Konta z Active Directory: Directory Connector i SSO

Typ: procedura

Dotyczy: Vaultwarden 1.37, Bitwarden Directory Connector, Active Directory na dc01/dc02

Czas: ~40 min

Efekt: uczciwa odpowiedź na pytanie, czy Vaultwarden umie logować kontami domenowymi tak jak Gitea. Dwa niezależne mechanizmy, synchronizacja kont z Directory Connectora i logowanie przez zewnętrznego dostawcę tożsamości OIDC, z opisem tego, co faktycznie potwierdzamy w dokumentacji, a czego nie.

Skróty użyte na tej stronie (6)

Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie
AD FS	Active Directory Federation Services: usługa federacji, w której logowanie do aplikacji i chmury sprawdzają serwery w firmie
API	Application Programming Interface: sposób, w jaki programy rozmawiają ze sobą
LDAP	Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA)
OIDC	OpenID Connect: protokół logowania przez zewnętrznego dostawcę tożsamości, na którym opiera się funkcja SSO w Vaultwardenie
SSO	Single Sign-On: jedno logowanie do wielu systemów

Zanim zaczniemy

> **Z ŻYCIA WZIĘTE**
>
> Ola pyta, czy da się podłączyć Vaultwardena do Active Directory tak samo prosto jak Giteę na stronie Logowanie kontem z Active Directory. Odpowiedź nie jest tak prosta: Vaultwarden nie ma własnego mechanizmu LDAP wbudowanego w serwer, tak jak Gitea. Ma za to dwie inne

drogi, każdą z innymi ograniczeniami, które warto poznać, zanim obiecamy zespołowi jedno logowanie do wszystkiego.

Pojęcie: Bitwarden Directory Connector. Osobna aplikacja na komputer, wydana przez firmę Bitwarden, która odczytuje użytkowników i grupy z katalogu (Active Directory, LDAP, Azure AD, G Suite, Okta) i wysyła je do organizacji przez API Bitwardena. Nie jest częścią serwera: instalujemy ją na stacji administratora, obok samego Vaultwardena.

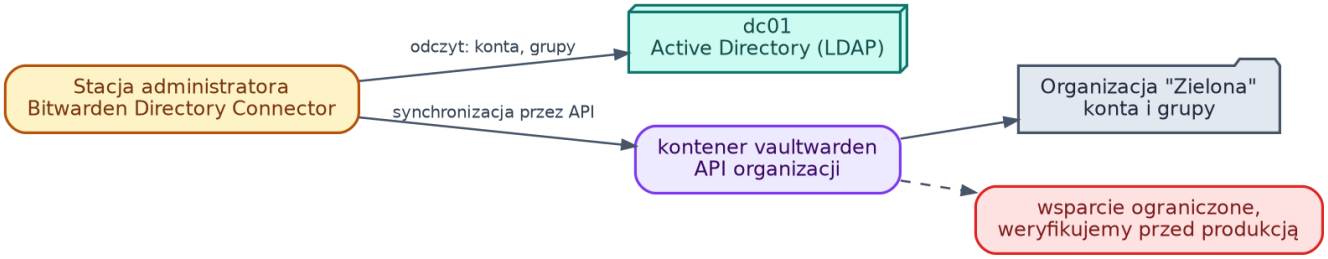
Pojęcie: SSO przez OIDC. Logowanie do Vaultwardena przez przekierowanie do zewnętrznego dostawcy tożsamości mówiącego protokołem OpenID Connect, na przykład Keycloak albo rolę AD FS. To osobna funkcja serwera, niezależna od Directory Connectora, dodana do Vaultwardena później i wciąż aktywnie rozwijana.

Wymaganie	Uwaga
Directory Connector: stacja administratora z Windows	aplikacja dostępna też na macOS i Linuksa, w Zielonej stawiamy ją na stacji IT
Directory Connector: konto techniczne do odczytu AD	wystarczy zwykłe konto z prawem odczytu katalogu, bez uprawnień zapisu
SSO: zewnętrzny dostawca tożsamości mówiący OIDC	w Zielonej go jeszcze nie mamy, może to być rola AD FS na kontrolerze domeny albo osobny Keycloak, decyzja wykracza poza tę stronę
Środowisko testowe przed produkcją	oba mechanizmy warto najpierw sprawdzić w laboratorium na `k3s01`, nie od razu na produkcyjnym `docker01`

Przebieg

1. Synchronizacja kont Directory Connectorem

Directory Connector rozmawia z serwerem tym samym API organizacji, którego używają zwykli użytkownicy Bitwardena do zapraszania członków. Vaultwarden odtwarza dużą część tego API, więc podstawowe zaproszenie kont z Active Directory do organizacji w wielu wdrożeniach działa. Forum Vaultwardena pokazuje to jednak jako temat zgłoszeń i próśb o poprawki, nie jako w pełni potwierdzoną, przetestowaną przez zespół projektu funkcję: watki „Directory Connector support" i „Improvements to the LDAP Directory Connector support" opisują ograniczenia i poprawki wnoszone przez społeczność, nie oficjalną gwarancję zgodności.



Directory Connector czyta konta z dc01 i wysyła je do organizacji Vaultwardena przez API, wsparcie ograniczone (kliknięcie otwiera pełny rozmiar)

Instalacja i pierwsze połączenie z serwerem:

```
Directory Connector → Settings → Server URL: https://hasla.zielona.example
```

Logowanie kontem, które ma prawo zapraszać członków do organizacji „Zielona":

```
Directory Connector → zaloguj się kontem Oli
```

Wskazanie źródła katalogu i zakresu synchronizacji:

```
Directory Connector → Directory type: Active Directory
Directory Connector → Server: dc01.ad.zielona.example
Directory Connector → Base DN: OU=Uzytkownicy,DC=ad,DC=zielona,DC=example
```

Uważaj: mapowanie grup Active Directory na kolekcje Vaultwardena, jedno z ustawień Directory Connectora, zależy od funkcji grup w organizacji Vaultwardena, dodanej stosunkowo niedawno. Sprawdzamy w dokumentacji aktualnej wersji, zanim założymy, że mapowanie zadziała identycznie jak w oficjalnym Bitwardenie, i testujemy na koncie testowym przed synchronizacją całego katalogu.

2. Logowanie przez SSO: OpenID Connect

Ta funkcja jest osobna od Directory Connectora: nie synchronizuje kont z wyprzedzeniem, tylko przekierowuje logowanie do zewnętrznego dostawcy tożsamości w chwili, gdy ktoś próbuje się zalogować. Włączamy ją zmiennymi środowiskowymi w `compose.yaml`, zgodnie z plikiem `.env.template` w repozytorium projektu, sprawdzonym dla aktualnej wersji przed wdrożeniem.



Logowanie SSO: przeglądarka przekierowana do dostawcy OIDC i z powrotem do Vaultwardena (kliknięcie otwiera pełny rozmiar)

```
services:
  vaultwarden:
    environment:
      - SSO_ENABLED=true
      - SSO_ONLY=false
      - SSO_AUTHORITY=https://idp.zielona.example/realms/zielona
      - SSO_CLIENT_ID=vaultwarden
      - SSO_CLIENT_SECRET=${VAULTWARDEN_SSO_SECRET}
```

`SSO_ONLY=false` zostawia też logowanie hasłem głównym obok SSO: przydatne na czas testów i dla kont serwisowych, które nie mają logować się przez przeglądarkę dostawcy tożsamości. `SSO_AUTHORITY` to adres realmu albo dzierżawcy dostawcy OIDC, z którego Vaultwarden pobiera resztę konfiguracji automatycznie.

Uważaj: SSO przez OIDC to funkcja stosunkowo nowa w Vaultwardenie i wciąż aktywnie rozwijana: w repozytorium projektu trafiają się zgłoszenia błędów specyficznych dla konkretnych dostawców tożsamości. Zanim wdrożymy ją produkcyjnie, sprawdzamy dokumentację dokładnie dla wersji, którą instalujemy, i testujemy logowanie na koncie, które nie ma dostępu do niczego krytycznego.

Weryfikacja

Sprawdzamy w panelu administracyjnym, że nowe konto z Directory Connectora rzeczywiście pojawiło się w organizacji:

```
/admin → Users
```

Sprawdzamy w logu kontenera, że Vaultwarden w ogóle widzi konfigurację SSO po restarcie:

```
docker compose logs vaultwarden | grep -i sso
```

Przykład:

```
vaultwarden  | [2026-09-28 11:15:02.004][vaultwarden::sso][INFO] SSO configuration loaded for authority https://idp.zielona.example/realms/zielona
```

Testujemy logowanie testowym kontem przez przycisk „Enterprise single sign-on" na ekranie logowania klienta, zanim udostępnimy je reszcie zespołu.

◫ ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran logowania Vaultwardena z widocznym przyciskiem „Enterprise single sign-on" pod polem na adres e-mail.

Wycofanie zmian

Wyłączenie SSO, bez usuwania kont, które już się przez nie zalogowały:

```
      - SSO_ENABLED=false
```

```
docker compose up -d
```

Odinstalowanie Directory Connectora nie cofa już zaproszonych kont: usuwamy je ręcznie z organizacji przez `Organizations → Zielona → Members`, tak jak każde inne konto.

Gdy coś nie zadziała

Objaw	Przyczyna	Co robimy
Directory Connector zgłasza błąd logowania do serwera	`Server URL` w ustawieniach wskazuje chmurę Bitwardena zamiast `https://hasla.zielona.example`	poprawiamy `Server URL` w `Settings` Directory Connectora
Konta z AD nie pojawiają się w organizacji mimo udanej synchronizacji	konto użyte do synchronizacji nie ma prawa zapraszać członków w organizacji „Zielona"	logujemy Directory Connector kontem z rolą właściciela albo administratora organizacji
Przycisk SSO nie pojawia się na ekranie logowania	`SSO_ENABLED` nie ustawione na `true` albo kontener nie przeładował zmiennych	sprawdzamy `docker compose logs vaultwarden \`

Objaw	Przyczyna	Co robimy
Logowanie przez SSO kończy się błędem po stronie dostawcy tożsamości	niezgodny `SSO_CLIENT_ID` / `SSO_CLIENT_SECRET` albo zły adres przekierowania zwrotnego w konfiguracji dostawcy	porównujemy adres callback z dokumentacją swojej wersji Vaultwardena i z konfiguracją aplikacji po stronie dostawcy OIDC

Powiązane: Pierwsza konfiguracja: panel admina, organizacja i zaproszenia · Logowanie kontem z Active Directory (Gitea, dla porównania) · Active Directory: konta, grupy, jednostki organizacyjne

Źródła: github.com/bitwarden/directory-connector · github.com/dani-garcia/vaultwarden, wiki „Enabling SSO support using OpenId Connect" · github.com/dani-garcia/vaultwarden, wiki „Syncing users from LDAP" · vaultwarden.discourse.group, wątki „Directory Connector support" i „Improvements to the LDAP Directory Connector support"

Revision #23
Created 2026-09-28 16:58:03 UTC by Tomasz Konieczny
Updated 2026-10-26 14:18:30 UTC by Tomasz Konieczny