Deckhouse Stronghold

Deckhouse Stronghold — корпоративное хранилище секретов, совместимое с HashiCorp Vault, для централизованного и безопасного управления ключами, паролями и доступами. Поддерживает динамические учётные данные, аудит и интеграцию с корпоративной аутентификацией (OIDC, LDAP), помогая автоматизировать безопасную работу приложений с конфиденциальными данными.

Blitz Identity Provider выступает OIDC-провайдером, а **Deckhouse Stronghold** — OIDC-клиентом (Relying Party).

В этой инструкции описано подключение **Stronghold Standalone** к **Blitz Identity Provider** по протоколу **OIDC (OpenID Connect)**.

Подключение выполняется в два этапа:

- Этап 1. Настройка на стороне Blitz Identity Provider;
- Этап 2. Настройка на стороне Stronghold.

> **Важно:**
>
> В инструкции для примера указано, что Stronghold доступен по адресу `https://stronghold.company.com`, а Blitz Identity Provider доступен по адресу `https://login.company.com`.
> Замените адреса на реальные перед применением инструкции.

Этап 1. Настройка на стороне Blitz Identity Provider

В консоли Blitz Identity Provider перейдите в раздел **Приложения**.

1. Создание пользователя для проверки

Создайте тестового пользователя через `blitz-console` (CLI или веб-консоль).

2. Создание OIDC-приложения для Stronghold

Создайте новое приложение:

- **Название:** stronghold
- **Base URL:** `https://stronghold.company.com`
- **Протокол:** OAuth 2.0 / OIDC

После создания получите:

- `client_id`
- `client_secret`

3. Настройка параметров OIDC клиента

Укажите:

- **Redirect / Callback URL:** `https://stronghold.company.com`
- Разрешённые scopes:
  - `openid` (обязательно);
  - `profile` (опционально);
  - `email` (опционально).

Сохраните

Этап 2. Настройка на стороне Stronghold

Теперь Stronghold настраивается как клиент OIDC.

1. Подготовка TLS и discovery URL

Необходимые значения:

- **Public URL Stronghold:** `https://stronghold.company.com`

- **OIDC Discovery URL Blitz:** `https://login.company.com/.well-known/openid-configuration`

Убедитесь, что TLS сертификаты валидны для DNS-имён.

2. Включение OIDC auth method в Stronghold

Добавьте OIDC метод аутентификации:

- Укажите **Discovery URL Blitz**
- Укажите `client_id` и `client_secret`, полученные ранее

3. Создание роли OIDC

Создайте роль (например, `default-1`):

- привязка к `client_id`
- redirect URL `https://stronghold.company.com`
- scopes `openid` `profile` `email`

4. Настройка ACL-policy

1. Создайте новую **policy** с названием `policy-name` в Stronghold через CLI-интерфейс командой:

```
d8 stronghold policy write policy-name policy-file.hcl
```

Или через API:

```
curl \
  --request POST \
  --header "X-Vault-Token: ..." \
  --data '{"policy":"path \"...\" {...} "}' \
  https://stronghold.example.com/v1/sys/policy/policy-name
```

2. Привяжите её к роли `default-1`

5. Проверка входа

Выполните вход в Stronghold через Blitz Identity Provider. Проверьте:

- доступ к KV;
- чтение/запись секретов согласно `policy-name`.

Возможные проблемы и их решение

Ошибка TLS при добавлении OIDC Discovery URL

Ошибка

`tls: failed to verify certificate`

Решение

1. Перевыпустить сертификат с корректными SAN:

- subjectAltName с DNS и URI
- keyUsage
- extendedKeyUsage=serverAuth
- basicConstraints=CA:FALSE

2. Исправить скрипт `/usr/share/identityblitz/scripts/configure.sh` в части генерации файла конфигурации. Итоговый файл конфигурации должен выглядеть следующим образом:

```
[req]
prompt=no
default_bits=4096
encrypt_key=no
default_md=sha256
```

```
distinguished_name=dn
x509_extensions=ext

[dn]
CN=your-domain.com

[ext]
subjectAltName = @alt_names
subjectKeyIdentifier = hash
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth
basicConstraints = CA:FALSE

[alt_names]
DNS.1 = your-domain.com
URI.1 = https://your-domain.com/blitz/saml
```

Результат успешной интеграции

- Stronghold авторизуется через Blitz как OIDC-провайдер.
- Права доступа разграничиваются через ACL-policy.

Проверенная конфигурация

- Stronghold (standalone): **v1.16.5 EE**
- Blitz Identity Provider: **5.31.4**
- ОС: **Rocky Linux 9.7 x86_64**
- ВМ: 1×node, 4 vCPU, 12 GB RAM, 60 GB disk

Версия #9
Создано 2026-02-13 10:15:38 UTC
Обновлено 2026-07-27 12:55:13 UTC