

11

Protection of sensitive data with the vault

Java Backend Developer I

Objetivos

Comprender los conceptos:

- Vault
 - Concepts
 - Tecnologías
 - Caso de Uso (en el laboratorio)
 - Azure Key Vault



Agenda

Revisión de los siguientes conceptos:

- Vault
 - Concepts
 - Tecnologías
 - Caso de Uso (en el laboratorio)
 - Azure Key Vault



Vault

Concepto

Vault es una herramienta para acceder de forma segura a secretos. Un secreto es cualquier cosa a la que se quiera tener severamente controlado como claves de API, contraseñas y certificados. Vault proporciona una interfaz para cualquier secreto a la vez que mantiene un control de acceso y un log de acceso detallado.



Vault

Características

Se engloban en tres aspectos de la seguridad: cifrado, control de acceso y ciclo de vida.

- Almacenamiento seguro de secretos: los secretos son cifrados previamente a ser almacenados en el almacenamiento persistente.
- Secretos dinámicos: puede generar secretos bajo demanda para bases de datos o algunos sistemas como AWS.
- Cifrado de datos: puede cifrar y descifrar datos sin almacenarlos.
- Concesión y renovación: tienen un tiempo de concesión asociado. Al finalizar los revoca -automáticamente, los clientes pueden solicitar renovar las concesiones mediante las API disponibles de Vault.
- Revocación: integra la funcionalidad de revocación, no solo secretos individuales sino jerarquías de secretos.



Vault

Tecnologías

Los motores de secretos son uno de los conceptos en el ámbito de Vault. Son componentes que permite almacenar, generar o cifrar datos. Algunos motores de secretos simplemente almacenan y leen datos, otros se conectan a otros servicios y generan credenciales dinámicamente bajo demanda. Otros motores de secretos proporcionan el cifrado como servicio, tokens de un solo uso, certificados y mucho más. Existen las siguientes tecnologías API actualmente:

- Secrets Engines
- KV Secrets Engine
- Databases Secrets Engine
- RabbitMQ Secrets Engine
- PKI Secrets Engine
- SSH Secrets Engine



Vault

Azure Key Vault

Es un servicio en la nube que proporciona un almacenamiento seguro de secretos. Puede almacenar de forma segura claves, contraseñas, certificados y otros secretos. Los almacenes de claves de Azure se pueden crear y administrar a través del portal de Azure. En esta guía de inicio rápido, crea una bóveda de claves y luego la usa para almacenar un secreto.



Vault

Key Vault

Permite acceder de forma segura a información confidencial desde sus aplicaciones:

- Las claves y los secretos están protegidos sin tener que escribir el código manualmente, y puede usarlos fácilmente en sus aplicaciones.
- Los clientes pueden poseer y administrar sus propias claves para que pueda centrarse en proporcionar las características de software fundamentales. De este modo, las aplicaciones no serán responsables de las claves y secretos del inquilino de sus clientes.
- La aplicación puede usar claves para firma y cifrado y aun así que la administración de claves sea externa a la aplicación, lo que le permite ser adecuada como aplicación distribuida geográficamente.



Vault

Key Vault

- Permite administrar certificados de Key Vault.

Composición de un certificado

- Cuando se crea un certificado de Key Vault, se crean también una clave direccionable y un secreto con el mismo nombre. La clave de Key Vault permite las operaciones de clave y el secreto de Key Vault permite la recuperación del valor del certificado como un secreto. Un certificado de Key Vault también contiene metadatos del certificado X.509 público.

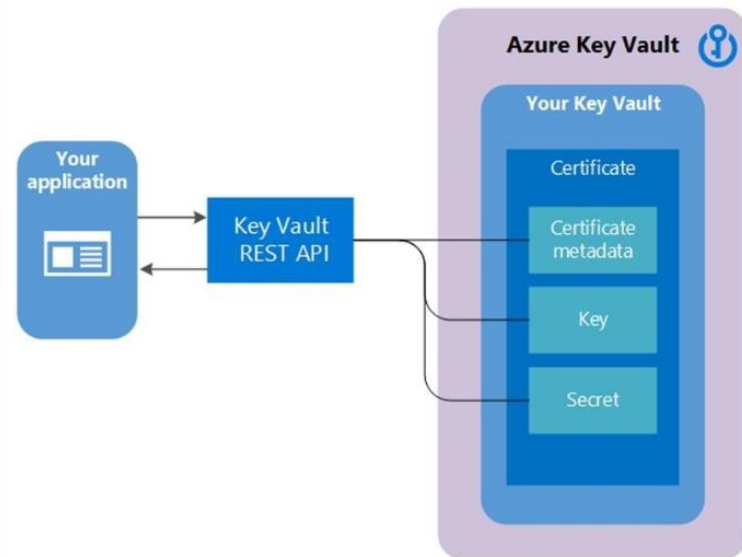


Vault

Key Vault

Composición de un certificado

- El identificador y la versión de los certificados es similar al de las claves y los secretos. Una versión específica de una clave direccionable y el secreto creados con la versión del certificado de Key Vault está disponible en la respuesta del certificado de Key Vault.



Lecturas adicionales

Para obtener información adicional, puede consultar los siguientes enlaces:

- <https://docs.microsoft.com/es-es/azure/key-vault/general/developers-guide>
- <https://docs.microsoft.com/en-us/azure/key-vault/secrets/quick-create-portal>



Resumen

En este capítulo, usted aprendió:

- Vault
 - Concepts
 - Tecnologías
 - Caso de Uso (en el laboratorio)
 - Azure Key Vault

