Secrets in Puppet

Meetup Puppet User Group DACH
09.02.2022

Was sind Secrets? Wie schützt man Secrets?

Secrets sind schützenswerte Informationen:

- Passwörter
- Keys und Zertifikate
- Tokens
- …

Secrets sollten verschlüsselt abgelegt (GIT) oder in einem Secrets Store hinterlegt werden (Hashicorp Vault)

Secrets sollten nicht als Plain-Text Diff angezeigt werden (Puppet Report)

Wie schützt man Secrets in GIT?

Hiera-EYAML oder Hiera-EYAML-GPG

EYAML = Encrypted YAML

Hiera-EYAML: ein public/private Key Paar (üblicherweise PKCS7)

Hiera-EYAML-GPG: GPG Keyring mit mehreren GPG Keys (für jeden User ein Key)

Wie schützt man Secrets im Puppet Report?

Sensitive Daten Typ

- ersetzt Plain Text Secrets im Report durch den String ‘[redacted value]’
- muss im Puppet Code hinterlegt werden

EYAML

Passwörter in GIT im Klartext.

Hiera-eyaml public-private Key Paar

1. Eyaml Installieren
   a. Puppet Server Agent: /opt/puppetlabs/puppet/bin/gem install hiera-eyaml
   b. Puppet Server Compiler: puppetserver gem install hiera-eyaml (ist bei neueren Puppet Server Versionen schon vorhanden!
2. Keys erzeugen: /opt/puppetlabs/puppet/bin/eyaml createkeys
3. Public Key in das Control-Repo, Private Key auf den Puppet Server
4. Hiera konfigurieren für eyaml

EYAML-GPG

Passwörter in GIT im Klartext.

Hiera-eyaml-gpg

1. Eyaml-GPG Installieren
   a. Puppet Server Agent: /opt/puppetlabs/puppet/bin/gem install hiera-eyaml-gpg ruby_gpg
   b. Puppet Server Compiler: puppetserver gem install hiera-eyaml-gpg ruby_gpg
2. GPG Key importieren: gpg --import <file>
3. Hiera konfigurieren für eyaml-gpg

Vault

Passwörter auslagern.

Hiera für Vault konfigurieren

1. Eyaml-GPG Installieren
   a. Puppet Server Agent: /opt/puppetlabs/puppet/bin/gem install vault debouncer
   b. Puppet Server Compiler: puppetserver gem install vault debouncer
2. Vault Token auf dem Puppet Server hinterlegen
3. Hiera konfigurieren für Vault

Sensitive Daten Typ

Passwörter im Report in Plain Text

Lösung: Sensitive Daten Typ (muss durch die Modul Entwickler zur Verfügung gestellt werden!)

Beispiel Code:

```
class application (
  Sensitive $db_pass,
){
}
```

Sensitive Daten Typ

Sensitive Daten in Hiera

- Hiera liefert den Daten Typ zurück, der auffindbar ist.
- Sensitive Date benötigen den Sensitive Daten Typ
- Hiera mitteilen, was man braucht:

```
lookup_options:
  application::db_pass:
    convert_to: Sensitive
```

Secrets in Puppet Demo

Meetup Puppet User Group DACH
09.02.2022