



Building an safe access into your cloud app with HashiCorp Vault

FOSDEM - 03/02/2018

Who Am I

- Thomas Gerbet (@el_suisse)
- @TuleapOpenALM contributor and maintainer
- @GreHackConf organizer
- Alpaca lover



A Bit of Context

- SaaS provider
- Main contributors of the software
 - We can develop specific feature for the SaaS usage
- Web based
 - REST API
 - PHP
- Single Tenant
- Support



SaaS and Access Management: Challenges

Customer's data are only as safe as the provider is

- Do not maintain unnecessary or permanent accesses
- Restrict access to selected team members
- Something bad will happen someday, plan for it

Accountability / Auditability

- What?
- When?
- Who?

• Keep things usable

- Must work for people doing the day-to-day job

HashiCorp Vault



HashiCorp

HashiCorp Vault Backends

Authentication

- AppRole
- AWS
- Google Cloud
- Kubernetes
- GitHub
- LDAP
- MFA
- Okta
- RADIUS
- TLS certs
- Tokens
- Username/Password

Audit

- File
- Syslog
- Socket

Secrets

- AWS
- Consul
- Databases
- Key/Value
- Nomad
- PKI
- RabbitMQ
- SSH
- TOTP
- Transit

Building its own dynamic Vault secret backend

• Vault supports plugins since August 2017

- Basic knowledge of Go is enough
- You can build for your specific use case
- Still get all the nice Vault features

• Support is needed in your software

- Be able to create (and revoke) short lived accounts
- Authenticate requests coming from Vault

Public-Key Cryptography is Awesome

No hardcoded credentials

- Vault generates and stores the private key
- Instances of your app only knows the public key to authenticate requests

• libsodium (Ed25519 signatures)

- Modern cryptography
- Bindings widely available
 - Go
 - golang.org/x/crypto/ed25519
 - PHP
 - \geq 7.2: standard library
 - ≤ 7.1 : extension or polyfill (thanks @ParagonIE)

Requesting an account



Plan for the worst

Revocation

- Immediate
- Granularity:
 - One specific lease
 - All leases of a specific user
 - All leases

Seal the Vault

- All operations are blocked
- Lets you minimize and assess damage in case of a detected intrusion

Outcome

HashiCorp Vault

- Integrates nicely in your existing infrastructure
- Highly flexible secrets management
- Audit capabilities

• One more sensitive endpoint in our software \otimes

- Still better than hardcoded credentials though

Usability

- Authenticate against Vault \rightarrow Request account \rightarrow Log into the instance
- Only CLI 😐

Questions?

