
Universidad
Tecmilenio®

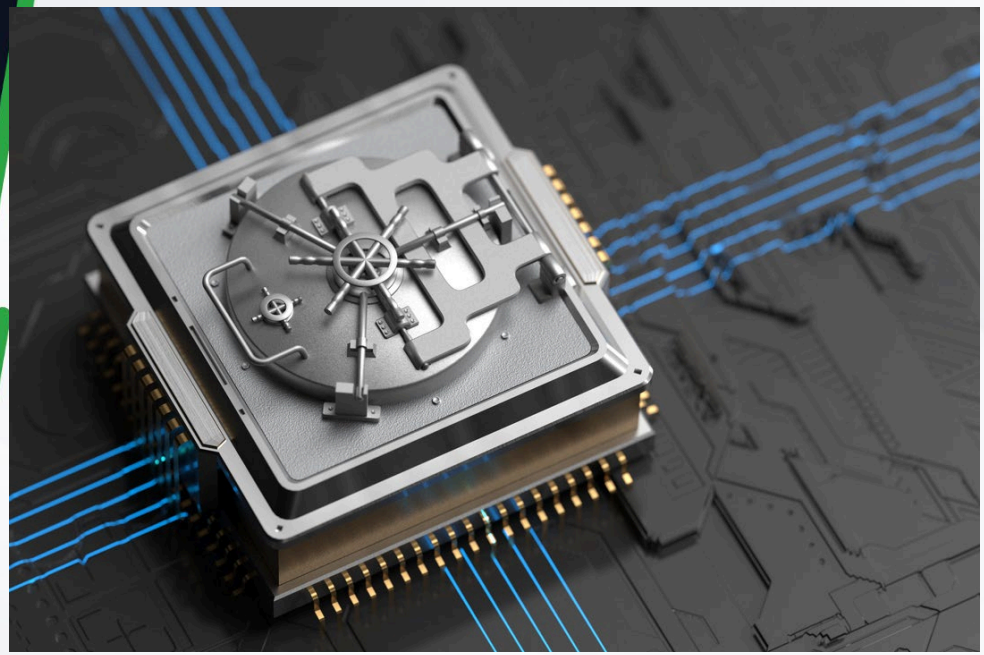
Universidad Tecmilenio

Seguridad en DevOps

Instalación y tokens Vault

Semana 8

Introducción



Todo sistema que proporciona seguridad a los desarrollos de software tiene sus propias particularidades y comandos.

Es necesario que estos conceptos estén muy claros para lograr el objetivo principal: brindar la seguridad necesaria al software desarrollado, de tal forma que los clientes queden satisfechos con el resultado final.

Dentro del sistema Vault existen diferentes comandos para lograr la correcta instalación y permitir el acceso a la información de manera segura, donde podrás comprender cómo funcionan dichos comandos y cómo los debes utilizar.

Explicación

¿Cómo instalar Vault localmente?

Pasos a seguir en Windows

- Abrir la consola de comandos: abrirás el menú de Windows y escribirás cmd.
- Escribir en la consola “vault”.
- Verificar que fue instalado correctamente.

Pasos a seguir en MacOS

- Descargar Homebrew en tu equipo, el cual es un paquete *open-source* exclusivo para el sistema Mac OS X. Lo podrás descargar del siguiente enlace: https://github.com/hashicorp/homebrew-tap
- Hacer clic en “Code”.
- Descomprimir el archivo y abrir la consola de comandos para realizar la instalación mediante el siguiente comando: brew tap hashicorp/tap
- Ejecutar el comando: brew install hashicorp/tap/vault
- Actualizar Vault a su última versión.
- Verificar que todo funcione correctamente.

Pasos a seguir en Linux

- Elegir la distribución de Linux.
- Abrir la consola de comandos y ejecutar el comando de acuerdo con la distribución elegida.
- Añadir el repositorio de HashiCorp.
- Instalar y actualizar la última versión.
- Verificar la instalación correcta.

Explicación

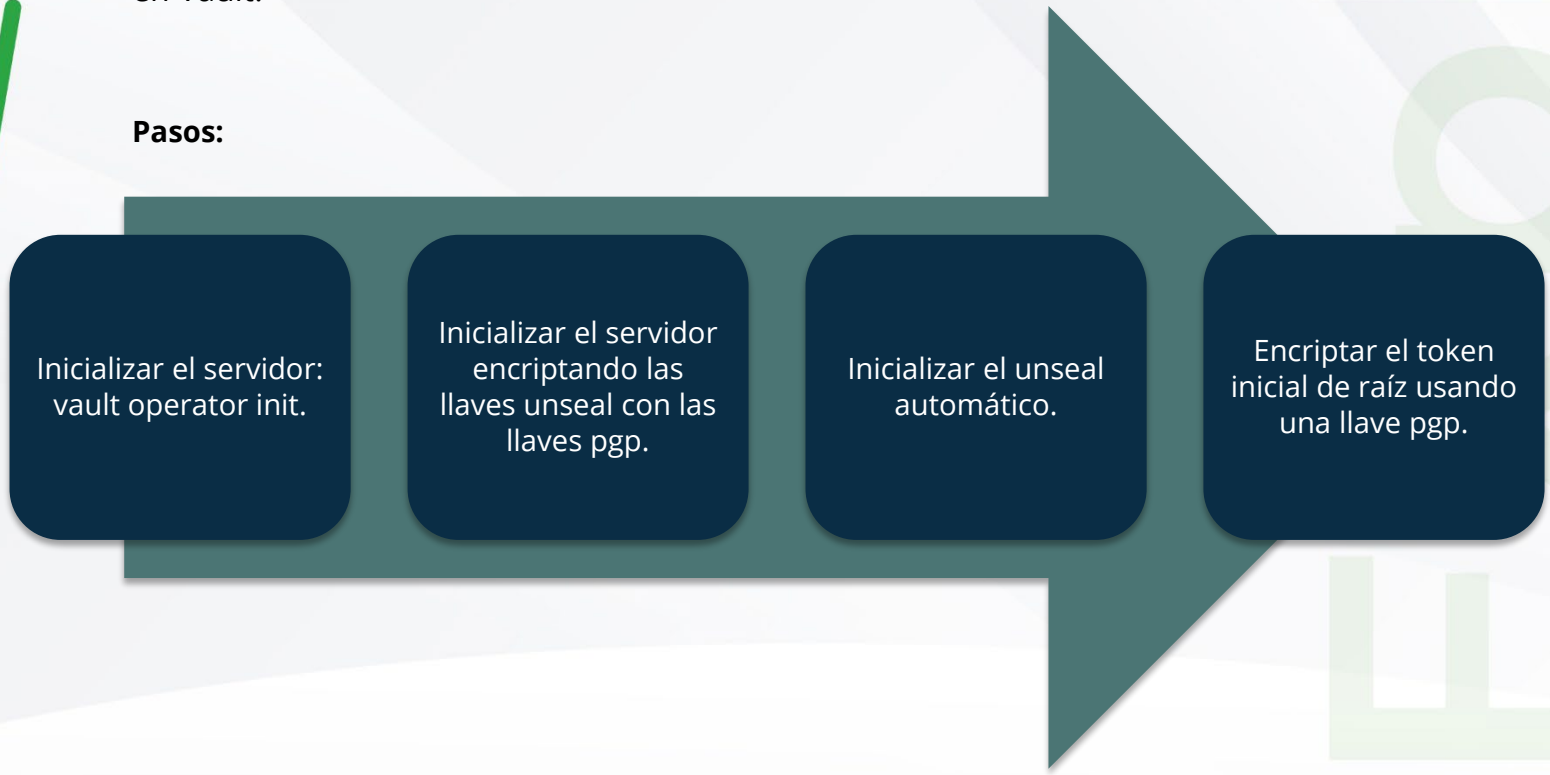
Init y unseal Vault

De acuerdo con HashiCorp (2021), para poder utilizar Vault de forma correcta es necesario que conozcas los comandos que contiene:

Init: se usa para inicializar el servidor.

Unseal (abierto): se utiliza para obtener la llave raíz en texto plano, de tal forma que puedas leer la llave desencriptada y así desencriptar la información, dando acceso a Vault. Por esta razón, primero debes usar unseal para hacer cualquier otra operación en Vault.

Pasos:



Explicación

Manejo y ciclo de vida de los tokens

De acuerdo con HashiCorp (2021-a), los tokens se consideran el principal método de autenticación en Vault, ya que se pueden utilizar directamente o como métodos de autenticación para generar los tokens de manera dinámica.

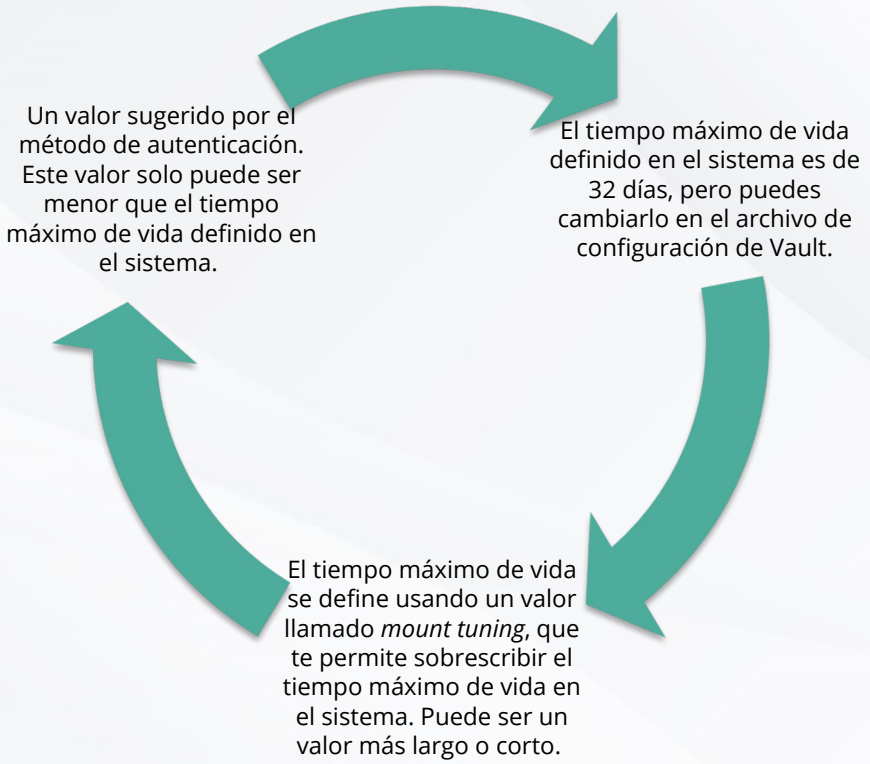
Existen dos tipos de token:

Características	Tokens de servicio	Tokens batch
Pueden ser tokens de raíz.	Sí	No
Logran crear tokens hijos.	Sí	No
Consiguen renovarse.	Sí	No
Pueden ser periódicos.	Sí	No
Tienen un tiempo de vida específico.	Sí	No
Tienen *accessors*.	Sí	No
Costo.	Pesado, necesita almacenarse.	Ligero, no tiene costo de almacenamiento.

Explicación

Manejo y ciclo de vida de los tokens

Ciclo de vida



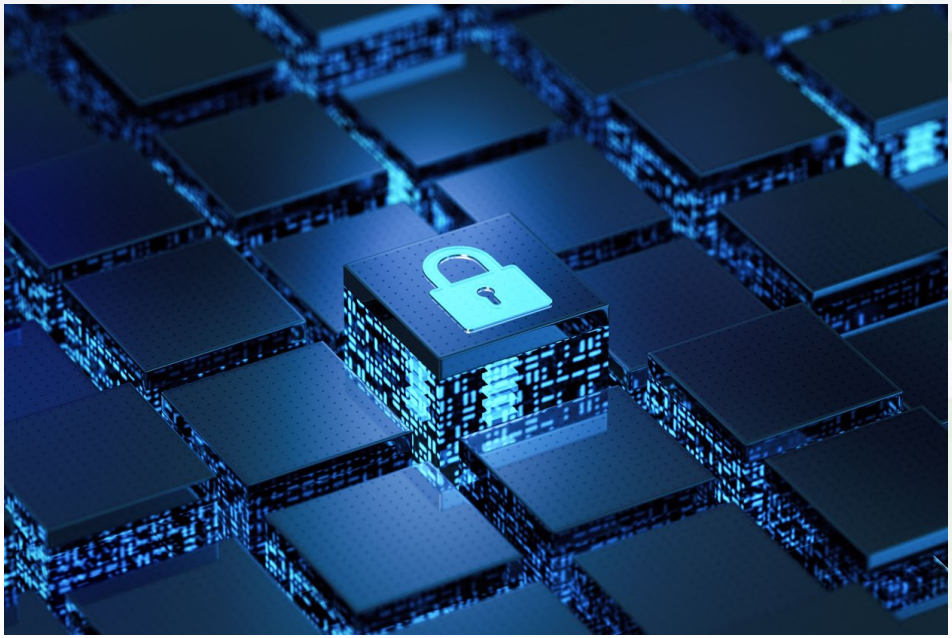
Ejercicio

Tu equipo de trabajo ha sido seleccionado para implementar la seguridad necesaria al nuevo desarrollo que se estará llevando a cabo en la empresa.

Tú y tu equipo han decidido que utilizarán el sistema de Vault para proporcionar dicha seguridad.

A. Instala Vault en tu equipo.
B. Verifica que se haya instalado correctamente.
C. Utiliza el método de unsealing para que puedas realizar diferentes acciones dentro de Vault.

1. Inicializa el servidor de Vault encriptando las llaves unseal con las llaves pgp.
2. Inicializa el unseal automático.
3. Encripta el token raíz usando la llave pgp.



Cierre

Vault es un sistema que te permite dar la seguridad necesaria a la información que almacenes con tu software desarrollado. Es de suma importancia que comprendas cómo se instala Vault y cómo realizas las acciones básicas, por ejemplo, inicializar el servidor y utilizar el método unseal para que puedas acceder a la información almacenada.

También es importante conocer la funcionalidad de los tokens dentro de Vault, los cuales son el primer método de autenticación en el sistema y te permitirán brindar mayor seguridad a tu desarrollo. Es una herramienta que te ayudará a administrar de forma remota todos los equipos que se encuentren dentro de la infraestructura de tu desarrollo, lo cual te permitirá crear y administrar tu infraestructura mediante código, instalar software, mejorar la seguridad y, lo mejor, todo mediante la automatización.

Bibliografía

• HashiCorp. (2021). *Seal/ Unseal*. Recuperado de https://www.vaultproject.io/docs/concepts/seal

• HashiCorp. (2021-a). *Tokens*. Recuperado de https://www.vaultproject.io/docs/concepts/tokens

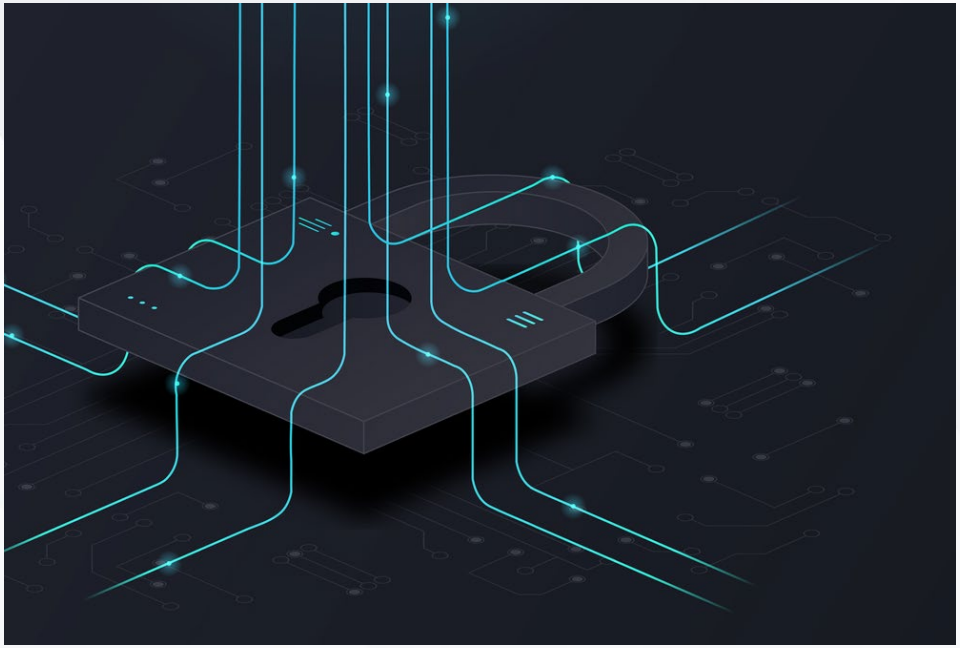
Universidad Tecmilenio

Seguridad en DevOps

Secret engines y políticas de Vault

Semana 8

Introducción



La mejor forma de enviar la información a almacenar es mediante el uso de los motores secretos, los cuales permiten la encriptación de la información al mandarla de un sistema a otro.

Adicional a esto, utilizarás las políticas para controlar quién tiene acceso a cada cosa, de tal forma que, si alguien intenta realizar un ciberataque, será fallido, ya que las llaves dinámicas y las políticas le bloquearán el acceso.

Explicación

Secret engines de Vault

Se utilizan para almacenar, generar y encriptar información. Tienen tres características clave: habilitar, deshabilitar y mover (HashiCorp, 2021-b).

Habilitar

- Se habilitan los motores de secretos en una ruta específica, con algunas excepciones. Por default se habilitan de acuerdo con su tipo, por ejemplo, si quieres habilitar un "aws" debes utilizar "aws/".

Deshabilitar

- Se deshabilita un motor existente. Cuando sucede esto, todos sus secretos son revocados y la información guardada para ese motor es eliminada en la capa física de almacenamiento.

Mover

- El comando sirve para mover la ruta de un motor. Al ejecutar este comando, se revocan todos los secretos, ya que estos se encuentran atados a la ruta donde se crearon.

Explicación

Secret engines en Vault

Universidad Tecmilenio

Explicación

PKI

Genera certificados X.509 dinámicos.	Implementación de revocaciones.	Certificados efímeros.	Pasos para ejecutar sus funciones.
•Te permitirá obtener los certificados que necesites sin tener que realizar manualmente la creación de la clave privada y el CSR, el envío a una CA para que sea verificado y firmado.	•Para evitar la implementación de revocaciones puedes hacer que tus TTL sean cortos, lo cual provoca que las CRL también sean cortas y con esto el motor de secretos podrá escalar grandes cargas de trabajo.	•Tienen la peculiaridad de que no necesitan ser almacenados en el disco, ya que los obtienes y se almacenan en memoria cuando se inicia la aplicación. Al cerrar la aplicación, el certificado se descarta, es decir, ya no se puede volver a utilizar.	• Adecuar el motor PKI. • Aumentar el TTL. • Configurar la CA. • Actualizar la localidad del CRL. • Configurar el rol que mapee un nombre en Vault. • Generar una nueva credencial.

Explicación

Motores de secretos K/V

Almacena secretos arbitrarios dentro del almacenamiento físico.

Existen dos formas de ejecutarlo: puedes configurarlo para que solo te almacene un valor por una clave o puedes usar el control de versiones.

Versión 1: cuando se ejecuta el back end sin versión, se guardará el valor más reciente en una clave. Lo anterior te da ciertos beneficios, ya que no necesitarás un gran almacenamiento para guardar cada clave, porque solo se guarda lo más reciente. Las solicitudes que reciba el motor serán atendidas más rápido, ya que accederá menos veces al almacenamiento y no se bloqueará el acceso.

Versión 2: cuando se ejecuta v2 del back end kv, la clave podrá guardar cierto número de versiones (por *default* son 10). Podrás recuperar los datos de las versiones anteriores en caso de que lo requieras. Para eliminar de forma permanente los datos de una versión, puedes usar el comando *destroy* o el punto final de la API, esto te permite restringir quién tiene permisos para eliminar de manera temporal, recuperar o eliminar datos de forma definitiva.

Explicación

Encriptación por servicio

Consiste en aplicar el algoritmo de cifrado a un texto plano, de tal forma que cuando ese texto se mande a su destino, todo se encuentre encriptado.

Vault tiene tres métodos de encriptación: mediante línea de comandos, API REST o consola web de administración (Picodotdev, 2021).

Línea de comandos:

1. Inicializa Vault.
2. Obtén una clave.
3. Hacer que Vault encripte y desencripte la información.
4. Vault te permite generar una nueva versión de la misma llave, de esta forma los datos que se encontraban en la llave anterior serán encriptados con la nueva versión de la llave.

De acuerdo con HashiCorp (2021-c), el método API Rest:

1. Inicializa Vault con la API.
2. Obtendrás el token raíz y la llave “Unseal”.
3. Aplica el proceso “Unseal” mediante el HTTP API.
4. Invoca la API para verificar que se haya inicializado correctamente.

Explicación

Políticas en Vault

Las políticas son utilizadas por Vault para controlar el comportamiento de los clientes, servidores, bases de datos, aplicaciones o el desarrollo implementado (HashiCordp, 2021-a).

Cuando Vault es inicializado se crea una política raíz, la cual es extremadamente poderosa, ya que te permitirá habilitar motores de secretos, definir políticas y configurar los métodos de autenticación. Dicha política es asignada al token raíz.

Las rutas son definidas por las políticas, ya que por default Vault quita las capacidades que tienen las rutas, con esto garantiza que sean seguras.

Explicación

Políticas en Vault

Pasos a seguir para configurar Vault y autenticarse a través de una instalación corporativa de LDAP o ActiveDirectory.

Vault debe ser configurado de tal forma que se pueda conectar a un método de autenticación. Para LDAP es necesario que Vault sepa la dirección del servidor y se conecte mediante TLS. Para validar la autenticación del servidor, Vault le pasará la información al método de autenticación.

Ya que se ha configurado la conexión, el equipo de seguridad creará una política (o usará una que ya existe) para dar el acceso a las rutas.

Ya que fue creada la política, su contenido se guarda en Vault. Para hacer referencia a la política, puedes utilizar el nombre de la misma.

El nombre te da acceso al contenido, de tal forma que se asigna una política interna con un sistema de autenticación de back end.

Explicación

Políticas en Vault
Flujo del usuario

Cuando el usuario trata de autenticarse con Vault mediante sus credenciales de LDAP, le proporciona a Vault datos como usuario y contraseña de LDAP.

Al momento de que Vault establece una conexión con LDAP y le solicita al servidor LDAP la autenticidad de las credenciales ingresadas, si el usuario y la contraseña son correctos, el servidor regresa la información al usuario, incluyendo los grupos de unidades organizativas.

Cuando Vault asigna el resultado del servidor LDAP a las políticas de Vault, utilizando la configuración del equipo de seguridad, lo que hace Vault es generar un token con las políticas establecidas.

Por último, Vault regresa el token al usuario, el cual contiene las políticas correctas, esto sucede por la configuración que puso el equipo de seguridad.

Universidad Tecmilenio

Ejercicio

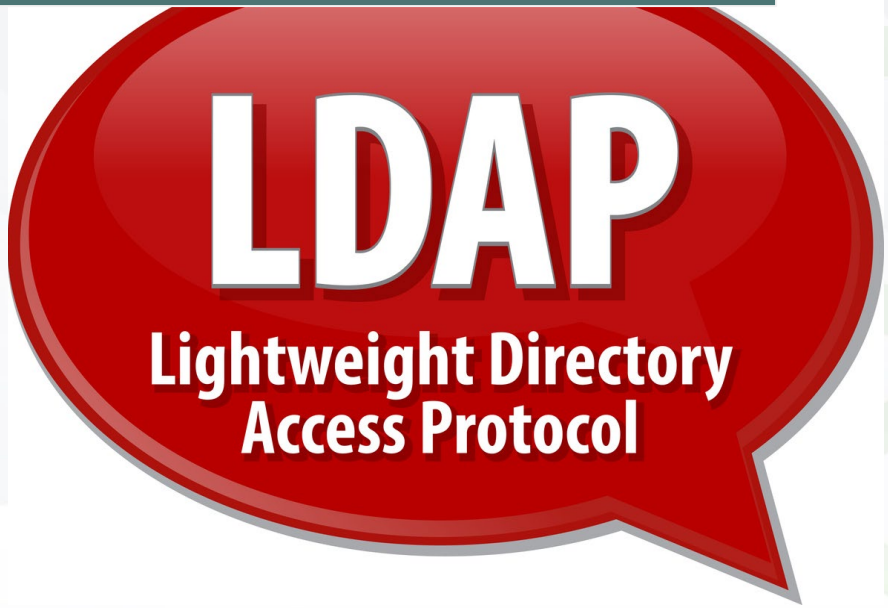
Te encuentras configurando la seguridad para un sistema enfocado en el alta, baja, consulta y modificación de clientes de un banco. Junto con tu equipo de seguridad, han decidido utilizar HashiCorp Vault para implementar la seguridad. Para llevar a cabo lo solicitado, necesitarás definir los siguientes puntos.

1. Establece el usuario administrador que podrá implementar las políticas necesarias de seguridad.

2. Define qué motor de secretos utilizarás para garantizar la seguridad del sistema.

3. Una vez realizados los dos pasos anteriores, ingresa a Vault y realiza lo siguiente:

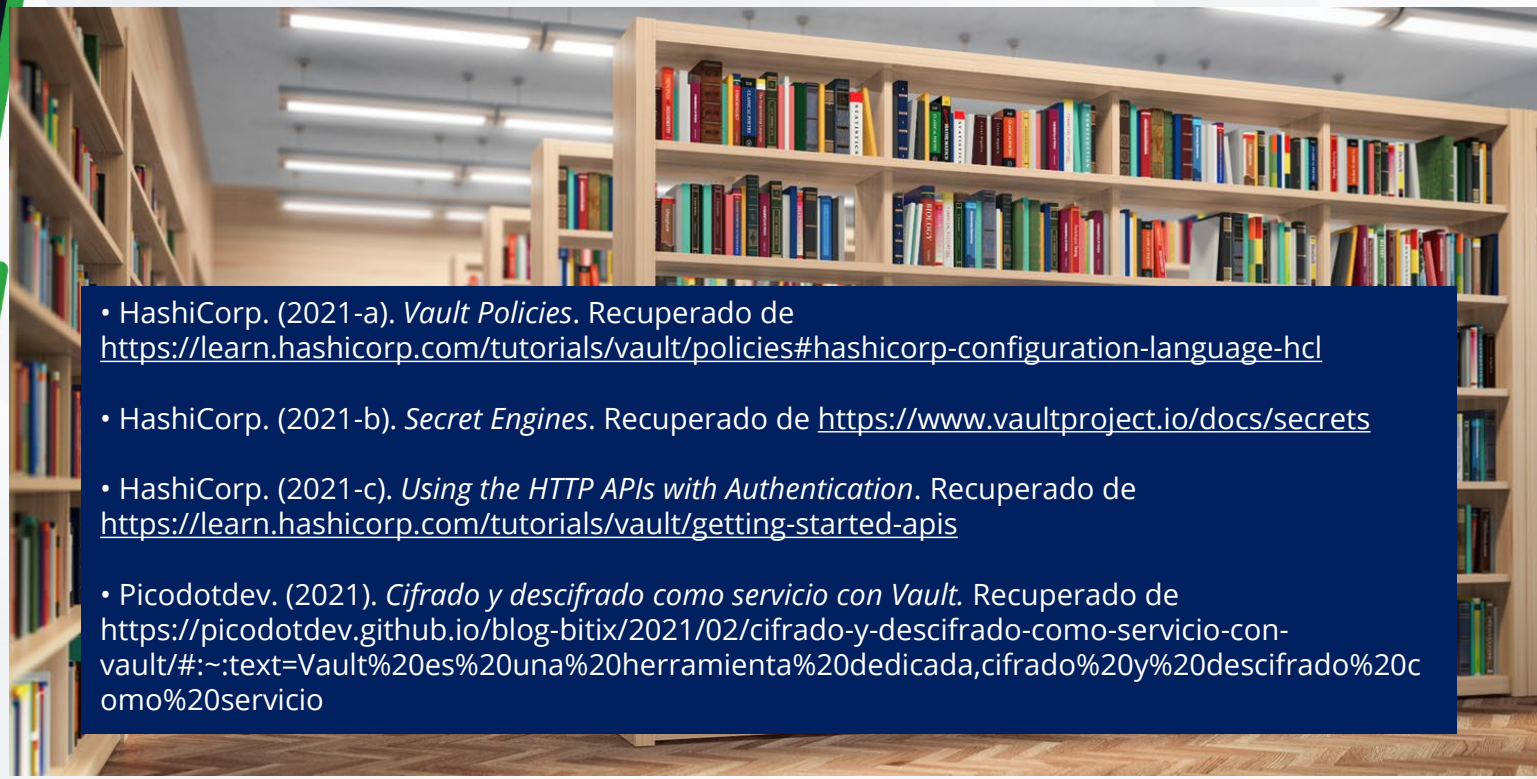
a. Configura Vault para conectarse al método de autenticación LDAP.
b. Crea una política que brinde el acceso a las rutas de Vault.
c. Haz una prueba de usuario intentando acceder a Vault mediante las credenciales de LDAP.



Cierre

Vault es un sistema que te permite dar la seguridad necesaria a la información que almacenes con tu software desarrollado. Para esto es de suma importancia que comprendas cómo funcionan las políticas y los motores de secretos, de tal manera que puedas utilizar estas dos grandes características del software para blindar tu desarrollo de cualquiera que quisiera acceder a la información.

Bibliografía



• HashiCorp. (2021-a). *Vault Policies*. Recuperado de https://learn.hashicorp.com/tutorials/vault/policies#hashicorp-configuration-language-hcl

• HashiCorp. (2021-b). *Secret Engines*. Recuperado de https://www.vaultproject.io/docs/secrets

• HashiCorp. (2021-c). *Using the HTTP APIs with Authentication*. Recuperado de https://learn.hashicorp.com/tutorials/vault/getting-started-apis

• Picodotdev. (2021). *Cifrado y descifrado como servicio con Vault.* Recuperado de https://picodotdev.github.io/blog-bitix/2021/02/cifrado-y-descifrado-como-servicio-con-vault/#:~:text=Vault%20es%20una%20herramienta%20dedicada,cifrado%20y%20descifrado%20como%20servicio

Universidad Tecmilenio

Seguridad en DevOps

Roles y autenticación en Vault

Semana 8

Introducción

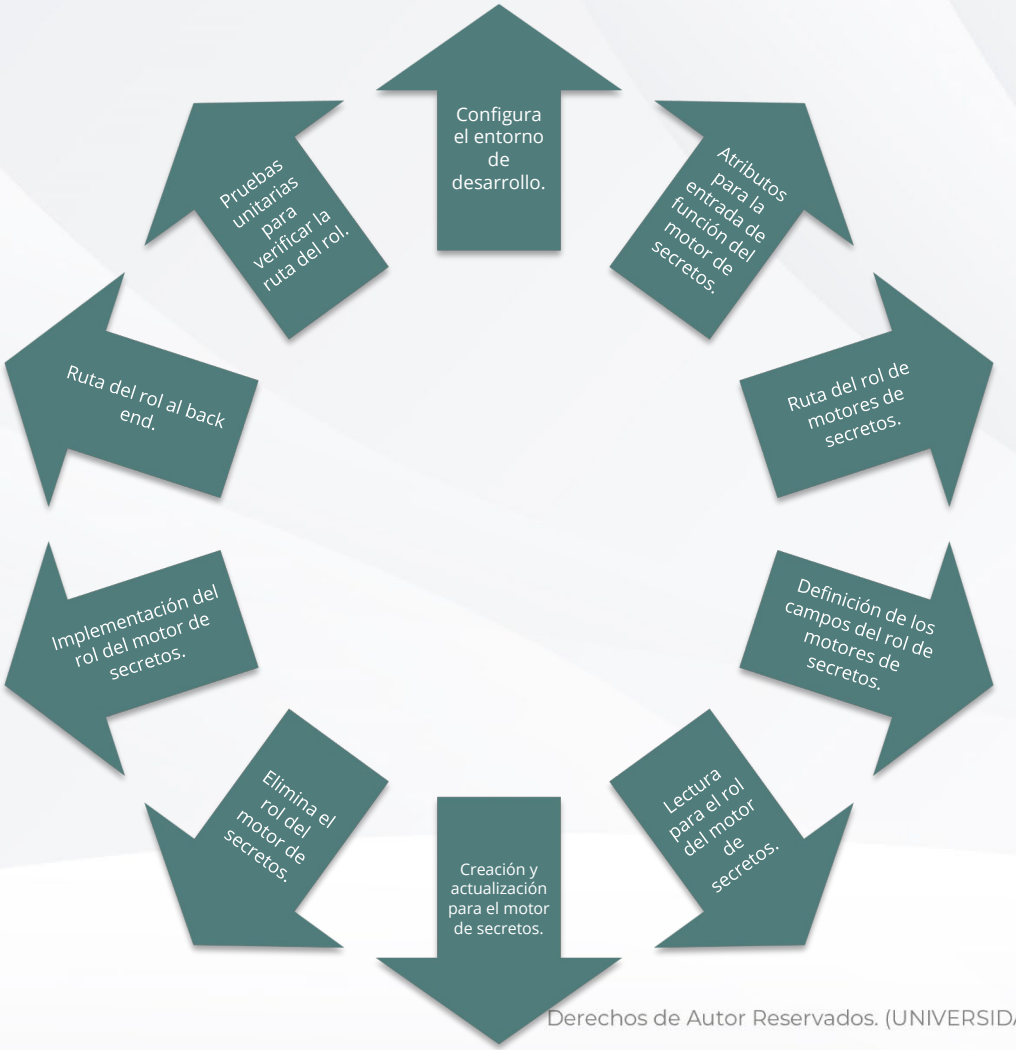
No todos los usuarios deben tener los mismos privilegios, ya que esto podría provocar una fuga de información, por lo que HashiCorp Vault cuenta con las definiciones de los roles y los métodos de autenticación, los cuales sirven para delimitar los permisos de un usuario, otorgando un mayor grado de seguridad al sistema.

Explicación

Roles de Vault

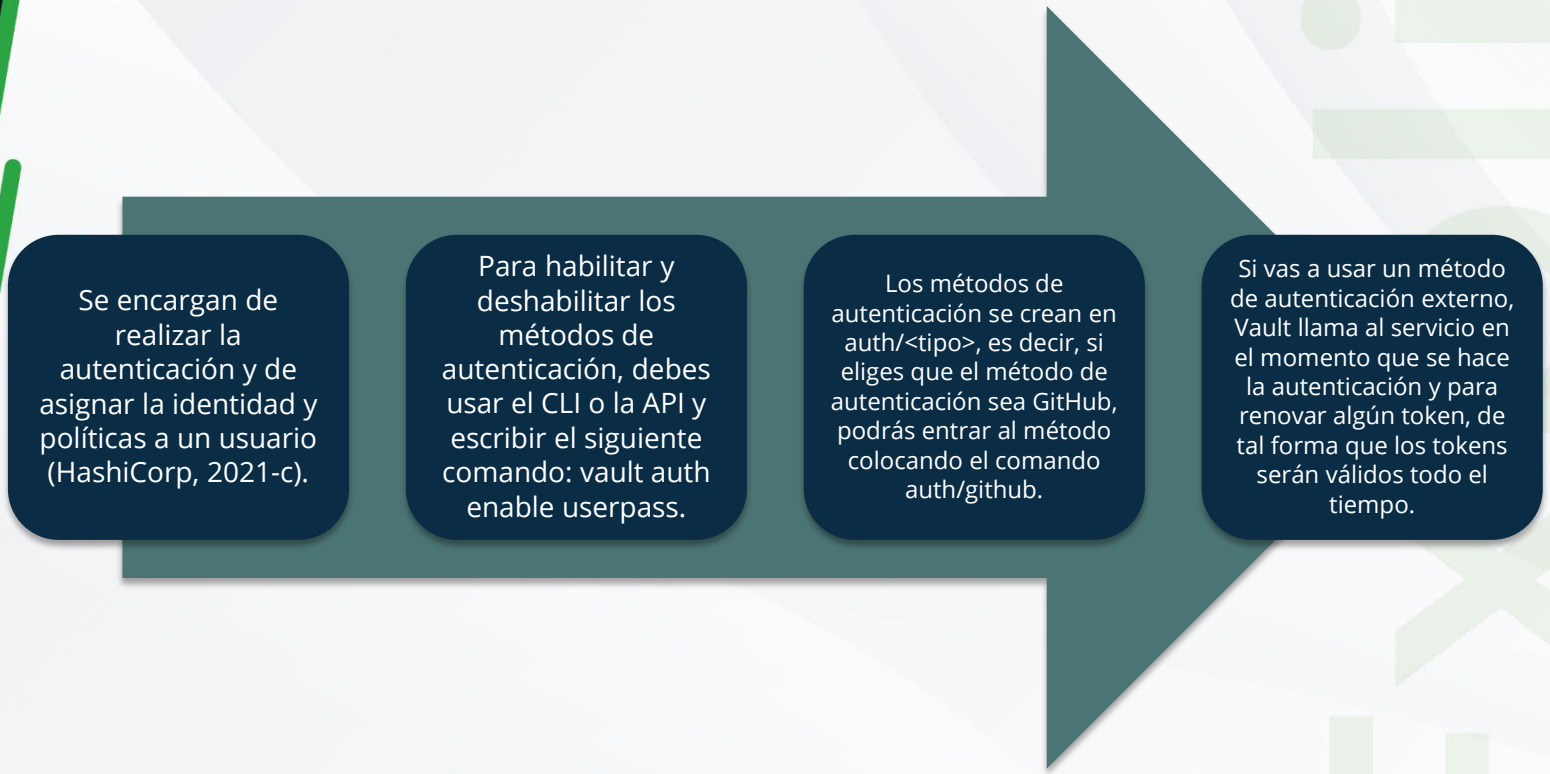
El rol es una identidad que se conforma por permisos, grupos o políticas (HashiCorp, 2021-a).

Pasos para establecer un rol:



Explicación

Métodos de autenticación de Vault



Explicación

Métodos de autenticación de Vault

AppRole

- Este método hace que las máquinas o aplicaciones se autentifiquen mediante funciones definidas por Vault. La ventaja es que te permite manejar muchas aplicaciones, ya que se enfoca en los flujos de trabajo automatizados (HashiCorp, 2021-b).

GitHub

- Este método consiste en autenticarse a través de un token de acceso personal de GitHub. Normalmente es el más utilizado para los humanos (HashiCorp, 2021-d). Para realizar la autenticación, puedes usar el CLI o la API.

Nombre de usuario y contraseña

- El usuario deberá utilizar un usuario y una contraseña para poder autenticarse. Para configurar las combinaciones del nombre de usuario y la contraseña, usarás la ruta usuario/. Con esto podrás leer nombres de usuario y contraseñas que vengan de una fuente externa.

Universidad Tecmilenio

Ejercicio

Una agencia automotriz muy importante del país solicita tus servicios y los de tu equipo para que los ayuden a implementar un sistema de seguridad.

Debes definir los roles y el método de autenticación para el nuevo sistema que se implementará en poco tiempo. Para esto, necesitas realizar los siguientes puntos:

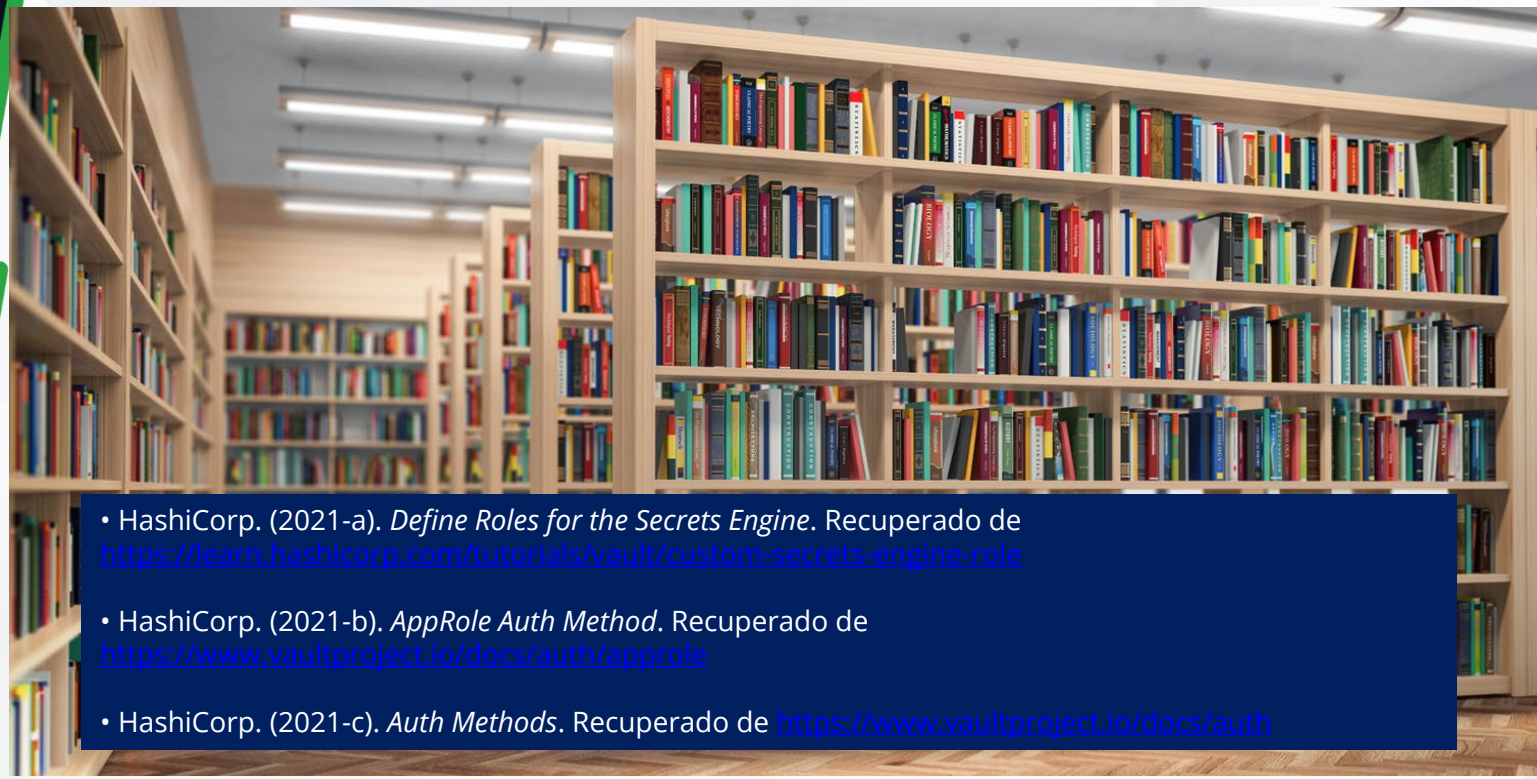
1. Determina los usuarios y sus roles.

2. Establece cuál será el método de autenticación para cada usuario y justifica el porqué.

3. De acuerdo con el método elegido, impleméntalo en Vault para al menos cinco usuarios, tomando en cuenta las siguientes indicaciones:

a. Ingresa al CLI para habilitar el método elegido.
b. Usa el comando vault auth enable -path=my-login para colocar el método elegido.
c. Realiza las configuraciones faltantes de acuerdo con los pasos que revisaste.

Bibliografía



• HashiCorp. (2021-a). *Define Roles for the Secrets Engine*. Recuperado de https://learn.hashicorp.com/tutorials/vault/custom-secrets-engine-role

• HashiCorp. (2021-b). *AppRole Auth Method*. Recuperado de https://www.vaultproject.io/docs/auth/approle

• HashiCorp. (2021-c). *Auth Methods*. Recuperado de https://www.vaultproject.io/docs/auth

Cierre

Los roles y los métodos de autenticación se utilizan para establecer qué pueden hacer los usuarios. Esto te permitirá añadir una capa de seguridad aun mayor y tendrás el control para saber en dónde fue la fuga de información, en caso de que existiera alguna.

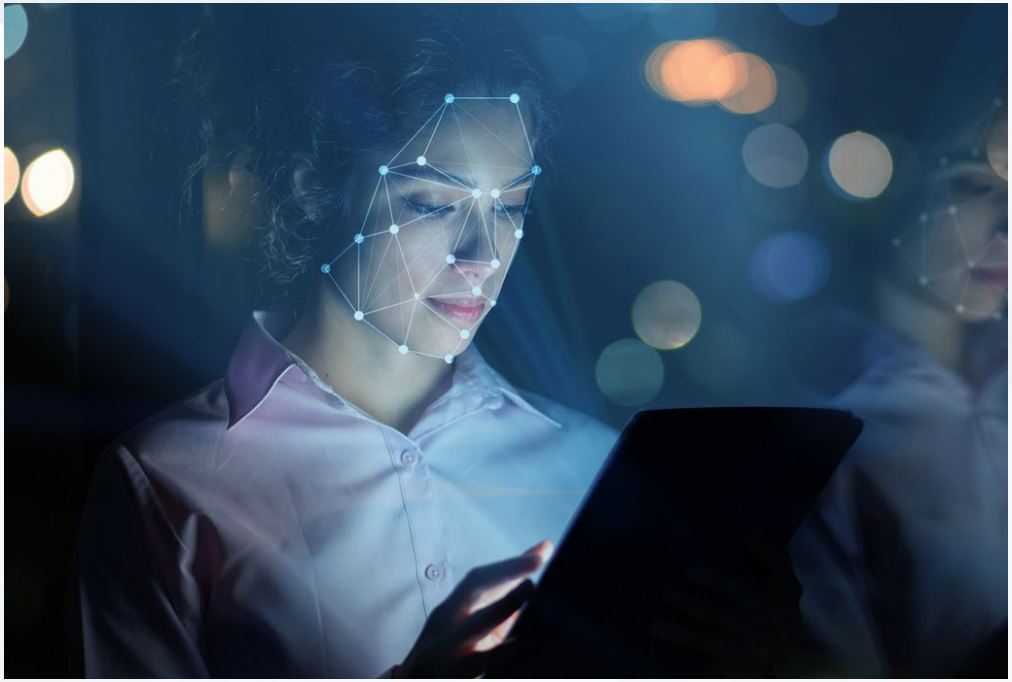
Necesitas roles y métodos de autenticación, ya que, si alguien llegara a perder sus credenciales y no tiene estos bloqueos, cualquier persona que tenga acceso a estas podría obtener toda la información y hacer lo que desee dentro del sistema.

Universidad Tecmilenio

Seguridad en DevOps

Credenciales y grupos en Vault

Semana 8



Dentro de los sistemas deben existir los mecanismos necesarios para protegerlos y Vault se encarga de brindar dicha protección. Para ello, utiliza dos herramientas: rotación de las credenciales y la creación de entidades y grupos.

La primera te permitirá rotar automáticamente las credenciales y la segunda asociar usuarios que sean del mismo cliente, asignándoles la misma política y brindándoles los mismos accesos.

Explicación

Rotación de credenciales en Vault

Existen diferentes credenciales encriptadas que son aprovechadas por diferentes procesos, resguardando datos importantes. La rotación de estas te ayudará a prevenir la fuga de información o que la información sea comprometida (HashiCorp, 2021-a).

Al momento en que inicializas el servidor de Vault, se encuentra en estado seal, el cual no te permitirá hacer ninguna configuración, así que debes aplicar el método unseal.

Para la rotación de credenciales, será necesario utilizar las operaciones rekey y rotate, que permitirán cambiar las llaves unseal, la llave raíz y la llave de encriptación.

La operación de rotar la podrás utilizar para proteger la información que se encuentre en el almacenamiento, a través de un cambio en la llave de encriptación. Esto quiere decir que la operación de rotar generará una nueva llave de encriptación, por lo tanto, la información almacenada será encriptada con esa llave.

Explicación

Entidades y grupos en Vault

Un cliente puede tener diferentes cuentas, ya que puede utilizar su propio proveedor de identidad que sea compatible con Vault. En ese caso, deberás habilitar dichos proveedores en el servidor de Vault, de tal forma que puedas realizar las entidades correspondientes (HashiCorp, 2021-b).

Los clientes se pueden configurar en Vault como entidades y las cuentas que tengan se pueden configurar como alias. Esto se realiza utilizando el motor de secretos de identidad, encargado de organizar cuáles son los clientes que Vault reconocerá y permitirá establecer la conexión.

Pasos para crear una entidad:
1. Deberás inicializar el servidor de Vault y colocar la palabra root para que tengas el token raíz.
2. Abre una nueva terminal y exporta la variable de ambiente para el CLI, con esto redireccionarás el CLI al servidor de Vault.
3. Exporta la variable de ambiente para el CLI, de manera que se autentifique con el servidor de Vault.
4. Usa el método de autenticación de usuario y contraseña.
5. Cambia las políticas y que se asocien correctamente con los dos usuarios.
6. Crea los usuarios y la entidad.

Explicación

Entidades y grupos en Vault (¿cómo crear grupos internos?)

Mediante CLI:

1. Crea una nueva política.
2. Crea un grupo.

Mediante API:

1. Crea el requerimiento para la política de API.
2. Crea la nueva política.
3. Crea el requerimiento para el grupo interno.
4. Crea el grupo interno y añade la entidad al grupo a través del endpoint /identity/group

Mediante Web UI

1. Haz clic en la opción de políticas y crea la política ACL.
2. Ahora escribe "nombre de la política" en el nombre de campo y pégalo en Política.
3. Luego haz clic en Crear política.
4. Ahora entra a la opción Acceso y elige Grupos.
5. Después selecciona Crear grupo.
6. Escribe la información del grupo como corresponde y haz clic en Crear.

Universidad Tecmilenio

Explicación

Entidades y grupos en Vault (¿cómo crear grupos externos?)

Mediante CLI:

1. Crea una nueva política.
2. Habilita el método de autenticación que hayas escogido.
3. Obtén el mount accessor del método de autenticación y guárdalo en el archivo acceso_nombredelmétodo.txt.
4. Realiza la configuración para apuntar Vault hacia tu organización.
5. Crea un grupo externo y guarda el id en group_id.txt.
6. Crea el alias del grupo.

Mediante API:

1. Crea el requerimiento para la política de API.
2. Crea la nueva política.
3. Habilita el método de autenticación escogido.
4. Coloca la organización para configurar el método de autenticación.
5. Obtén el valor del accessor del método de autenticación y guárdalo en el archivo accesor_nombredelmetodo.txt.
6. Crea el requerimiento para el grupo externo del API.
7. Crea el grupo externo y guarda el ID en group_id.txt.
8. Crea el requerimiento para el alias del grupo de API.
9. Crea el alias.

Mediante Web UI:
1. Entra a la opción de políticas y selecciona Crear política ACL.
2. Escribe el nombre del equipo en el campo de nombre y pega la política.
3. Luego haz clic en Crear política.
4. Para habilitar un nuevo método de autenticación, ingresa a Métodos de autenticación dentro de la opción Acceso.
5. Selecciona el método elegido.
6. En la ruta, escribe el nombre del método seleccionado y haz clic en Habilitar método.
7. Haz clic en la opción de Acceso y selecciona Grupos.
8. Selecciona Crear grupo y llena la información solicitada.
9. Haz clic en Crear.
10. Selecciona Añadir alias, escribe el nombre del alias y nuevamente selecciona el método de autenticación para el Auth Backend.
11. Haz clic en Crear.

Universidad Tecmilenio

Explicación

Vault provider para Terraform

Terraform, al no tener un sistema que proteja los secretos, para reducir el riesgo, el *provider* solicitará un token de Vault que tenga un tiempo de vida corto (TTL) (aproximadamente 20 minutos), lo cual provocará que Vault revoque las credenciales después de ese tiempo.

Es importante que recuerdes que Terraform puede leer la información solamente en la fase llamada “plan”. Una vez leída la información, escribirá el resultado en dicho plan.

Explicación

Vault provider en Terraform

Existen diferentes argumentos que el provider acepta. A continuación, revisarás algunos:

- Address (obligatorio llenarlo): se utiliza para colocar el URL del servidor de Vault.
- Add_address_to_env (es opcional llenarlo): su valor predeterminado es falso. En caso contrario, el valor de la variable vault_addr se colocará en el valor del address.
- Token (es opcional llenarlo): el token en Cault será utilizado por Terraform para el provider y la autenticación.
- Token_name (es opcional llenarlo): permite una referencia rastreable de la ejecución gracias a que es utilizado por Terraform para crear tokens secundarios.
- Ca_cert_file (es opcional llenarlo): ruta al archivo en el disco local que se utilizará para validar el actual certificado del servidor de Vault.
- Ca_cert_dir (es opcional llenarlo): ruta al directorio en el disco local que contiene uno o más certificados utilizados para validar el certificado vigente del servidor de Vault.
- Auth_login (es opcional llenarlo): obtiene el token que Terraform va a utilizar mediante auth/<method>/login.

Universidad Tecmilenio

Ejercicio

Te encuentras haciendo el desarrollo de un software para una universidad. El objetivo del software es el manejo de datos de todo su alumnado y personal que trabaja en la universidad.

Te piden realizar las entidades de tal forma que dos usuarios pertenezcan a la misma identidad.

1. Crea una política para asociarla a la entidad y al grupo que elaborarás (inventa la política).

2. Realiza la configuración de la entidad, incluyendo esos dos usuarios (inventa los usuarios y agrégalos).

3. Realiza la configuración para agregar la entidad a un mismo grupo.

Cierre

La rotación de credenciales te permitirá mantener la información segura, de tal forma que prevengas la fuga de esta o su corrupción. La configuración de las entidades y los grupos te permitirá tener un mejor control de los usuarios que podrán acceder a ciertas partes de la información del desarrollo. El provider de Vault permitirá la integración con Terraform con el objetivo de mantener tus secretos protegidos ante cualquier ciberataque.

Bibliografía

• HashiCorp. (2021-a). *Key Rotation*. Recuperado de https://www.vaultproject.io/docs/internals/rotation

• HashiCorp. (2021-b). *Identity: Entities and Groups*. Recuperado de https://learn.hashicorp.com/tutorials/vault/identity