TERMIDESK

РУКОВОДСТВО АДМИНИСТРАТОРА

СЛЕТ.10001-01 90 08

Версия 5.1. Выпуск от ноября 2024

Установка и настройка «Агрегатора»

ОГЛАВЛЕНИЕ

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 портала «Агрегатор»

Портал «Агрегатор» (далее - 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 (BPM).

Агрегатор должен быть установлен отдельно от узлов с ролями «Портал администратора», «Портал пользователя», «Менеджер рабочих мест». На этапе установки необходимо обеспечить для Агрегатора установку служб `termidesk-celery-beat` и `termidesk-celery-worker`, реализуемые пунктом инсталлятора «Менеджер рабочих мест (очереди)» (см. подраздел **Установка Агрегатора**).

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;
- «Портал 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 BPM на фермах поставщиков ресурсов;
- создание единого списка ресурсов (приложений, BPM) для пользователя с нескольких ферм поставщиков ресурсов.

1.3 . Типографские соглашения

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

2.2 . Требования к программному обеспечению

В среде функционирования должны быть предварительно установлены:

- операционная система (ОС) Astra Linux Special Edition версии 1.7 (минимальная версия - 1.7.3) и СУБД PostgreSQL версии 11 из состава репозитория ОС Astra Linux Special Edition версии 1.7. Из внешних по отношению к ОС Astra Linux Special Edition версии 1.7 СУБД поддерживается СУБД PostgreSQL версии 11 и выше;
- или ОС Astra Linux Special Edition версии 1.8 (минимальная версия - 1.8.1) и 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`:

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

где:

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

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

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

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

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

- убедиться, что ключ `release@uveon.ru` был успешно добавлен:

```
apt-key list
```

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

```
cat /var/repos/astra/GPG-KEY-PUBLIC
```

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

- обновить данные пакетного менеджера:

```
sudo apt update
```

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

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 Агрегатор 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», «Менеджера рабочих мест» 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:

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

После установки Termidesk 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**).

Узел 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). Если страница сразу не отобразилась, следует подождать 10-15 секунд и обновить ее.

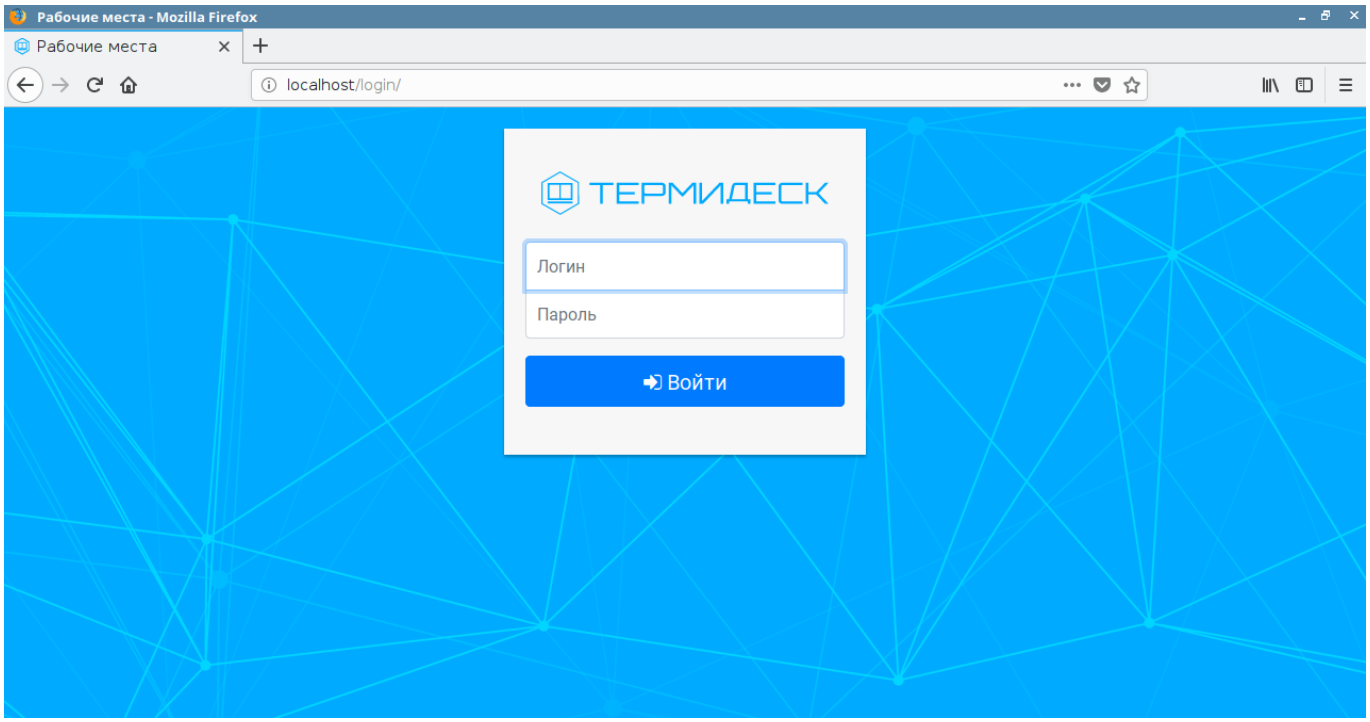

Рисунок 1 – Вход в портал «Агрегатор администратора»

Указанные IP-адреса используются в случае локальной установки. Если установка произведена на сервере, отличном от узла, на котором происходит проверка, необходимо вместо значений localhost или 127.0.0.1 использовать IP-адрес Агрегатора.

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`.

По умолчанию после установки вход в веб-портал «Агрегатор администратора» доступен только авторизованному пользователю ОС с ролью «Администратор». Пользователь ОС должен быть членом группы `astra-admin (1001)`. Для входа в веб-портал в полях «Логин» и «Пароль» нужно указать идентификатор пользователя ОС и его пароль соответственно, а затем нажать экранную кнопку **[Войти]**.

Проверка состояния компонентов выполняется командами:

```
systemctl status termidesk-vdi.service
systemctl status termidesk-celery-beat.service
systemctl status termidesk-celery-worker.service
```

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

3.3.2 . Автоматизированная установка Агрегатора

Перед установкой Агрегатор 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'
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**).

3.4 . 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:

```
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 Termidesk:

```
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 . 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 для подключения к фермам Termidesk;
- «Агрегатор универсальный»: предоставляет функции обоих вариантов - «Агрегатор администратора» и «Агрегатор пользователя».

Доступный тип веб-интерфейса определяется на этапе установки.

При установленном типе веб-интерфейса «Агрегатор администратора» в левой части веб-интерфейса находится панель, содержащая список основных функций:

- «Обзор»;
- «Компоненты»;
- «Настройки»;
- «Мониторинг».

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, перенаправляющие на соответствующие процедуры:

- «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, добавленных на Агрегатор;
- «База данных» - состояние БД, к которой подключен Агрегатор;
- «Rabbit MQ» - состояние брокера сообщений, к которому подключен Агрегатор.

4.3.2 . Функция «Компоненты»

При нажатии в левой части веб-интерфейса на функцию «Компоненты» открывается список, содержащий процедуры для подготовки агрегации ресурсов.

Функция «Компоненты» представлена следующими процедурами:

- «Домены аутентификации» - определяет настройку взаимодействия с источниками сведений о субъектах и их полномочиях;
- «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 «Настройки»

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

Функция «Настройки» представлена следующими процедурами:

- «Сайты» - определяет настройку размещения объединенных ресурсов для пользователей;
- «Шлюзы» - определяет настройку взаимодействия пользователей с ресурсами, предоставляемыми Агрегатором, через компонент «Шлюз».

4.3.4 . Функция «Мониторинг»

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

Функция «Мониторинг» представлена следующими процедурами:

- «Журналы» - позволяет просматривать события функционирования Агрегатора;
- «Аудит» - позволяет просматривать события входа и выхода из веб-интерфейса Агрегатора.

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.

5.2 . Домены аутентификации

5.2.1 . Общие сведения о доменах аутентификации

Домен аутентификации - источник сведений о субъектах и их полномочиях.

Для добавления домена аутентификации в веб-портале «Агрегатор администратора» следует перейти «Компоненты - Домены аутентификации», затем нажать экранную кнопку **[Создать]**.

Каждый домен аутентификации описывается перечнем параметров, требуемых для получения идентификаторов субъектов и информации о 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».

Созданный домен аутентификации можно отредактировать или удалить. Для этого в веб-портале «Агрегатор администратора» следует перейти «Компоненты - Домены аутентификации», затем пометить необходимый домен аутентификации и нажать соответственно экранную кнопку **[Изменить]** или **[Удалить]**.

5.2.2 . Добавление домена аутентификации MS AD (LDAP)

Для добавления домена аутентификации следует перейти «Компоненты - 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 1). Для проверки и сохранения параметров конфигурации нужно нажать экранную кнопку **[Тест]**, затем **[Сохранить]**.

Таблица 1 – 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. Параметр используется для поиска аналогичного домена «Универсального диспетчера», поэтому должен быть одинаковым как на портале «Агрегатор» (при его использовании), так и на «Универсальном диспетчере». Поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)
«Сервер LDAP»	IP-адрес или доменное имя сервера службы каталогов, являющегося источником сведений о субъектах и их полномочиях
«Порт»	TCP-порт, на котором запущена служба каталогов. Возможные стандартные значения: ▪ «389» (по умолчанию). Используется, если доступ к службе каталогов реализован осуществляется по протоколу LDAP; ▪ «636». Используется, если доступ к службе каталогов реализован осуществляется по протоколу LDAPS; ▪ «3268». Альтернативный порт. Используется, если доступ к службе каталогов реализован осуществляется по протоколу LDAP; ▪ «3269». Альтернативный порт. Используется, если доступ к службе каталогов реализован осуществляется по протоколу LDAPS. Для ускорения поиска пользователей в службе каталогов рекомендуется указывать альтернативный порт
«Использовать SSL»	Использовать защищенное соединение при взаимодействии со службой каталогов
«Учетная запись»	Учетная запись в формате Distinguished Name (DN) в домене MS AD (LDAP), используемая для подключения к службе каталогов. Пример: «CN=admin,OU=user,DC=test,DC=desk»
«Пароль учетной записи»	Набор символов, подтверждающий полномочия объекта для подключения к службе каталогов
«Таймаут»	Время ожидания (в секундах) ответа от службы каталогов. Значение по умолчанию: «10»

Параметр	Описание
«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). Вводимое значение не должно содержать пробелов: ▪ в начале и конце строки; ▪ рядом с разделителями (запятыми); ▪ в элементах пути (например, «DC=company name,DC=de»). Пример: «DC=test,DC=desk»
«Имя класса пользователя»	Атрибут класса пользователя в службе каталогов. Для корректного заполнения данного поля необходимо указать значение «person»
«Атрибут идентификатора пользователя»	Атрибут уникального имени или идентификатора пользователя в службе каталогов. Для корректного заполнения данного поля необходимо указать: ▪ значение «name», если активирован параметр «Использовать PKINIT»; 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. ▪ значение «SamAccountName» в остальных случаях
«Список атрибутов пользователя»	Список атрибутов, содержащий уникальные данные пользователя, разделенные запятыми. Для корректного заполнения данного поля необходимо указать значение «name»
«Имя атрибута группы»	Атрибут принадлежности к группе в службе каталогов. Для корректного заполнения данного поля необходимо указать значение «group»
«Атрибут имени группы»	Атрибут идентификатора группы, к которой относится субъект в службе каталогов. Для корректного заполнения данного поля необходимо указать: ▪ значение «distinguishedname», если включены параметры «Использовать рекурсивный поиск групп» или «Использовать обратный порядок проверки членства пользователей»; ▪ значение «name», если активирован параметр «Использовать PKINIT»; 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. ▪ значение «cn» в остальных случаях. 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. 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. Для корректного заполнения данного поля необходимо указать значение «member»
«Атрибут групп для LDAP-запросов»	Атрибут, определяющий группы пользователя при запросах к службе каталогов. Возможные значения: «objectClass», «objectCategory»

Параметр	Описание
«Использовать рекурсивный поиск групп»	При запросе групп пользователя будут учтены его родительские группы, в которых он состоит неявно. Если дополнительно включен параметр «Использовать обратный порядок проверки членства пользователей», то параметр «Использовать рекурсивный поиск групп» можно не включать. Возможные значения: ▪ «Да» - использовать рекурсивный поиск; ▪ «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». 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. При выключении этого параметра применяется настройка выбора «Атрибут групп для LDAP-запросов»: «objectClass» или «objectCategory». При включении этого параметра всегда применяется настройка выбора «Атрибут групп для LDAP-запросов»: «objectClass». Возможные значения: ▪ «Да» - использовать обратный порядок; ▪ «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. 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). 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». Возможные значения: ▪ «Да» - использовать механизм; ▪ «Нет» (по умолчанию) - не использовать механизм
«Порт PKINIT»	TCP/UDP порт, на котором запущена служба Kerberos. Значение по умолчанию: «88»

5.2.3 . 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.

Для добавления домена аутентификации следует перейти «Компоненты - 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 2). Для сохранения параметров конфигурации нужно использовать экранную кнопку **[Сохранить]**.

Таблица 2 – Данные для добавления аутентификации через OIDC

Параметр	Описание
«Название»	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
«Метка»	Информационное поле, используемое для идентификации объекта во внутренней структуре данных Termidesk. Начиная с Termidesk версии 5.1 поле может состоять из букв латинского алфавита, цифр, знаков «-» (дефис) и «_» (подчеркивание)
«Client ID»	Уникальный идентификатор приложения, полученный от службы идентификации IdP. Пример: «openid-test-cl»
«Client secret»	Ключ приложения, полученный от службы идентификации IdP
«Authorization endpoint»	URL-адрес авторизации службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/auth»
«Token endpoint»	URL-адрес получения токена службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/token»
«Userinfo endpoint»	URL-адрес получения информации о пользователе от службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/userinfo»
«JWKS URI»	URL-адрес получения сертификатов службы идентификации IdP. Пример: «http://192.0.2.2:8080/auth/realms/domain.local/protocol/openid-connect/certs»
«Scope»	Набор областей действия, поддерживаемый в службе идентификации IdP. Области действия определяются спецификацией протокола OAuth 2.0. Неполный список возможных значений (указываются через пробел): ▪ «openid» (обязательное значение для OIDC) - запуск аутентификации с использованием OIDC; ▪ «profile» - доступ к профилю пользователя; ▪ «email» - доступ к адресу электронной почты пользователя; ▪ «offline_access» - обновление токена доступа без необходимости повторной аутентификации; ▪ «groups» - доступ к списку ролей пользователя. Значение по умолчанию: «openid email profile groups». Если нужно указать другой набор значений, следует убедиться, что он поддерживается используемой службой идентификации IdP

Параметр	Описание
«Атрибут имени пользователя»	Имя атрибута, в котором хранится имя пользователя (логин) в службе идентификации IdP. Значение по умолчанию: «email»
«Проверка SSL»	Проверка использования SSL

5.2.4 . 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:

- создание - добавление существующей в службе каталогов группы в Termidesk;
- 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 добавления группы следует перейти «Компоненты - Домены аутентификации», затем в столбце «Название» сводной таблицы нажать на наименование домена аутентификации. В открывшемся окне в таблице «Группы» нажать экранную кнопку **[Создать]**.

Для добавления группы необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 3).

Таблица 3 – 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
«Домен аутентификации»	Выбор домена аутентификации, в который должна быть добавлена группа пользователей. Домен аутентификации должен быть добавлен через «Компоненты - Домены аутентификации» для возможности его выбора в этом параметре
«Статус»	Характеристика состояния субъектов группы при доступе к Агрегатору. Доступные значения: ▪ «Активный» - субъекты группы могут аутентифицироваться в портале «Агрегатор администратора» и/или «Агрегатор пользователя»; ▪ «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 Termidesk. Доступные значения параметра: ▪ «Пользователь» - субъекты группы не будут иметь доступ к порталу «Агрегатор администратора»; ▪ «Администратор» - субъекты группы будут иметь полный доступ к порталу «Агрегатор администратора»
«Метагруппа»	Характеристика использования метагруппы. Метагруппа - группа, объединяющая несколько стандартных групп в Агрегаторе. Рекомендуется оставить значение по умолчанию: «Нет»
«Отображать метагруппу»	Характеристика использования метагруппы. Рекомендуется оставить значение по умолчанию: «Нет»
«Группы пользователей»	Перечень групп, которые должны быть использованы в метагруппе. Параметр можно оставить пустым, если использование метагруппы не планируется и параметры «Метагруппа» и «Отображать метагруппу» имеют значение «Нет»

5.3 . 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. 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]**, после чего откроется окно (см. Рисунок 2) редактирования пользователя;
- 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.

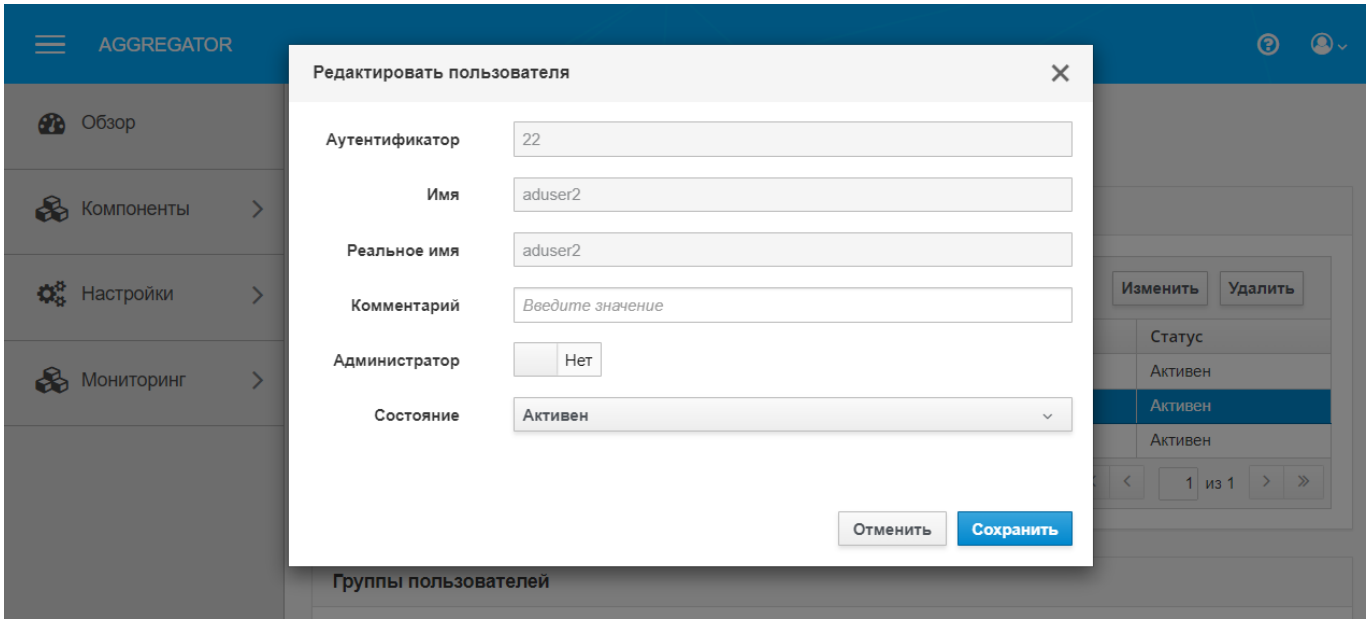

Рисунок 2 – Окно редактирования пользователя домена аутентификации

В окне редактирования пользователя доступны данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 4).

Таблица 4 – Данные для редактирования пользователя домена аутентификации

Параметр	Описание
«Аутентификатор»	Параметр используется во внутренней структуре данных Агрегатора, его нельзя изменить
«Имя»	Отображаемое имя субъекта в Агрегаторе. Параметр получен автоматически от службы каталогов, его нельзя изменить
«Реальное имя»	Параметр получен автоматически от службы каталогов, его нельзя изменить
«Комментарий»	Информационное сообщение, используемое для описания назначения пользователя
«Администратор»	Служебные функции субъекта при доступе к Агрегатору. Возможные значения: ▪ «Да» - субъект будет иметь доступ к порталу «Агрегатор администратора»; ▪ «Нет» - субъект не будет иметь доступ к порталу «Агрегатор администратора»
«Состояние»	Характеристика состояния субъекта при доступе к Агрегатору. Возможные значения: ▪ «Активен» - субъект может аутентифицироваться; ▪ «Неактивен» - субъект не может аутентифицироваться

5.4 . Фермы-поставщики ресурсов

5.4.1 . 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 добавления фермы в веб-портале «Агрегатор администратора» следует перейти «Компоненты - Фермы поставщиков ресурсов», затем нажать на экранную кнопку **[Создать]**.

Для редактирования информации о созданной ферме следует перейти «Компоненты - Фермы поставщиков ресурсов», затем выбрать необходимую ферму и нажать на экранную кнопку **[Изменить]**.

Для удаления фермы следует перейти «Компоненты - Фермы поставщиков ресурсов», затем выбрать необходимую ферму и нажать на экранную кнопку **[Удалить]**.

5.4.2 . Добавление фермы поставщиков ресурсов

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

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 5). Для сохранения параметров конфигурации нужно использовать экранную кнопку **[Сохранить]**.

> 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.

Таблица 5 – Данные для добавления фермы поставщика ресурсов

Параметр	Описание
«Название»	Текстовое наименование для добавляемой фермы
«Комментарий»	Информационное сообщение, используемое для описания назначения фермы
«Шлюз»	Выбор шлюза, через который пользователь будет получать ресурсы. Можно выбрать только одно значение. Шлюз должен быть добавлен через «Настройки - Шлюзы» для возможности его выбора в этом параметре
«Исключен»	Управление состоянием фермы. Возможные значения: ▪ «Да» - ферма не участвует в выдаче ресурсов (неактивна); ▪ «Нет» - ферма участвует в выдаче ресурсов (активна). 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
«Транспорт»	Протокол, по которому будет происходить подключение к узлу. Возможные значения: ▪ «HTTP» - незащищенное подключение; ▪ «HTTPS» - защищенное подключение.

Параметр	Описание
«Проверять сертификаты SSL»	Управление проверкой валидности SSL-сертификата. Параметр необходимо отключить в случае, если проверку валидности пройти не удается: ▪ на узлах фермы используются самоподписанные сертификаты; ▪ или на узлах фермы используются сертификаты, выпущенные центром сертификации, корневой сертификат которого не добавлен в список доверенных на узле Агрегатора. По умолчанию проверка валидности сертификатов включена
«Порт»	Порт, который будет использоваться при подключении по указанному в параметре «Транспорт» протоколу. При стандартных настройках для протокола HTTP используется порт 80, для протокола HTTPS - 443
«Продолжительность всех неудачных обходов, минут»	Продолжительность времени (в минутах), по истечении которого ферма считается неактивной, если она не подтверждает свое активное состояние. По умолчанию «0»
«Продолжительность обхода, минут»	Периодичность опроса фермы (в минутах) для подтверждения ее активности. По умолчанию «60» (каждые 60 минут). Пример: пусть параметру «Продолжительность обхода, минут» задано значение «60», а параметру «Продолжительность всех неудачных обходов, минут» 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
«Максимальное количество отказавших узлов»	Количество узлов в неактивном состоянии, при превышении которого ферма будет отмечена неактивной. По умолчанию «0»
«Приоритетная для групп пользователей»	Выбор группы пользователей, которой будет предоставлен приоритетный доступ к данной ферме. Параметр задает приоритетную ферму, на которую будут перенаправляться подключения указанной группы в обход балансировки подключений. Для каждой группы можно назначить только одну приоритетную ферму. Для восстановления балансировки подключений необходимо исключить группу из списка приоритетных для фермы

5.5 . Узлы

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

Отредактировать информацию об узле можно двумя способами:

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

- перейти «Компоненты - Узлы», затем выбрать необходимый узел и нажать на экранную кнопку **[Изменить]**.

Удалить узел можно двумя способами:

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

5.5.2 . Добавление узла Termidesk

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

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 6). Для сохранения параметров конфигурации нужно использовать экранную кнопку **[Сохранить]**. 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 6 – 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»	Параметр для доступа к API сервера. 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. Возможные значения: ▪ «Да» - узел активен; ▪ «Нет» - узел неактивен. Параметр используется для прекращения взаимодействия Агрегатора с узлом

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

5.6 . Сайты

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

Созданный сайт можно отредактировать или удалить. Для этого в веб-портале «Агрегатор администратора» следует перейти «Настройки - Сайты», затем пометить необходимый сайт и нажать соответственно экранную кнопку **[Изменить]** или **[Удалить]**.

5.6.2 . Добавление сайта

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

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 7). Для сохранения параметров конфигурации нужно использовать экранную кнопку **[Сохранить]**.

Таблица 7 – Данные для добавления сайта

Параметр	Описание
«Название»	Текстовое наименование добавляемого сайта
«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. 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. Группы пользователей должны быть добавлены в домене аутентификации («Компоненты - Домены аутентификации») для возможности их выбора в этом параметре
«Фермы поставщики ресурсов»	Выбор фермы или ферм, для которых будет создан сайт. Фермы поставщиков ресурсов должны быть добавлены через «Компоненты - Фермы поставщики ресурсов» для возможности их выбора в этом параметре
«Техобслуживание»	Управление режимом техобслуживания сайта. Режим техобслуживания - это запрет пользователям подключаться к сайту. Этот режим предназначен для проведения плановых регламентных или аварийных работ

Параметр	Описание
«Шаблон техобслуживания»	Выбор ранее созданного шаблона, текст из которого будет выведен пользователю при попытке подключиться к сайту, находящемся в режиме техобслуживания. Создание шаблона приведено в подразделе **Добавление шаблона техобслуживания**

5.6.3 . Добавление объединенного набора ресурсов

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

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 8). Для сохранения параметров конфигурации нужно использовать экранную кнопку **[Сохранить]**.

Таблица 8 – Данные для добавления объединенного набора ресурсов

Параметр	Описание
«Аутентификатор»	Параметр используется во внутренней структуре данных Агрегатора, его нельзя изменить
«Название»	Текстовое наименование добавляемого объединенного набора ресурсов
«Комментарий»	Информационное сообщение, используемое для описания назначения объединенного набора ресурсов
«Ферма»	Выбор фермы или ферм, для которых будут действовать правила объединенного набора ресурсов
«Публикуются идентичные ресурсы»	Характеристика публикуемых ресурсов: ▪ «Да» - все наборы ресурсов, опубликованные на фермах, идентичны; ▪ «Нет» - наборы ресурсов, опубликованные на фермах, неидентичны. 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. Агрегатор не проверяет, действительно ли все ресурсы на указанных фермах идентичны - это подтверждает администратор через указанный параметр
«Балансировка подключений»	Характеристика активации балансировки подключений: ▪ «Да» - подключения балансируются по схеме round-robin; ▪ «Нет» - подключения не балансируются
«Активен»	Характеристика состояния объединенного набора ресурсов: ▪ «Да» - объединенный набор ресурсов активен и доступен для пользователей; ▪ «Нет» - объединенный набор ресурсов неактивен и недоступен для пользователей
«Приоритет»	Приоритет отображения

5.7 . Шаблоны техобслуживания

5.7.1 . Общие сведения о шаблонах техобслуживания

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

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

Шаблон можно отредактировать или удалить. Для этого в веб-портале «Агрегатор администратора» следует перейти «Настройки - Шаблоны техобслуживания», затем пометить необходимый шаблон и нажать соответственно экранную кнопку **[Изменить]** или **[Удалить].**

5.7.2 . Добавление шаблона техобслуживания

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

Далее необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 9). Для сохранения параметров конфигурации нужно нажать экранную кнопку **[Сохранить]**.

Таблица 9 – 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

6 . НАСТРОЙКА ПОДКЛЮЧЕНИЯ ПОЛЬЗОВАТЕЛЕЙ ЧЕРЕЗ ШЛЮЗ

6.1 . 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 добавления Шлюза в веб-портале «Агрегатор администратора» следует перейти «Настройки - Шлюзы», затем нажать экранную кнопку **[Создать]**.

Созданный Шлюз можно отредактировать или удалить. Для этого в веб-портале «Агрегатор администратора» следует перейти «Настройки - Шлюзы», затем пометить необходимый сайт и нажать соответственно экранную кнопку **[Изменить]** или **[Удалить]**.

6.2 . Добавление шлюза

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

Затем необходимо заполнить данные, перечисленные в столбце «Параметр» следующей таблицы (см. Таблица 10). Для сохранения параметров конфигурации нужно нажать экранную кнопку **[Сохранить]**.

Таблица 10 – 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. Протокол WS (WebSocket) использует по умолчанию порт 80, протокол WSS использует по умолчанию порт 443. Администратор может задать нужное значение, если используется нестандартный порт. 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

7 . СИСТЕМНЫЕ НАСТРОЙКИ

7.1 . 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 (см. Таблица 10).

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

Таблица 11 – Параметры конфигурирования Агрегатора

Параметр	Значение по умолчанию	Описание
`TDSK_AUTOFS_IMAGES_ID`	`Не задано`	Параметр может быть задан на узлах «Универсального диспетчера». Используется для настройки шаблонов переносимых профилей. В качестве значения используются идентификаторы дисков. Пример: `TDSK_AUTOFS_IMAGES_ID=xx[,yy[,zz[,...]]]`
`DBHOST`	`Не задано`	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора». Определяет IP-адрес или FQDN СУБД PostgreSQL. Начальное значение задается на этапе подготовке среды функционирования и установки Termidesk
`DBPORT`	`5432`	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора». Определяет порт соединения с сервером БД
`DBSSL`	`Не задано`	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора». Определяет протокол подключения к БД. Возможные значения: `Disable`, `TLSv1.2`, `TLSv1.3`. Начальное значение задается на этапе установки Termidesk
`DBNAME`	`Не задано`	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора». Определяет имя БД. 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», «Менеджера рабочих мест (очереди)», «Агрегатора». Определяет имя пользователя, имеющего доступ к БД. Начальное значение задается на этапе подготовки среды функционирования перед установкой Termidesk

Параметр	Значение по умолчанию	Описание
DBPASS	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора». Определяет пароль пользователя, имеющего доступ к БД. 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. В стандартных установках значения менять не следует. Чтобы получить преобразованное значение пароля, следует воспользоваться утилитой `scramble`: ▪ для получения значения по стандартному алгоритму: `/opt/termidesk/bin/scramble --value <пароль> --type AES256`; ▪ для получения значения с увеличенным числом итераций преобразования: `/opt/termidesk/bin/scramble --value <пароль> --type AES256_V2`. Утилита `scramble` использует в качестве вектора преобразования значение из файла `/etc/opt/termidesk-vdi/termidesk.cookie`. Значение генерируется автоматически на этапе установки Termidesk

DBCERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».
		Определяет путь к сертификату mTLS для защищенного подключения к БД.
		mTLS - метод обеспечения защищенного соединения с БД через двустороннюю аутентификацию с использованием сертификатов.
		Для использования сертификата нужно:
		▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;
		▪ назначить владельцем файла пользователя `termidesk`:
		`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.crt`
		▪ изменить права на файл:
		`sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.crt`
		▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**)

DBKEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».
		Определяет путь к ключу mTLS для защищенного подключения к БД.
		Ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению:
		`openssl rsa -in <путь_к_файлу_ключа>.key -out <путь_сохранения_преобразованного_ключа>.key`
		Для использования ключа также нужно:
		▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;
		▪ назначить владельцем файла пользователя `termidesk`:
		`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.key`
		▪ изменить права на файл:
		`sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.key`
		▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен

Параметр	Значение по умолчанию	Описание

DBCHAIN	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».
		Определяет путь к промежуточному сертификату mTLS для защищенного подключения к БД.
		Для использования сертификата нужно:
		▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;
		▪ назначить владельцем файла пользователя `termidesk`:
		`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.pem`
		▪ изменить права на файл:
		`sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.pem`
		▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен

DJANGO_SECRET_KEY	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора». Используется для проверки данных, пересылаемых между компонентами Termidesk. Значение генерируется при установке Termidesk и должно быть одинаковым для всех узлов при распределенной установке
RABBITMQ_URL	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора». Определяет URL-адрес подключения к серверам RabbitMQ. Можно подключить до трех (включительно) серверов. Пароль подключения к серверу RabbitMQ, указанный в `RABBITMQ_URL`, хранится в конфигурационном файле `/etc/opt/termidesk-vdi/termidesk.conf` в преобразованном виде. Чтобы получить преобразованное значение пароля, следует воспользоваться утилитой `scramble`: ▪ для получения значения по стандартному алгоритму: `/opt/termidesk/bin/scramble --value <пароль> --type AES256`; ▪ для получения значения с увеличенным числом итераций преобразования: `/opt/termidesk/bin/scramble --value <пароль> --type AES256_V2`. Для использования преобразованного значения следует указать его в `RABBITMQ_URL` и выполнить перезапуск служб. Начальное значение `RABBITMQ_URL` задается на этапе установки
RABBITMQ_SSL	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора». Определяет протокол подключения к RabbitMQ. Возможные значения: `Disable`, `TLSv1.2`. Начальное значение задается на этапе установки
NODE_ROLES	Не задано	Параметр обязателен и задается на этапе установки. Определяет тип роли, с которой будет установлен Termidesk. Возможные значения: ▪ `ADMIN` - роль «Портал администратора»; ▪ `USER` - роль «Портал пользователя»; ▪ `TASKMAN` - роль «Менеджер рабочих мест»; ▪ `CELERYMAN` - роль «Менеджер рабочих мест (очереди)»; ▪ `AGGR_ADM` - роль «Агрегатор администратора»; ▪ `AGGR_USR` - роль «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». При переустановке значение параметра в конфигурационном файле будет перезаписано

Параметр	Значение по умолчанию	Описание
LOG_LEVEL	INFO	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора». Определяет уровень журналирования сообщений. Возможные значения: DEBUG, INFO, WARNING, ERROR, CRITICAL
LOG_ADDRESS	/dev/log	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора». 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», «Менеджера рабочих мест (очереди)», «Агрегатора». Определяет категорию сообщений syslog. Категория должна совпадать с настройками в конфигурационном файле /etc/syslog-ng/conffirst.d/termidesk.conf
HEALTH_CHECK_ACCESS_KEY	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора». Определяет токен доступа к API проверки состояния сервера. Начальное значение генерируется на этапе установки. При задании значения параметра следует руководствоваться правилом, что: ▪ размер должен составлять от 0 до 64 символа; ▪ должны использоваться символы в шестнадцатеричной системе (0-9, a-f). Значение также может быть сгенерировано через openssl: openssl rand -hex 32
METRICS_ACCESS_KEY	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора». Определяет токен доступа к API получения метрик сервера. Начальное значение генерируется на этапе установки. При задании значения параметра следует руководствоваться правилом, что: ▪ размер должен составлять от 0 до 64 символа; ▪ должны использоваться символы в шестнадцатеричной системе (0-9, a-f). Значение также может быть сгенерировано через openssl: openssl rand -hex 32
HEALTH_CHECK_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора». Определяет путь к сертификату SSL/TLS для защищенного подключения к API проверки состояния сервера. Для использования сертификата нужно: ▪ скопировать его в каталог /etc/opt/termidesk-vdi/; ▪ назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.pem ▪ изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.pem ▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен. Изначально параметр закомментирован (используется значение по умолчанию)

Параметр	Значение по умолчанию	Описание

HEALTH_CHECK_KEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора».
		Определяет путь к ключу SSL/TLS для защищенного подключения к API проверки состояния сервера.
		Ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению:
		`openssl rsa -in <путь_к_файлу_ключа>.key -out <путь_сохранения_преобразованного_ключа>.key`
		Для использования ключа также нужно:
		▪ скопировать его в каталог `/etc/opt/termidesk-vdi/`;
		▪ назначить владельцем файла пользователя `termidesk`:
		`sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.key`
		▪ изменить права на файл:
		`sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.key`
		▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен.
		Изначально параметр закомментирован (используется значение по умолчанию)

TASKMAN_HEALTH_CHECK_PORT	8100	Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест». Определяет порт, на котором работает веб-сервер для обслуживания API проверки состояния компонента «Менеджер рабочих мест». Изначально параметр закомментирован (используется значение по умолчанию)
TASKMAN_HEALTH_CHECK_IP	0.0.0.0	Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест». Определяет IP-адрес, с которым служба `termidesk-taskman` 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. Изначально параметр закомментирован (используется значение по умолчанию)
CELERY_BEAT_HEALTH_CHECK_PORT	8103	Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест (очереди)». Определяет порт, на котором работает веб-сервер для обслуживания API проверки состояния компонента «Менеджер рабочих мест (очереди)». 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 (очереди)». 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. Изначально параметр закомментирован (используется значение по умолчанию)
CELERY_WORKER_HEALTH_CHECK_PORT	8104	Параметр обязателен и задается на узлах с установленным «Менеджером рабочих мест (очереди)». Определяет порт, на котором работает веб-сервер для обслуживания API проверки состояния компонента «Менеджер рабочих мест (очереди)». 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 (очереди)». 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. Изначально параметр закомментирован (используется значение по умолчанию)

Параметр	Значение по умолчанию	Описание
REQUESTS_CA_BUNDLE	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора». Определяет путь к файлу с доверенным корневым сертификатом, задается для настройки работы с сертификатами собственных ЦС. По умолчанию параметр не используется (закомментирован)
EULA_ACCEPTED	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора». Определяет принятие лицензионного соглашения при установке. В случае автоматизированной установки наличие параметра обязательно
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». 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». Определяет путь к резервному сертификату для получения значения JWT-токена «Агрегатора». 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»). 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». 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». Определяет времени жизни (в секундах) JWT-токена, подписанного «Агрегатором»
AGGREGATOR_IMAGE_CACHE_LIFETIME_HOURS	672	Параметр обязателен и задается на узлах с установленным «Агрегатором». Определяет время жизни (в часах) кеша иконок фондов РМ. По истечении этого времени иконка обновляется
SECRETS_STORAGE_METHOD	Не задано	Параметр обязателен и задается на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди)», «Агрегатора». Определяет способ хранения паролей подключения к СУБД и RabbitMQ: ▪ config - пароли будут храниться в преобразованном виде в файле /etc/opt/termidesk-vdi/termidesk.conf; ▪ openbao - для хранения паролей будет использоваться хранилище паролей OpenBao (хранилище должно быть заранее создано и настроено). Хранилище паролей OpenBao должно быть реализовано в отказоустойчивом варианте, иначе Termidesk не будет работать в период простоя узлов OpenBao. Начальное значение задается на этапе установки

Параметр	Значение по умолчанию	Описание
SECRETS_OPENBAO_URL	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора». Определяет IP-адреса или FQDN узла и порта с установленным хранилищем OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao. Формат: http://<IP-адрес или FQDN>:8200. Подключение может выполняться по протоколу HTTPS, если OpenBao настроен соответствующим образом. Начальное значение задается на этапе установки
SECRETS_OPENBAO_TOKEN	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора». Определяет токен (Initial Root Token), сформированный при инициализации хранилища OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao. Начальное значение задается на этапе установки и хранится в конфигурационном файле /etc/opt/termidesk-vdi/termidesk.conf в преобразованном виде. Для преобразования значения параметра, заданного вручную, следует воспользоваться утилитой scramble: ▪ для получения значения по стандартному алгоритму: /opt/termidesk/bin/scramble --value <пароль> --type AES256; ▪ для получения значения с увеличенным числом итераций преобразования: /opt/termidesk/bin/scramble --value <пароль> --type AES256_V2.
SECRETS_OPENBAO_DB_PATH	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора». Определяет путь, настроенный на OpenBao для хранения пароля СУБД. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao. Начальное значение задается на этапе установки
SECRETS_OPENBAO_DB_ROLE_NAME	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора». Определяет роль, настроенную на OpenBao и имеющую доступ к паролю СУБД. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao. Начальное значение задается на этапе установки
SECRETS_OPENBAO_RABBITMQ_PATH	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора»». Определяет путь, настроенный на OpenBao для хранения пароля RabbitMQ. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao. Начальное значение задается на этапе установки
SECRETS_OPENBAO_RABBITMQ_ROLE_NAME	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора». Определяет роль, настроенную на OpenBao и имеющую доступ к паролю RabbitMQ. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao. Начальное значение задается на этапе установки

Параметр	Значение по умолчанию	Описание
SECRETS_OPENBAO_CLIENT_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора». Определяет путь к сертификату SSL/TLS для защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы. Для использования сертификата нужно: ▪ скопировать его в каталог /etc/opt/termidesk-vdi/; ▪ назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.crt ▪ изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.crt ▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**). Изначально параметр закомментирован (используется значение по умолчанию)
SECRETS_OPENBAO_CLIENT_KEY	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора». Определяет путь к ключу SSL/TLS для защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы. Ключ может иметь парольную защиту. Для использования ключа в Termidesk нужно преобразовать его к начальному значению: openssl rsa -in <путь_к_файлу_ключа>.key -out <путь_сохранения_преобразованного_ключа>.key Для использования ключа также нужно: ▪ скопировать его в каталог /etc/opt/termidesk-vdi/; ▪ назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.key ▪ изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.key ▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен. Изначально параметр закомментирован (используется значение по умолчанию)
SECRETS_OPENBAO_SERVER_CERT	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора». Определяет путь к промежуточному сертификату ЦС SSL/TLS для защищенного подключения к OpenBao. OpenBao должен быть настроен соответствующим образом. Пример конфигурации OpenBao приведен после таблицы. Для использования сертификата нужно: ▪ скопировать его в каталог /etc/opt/termidesk-vdi/; ▪ назначить владельцем файла пользователя termidesk: sudo chown termidesk:termidesk /etc/opt/termidesk-vdi/<путь_к_файлу>.pem ▪ изменить права на файл: sudo chmod 600 /etc/opt/termidesk-vdi/<путь_к_файлу>.pem ▪ установить корневой сертификат ЦС (см. подраздел **Установка корневого сертификата центра сертификации**), если ранее он не был установлен. Изначально параметр закомментирован (используется значение по умолчанию)
SECRETS_OPENBAO_TERMIDESK_PATH	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора». Определяет путь, настроенный на OpenBao для хранения паролей Termidesk. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao. Начальное значение задается на этапе установки

Параметр	Значение по умолчанию	Описание
SECRETS_OPENBAO_TERMIDESK_ROLE_NAME	Не задано	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора». Определяет роль, настроенную на OpenBao и имеющую доступ к паролям Termidesk. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao. Начальное значение задается на этапе установки
SECRETS_OPENBAO_KV_VERSION	1	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора». Используется для указания версии API OpenBao. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao. Возможные значения: ▪ 1 (по умолчанию); ▪ 2. Начальное значение задается на этапе установки
SECRETS_OPENBAO_CACHE_LIFETIME	5	Параметр может быть задан на узлах «Универсального диспетчера», «Менеджера рабочих мест», «Менеджера рабочих мест (очереди), «Агрегатора». 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. Параметр задается, если для SECRETS_STORAGE_METHOD задано значение openbao. Начальное значение задается на этапе установки
FLUENTD_CACHE	15	Параметр может быть задан на узлах «Универсального диспетчера». Определяет время (в секундах) кеширования параметров подключения к узлу «Ретранслятора». По умолчанию после установки время кеширования составляет 15 секунд. 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». Определяет таблицу хранения событий фермы Termidesk. По умолчанию после установки «Универсальный диспетчер» обращается к таблице «logs» БД «Ретранслятора». В случае, если в БД «Ретранслятора» для хранения событий используется другая таблица, следует раскомментировать параметр и указать новое имя таблицы
WSPROXY_TICKET_TIMEOUT	20	При штатном функционировании Terrmidesk менять параметр не рекомендуется. Параметр может быть задан на узлах «Универсального диспетчера». Определяет время ожидания отклика «Шлюза» и применяется для решения нештатных ситуаций, например: если параметр «Время ожидания соединения» по каким-либо причинам не используется в протоколе доставки, или если запрос к «Шлюзу» выполняется долго и подключение пользователя не устанавливается. По умолчанию после установки время ожидания составляет 20 секунд. В случае, если нужно изменить значение, следует раскомментировать параметр и задать ему новое значение

7.2 . Утилиты интерфейса командной строки для настройки Агрегатора

7.2.1 . 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 3).

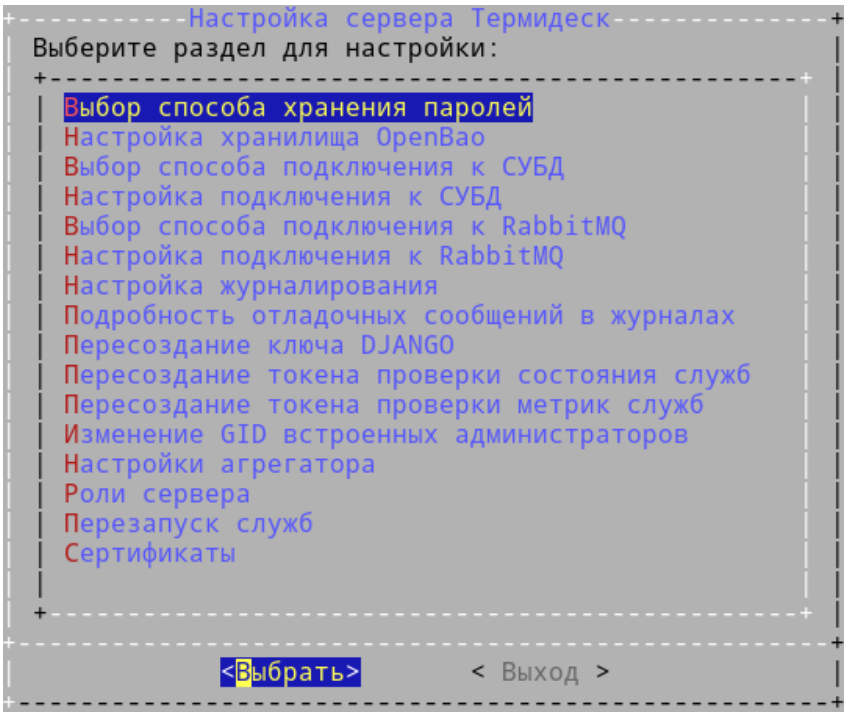

Рисунок 3 – Интерфейс утилиты termidesk-config

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`;

- «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 способа подключения к СУБД»: позволяет выбрать протокол при подключении к СУБД (параметр `DBSSL`);
- «Настройка подключения к СУБД»: позволяет настроить параметры подключения к СУБД:
  - «Адрес СУБД» - IP-адрес или FQDN СУБД PostgreSQL (параметр `DBHOST`);
  - «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», «Менеджер рабочих мест (очереди)», «Агрегатор администратора», «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`).

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».
Роль «Менеджер рабочих мест» не должна устанавливаться с «Агрегатором администратора» и (или) «Агрегатором пользователя».
Роль «Менеджер рабочих мест» (очереди) устанавливается с «Агрегатором администратора» и (или) «Агрегатором пользователя».

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

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

8 . СИСТЕМА АУДИТА

8.1 . 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 Агрегатор;
- `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.

8.2 . 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
```

8.3 . Просмотр журналов

Для просмотра общего журнала событий, связанного с функционированием Агрегатора и действиями субъектов доступа, следует перейти «Мониторинг – Журнал» (см. Рисунок 4), где визуализируются системные события с указанием уровня важности и источника возникновения события.

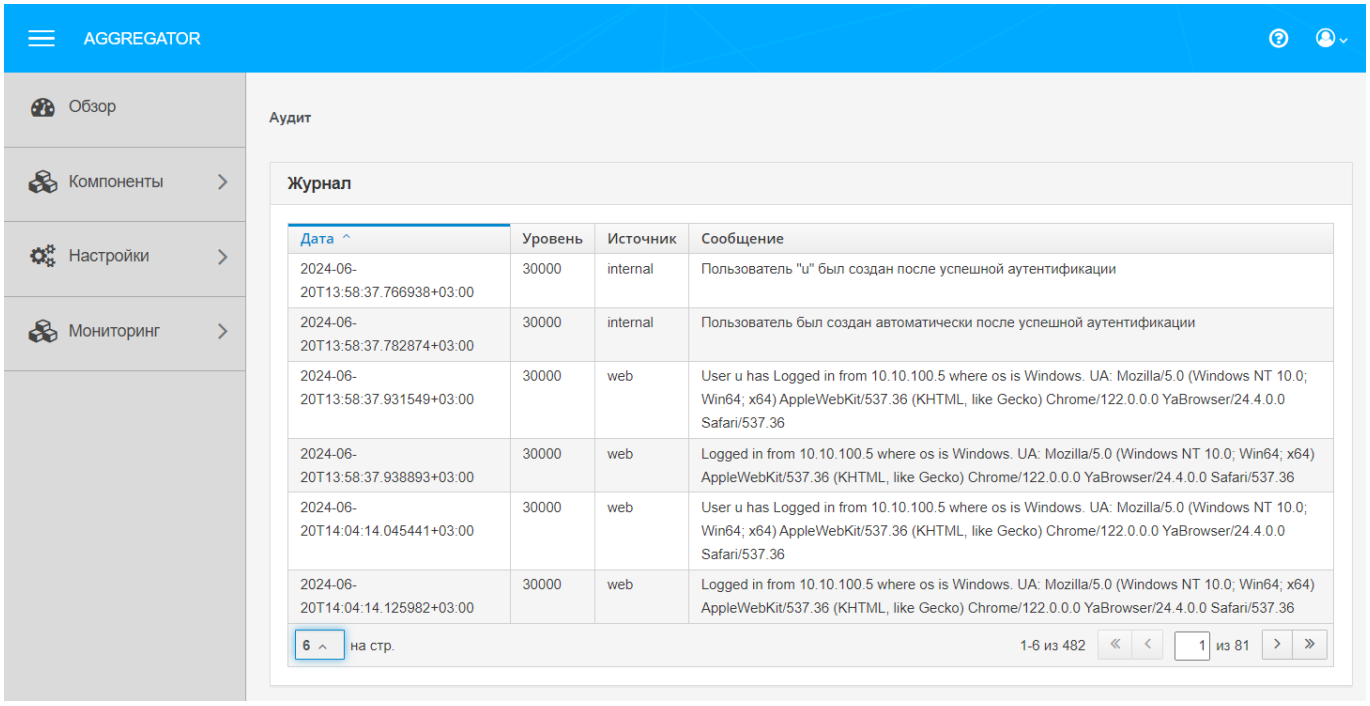

Рисунок 4 – Отображение общего журнала событий

Для просмотра журнала событий, связанного с действиями субъектов доступа, следует перейти «Мониторинг – Аудит» (см. Рисунок 5).

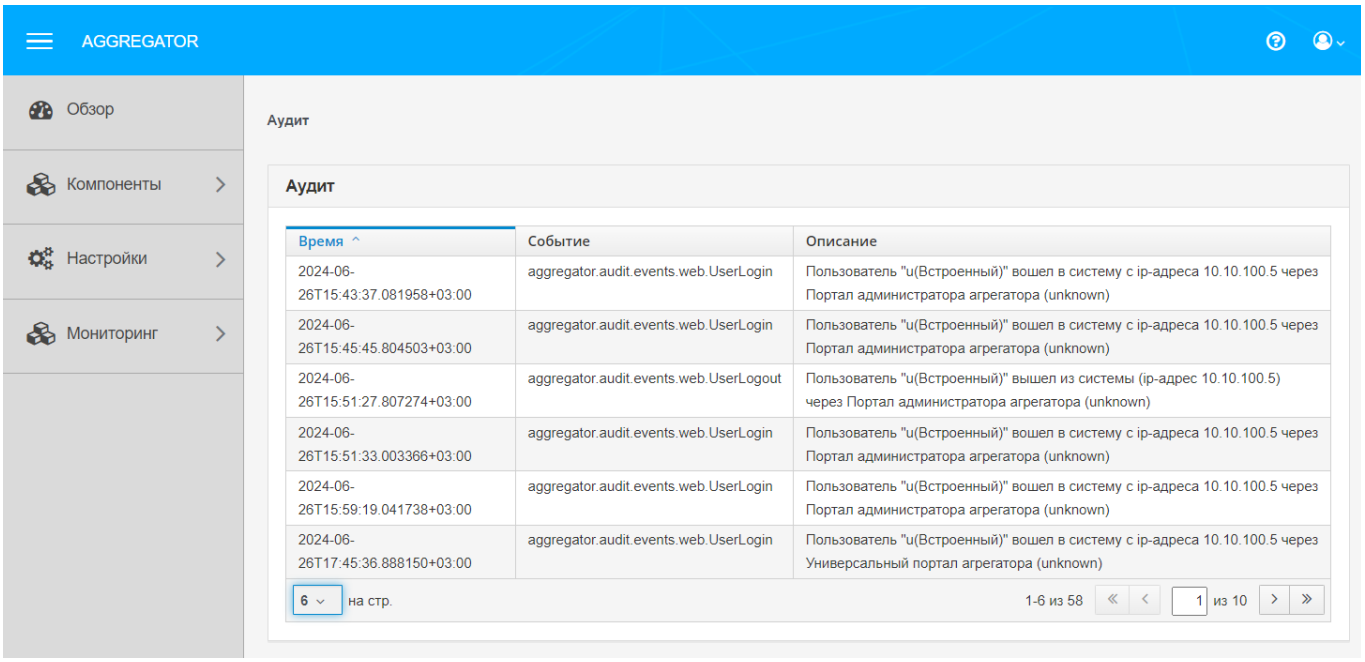

Рисунок 5 – Отображение журнала аудита

8.4 . Описание шаблонов событий аудита

8.4.1 . Типы данных регистрируемой информации событий аудита

При фиксации событий аудита используется ряд типов данных (см. Таблица 12) регистрируемой информации, состав которых может отличаться для разных событий.

Таблица 12 – Типы данных регистрируемой информации

Тип данных	Описание
Дата/время	Дата и время указываются в формате: `DD.MM.YYYY, hh:mm:ss`, где: `DD.MM.YYYY` обозначает «день» - «месяц» - «год»; `hh:mm:ss` обозначает элементы времени «час» - «минута» - «секунда»; «.» 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
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)

8.4.2 . Типы и шаблоны регистрируемых событий аудита

Список регистрируемых событий аудита и шаблоны к ним приведены в таблице (см. Таблица 13).

Таблица 13 – Список типов и шаблонов регистрируемых событий аудита

Событие	Состав регистрируемой информации	Шаблон регистрации события
События, связанные с объектом «Узлы»		
Добавление узла `aggregator.audit.events.provider.create`	Регистрируется: ▪ название узла (`provider_name`); ▪ имя пользователя (`user.name`); ▪ название домена аутентификации (`auth_name`); ▪ название фермы поставщиков ресурсов (`farm_name`)	«Пользователь `[user.name] ([auth_name])` создал узел `[provider_name]`в ферме `[farm_name]`»
Изменение узла `aggregator.audit.events.provider.update`	Регистрируется: ▪ название узла (`provider_name`); ▪ имя пользователя (`user.name`); ▪ название домена аутентификации (`auth_name`); ▪ название фермы поставщиков ресурсов (`farm_name`)	«Пользователь `[user.name] ([auth_name])` обновил узел `[provider_name]`в ферме `[farm_name]`»

Удаление узла aggregator.audit.events.provider.delete	Регистрируется: ▪ название узла (provider_name); ▪ имя пользователя (user.name); ▪ название домена аутентификации (auth_name); ▪ название фермы поставщиков ресурсов (farm_name)	«Пользователь [user.name] ([auth_name]) удалил узел [provider_name]в ферме [farm_name]»
События, связанные с объектом «Ферма поставщик ресурсов»		
Добавление фермы поставщиков ресурсов aggregator.audit.events.farms.create	Регистрируется: ▪ название фермы поставщиков ресурсов (farm_name); ▪ название домена аутентификации (auth_name); ▪ имя пользователя (user.name)	«Пользователь [user.name] ([auth_name]) создал ферму [farm_name]»
Изменение фермы поставщиков ресурсов aggregator.audit.events.farms.update	Регистрируется: ▪ название фермы поставщиков ресурсов (farm_name); ▪ название домена аутентификации (auth_name); ▪ имя пользователя (user.name)	«Пользователь [user.name] ([auth_name]) обновил ферму [farm_name]»
Удаление фермы поставщиков ресурсов aggregator.audit.events.farms.delete	Регистрируется: ▪ название фермы поставщиков ресурсов (farm_name); ▪ название домена аутентификации (auth_name); ▪ имя пользователя (user.name)	«Пользователь [user.name] ([auth_name]) удалил ферму [farm_name]»
События, связанные с объектом «Сайт»		
Добавление сайта aggregator.audit.events.site.create	Регистрируется: ▪ название сайта (site_name); ▪ название домена аутентификации (auth_name); ▪ имя пользователя (user.name)	«Пользователь [user.name] ([auth_name]) создал сайт [site_name]»
Изменение сайта aggregator.audit.events.site.update	Регистрируется: ▪ название сайта (site_name); ▪ название домена аутентификации (auth_name); ▪ имя пользователя (user.name)	«Пользователь [user.name] ([auth_name]) обновил сайт [site_name]»
Удаление сайта aggregator.audit.events.site.delete	Регистрируется: ▪ название сайта (site_name); ▪ название домена аутентификации (auth_name); ▪ имя пользователя (user.name)	«Пользователь [user.name] ([auth_name]) удалил сайт [site_name]»
Добавление правила aggregator.audit.events.rule.create	Регистрируется: ▪ имя пользователя (user.name); ▪ название домена аутентификации (auth_name); ▪ название правила для сайта (rule_name); ▪ название сайта (site_name)	«Пользователь [user.name] ([auth_name]) создал правило [rule_name] для сайта [site_name]»

Изменение правила `aggregator.audit.events.rule.update`	Регистрируется: ▪ имя пользователя (`user.name`); ▪ название домена аутентификации (`auth_name`); ▪ название правила для сайта (`rule_name`); ▪ название сайта (`site_name`)	«Пользователь `[user.name] ([auth_name])` обновил правило `[rule_name]` для сайта `[site_name]`»
Удаление правила `aggregator.audit.events.rule.delete`	Регистрируется: ▪ имя пользователя (`user.name`); ▪ название домена аутентификации (`auth_name`); ▪ название правила для сайта (`rule_name`); ▪ название сайта (`site_name`)	«Пользователь `[user.name] ([auth_name])` удалил правило `[rule_name]` из сайта `[site_name]`»
События, связанные с объектом «Шлюз»		
Добавление шлюза `aggregator.api.webui.gateway.create`	Регистрируется: ▪ название шлюза (`gateway_name`); ▪ имя пользователя (`user.name`); ▪ название домена аутентификации (`auth_name`)	«Пользователь `[user.name] ([auth_name])` создал шлюз `[gateway_name]`, используя аутентификатор `[auth_name]`»
Изменение шлюза `aggregator.api.webui.gateway.update`	Регистрируется: ▪ название шлюза (`gateway_name`); ▪ имя пользователя (`user.name`); ▪ название домена аутентификации (`auth_name`)	«Пользователь `[user.name] ([auth_name])` обновил шлюз `[gateway_name]`, используя аутентификатор `[auth_name]`»
Удаление шлюза `aggregator.api.webui.gateway.delete`	Регистрируется: ▪ название шлюза (`gateway_name`); ▪ имя пользователя (`user.name`); ▪ название домена аутентификации (`auth_name`)	«Пользователь `[user.name] ([auth_name])` удалил шлюз `[gateway_name]`, используя аутентификатор `[auth_name]`»
События, связанные с объектом «Домен аутентификации»		
Создание домена аутентификации `aggregator.audit.events.authenticators.create`	Регистрируется: ▪ название домена аутентификации (`auth_name`); ▪ имя пользователя (`user.name`)	«Пользователь `[user.name] ([auth_name])` создал аутентификатор `[auth_name]`»
Изменение домена аутентификации `aggregator.audit.events.authenticators.update`	Регистрируется: ▪ название домена аутентификации (`auth_name`); ▪ имя пользователя (`user.name`)	«Пользователь `[user.name] ([auth_name])` обновил аутентификатор `[auth_name]`»
Удаление домена аутентификации `aggregator.audit.events.authenticators.delete`	Регистрируется: ▪ название домена аутентификации (`auth_name`); ▪ имя пользователя (`user.name`)	«Пользователь `[user.name] ([auth_name])` удалил аутентификатор `[auth_name]`»

Добавление группы пользователей `aggregator.audit.events.authenticators.group.create`	Регистрируется: ▪ название домена аутентификации (`auth_name`); ▪ имя пользователя (`user.name`); ▪ название группы домена аутентификации (`group_name`)	«Пользователь `[user.name] ([auth_name])` создал группу `[group_name]` у аутентификатора `[auth_name]`»
Изменение группы пользователей `aggregator.audit.events.authenticators.group.update`	Регистрируется: ▪ название домена аутентификации (`auth_name`); ▪ имя пользователя (`user.name`); ▪ название группы домена аутентификации (`group_name`)	«Пользователь `[user.name] ([auth_name])` обновил группу `[group_name]` у аутентификатора `[auth_name]`»
Удаление группы пользователей `aggregator.audit.events.authenticators.group.delete`	Регистрируется: ▪ название домена аутентификации (`auth_name`); ▪ имя пользователя (`user.name`); ▪ название группы домена аутентификации (`group_name`)	«Пользователь `[user.name] ([auth_name])` удалил группу `[group_name]` у аутентификатора `[auth_name]`»
Изменение пользователя в домене `aggregator.audit.events.authenticators.user.update`	Регистрируется: ▪ имя пользователя, который производит действие (`user.name`); ▪ идентификатор пользователя, над которым производится действие (`auth.id`)	«Пользователь `[user.name] ([auth_name])` обновил пользователя с auth_id `[auth.id]`»
Удаление пользователя из домена `aggregator.audit.events.authenticators.user.delete`	Регистрируется: ▪ имя пользователя, который производит действие (`user.name`); ▪ идентификатор пользователя, над которым производится действие (`auth.id`)	«Пользователь `[user.name] ([auth_name])` удалил пользователя с auth_id `[auth.id]`»
События, связанные с объектом «Шаблоны техобслуживания»		
Создание шаблона техобслуживания `aggregator.audit.events.maintenance.template.create`	Регистрируется: ▪ название шаблона техобслуживания (`template_name`); ▪ название домена аутентификации (`auth_name`); ▪ имя пользователя (`user.name`)	«Пользователь `[user.name] ([auth_name])` создал шаблон техобслуживания `[template_name]`»
Изменение шаблона техобслуживания `aggregator.audit.events.maintenance.template.update`	Регистрируется: ▪ название шаблона техобслуживания (`template_name`); ▪ название домена аутентификации (`auth_name`); ▪ имя пользователя (`user.name`)	«Пользователь `[user.name] ([auth_name])` обновил шаблон техобслуживания `[template_name]`»
Удаление шаблона техобслуживания `aggregator.audit.events.maintenance.template.delete`	Регистрируется: ▪ название шаблона техобслуживания (`template_name`); ▪ название домена аутентификации (`auth_name`); ▪ имя пользователя (`user.name`)	«Пользователь `[user.name] ([auth_name])` удалил шаблон техобслуживания `[template_name]`»
События, связанные с пользователем		

Получение пользователем ресурсов `aggregator.audit.events.client.views.services_list`	Регистрируется: ▪ название домена аутентификации (`auth_name`); ▪ имя пользователя (`user.name`)	«Пользователь `[user.name] ([auth_name])` получил список доступных ресурсов»
Вход пользователя в систему `aggregator.audit.events.web.UserLogin`	Регистрируется: ▪ название домена аутентификации (`auth_name`); ▪ имя пользователя (`user.name`); ▪ IP-адрес, с которого был сделан запрос (`ip`)	«Пользователь `[user.name] ([auth_name])` вошел в систему с ip-адреса `[ip]`»
Выход пользователя из системы `aggregator.audit.events.web.UserLogout`	Регистрируется: ▪ название домена аутентификации (`auth_name`); ▪ имя пользователя (`user.name`); ▪ IP-адрес, с которого был сделан запрос (`ip`)	«Пользователь `[user.name] ([auth_name])` вышел из системы (ip-адрес `[ip]`)»

8.4.3 . Форматы регистрируемых событий аудита и их примеры

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

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

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

9 . ПЕРЕЧЕНЬ ТЕРМИНОВ

Термин	Определение
Агрегатор администратора	Веб-интерфейс управления Агрегатором. Устанавливается из пакета `termidesk-vdi`, при выборе пунктов «Агрегатор администратора», «Менеджер рабочих мест (очереди)»
Агрегатор пользователя	Веб-интерфейс пользователя для получения ресурсов, предоставляемых Агрегатором. Устанавливается из пакета `termidesk-vdi`, при выборе пунктов «Агрегатор пользователя», «Менеджер рабочих мест (очереди)»
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. 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. Устанавливается из пакета `termidesk-gateway`. Наименование службы после установки: `termidesk-gateway.service`
Портал администратора	Предоставляет веб-интерфейс для управления Termidesk и интерфейс `swagger` для доступа к ограниченному списку модулей документации по командам REST API
Портал пользователя	Предоставляет пользовательский веб-интерфейс Termidesk (без доступа к функциям управления) и интерфейс `swagger` для доступа к ограниченному списку модулей документации по командам REST API
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

10 . 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