Установка StarVault

1. Базовая установка StarVault

В этом разделе рассматривается установка с хранилищем типа **file**.

Данный вариант настоятельно не рекомендуется использовать в боевой среде, поскольку он не поддерживает высокую доступность.

Для развертывания StarVault в боевой среде воспользуйтесь инструкциями в разделе * Установка в режиме высокой доступности (HA).

1.1. Установка в операционной системе

Предварительные требования:

- На сервер установлена поддерживаемая операционная система (RedOS, Astra Linux, AlmaLinux).

Порядок действий:

1. Добавьте разрешающее правило на сетевом экране для TCP-порта 8200, например для firewalld:

```
firewall-cmd --add-port=8200/tcp --permanent
firewall-cmd --reload
```

В примере используется порт 8200, но вы можете использовать любой другой порт. Конфигурационный файл после установки расположен по пути **/etc/starvault.d/starvault.hcl**.

2. Выполните установку:

   - Для rpm-based систем:

```
curl https://repo-starvault.orionsoft.ru/utils/configs/starvault.repo -o
/etc/yum.repos.d/starvault.repo
sed -i 's/USERNAME/ПОЛЬЗОВАТЕЛЬ/g' /etc/yum.repos.d/starvault.repo ①
sed -i 's/PASSWORD/ПАРОЛЬ/g' /etc/yum.repos.d/starvault.repo ①
yum update
yum install starvault
```

     1. Замените `ПОЛЬЗОВАТЕЛЬ` и `ПАРОЛЬ`

   - Для deb-based систем:

```bash
curl https://repo-starvault.orionsoft.ru/utils/configs/starvault.list -o /etc/apt/sources.list.d/starvault.list
curl https://repo-starvault.orionsoft.ru/utils/configs/repo-starvault.conf -o /etc/apt/auth.conf.d/repo-starvault.conf
sed -i 's/USERNAME/ПОЛЬЗОВАТЕЛЬ/g' /etc/apt/auth.conf.d/repo-starvault.conf ①
sed -i 's/PASSWORD/ПАРОЛЬ/g' /etc/apt/auth.conf.d/repo-starvault.conf ①
apt update
apt install starvault
```

1. Замените `ПОЛЬЗОВАТЕЛЬ` и `ПАРОЛЬ`

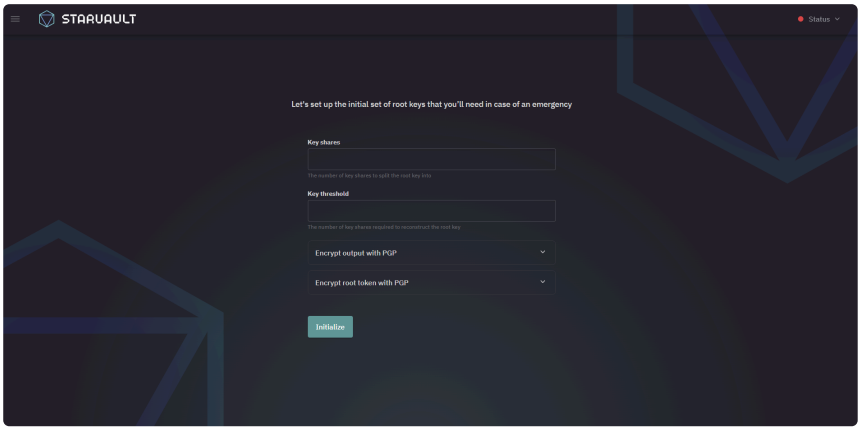
3. После установки пакета автоматически будет сгенерирован самоподписанный сертификат в директории **/opt/starvault/tls/**. Если вы планируете использовать сертификат выданный вашим Центром сертификации, то произведите замену сертификата и перезапустите службу:

```bash
systemctl restart starvault
```

4. Выполните инициализацию:

> Инициализация - это процесс настройки StarVault. Она происходит только один раз, когда сервер запускается с новым бэкендом, который никогда ранее не использовался с StarVault.

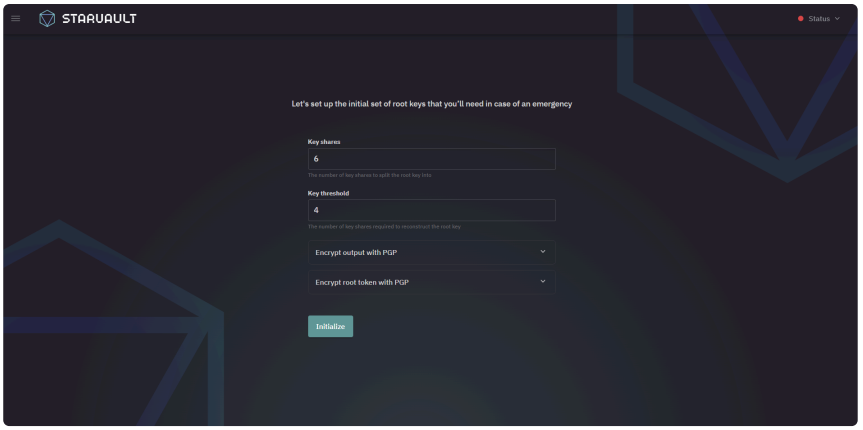
a. В браузере перейдите по адресу **https://SERVER-IP:8200**, где **SERVER-IP** - адрес сервера, на котором развертывается StarVault.



b. В поле **Key shares** введите количество долей ключа на которое будет разделён ключ распечатки

c. В поле **Key threshold** введите количество долей, которого будет достаточно для расшифровывания корневого ключа

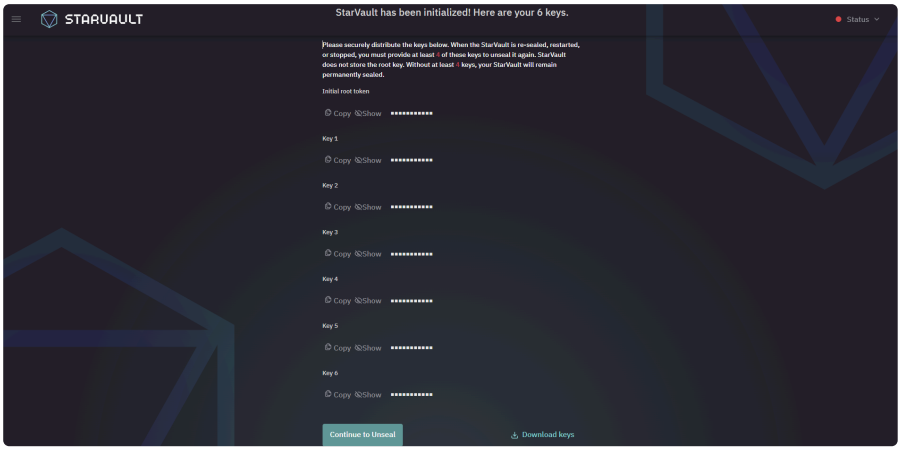
d. Нажмите **[Initialize]** для инициализации StarVault.



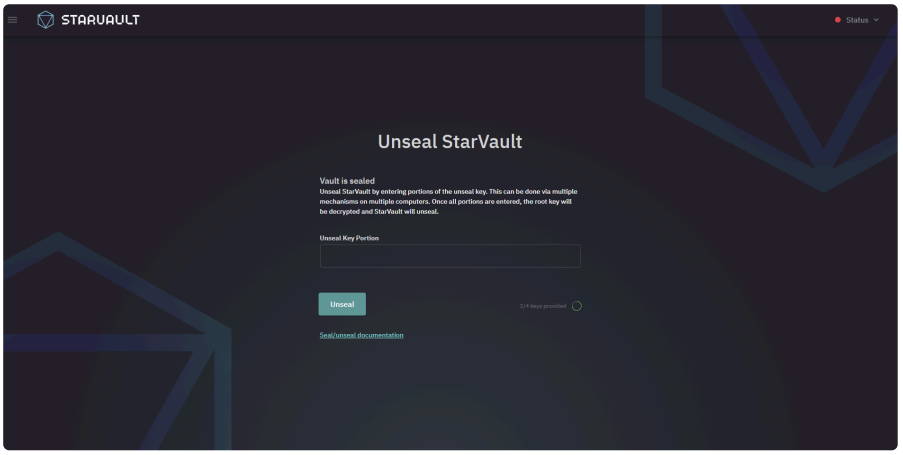
5. После того, как инициализация будет выполнена, на экране будут выведены все части ключа и корневой токен. Сохраните эти данные и нажмите **[Continue to Unseal]** для перехода к распечатыванию хранилища.

> Части ключа и начальный корневой токен крайне важны. Это единственный раз, когда все эти данные известны StarVault, а также единственный раз, когда они должны быть так близко друг к другу.

> Для быстрого сохранения вы можете загрузить токен и доли ключа в формате json, нажав **[Download keys]**.



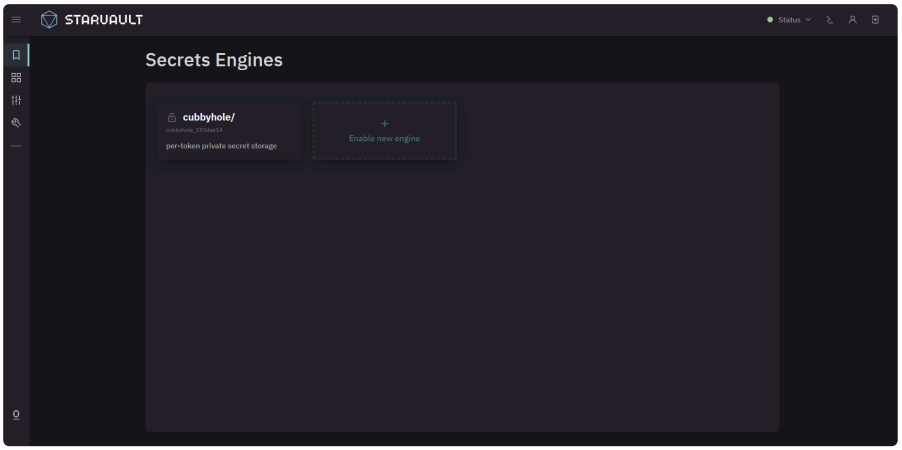
6. Поочередно введите доли ключа распечатки в поле **Unseal Key Portion** в необходимом количестве. После ввода каждой доли нажимайте Unseal



7. После ввода необходимого количества долей, хранилище будет распечатано, на что указывает статус:

8. На экране логина убедитесь, что выбран метод аутентификации **Token** и введите корневой токен, полученный после инициализации. Нажмите **[Sign In]** для входа.

9. При успешном входе вы увидите Secrets Engines.



2025 orionsoft. Все права защищены.

Настройка MFA с использованием TOTP

Проверьте вход в систему StarVault с помощью метода LDAP авторизации:

```bash
starvault login -method=ldap username=w.kluge password='Foo_b_ar123!'
```

Пример вывода:

```
Успешно! Вы прошли аутентификацию. Информация о токене, отображаемая ниже, уже сохранена в помощнике токена. Вам НЕ нужно снова выполнять команду "starvault login". Будущие запросы StarVault будут автоматически использовать этот токен.
```

Key	Value
`token`	`hvs.CAESIEipBa8DtnBePdnrElWEc0WOh2ONelkG-i0wDLAeuHYiGh4KHGh2cy5LMFB6NFJzR0RxcTdncnh6ejdDdXNhTk4`
`token_accessor`	`s7FUF7n3f8BbWzzWRAW0zvXV`
`token_duration`	`768h`
`token_renewable`	`true`
`token_policies`	`["default"]`
`identity_policies`	`[]`
`policies`	`["default"]`
`token_meta_username`	`w.kluge`

Для настройки метода MFA при входе в систему необходимо получить идентификационный токен пользователя `w.kluge`. После чего, необходимо экспортировать его значение в переменную среды `ENTITY_ID` для дальнейшего использования:

```bash
export ENTITY_ID=$(starvault login -method=ldap username=w.kluge \
    password='Foo_b_ar123!' -format=json \
    | jq -r '.auth.entity_id')
```

Для проверки идентификаицонного токена необходимо прописать следующий код:

```bash
echo $ENTITY_ID
fcf3f7bc-5042-11dd-53f5-917aaede9300
```

1. Включение метода многофакторной аутентификации при входе в систему

Необходимо разрешить метод многофакторной аутентификации входа, чтобы применить TOTP к методу аутентификации LDAP.

> Приложения-аутентификаторы не всегда поддерживают одни и те же алгоритмы шифрования. Вам следует узнать, какие алгоритмы поддерживает ваше предпочтительное приложение-аутентификатор. В документации «Настройка метода TOTP MFA» перечислены алгоритмы, поддерживаемые методом Login MFA TOTP. Приложение Google Authenticator, используемое в этом руководстве, поддерживает SHA256.

Настройте метод MFA TOTP для входа в систему и присвойте его идентификатор метода переменной среды `TOTP_METHOD_ID`.

BASH

```
TOTP_METHOD_ID=$(STARVAULT_TOKEN=root starvault write identity/mfa/method/totp \
    -format=json \
    generate=true \
    issuer=StarVault \
    period=30 \
    key_size=30 \
    algorithm=SHA256 \
    digits=6 | jq -r '.data.method_id')
```

Проверьте значение, с помощью команды:

BASH

```
echo $TOTP_METHOD_ID
29a3e898-50e6-5763-7fbe-834df79eea77
```

2. Генерация QR-кода в приложении-аутентификаторе

Введите следующий код для генерации QR-кода в формате PNG:

BASH

```
STARVAULT_TOKEN=root starvault write -field=barcode \
    /identity/mfa/method/totp/admin-generate \
    method_id=$TOTP_METHOD_ID entity_id=$ENTITY_ID \
    | base64 -d > /tmp/qr-code.png
```

Вы можете открыть изображение QR-кода из хост-системы разными способами в зависимости от вашей операционной системы. Вы можете использовать пример для Linux, macOS или Windows.

▶ Linux

▶ macOS

▶ Windows

Вы можете отсканировать это изображение с помощью приложения-аутентификатора, чтобы добавить StarVault TOTP. Для этого необходимо использовать приложение Google Authenticator.

3. Создание принудительного использования MFA при входе в систему

Зафиксируйте метод аутентификации LDAP для использования при создании принудительного применения MFA при входе в систему.

```bash
LDAP_ACCESSOR=$(STARVAULT_TOKEN=root starvault auth list -format=json \
    --detailed | jq -r '."ldap/".accessor')
```

Проверьте значение с помощью:

```bash
$ echo $LDAP_ACCESSOR
auth_ldap_cf1840a4
```

Создайте принудительный порядок:

```bash
STARVAULT_TOKEN=root starvault write /identity/mfa/login-enforcement/adtotp \
    mfa_method_ids="$TOTP_METHOD_ID" \
    auth_method_accessors=$LDAP_ACCESSOR
```

Пример вывода:

```bash
Успешно! Данные записаны в: identity/mfa/login-enforcement/adtotp
```

4. Вход в систему с помощью метода авторизации LDAP

Для этого необходимо использовать CLI, чтобы войти в систему с помощью метода LDAP авторизации во второй раз.

```bash
$ starvault login -method=ldap username=w.kluge password='Foo_b_ar123!'
Enter the passphrase for methodID "01194a79-e2d9-c038-029d-79b0091cafd0" of type
"totp":
```

Введите код TOTP из приложения аутентификатора, когда появится запрос.

Пример успешного вывода:

Key	Value
`token`	`hvs.CAESIE6K0E7BjHv2m1Gj2IAriFhBfUsB6xjtechsRIhL6-wbGh4KHGh2cy5VNDFTZE9XMm96UUN0UDZ1WWtKQm94SkI`
`token_accessor`	`SXxDMVRc35h9OBIdbTAf52RO`
`token_duration`	`768h`
`token_renewable`	`true`
`token_policies`	`["default"]`
`identity_policies`	`[]`
`policies`	`["default"]`
`token_meta_username`	`w.kluge`

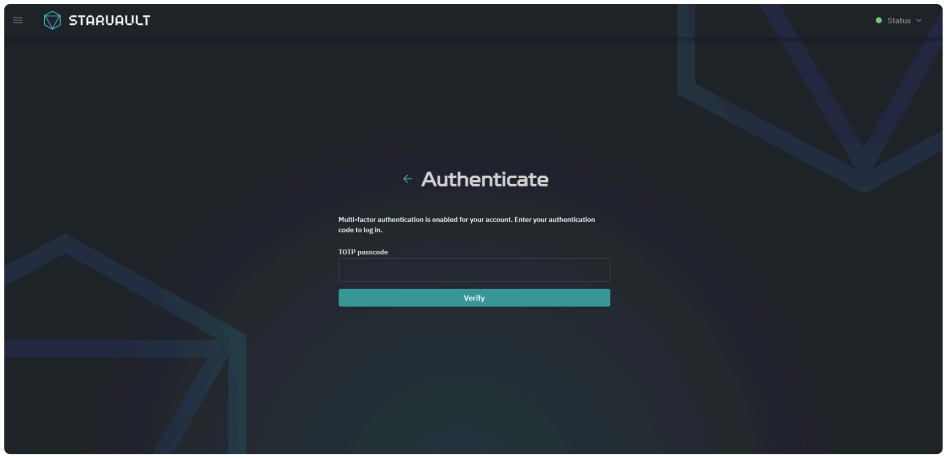
Вы прошли аутентификацию в StarVault с помощью Active Directory. Нажмите **[exit]**, чтобы выйти из контейнера.

Логин по коду TOTP также поддерживается при аутентификации в пользовательском интерфейсе StarVault.

Введите адрес: `http://127.0.0.1:8200`.

В выпадающем меню **Method** выберите **LDAP**.

Введите `w.kluge` в текстовом поле **Имя** пользователя и `Foo_b_ar123!` в текстовом поле **Пароль**, затем нажмите **[Войти]**.



5. Вывод

Как администратор, вы узнали, как включить и настроить функцию авторизации входа в систему с помощью метода LDAP авторизации и метода TOTP MFA.

В качестве пользователя вы узнали, как использовать метод входа в систему MFA при аутентификации в StarVault.

2025 orionsoft. Все права защищены.

Аудит StarVault с Opensearch для реагирования на инцеденты

1. Задача

Оператору StarVault или специалисту по безопасности необходимо реагировать на распространенные инцеденты, которые могут возникнуть при работе кластера StarVault.

Критические типы инцидентов, характерные для StarVault могут включать, но не ограничиваться следующим:

- Доступ пользователя
- Сбой аутентификации
- Скомпрометированный клиентский узел
- Раскрытые учетные данные

Обобщение информации о подобных инцидентах и адекватное реагирование на них в сжатые сроки имеет первостепенное значение для снижения воздействия на производство.

2. Решение

Есть возможность использовать устройства аудита StarVault и отправлять логи с них в инструмент управления информацией и событиями безопасности (SIEM) для объединения, проверки и оповещения. Это решение обеспечивает своевременную информацию для рабочих процессов реагирования на инциденты.

Opensearch с Opensearch Dashboards и Fluentd являются примерами доступных решений с открытым исходным кодом для агрегации и поиска журналов устройств аудита StarVault. В сценарии этого руководства эти технологии будут использоваться в качестве справочного материала, чтобы помочь вам понять, что возможно.

3. Представление сценария

Для выполнения этого сценария используется терминал и интерфейсы командной строки для StarVault и Docker.

Вы развернете и настроите контейнер StarVault в режиме разработки с 2 устройствами аудита:

- Устройство аудита на основе сокетов, которое отправляет логи устройства аудита в Fluentd для использования в Opensearch.
- Устройство аудита на основе файлов для использования в терминале.

4. Предварительные условия

- StarVault, установленный в системном PATH в виде бинарного файла.
- Установлен Docker.
  - Для этого сценария требуется не менее 4 ГБ памяти, выделенной для Docker.
- Вы развернули Opensearch с Opensearch Dashboards и Fluentd у себя в инфраструктуре.

Совет по использованию ресурсов Docker

Для выполнения этого практического лабораторного сценария вам необходимо настроить Docker с доступом к 4 ГБ оперативной памяти и 2 процессорам.

5. Запуск контейнера StarVault

Цель этого раздела - запустить контейнер StarVault, который вы будете использовать для всех действий, связанных с StarVault в сценарии.

Контейнер StarVault, который вы будете разворачивать, работает в режиме dev с хранилищем в памяти и заданным начальным значением `root` токена. Эта небезопасная конфигурация предназначена для простоты лабораторного сценария и не рекомендуется для использования в производстве.

Вы включите два устройства аудита: сокетное устройство аудита, на которое StarVault записывает логи для Elastic Agent, и файловое устройство, которое вы будете использовать из терминала.

1. Разверните контейнер StarVault

```bash
docker run \
  --name learn-starvault \
  --env 'VAULT_DEV_ROOT_TOKEN_ID=root' \
  --env 'VAULT_DEV_LISTEN_ADDRESS=0.0.0.0:8200' \
  --publish 8200:8200 \
  --restart unless-stopped \
  --detach \
  hub.orionsoft.ru/public/starvault:v1.2.0 server -dev
```

2. Экспортируйте переменную окружения для `starvault` CLI, чтобы обратиться к серверу StarVault.

```
$ export STARVAULT_ADDR='http://127.0.0.1:8200'
```

3. Экспортируйте переменную окружения для `starvault` CLI, чтобы аутентифицироваться на сервере StarVault.

```
$ export STARVAULT_TOKEN=root
```

> В рамках данного руководства для работы с StarVault вы можете использовать `root` токен. Однако рекомендуется использовать `root` токены только для первоначальной настройки или в чрезвычайных ситуациях. Лучше всего использовать токены с соответствующим набором политик в зависимости от вашей роли в организации.

4. Включите устройство аудита сокетов и укажите IP-адрес Fluentd, а также укажите тип TCP-сокета.

```
$ starvault audit enable socket \
    description="Socket audit device for Fluentd" \
    address=10.42.42.130:24224 \ ①
    socket_type=tcp \
    format=json
```

① IP адрес и порт Fluentd

Пример успешного вывода:

```
Success! Enabled the socket audit device at: socket/
```

5. Включите устройство аудита файловой системы и укажите путь к `/starvault/logs/starvault-audit.log`, который представляет собой том, сопоставленный с подкаталогом `log` текущего рабочего каталога.

```
$ starvault audit enable file \
    description="File audit device" \
    file_path=/starvault/logs/starvault-audit.log
```

Пример успешного вывода:

```
Success! Enabled the file audit device at: file/
```

Интеграция Opensearch StarVault получает необработанные журналы устройств аудита из StarVault, но добавляет несколько дополнительных полей, полезных для построения более сложных запросов. Эти поля не присутствуют в необработанном выходе устройств аудита StarVault, поэтому вы не найдете их в файловых журналах устройств аудита.

6. Резюме

Вы узнали, как интегрировать StarVault с Opensearch.

7. Очистка

1. Остановите контейнер.

```bash
$ docker stop learn-starvault
```

2. Снимите настройки переменных окружения.

```bash
$ unset STARVAULT_ADDR STARVAULT_TOKEN
```

8. Следующие шаги

Вы можете использовать методы, описанные в этом руководстве, для создания собственного решения для проверки и мониторинга логов устройств аудита. Например, вы можете расширить полученные здесь знания и запустить оповещения для обнаружения угроз безопасности с целью эффективного уведомления и обработки во время реагирования на инциденты.

Можно также рассмотреть расширенный вариант автоматического устранения определенных инцидентов на основе интерпретации содержимого логов устройств аудита.

2025 orionsoft. Все права защищены.