядок проверки членства пользователей» | Проверка соответствия членства пользователя в группах службы каталогов членству в группах домена аутентификации. Для работы функционала необходимо, чтобы был задан параметр «Атрибут имени группы».<br>Этот параметр нужно включить при большом количестве групп непосредственно на службе каталогов MS AD. В этом случае сначала будет проверяться вхождение пользователя в группы домена аутентификации (в том числе рекурсивно), затем будет происходить проверка найденных групп в службе каталогов MS AD.<br>При выключении этого параметра применяется настройка выбора «Атрибут групп для LDAP-запросов»: «objectClass» или «objectCategory».<br>При включении этого параметра всегда применяется настройка выбора «Атрибут групп для LDAP-запросов»: «objectClass».<br>Возможные значения:<br>▪ «Да» - использовать обратный порядок;<br>▪ «Нет» (по умолчанию) - не использовать обратный порядок |
| «Использовать PKINIT» | Использовать механизм аутентификации Kerberos PKINIT при аутентификации пользователя. PKINIT - механизм, позволяющий использовать сертификаты X.509 в качестве метода аутентификации.<br>Предполагается, что механизм аутентификации Kerberos PKINIT настроен в инфраструктуре организации и пользователю выданы соответствующие сертификаты и ключи для подключения (персональный сертификат, закрытый ключ к нему и корневой сертификат ЦС, на котором выпущен персональный сертификат).<br>При активации механизма аутентификации Kerberos PKINIT нужно указать актуальный порт в параметре «Порт PKINIT», а также указать нужные значения параметров «Атрибут имени группы» и «Атрибут идентификатора пользователя».<br>Возможные значения:<br>▪ «Да» - использовать механизм;<br>▪ «Нет» (по умолчанию) - не использовать механизм |
| «Порт PKINIT» | TCP/UDP порт, на котором запущена служба Kerberos.<br>Значение по умолчанию: «88» |
| «Использовать Kerberos» | Использовать механизм аутентификации по билету Kerberos.<br>Предполагается, что механизм аутентификации по билету Kerberos настроен в инфраструктуре организации (см. подразделы **Получение и добавление файла keytab для Kerberos-аутентификации** и **Настройка пользовательской рабочей станции для Kerberos-аутентификации**).<br>Для работы аутентификации по билету Kerberos на терминальных серверах MS RDS, необходимо выполнить дополнительную настройку «Сессионного агента», задав значения параметрам `MASTER_KEY` и `URL_BALANCER` в его конфигурационном файле.<br>Если используется аутентификация Kerberos, то нужно заполнить параметр «Путь до Keytab».<br>Возможные значения:<br>▪ «Да» - использовать механизм;<br>▪ «Нет» (по умолчанию) - не использовать механизм |

| Параметр | Описание |
|---|---|
| «Путь до Keytab» | Путь к файлу с ключами для сервисного аккаунта.<br>В зависимости от места хранения файла следует указать путь в формате:<br>▪ в случае стандартного хранения файла: «/etc/opt/termidesk-vdi/termidesk.keytab»;<br>▪ в случае хранения файла в хранилище hvac: «hvac-kv://secret#termidesk-admin/keytabs/kerberos». Формат задания пути приведен в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»**.<br>Если используется хранилище, то сгенерированный на контроллере домена `keytab`-файл должен быть преобразован к формату BASE64. |

### 6.1.3 . Получение и добавление файла keytab для Kerberos-аутентификации

Для получения `keytab`-файла на контроллере домена MS AD нужно:

- заранее создать учетную запись (сервисный аккаунт), от имени которой будет работать служба. Для создания учетной записи нужно на контроллере домена перейти в стандартную утилиту «Active Directory - пользователи и компьютеры»;
- в свойствах учетной записи во вкладке «Account» активировать параметр «This account supports Kerberos AES 256 bit encryption» (см. Рисунок 5);

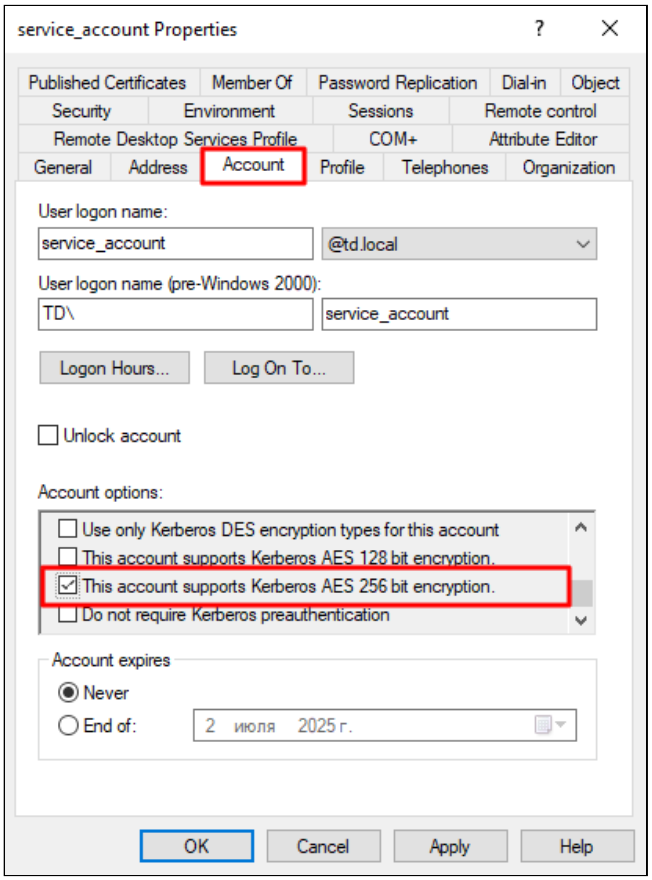



Рисунок 5 – Активация параметра «This account supports Kerberos AES 256 bit encryption»

- открыть интерфейс командной строки PowerShell и выполнить команду добавления службы для сервисного аккаунта:

```
setspn -A HTTP/disp.termidesk.local service_account
```

где:

`service_account` - наименование сервисного аккаунта;

- для просмотра списка служб сервисного аккаунта можно воспользоваться командой:

```
setspn -L service_account
```

- создать файл `termidesk-msad.keytab` для сервисного аккаунта:

```
ktpass -princ HTTP/disp.termidesk.local@TERMIDESK.LOCAL -mapuser
service_account@TERMIDESK.LOCAL -pass <пароль_сервисного_аккаунта> -ptype
KRB5_NT_PRINCIPAL -out termidesk-msad.keytab -crypto AES256-SHA1
```

где:

`HTTP/disp.termidesk.local` - указание ранее созданного субъекта-службы;

`service_account@TERMIDESK.LOCAL` - наименование сервисного аккаунта;

`-out termidesk-msad.keytab` - сохранение в файл `termidesk-msad.keytab`;

`-crypto AES256-SHA1` - алгоритм для преобразования `keytab`-файла.

⚠ Алгоритм преобразования `keytab`-файла следует выбирать согласно установленным политикам безопасности MS AD.

Полученный файл `termidesk-msad.keytab` следует передать на соответствующий узел для хранения. Файл может быть сохранен в файловой системе узла Termidesk или в хранилище OpenBao.

Для передачи файла на целевой узел нужно выполнить команду:

```
scp C:\Windows\System32\termidesk-msad.keytab localuser@192.0.2.30:termidesk-msad.keytab
```

где:

`C:\Windows\System32\termidesk-msad.keytab` - путь к `keytab`-файлу;

`localuser` - имя пользователя целевого узла;

`192.0.2.30` - IP-адрес целевого узла.

После передачи файла необходимо выполнить ряд действий в зависимости от выбранного хранилища.

При хранении файла в файловой системе узла Termidesk:

- переместить файл `termidesk-msad.keytab` в каталог `/etc/opt/termidesk-vdi`:

```
sudo mv /home/user/termidesk-msad.keytab /etc/opt/termidesk-vdi/
```

- сделать владельцем этого файла пользователя `termidesk`:

```
sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/termidesk-msad.keytab
```

- перезапустить службу `termidesk-vdi`:

```
sudo systemctl restart termidesk-vdi
```

При хранении файла в хранилище OpenBao:

- запустить интерпретатор Python:

```
sudo python3
```

- перевести файл в формат base64:

```
import base64 with open('/home/user/termidesk-msad.keytab', 'rb') as file:
keytab_bytes = file.read() keytab_base64 =
base64.b64encode(keytab_bytes).decode('utf-8') keytab_base64
```

где:

`/home/user/termidesk-msad.keytab` - путь к `keytab`-файлу;

- сохранить результат выполнения команды в хранилище OpenBao:

```
bao kv put secret/termidesk/ldap keytab='BQIAAABGAAIAC1VTVVA0MDcuTEFOAARIVFRQABJ0ZXJtaWRlc
2subXlkb21h aW4AAAABAAAAAAUAFwAQhKQHwhUvWGEJk92QgI/tNA=='
```

где:

`termidesk` - значение переменной `SECRETS_OPENBAO_TERMIDESK_PATH`, заданной в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf`;

`ldap` - путь к хранилищу OpenBao, где следует сохранить результат выполнения команды.

### 6.1.4 . Настройка пользовательской рабочей станции для Kerberos-аутентификации

Для корректной аутентификации пользовательская рабочая станция должна быть введена в соответствующий домен аутентификации Kerberos, используемый в ферме Termidesk и указанный в «Агрегаторе администратора».

По умолчанию билет Kerberos выдается автоматически при аутентификации пользователя в системе. Однако, если билет не был выдан автоматически, нужно:

- просмотреть список билетов:

```
klist
```

- получить билет Kerberos:

```
kinit -f termidesk@TERMIDESK.LOCAL
```

где:

`termidesk@TERMIDESK.LOCAL` - учетная запись, для которой запрашивается билет.

Kerberos-аутентификация через веб-браузер требует настройки параметров безопасности в зависимости от используемой ОС и типа браузера.

На пользовательской рабочей станции с ОС Microsoft Windows:

- при использовании веб-браузера, основанного на Chromium нужно настроить параметры безопасности браузера для зоны, в которой находится сервер Termidesk. Для этого:
  - перейти «Панель управления - Свойства браузера - Безопасность»;
  - в разделе «Выберите зону для параметры ее параметров безопасности» выбрать зону «Местная интрасеть», нажать экранную кнопку **[Сайты]**;
  - в окне «Местная интрасеть» нажать экранную кнопку **[Дополнительно]**;
  - в поле «Добавить в зону следующий узел» ввести FQDN сервера Termidesk, нажать экранную кнопку [Добавить] (см. Рисунок 6);

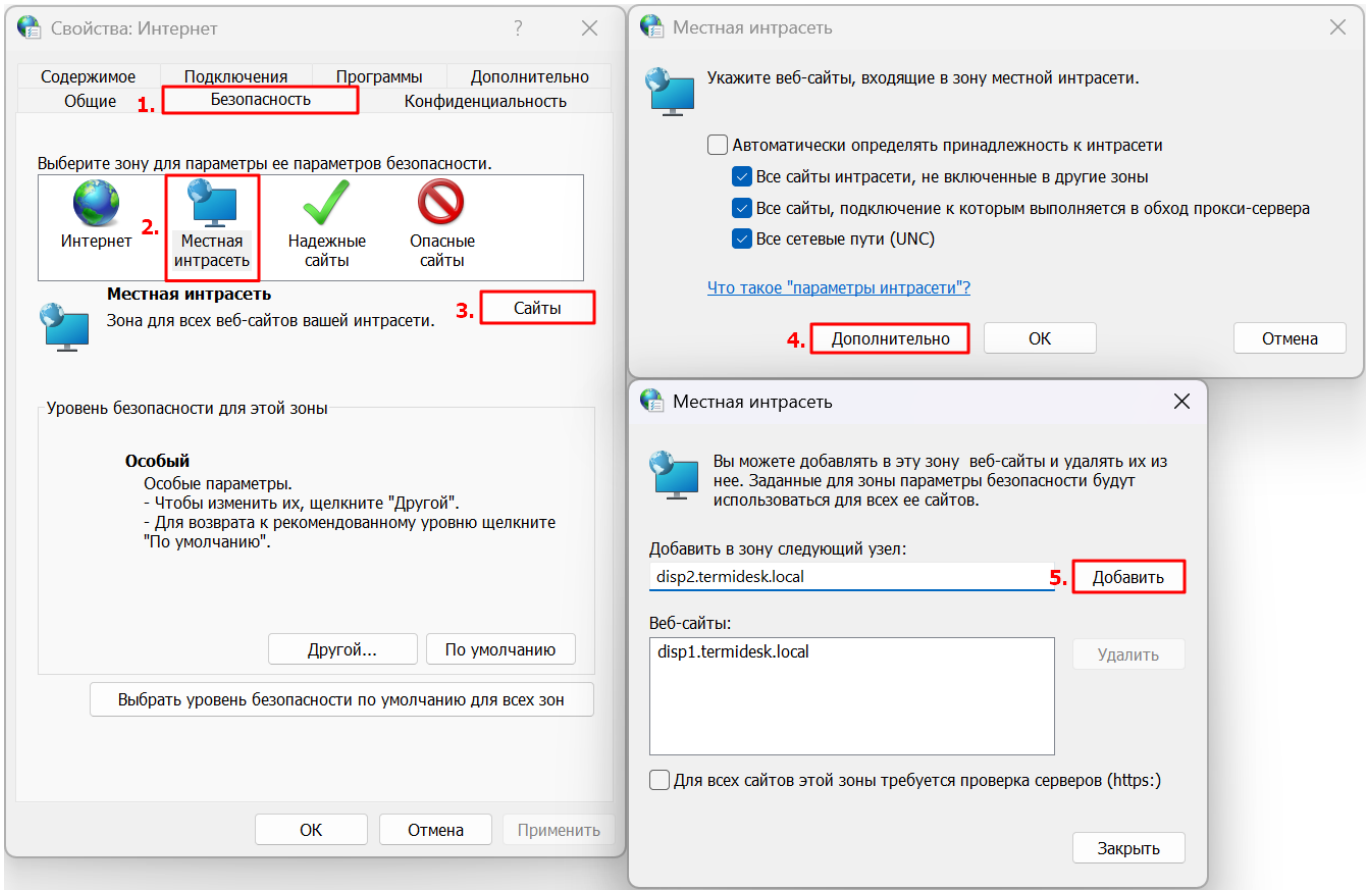



Рисунок 6 – Добавление FQDN компонента «Универсальный диспетчер» в зону «Местная интрасеть»

- при использовании в ОС Microsoft Windows веб-браузера Mozilla Firefox нужно:

- в адресной строке ввести `about:config`;
- присвоить соответствующие значения параметрам, перечисленным в таблице (см. Таблица 4).

Таблица 4 – Данные для настройки Kerberos-аутентификации через веб-браузер Mozilla Firefox в ОС Microsoft Windows

| Параметр | Значение |
|---|---|
| `network.negotiate-auth.allow-proxies` | `True` |
| `network.negotiate-auth.delegation-uris` | `.termidesk.local` |
| `network.negotiate-auth.trusted-uris` | `.termidesk.local` |

На пользовательской рабочей станции с ОС Astra Linux Special Edition:

- для настройки веб-браузера Chromium нужно:
  - в файл `/etc/chromium/policies/managed/policies.json` добавить строки:

```
{
    "AuthServerAllowlist": "*.termidesk.local" ,
    "AuthNegotiateDelegateAllowlist": "*.termidesk.local"
}
```

где:

`*.termidesk.local` - имя домена, для которого применяется Kerberos-аутентификация;

- для настройки веб-браузера Яндекс.Браузер нужно:
  - создать каталог `/etc/opt/yandex/browser/policies/managed`:

```
mkdir -p /etc/opt/yandex/browser/policies/managed
```

  - создать файл `/etc/opt/yandex/browser/policies/managed/policies.json` следующего содержания:

```
{
    "AuthServerAllowlist": "*.termidesk.local",
    "AuthNegotiateDelegateAllowlist": "*.termidesk.local"
}
```

- для настройки веб-браузера Mozilla Firefox нужно:
  - в адресной строке ввести `about:config`;
  - присвоить соответствующие значения параметрам, перечисленным в таблице (см. Таблица 5).

Таблица 5 – Данные для настройки Kerberos-аутентификации через веб-браузер Mozilla Firefox в ОС Astra Linux Special Edition

| Параметр | Значение |
|---|---|
| `network.negotiate-auth.allow-proxies` | `True` |
| `network.negotiate-auth.delegation-uris` | `.termidesk.local` |
| `network.negotiate-auth.trusted-uris` | `.termidesk.local` |

## 6.2 . Добавление домена аутентификации OIDC

OpenID Connect (OIDC) - это механизм, позволяющий приложению связаться со службой идентификации (Identity provider, IdP), получить данные о пользователе и вернуть их обратно в приложение. Таким образом OIDC обеспечивает аутентификацию администраторов и пользователей без необходимости ввода логина и пароля.

Служба идентификации IdP (например, keycloak) должна быть предварительно настроена в инфраструктуре организации для возможности использования OIDC как домена аутентификации.

Поддерживаются следующие типы аутентификации:

- по идентификатору и секрету. В этом случае используются параметры «Client ID» и «Client Secret», заданные в службе идентификации IdP;
- по подписанному JWT-токену. В этом случае используются параметры «Client ID» и «Signed Jwt», заданные в службе идентификации IdP. Закрытый ключ, использующийся для подписи JWT-токена, должен быть загружен на узлы Агрегатора («Агрегатор администратора», «Агрегатор пользователя»).

Для добавления домена аутентификации следует перейти «Системные параметры - Домены аутентификации», а затем нажать экранную кнопку **[Создать]** и выбрать из выпадающего списка «OIDC аутентификация». Далее заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 6). Для сохранения параметров конфигурации нужно использовать экранную кнопку **[Создать]**.

Таблица 6 – Данные для добавления аутентификации через OIDC

| Параметр | Описание |
|---|---|
| «Название» | Параметр обязателен для заполнения.<br>Текстовое наименование домена аутентификации |
| «Комментарий» | Информационное сообщение, используемое для описания назначения источника сведений о субъектах и их полномочиях |
| «Приоритет» | Приоритет использования домена аутентификации при проверке субъекта и его полномочий |

| Параметр | Описание |
|---|---|
| «Метка» | Параметр обязателен для заполнения.<br>Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk.<br>Начиная с Termidesk версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание) |
| «Субъекты» | Параметр обязателен для заполнения.<br>Выбор субъектов, для которых будет доступен домен аутентификации.<br>Возможные значения:<br>▪ «Все» - домен аутентификации будет доступен как для пользователей, так и для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале администратора», «Портале пользователя», «Портале универсальном», и при подключении из компонента «Клиент»;<br>▪ «Администраторы и персонал» - домен аутентификации будет доступен только для администраторов и персонала. Такое значение выбирается, если домен аутентификации должен быть доступен только на «Портале администратора» или «Портале универсальном»;<br>▪ «Пользователи» - домен аутентификации будет доступен только для пользователей. Такое значение выбирается, если домен аутентификации должен быть доступен на «Портале пользователя», «Портале универсальном» или при подключении пользователя из компонента «Клиент»;<br>▪ «Система» - домен аутентификации не будет доступен ни для пользователей, ни для администраторов и персонала |
| «Client ID» | Уникальный идентификатор приложения, полученный от службы идентификации IdP.<br>Пример: «openid-test-cl» |
| «Client secret» | Ключ приложения, полученный от службы идентификации IdP.<br>Параметр должен быть пустым, если задан параметр «Приватный Ключ» |
| «Authorization endpoint» | Параметр обязателен для заполнения.<br>URL-адрес авторизации службы идентификации IdP.<br>Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/auth» |
| «Token endpoint» | Параметр обязателен для заполнения.<br>URL-адрес получения токена службы идентификации IdP.<br>Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/token» |
| «Userinfo endpoint» | Параметр обязателен для заполнения.<br>URL-адрес получения информации о пользователе от службы идентификации IdP.<br>Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/userinfo» |

| Параметр | Описание |
|---|---|
| «JWKS URI» | URL-адрес получения сертификатов службы идентификации IdP.<br>Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/certs» |
| «Logout URL» | Параметр обязателен для заполнения.<br>URL-адрес получения информации о завершении сессии пользователя от службы идентификации IdP.<br>Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/logout» |
| «Scope» | Набор областей действия, поддерживаемый в службе идентификации IdP.<br>Области действия определяются спецификацией протокола OAuth 2.0.<br>Неполный список возможных значений (указываются через пробел):<br>▪ «openid» (обязательное значение для OIDC) - запуск аутентификации с использованием OIDC;<br>▪ «profile» - доступ к профилю пользователя;<br>▪ «email» - доступ к адресу электронной почты пользователя;<br>▪ «offline_access» - обновление токена доступа без необходимости повторной аутентификации;<br>▪ «groups» - доступ к списку ролей пользователя.<br>Значение по умолчанию: «openid email profile groups».<br>Если нужно указать другой набор значений, следует убедиться, что он поддерживается используемой службой идентификации IdP |
| «Имя пользователя» | Имя атрибута, в котором хранится имя пользователя (логин) в службе идентификации IdP.<br>Значение по умолчанию: «email» |
| «Проверка SSL» | Проверка использования SSL |

### 6.3 . Действия над группами в домене аутентификации

Группы - перечень объектов домена аутентификации, определяющих разрешения пользователей на доступ к фондам РМ. Перечень групп, доступных для добавления, запрашивается «Агрегатором» у домена аутентификации.

Доступны следующие действия над группами домена аутентификации:

- добавление существующей в службе каталогов группы;
- редактирование;
- удаление;
- просмотр сведений таблицы «Группы».

Редактирование и удаление групп в домене аутентификации в веб-портале «Агрегатор администратора» не приводит к каким-либо изменениям объекта в службе каталогов.

Для просмотра списка групп следует перейти «Системные параметры - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне перейти во вкладку «Группы».

Основные параметры списка приведены в таблице (см. Таблица 7).

Таблица 7 – Параметры списка групп доменов аутентификации

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование группы домена аутентификации |
| «Комментарий» | Информационное сообщение, используемое для описания группы |
| «Статус» | Характеристика состояния группы |

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца.
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Для добавления группы следует перейти «Системные параметры - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне во вкладке «Группы» нажать экранную кнопку **[Добавить]**.

Для добавления группы необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 8).

Таблица 8 – Данные для добавления группы домена аутентификации

| Параметр | Описание |
|---|---|
| «Название» | Наименование группы, полученное от домена аутентификации. Для выбора группы из списка доступных нужно начать ввод ее наименования |
| «Комментарий» | Информационное сообщение, используемое для описания группы |
| «Статус» | Характеристика состояния субъектов группы при доступе к «Агрегатору».<br>Доступные значения:<br>▪ «Активный» - субъекты группы могут аутентифицироваться в портале «Агрегатор администратора» и/или «Агрегатор пользователя»;<br>▪ «Неактивный» - субъекты группы не могут аутентифицироваться в портале «Агрегатор администратора» и/или «Агрегатор пользователя» |

| Параметр | Описание |
|---|---|
| «Тип учетной записи» | Служебные функции субъектов группы при доступе к «Агрегатору».<br>Доступные значения параметра:<br>▪ «Пользователь» - субъекты группы не будут иметь доступ к порталу «Агрегатор администратора»;<br>▪ «Администратор» - субъекты группы будут иметь полный доступ к порталу «Агрегатор администратора» |
| «Роли» | Назначение служебных функций пользователям группы.<br>Доступность выбора значений зависит от параметра «Тип учетной записи» и того, созданы ли роли на странице «Системные параметры - Управление ролями» |
| «Метагруппа» | Характеристика использования метагруппы.<br>Метагруппа - группа, объединяющая несколько стандартных групп в «Агрегаторе».<br>Рекомендуется не использовать параметр |
| «Отображать метагруппу» | Характеристика использования метагруппы.<br>Рекомендуется не использовать параметр |

### 6.4 . Действия над пользователями в домене аутентификации

Пользователи – перечень объектов, имеющих в рамках домена аутентификации служебные функции на использование объединенных ресурсов. Пользователи будут автоматически добавлены в домен аутентификации после авторизации на сайте «Агрегатора».

Доступны следующие действия над пользователями внутри домена аутентификации:

- редактирование;
- удаление;
- просмотр сведений.

> ⓘ В «Агрегаторе» предусмотрена возможность автоматической регистрации пользователей при запросе опубликованных ресурсов на «Универсальном диспетчере».
> Для этого нужно добавить идентичные группы в соответствующих доменах аутентификации «Агрегатора» и «Универсального диспетчера». После входа пользователя на «Агрегатор» и запроса ресурсов с «Универсального диспетчера» его учетная запись будет автоматически зарегистрирована, если он состоит в группах, существующих на «Универсальном диспетчере».
> Редактирование и удаление пользователя в домене аутентификации в веб-портале не приводит к каким-либо изменениям объекта в службе каталогов.
> «Агрегатор» хранит информацию о назначении прав пользователя в БД, поэтому в случае, если пользователь должен быть исключен из группы администрирования, то необходимо удалить пользователя из группы непосредственно в доменной службе каталогов и на стороне «Агрегатора» одновременно.

Для просмотра списка групп следует перейти «Системные параметры - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне перейти во вкладку «Пользователи».

Основные параметры списка приведены в таблице (см. Таблица 9).

Таблица 9 – Параметры списка пользователей доменов аутентификации

| Параметр | Описание |
|---|---|
| «Имя» | Отображаемое имя пользователя в «Агрегаторе» |
| «Полное имя» | Имя пользователя, полученное от службы каталогов |
| «Администратор» | Характеристика, является ли пользователь администратором |
| «Комментарий» | Информационное сообщение, используемое для описания пользователя |
| «Статус» | Характеристика состояния пользователя |

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца.
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Для редактирования информации о пользователе следует перейти «Компоненты - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне в таблице «Пользователи» выделить строку с именем пользователя и нажать экранную кнопку **[Изменить]**.

В окне редактирования пользователя доступны данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 10).

Таблица 10 – Данные для редактирования пользователя домена аутентификации

| Параметр | Описание |
|---|---|
| «Имя» | Отображаемое имя пользователя в «Агрегаторе». Параметр получен автоматически от службы каталогов, его нельзя изменить |
| «Реальное имя» | Имя пользователя в службе каталогов |
| «Комментарий» | Информационное сообщение, используемое для описания назначения пользователя |

| Параметр | Описание |
|---|---|
| «Статус» | Характеристика состояния пользователя при доступе к «Агрегатору».<br>Возможные значения:<br>▪ «Активен» - пользователь может аутентифицироваться;<br>▪ «Неактивен» - пользователь не может аутентифицироваться |
| «Тип пользователя» | Служебные функции субъекта при доступе к «Агрегатору». Значение наследуется от группы, в которую входит пользователь. При этом по умолчанию тип учетной записи устанавливается в значение с более высоким уровнем прав.<br>Пример: если пользователь одновременно состоит в группе с типом учетной записи «Администратор» и группе с типом «Пользователь», то по умолчанию для пользователя будет установлен тип учетной записи «Администратор».<br>Доступные значения параметра:<br>▪ «Пользователь» - субъект не будет иметь доступ к «Агрегатору администратора». При выборе этого значения параметр «Роли» будет недоступен;<br>▪ «Персонал» - субъект будет иметь доступ к странице «Обзор» и будет обладать набором разрешений, определенных служебными функциями. При выборе этого значения в параметре «Роль» можно выбрать одно или несколько значений классов администратора, созданных на странице «Системные параметры - Управление ролями» (см. подраздел **Назначение служебных функций администраторам**);<br>▪ «Администратор» - субъект будет иметь полный доступ к «Порталу администратора». При выборе этого значения параметр «Роли» будет недоступен |
| «Группы» | Наименования групп, используемых для определения разрешений по доступу к фондам РМ.<br>Список групп пользователя будет получен автоматически от службы каталогов |
| «Роли» | Назначение служебной функции указанному пользователю.<br>Доступность выбора значений зависит от параметра «Тип пользователя» и того, созданы ли роли на странице «Системные параметры - Управление ролями».<br>Назначение параметра «Роли» будет доступно, если «Тип пользователя» соответствует «Персонал» |

# 7 . ФЕРМЫ ПОСТАВЩИКОВ РЕСУРСОВ

## 7.1 . Общие сведения о фермах поставщиков ресурсов

Ферма - логическое объединение узлов, взаимодействующих с одной БД.

Ферма поставщиков ресурсов - ферма, объединяющая установку узлов Termidesk. Например, узел «Портал администратора» и узел «Портал пользователя» могут быть объединены в одну ферму поставщиков ресурсов.

Для отображения списка ферм поставщиков ресурсов следует перейти «Инфраструктура - Фермы поставщиков ресурсов». Основные параметры списка приведены в таблице (см. Таблица 11).

Таблица 11 – Параметры списка ферм поставщиков ресурсов

| Параметр | Описание |
|---|---|
| «ID» | Идентификатор фермы |
| «Название» | Текстовое наименование фермы |
| «Комментарий» | Информационное сообщение, используемое для описания фермы |
| «Шлюз» | Шлюз, используемый в ферме |
| «Узлы» | Узлы, используемые в ферме |
| «Транспорт» | Протокол, используемый для подключения к узлу фермы |
| «Порт» | Порт, используемый для протокола |
| «Время обхода» | Периодичность (в минутах) опроса фермы |
| «Группы приоритетов» | Группы пользователей, которым предоставлен приоритетный доступ к ферме |
| «Исключен» | Характеристика использования фермы |
| «SSL» | Характеристика использования проверки валидности SSL-сертификата |
| «Статус» | Характеристика состояния фермы |
| «Дата создания» | Временная метка создания фермы |
| «Дата обновления» | Временная метка обновления фермы |

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**;

- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца.
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Для добавления фермы следует перейти «Инфраструктура - Фермы поставщиков ресурсов», затем нажать на экранную кнопку **[Создать]**.

Созданную ферму поставщиков ресурсов можно:

- редактировать, для этого нужно пометить ферму и нажать на экранную кнопку **[Изменить]**;
- удалить, для этого нужно пометить ферму и нажать на экранную кнопку **[Удалить]**.

### 7.2 . Добавление фермы поставщиков ресурсов

Для добавления фермы поставщиков ресурсов следует перейти «Инфраструктура - Фермы поставщиков ресурсов», а затем нажать экранную кнопку **[Создать]**.

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 12). Для сохранения параметров конфигурации нужно нажать экранную кнопку **[Создать]**.

> Перед тем, как ферма поставщиков ресурсов будет выдана пользователю, производится проверка наличия в ней свободных ВМ в кеше 1-го и 2-го уровней, а также назначенных пользователю ВМ. Если свободных или назначенных ВМ нет, ферма не отобразится пользователю.
> В случае неудачи при аутентификации между «Агрегатором» и «Универсальным диспетчером» фермы, она будет игнорироваться для выдачи пользователю до восстановления работоспособности. Для восстановления работоспособности следует проверить значение параметра `AGGREGATOR_ACCESS_TOKEN_TITLE` (см. подраздел **Параметры конфигурирования «Агрегатора»**).

Таблица 12 – Данные для добавления фермы поставщиков ресурсов

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование для добавляемой фермы |
| «Комментарий» | Информационное сообщение, используемое для описания назначения фермы |
| «Длительность обхода» | Периодичность опроса фермы (в минутах) для подтверждения ее активности.<br>По умолчанию «60» (каждые 60 минут).<br>Пример: пусть параметру «Длительность обхода» задано значение «60», а параметру «Длительность обхода при всех ошибках» задано значение «5». В таком случае, если ферма не пришлет свое состояние в момент опроса (через 60 минут), то через 5 минут, если ферма так и не отправит свое состояние, она будет отмечена неактивной |
| «Длительность обхода при всех ошибках» | Продолжительность времени (в минутах), по истечении которого ферма считается неактивной, если она не подтверждает свое активное состояние.<br>По умолчанию «0» |

| Параметр | Описание |
|---|---|
| «Максимум неудачных серверов на запрос» | Количество узлов в неактивном состоянии, при превышении которого ферма будет отмечена неактивной.<br>По умолчанию «0» |
| «Приоритетные группы» | Выбор группы пользователей, которой будет предоставлен приоритетный доступ к данной ферме.<br>Параметр задает приоритетную ферму, на которую будут перенаправляться подключения указанной группы в обход балансировки подключений.<br>Для каждой группы можно назначить только одну приоритетную ферму.<br>Для восстановления балансировки подключений необходимо исключить группу из списка приоритетных для фермы |
| «Транспорт» | Протокол, по которому будет происходить подключение к узлу.<br>Возможные значения:<br>▪ «HTTP» - незащищенное подключение;<br>▪ «HTTPS» (по умолчанию) - защищенное подключение |
| «Порт» | Порт, который будет использоваться при подключении по указанному в параметре «Транспорт» протоколу.<br>При стандартных настройках для протокола HTTP используется порт 80, для протокола HTTPS - 443.<br>По умолчанию «443» |
| «Шлюз» | Выбор шлюза, через который пользователь будет получать ресурсы. Можно выбрать только одно значение.<br>Шлюз должен быть добавлен через «Управление - Шлюзы» для возможности его выбора в этом параметре |
| «Активна» | ⚠ Может быть активирован либо параметр «Активна», либо параметр «Исключена».<br>Управление состоянием фермы. При активации параметра ферма участвует в выдаче ресурсов |
| «Исключена» | ⚠ Может быть активирован либо параметр «Активна», либо параметр «Исключена».<br>Управление состоянием фермы. При активации параметра ферма не участвует в выдаче ресурсов.<br><br>Параметр используется для прекращения взаимодействия «Агрегатора» с фермой, которая по каким-либо причинам выведена из стандартного рабочего состояния. Если ресурс, запрашиваемый пользователем, фактически расположен на нескольких фермах, и какая-то из них вышла из стандартного рабочего состояния, то следует исключить эту ферму из списка опрашиваемых. В таком случае балансировка подключений пользователей будет происходить только для активных ферм |
| «Проверять SSL» | Управление проверкой валидности SSL-сертификата. Параметр необходимо отключить в случае, если проверку валидности пройти не удается:<br>▪ на узлах фермы используются самоподписанные сертификаты;<br>▪ или на узлах фермы используются сертификаты, выпущенные центром сертификации, корневой сертификат которого не добавлен в список доверенных на узле «Агрегатора».<br>По умолчанию проверка валидности сертификатов отключена |

# 8 . УЗЛЫ

## 8.1 . Общие сведения об узлах

Узел - аппаратный или виртуальный сервер компонента «Универсальный диспетчер».

Несколько узлов, взаимодействующих с единой БД, объединяются в одну ферму поставщиков ресурсов.

Для отображения списка узлов следует перейти «Инфраструктура - Узлы». Основные параметры списка приведены в таблице (см. Таблица 13).

Таблица 13 – Параметры списка узлов

| Параметр | Описание |
|---|---|
| «ID» | Идентификатор узла |
| «Название» | Текстовое наименование узла |
| «Хост» | IP-адрес или FQDN узла |
| «Токен» | Токен доступа к API узла |
| «Статус» | Характеристика состояния узла |
| «Дата создания» | Временная метка создания узла |
| «Дата обновления» | Временная метка обновления узла |

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца.
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Для добавления узла в веб-портале «Агрегатор администратора» следует перейти «Инфраструктура - Фермы поставщиков ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование фермы. В открывшемся окне «Узлы фермы» нажать экранную кнопку **[Добавить узел]**.

Отредактировать информацию об узле можно двумя способами:

- перейти «Инфраструктура - Фермы поставщиков ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование фермы. В открывшемся окне «Узлы фермы» нажать экранную кнопку **[Изменить]**;
- перейти «Инфраструктура - Узлы», затем выбрать необходимый узел и нажать на экранную кнопку **[Изменить]**.

Удалить узел можно двумя способами:

- перейти «Инфраструктура - Фермы поставщиков ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование фермы. В открывшемся окне «Узлы фермы» нажать экранную кнопку **[Удалить]**;
- перейти «Инфраструктура - Узлы», затем выбрать необходимый узел и нажать на экранную кнопку **[Удалить]**.

## 8.2 . Добавление узла Termidesk

Для добавления узла Termidesk следует перейти «Инфраструктура - Фермы поставщиков ресурсов», затем в столбце «Название» сводной таблицы нажать на наименование фермы. В открывшемся окне «Узлы фермы» нажать экранную кнопку **[Добавитьузел]**.

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 14). Для сохранения параметров конфигурации нужно использовать экранную кнопку **[Добавить]**. При сохранении будет запрошена проверка состояния `healthcheck` и узел будет сохранен, если он существует и ответил на запрос.

> ⓘ Узлы, которые по каким-то причинам вышли из строя и перестали отвечать на запрос проверки состояния `healthcheck`, автоматически будут помечены как неактивные и не будут участвовать в балансировке подключений и выдаче ресурсов пользователю.
> Если узел вновь ответил на запрос проверки состояния `healthcheck`, его состояние изменится на активное.

Таблица 14 – Данные для добавления узла Termidesk

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование добавляемого узла |
| «Хост» | IP-адрес или FQDN сервер с установленным компонентом «Универсальный диспетчер» («Портал пользователя» или «Портал универсальный»), который добавляется в качестве узла |
| «Токен авторизации» | Токен для доступа к API добавляемого узла.<br>Значение параметра может быть получено из переменной `HEALTH_CHECK_ACCESS_KEY`, определенной в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` узла «Универсального диспетчера» |
| «Активен» | Характеристика состояния узла.<br>Если параметр отключен, то «Агрегатор» прекратит взаимодействие с узлом |

Для просмотра всех добавленных узлов с привязкой к ферме поставщиков ресурсов следует перейти «Инфраструктура - Узлы».

# 9 . САЙТЫ

## 9.1 . Общие сведения о сайтах

Сайт - физическая площадка, на которой может быть развернута одна или несколько ферм. Сайт объединяет одну или несколько добавленных ферм и является единой точкой входа для получения ресурсов пользователями.

Обязательным условием для использования сайта является создание объединенного набора ресурсов, представляющего собой правила, при которых сайт функционирует. Если не будет создан объединенный набор ресурсов или он будет неактивен, сайт будет недоступен для пользователей.

Для отображения списка сайтов следует перейти «Управление - Сайты». Основные параметры списка приведены в таблице (см. Таблица 15).

Таблица 15 – Параметры списка сайтов

| Параметр | Описание |
|---|---|
| «ID» | Идентификатор сайта |
| «Название» | Текстовое наименование сайта |
| «Комментарий» | Информационное сообщение, используемое для описания фермы |
| «URI» | Адрес начальной страницы для входа на сайт |
| «Группы пользователей» | Количество групп пользователей домена аутентификации, которые могут аутентифицироваться на сайте |
| «Фермы» | Перечень ферм, используемых для сайта |
| «Техобслуживание» | Характеристика состояния техобслуживания сайта |
| «Шаблоны техобслуживания» | Наименование шаблона техобслуживания, используемого для сайта |

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца.
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Для добавления сайта в веб-портале «Агрегатор администратора» следует перейти «Управление - Сайты», затем нажать экранную кнопку **[Создать]**.

Созданный сайт можно:

- редактировать, для этого нужно пометить сайт и нажать на экранную кнопку **[Изменить]**;
- удалить, для этого нужно пометить сайт и нажать на экранную кнопку **[Удалить]**.

## 9.2 . Добавление сайта

Для добавления сайта следует перейти «Управление - Сайты», а затем нажать экранную кнопку **[Создать]**.

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 16). Для сохранения параметров конфигурации нужно использовать экранную кнопку **[Создать]**.

Таблица 16 – Данные для добавления сайта

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование добавляемого сайта.<br>Наименование может содержать только буквы латинского алфавита, цифры, знаки «-» (дефис) |
| «Комментарий» | Информационное сообщение, используемое для описания назначения сайта |
| «URI» | Адрес начальной страницы для входа на сайт |
| «Домен аутентификации» | Выбор домена аутентификации, пользователи которого смогут аутентифицироваться на сайте.<br>Домен аутентификации должен быть добавлен через «Компоненты - Домены аутентификации» для возможности его выбора в этом параметре |
| «Группы пользователей» | Выбор группы или групп пользователей домена аутентификации, которые могут аутентифицироваться на сайте.<br>Группы пользователей должны быть добавлены в домене аутентификации («Компоненты - Домены аутентификации») для возможности их выбора в этом параметре.<br>Список групп пользователей будет отображен после выбора домена в параметре «Домен аутентификации» |
| «Пользователи» | Выбор пользователей, которые могут аутентифицироваться на сайте.<br>Пользователи должны быть добавлены в домене аутентификации («Компоненты - Домены аутентификации») для возможности их выбора в этом параметре.<br>Список пользователей будет отображен после выбора домена в параметре «Домен аутентификации».<br>Для удобства нахождения пользователя можно воспользоваться формой поиска, расположенной в верхней части выпадающего блока параметра «Пользователи» |
| «Фермы поставщиков ресурсов» | Выбор фермы или ферм, для которых будет создан сайт.<br>Фермы поставщиков ресурсов должны быть добавлены через «Компоненты - Фермы поставщиков ресурсов» для возможности их выбора в этом параметре |
| «Техобслуживание» | Управление режимом техобслуживания сайта.<br>Режим техобслуживания - это запрет пользователям подключаться к сайту. Этот режим предназначен для проведения плановых регламентных или аварийных работ |
| «Шаблон техобслуживания» | Выбор ранее созданного шаблона, текст из которого будет выведен пользователю при попытке подключиться к сайту, находящемуся в режиме техобслуживания.<br>Создание шаблона приведено в подразделе **Добавление шаблона техобслуживания** |

| Параметр | Описание |
|---|---|
| «Разрешить сохранение имени пользователя в клиенте» | Управление параметром сохранения имени пользователя в компоненте «Клиент» при подключении к «Агрегатору».<br>По умолчанию параметр не активирован |
| «Сохранять пароль пользователя» | Сохранение пароля пользователя в компоненте «Клиент» при подключении к «Агрегатору».<br>По умолчанию параметр не активирован |
| «Скрывать недоступные ресурсы» | Управление сокрытием недоступных ресурсов при подключении пользователя к «Агрегатору».<br>Если параметр активирован, недоступные ресурсы не будут отображаться пользователю.<br>Если параметр не активирован, то недоступные ресурсы будут отображены пользователю, но он не сможет к ним подключиться.<br>По умолчанию параметр активирован |
| «Периодичность фонового обновления списка приложений» | Параметр определяет периодичность (в секундах), с которой будет происходить обновление списка ресурсов в интерфейсе «Клиента».<br>Возможные значения: от 60 до 28800.<br>Значение по умолчанию: «300» |
| «Обновлять список ресурсов при каждом запуске ресурса» | Управление режимом обновления списка ресурсов.<br>Возможные значения:<br>▪ «Не задано» (по умолчанию) - выбор режима будет задан пользователем в интерфейсе «Клиента»;<br>▪ «Включено» - обновление списка ресурсов будет происходить при запуске какого-либо ресурса пользователем;<br>▪ «Выключено» - обновление списка ресурсов не будет происходить при запуске какого-либо ресурса пользователем |

## 9.3 . Добавление объединенного набора ресурсов

Для добавления объединенного набора ресурсов следует перейти «Управление - Сайты», затем в столбце «Название» сводной таблицы нажать на наименование сайта. На открывшейся странице нажать экранную кнопку **[Добавить]**.

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 17). Для сохранения параметров конфигурации нужно использовать экранную кнопку **[Добавить]**.

Таблица 17 – Данные для добавления объединенного набора ресурсов

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование добавляемого объединенного набора ресурсов |
| «Комментарий» | Информационное сообщение, используемое для описания назначения объединенного набора ресурсов |
| «Приоритет» | Приоритет отображения |
| «Фермы» | Выбор фермы или ферм, для которых будут действовать правила объединенного набора ресурсов |

| Параметр | Описание |
|---|---|
| «Публикуются идентичные ресурсы» | Характеристика публикуемых ресурсов:<br>▪ «Да» - все наборы ресурсов, опубликованные на фермах, идентичны;<br>▪ «Нет» - наборы ресурсов, опубликованные на фермах, неидентичны.<br>Параметр определяет, будет ли «Агрегатор» опрашивать каждую ферму для получения всех ресурсов. Если отмечено, что все ресурсы идентичны на указанных фермах, ресурсы будут получены только от одной фермы. Если ресурсы неидентичны на фермах, они будут получены от каждой из ферм.<br>Агрегатор не проверяет, действительно ли все ресурсы на указанных фермах идентичны - это подтверждает администратор через указанный параметр |
| «Балансировка подключений» | Характеристика активации балансировки подключений:<br>▪ «Да» - подключения балансируются по схеме round-robin;<br>▪ «Нет» - подключения не балансируются |
| «Активен» | Характеристика состояния объединенного набора ресурсов:<br>▪ «Да» - объединенный набор ресурсов активен и доступен для пользователей;<br>▪ «Нет» - объединенный набор ресурсов неактивен и недоступен для пользователей |

# 10 . ШАБЛОНЫ ТЕХОБСЛУЖИВАНИЯ

## 10.1 . Общие сведения о шаблонах техобслуживания

Шаблон техобслуживания определяет текст сообщения, отправляемое пользователю при попытке подключиться к сайту, находящемуся в режиме техобслуживания.

Для отображения списка шаблонов техобслуживания следует перейти «Управление - Шаблоны техобслуживания». Основные параметры списка приведены в таблице (см. Таблица 18).

Таблица 18 – Параметры списка шаблонов техобслуживания

| Параметр | Описание |
|---|---|
| «ID» | Идентификатор шаблона |
| «Название» | Текстовое наименование шаблона |
| «Комментарий» | Информационное сообщение, используемое для описания шаблона |
| «Сообщение» | Сообщение, используемое в шаблоне |
| «Дата создания» | Временная метка создания шаблона |

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**;

- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца.
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Для добавления шаблона в веб-портале «Агрегатор администратора» следует перейти «Управление - Шаблоны техобслуживания», затем нажать экранную кнопку **[Создать]**.

Созданный шаблон техобслуживания можно:

- редактировать, для этого нужно пометить шаблон и нажать на экранную кнопку **[Изменить]**;
- удалить, для этого нужно пометить шаблон и нажать на экранную кнопку **[Удалить]**.

## 10.2 . Добавление шаблона техобслуживания

Для добавления шаблона следует перейти «Управление - Шаблоны техобслуживания», затем нажать экранную кнопку **[Создать]**.

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 19). Для сохранения параметров конфигурации нужно нажать экранную кнопку **[Создать]**.

Таблица 19 – Данные для добавления шаблона техобслуживания

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование добавляемого шаблона |
| «Комментарий» | Информационное сообщение, используемое для описания назначения шаблона |
| «Сообщение» | Текст сообщения, которое будет отображено пользователю |

# 11 . НАСТРОЙКА ПОДКЛЮЧЕНИЯ ПОЛЬЗОВАТЕЛЕЙ ЧЕРЕЗ ШЛЮЗ

## 11.1 . Общие сведения по использованию шлюза

Шлюз «Агрегатора» - аппаратный или виртуальный сервер, на котором установлен компонент «Шлюз» Termidesk. Использование шлюза делает доступным сценарий, при котором пользователь запрашивает ресурсы, доступ к которым не осуществляется напрямую.

Типовой сценарий для использования шлюза:

- в сетевой инфраструктуре организации существует сегмент, скрытый от внешних подключений;
- в указанном сегменте развернута ферма поставщиков ресурсов, в которой используется сервер с компонентом «Шлюз» для туннелирования протоколов доставки;
- в другом сегменте сетевой инфраструктуры организации развернут «Агрегатор».

В таком сценарии целесообразно в одном сегменте с «Агрегатором» установить еще один сервер с компонентом «Шлюз» (шлюз «Агрегатора»), адрес которого будет подставлен в параметрах подключения к ресурсу, отдаваемых пользователю, вместо адреса «Шлюза» фермы поставщиков ресурсов.

Для отображения списка шлюзов следует перейти «Управление - Шлюзы». Основные параметры списка приведены в таблице (см. Таблица 20).

Таблица 20 – Параметры списка шлюзов

| Параметр | Описание |
|---|---|
| «ID» | Идентификатор шлюза |
| «Название» | Текстовое наименование шлюза |
| «URL» | Адрес шлюза, обеспечивающего формирование и поддержание соединения |

Поддерживается:

- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца.

- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Для добавления шлюза в веб-портале «Агрегатор администратора» следует перейти «Управление - Шлюзы», затем нажать экранную кнопку **[Создать]**.

Созданный шлюз можно:

- редактировать, для этого нужно пометить шлюз и нажать на экранную кнопку **[Изменить]**;
- удалить, для этого нужно пометить шлюз и нажать на экранную кнопку **[Удалить]**.

### 11.2 . Добавление шлюза

Для добавления шлюза следует перейти «Управление - Шлюзы», а затем нажать экранную кнопку **[Создать]**.

Затем необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (see page 0). Для сохранения параметров конфигурации нужно нажать экранную кнопку **[Создать]**.

Таблица 21 – Данные для добавления шлюза

| Параметр | Описание |
|---|---|
| «Название» | Текстовое наименование добавляемого шлюза |
| «URL» | Адрес сервера с установленным компонентом «Шлюз» в формате `ws(s)://192.0.2.30:5099`, обеспечивающего формирование и поддержание соединения.<br>Протокол WS (WebSocket) использует по умолчанию порт 80, протокол WSS использует по умолчанию порт 443. Администратор может задать нужное значение, если используется нестандартный порт.<br>Параметр `192.0.2.30:5099` - доступный IP-адрес сервера и его порт. Пример IP-адреса приведен в соответствии с RFC 5737, он должен быть заменен на актуальный, используемый согласно схеме адресации, принятой в инфраструктуре организации |

# 12 . СИСТЕМНЫЕ НАСТРОЙКИ

## 12.1 . Назначение служебных функций администраторам

Для администраторов «Агрегатора» реализовано разделение доступных служебных функций.

Для назначения доступных служебных функций следует перейти «Системные параметры - Управление ролями» и нажать экранную кнопку [Создать роль] (см. Рисунок 7).

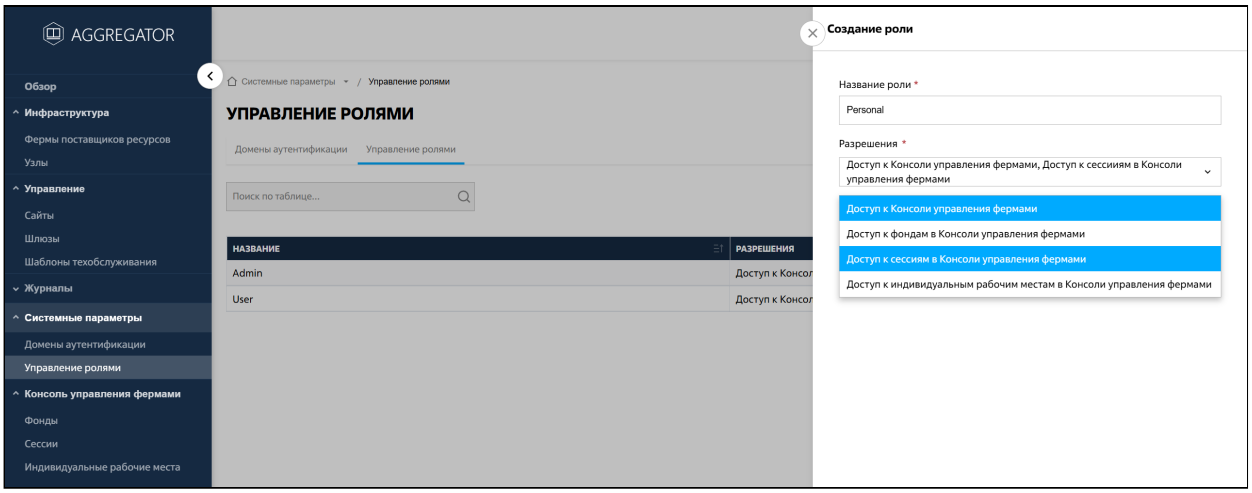



Рисунок 7 – Окно назначения пользовательских разрешений

При добавлении функции необходимо ввести текстовое наименование создаваемого класса администратора, а также выбрать список назначаемых разрешений.

Список разрешений для назначения служебных функций администраторам перечислен в следующей таблице (см. Таблица 22).

Таблица 22 – Список доступных для выбора разрешений

| Разрешение | Описание |
|---|---|
| «Доступ к Консоли управления фермами» | Предоставляет доступ на чтение страницы «Консоль управления фермами».<br>Разрешение позволяет выполнять просмотр:<br>▪ раздела «Фонды»;<br>▪ раздела «Сессии»;<br>▪ раздела «Индивидуальные рабочие места» |
| «Доступ к фондам в Консоли управления фермами» | Предоставляет доступ на чтение страницы «Консоль управления фермами - Фонды». Разрешение позволяет:<br>▪ просматривать раздел «Фонды» и выполнять действия в разделе:<br>• просматривать список фондов РМ;<br>• управлять политиками фонда РМ;<br>• редактировать фонды РМ;<br>• управлять режимом техобслуживания фонда РМ |

| Разрешение | Описание |
|---|---|
| «Доступ к сессиям в Консоли управления фермами» | Предоставляет доступ на чтение страницы «Консоль управления фермами - Сессии». Разрешение позволяет:<br>▪ просматривать раздел «Сессии» и выполнять действия в разделе:<br>• просматривать список сессий;<br>• отключать сессию;<br>• завершать сессию;<br>• выполнять подключение к сессии через компонент «Удаленный помощник» |
| «Доступ к индивидуальным рабочим местам в Консоли управления фермами» | Предоставляет доступ на чтение страницы «Консоль управления фермами - Индивидуальные рабочие места». Разрешение позволяет:<br>▪ просматривать раздел «Индивидуальные рабочие места» и выполнять действия в разделе:<br>• просматривать список РМ;<br>• управлять состоянием РМ;<br>• назначать владельца РМ;<br>• управлять режимом техобслуживания РМ |

Класс администратора может быть назначен определенному пользователю. Для назначения созданного класса следует перейти «Системные параметры - Домены аутентификации» и затем в столбце «Название» сводной таблицы выбрать домен аутентификации, в который входит пользователь.

На открывшейся странице в таблице «Пользователи» нужно выбрать пользователя и нажать экранную кнопку **[Изменить]**. В открывшейся форме редактирования пользователя в поле «Роли» выбрать класс (см. Рисунок 8).

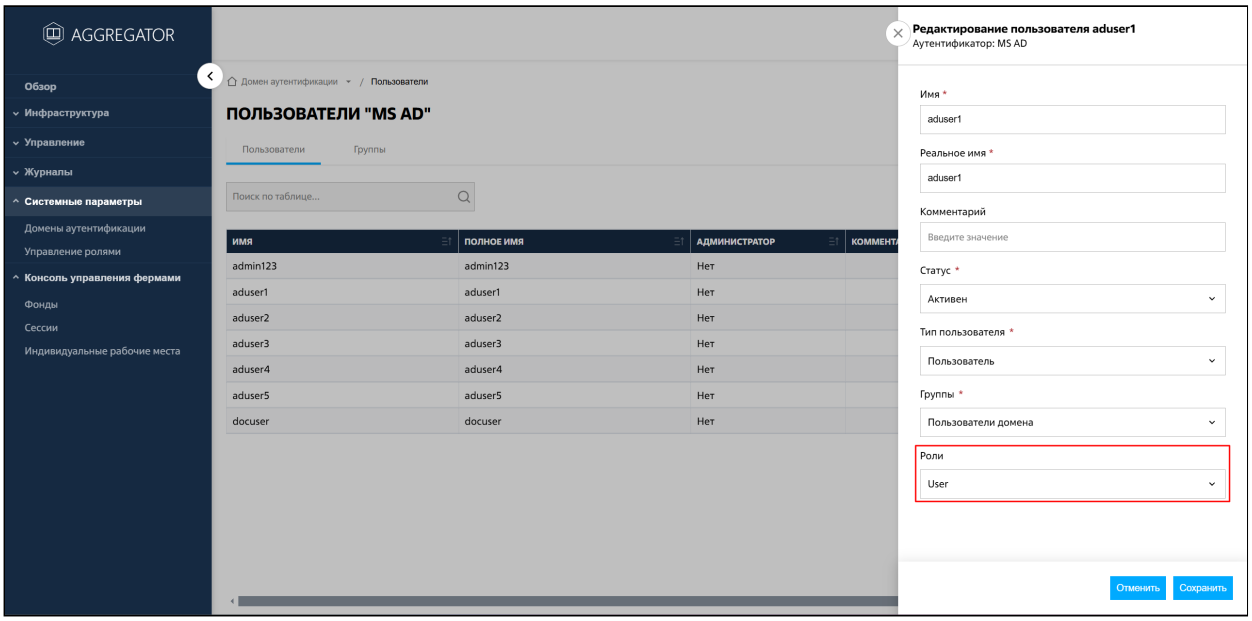



Рисунок 8 – Окно назначения пользовательских ролей

⚠ Параметр «Персонал» указывает, что пользователь является оператором «Агрегатора» (класс администратора с ограниченными полномочиями).

## 12.2 . Параметры конфигурирования «Агрегатора»

Для настройки «Агрегатора» используется конфигурационный файл `/etc/opt/termidesk-vdi/termidesk.conf`.

> ⓘ При установке пакета `termidesk-vdi` возможно активировать режим отладки через переменную окружения `TDSK_PKG_DEBUG=1`.

Полный перечень параметров, задающихся через файл, приведен в таблице.

Указанные параметры можно поменять также через утилиту `termidesk-config` (см. подраздел **Утилита termidesk-config**).

Таблица 23 – Параметры конфигурирования «Агрегатора»

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| Настройки параметров перемещаемых профилей | | |
| `TDSK_AUTOFS_IMAGES_ID` | Не задано | Параметр может быть задан на узлах «Универсального диспетчера».<br>Используется для настройки шаблонов перемещаемых профилей. В качестве значения используются идентификаторы дисков.<br>Пример: `TDSK_AUTOFS_IMAGES_ID=xx[,yy[,zz[,...]]]` |
| Настройки подключения к СУБД | | |
| `DB_CLUSTER_MODE` | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет тип установки СУБД, к которой осуществляется подключение.<br>Возможные значения:<br>▪ `single` - подключение производится к отдельному серверу СУБД;<br>▪ `cluster` - подключение производится к кластеру СУБД |
| `DBHOST` | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет IP-адрес или FQDN СУБД PostgreSQL.<br>Начальное значение задается на этапе подготовке среды функционирования и установки Termidesk |
| `DBHOST2` | Не задано | Параметр необязательный, может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет IP-адрес или FQDN дополнительного узла СУБД PostgreSQL, если используется подключение к кластеру СУБД (см. параметр `DB_CLUSTER_MODE`).<br>Начальное значение задается на этапе установки Termidesk |
| `DBHOST3` | Не задано | Параметр необязательный, может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет IP-адрес или FQDN дополнительного узла СУБД PostgreSQL, если используется подключение к кластеру СУБД (см. параметр `DB_CLUSTER_MODE`).<br>Начальное значение задается на этапе установки Termidesk |
| `DBPORT` | 5432 | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет порт соединения с сервером БД |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| DBSSL | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет протокол подключения к БД.<br>Возможные значения:<br>▪ Disable;<br>▪ TLSv1.2;<br>▪ TLSv1.3.<br>Начальное значение задается на этапе установки Termidesk |
| DBNAME | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет имя БД.<br>Начальное значение задается на этапе подготовки среды функционирования перед установкой Termidesk |
| DBUSER | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет имя пользователя, имеющего доступ к БД.<br>Начальное значение задается на этапе подготовки среды функционирования перед установкой Termidesk |
| DBPASS | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет пароль пользователя, имеющего доступ к БД.<br>Начальное значение задается на этапе подготовки среды функционирования во время установки Termidesk и хранится в конфигурационном файле /etc/opt/termidesk-vdi/termidesk.conf в преобразованном виде.<br>В стандартных установках значения менять не следует.<br>Чтобы получить преобразованное значение пароля, следует воспользоваться утилитой scramble:<br>▪ для получения значения по стандартному алгоритму: /opt/termidesk/bin/scramble --value <пароль> --type AES256;<br>▪ для получения значения с увеличенным числом итераций преобразования: /opt/termidesk/bin/scramble --value <пароль> --type AES256_V2.<br>Если значение пароля указывается в формате ключа (значение предваряется символом «-»), то следует изменить его передачу в параметр--value:<br>/opt/termidesk/bin/scramble --value=<-пароль> --type AES256<br>Утилита scramble использует в качестве вектора преобразования значение из файла /etc/opt/termidesk-vdi/termidesk.cookie. Значение генерируется автоматически на этапе установки Termidesk |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| DBCERT | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет путь к клиентскому сертификату mTLS для защищенного подключения к БД.<br>mTLS - метод обеспечения защищенного соединения с БД через двустороннюю аутентификацию с использованием сертификатов.<br>Для использования сертификата нужно:<br>▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;<br>▪ назначить владельцем файла пользователя `termidesk`:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**).<br>Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:<br>`DBCERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'` |
| DBKEY | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет путь к ключу mTLS для защищенного подключения к БД.<br>Ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению:<br>`openssl rsa -in <путь_к_файлу_ключа.key> -out <путь_сохранения_преобразованного_ключа.key>`<br>Для использования ключа также нужно:<br>▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;<br>▪ назначить владельцем файла пользователя `termidesk`:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.<br>Ключ может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:<br>`DBKEY='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/key'` |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| DBCHAIN | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет путь к промежуточному сертификату mTLS для защищенного подключения к БД.<br>Для использования сертификата нужно:<br>▪ скопировать его в каталог /etc/opt/termidesk-vdi/;<br>▪ назначить владельцем файла пользователя termidesk:<br>sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem<br>▪ изменить права на файл:<br>sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.<br>Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:<br>DBCHAIN='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/ca' |
| Настройка проверки данных при взаимодействии компонентов Termidesk | | |
| DJANGO_SECRET_KEY | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Используется для проверки данных, пересылаемых между компонентами Termidesk. Значение генерируется при установке Termidesk и должно быть одинаковым для всех узлов при распределенной установке |
| Настройка подключения к RabbitMQ | | |
| RABBITMQ_URL | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет URL-адрес подключения к серверам RabbitMQ. Можно подключить до трех (включительно) серверов.<br>Пароль подключения к серверу RabbitMQ, указанный в RABBITMQ_URL, хранится в конфигурационном файле /etc/opt/termidesk-vdi/termidesk.conf в преобразованном виде.<br>Чтобы получить преобразованное значение пароля, следует воспользоваться утилитой scramble:<br>▪ для получения значения по стандартному алгоритму:<br>/opt/termidesk/bin/scramble --value <пароль> --type AES256<br>▪ для получения значения с увеличенным числом итераций преобразования:<br>/opt/termidesk/bin/scramble --value <пароль> --type AES256_V2<br>Если значение пароля указывается в формате ключа (значение предваряется символом «-»), то следует изменить его передачу в параметр--value:<br>/opt/termidesk/bin/scramble --value=<-пароль> --type AES256<br>Для использования преобразованного значения следует указать его в RABBITMQ_URL и выполнить перезапуск служб.<br>Начальное значение RABBITMQ_URL задается на этапе установки |
| RABBITMQ_SSL | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет протокол подключения к RabbitMQ.<br>Возможные значения: Disable, TLSv1.2.<br>Начальное значение задается на этапе установки |
| Настройки защищенного подключения к RabbitMQ | | |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| CELERY_BROKER_CERT | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет путь к клиентскому сертификату mTLS для защищенного подключения к RabbitMQ.<br>Для использования сертификата нужно:<br>▪ скопировать его в каталог /etc/opt/termidesk-vdi/;<br>▪ назначить владельцем файла пользователя termidesk:<br>sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt<br>▪ изменить права на файл:<br>sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.<br>Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:<br>CELERY_BROKER_CERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem' |
| CELERY_BROKER_KEY | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет путь к закрытому ключу mTLS для защищенного подключения к RabbitMQ.<br>Ключ может иметь парольную защиту. Для использования в Termidesk нужно преобразовать его к начальному значению:<br>openssl rsa -in <путь_к_файлу_ключа.key> -out <путь_сохранения_преобразованного_ключа.key><br>Для использования ключа также нужно:<br>▪ скопировать его в каталог /etc/opt/termidesk-vdi/;<br>▪ назначить владельцем файла пользователя termidesk:<br>sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key<br>▪ изменить права на файл:<br>sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.<br>Ключ может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:<br>CELERY_BROKER_KEY='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/key' |
| CELERY_BROKER_CA | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет путь к корневому сертификату ЦС mTLS для защищенного подключения к RabbitMQ.<br>Для использования сертификата нужно:<br>▪ скопировать его в каталог /etc/opt/termidesk-vdi/;<br>▪ назначить владельцем файла пользователя termidesk:<br>sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt<br>▪ изменить права на файл:<br>sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**).<br>Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:<br>CELERY_BROKER_CA='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/ca' |
| Настройки установленных ролей Termidesk | | |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| NODE_ROLES | Не задано | Параметр обязателен и задается на этапе установки.<br>Определяет тип роли, с которой будет установлен Termidesk. Возможные значения:<br>▪ ADMIN - роль «Портал администратора»;<br>▪ USER - роль «Портал пользователя»;<br>▪ CELERYMAN - роль «Менеджер рабочих мест»;<br>▪ AGGR_ADM - роль «Агрегатор администратора»;<br>▪ AGGR_USR - роль «Агрегатор пользователя».<br>Установка ролей «Агрегатор администратора» и/или «Агрегатор пользователя» должна производиться на узле, отличном от «Портала администратора» и/или «Портала пользователя».<br>Таким образом одновременно на одном узле могут быть заданы роли:<br>▪ либо ADMIN и (или) USER;<br>▪ либо AGGR_ADM и (или) AGGR_USR.<br>При переустановке значение параметра в конфигурационном файле будет перезаписано |
| Настройки журналирования | | |
| LOG_LEVEL | INFO | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет уровень журналирования сообщений.<br>Возможные значения: DEBUG, INFO, WARNING, ERROR, CRITICAL |
| LOG_ADDRESS | /dev/log | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет адрес отправки записей в системный журнал. Обычно это /dev/log для Linux-систем. Возможно указать IP-адрес и порт |
| LOG_FACILITY | local3 | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет категорию сообщений syslog.<br>Категория должна совпадать с настройками в конфигурационном файле /etc/syslog-ng/conffirst.d/termidesk.conf |
| Настройки токена доступа к API для проверок состояния служб Termidesk | | |
| HEALTH_CHECK_ACCESS_KEY | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет токен доступа к API проверки состояния сервера. Начальное значение генерируется на этапе установки.<br>При задании значения параметра следует руководствоваться правилом, что:<br>▪ размер должен составлять от 0 до 64 символа;<br>▪ должны использоваться символы в шестнадцатеричной системе (0-9, a-f).<br>Значение также может быть сгенерировано через openssl:<br>openssl rand -hex 32 |
| Настройки токена доступа к API получения метрик узла | | |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| METRICS_ACCESS_KEY | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет токен доступа к API получения метрик узла. Начальное значение генерируется на этапе установки.<br>При задании значения параметра следует руководствоваться правилом, что:<br>▪ размер должен составлять от 0 до 64 символа;<br>▪ должны использоваться символы в шестнадцатеричной системе (0-9, a-f).<br>Значение также может быть сгенерировано через openssl:<br>`openssl rand -hex 32` |
| Настройки защищенного подключения для проверок состояния служб «Менеджера рабочих мест» | | |
| HEALTH_CHECK_CERT | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора» (в зависимости от варианта установки).<br>Определяет путь к сертификату SSL/TLS для защищенного подключения к API проверки состояния служб «Менеджера рабочих мест».<br>Для использования сертификата нужно:<br>▪ скопировать его в каталог /etc/opt/termidesk-vdi/;<br>▪ назначить владельцем файла пользователя termidesk:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.<br>Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:<br>`HEALTH_CHECK_CERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'` |
| HEALTH_CHECK_KEY | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора» (в зависимости от варианта установки).<br>Определяет путь к ключу SSL/TLS для защищенного подключения к API проверки состояния служб «Менеджера рабочих мест».<br>Ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению:<br>`openssl rsa -in <путь_к_файлу_ключа.key> -out <путь_сохранения_преобразованного_ключа.key>`<br>Для использования ключа также нужно:<br>▪ скопировать его в каталог /etc/opt/termidesk-vdi/;<br>▪ назначить владельцем файла пользователя termidesk:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.<br>Ключ может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:<br>`HEALTH_CHECK_KEY='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/key'` |
| Настройки компонента «Менеджер рабочих мест» (службы termidesk-celery-beat) | | |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| CELERY_BEAT_HEALTH_CHECK_PORT | 8103 | Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест».<br>Определяет порт, на котором работает веб-сервер для обслуживания API проверки состояния компонента «Менеджер рабочих мест».<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| CELERY_BEAT_HEALTH_CHECK_IP | 0.0.0.0 | Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест».<br>Определяет IP-адрес, с которым служба `termidesk-celery-beat` регистрируется в подсистеме проверки состояния на странице «Инфраструктура» Termidesk. Опрос состояния службы будет проводиться по этому адресу. Если IP-адрес не задан, то будет использоваться имя (hostname) или FQDN узла.<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| Настройки компонента «Менеджер рабочих мест» (службы `termidesk-celery-worker`) | | |
| CELERY_WORKER_HEALTH_CHECK_PORT | 8104 | Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест».<br>Определяет порт, на котором работает веб-сервер для обслуживания API проверки состояния компонента «Менеджер рабочих мест».<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| CELERY_WORKER_HEALTH_CHECK_IP | 0.0.0.0 | Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест».<br>Определяет IP-адрес, с которым служба `termidesk-celery-worker` регистрируется в подсистеме проверки состояния на странице «Инфраструктура». Опрос состояния службы будет проводиться по этому адресу. Если IP-адрес не задан, то будет использоваться имя (hostname) или FQDN узла.<br>Изначально параметр закомментирован (используется значение по умолчанию) |
| Настройки подключения к серверу «Удаленного помощника» | | |
| REMOTE_ASSISTANT_SERVER_CERT | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора».<br>Определяет путь к серверному сертификату SSL/TLS для проверки подключения к «Удаленному помощнику».<br>Для использования сертификата нужно:<br>▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;<br>▪ назначить владельцем файла пользователя `termidesk`:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.<br>Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:<br>`REMOTE_ASSISTANT_SERVER_CERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'` |
| Настройки доверенных корневых сертификатов | | |
| REQUESTS_CA_BUNDLE | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет путь к файлу с доверенным корневым сертификатом, задается для настройки работы с сертификатами собственных ЦС.<br>По умолчанию параметр не используется (закомментирован) |
| Настройки принятия лицензионного соглашения | | |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| EULA_ACCEPTED | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет принятие лицензионного соглашения при установке. В случае автоматизированной установки наличие параметра обязательно |
| Настройки взаимодействия между узлами «Агрегатора» и «Универсального диспетчера» | | |
| AGGREGATOR_JWT_SSL_CERT | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», использующихся в фермах, подключаемых к «Агрегатору». Обязателен для заполнения в случае, если в инфраструктуре также используется «Агрегатор».<br>Определяет путь к сертификату для получения значения JWT-токена «Агрегатора» |
| AGGREGATOR_JWT_SSL_CERT_SECOND | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», использующихся в фермах, подключаемых к «Агрегатору». Обязателен для заполнения в случае, если в инфраструктуре также используется «Агрегатор».<br>Определяет путь к резервному сертификату для получения значения JWT-токена «Агрегатора».<br>Если сертификат, заданный в AGGREGATOR_JWT_SSL_CERT, станет невалидным, то будет использоваться сертификат, указанный в AGGREGATOR_JWT_SSL_CERT_SECOND |
| AGGREGATOR_JWT_SSL_KEY | Не задано | Параметр обязателен и задается на узлах с установленным «Агрегатором» (портал «Агрегатор пользователя»).<br>Определяет путь к ключу для подписи JWT-токена «Агрегатора» |
| AGGREGATOR_ACCESS_TOKEN_TITLE | Termidesk JWT Title | Параметр обязателен и должен быть одинаковым на всех узлах, работающих совместно: на «Агрегаторе» (портал «Агрегатор пользователя»), на «Универсальных диспетчерах», подключаемых к «Агрегатору».<br>Задает заголовок JWT-токена, предназначенный для настройки взаимодействия между «Агрегатором» и «Универсальным диспетчером» |
| AGGREGATOR_ACCESS_TOKEN_TTL_SECONDS | 600 | Параметр обязателен и задается на узлах с установленным «Агрегатором».<br>Определяет времени жизни (в секундах) JWT-токена, подписанного «Агрегатором» |
| AGGREGATOR_IMAGE_CACHE_LIFETIME_HOURS | 672 | Параметр обязателен и задается на узлах с установленным «Агрегатором».<br>Определяет время жизни (в часах) кеша иконок фондов РМ. По истечении этого времени иконка обновляется |
| Настройки подключения к хранилищу паролей OpenBao | | |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| SECRETS_STORAGE_METHOD | Не задано | Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет способ хранения паролей подключения к СУБД и RabbitMQ:<br>▪ `config` - пароли будут храниться в преобразованном виде в файле `/etc/opt/termidesk-vdi/termidesk.conf`;<br>▪ `hvac` - для хранения паролей будет использоваться хранилище паролей OpenBao или Hashicorp Vault (хранилище должно быть заранее создано и настроено). Подробная информация по этому способу хранения паролей приведена в подразделе **Хранение чувствительной информации с выбранным способом хранения «hvac»** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»;<br>▪ `openbao` - для хранения паролей будет использоваться хранилище паролей OpenBao (хранилище должно быть заранее создано и настроено). При этом пароли располагаются внутри хранилища, имена контейнеров хранения генерируются автоматически.<br>Хранилище паролей OpenBao должно быть реализовано в отказоустойчивом варианте, иначе Termidesk не будет работать в период простоя узлов OpenBao.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_URL | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет IP-адреса или FQDN узла и порта с установленным хранилищем OpenBao.<br>Параметр задается, если для `SECRETS_STORAGE_METHOD` задано значение `openbao` или `hvac`.<br>Формат: `http://<IP-адрес или FQDN>:8200`. Подключение может выполняться по протоколу HTTPS, если OpenBao настроен соответствующим образом.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_TOKEN | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет токен (Initial Root Token), сформированный при инициализации хранилища OpenBao.<br>Параметр задается, если для `SECRETS_STORAGE_METHOD` задано значение `openbao` или `hvac`.<br>Начальное значение задается на этапе установки и хранится в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` в преобразованном виде.<br>Для преобразования значения параметра, заданного вручную, следует воспользоваться утилитой `scramble`:<br>▪ для получения значения по стандартному алгоритму:<br>`/opt/termidesk/bin/scramble --value <пароль> --type AES256`<br>▪ для получения значения с увеличенным числом итераций преобразования:<br>`/opt/termidesk/bin/scramble --value <пароль> --type AES256_V2`<br>Если значение пароля указывается в формате ключа (значение предваряется символом «-»), то следует изменить его передачу в параметр `--value`:<br>`/opt/termidesk/bin/scramble --value=<-пароль> --type AES256` |
| SECRETS_OPENBAO_DB_PATH | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет путь, настроенный на OpenBao для хранения пароля СУБД.<br>Параметр задается, если для `SECRETS_STORAGE_METHOD` задано значение `openbao` или `hvac`.<br>Начальное значение задается на этапе установки |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| SECRETS_OPENBAO_DB_ROLE_NAME | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет роль, настроенную на OpenBao и имеющую доступ к паролю СУБД.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_RABBITMQ_PATH | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора»».<br>Определяет путь, настроенный на OpenBao для хранения пароля RabbitMQ.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_RABBITMQ_ROLE_NAME | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет роль, настроенную на OpenBao и имеющую доступ к паролю RabbitMQ.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_CLIENT_CERT | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет путь к сертификату mTLS для защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы.<br>Для использования сертификата нужно:<br>▪ скопировать его в каталог /etc/opt/termidesk-vdi/;<br>▪ назначить владельцем файла пользователя termidesk:<br>sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.crt<br>▪ изменить права на файл:<br>sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.crt<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.<br>Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:<br>SECRETS_OPENBAO_CLIENT_CERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem' |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| SECRETS_OPENBAO_CLIENT_KEY | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет путь к ключу mTLS для защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы.<br>Ключ может иметь парольную защиту. Для использования ключа в Termidesk нужно преобразовать его к начальному значению:<br>`openssl rsa -in <путь_к_файлу_ключа.key> -out <путь_сохранения_преобразованного_ключа.key>`<br>Для использования ключа также нужно:<br>▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;<br>▪ назначить владельцем файла пользователя `termidesk`:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.key`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.key`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.<br>Ключ может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:<br>`SECRETS_OPENBAO_CLIENT_KEY='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/key'` |
| SECRETS_OPENBAO_SERVER_CERT | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет путь к промежуточному сертификату ЦС mTLS для защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы.<br>Для использования сертификата нужно:<br>▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;<br>▪ назначить владельцем файла пользователя `termidesk`:<br>`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<имя>.pem`<br>▪ изменить права на файл:<br>`sudo chmod 600 /etc/opt/termidesk-vdi/<имя>.pem`<br>▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.<br>Сертификат может быть расположен в специальном хранилище паролей, в этом случае указывается путь к нему (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**). Пример задания сертификата из хранилища:<br>`SECRETS_OPENBAO_SERVER_CERT='hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem'` |
| SECRETS_OPENBAO_TERMIDESK_PATH | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет путь, настроенный на OpenBao для хранения паролей Termidesk.<br>Параметр задается, если для `SECRETS_STORAGE_METHOD` задано значение `openbao` или `hvac`.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_TERMIDESK_ROLE_NAME | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет роль, настроенную на OpenBao и имеющую доступ к паролям Termidesk.<br>Параметр задается, если для `SECRETS_STORAGE_METHOD` задано значение `openbao` или `hvac`.<br>Начальное значение задается на этапе установки |

| Параметр | Значение по умолчанию | Описание |
|---|---|---|
| SECRETS_OPENBAO_KV_VERSION | 1 | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Используется для указания версии API OpenBao.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac.<br>Возможные значения:<br>▪ 1 (по умолчанию);<br>▪ 2.<br>Начальное значение задается на этапе установки |
| SECRETS_OPENBAO_CACHE_LIFETIME | 5 | Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Агрегатора».<br>Определяет время (в секундах) хранения пароля, полученного от OpenBao, во внутренней памяти. Позволяет сохранить полученный от OpenBao пароль на некоторое время в кеше для сокращения количества обращений к OpenBao.<br>Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao или hvac.<br>Начальное значение задается на этапе установки |
| Настройки взаимодействия с узлом «Ретранслятора» | | |
| FLUENTD_CACHE | 15 | Параметр может быть задан на узлах «Универсального диспетчера».<br>Определяет время (в секундах) кеширования параметров подключения к узлу «Ретранслятора».<br>По умолчанию после установки время кеширования составляет 15 секунд.<br>В случае, если нужно изменить значение, следует раскомментировать параметр и задать ему новое значение |
| FLUENTD_TABLE | logs | Параметр может быть задан на узлах «Универсального диспетчера».<br>Определяет таблицу хранения событий фермы Termidesk.<br>По умолчанию после установки «Универсальный диспетчер» обращается к таблице «logs» БД «Ретранслятора».<br>В случае, если в БД «Ретранслятора» для хранения событий используется другая таблица, следует раскомментировать параметр и указать новое имя таблицы |
| Настройки «Шлюза» | | |
| WSPROXY_PUB_KEY_FILE | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора».<br>Задает путь к открытому ключу id_rsa.pub. Используется для подписи токенов при взаимной аутентификации «Шлюза» и «Универсального диспетчера», «Агрегатора».<br>По умолчанию создается при первой установке и хранится в подкаталоге wsproxy. Явно задавать путь следует только при использовани внешнего хранилища (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**).<br>Пример:<br>WSPROXY_PUB_KEY_FILE='hvac-kv://secret#termidesk-admin/wsproxy/pub' |
| WSPROXY_PRIV_KEY_FILE | Не задано | Параметр может быть задан на узлах «Универсального диспетчера», «Агрегатора».<br>Задает путь к закрытому ключу id_rsa. Используется для подписи токенов при взаимной аутентификации «Шлюза» и «Универсального диспетчера», «Агрегатора».<br>По умолчанию создается при первой установке и хранится в подкаталоге wsproxy. Явно задавать путь следует только при использовани внешнего хранилища (см. подраздел **Хранение чувствительной информации с выбранным способом хранения «hvac»**).<br>Пример:<br>WSPROXY_PRIV_KEY_FILE='hvac-kv://secret#termidesk-admin/wsproxy/priv' |

## 12.3 . Утилиты интерфейса командной строки для настройки Агрегатора

### 12.3.1 . Утилита termidesk-config

Утилита `termidesk-config` используется для переопределения настроек, заданных на этапе установки, и вносит изменения в конфигурационный файл `/etc/opt/termidesk-vdi/termidesk.conf` (см. подраздел **Параметры конфигурирования компонентов «Универсальный диспетчер», «Менеджер рабочих мест»**).

Для вызова утилиты следует:

- в интерфейсе командной строки перейти в каталог `/opt/termidesk/sbin/`:

```
cd /opt/termidesk/sbin/
```

- выполнить запуск:

```
sudo ./termidesk-config
```

- откроется интерфейс утилиты (см. Рисунок 9).

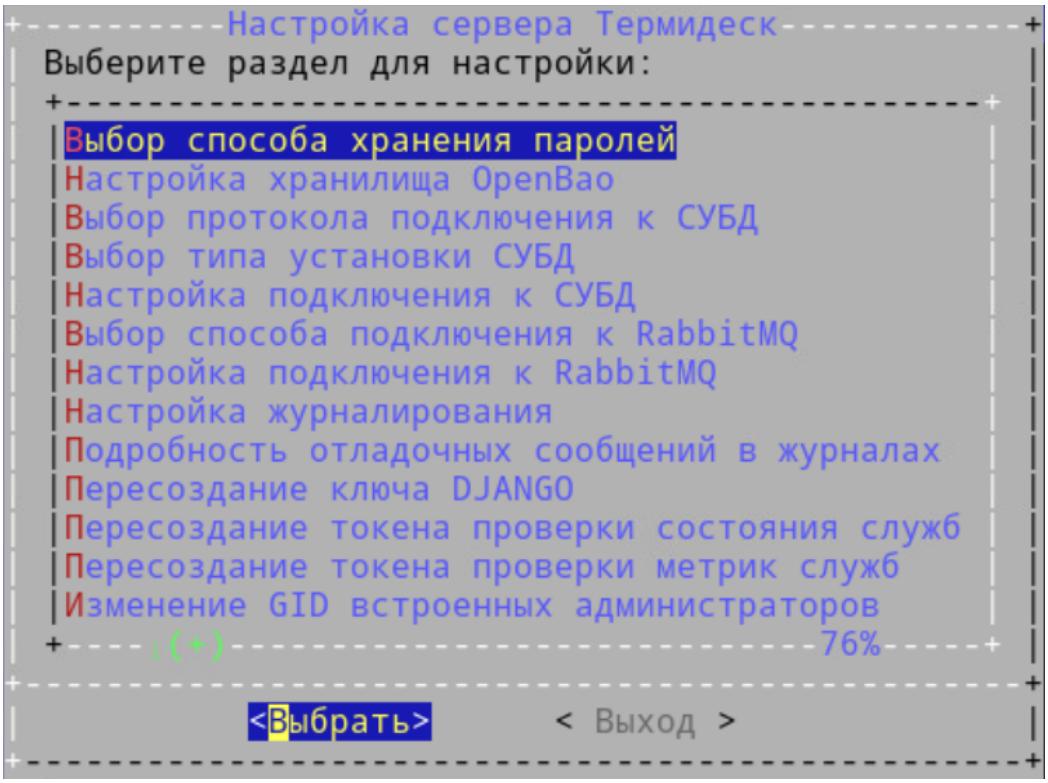



Рисунок 9 – Интерфейс утилиты termidesk-config

Доступны следующие функции утилиты:

- «Выбор способа хранения паролей»: позволяет настроить способ хранения паролей подключения к СУБД и RabbitMQ (параметр `SECRETS_STORAGE_METHOD`):

- «config» - пароли будут храниться в преобразованном виде в файле `/etc/opt/termidesk-vdi/termidesk.conf`;
- «hvac» (рекомендуемый способ для безопасного хранения) - для хранения паролей будет использоваться хранилище паролей OpenBao или Hashicorp Vault (хранилище должно быть заранее создано и настроено);
- «openbao» - для хранения паролей будет использоваться хранилище паролей OpenBao (хранилище должно быть заранее создано и настроено).

В случае выбора «openbao» необходимо выполнить настройку подключения к хранилищу через функцию «Настройка хранилища OpenBao»;

- «Настройка хранилища OpenBao»: позволяет настроить параметры подключения к хранилищу и задать параметры, настроенные непосредственно на хранилище:
  - «URL хранилища» - IP-адрес или FQDN узла и порт с установленным хранилищем OpenBao (параметр `SECRETS_OPENBAO_URL`). Формат: `http://<IP-адрес>:8200` или `http://<FQDN>:8200`. Подключение может выполняться по протоколу HTTPS, если OpenBao настроен соответствующим образом;
  - «Версия API OpenBao» - установленная версия API на OpenBao (параметр `SECRETS_OPENBAO_KV_VERSION`). Может принимать значения: «1» или «2»;
  - «Токен доступа к хранилищу» - токен (Initial Root Token), который был сформирован при инициализации хранилища (параметр `SECRETS_OPENBAO_TOKEN`);
  - «Путь к паролю СУБД» - путь, настроенный на OpenBao для хранения пароля СУБД (параметр `SECRETS_OPENBAO_DB_PATH`);
  - «Роль доступа к паролю СУБД» - роль, настроенная на OpenBao, которая имеет доступ к паролю СУБД (параметр `SECRETS_OPENBAO_DB_ROLE_NAME`);
  - «Путь к паролям RabbitMQ» - путь, настроенный на OpenBao для хранения пароля RabbitMQ (параметр `SECRETS_OPENBAO_RABBITMQ_PATH`);
  - «Роль доступа к паролям RabbitMQ» - роль, настроенная на OpenBao, которая имеет доступ к паролю RabbitMQ (параметр `SECRETS_OPENBAO_RABBITMQ_ROLE_NAME`);
  - «Путь к паролям Termidesk» - путь, настроенный на OpenBao для хранения пароля Termidesk (параметр `SECRETS_OPENBAO_TERMIDESK_PATH`);
  - «Роль доступа к паролям Termidesk» - роль, настроенная на OpenBao, которая имеет доступ к паролю Termidesk (параметр `SECRETS_OPENBAO_TERMIDESK_ROLE_NAME`);
  - «Время кеширования паролей, сек» - время (в секундах) хранения пароля, полученного от OpenBao, во внутренней памяти (параметр `SECRETS_OPENBAO_CACHE_LIFETIME`);
- «Выбор протокола подключения к СУБД»: позволяет выбрать протокол при подключении к СУБД (параметр `DBSSL`);

- «Выбор типа установки СУБД»: позволяет выбрать тип СУБД, к которой будет подключаться Termidesk (параметр DB_CLUSTER_MODE);
- «Настройка подключения к СУБД»: позволяет настроить параметры подключения к СУБД:
  - «Адрес СУБД» - IP-адрес или FQDN СУБД PostgreSQL (параметр DBHOST);
  - «Адрес СУБД (узел 2)»: IP-адрес или FQDN дополнительного узла СУБД (параметр DBHOST2);
  - «Адрес СУБД (узел 3)»: IP-адрес или FQDN дополнительного узла СУБД (параметр DBHOST3);
  - «Порт СУБД» - порт, который используется для соединения с сервером БД (параметр DBPORT);
  - «Имя базы данных» - имя БД (параметр DBNAME);
  - «Имя пользователя» - имя пользователя для подключения к БД (параметр DBUSER);
  - «Пароль» - пароль пользователя в открытом виде (параметр DBPASS);
- «Выбор способа подключения к RabbitMQ»: позволяет выбрать протокол при подключении к RabbitMQ (параметр RABBITMQ_SSL);
- «Настройка подключения к RabbitMQ»: позволяет настроить параметры подключения к RabbitMQ (параметр RABBITMQ_URL). При запросе пароль задается в открытом виде;
- «Настройка журналирования»: позволяет настроить параметры журналирования, такие как «Адрес логгера» (параметр LOG_ADDRESS), «Поток (facility) журнала» (параметр LOG_FACILITY);
- «Подробность отладочных сообщений в журналах»: позволяет выбрать уровень подробности отладочных сообщений (параметр LOG_LEVEL);
- «Пересоздание ключа DJANGO»: позволяет переопределить значение ключа DJANGO (параметр DJANGO_SECRET_KEY), создаваемого на этапе установки. Переопределение ключа может понадобиться при его компрометации;
- «Пересоздание я токена проверки состояния служб»: позволяет переопределить значение токена проверки состояния служб (параметр HEALTH_CHECK_ACCESS_KEY). Переопределение токена может понадобиться при его компрометации;
- «Пересоздание токена проверки метрик служб»: позволяет переопределить значение токена проверки метрики служб (параметр METRICS_ACCESS_KEY). Переопределение токена может понадобиться при его компрометации;
- «Изменение GID встроенных администраторов»: позволяет назначить идентификатор группы, использующегося для встроенного домена. Изменение идентификатора может понадобиться, если встроенная в ОС группа администраторов отличается от astra-admin (1001) или если нужно предоставить права администрирования Termidesk группе непривилегированных пользователей;

- «Настройки Агрегатора»: позволяет переопределить настройки портала «Агрегатор»:
  - «Время жизни токена Агрегатора, секунд» - время жизни JWT-токена (параметр `AGGREGATOR_ACCESS_TOKEN_TTL_SECONDS`, доступная для изменения только на узле с установленным порталом «Агрегатор»);
  - «Заголовок JWT-токена Агрегатора» - заголовок JWT-токена, предназначенный для настройки взаимодействия между порталом «Агрегатор» и «Универсальным диспетчером». Параметр должен быть одинаковым на всех узлах, работающих совместно: на порталах «Агрегатора», на «Универсальных диспетчерах» (параметр `AGGREGATOR_ACCESS_TOKEN_TITLE`);
  - «Время кеширования иконок фондов, часов» - время жизни кеша иконок фондов (параметр `AGGREGATOR_IMAGE_CACHE_LIFETIME_HOURS`);
- «Роли сервера»: позволяет изменить роли, которые запускаются на узле. Доступные роли: «Портал администратора», «Портал пользователя», «Менеджер рабочих мест», «Агрегатор администратора», «Агрегатор пользователя»;

Установка ролей «Агрегатор администратора» и (или) «Агрегатор пользователя» должна производиться на узле, отличном от «Портала администратора» и (или) «Портала пользователя», «Менеджера рабочих мест».
Смена ролей через функцию «Роли сервера» в этом случае не предусмотрена: нельзя ранее установленные «Портал администратора» и (или) «Портал пользователя» перенастроить на использование ролей «Агрегатор администратора» и (или) «Агрегатор пользователя».

- «Перезапуск служб» - позволяет выполнить перезапуск служб Termidesk;
- «Сертификаты» - позволяет выполнить настройку сертификатов и ключей:

Пункт «Серт. для расшифровки JWT-токена» настраивается только на узле с установленным «Универсальным диспетчером» («Портал администратора» и (или) «Портал пользователя») фермы Termidesk.
Пункт «Прив. ключ для подписи JWT-токена» настраивается только на узле портала «Агрегатор» («Агрегатор администратора» и (или) «Агрегатор пользователя»).
Оставшиеся пункты могут быть настроены на обоих узлах индивидуально.

  - «Сертификат Health Check» - путь к сертификату для защищенного подключения к API проверки состояния (параметр `HEALTH_CHECK_CERT`);
  - «Секр. ключ Health Check» - путь к ключу для защищенного подключения к API проверки состояния (параметр `HEALTH_CHECK_KEY`);
  - «Сертификат Postgres mTLS» - путь к сертификату для защищенного подключения к СУБД (параметр `DBCERT`);
  - «Секр. ключ Postgres mTLS» - путь к ключу для защищенного подключения к СУБД (параметр `DBKEY`);

- «Серт. промеж. ЦС Postgres mTLS» - путь к корневому и промежуточным сертификатам mTLS для защищенного подключения к СУБД (параметр `DBCHAIN`);
- «Сертификат OpenBao mTLS» - путь к сертификату для защищенного подключения к OpenBao (параметр `SECRETS_OPENBAO_CLIENT_CERT`);
- «Секр. ключ OpenBao mTLS» - путь к ключу для защищенного подключения к OpenBao (параметр `SECRETS_OPENBAO_CLIENT_KEY`);
- «Серт. промеж. ЦС OpenBao mTLS» - путь к корневому и промежуточным сертификатам mTLS для защищенного подключения к OpenBao (параметр `SECRETS_OPENBAO_SERVER_CERT`);
- «Осн. серт. для расшифровки JWT-токена» - путь к сертификату для получения значения JWT-токена портала «Агрегатор» (параметр `AGGREGATOR_JWT_SSL_CERT`);
- «Рез. серт. для расшифровки JWT-токена» - путь к резервному сертификату для получения значения JWT-токена портала «Агрегатор» (параметр `AGGREGATOR_JWT_SSL_CERT_SECOND`);
- «Секр. ключ для подписи JWT-токена» - путь к ключу для подписи JWT-токена портала «Агрегатор» (параметр `AGGREGATOR_JWT_SSL_KEY`);
- «Сертификат для подключения к серверу RA» - путь к серверному сертификату SSL/TLS для проверки подключения к «Удаленному помощнику» (`REMOTE_ASSISTANT_SERVER_CERT`);
- «Сертификат RabbitMQ mTLS» - путь к клиентскому сертификату SSL/TLS для защищенного подключения к RabbitMQ (`CELERY_BROKER_CERT`);
- «Секр.ключ RabbitMQ mTLS» - путь к клиентскому ключу SSL/TLS для защищенного подключения к RabbitMQ (`CELERY_BROKER_KEY`);
- «Серт. ЦС RabbitMQ mTLS» - путь к корневому сертификату ЦС SSL/TLS для защищенного подключения к RabbitMQ (`CELERY_BROKER_CA`);
- «Публичный ключ ws-proxy»: путь к открытому ключу `id_rsa.pub`. Явно задавать путь следует только при использовани внешнего хранилища (`WSPROXY_PUB_KEY_FILE`);
- «Секретный ключ ws-proxy»: путь к озакрытому ключу `id_rsa`. Явно задавать путь следует только при использовани внешнего хранилища (`WSPROXY_PRIV_KEY_FILE`);

- «Перезапуск служб»: позволяет выполнить перезапуск служб Termidesk.

> После выполнения изменений в любом из разделов рекомендуется воспользоваться пунктом «Перезапуск служб» для применения изменений.

# 13 . КОНСОЛЬ УПРАВЛЕНИЯ ФЕРМАМИ

## 13.1 . Общие сведения по управлению из консоли

Консоль управления фермами предназначена для централизованного администрирования фондов РМ, сессий и индивидуальных РМ.

⚠ Доступ к разделу «Консоль управления фермами» определяется политикой «Доступ к Консоли управления фермами» (см. подраздел **Управление ролями**).

Раздел предоставляет доступ к следующим функциональным возможностям:

- «Фонды» - отображает сведения о фондах РМ, размещенных в фермах поставщиков ресурсов; позволяет управлять политиками и режимом техобслуживания фондов РМ;
- «Сессии» - отображает сведения о сессиях; позволяет управлять их состоянием, выполнять подключение к активным сессиям пользователей через компонент «Удаленный помощник»;
- «Индивидуальные рабочие места» - отображает сведения о РМ из всех фондов; позволяет управлять состоянием и режимом техобслуживания РМ.

## 13.2 . Управление фондами РМ

Для отображения списка фондов РМ следует перейти «Консоль управления фермами - Фонды». Основные параметры списка приведены в Агрегатор. Управление фондами.

⚠ Доступ к разделу «Фонды» определяется разрешениями «Доступ к Консоли управления фермами» и «Доступ к фондам в Консоли управления фермами» (см. подраздел **Управление ролями**).

Таблица 24 – Параметры списка фондов РМ

| Параметр | Описание |
|---|---|
| «Фонд рабочих мест» | Наименование фонда РМ |
| «Ферма» | Наименование фермы, в составе которой находится фонд РМ |
| «Статус» | Состояние готовности фонда РМ |
| «Места» | Общее количество РМ в фонде |
| «Готовятся» | Количество подготавливаемых РМ |
| «Выбор протокола» | Флаг возможности выбора пользователем протокола доставки при работе с фондом РМ.<br>Значение определяется политикой фонда РМ «Выбор пользователем протокола доставки» |
| «Группа рабочих мест» | Принадлежность фонда группе РМ |
| «Шаблон» | Шаблон РМ, примененный в фонде |

| Параметр | Описание |
|---|---|
| «Комментарий» | Информационное сообщение, используемое для описания назначения фонда РМ |

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца.
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Над фондом РМ можно выполнять следующие действия:

- управлять политиками фонда РМ (см. подраздел **Политики фонда РМ** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»);
- редактировать фонд РМ (см. подраздел **Общие сведения о фонде РМ** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»);
- управлять режимом техобслуживания фонда РМ (см. подраздел **Режим техобслуживания фонда для ВРМ** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»).

### 13.3 . Управление сессиями

Для отображения списка сессий следует перейти «Консоль управления фермами - Сессии». Основные параметры списка приведены в таблице (см. Таблица 25).

> ⚠ Доступ к разделу «Сессии» определяется разрешениями «Доступ к Консоли управления фермами» и «Доступ к сессиям в Консоли управления фермами» (см. подраздел **Управление ролями**).

Таблица 25 – Параметры списка сессий

| Параметр | Описание |
|---|---|
| «Дата и время» | Дата и время входа пользователя на РМ |
| «Пользователь» | Имя пользователя, которому было выдано РМ |
| «IP-адрес» | IP-адрес инициатора сессии |
| «Хост» | Наименование инициатора сессии |
| «Место» | Наименование РМ, выданного пользователю |
| «IP места» | IP-адрес РМ, выданного пользователю |
| «ИД места» | Идентификатор РМ, выданного пользователю |
| «Фонд» | Наименование фонда, в составе которого находится выданное РМ |
| «Ферма» | Наименование фермы, в составе которой находится выданное РМ |

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**;
- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца.
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Подробные сведения о доступных действиях над сессиями содержатся в подразделе **Управление активными сессиями** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

### 13.4 . Управление индивидуальными рабочими местами

Для отображения списка РМ из всех фондов следует перейти «Консоль управления фермами - Индивидуальные рабочие места». Основные параметры списка приведены в таблице (см. Таблица 26).

⚠ Доступ к разделу «Индивидуальные рабочие места» определяется разрешениями «Доступ к Консоли управления фермами» и «Доступ к индивидуальным рабочим местам в Консоли управления фермами» (см. подраздел **Управление ролями**).

Таблица 26 – Параметры списка индивидуальных рабочих мест

| Параметр | Описание |
|---|---|
| «Дата и время создания» | Временная метка выполнения публикации РМ |
| «Уникальный ИД» | Уникальный идентификатор РМ: MAC-адрес или номер сессии |
| «Редакция» | Порядковый номер версии публикации |
| «IP-адрес» | IP-адрес, назначенный РМ |
| «Название» | Наименование РМ |
| «Уровень кеша» | Уровень кеша, на котором находится РМ |
| «Дата и время последнего логина» | Временная метка последней успешной аутентификации пользователя |
| «Фонд» | Наименование фонда РМ и ссылка на него |
| «Ферма» | Наименование фермы, в составе которой находится РМ |
| «Статус» | Флаг использования публикации РМ из фонда РМ |
| «Статус обновлен» | Временная метка обновления статуса |
| «Используется» | Флаг назначения РМ. Значение «Нет» свидетельствует о том, что РМ находится в кеше |
| «Хост источника» | Наименование инициатора выдачи РМ |
| «IP источника» | IP-адрес инициатора выдачи РМ |
| «Владелец» | Субъект, запросивший выдачу РМ |
| «Версия агента» | Версия компонента «Агент», установленного в гостевой ОС РМ |

Поддерживается:

- обновление значений таблицы, для этого используется графический элемент . Для задания периода обновления или его отключения следует использовать выпадающий список со значениями интервала в минутах, расположенный рядом с указанным элементом;
- поиск записей по таблице;
- изменение внешнего вида таблицы.

Внешний вид таблицы можно модифицировать, изменив:

- список отображаемых столбцов. Для изменения списка нужно воспользоваться графическим элементом и отметить наименования столбцов, которые будут отображены, или снять

отметку с наименований, которые должны быть скрыты из отображения. Для возврата к исходному состоянию отображения следует воспользоваться экранной кнопкой **[Сбросить]**;

- ширину столбцов. Для изменения ширины нужно нажать и удерживать левую кнопку мыши на границе столбцов, перемещая ее в сторону расширения или сужения столбца.
- сортировку записей. Для сортировки нужно воспользоваться графическим элементом для соответствующего столбца.

Подробные сведения о доступных действиях над РМ содержатся в подразделе **Управление состоянием ВМ в назначенном фонде РМ** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

# 14 . СИСТЕМА АУДИТА

## 14.1 . Журналы

Журналы «Агрегатора» хранятся в каталоге `/var/log/termidesk`.

Установлены следующие журналы «Агрегатора», разделенные по типам записываемых в них событий:

- `auth.log` - записываются события об авторизации субъектов в «Агрегаторе»;
- `celery-beat.log` - записываются события периодической проверки состояния обработчика заданий через RabbitMQ. Поддерживается автоматическая ротация журнала для исключения возможности переполнения пространства диска;
- `celery-worker.log` - записываются события обработчика заданий через RabbitMQ. Поддерживается автоматическая ротация журнала для исключения возможности переполнения пространства диска;
- `other.log` - записываются события модулей «Агрегатора»;
- `database.log` - записываются отладочные события БД;
- `termidesk.log` - записываются события работы компонента «Универсальный диспетчер»;
- `use.log` - записываются события подключения пользователей к ресурсам;
- `aggregator.log` - записываются события работы «Агрегатора».

## 14.2 . Настройка журналирования

Уровень журналирования задается параметром `LOG_LEVEL` в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf`.

Для изменения уровня журналирования нужно:

- изменить параметр `LOG_LEVEL`;
- перезапустить службы:

```
sudo systemctl restart termidesk-vdi.service termidesk-celery-beat.service termidesk-celery-worker.service
```

## 14.3 . Просмотр журналов

### 14.3.1 . Просмотр системного журнала

Для просмотра общего журнала событий, связанного с функционированием «Агрегатора» и действиями субъектов доступа, следует перейти «Журналы - Системные журналы» (см. Рисунок 10), где визуализируются системные события с указанием уровня важности и источника возникновения события. На странице поддерживается поиск записей по таблице.

Системный журнал может быть выгружен в `csv`-файл при помощи графического элемента , при этом поддерживается:

- выгрузка всех событий;
- выгрузка событий текущей страницы.

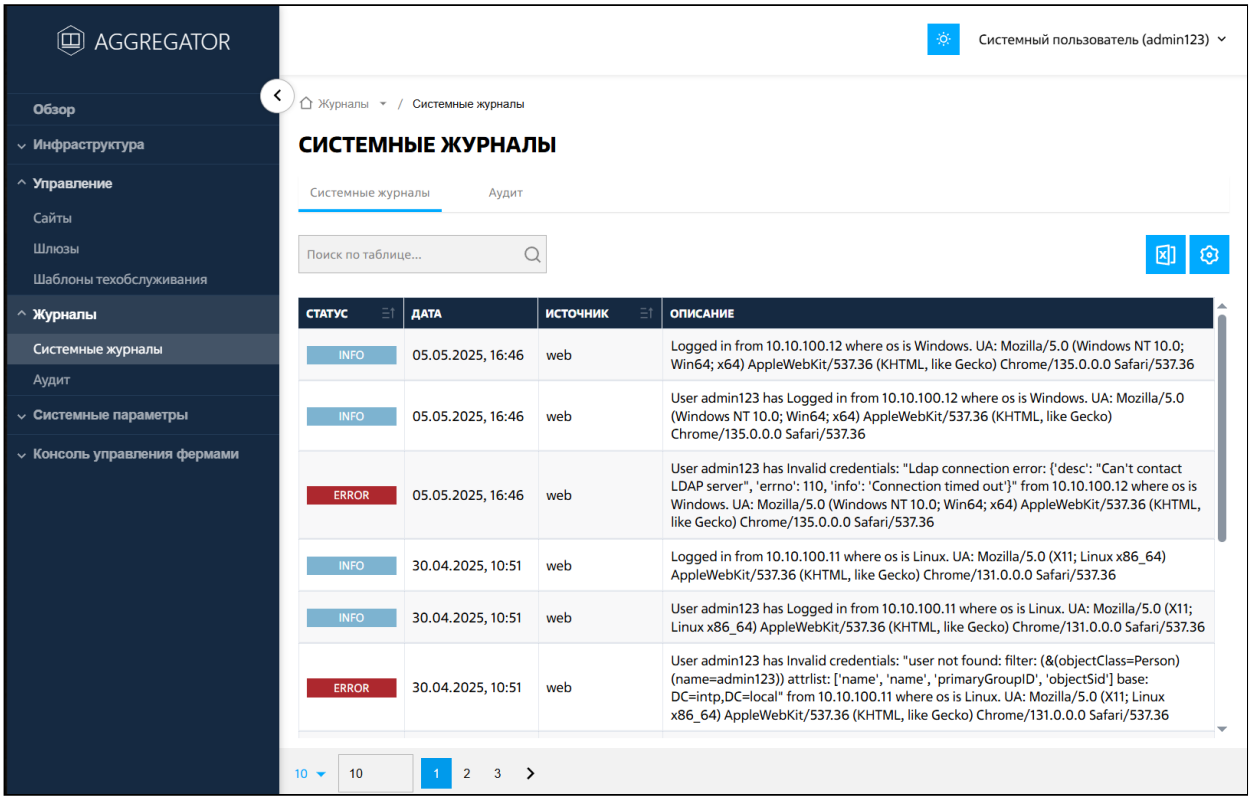



Рисунок 10 – Отображение общего журнала событий

### 14.3.2 . Просмотр журнала аудита

Для просмотра журнала событий, связанного с действиями субъектов доступа, следует перейти «Журналы - Аудит» (см. Рисунок 11). На странице поддерживается поиск записей по таблице.

Журналу аудита может быть выгружен в csv-файл при помощи графического элемента , при этом поддерживается:

- выгрузка всех событий;
- выгрузка событий текущей страницы.

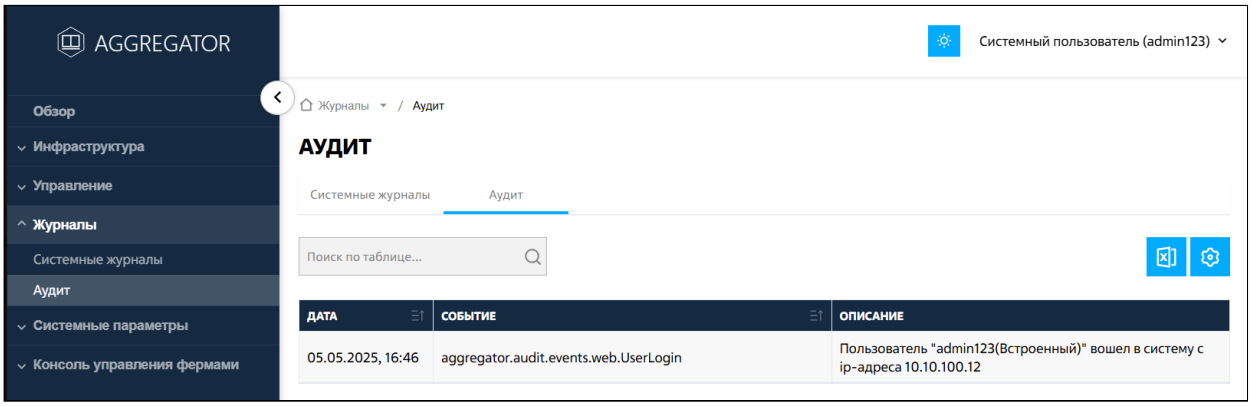



Рисунок 11 – Отображение журнала аудита

## 14.4 . Описание шаблонов событий аудита

### 14.4.1 . Типы данных регистрируемой информации событий аудита

При фиксации событий аудита используется ряд типов данных (см. Таблица 27) регистрируемой информации, состав которых может отличаться для разных событий.

Таблица 27 – Типы данных регистрируемой информации

| Тип данных | Описание |
|---|---|
| Дата/время | Дата и время указываются в формате: `DD.MM.YYYY, hh:mm:ss`, где:<br>`DD.MM.YYYY` обозначает «день» - «месяц» - «год»;<br>`hh:mm:ss` обозначает элементы времени «час» - «минута» - «секунда»;<br>«`.`» и «`:`» используются как разделители в обозначениях даты и времени дня соответственно |
| Имя/логин | Идентификационные данные субъекта, совершающего доступ к объекту |
| Наименование параметра/секции/политики | Указывает объект, над которым производится действие |
| Значение | Указывается значение, которое принимал или принял объект после выполнения над ним операции |
| Тип объекта/сущности | Указывает тип объекта, над которым производится действие |
| Действие | Название операции, которую совершил субъект над объектом |
| Результат | Результат выполнения действия |
| Уровень важности | Показатель критичности события |
| Идентификатор | Указывают уникальную (для соответствующего объекта) последовательность чисел для его однозначной идентификации |
| IP-адрес | 32-битовое число. Формой записи IP-адреса является запись в виде четырех десятичных чисел значением от 0 до 255, разделенных точками (например, 192.0.2.1) |

### 14.4.2 . Типы и шаблоны регистрируемых событий аудита

Список регистрируемых событий аудита и шаблоны к ним приведены в таблице (см. Таблица 28).

Таблица 28 – Список типов и шаблонов регистрируемых событий аудита

| Событие | Состав регистрируемой информации | Шаблон регистрации события |
|---|---|---|
| **События, связанные с объектом «Узлы»** | | |
| Добавление узла<br>`aggregator.audit.events.provider.create` | Регистрируется:<br>▪ название узла (`provider_name`);<br>▪ имя пользователя (`username`);<br>▪ название домена аутентификации (`authenticator_name`);<br>▪ название фермы поставщиков ресурсов (`farm_name`) | «Пользователь `[username]` (`[authenticator_name]`) создал узел `[provider_name]`в ферме `[farm_name]`» |
| Изменение узла<br>`aggregator.audit.events.provider.update` | Регистрируется:<br>▪ название узла (`provider_name`);<br>▪ имя пользователя (`username`);<br>▪ название домена аутентификации (`authenticator_name`);<br>▪ название фермы поставщиков ресурсов (`farm_name`) | «Пользователь `[username]` (`[authenticator_name]`) обновил узел `[provider_name]`в ферме `[farm_name]`» |
| Удаление узла<br>`aggregator.audit.events.provider.delete` | Регистрируется:<br>▪ название узла (`provider_name`);<br>▪ имя пользователя (`username`);<br>▪ название домена аутентификации (`authenticator_name`);<br>▪ название фермы поставщиков ресурсов (`farm_name`) | «Пользователь `[username]` (`[authenticator_name]`) удалил узел `[provider_name]`из фермы `[farm_name]`» |
| **События, связанные с объектом «Ферма поставщик ресурсов»** | | |
| Добавление фермы поставщиков ресурсов<br>`aggregator.audit.events.farms.create` | Регистрируется:<br>▪ название фермы поставщиков ресурсов (`farm_name`);<br>▪ название домена аутентификации (`authenticator_name`);<br>▪ имя пользователя (`username`) | «Пользователь `[username]` (`[authenticator_name]`) создал ферму `[farm_name]`» |
| Изменение фермы поставщиков ресурсов<br>`aggregator.audit.events.farms.update` | Регистрируется:<br>▪ название фермы поставщиков ресурсов (`farm_name`);<br>▪ название домена аутентификации (`authenticator_name`);<br>▪ имя пользователя (`username`) | «Пользователь `[username]` (`[authenticator_name]`) обновил ферму `[farm_name]`» |
| Удаление фермы поставщиков ресурсов<br>`aggregator.audit.events.farms.delete` | Регистрируется:<br>▪ название фермы поставщиков ресурсов (`farm_name`);<br>▪ название домена аутентификации (`authenticator_name`);<br>▪ имя пользователя (`username`) | «Пользователь `[username]` (`[authenticator_name]`) удалил ферму `[farm_name]`» |
| **События, связанные с объектом «Сайт»** | | |
| Добавление сайта<br>`aggregator.audit.events.site.create` | Регистрируется:<br>▪ название сайта (`site_name`);<br>▪ название домена аутентификации (`authenticator_name`);<br>▪ имя пользователя (`username`) | «Пользователь `[username]` (`[authenticator_name]`) создал сайт `[site_name]`» |
| Изменение сайта<br>`aggregator.audit.events.site.update` | Регистрируется:<br>▪ название сайта (`site_name`);<br>▪ название домена аутентификации (`authenticator_name`);<br>▪ имя пользователя (`username`) | «Пользователь `[username]` (`[authenticator_name]`) обновил сайт `[site_name]`» |

| | | |
|---|---|---|
| Удаление сайта<br>aggregator.audit.events.site.delete | Регистрируется:<br>▪ название сайта (site_name);<br>▪ название домена аутентификации (authenticator_name);<br>▪ имя пользователя (username) | «Пользователь [username] ([authenticator_name]) удалил сайт [site_name]» |
| Добавление правила<br>aggregator.audit.events.rule.create | Регистрируется:<br>▪ имя пользователя (username);<br>▪ название домена аутентификации (authenticator_name);<br>▪ название правила для сайта (rule_name);<br>▪ название сайта (site_name) | «Пользователь [username] ([authenticator_name]) создал правило [rule_name] в сайте [site_name]» |
| Изменение правила<br>aggregator.audit.events.rule.update | Регистрируется:<br>▪ имя пользователя (username);<br>▪ название домена аутентификации (authenticator_name);<br>▪ название правила для сайта (rule_name);<br>▪ название сайта (site_name) | «Пользователь [username] ([authenticator_name]) обновил правило [rule_name] в сайте [site_name]» |
| Удаление правила<br>aggregator.audit.events.rule.delete | Регистрируется:<br>▪ имя пользователя (username);<br>▪ название домена аутентификации (authenticator_name);<br>▪ название правила для сайта (rule_name);<br>▪ название сайта (site_name) | «Пользователь [username] ([authenticator_name]) удалил правило [rule_name] в сайте [site_name]» |
| **События, связанные с объектом «Шлюз»** | | |
| Добавление шлюза<br>aggregator.api.webui.gateway.create | Регистрируется:<br>▪ название шлюза (gateway_name);<br>▪ имя пользователя (username);<br>▪ название домена аутентификации (authenticator_name) | «Пользователь [username] ([authenticator_name]) создал шлюз [gateway_name]» |
| Изменение шлюза<br>aggregator.api.webui.gateway.update | Регистрируется:<br>▪ название шлюза (gateway_name);<br>▪ имя пользователя (username);<br>▪ название домена аутентификации (authenticator_name) | «Пользователь [username] ([authenticator_name]) обновил шлюз [gateway_name]» |
| Удаление шлюза<br>aggregator.api.webui.gateway.delete | Регистрируется:<br>▪ название шлюза (gateway_name);<br>▪ имя пользователя (username);<br>▪ название домена аутентификации (authenticator_name) | «Пользователь [username] ([authenticator_name]) удалил шлюз [gateway_name]» |
| **События, связанные с объектом «Домен аутентификации»** | | |
| Создание домена аутентификации<br>aggregator.audit.events.authenticators.create | Регистрируется:<br>▪ название домена аутентификации (authenticator_name);<br>▪ имя пользователя (username) | «Пользователь [username] ([authenticator_name]) создал аутентификатор [authenticator_name]» |
| Изменение домена аутентификации<br>aggregator.audit.events.authenticators.update | Регистрируется:<br>▪ название домена аутентификации (authenticator_name);<br>▪ имя пользователя (username) | «Пользователь [username] ([authenticator_name]) обновил аутентификатор [authenticator_name]» |

| | | |
|---|---|---|
| Удаление домена аутентификации<br>aggregator.audit.events.authenticators.delete | Регистрируется:<br>▪ название домена аутентификации (authenticator_name);<br>▪ имя пользователя (username) | «Пользователь [username] ([authenticator_name]) удалил аутентификатор [authenticator_name]» |
| Добавление группы пользователей<br>aggregator.audit.events.authenticators.group.create | Регистрируется:<br>▪ название домена аутентификации (authenticator_name);<br>▪ имя пользователя (username);<br>▪ название группы домена аутентификации (group_name) | «Пользователь [username] ([authenticator_name]) создал группу [group_name] в домене [authenticator_name]» |
| Изменение группы пользователей<br>aggregator.audit.events.authenticators.group.update | Регистрируется:<br>▪ название домена аутентификации (authenticator_name);<br>▪ имя пользователя (username);<br>▪ название группы домена аутентификации (group_name) | «Пользователь [username] ([authenticator_name]) обновил группу [group_name] в домене [authenticator_name]» |
| Удаление группы пользователей<br>aggregator.audit.events.authenticators.group.delete | Регистрируется:<br>▪ название домена аутентификации (authenticator_name);<br>▪ имя пользователя (username);<br>▪ название группы домена аутентификации (group_name) | «Пользователь [username] ([authenticator_name]) удалил группу [group_name] у домена [authenticator_name]» |
| Изменение пользователя в домене<br>aggregator.audit.events.authenticators.user.update | Регистрируется:<br>▪ имя пользователя, который производит действие (username);<br>▪ идентификатор пользователя, над которым производится действие (updated_user) | «Пользователь [username] ([authenticator_name]) обновил пользователя [updated_user]» |
| Удаление пользователя из домена<br>aggregator.audit.events.authenticators.user.delete | Регистрируется:<br>▪ имя пользователя, который производит действие (username);<br>▪ идентификатор пользователя, над которым производится действие (deleted_user) | «Пользователь [username] ([authenticator_name]) удалил пользователя [deleted_user]» |
| Создание пользователя при входе<br>aggregator.audit.events.authenticators.user.create | Регистрируется:<br>▪ название домена аутентификации (authenticator_name);<br>▪ имя пользователя (username) | «При логине был создан пользователь [username] ([authenticator_name])» |
| **События, связанные с объектом «Шаблоны техобслуживания»** | | |
| Создание шаблона техобслуживания<br>aggregator.audit.events.maintenance.template.create | Регистрируется:<br>▪ название шаблона техобслуживания (template_name);<br>▪ название домена аутентификации (authenticator_name);<br>▪ имя пользователя (username) | «Пользователь [username] ([authenticator_name]) создал шаблон техобслуживания [template_name]» |
| Изменение шаблона техобслуживания<br>aggregator.audit.events.maintenance.template.update | Регистрируется:<br>▪ название шаблона техобслуживания (template_name);<br>▪ название домена аутентификации (authenticator_name);<br>▪ имя пользователя (username) | «Пользователь [username] ([authenticator_name]) обновил шаблон техобслуживания [template_name]» |

| | | |
|---|---|---|
| Удаление шаблона техобслуживания<br>aggregator.audit.events.maintenance.template.delete | Регистрируется:<br>▪ название шаблона техобслуживания (template_name);<br>▪ название домена аутентификации (authenticator_name);<br>▪ имя пользователя (username) | «Пользователь [username] ([authenticator_name]) удалил шаблон техобслуживания [template_name]» |
| **События, связанные с пользователем** | | |
| Получение пользователем списка доступных ресурсов<br>aggregator.audit.events.client.views.services_list | Регистрируется:<br>▪ название домена аутентификации (authenticator_name);<br>▪ имя пользователя (username) | «Пользователь [username] ([authenticator_name])получил список доступных ресурсов» |
| Вход пользователя в систему через веб-интерфейс<br>aggregator.audit.events.web.UserLogin | Регистрируется:<br>▪ название домена аутентификации (authenticator_name);<br>▪ имя пользователя (username);<br>▪ роль пользователя (role);<br>▪ IP-адрес, с которого был сделан запрос (ip);<br>▪ тип портала (portal) | «[role] [username] ([authenticator_name]) вошел в систему с ip-адреса [ip] через [portal]» |
| Выход пользователя из веб-интерфейса<br>aggregator.audit.events.web.UserLogout | Регистрируется:<br>▪ название домена аутентификации (authenticator_name);<br>▪ имя пользователя (username);<br>▪ роль пользователя (role);<br>▪ IP-адрес, с которого был сделан запрос (ip);<br>▪ тип портала (portal) | «[role] [username] ([authenticator_name]) вышел из системы (ip-адрес [ip]) через [portal]» |
| Предоставление пользователю параметров подключения к ресурсу<br>aggregator.audit.events.client.views.resource_connect | Регистрируется:<br>▪ название домена аутентификации (authenticator_name);<br>▪ имя пользователя (username);<br>▪ IP-адрес, с которого был сделан запрос (ip) | «Пользователь [username] ([authenticator_name]) подключился к ресурсу с IP [ip]» |
| Запрос пользователем ресурсов<br>aggregator.audit.events.client.views.user_requested_resource | Регистрируется:<br>▪ название домена аутентификации (authenticator_name);<br>▪ имя пользователя (username);<br>▪ IP-адрес, с которого был сделан запрос (ip) | «Пользователь [username] ([authenticator_name]) запросил ресурс с IP [ip]» |
| Аутентификация пользователя на «Универсальном диспетчере»<br>aggregator.audit.events.user.authentication_on_dispatcher | Регистрируется:<br>▪ название домена аутентификации (authenticator_name);<br>▪ имя пользователя (username);<br>▪ имя узла фермы (dispatcher_name) | «Пользователь [username] ([authenticator_name]) аутентифицировался на диспетчере подключений [dispatcher_name] » |
| Аутентификация пользователя на «Агрегаторе»<br>aggregator.audit.events.user.authentication_on_aggregator_from_arm | Регистрируется:<br>▪ название домена аутентификации (authenticator_name);<br>▪ имя пользователя (username);<br>▪ имя пользовательской рабочей станции (name) | «Пользователь [username] ([authenticator_name]) аутентифицировался на Агрегаторе с АРМ [name]» |

| | | |
|---|---|---|
| Подключение пользователя к виртуальному рабочему месту<br>`aggregator.audit.events.user.connection_to_warm` | Регистрируется:<br>▪ название домена аутентификации (`authenticator_name`);<br>▪ имя пользователя (`username`);<br>▪ IP-адрес виртуального рабочего места (`warm_ip`);<br>▪ имя виртуального рабочего места (`warm_name`) | «Пользователь `[username]` (`[authenticator_name]`) подключился к ВАРМ `[warm_name]` по ip-адресу `[warm_ip]`» |
| Подключение пользователя через «Шлюз»<br>`aggregator.audit.events.user.connection_through_gateway` | Регистрируется:<br>▪ название домена аутентификации (`authenticator_name`);<br>▪ имя пользователя (`username`);<br>▪ IP-адрес (`gateway_ip`);<br>▪ имя «Шлюза» (`gateway_name`) | «Пользователь `[username]` (`[authenticator_name]`) подключился через шлюз `[gateway_name]` с ip-адреса `[gateway_ip]`» |
| Аутентификация пользователя на «Агрегаторе»<br>`aggregator.audit.events.web.aggregator.UserLogin` | Регистрируется:<br>▪ название домена аутентификации (`authenticator_name`);<br>▪ имя пользователя (`username`);<br>▪ IP-адрес, с которого был сделан запрос (`ip`);<br>▪ имя ВМ (`aggregator_hostname`);<br>▪ IP-адрес ВМ (`aggregator_ip`);<br>▪ информация о «Клиенте» Termidesk (`user_agent`) | «Пользователь `[username]` (`[authenticator_name]`) подключился через `[user_agent]` с АРМ `[ip]` к агрегатору `[aggregator_hostname]` (`[aggregator_ip]`)» |
| Подключение пользователя к рабочему месту или терминальному приложению<br>`aggregator.audit.events.web.aggregator.UserConnectToVW` | Регистрируется:<br>▪ название домена аутентификации (`authenticator_name`);<br>▪ имя пользователя (`username`);<br>▪ имя «Универсального диспетчера» (`dispatcher_hostname`);<br>▪ IP-адрес «Универсального диспетчера» (`dispatcher_ip`);<br>▪ имя рабочего места (`vw_hostname`);<br>▪ IP-адрес рабочего места (`vw_ip`);<br>▪ имя шлюза (`gateway_hostname`);<br>▪ IP-адрес шлюза (`gateway_ip`) | «Пользователь `[username]` (`[authenticator_name]`) подключился к ВРМ `[vw_hostname]` (`[vw_ip]`) через диспетчер `[dispatcher_hostname]` (`[dispatcher_ip]`) и шлюз `[gateway_hostname]` (`[gateway_ip]`)» |

### 14.4.3 . Форматы регистрируемых событий аудита и их примеры

Каждая запись аудита в веб-интерфейсе отображается в формате: `[Дата и время][Событие][Текст события согласно шаблону]`.

Пример отображения записи аудита «Создание домена аутентификации» в веб-интерфейсе на странице «Мониторинг - Аудит»:

| Дата | Событие | Текст события |
|---|---|---|
| 2024-08-19T21:58:06.484+03:00 | aggregator.audit.events.aggregator.authenticators.create | «Пользователь "admin123(Встроенный)" создал аутентификатор "1"» |

# 15 . ХРАНЕНИЕ ЧУВСТВИТЕЛЬНОЙ ИНФОРМАЦИИ

## 15.1 . Хранение чувствительной информации с выбранным способом хранения «hvac»

Способ хранения паролей выбирается на этапе установки Termidesk. Способ хранения паролей «hvac» подразумевает, что будет использоваться хранилище OpenBao или Hashicorp Vault. Хранилище при этом должно быть заранее создано и настроено. При использовании Hashicorp Vault со схемой AD (Active Directory) поддерживается автоматическое обновление паролей.

При этом способе чувствительная информация (имена учетных записей, пароли, открытые и закрытые ключи, keytab-файлы, токены) хранится в контейнерах, пути к которым задаются вручную.

В контейнерах может содержаться как динамически обновляемая чувствительная информация, так и статическая. Поэтому в Termidesk для определения типа информации используются префиксы при задании пути к контейнеру хранения:

- `hvac-ad:// ` - префикс используется для динамически обновляемой чувствительной информации. Может быть задан только для хранилища Hashicorp Vault;
- `hvac-kv:// ` - префикс используется для статической чувствительной информации. Может быть задан как для хранилища OpenBao, так и для Hashicorp Vault.

Для корректной работы Termidesk со статической чувствительной информацией в хранилище должна быть повторена структура данных Active Directory. Контейнер, содержащий чувствительную информацию, должен содержать параметры:

- `current_password` - пароль учетной записи;
- `username` - имя учетной записи.

Пример:

```
{
    'current_password': '?@09AZ3PlvTzMKhsvZ91YFyVjVRHceYQ34eizKcKhVNHPjQJ46kvGGdsBPSkRcE9',
    'username': 'adfs-s'
},
```

Помимо указания префикса должна использоваться точка монтирования (mount point), заданная администратором в хранилище.

Таким образом общий формат указания пути к контейнеру хранения чувствительной информации в Termidesk выглядит следующим образом:

Символ «/» определяет, что должно быть возвращено все содержимое контейнера.
Если нужно вернуть значение конкретной переменной (key) контейнера, символ «/» не используется.

- если нужно вернуть всю информацию из контейнера:

```
<префикс> <точка_монтирования#> <путь_к_контейнеру>/
```

- если нужно вернуть только значение конкретного параметра:

```
<префикс> <точка_монтирования#> <путь_к_параметру_в_хранилище>
```

Допустим, в хранилище создан контейнер со статической информацией `termidesk` и точкой монтирования `secret`:

```
vault kv get secret/termidesk
```

Контейнер содержит следующие параметры:

```
========== Data ==========
Key                 Value
---                 -----
current_password    my_password
username            Администратор
```

В этом случае в Termidesk следует указывать:

- для возврата всех параметров: `hvac-kv://secret#termidesk/` (будет возвращено: `{'current_password': 'my_password', 'username': 'Администратор'}`);
- для возврата значения параметра `username`: `hvac-kv://secret#termidesk/username` (будет возвращено: `'Администратор'`).

Дополнительные примеры приведены в таблице (see page 0).

Таблица 29 – Примеры указания путей к чувствительной информации в Termidesk

| Команда в хранилище | Указание пути в Termidesk |
|---|---|
| Команда записи роли в хранилище:<br>`vault write ad/roles/vvddaa service_account_name="vvddaa@domain.local"` | `hvac-ad://ad#vvddaa/`<br>где:<br>`hvac-ad://` - префикс;<br>`ad#` - точка монтирования;<br>`vvddaa/` - путь к роли |
| Команда записи сертификата в хранилище:<br>`vault kv put secret/termidesk-admin/ssl-cert-snakeoil pem=@astra.local.pem`<br>⚠ Команды вида `vault kv put` перезаписывают контейнер сразу целиком, поэтому если задание сертификата и ключа будет разделено на разные команды, то в контейнере окажется только то, что добавлялось последним. | `hvac-kv://secret#termidesk-admin/ssl-cert-snakeoil/pem`<br>где:<br>`hvac-kv://` - префикс;<br>`secret#` - точка монтирования;<br>`termidesk-admin/ssl-cert-snakeoil/` - путь к контейнеру;<br>`pem` - сертификат |

| Команда в хранилище | Указание пути в Termidesk |
| --- | --- |
| Сгенерированный на контроллере домена keytab-файл должен быть преобразован к формату BASE64 для использования в хранилище:<br>`base64 termidesk.keytab > termidesk.keytab.b64`<br>Команда записи keytab-файла в хранилище:<br>`vault kv put secret/termidesk-admin/keytabs termidesk=@kerberos.keytab.b64`<br>Пример команды для преобразования файла и одновременной записи в хранилище:<br>`vault kv put secret/termidesk-admin/keytabs termidesk="$(base64 -w 0 termidesk.keytab)"` | `hvac-kv://secret#termidesk-admin/keytabs/termidesk`<br>где:<br>`hvac-kv://` - префикс;<br>`secret#` - точка монтирования;<br>`termidesk-admin/keytabs/` - путь к контейнеру;<br>`termidesk` - keytab-файл |

# 16 . ПЕРЕЧЕНЬ ТЕРМИНОВ

| Термин | Определение |
|---|---|
| Агрегатор администратора | Веб-интерфейс управления «Агрегатором». Устанавливается из пакета `termidesk-vdi`, при выборе пункта «Агрегатор администратора» |
| Агрегатор пользователя | Веб-интерфейс пользователя для получения ресурсов, предоставляемых «Агрегатором». Устанавливается из пакета `termidesk-vdi`, при выборе пункта «Агрегатор пользователя» |
| Домен аутентификации | Способ проверки субъектов и их полномочий |
| Компонент «Универсальный диспетчер» | Компонент Termidesk. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им РМ и контроля доставки РМ.<br>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.<br>Устанавливается из пакета `termidesk-gateway`. Наименование службы после установки: `termidesk-gateway.service` |
| Портал администратора | Предоставляет веб-интерфейс для управления фермой Termidesk и интерфейс `swagger` для доступа к ограниченному списку модулей документации по командам REST API |
| Портал пользователя | Предоставляет пользовательский веб-интерфейс фермы Termidesk (без доступа к функциям управления) и интерфейс `swagger` для доступа к ограниченному списку модулей документации по командам REST API |
| Рабочее место | Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа.<br>Под РМ подразумеваются как виртуальные РМ, так и терминальные рабочие столы или приложения |
| Сайт | Физическая площадка, на которой может быть развернута одна или несколько ферм |
| Узел | Аппаратный или виртуальный сервер компонента «Универсальный диспетчер» |
| Ферма поставщиков ресурсов | Ферма, объединяющая установку основных узлов Termidesk, взаимодействующих с единой БД |

# 17 . ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

| Сокращение | Пояснение |
|---|---|
| БД | База данных |
| ВМ | Виртуальная машина |
| ВРМ | Виртуальное рабочее место |
| КД | Контроллер домена |
| ОС | Операционная система |
| ПО | Программное обеспечение |
| РМ | Рабочее место |
| СУБД | Система управления базами данных |
| ЦС | Центр сертификации |
| API | Application Programming Interface (интерфейс прикладного программирования) |
| DHCP | Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста) |
| DN | Domain Name (доменное имя) |
| DNS | Domain Name System (система доменных имен) |
| FQDN | Fully Qualified Domain Name (полностью определенное имя домена) |
| GID | Group Identification Data (идентификатор группы) |
| HTTP | HyperText Transfer Protocol (протокол передачи гипертекста) |
| HTTPS | Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования) |
| IdP | Identity Provider (сервис, управляющий идентификационной информацией) |
| IP | Internet Protocol (межсетевой протокол) |
| JWT | JSON Web Token (открытый стандарт для создания токенов доступа) |
| LDAP | Lightweight Directory Access Protocol (легковесный протокол доступа к службам каталогов) |
| MS AD | Microsoft Active Directory Domain Service (службы каталогов Microsoft) |
| mTLS | Multiplexed Transport Layer Security (протокол, основанный на TLS с усиленной безопасностью) |
| NTP | Network Time Protocol (протокол сетевого времени) |
| OIDC | OpenID Connect (протокол аутентификации, построенный поверх стандарта OAuth 2.0.) |
| OU | Organizational Unit (организационная единица) |
| PKINIT | Public Key Cryptography for Initial Authentication (механизм Kerberos, позволяющий использовать сертификаты X.509) |

| Сокращение | Пояснение |
|---|---|
| REST | Representational State Transfer (программная архитектура, определяющая условия работы API) |
| RFC | Request for Comments (рабочее предложение Интернет) |
| SSL | Secure Sockets Layer (криптографический протокол) |
| TCP | Transmission Control Protocol (протокол управления передачей) |
| TLS | Transport Layer Security (протокол защиты транспортного уровня) |
| UDP | User Datagram Protocol (протокол пользовательских датаграмм) |
| URI | Uniform Resource Identifier (унифицированный идентификатор ресурса) |
| URL | Uniform Resource Locator (унифицированный указатель ресурса) |
| W3C | World Wide Web Consortium (Консорциум Всемирной паутины) |
| WS | WebSocket (двунаправленный протокол, позволяющий клиенту установить связь с сервером) |
| WSS | WebSocketSecure (двунаправленный протокол, позволяющий клиенту установить защищенную связь с сервером) |

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