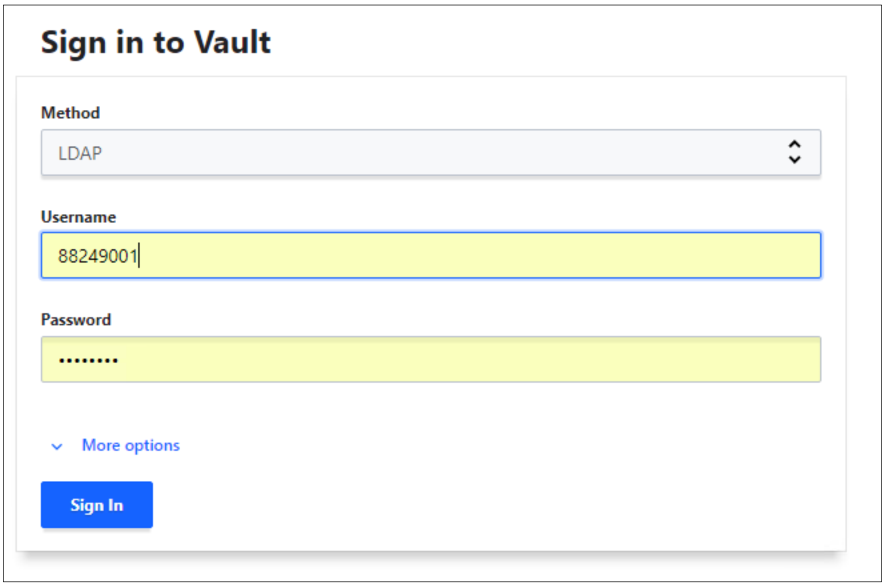
ACCESO A LA PLATAFORMA HASHICORP VAULT

LDAP es el método de autenticación habilitado para el acceso a Hashicorp Vault. Por lo cual los usuarios permitidos pueden acceder ingresando su usuario y contraseña de red en la página web del login de la plataforma web. Se detallan los ambientes:

AMBIENTE	URL
DESARROLLO – CALIDAD	https://vaultdesaqa.domibco.com.pe:8200
PRODUCCIÓN	https://vault.domibco.com.pe:8200

Para poder ingresar a la plataforma, debemos ingresar a la url previamente mencionados y seleccionar el método LDAP, ingresando con su cuenta de red



Sign in to Vault

Method: LDAP

Username: 88249001

Password: ••••••••

Imagen 01 Interfaz Web para Login - Hashicorp Vault

CREACIÓN DE SECRETOS

Una vez dentro de la plataforma, para crear un nuevo secreto debemos seleccionar el engine donde estará almacenado el secreto y hacer click en la opción “Create secret”

Para el ejemplo se esta seleccionando el engine de desarrollo

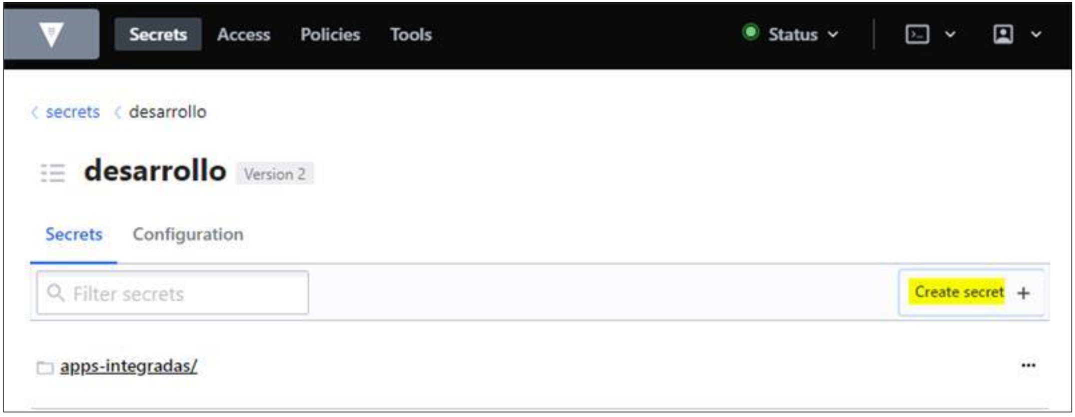
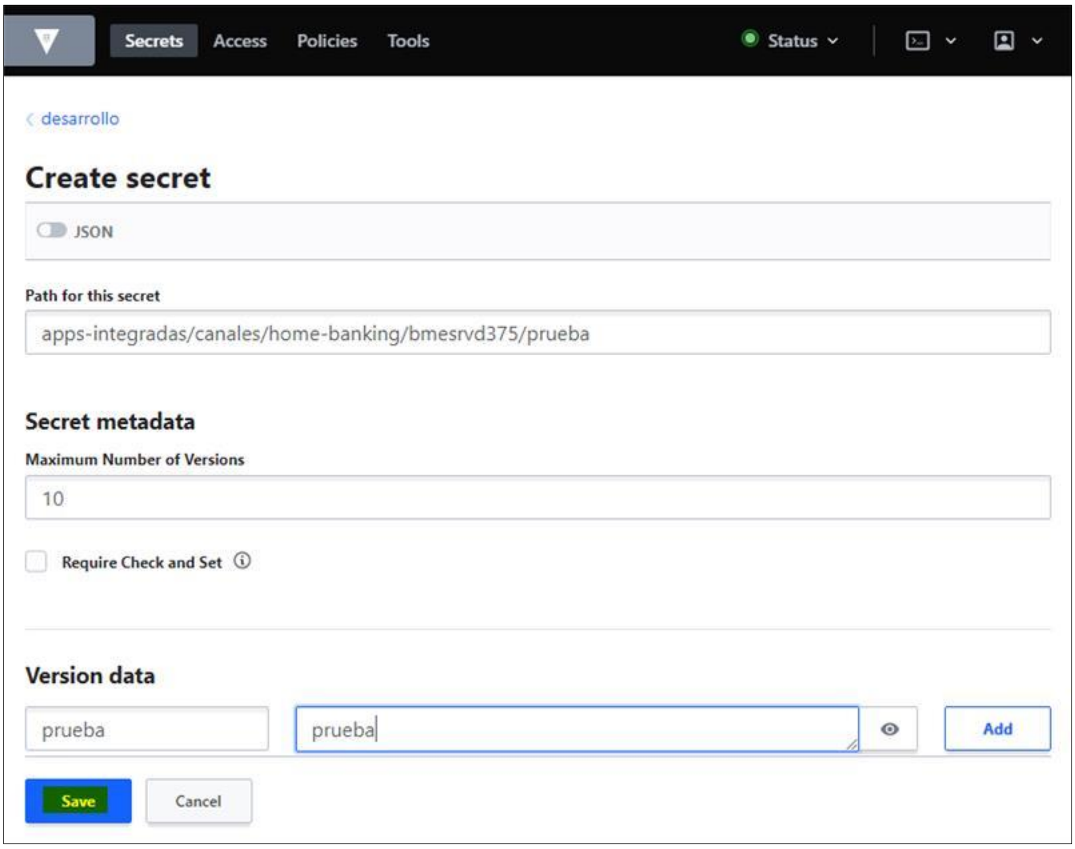


Imagen 02 Creación de secreto en Hashicorp Vault

Al intentar crear un nuevo secreto hashicorp vault solicita varios datos como el path donde estará nuestro secreto y los secretos correspondientes.



‹ desarrollo

Create secret

JSON

Path for this secret: apps-integradas/canales/home-banking/bmesrvd375/prueba

Secret metadata

Maximum Number of Versions: 10

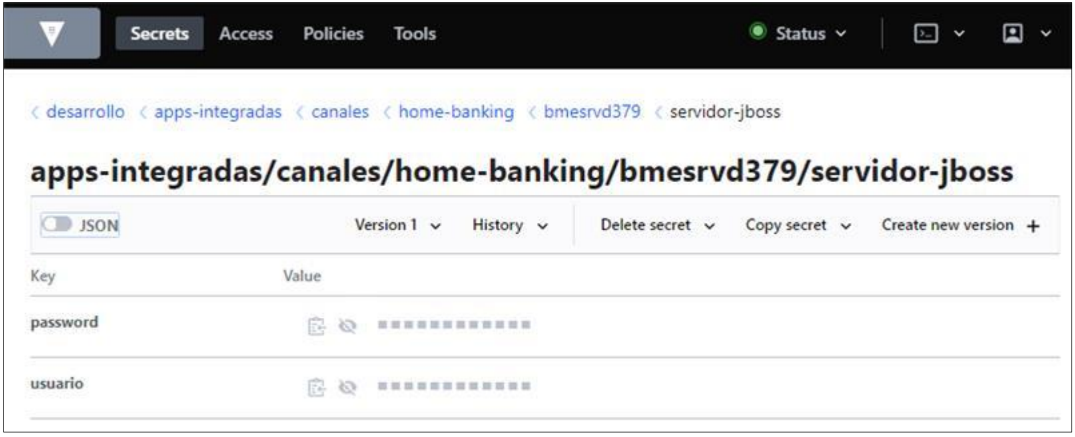
□ Require Check and Set

Version data

prueba | prueba

Imagen 03 Almacenar secreto en Hashicorp Vault

Una vez creado el secreto, vault nos mostrará un formato como el siguiente:



‹ desarrollo ‹ apps-integradas ‹ canales ‹ home-banking ‹ bmesrvd379 ‹ servidor-jboss

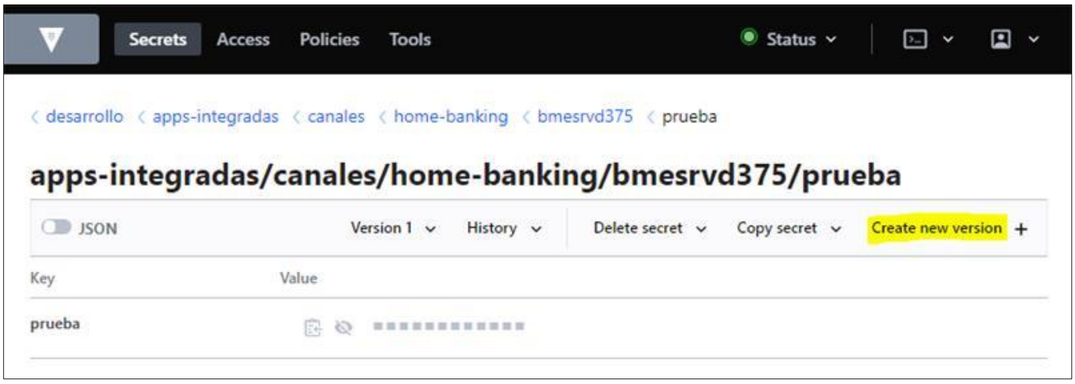
apps-integradas/canales/home-banking/bmesrvd379/servidor-jboss

Key	Value
password	■■■■■■■■■■■■■
usuario	■■■■■■■■■■■■■

Imagen 04 Secreto almacenado en Hashicorp Vault

ACTUALIZAR SECRETOS

En el caso se requiera modificar el secreto, debemos seleccionar la opción “Create new version”.



desarrollo < apps-integradas < canales < home-banking < bmesrvd375 < prueba

apps-integradas/canales/home-banking/bmesrvd375/prueba

Key	Value
prueba	•••••••••••••

Imagen 05 Actualizar secreto en Hashicorp Vault

CREAR UNA POLÍTICA

Para crear una nueva política debemos seleccionar la opción “Policies” y luego la opción “Create ACL policy”

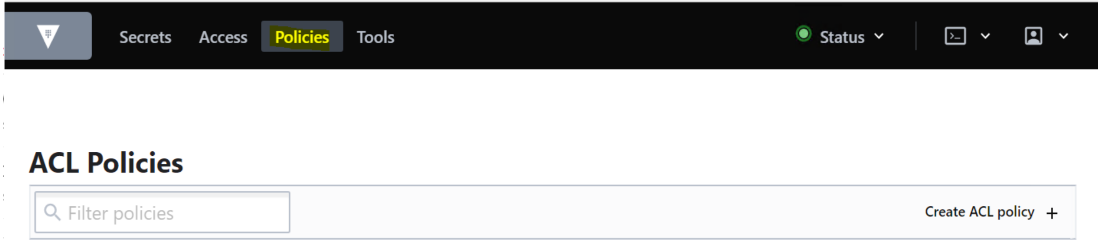
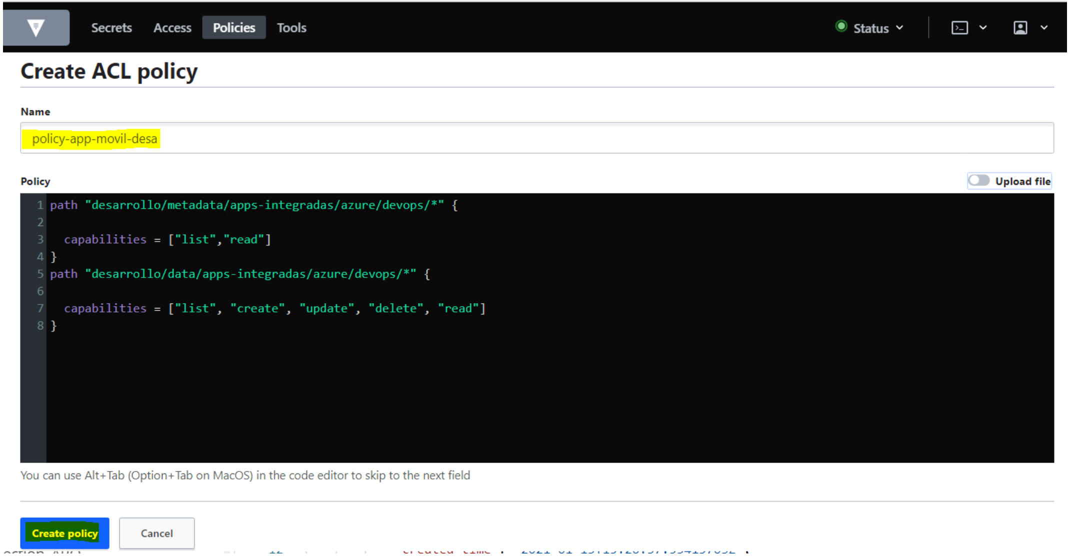


Imagen 06 Creación de política den Hashicorp Vault

Hashicorp Vault, dentro de la creación de secretos acepta formatos json para lo cual debemos ingresar un formato válido al igual que el nombre de la política(validar el formato **policy-nombre-aplicación-ambiente**)



Name: policy-app-movil-desa

Policy

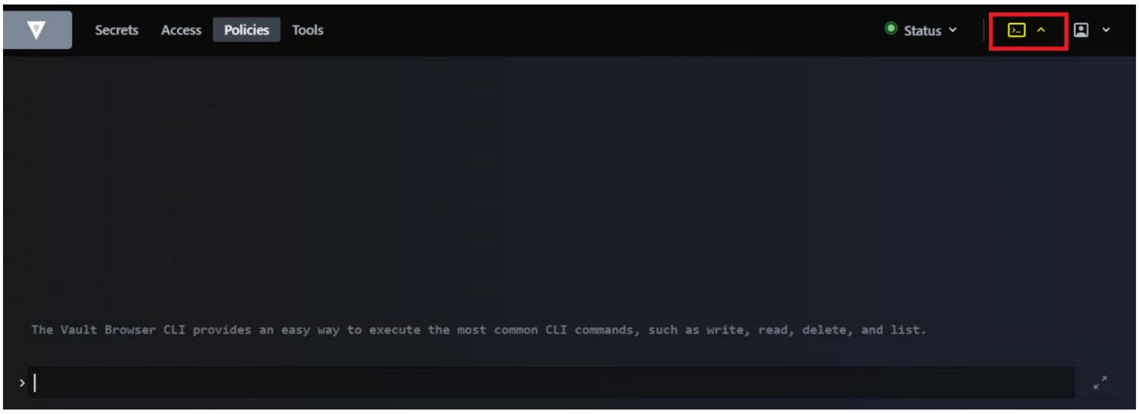
```
path "desarrollo/metadata/apps-integradas/azure/devops/*" {

  capabilities = ["list","read"]
}
path "desarrollo/data/apps-integradas/azure/devops/*" {

  capabilities = ["list", "create", "update", "delete", "read"]
}
```

You can use Alt+Tab (Option+Tab on MacOS) in the code editor to skip to the next field

Imagen 07 Formato de política den Hashicorp Vault

CREAR UN APPROLE

Hashicorp vault, maneja una Shell que nos permite ingresar ciertos comandos



```
The Vault Browser CLI provides an easy way to execute the most common CLI commands, such as write, read, delete, and list.

>
```

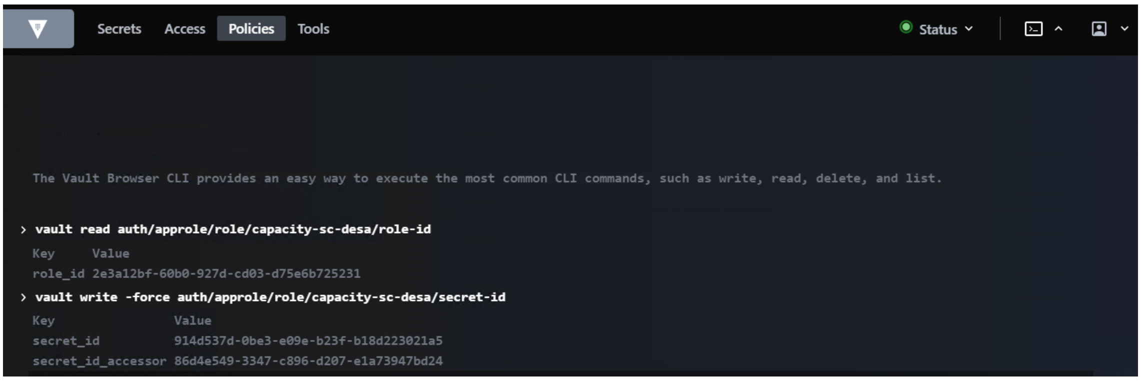
Imagen 08 Shell de hashicorp vault

Comando para crear un approle

- vault write auth/approle/role/nombre-de-app-role token_policies="nombre-de-politica " token_ttl=1h

Comando para obtener role id y secret id

- vault read auth/approle/role/ nombre-de-app-role/role-id
- vault write -f auth/approle/role/ nombre-de-app-role/secret-id



```
The Vault Browser CLI provides an easy way to execute the most common CLI commands, such as write, read, delete, and list.

> vault read auth/approle/role/capacity-sc-desa/role-id
 Key     Value
 role_id 2e3a12bf-60b0-927d-cd03-d75e6b725231
> vault write -force auth/approle/role/capacity-sc-desa/secret-id
 Key                Value
 secret_id          914d537d-0be3-e09e-b23f-b18d223021a5
 secret_id_accessor 86d4e549-3347-c896-d207-e1a73947bd24
```

Imagen 08 Secret id y role id