200 XP

Prueba de conocimientos

7 minutos

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

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?

- ○ Establezca el nivel de acceso público en contenedor.
- ◉ Genere un token de firma de acceso compartido (SAS) para el contenedor.

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

- ○ Comparta la etiqueta de entidad de contenedor (ETag) con el miembro del personal eventual.

2. 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.

- ○ Usar firmas de acceso compartido para las aplicaciones de producción. A continuación, use las claves de acceso para las aplicaciones de desarrollo.
- ○ Usar directivas de acceso almacenadas para las aplicaciones de producción. Además, emplee el uso compartido de recursos entre orígenes para las aplicaciones de desarrollo.

3. 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 basada en el tiempo al contenedor de blobs. Y cree una etiqueta para identificar los elementos que se protegen.
- ◉ Agregue una directiva de retención de suspensión legal al contenedor de blobs. Además, identifique una etiqueta para los elementos que se protegen.

✔ **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.).**

- ○ Configure un período de retención de dos semanas con una opción para renovar. Después, agregue una directiva de retención basada en el tiempo al contenedor de blobs.

4. 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.**

- ( ) Azure Files no puede autenticarse en Active Directory Domain Services local.
- ( ) Azure Files puede usar RBAC para permisos de nivel de recurso compartido o de directorio o archivo.

5. 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?

- ( ) Las solicitudes de almacenamiento pueden ser HTTPS o HTTP.
- ( ) Las solicitudes de almacenamiento deben ser SMB con la marca de acceso a datos habilitada.
- (●) 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.**

Siguiente unidad: Resumen

Continuar >

¿Cómo lo estamos haciendo? ☆ ☆ ☆ ☆ ☆