Gestión de secretos Con vault

¿Quién soy?

ReD

Defensor de la privacidad
Entusiasta de la tecnología
Especialista en seguridad
Cofundador de M4H
Cofundador de Hacklabs
Formador cuando me dejan

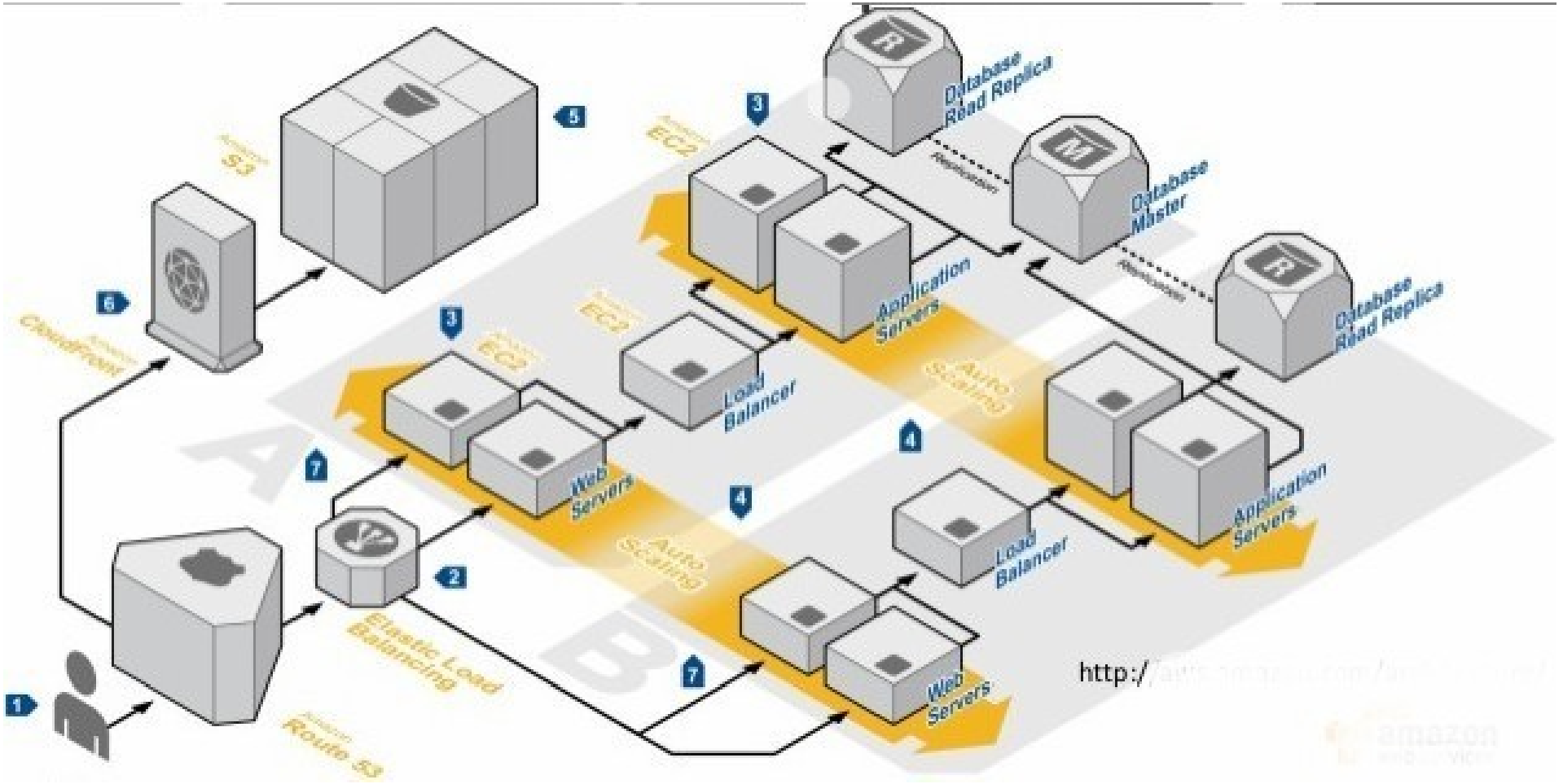
¿Qué son los secretos?

- Contraseñas
- Keytabs
- Certificados
- ...

Infraestructuras Legacy

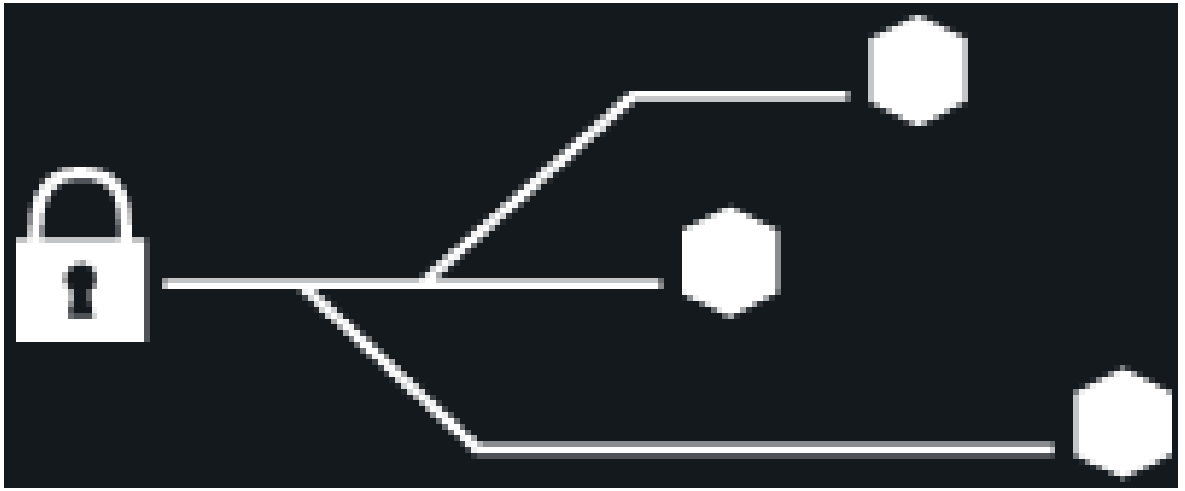
Infraestructuras modernas

Infraestructuras modernas



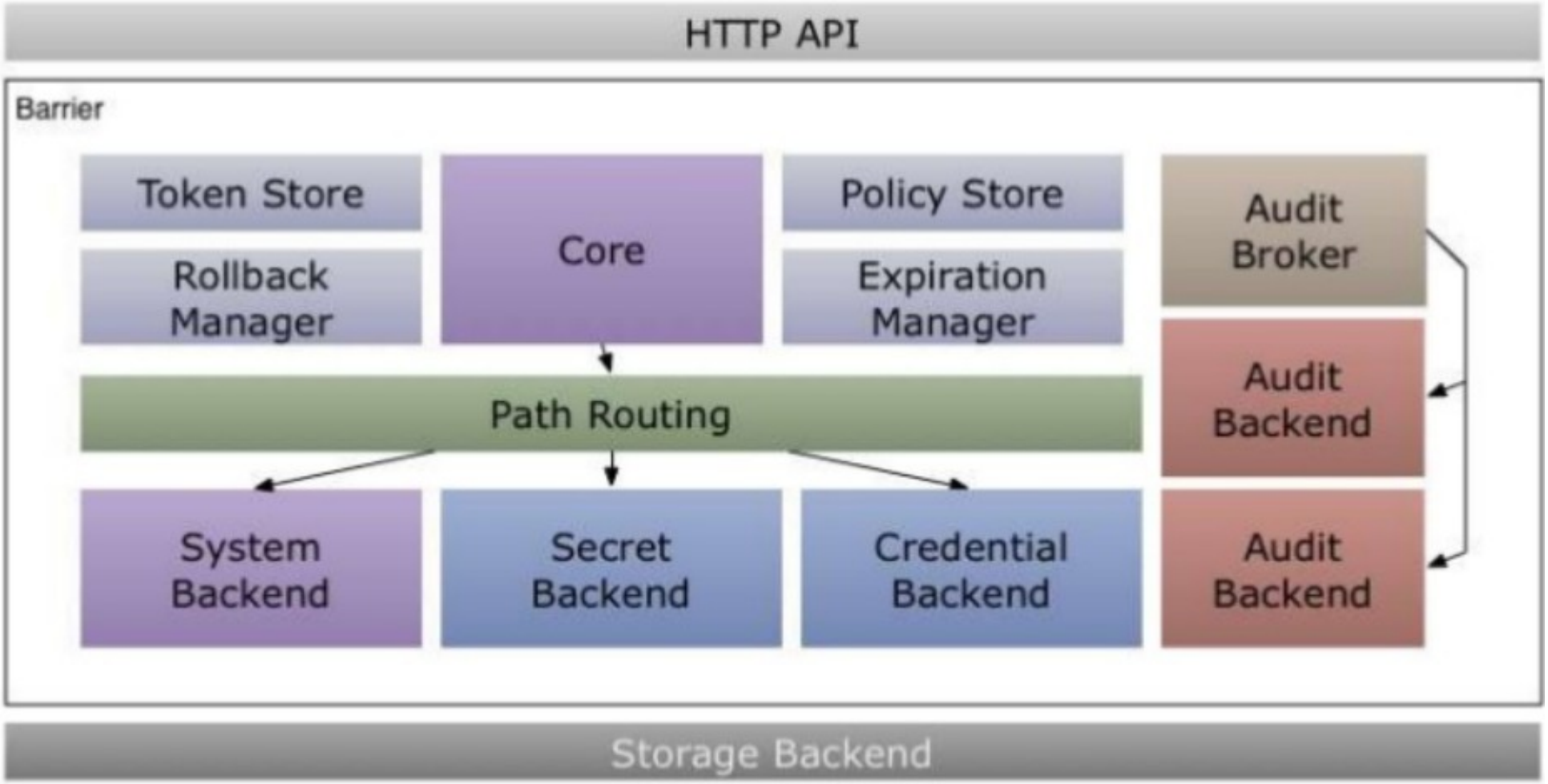
Gestión de secretos

- soluciones
  - Azure Key Vault
  - Management Service (KMS)

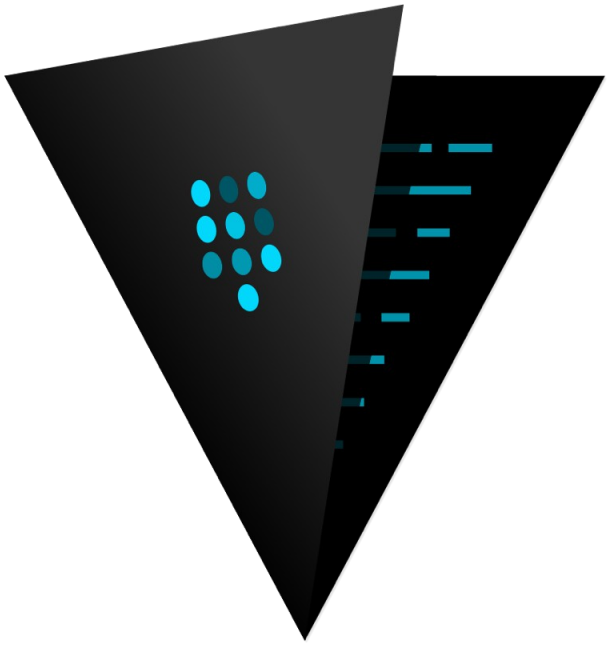


- Terraform
- Consul
- Vagrant
- Vault
- ...

Vault


HTTP API
Barrier
Token Store
Rollback Manager
Core
Policy Store
Expiration Manager
Audit Broker
Audit Backend
Audit Backend
Path Routing
System Backend
Secret Backend
Credential Backend
Storage Backend

Vault



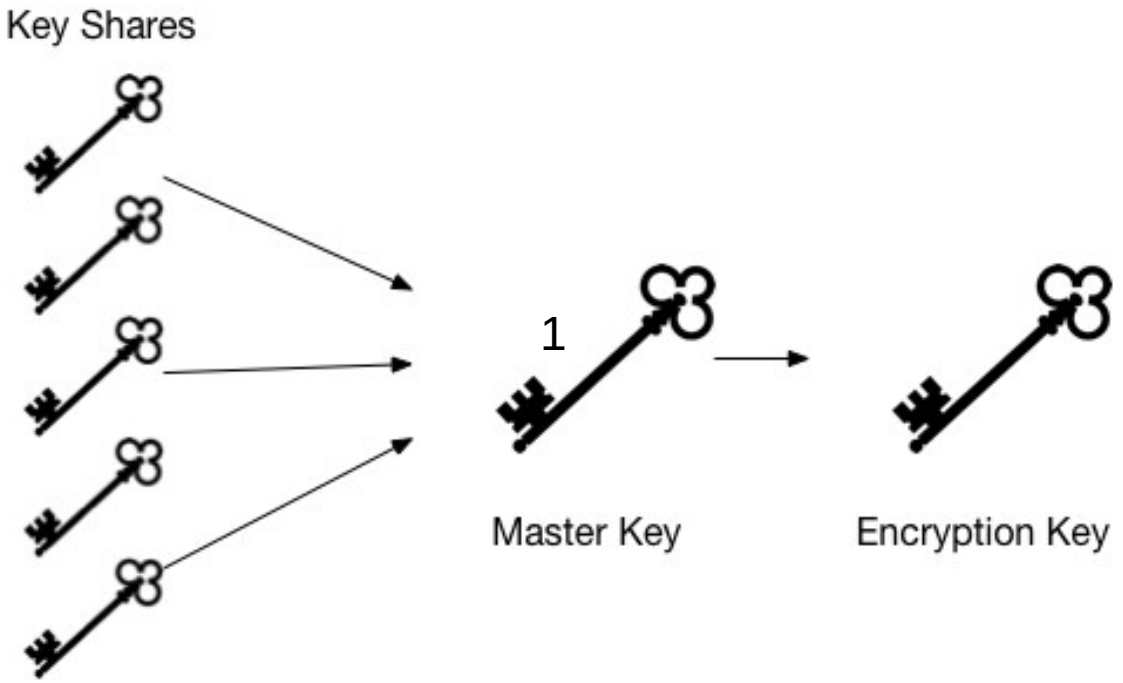
- Comandos por CLI
- Comandos por REST

Vault - inicialización

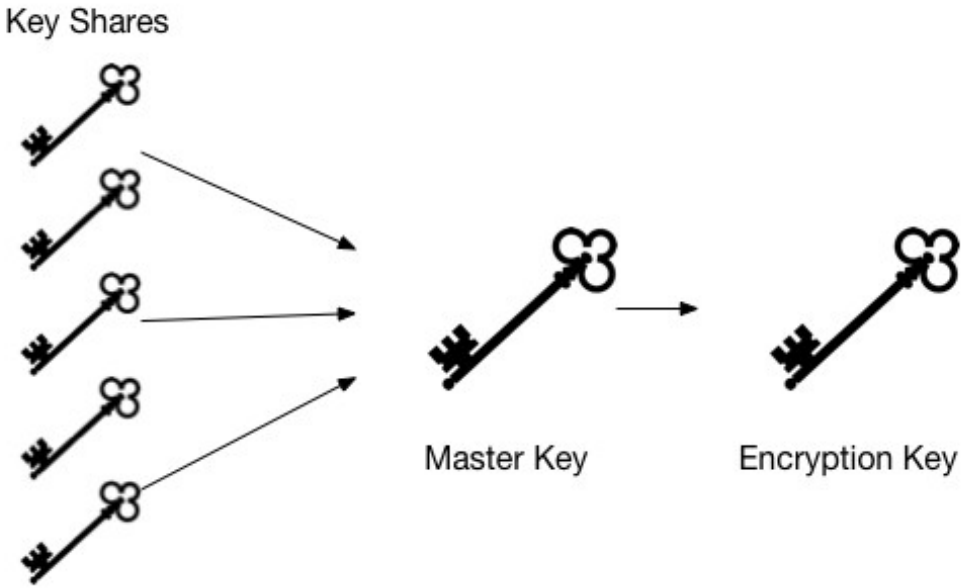
- Arranca sellado
  - Verificar estado y desellar
- Desellado
  - se realiza con x shares
- Sellado cualquier token **root**

Keys

- Shamir's Secret Sharing
- Política de Two-man rule
- Default 5 shares, 3 necesarios
- **Rekey/rotate**



Keys

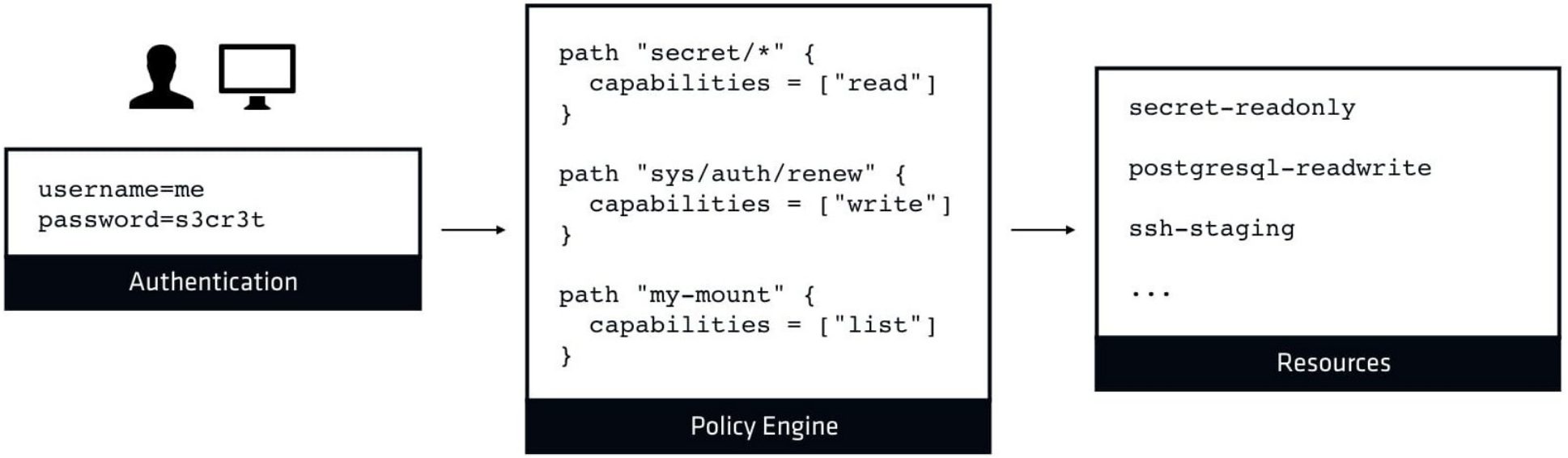


Las shares generan la master key necesaria para leer la descryption/encryption key

Vault - flujo

Cliente--TLS+Token-->server--[TLS]-->Backend

Vault Paths


username=me
password=s3cr3t
Authentication
path "secret/*" {
capabilities = ["read"]
}
path "sys/auth/renew" {
capabilities = ["write"]
}
path "my-mount" {
capabilities = ["list"]
}
Policy Engine
secret-readonly
postgresql-readwrite
ssh-staging
...
Resources

Propiedades del token

- **ID** - The primary ID of a token is a randomly generated UUID
- **Display Name** – Opt. a human readable display name
- **Metadata** - Metadata used for audit logging
- **Number of Uses** – Opt. a restricted use count
- **Parent ID** – Opt. a parent token which created this child token
- **Policies** - An associated list of ACL policies
- **Source Path** - The path at which the token was generated

Inmutable una vez creado.

Funcionamiento token

- Un token puede hacer hijos.
- Limitar el número de usos.
- Los tokens se pueden revocar o expirar.

Backends

- **read/write/delete** como un pequeño fs
- No soporta directorios relativos
- Un backend no puede acceder a otro backend
- **Mount/Unmount/Remount**
- MongoDB, Cassandra, SSH, desarrollo, …
- Más I/O en el storage backend que CPU

Backends

- Secret Backends
- Auth Backends
- PKI Secret Backend
- …

ACLs

- Basadas en políticas
- **Política default** deny cualquier rama.
- Políticas definen granularidad de la rama
- El token root funciona como en linux hay política de sudo.

ACLs

```
path "secret/test/*" {
  policy = "write"
}

path "secret/*" {
  policy = "read"
}

path "secret/classified/*" {
  capabilities = ["deny"]
}
```

Ejemplo

- Lectura

```
$ curl \
    -H "X-Vault-Token: f3b09679-3001-009d-2b80-9c306ab81aa6" \
    -X GET \
    http://127.0.0.1:8200/v1/secret/?list=true
```

- Escritura

```
$ curl \
    -H "X-Vault-Token: f3b09679-3001-009d-2b80-9c306ab81aa6" \
    -H "Content-Type: application/json" \
    -X POST \
    -d '{"value":"bar"}' \
    http://127.0.0.1:8200/v1/secret/baz
```

¿Preguntas?

red@nosoloaulas.com