**Introducción**

Azure Storage proporciona un completo conjunto de funcionalidades de seguridad que colaboran entre sí para permitir a los desarrolladores compilar aplicaciones seguras.

En este módulo, su empresa está almacenando datos confidenciales (incluida información personal) en Azure Storage. Los datos se usan internamente y también los usan desarrolladores de aplicaciones externas. Es responsable de garantizar que los datos sean seguros para todos los usuarios. Se le encarga proporcionar soluciones de configuración para conceder acceso seguro a la información.

**Objetivos de aprendizaje**

En este módulo aprenderá a:

* Configure una firma de acceso compartido, incluido el identificador uniforme de recursos (URI) y los parámetros de SAS.
* Configure el cifrado de Azure Storage.
* Implementar claves administradas por el cliente.
* Recomiende oportunidades para mejorar la seguridad de Azure Storage.

**Aptitudes evaluadas**

El contenido del módulo le ayuda a prepararse para el [examen AZ-104: Administrador de Microsoft Azure](https://learn.microsoft.com/es-es/certifications/exams/az-104). Los conceptos del módulo tratan los siguientes aspectos:

Implementación y administración del almacenamiento (15-20 %)

* Almacenamiento seguro
  + Creación de tokens de firma de acceso compartido (SAS)
  + Administración de las claves de acceso
  + Configuración de la autenticación de Microsoft Entra para una cuenta de almacenamiento de Azure

**Revisión de las estrategias de seguridad de Azure Storage**

Los administradores usan distintas estrategias para garantizar que sus datos estén seguros. Entre los enfoques comunes se incluyen el cifrado, la autenticación, la autorización y el control de acceso de usuarios con credenciales, permisos de archivo y firmas privadas. Azure Storage ofrece un conjunto de funcionalidades de seguridad basadas en estrategias comunes que le ayudarán a proteger los datos.

**Cosas que debe saber sobre las estrategias de seguridad de Azure Storage**

Veamos algunas de las características de seguridad de Azure Storage.

* **Cifrado**. Todos los datos escritos en Azure Storage se cifran automáticamente con el cifrado de Azure Storage.
* **Autenticación**. Microsoft Entra ID y el control de acceso basado en roles (RBAC) son compatibles con Azure Storage para las operaciones de administración de recursos y las operaciones de datos.
  + Asigne roles RBAC en el ámbito de la cuenta de almacenamiento de Azure a las entidades de seguridad y use Microsoft Entra ID para autorizar las operaciones de administración de recursos, como la administración de claves.
  + La integración de Microsoft Entra se admite para las operaciones de datos en Azure Blob Storage y Azure Queue Storage.
* **Datos en tránsito**. Los datos se pueden proteger en tránsito entre una aplicación y Azure usando cifrado de cliente, HTTPS o SMB 3.0.
* **Cifrado de discos**. Los discos del sistema operativo y los discos de datos que Azure Virtual Machines usa se pueden cifrar mediante Azure Disk Encryption.
* **Firmas de acceso compartido**. Se puede conceder acceso delegado a los objetos de datos en Azure Storage mediante el uso de una firma de acceso compartido (SAS).
* **Autorización**. Todas las solicitudes que se realicen en un recurso protegido en Blob Storage, Azure Files, Queue Storage o Azure Cosmos DB (Azure Table Storage) deben estar autorizadas. La autorización garantiza que los recursos de la cuenta de almacenamiento estén accesibles únicamente cuando así lo quiera y solo para los usuarios o las aplicaciones a los que conceda acceso.

**Cosas que deben tenerse en cuenta al usar la seguridad de autorización**

Revise las estrategias siguientes para autorizar solicitudes en Azure Storage. Piense en qué estrategias de seguridad funcionarían para su instancia de Azure Storage.

| **Estrategia de autorización** | **Descripción** |
| --- | --- |
| **Microsoft Entra ID** | Microsoft Entra ID es el servicio de administración de identidades y acceso basada en la nube de Microsoft. Con Microsoft Entra ID, puede asignar acceso específico a usuarios, grupos o aplicaciones mediante el control de acceso basado en roles. |
| **Clave compartida** | La autorización de clave compartida se basa en las claves de acceso de la cuenta de almacenamiento de Azure y en otros parámetros para generar una cadena de firma cifrada. La cadena se pasa en la solicitud, en el encabezado de autorización. |
| **Firmas de acceso compartido** | Una firma de acceso compartido (SAS) delega el acceso a un recurso determinado de la cuenta de almacenamiento de Azure con los permisos especificados y durante un intervalo de tiempo concreto. |
| **Acceso anónimo a contenedores y blobs** | Opcionalmente, puede hacer que los recursos de blobs se hagan públicos en los contenedores o blobs. Cualquier usuario puede acceder a un contenedor o blob público para consultarlo de forma anónima. Las solicitudes de lectura para contenedores y blobs públicos no requieren autorización. |

**Creación de firmas de acceso compartido**

Una firma de acceso compartido (SAS) es un identificador de recursos uniforme (URI) que concede derechos de acceso restringido a recursos de Azure Storage. Una SAS es una forma segura de compartir los recursos de almacenamiento sin poner en peligro las claves de cuenta.

Puede proporcionar una SAS a los clientes que no deben tener acceso a la clave de la cuenta de almacenamiento. Mediante la distribución de un URI de SAS entre estos clientes, les concede acceso a un recurso durante un período de tiempo específico.

**Aspectos que se deben saber sobre las firmas de acceso compartido**

Vamos a revisar algunas características de una SAS.

* Una SAS le ofrece control granular del tipo de acceso que se concede a los clientes que tienen la SAS.
* Una SAS de nivel de cuenta puede delegar el acceso a varios servicios de Azure Storage, como blobs, archivos, colas y tablas.
* Puede especificar el intervalo de tiempo para el que una SAS es válida, incluida la hora de inicio y la hora de expiración.
* Especifique los permisos concedidos por la SAS. Una SAS para un blob podría conceder permisos de lectura y escritura a ese blob, pero no permisos de eliminación.
* SAS proporciona control de nivel de cuenta y de nivel de servicio.
  + Una SAS de **nivel de cuenta** delega el acceso a los recursos en uno o varios de los servicios de Azure Storage.
  + Una SAS de **nivel de servicio** administra el acceso a un recurso en un solo servicio de Azure Storage.

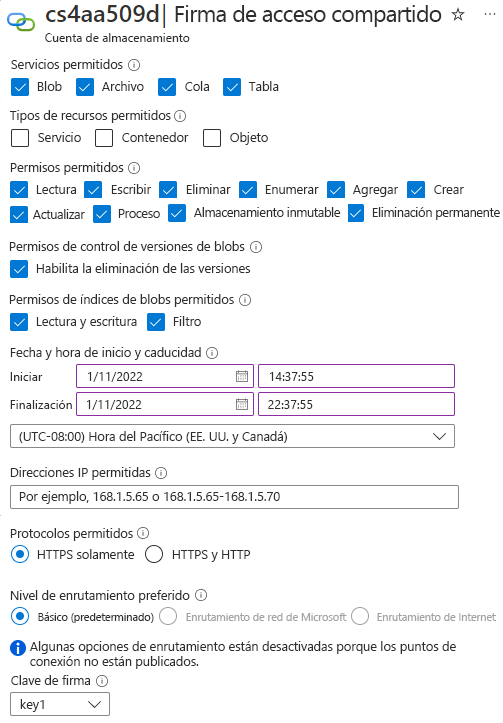
**Nota**

Una **directiva de acceso almacenada** puede proporcionar otro nivel de control cuando se utiliza una SAS de nivel de servicio en el lado servidor. Puede agrupar SAS y proporcionar otras restricciones mediante una directiva de acceso almacenada.

* Hay opciones de configuración de SAS opcionales:
  + **Direcciones IP**. Puede identificar una dirección IP o un intervalo de direcciones IP de las que Azure Storage aceptará la SAS. Configure esta opción para especificar un intervalo de direcciones IP que pertenecen a su organización.
  + **Protocolos** Puede especificar el protocolo sobre el que Azure Storage acepta la SAS. Configure esta opción para restringir el acceso a los clientes mediante HTTPS.

**Configuración de una firma de acceso compartido**

En Azure Portal, se configuran varias opciones para crear una SAS. A medida que revise estos detalles, tenga en cuenta cómo puede implementar firmas de acceso compartido en la solución de seguridad de almacenamiento.



* **Método de firma**: elija el método de firma, como clave de cuenta o clave de delegación de usuarios.
* **Clave de firma**: seleccione la clave de firma de la lista de claves.
* **Permisos**: seleccione los permisos concedidos por la SAS, como lectura o escritura.
* **Fecha y hora de inicio y expiración**: especifique el intervalo de tiempo para el que la SAS es válida. Establezca la hora de inicio y la hora de expiración.
* **Direcciones IP permitidas**: (opcional) puede identificar una dirección IP o un intervalo de direcciones IP de las que Azure Storage aceptará la SAS.
* **Protocolos permitidos**: (opcional) seleccione el protocolo sobre el que Azure Storage acepta la SAS.

**Determinación del cifrado de Azure Storage**

El cifrado de Azure Storage para datos en reposo protege sus datos al asegurarse de que se cumplen los compromisos de seguridad y cumplimiento de la organización. Los procesos de cifrado y descifrado se realizan de forma automática. Dado que los datos están protegidos de forma predeterminada, no es necesario modificar el código ni las aplicaciones.

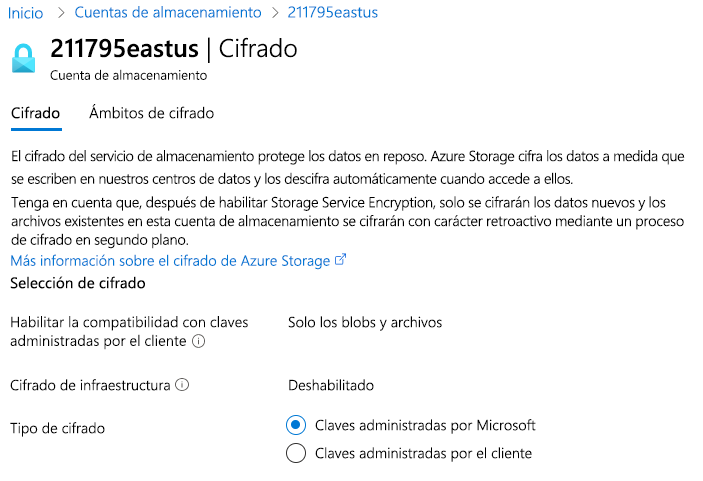
**Cosas que debe saber sobre el cifrado de Azure Storage**

Examine las características siguientes del cifrado de Azure Storage.

* Los datos se cifran automáticamente antes de conservarlos en Azure Managed Disks, Azure Blob Storage, Azure Queue Storage, Azure Cosmos DB, Azure Table Storage o Azure Files.
* Los datos se descifran automáticamente antes de recuperarlos.
* El cifrado de Azure Storage, el cifrado en reposo, el descifrado y la administración de claves son transparentes para los usuarios.
* Todos los datos escritos en Azure Storage se cifran mediante el Estándar de cifrado avanzado (AES) de 256 bits. AES es uno de los cifrados de bloque más seguros que existen.
* El cifrado de Azure Storage está habilitado para todas las cuentas de almacenamiento, nuevas o existentes, y no se puede deshabilitar.

**Configuración del cifrado de Azure Storage**

En Azure Portal, especifique el tipo de cifrado para configurar el cifrado de Azure Storage. Puede encargarse de administrar las claves o elegir que las administre Microsoft. Considere cómo puede implementar el cifrado de Azure Storage para la seguridad del almacenamiento.



**Creación de claves administradas por el cliente**

Para la solución de seguridad de Azure Storage, puede usar Azure Key Vault para administrar las claves de cifrado. Las API de Azure Key Vault se pueden usar para generar claves de cifrado. También puede crear sus propias claves de cifrado y almacenarlas en un almacén de claves.

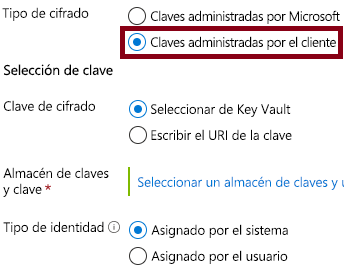
**Cosas que debe saber sobre las claves administradas por el cliente**

Tenga en cuenta las siguientes características de las claves administradas por el cliente.

* Al crear sus propias claves (denominadas claves *administradas por el cliente*), tiene mayor flexibilidad y control.
* Puede crear, deshabilitar, auditar, rotar y definir controles de acceso para sus claves de cifrado.
* Las claves administradas por el cliente se pueden usar con el cifrado de Azure Storage. Puede usar una clave nueva o un almacén de claves y una clave existentes. La cuenta de almacenamiento de Azure y el almacén de claves deben estar en la misma región, pero pueden estar en distintas suscripciones.

**Configuración de claves administradas por el cliente**

En Azure Portal, puede configurar claves de cifrado administradas por el cliente. Puede crear sus propias claves o hacer que Microsoft las administre. Considere cómo puede usar Azure Key Vault para crear sus propias claves de cifrado administradas por el cliente.



* **Tipo de cifrado**: elija cómo se administra la clave de cifrado, si lo hace Microsoft o usted mismo (cliente).
* **Clave de cifrado**: escriba un URI para especificar una clave de cifrado o seleccione una clave de un almacén de claves existente.

**Aplicar procedimientos recomendados de seguridad para Azure Storage**

Hemos revisado cómo crear y trabajar con una firma de acceso compartido (SAS) y las ventajas que puede proporcionar a la solución de seguridad de almacenamiento.

Es importante comprender que, al usar una SAS en la aplicación, puede haber riesgos potenciales.

* Si se compromete la seguridad de una SAS, cualquiera que la obtenga podrá utilizarla, incluido un usuario malintencionado.
* Si una SAS proporcionada para una aplicación cliente expira y la aplicación no puede recuperar una nueva SAS del servicio, la funcionalidad de la aplicación puede verse afectada.

Vea este vídeo para obtener más ideas sobre cómo proteger el almacenamiento. Este vídeo se basa en [Sugerencias y trucos de Azure #272: Procedimientos recomendados de seguridad de Azure](https://microsoft.github.io/AzureTipsAndTricks/blog/blog/tip272.html).

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

<https://youtu.be/mntOLLNejUo?list=PLLasX02E8BPCNCK8Thcxu-Y-XcBUbhFWC>

**Recomendaciones para administrar riesgos**

Echemos un vistazo a algunas recomendaciones que pueden ayudar a mitigar los riesgos al trabajar con una SAS.

| **Recomendación** | **Descripción** |
| --- | --- |
| **Uso siempre de HTTPS para la creación y distribución** | Si se pasa una SAS a través de HTTP, un atacante podría interceptarla y usarla. Estos ataques de tipo *Man in the middle* pueden poner en peligro los datos confidenciales o permitir que un usuario malintencionado dañe los datos. |
| **Haga referencia a las directivas de acceso almacenadas cuando sea posible.** | Las directivas de acceso almacenadas le ofrecen la posibilidad de revocar permisos sin tener que volver a generar las claves de cuenta de almacenamiento. Establezca una fecha de expiración futura para la clave de la cuenta de almacenamiento. |
| **Establecer tiempos de expiración a corto plazo para una SAS no planeada** | Si una SAS está en peligro, puede mitigar los ataques limitando la validez de SAS a un breve tiempo. Este procedimiento es importante si no puede hacer referencia a una directiva de acceso almacenada. Las expiraciones a corto plazo también limitan la cantidad de datos que puede escribirse en un blob mediante la limitación del tiempo disponible para cargarlos. |
| **Requerir que los clientes renueven automáticamente la SAS**. | Requiera a los clientes que renueven la SAS antes de la fecha de expiración. Al renovar anticipadamente, da margen para diversos reintentos si el servicio que proporciona la SAS no está disponible. |
| **Planear cuidadosamente la hora de inicio de SAS** | Si establece la hora de inicio de la SAS en ahora, pueden producirse errores intermitentes durante los primeros minutos debido al sesgo del reloj (diferencias en la hora actual según las distintas máquinas). En general, establezca la hora de inicio sea al menos 15 minutos en el pasado. O bien, no establezca una hora de inicio específica, lo que hace que la SAS sea válida inmediatamente en todos los casos. Las mismas condiciones se aplican generalmente a la hora de expiración. Puede observar hasta 15 minutos de sesgo del reloj en cualquier dirección de cualquier solicitud. Para los clientes con una versión API REST anterior a 2012-02-12, la duración máxima de una SAS que no hace referencia a una directiva de acceso almacenada es de 1 hora. Se producirá un error en las directivas que especifican un período más largo. |
| **Definir los permisos de acceso de los recursos** | Un procedimiento recomendado de seguridad es proporcionar al usuario los privilegios mínimos necesarios. Si un usuario solo necesita acceso de lectura en una única entidad, concédale acceso de lectura a esa única entidad y no acceso de lectura, escritura o eliminación a todas las entidades. Esta práctica también ayuda a reducir los daños si se pone en peligro una SAS porque esta tiene menos poder en manos de un atacante. |
| **Descripción de la facturación de la cuenta para el uso, incluida una SAS** | Si proporciona acceso de escritura a un blob, un usuario puede seleccionar cargar un blob de 200 GB. Si le proporciona también acceso de lectura, puede seleccionar descargar el blob 10 veces, lo que le supone 2 TB de costos de salida. Proporcione de nuevo permisos limitados para ayudar a mitigar acciones potenciales de usuarios malintencionados. Use una SAS de corta duración para reducir esa amenaza, pero tenga en cuenta el sesgo del reloj y la hora final. |
| **Validar los datos escritos mediante una SAS** | Cuando una aplicación cliente escribe datos en la cuenta de almacenamiento de Azure, tenga en cuenta que pueden existir problemas con esos datos. Si la aplicación requiere datos validados o autorizados, valide los datos después de escribirlos, pero antes de usarlos. Esta práctica también le protege frente a los datos erróneos o malintencionados que se escriben en la cuenta, ya sea mediante un usuario que adquirió correctamente la SAS o un usuario que aproveche una SAS errónea. |
| **No dar por sentado que una SAS siempre será la opción correcta** | En algunas ocasiones, los riesgos asociados a una operación determinada en la cuenta de almacenamiento superan las ventajas del uso de una SAS. Para esas operaciones, cree un servicio de nivel medio que escriba en la cuenta de almacenamiento después de llevar a cabo una auditoría, autenticación o validación de la regla de negocio. A veces también es más sencillo administrar el acceso de otras formas. Si desea que todos los blobs de un contenedor puedan leerse públicamente, puede hacer que el contenedor sea público en lugar de proporcionar un SAS a cada cliente para obtener acceso. |
| **Supervisar las aplicaciones con Azure Storage Analytics** | Puede usar el registro y las métricas para observar cualquier pico en los errores de autenticación. Es posible que vea picos de una interrupción en el servicio del proveedor de SAS o la eliminación involuntaria de una directiva de acceso almacenada. |

**Prueba de conocimientos**

200 XP

* 3 minutos

Su empresa usa una cuenta de almacenamiento de Azure para almacenar grandes cantidades de archivos de audio y vídeo. Los contenedores se usan para almacenar cada uno de los tipos de archivo y el acceso se limita a esos archivos multimedia. Además, solo se puede acceder a los archivos a través de firmas de acceso compartido.

* La empresa quiere poder revocar el acceso a los archivos y cambiar el período durante el que los usuarios pueden acceder a ellos.
* La empresa está planeando un modelo de delegación para Azure Storage. Las aplicaciones del entorno de producción deben tener acceso sin restricciones a los recursos de Azure Storage.
* Está investigando cómo usar reglas de configuración de red, firmas de acceso compartido (SAS) y directivas de acceso almacenadas para implementar el acceso seguro a Azure Storage.

**Responda a las siguientes preguntas**

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

Principio del formulario

**1. ¿Qué solución es la forma más fácil de implementar el almacenamiento seguro para los archivos multimedia de la empresa?**

1. Cree una firma de acceso compartido (SAS) para cada usuario y elimine la SAS para evitar el acceso.
2. Cree directivas de acceso almacenadas para cada contenedor para permitir la revocación del acceso o el cambio de la duración.
3. Vuelva a generar periódicamente la clave de cuenta para controlar el acceso a los archivos.

**2. ¿Cuál es la regla de red predeterminada al configurar el acceso de red a la cuenta de Azure Storage?**

1. Permita todas las conexiones desde todas las redes.
2. Permita todas las conexiones desde un intervalo de direcciones IP privadas.
3. Deniegue todas las conexiones desde todas las redes.

**3. ¿Cuál es la mejor forma de implementar el acceso seguro a Azure Storage para los usuarios de la empresa?**

1. Use firmas de acceso compartido para las aplicaciones de producción.
2. Use claves de acceso para las aplicaciones de producción.
3. Use directivas de acceso almacenadas para las aplicaciones de producción.
4. B
5. A
6. B

Final del formulario

**Resumen y recursos**

Los administradores de Azure deben estar familiarizados con cómo configurar la seguridad del almacenamiento.

En este módulo, ha examinado varias opciones para proteger Azure Storage. Ha descubierto cómo configurar firmas de acceso compartido (SAS), incluido el identificador uniforme de recursos (URI) y los parámetros de SAS. Ha revisado cómo implementar claves administradas por el cliente y definir directivas de acceso almacenadas para configurar el cifrado de Azure Storage. Ha explorado oportunidades para mejorar la solución de seguridad de Azure Storage.