Notas de la sesión 01

miércoles, 24 de agosto de 2022

19:22

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.

1. 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?

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.

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

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.

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

1. 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.

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.

Resumen

Azure Key Vault es un almacén seguro basado en la nube para almacenar los certificados y secretos para su uso en las soluciones de Azure.

Debería poder:

* Definir lo que es un almacén de claves y cómo protege certificados y secretos
* Implementar y configurar Azure Key Vault
* Proteger el acceso y la administración del almacén de claves
* Almacenar claves y secretos en el almacén de claves
* Explorar consideraciones de seguridad clave, como la rotación de claves y la copia de seguridad o recuperación

Notas de la sesión 02

Comprobación de conocimientos

1. ¿Qué método usa Microsoft Azure App Service para obtener las credenciales de los usuarios que intentan acceder a una aplicación?

Redireccionamiento a un punto de conexión de proveedor. Las aplicaciones de Microsoft Azure App Service redirigen las solicitudes a un punto de conexión que inicia la sesión de los usuarios para ese proveedor. App Service puede dirigir automáticamente a todos los usuarios no autenticados al punto de conexión de inicio de sesión para estos.

1. ¿Qué tipo de identidades de servicio administradas se pueden crear?

Asignadas por el sistema y asignadas por el usuario. Hay dos tipos de identidades administradas: una identidad administrada asignada por el sistema se habilita directamente en una instancia de servicio de Azure. Cuando se habilita la identidad, Azure crea una identidad para la instancia del servicio en el inquilino de Azure AD de confianza de la suscripción de la instancia. La creación de una aplicación con una identidad asignada por el usuario requiere que una organización cree la identidad y, luego, agregue el identificador de recurso a la configuración de la aplicación.

1. Una aplicación de App Service almacena gráficos de página en una cuenta de almacenamiento de Azure. La aplicación debe autenticarse mediante programación en la cuenta de almacenamiento, ¿qué se debe configurar?

Crear una identidad administrada. Una identidad administrada es una entidad de seguridad de Azure AD que representa al recurso (aplicación). Las identidades administradas pueden ser administradas por el usuario o por el sistema.

1. ¿Cómo cambia el uso de identidades administradas para recursos de Azure la forma en que una aplicación se autentica en Azure Key Vault?

La aplicación obtiene los tokens de un servicio de tokens en lugar de hacerlo de Azure Active Directory. Al habilitar la identidad administrada en una aplicación web, Azure activa un servicio REST de concesión de token independiente para que la aplicación lo use específicamente. La aplicación solicitará tokens de este servicio, en lugar de Azure Active Directory.

Resumen

Mejore la seguridad de las aplicaciones para proteger los datos y los sistemas a los que puede acceder la aplicación. Use las identidades para limitar quién puede ejecutar una aplicación y lo que pueden hacer.

Debería poder:

* Registrar una aplicación en Azure mediante el registro de aplicaciones
* Seleccionar y configurar los usuarios de Azure AD que pueden acceder a cada aplicación
* Configurar e implementar certificados de aplicación web

Notas de la sesión 03

Comprobación de conocimientos

1. Es necesario proporcionar a un empleado del personal eventual acceso temporal de solo lectura al contenido de un contenedor de cuentas de almacenamiento de Azure denominado "Media". Es importante conceder acceso respetando el principio de seguridad de privilegios mínimos. ¿Qué se debe configurar?

Genere un token de SAS para el contenedor. La SAS puede proporcionar acceso de solo lectura.

1. Una empresa tiene tanto un entorno de desarrollo como de producción. El entorno de desarrollo necesita acceso limitado en el tiempo al almacenamiento. El entorno de producción necesita acceso sin restricciones a los recursos de almacenamiento. Para configurar el acceso al almacenamiento para cumplir con los requisitos. ¿Qué opciones de configuración hay que elegir?

Use firmas de acceso compartido para las aplicaciones de desarrollo. Y use claves de acceso para las aplicaciones de producción. Las firmas de acceso compartido ofrecen una manera de proporcionar un acceso de almacenamiento más granular que las claves de acceso. Por ejemplo, limite el acceso a “solo lectura” y, después, limite los servicios y tipos de recursos. Las firmas de acceso compartido se pueden configurar durante un período de tiempo especificado, lo que cumple los requisitos del escenario. Las claves de acceso proporcionan acceso sin restricciones a los recursos de almacenamiento, que es el requisito para las aplicaciones de producción en este escenario.

1. Se está auditado una empresa. No se sabe cuánto tiempo tardará en realizarse la auditoría, pero durante ese tiempo los archivos no se deben cambiar ni quitar. Se pueden leer o crear nuevos archivos. ¿Qué se debe hacer para configurar esto?

Agregue una directiva de retención de suspensión legal al contenedor de blobs. Identifique una etiqueta para los elementos que se protegen. Si el intervalo de retención no se conoce, los usuarios pueden establecer suspensiones legales para almacenar los datos inmutables hasta que estas desaparezcan. Cuando se establece una directiva de suspensión legal, se pueden crear y leer blobs, pero no se pueden modificar ni eliminar. Cada suspensión legal está asociada a una etiqueta alfanumérica definida por el usuario que se usa como una cadena de identificación (por ejemplo, un identificador de caso, un nombre de evento, etc.).

1. Al configurar un recurso compartido de archivos de Azure para el grupo de negocios, ¿cuál de las siguientes condiciones es verdadera?

Azure Files puede autenticarse en Azure Active Directory Domain Services. Azure Files puede autenticarse con Azure AD.

1. Al configurar la transferencia segura necesaria, la oficina de cumplimiento debe comprender cómo se protegen las conexiones cuando se realizan llamadas operativas de la API de REST a una cuente de Azure Storage. ¿Qué información se debe proporcionar a continuación?

De forma predeterminada, las nuevas cuentas de almacenamiento tienen habilitada la transferencia segura necesaria. Para ayudar a proteger los datos, la transferencia segura está habilitada de forma predeterminada en las nuevas cuentas de almacenamiento.

Resumen

Proteja siempre los datos y asegúrese siempre de saber dónde se almacenan, de forma que esté protegido por las leyes de soberanía de datos. En este módulo ha visto cómo proteger el acceso a los datos y los archivos y después ha explorado cómo se cifran los datos en reposo y en tránsito.

Debería poder:

* Definición de la soberanía de datos y cómo se logra en Azure
* Configuración del acceso de Azure Storage de forma segura y administrada
* Cifrado de los datos mientras están en reposo y en tránsito
* Aplicación de reglas para la retención de datos

Notas de la sesión 04

Comprobación de conocimientos

1. Un administrador de base de datos SQL ha leído recientemente sobre ataques por inyección de código SQL. Pregunta qué se puede hacer para minimizar el riesgo de este tipo de ataque. ¿Cuál de las siguientes características ayudará a proteger la base de datos?

Protección contra amenazas avanzada. Advanced Threat Protection es una característica de Advanced Data Security para bases de datos. La característica proporciona alertas cuando se produce un posible ataque, como inyección de código SQL.

1. Una organización proporciona un servicio de soporte para sus clientes. Los representantes de servicio deben identificar a las personas que llaman mediante los cuatro últimos números de su tarjeta de crédito. Es necesario asegurarse de que el número completo de la tarjeta de crédito no esté totalmente expuesto a los representantes de servicio. ¿Cuál de las siguientes opciones debe implementar?

Enmascaramiento dinámico de datos. El enmascaramiento dinámico de datos limita la exposición de información confidencial ocultándolos a los usuarios sin privilegios. Esta característica permite a los clientes designar la cantidad de datos confidenciales que se revelarán.

1. Los auditores deben estar seguros de que los datos confidenciales de la base de datos siempre permanecen cifrados en reposo, en tránsito y en uso. Para garantizar a los auditores que esto se está haciendo, ¿cuál de las siguientes características está configurada?

Always Encrypted ayuda a proteger la información confidencial en reposo en el servidor, durante el movimiento entre el cliente y el servidor, y mientras los datos están en uso. Always Encrypted garantiza que los datos confidenciales nunca van a aparecer como texto no cifrado dentro del sistema de base de datos. Después de configurar el cifrado de datos, solo las aplicaciones cliente o los servidores de aplicaciones que tienen acceso a las claves pueden acceder a los datos de texto no cifrado. Always Encrypted utiliza el algoritmo AEAD\_AES\_256\_CBC\_HMAC\_SHA\_256 para cifrar los datos de la base de datos.

1. Una aplicación web de App Service usa una base de datos SQL. Los usuarios deben autenticarse en la base de datos con sus credenciales de Azure AD. ¿Cuál de las siguientes tareas de configuración habilitaría esto?

Creación de usuarios en cada base de datos. No cree usuarios en la base de datos maestra. En su lugar, se deben crear usuarios contenidos en cada base de datos.

1. ¿Qué tipo de reglas de firewall se pueden configurar para una base de datos de Azure SQL?

Reglas de firewall de nivel de servidor. Se pueden crear reglas de firewall de nivel de servidor y reglas de firewall de nivel de base de datos. Las reglas de firewall de IP de nivel de servidor permiten a los clientes acceder a toda la base de Azure SQL Database, es decir, todas las bases de datos dentro del mismo servidor de base de datos SQL. Estas reglas se almacenan en la base de datos maestra. Las reglas de firewall de IP de nivel de base de datos permiten a los clientes acceder a determinadas bases de datos seguras dentro del mismo servidor de base de datos SQL. Puede crear estas reglas para cada base de datos (incluida la base de datos maestra) y se almacenan en las bases de datos individuales.

Resumen

Asegurarse de que los datos están seguros cuando se almacenan en bases de datos SQL de Azure es una opción imprescindible para cada ingeniero de seguridad de Azure. Azure proporciona varias características para ayudar a bloquear las bases de datos y supervisar su seguridad.

Debería poder:

* Configurar qué usuarios y aplicaciones tienen acceso a las bases de datos SQL.
* Bloquear el acceso a los servidores mediante firewalls.
* Detectar, clasificar y auditar el uso de los datos.
* Cifrar y proteger los datos mientras están almacenados en la base de datos.