

Руководство администратора

1. Общие сведения

В данном руководстве представлено описание и основные операции с такими компонентами как механизмы управления секретами, методы аутентификации, политики и устройства аудита.

2. Подготовка рабочей среды

Задачи по администрированию компонентов StarVault можно выполнять через UI, CLI или API.

Использование UI не требует специальной подготовки рабочего места. Достаточно при использовании самоподписанного сертификата ЦС добавить его в доверенные, чтобы избавиться от предупреждения при переходе в UI.

Для использования StarVault CLI самоподписанный сертификат ЦС **обязательно** должен быть добавлен в доверенные, в ином случае команды `starvault` будут возвращать ошибку. Например, в RedHat-based дистрибутивах выполните следующие действия:

```
cp /opt/starvault/tls/starvault-ca.pem /etc/pki/ca-trust/source/anchors/  
update-ca-trust enable  
update-ca-trust extract
```

BASH | 

3. Содержание раздела

Переходите в нужный раздел по быстрым ссылкам:

- [Хранилище](#)
 - [Распечатывание хранилища](#)
 - [Ротация ключей](#)
 - [Встроенное хранилище](#)
- [Механизмы управления секретами](#)
 - [Механизм секретов Cubbyhole](#)
 - [Базы данных](#)

- MySQL/MariaDB
- Oracle
- PostgreSQL
- Механизм секретов Identity
- Механизм секретов KV
- Механизм секретов Kubernetes
- Механизм секретов LDAP
- Механизм секретов PKI
 - Настройка и использование
 - Настройка корневого центра сертификации
 - Настройка промежуточного центра сертификации
 - Рекомендации
 - Решение проблем с ACME
 - Rotation primitives
- RabbitMQ
- Механизм секретов SSH
- Механизм секретов TOTP
- Механизм управления секретами Transit
- Управление доступом
 - Аутентификация на основе токенов
 - Методы аутентификации
 - AppRole
 - JWT/OIDC
 - Провайдер OIDC
 - Kerberos
 - Kubernetes
 - LDAP
 - LDAP Meta
 - Login MFA
 - RADIUS
 - TLS сертификаты
 - Токены

- Логин и пароль
 - Логин и пароль. Расширенный
- Аренда, обновление и отзыв
- Блокировка пользователей
- Идентификация
- OIDC провайдер
- Политики доступа
- Аудит
 - Устройство для файлового аудита
 - Устройство аудита Syslog
 - Устройство аудита Socket
- Телеметрия
 - Включение сбора телеметрии
 - Ключевые метрики для общей проверки работоспособности
 - Описание метрик
 - Основные системные метрики
 - Метрики логирования
 - Метрики аутентификации
 - Метрики доступности
 - Метрики базы данных
 - Метрики политик
 - Метрики встроенного хранилища
 - Метрики секретов
 - Полный список метрик
- Рекомендации
 - Рекомендации по настройке
 - Рекомендации по обеспечению безопасности
 - Контроль расходования ресурсов
 - Настройка производительности
- Инструкции
 - Миграция точек монтирования
 - Работа с пользователями, группами

- Ограничение доступа при расследовании инцидентов
- Отправка логов аудита в OpenSearch
- Измерение производительности
- Использование шаблонов в политиках доступа
- Настройка политик паролей
- Диагностика проблем с запуском
- Настройка MFA с использованием TOTP

Руководство по установке платформы

1. Общие сведения

В данном разделе описаны различные способы установки платформы. StarVault поддерживает установку в нескольких вариантах, в зависимости от требований к среде эксплуатации:

1. **Установка в ОС Linux** — простой вариант установки с файловым хранилищем. Не рекомендуется для боевой среды, поскольку не поддерживает высокую доступность.
2. **Установка в режиме высокой доступности (HA)** — StarVault может работать в кластерном режиме с несколькими серверами. Поддержка HA определяется типом хранилища и активируется автоматически, если она доступна. Один из узлов становится активным, остальные — резервными.
3. **Установка в Kubernetes** — возможно развертывание через официальный Helm-чарт в трёх конфигурациях:
 - **Dev** — одиночный сервер StarVault в оперативной памяти для тестирования StarVault;
 - **Standalone** -- одиночный сервер StarVault, сохраняющий данные в томе с помощью бэкенда файлового хранилища (по умолчанию);
 - **High-Availability (HA)** — кластер серверов StarVault, использующих бэкенд хранения высокой доступности.
4. **Установка в Docker Compose или Podman Compose** — поддерживается развертывание через контейнерные среды.
5. **Тестовый режим** — запуск через `Starvault server -dev` без предварительной настройки. Подходит для разработки и экспериментов. Все функции StarVault доступны, но используются небезопасные настройки по умолчанию.

Также в рамках раздела описан процесс миграции секретов из HashiCorp Vault в StarVault. Для быстрого перемещения по разделам воспользуйтесь ссылками в содержании.

2. Содержание раздела

- [Варианты установки](#)
 - [Установка в ОС Linux](#)
 - [Установка в режиме высокой доступности \(HA\)](#)

- Установка в Kubernetes
 - Общие сведения об установке с помощью HELM
 - Установка с помощью HELM
 - Параметры Helm
 - Примеры конфигураций
- Установка в среде выполнения контейнеров
- Установка в тестовом режиме
- Параметры конфигурации
 - Рекомендации по автоматизации
 - Блок конфигурации istener
 - Блок конфигурации seal
 - Опция service registration
 - Блок конфигурации storage
 - Filesystem
 - In-memory
 - PostgreSQL
 - Integrated Storage
 - Блок конфигурации telemetry
 - Блок конфигурации ui
 - Блок конфигурации блокировки пользователей
 - Логирование выполненных запросов
- Миграция секретов из Vault в StarVault



История изменений

Данный раздел содержит историю изменений StarVault

История изменений

- v1