



Automatisierte Installation des Passwort- Management Systems Vaultwarden via Puppet

Noah van Altena
IPA Präsentation
4. April 2025

Übersicht



- Ausgangslage
- Aufgabenstellung
- Puppet
- Realisierung
- Resultat
- Herausforderung
- Kritik
- Ausblick
- Fazit

Ausgangslage



- Veraltetes MediaWiki-basiertes Passwort-Management-System
- Keine selektive Freigabe von Passwörtern, rein webbasierter Zugriff
- Bedarf an einer modernen, zentralisierten Lösung

Aufgabenstellung



- Entwicklung einer Puppet-Rolle zur automatisierten Installation und Konfiguration von Vaultwarden
- Umsetzung aller Funktionalitäten: Webinterface, Datenbankbindung, LDAP-Authentisierung via HTTP-Basic-Auth-Challenge
- Integration in eine CI/CD-Pipeline mit automatisierter Validierung und Unit Tests

Puppet



- Konfigurationsmanagement-Tool für die automatisierte Systemverwaltung
- Nutzung von Rollen, Profilen und Modulen für Modularität
- Hiera: Trennung von Daten und Code für flexible Konfiguration
- Environments: Darstellung verschiedener Entwicklungsstadien (Test, Integration, Produktion)

Realisierung



- Hauptklasse `init.pp` bindet alle Unterklassen (install, database, config, service) ein
- Templates (z. B. `vaultwarden.cfg.erb`) setzen konfigurationsrelevante Parameter um
- Hier ermöglicht das Überschreiben von Standardwerten

```
class vault_vaultwarden {  
  include vault_vaultwarden::install  
  include vault_vaultwarden::database  
  include vault_vaultwarden::config  
  include vault_vaultwarden::service  
}
```

```
## Domain settings  
DOMAIN=<%= @domain %>  
## Mail specific settings  
SMTP_FROM=<%= @smtp_from %>  
## Controls if new users can register  
SIGNUPS_ALLOWED=<%= @signups_allowed %>
```

```
vault_vaultwarden::config::domain: "https://vaultwarden-test.stepping-stone.ch"  
vault_vaultwarden::config::smtp_from: "%{lookup('stoney_mail_client::account')}"  
vault_vaultwarden::config::signups_allowed: false
```

Resultat



- Vollautomatisierte Installation und Konfiguration von Vaultwarden
- 100+ Optionen via Hiera konfigurierbar
- Integrierter Webserver, Datenbank und LDAP-Authentisierung via HTTP-Auth
- CI/CD-Pipeline prüft Änderungen auf Syntax und Fehler

Resultat



stepping stone

Firefox browser window showing the Vaultwarden web interface. The address bar shows `https://vaultwarden-test.stepping-stone.ch/#/vault`. A green notification box at the top right says "Item saved".

Vaultwarden Password Manager

All vaults

FILTERS

Search vault

- All vaults
 - My vault
 - stepping stone AG
 - New organisation
- All items
 - Favourites
 - Login
 - Card
 - Identity
 - Secure note
 - Folders
 - No folder
 - Collections
 - Testcollection
 - Bin

<input type="checkbox"/> All	Name	Owner
<input type="checkbox"/>	Test Password Test Username	Me

Bottom navigation: Password Manager, Admin Console

Pipeline Jobs 2 Tests 0



Herausforderung



- Konfigurationsoptionen im Puppet Modul abbilden
 - Werden via If-Else statements im Template verwaltet
- Optimierung von Lookups und Entfernung fest kodierter Werte
- Load Balancer mit exportierten Ressourcen konfigurieren

Pro:

- Open-Source: Keine Lizenzkosten
- Self-hosted
- Modernes Webinterface
- API + CLI-Unterstützung: Ermöglicht Integration in Automatisierung und Skripte.
- Webbrowser-Add-ons
- Geringe Systemanforderungen

Contra:

- Keine native LDAP-Anbindung
- Authentifizierung über HTTP Basic Auth oder externen Reverse Proxy (z. B. Apache/Nginx) möglich
- Kein offizieller Support: Zwar gibt es eine aktive Community, aber keinen bezahlten Enterprise-Support.
- Vaultwarden ist ein inoffizieller Rust-Port von Bitwarden Server (Community-Projekt, nicht das offizielle Bitwarden Inc.-Produkt).

Ausblick



- Testen der CLI und API Komponenten
- Sicherheitstests und Überprüfung der erstellten Rolle
- Planen der gewollten Standardkonfigurationen
- Einführung in produktive Umgebung
- Datenmigration der Passwörter in Vaultwarden
- Schreiben von Benutzeranleitungen

Fazit



- Erfolgreiches Projekt mit hoher Automatisierung und Stabilität
- Fundiertes technisches Wissen und wertvolle Praxiserfahrungen gewonnen
- Entscheidungsgrundlage für den produktiven Einsatz von Vaultwarden geschaffen

Fragen?

