200 XP

Prueba de conocimientos

7 minutos

Elija la respuesta más adecuada para cada una de las preguntas siguientes. Después, seleccione **Comprobar las respuestas**.

Comprobación de conocimientos

1. ¿Cuál de los siguientes elementos se debe almacenar en Azure Key Vault?

- (●) Secreto
  - ✔ **Los secretos se pueden almacenar en el almacén de claves.**
- ( ) Vínculos al certificado externo
- ( ) Administración de identidades

2. Un grupo selecto de usuarios debe poder crear y eliminar claves en el almacén de claves. Al autenticarse en el plano de datos mediante Azure AD, ¿qué herramienta de seguridad se debe usar para autorizar el acceso en un nivel de rol a estos usuarios?

- ( ) Directivas de acceso de Key Vault
- (●) Control de acceso basado en rol
  - ✔ **Control de acceso basado en rol. Para crear y eliminar almacenes de claves en el plano de datos, debe conceder acceso con RBAC. El uso de directivas de acceso no le proporcionaría control de nivel de rol y no sigue las reglas de privilegios mínimos, como, por ejemplo, Colaborador de almacén de claves.**
- ( ) Autenticación de Azure AD

3. ¿Cuál de estas afirmaciones describe mejor el proceso de autorización y autenticación de Azure Key Vault?

Las aplicaciones se autentican en un almacén con el nombre de usuario y la contraseña del jefe de desarrollo y tienen acceso total a todos los secretos del almacén.

- ◉ Las aplicaciones y los usuarios se autentican en un almacén con sus identidades de Azure Active Directory y se les autoriza a realizar distintas acciones en todos los secretos del almacén.

  ✔ **La autenticación de Key Vault usa las identidades de Azure Active Directory. Las directivas de acceso se usan para proporcionar autorización para las acciones que se aplican a cada secreto en el almacén.**

- ○ Las aplicaciones y los usuarios se autentican en un almacén con una cuenta Microsoft y se les autoriza a acceder a secretos específicos.

4. ¿Cómo ayuda Azure Key Vault a proteger los secretos después de que la aplicación los haya cargado?

- ○ Azure Key Vault genera automáticamente un secreto nuevo después de cada uso.
- ○ Azure Key Vault efectúa un cifrado doble de los secretos y solicita a la aplicación que los descifre de forma local cada vez que se utilizan.
- ◉ No protege los secretos. Los secretos quedan desprotegidos una vez que la aplicación los ha cargado.

  ✔ **No protege los secretos. Una vez que una aplicación ha cargado los secretos, quedan desprotegidos. Asegúrese de no registrarlos, almacenarlos ni devolverlos en las respuestas del cliente.**

5. Un administrador quiere saber más sobre las claves protegidas por software y las claves protegidas por hardware. Elija el tema correcto que podría explicar al administrador.

- ○ Solo las claves protegidas por hardware se cifran en reposo.
- ○ Las claves protegidas por software no están aisladas de la aplicación.
- ◉ Las operaciones criptográficas protegidas por software se realizan en software y las operaciones criptográficas protegidas por hardware se realizan dentro del HSM.

✔ Las operaciones criptográficas se realizan dentro de cada módulo. Las claves HSM ofrecen garantía del nivel 2 de FIPS 140-2. La principal diferencia (además del precio) con respecto a una clave protegida con software es que las operaciones criptográficas se realizan en software mediante servicios de proceso de Azure, mientras que, para las claves protegidas con HSM, se realizan dentro del HSM.

Siguiente unidad: Resumen

Continuar >

¿Cómo lo estamos haciendo? ☆ ☆ ☆ ☆ ☆