Vaultwarden: częste problemy

Poziom: operacyjny **Dotyczy: Vaultwarden 1.37, Nginx jako reverse proxy, MailCow**

Czas: ~20 min

Zestawienie objawów, na które zespół IT trafia najczęściej przy pracy z Vaultwardenem: dostęp przez HTTPS, powiadomienia na żywo, pocztę i panel administracyjny. Tabela niżej daje szybką odpowiedź, rozwinięcie pod nią tłumaczy przyczynę do końca.

Skróty użyte na tej stronie (6)

Skrót	Co znaczy
HTTPS	HTTP zabezpieczony szyfrowaniem TLS
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
KDF	Key Derivation Function, funkcja wyprowadzenia klucza: algorytm obliczający z hasła głównego klucz szyfrujący sejf, celowo powolny, żeby utrudnić łamanie hasła siłową metodą
SMTP	Simple Mail Transfer Protocol: protokół wysyłania poczty
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
WebSocket	stałe, dwukierunkowe połączenie przeglądarki z serwerem, przez które Home Assistant na żywo odświeża panele; serwer pośredniczący musi przekazywać nagłówki Upgrade i Connection

Fiszka

TYLKO ODCZYT

Sprawdzenie logu kontenera Vaultwardena: docker compose logs

```
docker compose -f /docker/compose/vaultwarden/compose.yaml logs --tail 100 vaultwarden
```

Pierwsze miejsce diagnozy niemal każdego z objawów niżej.

□□ **docker** = narzędzie do kontenerów

□□ TYLKO ODCZYT

Sprawdzenie aktualnej wartości DOMAIN: docker compose exec env

```
docker compose -f /docker/compose/vaultwarden/compose.yaml exec vaultwarden printenv DOMAIN
```

Przykład:

```
https://hasla.zielona.example
```

□□ **docker** = narzędzie do kontenerów

□□ TYLKO ODCZYT

Sprawdzenie, czy serwer w ogóle odpowiada: curl /alive

```
curl -s https://hasla.zielona.example/alive
```

Endpoint `/alive` zwraca samą datę serwera, bez logowania: szybki test, że Nginx i kontener w ogóle rozmawiają, zanim zaczniemy szukać przyczyny głębiej.

□□ **curl** = client URL: pobieranie i wysyłanie przez HTTP z terminala

Częste błędy

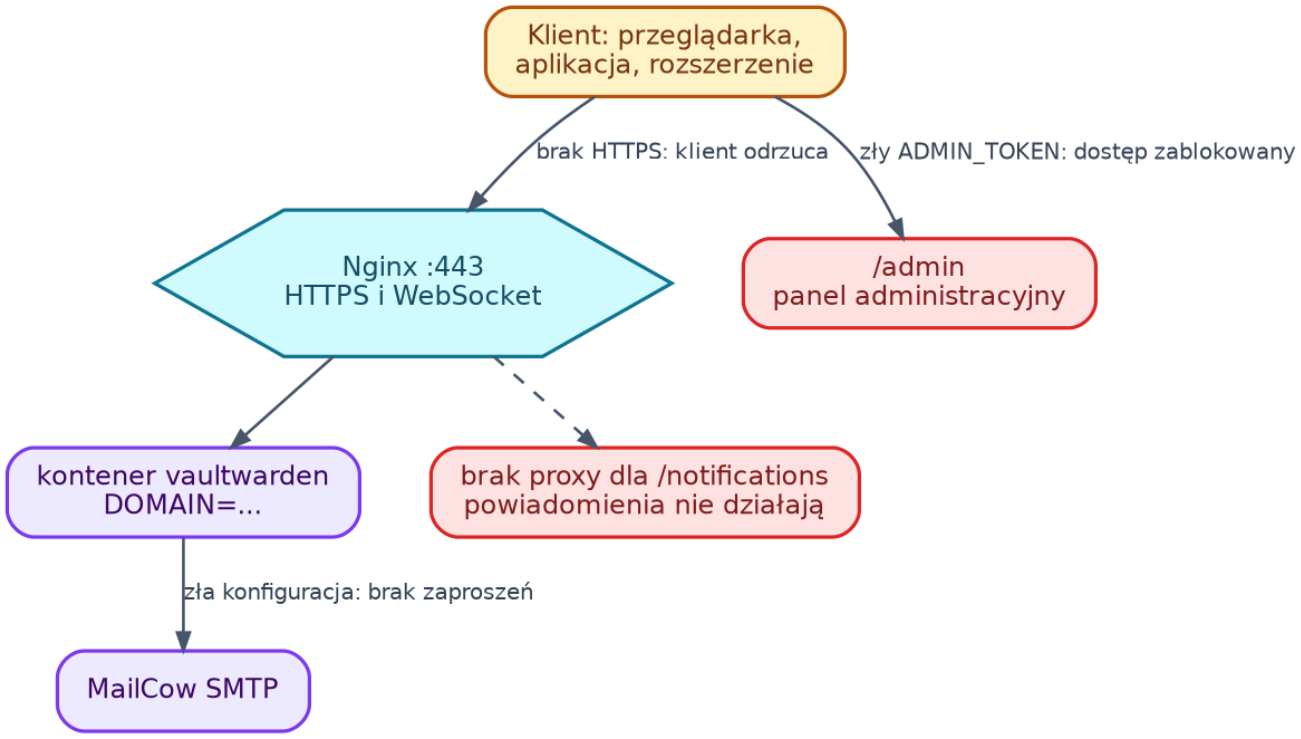
Objaw	Przyczyna	Co robimy
Klient nie odblokowuje sejfu, mimo że strona się otwiera	dostęp po `http://` zamiast `https://`, przeglądarka blokuje Web Crypto API poza bezpiecznym kontekstem	otwieramy wyłącznie adres z `https://`, sprawdzamy certyfikat w Nginksie
Powiadomienia w interfejsie i synchronizacja między urządzeniami nie działają na żywo	Nginx nie przekazuje nagłówków `Upgrade` / `Connection` dla ścieżki `/notifications/hub`	uzupełniamy blok `location /notifications/hub` w konfiguracji Nginksa
Linki w mailach z zaproszeniami wskazują zły adres	`DOMAIN` w `compose.yaml` niezgodny z rzeczywistym adresem instancji	poprawiamy `DOMAIN`, `docker compose up -d`

Objaw	Przyczyna	Co robimy
Zaproszenia i powiadomienia mailowe nie wychodzą	zła konfiguracja SMTP albo MailCow nieosiągalny z `docker01`	`docker compose logs vaultwarden \

Objaw	Przyczyna	Co robimy
Panel `/admin` odrzuca poprawne hasło	`ADMIN_TOKEN` w `.env` niezgodny z hasłem użytym przy `vaultwarden hash`, albo literówka przy wklejaniu hasza w cudzysłowie	generujemy nowy hasz komendą `vaultwarden hash`, wklejamy cały ciąg `$argon2id$...` w pojedynczym cudzysłowie
Panel `/admin` w ogóle nie otwiera się w przeglądarce	`ADMIN_TOKEN` nieustawiony albo pusty, co w niektórych wersjach wyłącza panel całkowicie	sprawdzamy `docker compose exec vaultwarden printenv ADMIN_TOKEN`, uzupełniamy zmienną i restartujemy kontener
Ktoś zapomniał hasła głównego i prosi o odzyskanie	hasło główne nigdy nie trafia na serwer, sam Vaultwarden nie ma jak go sprawdzić ani odtworzyć	patrz rozwinięcie „Zapomniane hasło główne" niżej

HTTPS, WebSocket i droga żądania

Zanim zaczniemy szukać przyczyny konkretnego objawu, przypominamy sobie, którędy w ogóle idzie żądanie od klienta do kontenera, i gdzie w tej drodze mogą leżeć najczęstsze błędy konfiguracji.



Klient, Nginx i kontener vaultwarden: gdzie leżą najczęstsze przyczyny błędów HTTPS, WebSocket, SMTP i panelu admina (kliknięcie otwiera pełny rozmiar)

Brak HTTPS blokuje klienta jeszcze przed dotarciem do samego Vaultwardena, po stronie przeglądarki. Brak przekazywania `Upgrade`/`Connection` dla `/notifications/hub` nie blokuje logowania ani zapisu haseł, tylko powiadomienia na żywo: objaw łatwy do przeoczenia, bo reszta interfejsu działa normalnie, tylko zmiany trzeba odświeżać ręcznie.

Zapomniane hasło główne

> **Pojęcie: KDF.** Funkcja wyprowadzenia klucza: algorytm, który z hasła głównego i dodatkowej soli oblicza klucz szyfrujący sejf, w sposób celowo powolny i trudny do przyspieszenia sprzętowo. Bitwarden i Vaultwarden liczą go zawsze w kliencie, w przeglądarce albo w aplikacji, nigdy na serwerze.

Serwer Vaultwarden przechowuje tylko zaszyfrowane dane i skrót pochodny hasła użyty do samej weryfikacji logowania, nigdy hasła głównego ani klucza wystarczającego do odszyfrowania sejfu. To zamierzona cecha bezpieczeństwa, ta sama co w oficjalnym Bitwardenie: nawet ktoś z pełnym dostępem administracyjnym do serwera i do bazy danych nie odczyta zawartości niczyjego sejfu bez hasła głównego tej osoby.

Jedyna droga odzyskania dostępu bez znajomości hasła to wcześniej włączona polityka organizacji `Account recovery administration`, opisana na stronie Pierwsza konfiguracja: panel admina, organizacja i zaproszenia. Włączenie jej działa tylko na przyszłość: osoba musi zaakceptować udział w mechanizmie odzyskiwania, zanim zapomni hasła, bo dopiero wtedy jej klucz szyfrujący zostaje dodatkowo zaszyfrowany kluczem organizacji. Konto bez wcześniej włączonej i zaakceptowanej polityki, które straci hasło główne, traci dostęp do swojego sejfu bezpowrotnie: jedyne wyjście to założenie konta od nowa i odtworzenie haseł ręcznie albo z ich innych źródeł.

> W Zielonej włączamy `Account recovery administration` dla całej organizacji od razu przy zaproszeniu nowej osoby, zamiast czekać, aż ktoś zapomni hasła i będzie już za późno na przygotowanie odzyskiwania.

□□ Ćwiczenia

1. Pani Halina zgłasza, że nie może zalogować się do rozszerzenia Vaultwarden w domu, mimo że w biurze działa bez problemu. Wskazujemy najbardziej prawdopodobną przyczynę.

Odpowiedź

Najpierw sprawdzamy, czy w domu w ogóle otwiera się adres `https://hasla.zielona.example` po HTTPS: jeśli firma wystawia go tylko wewnątrz sieci firmowej, bez VPN dom nie ma jak się połączyć. Jeśli adres się otwiera, ale logowanie mimo to nie działa, sprawdzamy `Self-hosted → Server URL` w ustawieniach rozszerzenia na tym domowym komputerze.

1. Zespół zgłasza, że zmiany w kolekcji widoczne są dopiero po ręcznym odświeżeniu strony, nigdy same. Wskazujemy, co sprawdzamy w pierwszej kolejności.

Odpowiedź

Konfigurację Nginksa dla ścieżki `/notifications/hub`: brak przekazywania nagłówków `Upgrade` i `Connection` wyłącza powiadomienia na żywo, ale nie blokuje reszty interfejsu, więc łatwo pomylić ten objaw z czymś poważniejszym.

1. Handlowiec zgubił kartkę z hasłem głównym i prosi administratora o zresetowanie go tak, jak resetuje się hasło domenowe w Active Directory. Wyjaśniamy, dlaczego to nie zawsze jest możliwe.

Odpowiedź

Hasło główne nigdy nie trafia na serwer: klucz szyfrujący sejf powstaje z niego lokalnie w kliencie. Bez wcześniej włączonej i zaakceptowanej przez tę osobę polityki `Account recovery administration` administrator nie ma żadnego technicznego sposobu na odczytanie ani zresetowanie dostępu do istniejącego sejfu, w odróżnieniu od hasła domenowego w Active Directory.

Powiązane: Instalacja Vaultwardena w Dockerze · Pierwsza konfiguracja: panel admina, organizacja i zaproszenia · Konta z Active Directory: Directory Connector i SSO · Kopia zapasowa i aktualizacja Vaultwardena

Źródła: github.com/dani-garcia/vaultwarden, wiki „Enabling admin page" i „Enabling WebSocket notifications" · bitwarden.com/help, artykuły o hasle głównym i KDF · dokumentacja Nginx, dyrektywy `proxy_set_header Upgrade` / `Connection`

Revision #23
Created 2026-09-28 16:58:06 UTC by Tomasz Konieczny
Updated 2026-10-26 14:18:33 UTC by Tomasz Konieczny