



Zarządzanie kluczami tajnymi w środowiskach DevOps

Połączenie szybkości, elastyczności i bezpieczeństwa

Szybkie, iteracyjne cykle pracy DevOps często uwidaczniają wiele luk w zabezpieczeniach związanych bezpośrednio z zarządzaniem uprawnieniami. Każdy kontener, serwer czy aplikacja może wymagać dostępu uprzywilejowanego a to znacznie rozszerza powierzchnię ataku dla intruzów poszukujących punktu wejścia. Pogodzenie szybkich, dynamicznych praktyk DevOps oraz wdrożeń RPA z niezbędnymi politykami bezpieczeństwa bywa trudne. DevOps Secrets Vault firmy Delinea automatyzuje zarządzanie kluczami tajnymi, by zapewnić zespołom DevOps szybkość i elastyczność potrzebne do produktywnej pracy bez zaniedbywania bezpieczeństwa. Rozwiązanie to sprawdza się we wszystkich sytuacjach, w których urządzenia wymieniają się kluczami tajnymi, w tym na potrzeby baz danych oraz aplikacji podczas wdrażania oprogramowania i infrastruktury, testowania, organizowania i konfiguracji.

✓ Większa sprawność, łatwiejsza obsługa i mniejszy nakład pracy

- Kluczami tajnymi możesz zarządzać odpowiednio do szybkości i skali potoków DevOps oraz wdrożeń RPA.
- Zasady DevOps i RPA możesz stosować bezpiecznie bez konieczności obciążania lokalnej instancji magazynu kluczy.
- Wyeliminuj ryzyko niespójnych instancji magazynu kluczy i zmniejsz koszt posiadania dzięki rozwiązaniu SaaS.
- Wystawiaj certyfikaty X.509 i SSH, umożliwiając automatyczne podpisywanie i dystrybucję certyfikatów.

✓ Szybki dostęp do funkcjonalności

- Szybkie rozpoczęcie pracy z chmurowym rozwiązaniem, które udostępnia interfejsy REST API i wiersza poleceń.
- Łączność z dowolną platformą w potoku DevOps lub wdrożeniu RPA.
- Korzyści z nieograniczonej skalowalności.

✓ Maksymalizacja produktywności zespołów programistycznych, ds. bezpieczeństwa i operacyjnych

- Automatyczne cofanie przydziału niepotrzebnych już kluczy tajnych.
- Minimalizacja niekontrolowanego przyrostu kont uprzywilejowanych
- Elastyczność dzięki rozwiązaniu współdzielącemu z dowolnymi platformami.
- Brak konieczności budowania i utrzymywania własnej infrastruktury.

✓ Redukcja ryzyka operacji w dynamicznych, elastycznych środowiskach

- Zabezpieczenie powierzchni ataku dzięki kontroli nad dostępem uprzywilejowanym
- Brak konieczności zapisywania na stałe kluczy tajnych w kodzie i skryptach.
- Scentralizowane, ujednolicone i umożliwiające audyt zarządzanie dostępem do kluczy tajnych oraz jego egzekwowanie.
- Eliminacja ciągłego dostępu do infrastruktury o znaczeniu krytycznym przy użyciu dynamicznych kluczy tajnych.

Rozwijaj nowoczesne środowiska DevOps bezpiecznie i bezproblemowo.

DevOps Secrets Vault to magazyn umożliwiający szybkie tworzenie, archiwizowanie i pobieranie kluczy tajnych. Centralizuje on zarządzanie, egzekwuje zdania kontroli dostępu i zapewnia automatyczne rejestrowanie działań do celów śledzenia. Umożliwia minimalizację przyrostu kont z uprawnieniami i wzmacnia powierzchnię ataku, aby obniżyć ryzyko bez uszczerbku dla produktywności.

Bezpieczny magazyn kluczy tajnych dla DevOps – zapisuj poświadczenia dające uprawnienia w szyfrowanym, scentralizowanym magazynie o modelu SaaS w ciągu minut, a nie godzin.

Centralizacja kluczy tajnych – wyeliminuj zróżnicowane instancje magazynów kluczy tajnych na rzecz rozwiązania współpracującego z różnymi platformami, które egzekwuje bezpieczny dostęp do kluczy tajnych i umożliwia pełny audyt.

Automatyzacja i skalowanie – wybierz automatyczny interfejs (wiersz poleceń i API) zbudowany pod kątem szybkości i skali potoków DevOps oraz wdrożeń RPA.

Zarządzanie kluczami tajnymi – wyeliminuj ciągły dostęp do baz danych (MySQL, PostgreSQL i Oracle) oraz platform chmurowych (AWS, Azure i GCP).

Wystawianie certyfikatów – wystawiaj certyfikaty X.509 i SSH, umożliwiając automatyczne podpisywanie i dystrybucję certyfikatów.

```
(3) Pass (linux only)
(4) Windows Credential Manager (windows only)
Selection:
Please enter directory for file store (default:/root/.thy):
Please enter cache strategy for secrets:
(1) Never (default)
(2) Server then cache
(3) Cache then server
(4) Cache then server, but allow expired cache if server unreachable
Selection:
Please enter auth type:
(1) Password (default)
(2) Client Credential
(3) AWS IAM (federated)
(4) Azure (federated)
Selection:
Please enter username for password auth: admin
Please enter password for password auth:
Please enter password for password auth (confirm):
rootcollector:~/.thyotic# ./thy auth
{
  "accessToken": "eyJhbGciOiJIUzI1NiIsInR5cCI6IWRXVj09LWVhbnR5bW91ZS5ldGVuYX0iLCJ1bm91ZSI6IjE0MDA4NTAxOTQ5Im",
  "refreshToken": "eyJhbGciOiJIUzI1NiIsInR5cCI6IWRXVj09LWVhbnR5bW91ZS5ldGVuYX0iLCJ1bm91ZSI6IjE0MDA4NTAxOTQ5Im",
  "expiresIn": 3600,
  "granted": "2019-02-11T00:45:13.258727771Z",
  "refreshToken": "eyJhbGciOiJIUzI1NiIsInR5cCI6IWRXVj09LWVhbnR5bW91ZS5ldGVuYX0iLCJ1bm91ZSI6IjE0MDA4NTAxOTQ5Im",
  "tokenType": "bearer"
}
rootcollector:~/.thyotic# ./thy secret read main
{"attributes": null, "data": {"password": "nothing2"}, "id": "d94a8203-b70f-4a0f-b9ac-e1881b4f04fd", "path": "main"}
rootcollector:~/.thyotic# ./thy secret read main -b
{"attributes": null, "data": {"password": "nothing2"}, "id": "d94a8203-b70f-4a0f-b9ac-e1881b4f04fd", "path": "main"}
```

✓ Najważniejsze funkcje

Ochrona kluczy tajnych potrzebnych zespołom DevOps oraz narzędziom zrobotyzowanej automatyzacji procesów (RPA) do korzystania z aplikacji, usług oraz baz danych dzięki:

- Zaawansowanej automatyzacji
- Nieograniczonej skalowalności
- Buforowaniu lokalnemu
- Uwierzytelnianiu w chmurze
- Wysokiej dostępności i odzyskiwaniu danych po awarii
- Uwierzytelnianiu przy użyciu OpenID Connect
- Dynamicznym kluczom tajnym do IaaS i baz danych
- Wystawianiu certyfikatów
- Obsłudze wielu języków i narzędzi CI/CD
- Integracji z narzędziami PAM i SIEM
- Tymczasowym poświadczeniom z określonym czasem życia
- Jednorazowym adresem URL do ładowania początkowego

Wypróbuj DevOps Secrets Vault bezpłatnie: [Delinea.com](https://delinea.com)

Delinea

Delinea jest produkującym producentem rozwiązań do zarządzania dostępem uprzywilejowanym (PAM, privileged access management) dla nowoczesnych, hybrydowych przedsiębiorstw. Upraszczamy dostęp uprzywilejowany, podnosząc równocześnie poziom bezpieczeństwa, zapewniając zgodność z regulacjami prawnymi i zmniejszając ryzyko. Delinea zapewnia bezpieczeństwo dla ponad 14 000 klientów z całego świata. Do grona naszych klientów należą największe na świecie instytucje finansowe, agencje wywiadowcze oraz firmy z branży infrastruktury o znaczeniu krytycznym. delinea.com