

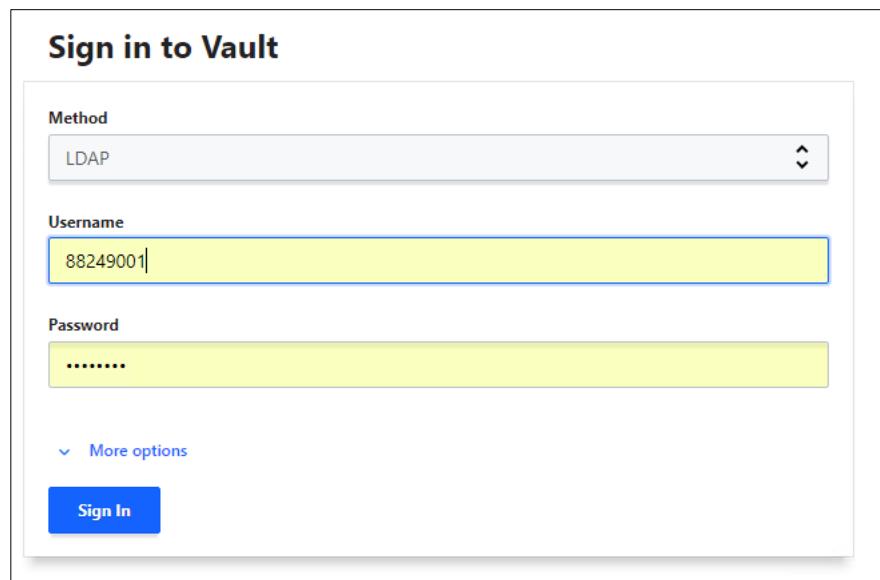
ACCESO A LA PLATAFORMA HASHICORP VAULT	2
CREACIÓN DE SECRETOS	2
ACTUALIZAR SECRETOS	3
CREAR UNA POLÍTICA.....	4
CREAR UN APPROLE.....	4

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://vaultdesaga.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



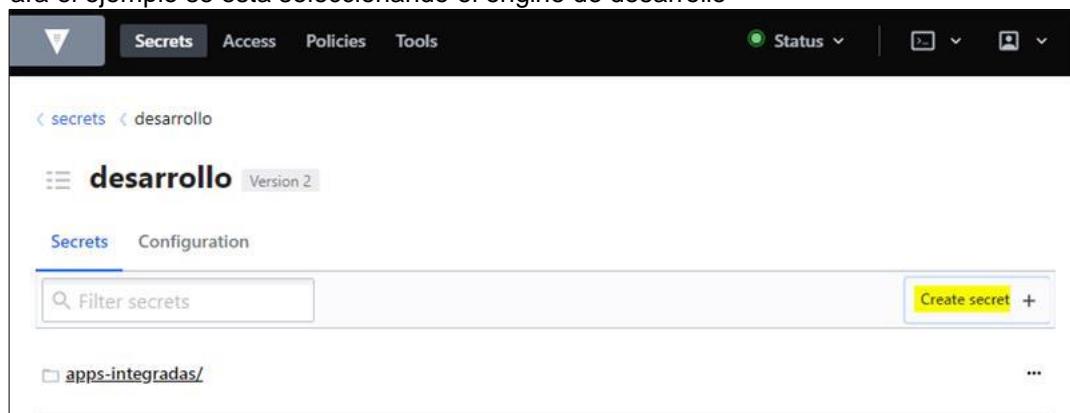
The screenshot shows the 'Sign in to Vault' page. The 'Method' dropdown is set to 'LDAP'. The 'Username' field contains '88249001'. The 'Password' field is obscured by dots. Below the password field is a 'More options' link. At the bottom is a blue 'Sign In' button.

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



The screenshot shows the 'desarrollo' secrets engine. At the top, there's a 'Create secret +' button. Below it is a search bar with 'Filter secrets'. Underneath is a list of secrets, with 'apps-integradas/' being the first item. The 'Secrets' tab is active, while 'Configuration' is also present. The URL in the address bar is 'https://vaultdomibco.com.pe:8200/secrets/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.

The screenshot shows the 'Create secret' page in Hashicorp Vault. At the top, there are tabs for Secrets, Access, Policies, and Tools. On the right, there are status indicators and navigation icons. The main area has a breadcrumb trail: '< desarrollo'. The title is 'Create secret'. There is a 'JSON' toggle button. A 'Path for this secret' field contains the value 'apps-integradas/canales/home-banking/bmesrvd375/prueba'. Below this, under 'Secret metadata', there is a 'Maximum Number of Versions' field set to '10' and a checkbox for 'Require Check and Set'. In the 'Version data' section, there are two input fields: one with 'prueba' and another with 'prueba'. Below these are 'Save' and 'Cancel' buttons. The entire interface is contained within a light gray border.

Imagen 03 Almacenar secreto en Hashicorp Vault

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

The screenshot shows a stored secret in Hashicorp Vault. The breadcrumb trail is '< desarrollo < apps-integradas < canales < home-banking < bmesrvd379 < servidor-jboss'. The path is highlighted in bold as 'apps-integradas/canales/home-banking/bmesrvd379/servidor-jboss'. The interface includes a 'JSON' toggle, version controls (Version 1), history, delete, copy, and create new version options. Below, a table lists key-value pairs: 'password' and 'usuario', both with masked values. The entire interface is contained within a light gray border.

Imagen 04 Secreto almacenado en Hashicorp Vault

ACTUALIZAR SECRETOS

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

The screenshot shows the Hashicorp Vault web interface. At the top, there's a navigation bar with tabs for Secrets, Access, Policies, and Tools. The Policies tab is currently selected. Below the navigation bar, the URL path is displayed: < desarrollo < apps-integradas < canales < home-banking < bmesrvd375 < prueba. The main content area is titled "apps-integradas/canales/home-banking/bmesrvd375/prueba". A toolbar below the title includes options for JSON, Version 1, History, Delete secret, Copy secret, and Create new version. A table below the toolbar lists a single key-value pair: "prueba" with a value of "*****".

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”

The screenshot shows the Hashicorp Vault interface with the Policies tab selected. Below the navigation bar, the URL path is < desarrollo < policies. The main content area is titled "ACL Policies" and contains a search bar labeled "Filter policies" and a button labeled "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**)

The screenshot shows the "Create ACL policy" form. The "Name" field contains "policy-app-movil-desa". The "Policy" field contains the following JSON code:

```
1 path "desarrollo/metadata/apps-integradas/azure/devops/**" {
2
3     capabilities = ["list","read"]
4 }
5 path "desarrollo/data/apps-integradas/azure/devops/**" {
6
7     capabilities = ["list", "create", "update", "delete", "read"]
8 }
```

At the bottom of the form, there's a note: "You can use Alt+Tab (Option+Tab on MacOS) in the code editor to skip to the next field". Below the form are two buttons: "Create policy" and "Cancel".

Imagen 07 Formato de política den Hashicorp Vault

CREAR UN APPROLE

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



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 screenshot shows the Hashicorp Vault Browser CLI interface. At the top, there is a navigation bar with tabs: Secrets, Access, Policies (selected), and Tools. On the right side of the header, there are status indicators and icons for refresh, search, and dropdown menus. Below the header is a dark main area containing a command-line interface. A message at the top of the CLI area reads: "The Vault Browser CLI provides an easy way to execute the most common CLI commands, such as write, read, delete, and list." Below this message, there is a command history and output. The history shows two commands:
> **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