**Introducción**

Este módulo está diseñado para proporcionar a los administradores los conocimientos y aptitudes necesarios para planear e implementar medidas de seguridad completas para los recursos de almacenamiento de Azure, protegiendo la integridad, la confidencialidad y la disponibilidad de los datos.

**Escenario**

Imagine que es un administrador de almacenamiento de Azure responsable de administrar los recursos de almacenamiento del entorno de Azure de la organización. La organización confía en los servicios de almacenamiento de Azure para almacenar datos confidenciales y debe asegurarse de que estos datos estén protegidos contra amenazas de seguridad de datos y acceso no autorizado.

**Objetivos de aprendizaje**

Al final de este módulo, los participantes podrán:

* Planee e implemente estrategias de seguridad para los recursos de almacenamiento de Azure para proteger los datos en reposo y en tránsito.
* Configure el control de acceso de las cuentas de almacenamiento para administrar los permisos de forma eficaz.
* Administre el ciclo de vida de las claves de acceso de la cuenta de almacenamiento para mantener la seguridad.
* Seleccione y configure los métodos adecuados para acceder a Azure Files, Blob Storage, Tablas y Colas en función de casos de uso específicos.
* Implemente medidas de seguridad, como la eliminación temporal, las copias de seguridad, el control de versiones y el almacenamiento inmutable para protegerse frente a amenazas de seguridad de datos.
* Configure Bring Your Own Key (BYOK) para mejorar el cifrado de datos y la administración de claves.
* Habilite el cifrado doble en el nivel de infraestructura de Azure Storage para proporcionar una capa adicional de seguridad.

**Objetivos**

El módulo tiene como objetivo dotar a los participantes de los conocimientos y habilidades necesarios para diseñar, implementar y administrar estrategias de seguridad completas para los recursos de almacenamiento de Azure. Los participantes podrán proteger los datos en reposo y en tránsito, administrar el control de acceso de forma eficaz e implementar medidas de cifrado y protección de datos para garantizar la seguridad de los recursos de datos críticos.

**Configuración del control de acceso para las cuentas de almacenamiento**

Todas las solicitudes realizadas en un recurso protegido en Blob, File, Queue o Table service deben estar autorizadas. La autorización garantiza que los recursos de la cuenta de almacenamiento estén accesibles únicamente en el momento que defina y solo para los usuarios o las aplicaciones a los que conceda acceso.

En la tabla siguiente se describen las opciones que ofrece Azure Storage para autorizar el acceso a los recursos:

| **Artefacto de Azure** | **Clave compartida (clave de cuenta de almacenamiento)** | **Firma de acceso compartido (SAS)** | **Microsoft Entra ID** | **Active Directory Domain Services locales** | **Acceso de lectura público anónimo** |
| --- | --- | --- | --- | --- | --- |
| Azure Blobs | Compatible | Admitido | Admitido | No compatible | Compatible |
| Azure Files (SMB) | Compatible | No compatible | Compatible con Microsoft Entra Domain Services o Microsoft Entra Kerberos | Admitido, las credenciales deben sincronizarse con Microsoft Entra ID | No compatible |
| Azure Files (REST) | Compatible | Admitido | Admitido | No compatible | No compatible |
| Colas de Azure | Compatible | Admitido | Admitido | No compatible | No compatible |
| Azure Tables | Compatible | Admitido | Admitido | No compatible | No compatible |

Cada opción de autorización se describe brevemente a continuación:

**Microsoft Entra ID**: Microsoft Entra es el servicio de administración de identidad y acceso basado en la nube de Microsoft. La integración de Microsoft Entra ID está disponible para los servicios Blobs, Files, Cola y Tabla. Con Microsoft Entra ID, es posible asignar acceso específico a usuarios, grupos o aplicaciones mediante el control de acceso basado en roles (RBAC).

**Autorización de Microsoft Entra Domain Services** para Azure Files: Azure Files admite la autorización basada en identidades a través del Bloque de mensajes del servidor (SMB) a través de Microsoft Entra Domain Services. Puede usar RBAC para el control específico de acceso de los clientes a los recursos de Azure Files en una cuenta de almacenamiento.

**Autorización de Microsoft Entra ID** para Azure Files: Azure Files admite la autorización basada en identidades sobre SMB mediante Microsoft Entra ID. El servicio de dominio de Microsoft Entra se puede hospedar en máquinas locales o en máquinas virtuales de Azure. El acceso de SMB a Files se admite mediante el uso de las credenciales de Microsoft Entra ID de las máquinas unidas a un dominio, independientemente de que sea local o en Azure. Es posible usar RBAC para el control de acceso de nivel de recurso compartido y la lista de control de acceso discrecional (DACL) del sistema de archivos de nueva tecnología (NTFS) para la aplicación de permisos de nivel de archivo y directorio.

**Clave compartida**: La autorización de clave compartida se basa en las claves de acceso de la cuenta y otros parámetros para generar una cadena de firma cifrada que se pasará en la solicitud en el encabezado de autorización.

**Firmas de acceso compartido**: Las firmas de acceso compartido (SAS) delegan el acceso a un recurso determinado de la cuenta con los permisos especificados y durante un intervalo de tiempo especificado.

**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.

La autenticación y autorización del acceso a los datos de blobs, archivos, colas y tablas con Microsoft Entra ID proporciona mayor seguridad y facilidad de uso con respecto a otras opciones de autorización. Por ejemplo, al usar Microsoft Entra ID, evita tener que almacenar la clave de acceso de la cuenta con el código, como se hace con la autorización de clave compartida. Aunque puede seguir usando la autorización de clave compartida con las aplicaciones de blob y cola, Microsoft recomienda pasar a Microsoft Entra ID siempre que sea posible.

De forma similar, aún puede usar firmas de acceso compartido (SAS) para conceder acceso específico a los recursos en su cuenta de almacenamiento, pero Microsoft Entra ID ofrece capacidades similares sin necesidad de administrar tokens de SAS ni preocuparse sobre cómo revocar una SAS en peligro.

**Administración del ciclo de vida de las claves de acceso de la cuenta de almacenamiento**

Cuando se crea una cuenta de almacenamiento, Azure genera dos claves de acceso de cuenta de almacenamiento de 512 bits para esa cuenta. Estas claves se pueden usar para autorizar el acceso a los datos de su cuenta de almacenamiento mediante la autorización de clave compartida o tokens de SAS firmados con la clave compartida.

Microsoft recomienda usar Azure Key Vault para administrar las claves de acceso, así como rotar y volver a generar las claves de forma periódica. El uso de Azure Key Vault facilita la rotación de las claves sin ocasionar interrupciones en las aplicaciones. También puede rotar las claves de forma manual.

**Protección de las claves de acceso**

Las claves de acceso de la cuenta de almacenamiento proporcionan acceso total a la configuración de una cuenta de almacenamiento, así como a los datos. Siempre debe proteger las claves de acceso. Use Azure Key Vault para administrar y rotar las claves de forma segura. El acceso a la clave compartida concede a un usuario acceso total a la configuración de una cuenta de almacenamiento y sus datos. El acceso a las claves compartidas debe estar cuidadosamente limitado y supervisado. Use tokens de SAS con un ámbito limitado de acceso en escenarios en los que no se puede usar la autorización basada en Microsoft Entra ID. Evite codificar de forma rígida las claves de acceso o guardarlas en cualquier lugar en texto sin formato que sea accesible a otras personas. Rote las claves si cree que se pudieron haber puesto en peligro.

**Visualización de claves de acceso de cuenta**

Puede ver y copiar las claves de acceso a la cuenta con Azure Portal, PowerShell o la CLI de Azure. Azure Portal también proporciona una cadena de conexión para la cuenta de almacenamiento que puede copiar.

Para ver y copiar la cadena de conexión o las claves de acceso de la cuenta de almacenamiento desde Azure Portal:

1. En Azure Portal, vaya a la cuenta de almacenamiento.
2. En Seguridad y redes, seleccione Claves de acceso. Aparecen las claves de acceso de la cuenta, así como la cadena de conexión completa de cada clave.
3. Seleccione Mostrar claves para mostrar las claves de acceso y las cadenas de conexión y habilitar los botones para copiar los valores.
4. En key1, copie el Valor de clave. Seleccione el botón Copiar para copiar la clave de la cuenta.
5. Como alternativa, puede copiar la cadena de conexión completa. En key1, busque el valor Cadena de conexión. Seleccione el botón Copiar para copiar la cadena correspondiente.

Puede utilizar cualquiera de las dos claves para acceder a Azure Storage, pero en general es recomendable usar la primera clave y reservar el uso de la segunda clave para cuando se roten las claves.

Para ver o leer las claves de acceso de una cuenta, el usuario debe ser un administrador de servicios o debe tener asignado un rol de Azure que incluya **Microsoft.Storage/storageAccounts/listkeys/action**. Algunos de los roles integrados de Azure que incluyen esta acción son los de **Propietario**, **Colaborador** y los **Roles de servicio del operador de claves de cuentas de almacenamiento**.

**Uso de Azure Key Vault para administrar las claves de acceso**

Microsoft recomienda usar Azure Key Vault para administrar y rotar las claves de acceso. La aplicación puede acceder de forma segura a las claves en Key Vault, de modo que puede evitar almacenarlas en el código de la aplicación.

**Rotación manual de las claves de acceso**

Microsoft recomienda rotar las claves de acceso periódicamente para ayudar a proteger la cuenta de almacenamiento. De ser posible, use Azure Key Vault para administrar las claves de acceso. Si no está usando Key Vault, deberá rotar las claves manualmente.

Para poder rotar las claves, se asignan dos claves de acceso. De este modo, se garantiza que la aplicación mantiene el acceso a Azure Storage a lo largo del proceso.

Para rotar las claves de acceso a la cuenta de almacenamiento en Azure Portal:

1. Actualice las cadenas de conexión en el código de su aplicación para hacer referencia a la clave de acceso secundaria de la cuenta de almacenamiento.
2. Vaya a la cuenta de almacenamiento en Azure Portal.
3. En **Seguridad y redes**, seleccione **Claves de acceso**.
4. Para regenerar la clave de acceso principal de la cuenta de almacenamiento, seleccione el botón Regenerar que se encuentra junto a la clave de acceso principal.
5. Actualice las cadenas de conexión en su código para hacer referencia a la nueva clave de acceso primaria.
6. Vuelva a generar la clave de acceso secundaria de la misma forma.

Para rotar las claves de acceso de una cuenta, el usuario debe ser un administrador de servicios o debe tener asignado un rol de Azure que incluya **Microsoft.Storage/storageAccounts/regeneratekey/Action**. Algunos de los roles integrados de Azure que incluyen esta acción son los de **Propietario**, **Colaborador** y los **Roles de servicio del operador de claves de cuentas de almacenamiento**.

**Creación de una directiva de expiración de clave**

Una directiva de expiración de claves le permite establecer un aviso para rotar las claves de acceso de la cuenta. El aviso se muestra si ha transcurrido el intervalo especificado y las claves aún no se han rotado. Después de crear una directiva de expiración de clave, puede supervisar el cumplimiento de las cuentas de almacenamiento para asegurarse de que las claves de acceso a la cuenta se rotan periódicamente.

Para crear una directiva de expiración de claves en Azure Portal, haga lo siguiente:

1. En Azure Portal, vaya a la cuenta de almacenamiento.
2. En **Seguridad y redes**, seleccione **Claves de acceso**. Aparecen las claves de acceso de la cuenta, así como la cadena de conexión completa de cada clave.
3. Seleccione el botón **Establecer recordatorio de rotación**. Si el botón **Establecer recordatorio de rotación** está atenuado, tendrá que rotar cada una de las claves. Siga los pasos descritos en Rotación manual de las claves de acceso para rotar las claves.
4. En Establecer un recordatorio para rotar las claves de acceso, active la casilla **Habilitar recordatorios de rotación de claves** y establezca una frecuencia para el recordatorio.
5. Seleccione **Guardar**.

**Comprobación de infracciones de la directiva de expiración de claves**

Puede supervisar sus cuentas de almacenamiento con la directiva de Azure para asegurarse de que las claves de acceso a la cuenta se han rotado dentro del período recomendado. Azure Storage proporciona una directiva integrada para asegurarse de que las claves de acceso a la cuenta de almacenamiento no han expirado.

**Asignación de la directiva integrada para un ámbito de recursos**

Siga estos pasos para asignar la directiva integrada al ámbito adecuado en Azure Portal:

1. En Azure Portal, busque Directiva para mostrar el panel Azure Policy.
2. Seleccione **Asignaciones** en la sección **Creación**.
3. Seleccione **Asignar directiva**.
4. En la pestaña **Conceptos básicos** de la página **Asignar directiva**, en la sección **Ámbito**, especifique el ámbito de la asignación de directivas. Seleccione el botón Más para elegir la suscripción y el grupo de recursos opcional.
5. Para el campo **Definición de directiva**, seleccione el botón **Más** y escriba las *claves de cuenta de almacenamiento* en el campo **Buscar**. Seleccione la definición de directiva denominada **Las claves de la cuenta de almacenamiento no deben haber expirado**.
6. Seleccione **Revisar + crear** para asignar la definición de directiva al ámbito especificado.

**Supervisión del cumplimiento de la directiva de expiración clave**

Para supervisar el cumplimiento de las cuentas de almacenamiento con la directiva de expiración de claves, siga estos pasos:

1. En el panel Azure Policy, busque la definición de directiva integrada para el ámbito especificado en la asignación de directivas. Es posible buscar *Claves de cuenta de almacenamiento; no debería haber expirado* en el cuadro **Buscar** para filtrar la directiva integrada.
2. Seleccione el nombre de la directiva con el ámbito deseado.
3. En la página **Asignación de directivas** de la directiva integrada, seleccione **Ver compatibilidad**. Todas las cuentas de almacenamiento de la suscripción y del grupo de recursos especificados que no cumplen los requisitos de la directiva aparecen en el informe de cumplimiento.

Para que una cuenta de almacenamiento cumpla con los requisitos, rote las claves de acceso de la cuenta.

**Selección y configuración de un método adecuado para acceder a Azure Files**

**Nota**

Azure Storage admite el uso de Microsoft Entra ID para autorizar solicitudes a datos de blobs. Con Microsoft Entra ID, puede usar el control de acceso basado en rol de Azure (Azure RBAC) para conceder permisos a una entidad de seguridad, que puede ser un usuario, un grupo o una entidad de servicio de aplicación. Microsoft Entra ID autentica la entidad de seguridad para devolver un token de OAuth 2.0. Después, el token se puede usar para autorizar una solicitud en Blob service.

La autorización con Microsoft Entra ID proporciona más seguridad y facilidad de uso que la autorización con clave compartida. Microsoft recomienda usar la autorización de Microsoft Entra con las aplicaciones de blobs siempre que sea posible para garantizar el acceso con privilegios mínimos necesarios.

La autorización con credenciales de Microsoft Entra ID está disponible para todas las cuentas de propósito general y de Blob Storage en todas las regiones públicas y nubes nacionales. Solo las cuentas de almacenamiento creadas con el modelo de implementación de Azure Resource Manager admiten la autorización de Microsoft Entra.

Blob Storage también admite la creación de firmas de acceso compartido (SAS) firmadas con credenciales de Microsoft Entra.

**Introducción a Microsoft Entra ID para blobs**

Cuando una entidad de seguridad (un usuario, un grupo o una aplicación) intenta acceder a un recurso de blob, la solicitud debe autorizarse, a menos que sea un blob disponible para acceso anónimo. Con Microsoft Entra ID, el acceso a un recurso es un proceso de dos pasos:

1. En primer lugar, se autentica la identidad de la entidad de seguridad y se devuelve un token de OAuth 2.0.
   * El paso de autenticación exige que una aplicación solicite un token de acceso de OAuth 2.0 en tiempo de ejecución. Si una aplicación se ejecuta desde una entidad de Azure como una máquina virtual de Azure, un conjunto de escalado de máquinas virtuales o una aplicación de Azure Functions, puede usar una identidad administrada para acceder a los datos de blobs.
2. Después, el token se pasa como parte de una solicitud a Blob service y el servicio lo usa para autorizar el acceso al recurso especificado.
   * El paso de la autorización exige que se asignen uno o varios roles Rol RBAC de Azure a la entidad de seguridad que realiza la solicitud.

**Uso de una cuenta de Microsoft Entra con el portal, PowerShell o la CLI de Azure**

Uso de Microsoft Entra ID para autorizar el acceso en el código de la aplicación.

Para autorizar el acceso a Azure Storage con Microsoft Entra ID, puede usar una de las siguientes bibliotecas cliente para adquirir un token de OAuth 2.0:

* La biblioteca cliente de Azure Identity se recomienda para la mayoría de los escenarios de desarrollo.
* La Biblioteca de autenticación de Microsoft (MSAL) puede ser adecuada para determinados escenarios avanzados.

**Biblioteca cliente de Azure Identity**

La biblioteca cliente de Azure Identity simplifica el proceso de obtener un token de acceso de OAuth 2.0 para la autorización con Microsoft Entra ID a través del SDK de Azure. Las versiones más recientes de las bibliotecas cliente de Azure Storage para .NET, Java, Python, JavaScript y Go se integran con las bibliotecas de Azure Identity para dichos lenguajes para proporcionar un medio sencillo y seguro de obtener un token de acceso para la autorización de las solicitudes de Azure Storage.

Una ventaja de la biblioteca cliente de Azure Identity es que permite usar el mismo código para adquirir el token de acceso tanto si la aplicación se ejecuta en el entorno de desarrollo como en Azure. La biblioteca cliente de Azure Identity devuelve un token de acceso para una entidad de seguridad. Cuando el código se ejecuta en Azure, la entidad de seguridad puede ser una identidad administrada para recursos de Azure, una entidad de servicio, un usuario o un grupo. En el entorno de desarrollo, la biblioteca cliente proporciona un token de acceso para un usuario o una entidad de servicio con fines de prueba.

El token de acceso devuelto por la biblioteca cliente de Azure Identity se encapsula en una credencial de token. A continuación, puede usar la credencial de token para obtener un objeto de cliente de servicio que se usará para realizar operaciones autorizadas en Azure Storage. Una manera sencilla de obtener el token de acceso y la credencial de token es usar la clase **DefaultAzureCredential** proporcionada por la biblioteca cliente de Azure Identity. **DefaultAzureCredential** intenta obtener la credencial del token probando secuencialmente varios tipos de credenciales diferentes. **DefaultAzureCredential** funciona tanto en el entorno de desarrollo como en Azure.

**Biblioteca de autenticación de Microsoft (MSAL)**

Aunque Microsoft recomienda usar la biblioteca cliente de Azure Identity siempre que sea posible, podría ser adecuado usar la biblioteca MSAL en determinados escenarios avanzados. Para más información, consulte Más información sobre MSAL.

Cuando se usa MSAL para adquirir un token de OAuth para el acceso a Azure Storage, debe proporcionar un recurso de Microsoft Entra ID. Un identificador de recurso de Microsoft Entra indica el público con el que se puede usar un token emitido para proporcionar acceso a un recurso de Azure. En el caso de Azure Storage, el identificador de recurso puede ser específico de una sola cuenta de almacenamiento o puede aplicarse a cualquiera de ellas.

Cuando se proporciona un identificador de recurso específico de una sola cuenta de almacenamiento y servicio, el identificador de recurso se usa para adquirir un token para autorizar solicitudes a la cuenta y el servicio especificados. En la tabla siguiente se muestra el valor que se usará para el identificador de recurso, en función de la nube con la que esté trabajando. Reemplace <account-name> por el nombre de la cuenta de almacenamiento.

| **Nube** | **Identificador del recurso** |
| --- | --- |
| Azure Global | ejemplo: account-name.blob.core.windows.net |
| Azure Government | ejemplo: account-name.blob.core.usgovcloudapi.net |
| Azure China 21Vianet | ejemplo: account-name.blob.core.chinacloudapi.cn |

También puede proporcionar un id. de recurso que se aplique a cualquier cuenta de almacenamiento, como se muestra en la tabla siguiente. Este id. de recurso es el mismo para todas las nubes públicas y soberanas y se usa para adquirir un token para autorizar las solicitudes a cualquier cuenta de almacenamiento.

| **Nube** | **Identificador del recurso** |
| --- | --- |
| Azure Global Azure Government Azure China 21Vianet | ejemplo: storage.azure.com |

**Asignación de roles de Azure para derechos de acceso**

Microsoft Entra autoriza los derechos de acceso a los recursos protegidos mediante el RBAC de Azure. Azure Storage define un conjunto de roles RBAC integrados que abarcan conjuntos comunes de permisos utilizados para acceder a los datos de blob. También puede definir roles personalizados para el acceso a datos de blobs.

Una entidad de seguridad de Microsoft Entra puede ser un usuario, un grupo, una entidad de servicio de aplicación o una identidad administrada para recursos de Azure. Los roles RBAC que se asignan a una entidad de seguridad determinan los permisos que la entidad de seguridad tiene para el recurso especificado.

En algunos casos, puede que necesite habilitar el acceso específico a los recursos de blob o simplificar los permisos cuando tenga un gran número de asignaciones de roles para un recurso de almacenamiento. Puede usar el control de acceso basado en atributos de Azure (Azure ABAC) para configurar las condiciones de asignación de roles. Puede usar condiciones con un rol personalizado o seleccionar roles integrados.

**Nota**

Al crear una cuenta de Azure Storage, no se le asignan automáticamente permisos para acceder a los datos a través de Microsoft Entra ID. Tiene que asignarse a sí mismo de forma explícita un rol de Azure para acceder a Blob Storage. Puede asignarlo al nivel de su suscripción, grupo de recursos, cuenta de almacenamiento o un contenedor.

**Ámbito de recursos**

Antes de asignar un rol de Azure RBAC a una entidad de seguridad, determine el ámbito de acceso que debería tener la entidad de seguridad. Los procedimientos recomendados dictan que siempre es mejor conceder únicamente el ámbito más restringido posible. Los roles de Azure RBAC definidos en un ámbito más amplio los heredan los recursos que están debajo de ellos.

Puede limitar el acceso a los recursos de blobs de Azure en los niveles siguientes, empezando por el ámbito más reducido:

* **Un contenedor individual.** En este ámbito, una asignación de rol se aplica a todos los blobs del contenedor, y a las propiedades y metadatos del contenedor.
* **La cuenta de almacenamiento.** En este ámbito, una asignación de roles se aplica a todos los contenedores y sus blobs.
* **El grupo de recursos.** En este ámbito, se aplica una asignación de roles a todos los contenedores de todas las cuentas de almacenamiento del grupo de recursos.
* **La suscripción.** En este ámbito, se aplica una asignación de roles a todos los contenedores de todas las cuentas de almacenamiento de todos los grupos de recursos de la suscripción.
* **Un grupo de administración.** En este ámbito, se aplica una asignación de roles a todos los contenedores de todas las cuentas de almacenamiento de todos los grupos de recursos de todas las suscripciones del grupo de administración.

**Roles integrados de Azure para blobs**

Azure RBAC proporciona varios roles integrados para autorizar el acceso a los datos de blobs mediante Microsoft Entra ID y OAuth. Entre los roles que proporcionan permisos a los recursos de datos en Azure Storage están, por ejemplo, los siguientes:

* Propietario de datos de Storage Blob: se usa para establecer la propiedad y administrar el control de acceso POSIX en Azure Data Lake Storage Gen2. Para más información, consulte Control de acceso en Azure Data Lake Storage Gen2.
* Colaborador de datos de Storage Blob: se usa para conceder permisos de lectura, escritura y eliminación a los recursos de almacenamiento de blobs.
* Lector de datos de Storage Blob: se usa para conceder permisos de solo lectura a los recursos de almacenamiento de blobs.
* Delegador de Blob Storage: obtiene una clave de delegación de usuarios que se usa para crear una firma de acceso compartido que se firma con credenciales de Microsoft Entra para un contenedor o un blob.

Solo los roles definidos explícitamente para el acceso a datos permiten a una entidad de seguridad acceder a los datos de blobs. Los roles integrados, como Propietario, Colaborador y Colaborador de la cuenta de almacenamiento, permiten que una entidad de seguridad administre una cuenta de almacenamiento, pero no proporcionan acceso a los datos de blob dentro de esa cuenta a través de Microsoft Entra ID. Sin embargo, si un rol incluye Microsoft.Storage/storageAccounts/listKeys/action, el usuario al que se haya asignado ese rol podrá acceder a los datos de la cuenta de almacenamiento mediante la autorización de clave compartida con las claves de acceso de la cuenta. Para obtener más información, vea Elección de la forma de autorizar el acceso a los datos de blob en Azure Portal.

**Acceso a datos con una cuenta de Microsoft Entra**

El acceso a los datos de blob a través de Azure Portal, PowerShell o la CLI de Azure se puede autorizar mediante la cuenta de Microsoft Entra del usuario o mediante las claves de acceso de la cuenta (autorización de clave compartida).

**Precaución**

No se recomienda la autorización con clave compartida, ya que puede ser menos segura. Para obtener una seguridad óptima, deshabilite la autorización mediante clave compartida para la cuenta de almacenamiento, como se describe en **Impedir la autorización de clave compartida para una cuenta de Azure Storage**.

El uso de claves de acceso y cadenas de conexión debe limitarse a la prueba inicial de aplicaciones de concepto o prototipos de desarrollo que no tienen acceso a datos confidenciales o de producción. De lo contrario, siempre se deben preferir las clases de autenticación basadas en tokens disponibles en el SDK de Azure al autenticarse en los recursos de Azure.

Microsoft recomienda que los clientes usen Microsoft Entra ID o una firma de acceso compartido (SAS) para autorizar el acceso a los datos de Azure Storage.

**Acceso a datos desde Azure Portal**

Azure Portal puede usar su cuenta de Microsoft Entra o las claves de acceso de la cuenta para acceder a datos de blob en una cuenta de Azure Storage. El esquema de autorización que use Azure Portal depende de los roles de Azure que tenga asignados.

Si intenta acceder a datos de blobs, Azure Portal primero comprueba si tiene asignado un rol de Azure con **Microsoft.Storage/storageAccounts/listkeys/action**. Si tiene un rol asignado con esta acción, Azure Portal usa la clave de cuenta para acceder a los datos de blobs mediante la autorización de clave compartida. Si no tiene un rol asignado con esta acción, Azure Portal intenta acceder a los datos mediante la cuenta de Microsoft Entra.

Para acceder a los datos de blob desde Azure Portal mediante su cuenta de Microsoft Entra, necesita permisos para acceder a los datos del blob y también necesita permisos para navegar por los recursos de la cuenta de almacenamiento en Azure Portal. Los roles integrados que proporciona Azure Storage conceden acceso a recursos de blobs, pero no conceden permisos a los recursos de la cuenta de almacenamiento. Por este motivo, el acceso al portal también requiere la asignación de un rol de Azure Resource Manager, como el rol Lector, con ámbito limitado al nivel de la cuenta de almacenamiento o superior. El rol **Lector** concede los permisos más restringidos, pero otro rol de Azure Resource Manager que conceda acceso a los recursos de administración de la cuenta de almacenamiento también es aceptable.

Azure Portal indica qué esquema de autorización se está usando al examinar un contenedor.

**Seleccionar y configurar un método adecuado para acceder a Azure Blob Storage**

Cuando se accede a los datos de archivos mediante Azure Portal, este realiza solicitudes a Azure Files en segundo plano. Estas solicitudes se pueden autorizar mediante la cuenta de Microsoft Entra o la clave de acceso a la cuenta de almacenamiento. El portal indica qué método está usando, y le permite alternar entre ambos si tiene los permisos adecuados.

También puede especificar cómo autorizar una operación de recurso compartido de archivos individual en Azure Portal. De forma predeterminada, el portal usa el método que ya esté usando para autorizar todos los recursos compartidos de archivos, pero tiene la opción de cambiar esta configuración para recursos compartidos de archivos individuales.

**Permisos necesarios para acceder a datos de archivos**

Necesitará permisos específicos según cómo quiera autorizar el acceso a los datos de archivos en Azure Portal. En la mayoría de los casos, estos permisos se proporcionan a través del control de acceso basado en roles de Azure (Azure RBAC).

**Uso de la cuenta de Microsoft Entra**

Para acceder a datos de archivos desde Azure Portal con la cuenta de Microsoft Entra, se deben cumplir estas dos premisas:

* Tiene asignado un rol (ya sea integrado o personalizado) que proporciona acceso a los datos de archivos.
* Tiene asignado como mínimo el rol Lector de Azure Resource Manager, con el ámbito establecido en el nivel de la cuenta de almacenamiento o en un nivel superior. El rol Lector concede los permisos más restringidos, pero otro rol de Azure Resource Manager que conceda acceso a los recursos de administración de la cuenta de almacenamiento también es aceptable.

El rol Lector de Azure Resource Manager permite a los usuarios ver recursos de la cuenta de almacenamiento, pero no modificarlos. No proporciona permisos de lectura en los datos de Azure Storage, sino únicamente en los recursos de administración de la cuenta. El rol Lector es necesario para que los usuarios puedan navegar a recursos compartido de archivos en Azure Portal.

Hay dos nuevos roles integrados que tienen los permisos necesarios para acceder a los datos de archivo con OAuth:

* Lector con privilegios de datos de archivos de Storage
* Colaborador con privilegios de datos de archivos de Storage

El rol **Colaborador con privilegios de datos de archivos de almacenamiento** tiene permisos para leer, escribir, eliminar y modificar permisos ACL/NTFS en archivos o directorios de recursos compartidos de archivos de Azure. No se admite la modificación de ACL o permisos NTFS a través de Azure Portal.

Los roles personalizados pueden admitir diferentes combinaciones de los mismos permisos que proporcionan los roles integrados.

**Uso de la clave de acceso de la cuenta de almacenamiento**

Para acceder a los datos de archivos con la clave de acceso a la cuenta, debe tener asignado un rol de Azure que incluya la acción de Azure RBAC **Microsoft.Storage/storageAccounts/listkeys/action**. Este rol de Azure puede ser un rol integrado o personalizado. Los roles integrados que **Microsoft.Storage/storageAccounts/listkeys/action** admite son los siguientes, presentados en orden de permisos mínimos a máximos:

* Rol Lector y acceso a los datos
* El rol Colaborador de una cuenta de almacenamiento
* El rol Colaborador de Azure Resource Manager
* El rol Propietario de Azure Resource Manager

Al intentar acceder a los datos de archivos en Azure Portal, este comprueba primero si tiene asignado un rol con **Microsoft.Storage/storageAccounts/listkeys/action**. Si se le ha asignado un rol con esta acción, Azure Portal usa la clave de cuenta de almacenamiento para tener acceso a los datos de archivos. Si no tiene un rol asignado con esta acción, el portal intenta acceder a los datos mediante la cuenta de Microsoft Entra.

Cuando una cuenta de almacenamiento está bloqueada con un bloqueo **ReadOnly** de Azure Resource Manager, no se permite la operación **Crear lista de claves** para esa cuenta de almacenamiento. **Crear lista de claves** es una operación POST y todas las operaciones POST se impiden cuando se configura un bloqueo **ReadOnly** para la cuenta. Por esta razón, cuando la cuenta está bloqueada con un bloqueo **ReadOnly**, los usuarios deben usar las credenciales de Microsoft Entra para acceder a los datos de archivo en el portal.

Los roles clásicos de administrador de suscripciones **Administrador de servicios** y **Coadministrador** equivalen al rol Propietario de Azure Resource Manager. El rol Propietario engloba todas las acciones, incluyendo **Microsoft.Storage/storageAccounts/listkeys/action**, por lo que un usuario con uno de estos roles administrativos también puede acceder a datos de archivos con la clave de cuenta de almacenamiento.

**Especificar cómo autorizar operaciones en un recurso compartido de archivos específico**

Puede cambiar el método de autenticación para recursos compartidos de archivos individuales. De manera predeterminada, el portal usar el método de autenticación actual. Para determinar el método de autenticación actual, siga estos pasos.

1. Vaya a la cuenta de almacenamiento en Azure Portal y seleccione **Almacenamiento de datos**>**Recursos compartidos de archivos** en el panel de navegación izquierdo.
2. Seleccione un recurso compartido de archivos.
3. Haga clic en **Examinar**.
4. El método de autenticación indica si actualmente usa la clave de acceso a la cuenta de almacenamiento o la cuenta de Microsoft Entra para autenticar y autorizar las operaciones del recurso compartido de archivos. Si actualmente se autentica mediante la clave de acceso a la cuenta de almacenamiento, verá **Clave de acceso** especificado como método de autenticación, tal como en la siguiente imagen. Si se autentica mediante la cuenta de Microsoft Entra, verá **Cuenta de usuario de Microsoft Entra** especificado en su lugar.

**Autentíquese con su cuenta de Microsoft Entra.**

Para cambiar mediante la cuenta de Microsoft Entra, seleccione el vínculo resaltado en la imagen que indica Cambiar a la cuenta de usuario de Microsoft Entra. Si posee los permisos adecuados a través de los roles de Azure que tiene asignados, podrá continuar. Sin embargo, si carece de los permisos necesarios, verá un mensaje de error que indica que no tiene permisos para crear una lista de los datos mediante la cuenta de usuario con Microsoft Entra ID.

Se requieren dos permisos de RBAC adicionales para usar la cuenta de Microsoft Entra:

* Microsoft.Storage/storageAccounts/fileServices/readFileBackupSemantics/action
* Microsoft.Storage/storageAccounts/fileServices/writeFileBackupSemantics/action

La lista no contendrá ningún recurso compartido de archivos si su cuenta de Microsoft Entra no tiene permisos para verlos.

**Autenticación con la clave de acceso de la cuenta de almacenamiento**

Para cambiar al uso de la clave de acceso de la cuenta, seleccione el vínculo que indica Cambiar a la clave de acceso. Si tiene acceso a la clave de cuenta de almacenamiento, podrá continuar. Sin embargo, si no tiene acceso a la clave de cuenta, verá un mensaje de error que indica que no tiene permisos para usar la clave de acceso para crear una lista de los datos.

No aparecen recursos compartidos de archivos en la lista si no tiene acceso a la clave de acceso de la cuenta de almacenamiento.

**El valor predeterminado es la autorización de Microsoft Entra en Azure Portal**

Al crear una cuenta de almacenamiento, puede especificar que Azure Portal realice la autorización con Microsoft Entra ID de forma predeterminada cuando un usuario vaya a los datos de archivos. También puede configurar esta opción para una cuenta de almacenamiento existente. Esta configuración especifica solo el método de autorización predeterminado. Tenga en cuenta que un usuario puede invalidar esta configuración y elegir autorizar el acceso a datos con la clave de la cuenta de almacenamiento.

Para especificar que el portal usará la autorización con Microsoft Entra de forma predeterminada para el acceso a datos al crear una cuenta de almacenamiento, siga estos pasos:

1. Cree una cuenta de almacenamiento; siga las instrucciones de Creación de una cuenta de almacenamiento.
2. En la pestaña **Opciones avanzadas**, en la sección **Seguridad**, seleccione la casilla situada junto a **Autorización predeterminada con Azure Active Directory en Azure Portal**.
3. Seleccione **Revisar y crear** para ejecutar la validación y crear la cuenta de almacenamiento.

Para actualizar esta configuración para una cuenta de almacenamiento existente, siga estos pasos:

1. Vaya a la información general de la cuenta de almacenamiento en Azure Portal.
2. En **Configuración**, seleccione **Configuración**.
3. Establezca **Valor predeterminado para la autorización de Microsoft Entra** en **Azure Portal** en **Habilitado**.

**Selección y configuración de un método adecuado para acceder a Azure Tables**

Azure Storage admite el uso de Microsoft Entra ID para autorizar solicitudes a datos de tabla. Con Microsoft Entra ID, puede usar el control de acceso basado en rol de Azure (RBAC de Azure) para conceder permisos a una entidad de seguridad, que puede ser un usuario o una entidad de servicio de aplicación. La entidad de seguridad principal es autenticada por Microsoft Entra ID para devolver un token OAuth 2.0. Después, el token se puede usar para autorizar una solicitud en Table service.

La autorización de solicitudes contra Azure Storage con Microsoft Entra ID proporciona mayor seguridad y facilidad de uso que la autorización de clave compartida. Microsoft recomienda utilizar la autorización Microsoft Entra con sus aplicaciones de tabla siempre que sea posible para garantizar el acceso con los privilegios mínimos requeridos.

La autorización con Microsoft Entra ID está disponible para todos los usos generales en todas las regiones públicas y nubes nacionales. Solo las cuentas de almacenamiento creadas con el modelo de implementación de Azure Resource Manager admiten la autorización de Microsoft Entra.

**Información general de Microsoft Entra ID para tablas**

Cuando una entidad de seguridad (un usuario, un grupo o una aplicación) intenta acceder a un recurso de tabla, la solicitud debe estar autorizada. Con Microsoft Entra ID, el acceso a un recurso es un proceso de dos pasos. En primer lugar, se autentica la identidad de la entidad de seguridad y se devuelve un token de OAuth 2.0. Después, el token se pasa como parte de una solicitud a Table service y el servicio lo usa para autorizar el acceso al recurso especificado.

El paso de autenticación exige que una aplicación solicite un token de acceso de OAuth 2.0 en tiempo de ejecución. Si una aplicación se ejecuta desde una entidad de Azure como una máquina virtual de Azure, un conjunto de escalado de máquinas virtuales o una aplicación de Azure Functions, puede usar una identidad administrada para el acceso a las tablas.

El paso de autorización exige que se asignen uno o varios roles de Azure a la entidad de seguridad. Azure Storage proporciona roles de Azure que abarcan conjuntos comunes de permisos para datos de tablas. Los roles que se asignan a una entidad de seguridad determinan los permisos que tiene esa entidad de seguridad.

**Asignación de roles de Azure para derechos de acceso**

Microsoft Entra autoriza los derechos de acceso a recursos protegidos mediante el control de acceso basado en roles de Azure (Azure RBAC). Azure Storage define un conjunto de roles integrados de Azure que abarcan conjuntos comunes de permisos utilizados para acceder a los datos de tablas. También puede definir roles personalizados para el acceso a datos de tablas.

Cuando un rol de Azure se asigna a una entidad de seguridad de Microsoft Entra, Azure concede a esa entidad de seguridad acceso a los recursos. Una entidad de seguridad Microsoft Entra puede ser un usuario, un grupo, una entidad de seguridad de servicio de aplicación o unaidentidad administrada para recursos de Azure.

**Ámbito de recursos**

Antes de asignar un rol de Azure RBAC a una entidad de seguridad, determine el ámbito de acceso que debería tener la entidad de seguridad. Los procedimientos recomendados dictan que siempre es mejor conceder únicamente el ámbito más restringido posible. Los roles de Azure RBAC definidos en un ámbito más amplio los heredan los recursos que están debajo de ellos.

Puede limitar el acceso a los recursos de tabla de Azure en los niveles siguientes, empezando por el ámbito más reducido:

* **Una tabla individual**. En este ámbito, se aplica una asignación de roles a la tabla especificada.
* **La cuenta de almacenamiento.** En este ámbito, se aplica una asignación de roles a todas las tablas de la cuenta.
* **El grupo de recursos.** En este ámbito, se aplica una asignación de roles a todas las tablas de todas las cuentas de almacenamiento del grupo de recursos.
* **La suscripción.** En este ámbito, se aplica una asignación de roles a todas las tablas de todas las cuentas de almacenamiento de todos los grupos de recursos de la suscripción.
* **Un grupo de administración.** En este ámbito, se aplica una asignación de roles a todas las tablas de todas las cuentas de almacenamiento de todos los grupos de recursos de todas las suscripciones del grupo de administración.

**Roles integrados de Azure para tablas**

Azure RBAC proporciona roles integrados para autorizar el acceso a datos de tabla con Microsoft Entra ID y OAuth. Entre los roles integrados que proporcionan permisos a las tablas en Azure Storage están, por ejemplo, los siguientes:

* Colaborador de datos de tabla de Storage: se usa para conceder permisos de lectura, escritura y eliminación a los recursos de Table Storage.
* Lector de datos de tabla de Storage: se usa para conceder permisos de solo lectura a los recursos de Table Storage.

Solo los roles definidos explícitamente para el acceso a datos permiten a una entidad de seguridad acceder a los datos de tablas. Los roles integrados, como **Propietario**, **Colaborador** y **Colaborador de la cuenta de almacenamiento**, permiten que una entidad de seguridad administre una cuenta de almacenamiento, pero no proporcionan acceso a los datos de tablas dentro de esa cuenta a través de Microsoft Entra ID. Sin embargo, si un rol incluye **Microsoft.Storage/storageAccounts/listKeys/action**, el usuario al que se haya asignado ese rol podrá acceder a los datos de la cuenta de almacenamiento mediante la autorización de clave compartida con las claves de acceso de la cuenta.

Las asignaciones de roles de Azure pueden tardar hasta 30 minutos en propagarse.

**Seleccionar y configurar un método adecuado para acceder a Azure Queues**

Cuando se accede a los datos de cola desde Azure Portal, este realiza ciertas solicitudes a Azure Storage en segundo plano. Una solicitud a Azure Storage se puede autorizar mediante la cuenta de Microsoft Entra o la clave de acceso a la cuenta de almacenamiento. El portal indica qué método está usando, y le permite alternar entre ambos si tiene los permisos adecuados.

**Permisos necesarios para acceder a datos de cola**

Necesitará permisos específicos según cómo quiera autorizar el acceso a los datos de cola en Azure Portal. En la mayoría de los casos, estos permisos se proporcionan a través del control de acceso basado en rol de Azure (Azure RBAC).

**Uso de la clave de acceso de la cuenta**

Para acceder a los datos de cola con la clave de acceso a la cuenta, debe tener asignado un rol de Azure que incluya la acción de Azure RBAC Microsoft.Storage/storageAccounts/listkeys/action. Este rol de Azure puede ser un rol integrado o personalizado. Los roles integrados que Microsoft.Storage/storageAccounts/listkeys/action admite son los siguientes, en orden de permisos mínimos a máximos:

* Rol Lector y acceso a los datos
* El rol Colaborador de una cuenta de almacenamiento
* El rol Colaborador de Azure Resource Manager
* El rol Propietario de Azure Resource Manager

Cuando intentó acceder a los datos de cola en Azure Portal, este comprueba primero si tiene asignado un rol con Microsoft.Storage/storageAccounts/listkeys/action. Si se le ha asignado un rol con esta acción, Azure Portal usa la clave de cuenta para tener acceso a los datos de cola. Si no tiene un rol asignado con esta acción, el portal intenta acceder a los datos mediante la cuenta de Microsoft Entra.

**Uso de la cuenta de Microsoft Entra**

Para acceder a datos de colas desde Azure Portal con la cuenta de Microsoft Entra, se deben cumplir estas dos premisas:

* Tiene asignado un rol (ya sea integrado o personalizado) que proporciona acceso a los datos de cola.
* Tiene asignado como mínimo el rol Lector de Azure Resource Manager, con el ámbito establecido en el nivel de la cuenta de almacenamiento o en un nivel superior. El rol Lector concede los permisos más restringidos, pero otro rol de Azure Resource Manager que conceda acceso a los recursos de administración de la cuenta de almacenamiento también es aceptable.

El rol Lector de Azure Resource Manager permite a los usuarios ver recursos de la cuenta de almacenamiento, pero no modificarlos. No proporciona permisos de lectura en los datos de Azure Storage, sino únicamente en los recursos de administración de la cuenta. El rol Lector es necesario para que los usuarios puedan navegar a colas en Azure Portal.

Los roles personalizados pueden admitir diferentes combinaciones de los mismos permisos que proporcionan los roles integrados.

**Desplazamiento a colas en Azure Portal**

Para ver datos de cola en Azure Portal, vaya a la sección Información general de la cuenta de almacenamiento y haga clic en los vínculos de Colas. También puede navegar a la sección Queue service del menú.

**Determinar el método de autenticación actual**

Al ir a una cola, Azure Portal indica si lo que se usa actualmente para autenticarse es la clave de acceso de la cuenta o la cuenta de Microsoft Entra.

**Autenticación con la clave de acceso de la cuenta**

Si se autentica mediante la clave de acceso a la cuenta, verá Clave de acceso especificado como método de autenticación en Azure Portal.

Para cambiar y usar la cuenta de Microsoft Entra, haga clic en el vínculo que aparece resaltado en la imagen. Si posee los permisos adecuados a través de los roles de Azure que tiene asignados, podrá continuar. Pero, si no los tiene, verá un mensaje de error como el siguiente:

Tenga en cuenta que la lista no contendrá ninguna cola si su cuenta de Microsoft Entra ID no tiene permisos para verlas. Haga clic en el vínculo Cambiar a la clave de acceso para usar la clave de acceso para intentar autenticarse de nuevo.

**Autenticación con la cuenta de Microsoft Entra ID**

Si se autentica utilizando la cuenta de Microsoft Entra ID, verá Cuenta de usuario de Microsoft Entra ID especificado como método de autenticación en Portal.

El valor predeterminado de la autorización de Microsoft Entra ID en Azure Portal

Al crear una cuenta de almacenamiento, puede especificar que Azure Portal realice la autorización con Microsoft Entra ID de manera predeterminada cuando un usuario vaya a los datos de colas. También puede configurar esta opción para una cuenta de almacenamiento existente. Esta configuración especifica solo el método de autorización predeterminado, por lo que debe tener en cuenta que un usuario puede invalidar esta configuración y elegir autorizar el acceso a datos con la clave de la cuenta.

Para especificar que el portal usará la autorización de Microsoft Entra ID de forma predeterminada para el acceso a datos al crear una cuenta de almacenamiento, siga estos pasos:

1. Cree una cuenta de almacenamiento; siga las instrucciones de Creación de una cuenta de almacenamiento.
2. En la pestaña Opciones avanzadas, en la sección Seguridad, active la casilla situada junto a Predeterminada para la autorización de Microsoft Entra ID en Azure Portal.
3. Seleccione el botón Revisar y crear para ejecutar la validación y crear la cuenta.

Para actualizar esta configuración para una cuenta de almacenamiento existente, siga estos pasos:

1. Vaya a la información general de su cuenta en Azure Portal.
2. En Configuración, seleccione Configuración.
3. Establezca Default (Predeterminado) en Autorización de Microsoft Entra en Azure Portal en Habilitado.

**Seleccionar y configurar los métodos adecuados para proteger de amenazas de seguridad de datos, incluidas las eliminaciones temporales, las copias de seguridad, el control de versiones y el almacenamiento inmutable**

Azure Storage proporciona protección de datos para Blob Storage y Azure Data Lake Storage Gen2 que le ayudarán a prepararse para escenarios en los que necesite recuperar datos que se han eliminado o sobrescrito. Es importante pensar en la mejor manera de proteger los datos antes de que se produzca un incidente que podría ponerlos en peligro.

**Recomendaciones para la protección de datos básica**

Si está buscando cobertura básica de protección de datos para su cuenta de almacenamiento y los datos que contiene, Microsoft recomienda realizar los siguientes pasos para comenzar:

* Configure un bloqueo de Azure Resource Manager en la cuenta de almacenamiento para protegerla de la eliminación o de los cambios de configuración.
* Habilite la eliminación temporal de contenedores para la cuenta de almacenamiento con el fin de recuperar un contenedor eliminado y su contenido.
* Guarde el estado de un blob a intervalos regulares:
  + En el caso de las cargas de trabajo de Blob Storage, habilite el control de versiones de blobs para guardar automáticamente el estado de los datos cada vez que se sobrescriba un blob.
  + En el caso de las cargas de trabajo de Azure Data Lake Storage, realice instantáneas manuales para guardar el estado de los datos en un momento determinado.

**Introducción a las opciones de protección de datos**

En la tabla siguiente se resumen las opciones disponibles en Azure Storage para los escenarios comunes de protección de datos. Elija los escenarios correspondientes a su situación para obtener más información sobre las opciones disponibles. No todas las características están disponibles en este momento para las cuentas de almacenamiento que tienen habilitado un espacio de nombres jerárquico.

| **Escenario** | **Opción de protección de datos** | **Recomendaciones** | **Ventaja de protección** | **Disponible para Data Lake Storage** |
| --- | --- | --- | --- | --- |
| Evitar que se elimine o modifique una cuenta de almacenamiento. | Bloqueo de Azure Resource Manager | Bloquee todas las cuentas de almacenamiento con un bloqueo de Azure Resource Manager a fin de impedir su eliminación. | Protege la cuenta de almacenamiento contra la eliminación o los cambios de configuración.  No protege los contenedores o blobs de la cuenta contra la eliminación o sobrescritura. | Sí |
| Impedir que una versión de blob se elimine durante un intervalo determinado por el usuario. | Directiva de inmutabilidad de una versión de blob | Establezca una directiva de inmutabilidad en una versión de blob individual para proteger documentos críticos para la empresa; por ejemplo, con el fin de cumplir los requisitos de cumplimiento normativo o legal. | Protege una versión de blob frente a la eliminación y frente a la sobrescritura de sus metadatos. Una operación de sobrescritura crea una nueva versión.  Si al menos un contenedor tiene habilitada la inmutabilidad a nivel de versión, la cuenta de almacenamiento también está protegida contra la eliminación. Se produce un error en la eliminación del contenedor si existe al menos un blob en el contenedor. | No |
| Impedir que un contenedor y sus blobs se eliminen o modifiquen durante un intervalo determinado por el usuario. | Directiva de inmutabilidad de un contenedor | Establezca una directiva de inmutabilidad en un contenedor para proteger documentos críticos para la empresa; por ejemplo, con el fin de cumplir los requisitos de cumplimiento normativo o legal. | Protege un contenedor y sus blobs de cualquier eliminación y sobrescritura.  Cuando está vigente una suspensión legal o una directiva de retención de duración limitada bloqueada, la cuenta de almacenamiento también está protegida contra la eliminación. Los contenedores para los que no se ha establecido ninguna directiva de inmutabilidad no están protegidos contra la eliminación. | Sí |
| Restaurar un contenedor eliminado en un intervalo específico. | Eliminación temporal de contenedores | Habilite la eliminación temporal de contenedores para todas las cuentas de almacenamiento, con un intervalo de retención mínimo de siete días.  Habilite el control de versiones de blobs y la eliminación temporal de blobs junto con la eliminación temporal de contenedores para proteger blobs concretos de un contenedor.  Almacene contenedores que requieran diferentes períodos de retención en cuentas de almacenamiento independientes. | Se puede restaurar un contenedor eliminado y su contenido dentro del período de retención.  Solo se pueden restaurar las operaciones de nivel de contenedor (por ejemplo, Eliminar contenedor). La eliminación temporal de contenedores no permite restaurar un blob individual en el contenedor si dicho blob se eliminó. | Sí |
| Guardar automáticamente el estado de un blob en una versión anterior cuando se sobrescribe. | Control de versiones de blobs | Habilite el control de versiones de blobs, junto con la eliminación temporal de contenedores y la eliminación temporal de blobs, para las cuentas de almacenamiento en las que necesita protección óptima para los datos de blobs.  Almacene datos de blobs que no requieran el control de versiones en una cuenta independiente para limitar los costos. | Cada operación de escritura de blobs crea una versión. La versión actual de un blob se puede restaurar a partir de una versión anterior si se elimina o sobrescribe la versión actual. | No |
| Restaurar una versión de blob o un blob eliminado en un intervalo especificado. | Eliminación temporal de blobs | Habilite la eliminación temporal de blobs para todas las cuentas de almacenamiento, con un intervalo de retención mínimo de siete días.  Habilite el control de versiones de blobs y la eliminación temporal de contenedores junto con la eliminación temporal de blobs para una protección óptima de los datos del blob.  Almacene blobs que requieran diferentes períodos de retención en cuentas de almacenamiento independientes. | Se puede restaurar una versión de blob o un blob eliminado en el período de retención. | Sí |
| Restaurar un conjunto de blobs en bloques a un momento dado anterior. | Restauración a un momento dado | Si quiere restaurar a un momento dado para revertir a un estado anterior, diseñe la aplicación a fin de que elimine los blobs en bloques individuales en lugar de eliminar los contenedores. | Un conjunto de blobs en bloques se puede revertir al estado que tenía en un punto concreto del pasado.  Solo se revierten las operaciones realizadas en los blobs en bloques. No se revierten las operaciones realizadas en contenedores, blobs en páginas o blobs en anexos. | No |
| Guardar manualmente el estado de un blob en un momento dado. | Instantánea de blob | Se recomienda como alternativa al control de versiones de blobs cuando el control de versiones no es adecuado para su escenario debido a los costos u otras consideraciones, o cuando la cuenta de almacenamiento tiene habilitado un espacio de nombres jerárquico. | Un blob se puede restaurar a partir de una instantánea si se sobrescribe el blob. Si se elimina el blob, también se eliminan las instantáneas. | Sí, en versión preliminar |
| Un blob se puede eliminar o sobrescribir, pero los datos se copian periódicamente en una segunda cuenta de almacenamiento. | Implemente su propia solución para copiar datos a una segunda cuenta mediante la replicación de objetos de Azure Storage o una herramienta, como AzCopy o Azure Data Factory. | Recomendado para una protección óptima contra acciones intencionadas inesperadas o escenarios impredecibles.  Cree la segunda cuenta de almacenamiento en la misma región que la cuenta principal para evitar la generación de cargos de salida. | Los datos se pueden restaurar a partir de la segunda cuenta de almacenamiento si la cuenta principal se ve comprometida de alguna manera. | Se admiten AzCopy y Azure Data Factory.  No se admite la replicación de objetos. |

**Protección de datos por tipo de recurso**

En la tabla siguiente se resumen las opciones de protección de datos de Azure Storage según los recursos protegidos.

| **Opción de protección de datos** | **Protege una cuenta frente a la eliminación** | **Protege un contenedor frente a la eliminación** | **Protege un objeto frente a la eliminación** | **Protege un objeto frente a la sobrescrituras** |
| --- | --- | --- | --- | --- |
| Bloqueo de Azure Resource Manager | Sí | No | N.º | No |
| Directiva de inmutabilidad de una versión de blob | Sí | Sí | Sí | Sí |
| Directiva de inmutabilidad de un contenedor | Sí | Sí | Sí | Sí |
| Eliminación temporal de contenedores | No | Sí | No | No |
| Control de versiones de blobs | No | No | Sí | Sí |
| Eliminación temporal de blobs | No | No | Sí | Sí |
| Restauración a un momento dado | No | No | Sí | Sí |
| Instantánea de blob | No | N.º | No | Sí |
| Implementación de una solución propia para copiar datos en una segunda cuenta | No | Sí | Sí | Sí |

* Un bloqueo de Azure Resource Manager no protege un contenedor frente a la eliminación.
* Se produce un error en la eliminación de la cuenta de almacenamiento si hay al menos un contenedor que tenga habilitado el almacenamiento inmutable a nivel de versión.
* Se produce un error en la eliminación del contenedor si existe al menos un blob en el contenedor, independientemente de si la directiva está bloqueada o desbloqueada.
* Sobrescribir el contenido de la versión actual del blob crea una nueva versión. Una directiva de inmutabilidad protege los metadatos de una versión frente a la sobrescritura.
* Mientras esté en vigor una retención legal o una directiva de retención de duración definida bloqueada en el ámbito del contenedor, la cuenta de almacenamiento también estará protegida contra la eliminación.
* Actualmente no es compatible con cargas de trabajo de Data Lake Storage.
* AzCopy y Azure Data Factory son opciones compatibles con cargas de trabajo de Blob Storage y Data Lake Storage. La replicación de objetos solo se admite para las cargas de trabajo de Blob Storage.

**Recuperación de datos eliminados o sobrescritos**

Si necesita recuperar los datos que se han sobrescrito o eliminado, la forma de proceder dependerá de las opciones de protección de datos que haya habilitado y de los recursos afectados. En la tabla siguiente se describen las acciones que puede realizar para recuperar los datos.

| **Recurso eliminado o sobrescrito** | **Posibles acciones de recuperación** | **Requisitos para la recuperación** |
| --- | --- | --- |
| Cuenta de almacenamiento | Tratar de recuperar la cuenta de almacenamiento eliminada. | La cuenta de almacenamiento se creó originalmente con el modelo de implementación de Azure Resource Manager y se eliminó en los últimos 14 días. No se ha creado una cuenta de almacenamiento con el mismo nombre desde que se eliminó la cuenta original. |
| Contenedor | Recuperar el contenedor eliminado temporalmente y su contenido. | La eliminación temporal del contenedor está habilitada y el período de retención de la eliminación temporal del contenedor todavía no ha expirado. |
| Contenedores y blobs | Restaurar datos a partir de una segunda cuenta de almacenamiento. | Todas las operaciones de contenedores y blobs se han replicado eficazmente en una segunda cuenta de almacenamiento. |
| Blob (cualquier tipo) | Restauración de un blob a partir de una versión anterior | El control de versiones de blobs está habilitado y el blob tiene una o más versiones anteriores. |
| Blob (cualquier tipo) | Recuperar un blob eliminado temporalmente | La eliminación temporal de blobs está habilitada y el intervalo de retención de la eliminación temporal no ha expirado. |
| Blob (cualquier tipo) | Restaurar un blob a partir de una instantánea | El blob tiene una o varias instantáneas. |
| Conjunto de blobs en bloques | Recuperación de un conjunto de blobs en bloques en su estado en un momento dado anterior | La restauración a un momento dado está habilitada y el punto de restauración se encuentra en el intervalo de retención. La cuenta de almacenamiento no se ha puesto en peligro ni está dañada. |
| Versión de un blob | Recuperación de una versión eliminada temporalmente | La eliminación temporal de blobs está habilitada |

**Recuperación ante desastres**

Azure Storage siempre mantiene varias copias de los datos, con el fin de protegerlos de eventos planeados y no planeados, como errores transitorios del hardware, interrupciones del suministro eléctrico o cortes de la red, y desastres naturales masivos. La redundancia garantiza que la cuenta de almacenamiento cumple sus objetivos de disponibilidad y durabilidad, aunque se produzcan errores.

Si se produce un error en un centro de datos, si la cuenta de almacenamiento es redundante en dos regiones geográficas (con redundancia geográfica), tendrá la opción de conmutar por error la cuenta de la región primaria a la secundaria.

La conmutación por error administrada por el cliente no se admite actualmente para las cuentas de almacenamiento con un espacio de nombres jerárquico habilitado.

**Configurar Bring your own key (BYOK)**

**Escenario**

Un cliente de Key Vault desea transferir de forma segura una clave desde su módulo de seguridad de hardware (HSM) local fuera de Azure, en el HSM que respalda Azure Key Vault. El proceso de importación de una clave generada fuera de Key Vault se conoce como Bring Your Own Key (BYOK).

A continuación se indican los requisitos:

* La clave que se va a transferir nunca existe fuera de un HSM en formato de texto sin formato.
* Fuera de un HSM, la clave que se va a transferir siempre está protegida por una clave contenida en el HSM de Azure Key Vault.

**Terminología**

| **Nombre de clave** | **Tipo de clave** | **Origen** | **Descripción** |
| --- | --- | --- | --- |
| Clave de intercambio de claves (KEK) | RSA | HSM de Azure Key Vault | Un par de claves RSA respaldadas por HSM generado en Azure Key Vault. |
| Clave de encapsulado | AES | HSM del proveedor | Una clave AES [**efímera**] generada por HSM local |
| Clave de destino | RSA, EC, AES (solo HSM administrado) | HSM del proveedor | La clave que se va a transferir al HSM de Azure Key Vault. |

**Clave de intercambio de claves**: Una clave respaldada por HSM que el cliente genera en el almacén de claves donde se importará la clave BYOK. Esta KEK debe tener las siguientes propiedades:

* Es una clave RSA-HSM (4096, 3072 o 2048 bits).
* Tendrá el parámetro key\_ops fijo (solo ‘import’), que permitirá su uso solo durante BYOK.
* Debe estar en el mismo almacén donde se va a importar la clave de destino.

**Pasos de usuario**

Para realizar una transferencia de claves, un usuario debe realizar los pasos siguientes:

1. Generar la KEK.
2. Recuperar la clave pública de la KEK.
3. Usar la herramienta BYOK suministrada por el proveedor de HSM para importar la KEK en el HSM de destino y exportar la clave de destino protegida por la KEK.
4. Importar la clave de destino protegida en Azure Key Vault.

Los clientes utilizan la herramienta BYOK y la documentación suministrada por el proveedor de HSM para completar el paso 3. Genera un Blob de transferencia de claves (un archivo ".byok").

**Restricciones de HSM**

Los módulos HSM existentes pueden aplicar restricciones en la clave que administran, entre las que se incluyen:

* Es posible que sea necesario configurar el módulo HSM para permitir la exportación basada en el encapsulado de claves.
* Es posible que sea necesario marcar la clave de destino **atributo Cryptoki (CKA)**\_EXTRACTABLE para que el HSM permita la exportación controlada
* En algunos casos, es posible que la KEK y la clave de ajuste deban marcarse como CKA\_TRUSTED, lo que permite que se use para encapsular las claves en HSM.

Por lo general, la configuración del HSM de origen está fuera del ámbito de esta especificación. Microsoft espera que el proveedor de HSM genere la documentación que acompaña a la herramienta BYOK de modo que incluya estos pasos de configuración.

**Nota**

Se pueden realizar varios de estos pasos mediante otras interfaces, como Azure PowerShell y Azure Portal. También se pueden realizar mediante programación con funciones equivalentes en Key Vault SDK.

**Generar la KEK**

Use el comando az keyvault key create para crear KEK con las operaciones de clave establecidas para importar.

**Nota**

Los servicios admiten diferentes longitudes de KEK. Azure SQL, por ejemplo, solo admite longitudes de clave de 2048 o 3072 bytes.

**Recuperar la clave pública de la KEK.**

Descargar la parte de la clave pública de la KEK y guardarla en un archivo PEM.

**Generar el blob de transferencia de claves con la herramienta de BYOK suministrada por el proveedor de HSM.**

El cliente usa la herramienta BYOK suministrada por el proveedor de HSM para crear un blob de transferencia de claves (almacenado como un archivo ".byok"). Clave pública KEK como un **.Privacy-Enhanced Mail** (archivo.pem) será una de las entradas de esta herramienta.

**Blob de transferencia de claves**

A largo plazo, Microsoft quiere usar **estándares de criptografía de clave pública** (PKCS) #11 **Mecanismo de atributo Cryptoki** (CKM)\_**Rivest–Shamir-Adleman** (RSA)\_**Estándar de cifrado avanzado (AES)**\_**Key Exchange Key** (KEY)\_WRAP mecanismo para transferir la clave de destino a Azure Key Vault, ya que este mecanismo genera un único blob y, lo que es más importante, la clave AES intermedia se controla mediante los dos HSM y se garantiza que es efímera. Este mecanismo no está disponible actualmente en algunos HSM, pero la combinación de proteger la clave de destino con CKM\_AES\_KEY\_WRAP\_PAD mediante una clave AES y proteger la clave AES con CKM\_RSA\_PKCS\_**relleno óptimo de cifrado asimétrico** (OAEP) genera un blob equivalente.

El texto no cifrado de la clave de destino depende del tipo de clave:

* Para una clave RSA, la codificación **notación de sintaxis abstracta** (ASN.1) **DistinguishedEncoding Rules** (DER) de clave privada Request for Comments [RFC3447] encapsulada en PKCS#8 [RFC5208].
* Para un **Par de claves de curva elíptica** (clave EC), la codificación ASN.1 DER de clave privada [RFC5915] encapsulada en PKCS#8 [RFC5208].
* Para una clave de octeto, los bytes sin formato de la clave.

Los bytes de la clave de texto no cifrado se transforman mediante el mecanismo CKM\_RSA\_AES\_KEY\_WRAP:

* Se genera una clave AES efímera y se cifra con la clave RSA de ajuste mediante RSA-OAEP con un **algoritmo hash seguro** (SHA1).
* La clave de texto no cifrado codificada se cifra con la clave AES mediante el encapsulado de claves AES con relleno.
* La clave AES cifrada y la clave de texto no cifrado cifrada se concatenan para generar el blob de texto cifrado final.

El formato del blob de transferencia usa la serialización compacta de cifrado web (RFC7516) de **notación de objetos JavaScript** (JSON) principalmente como vehículo para entregar los metadatos necesarios al servicio para un correcto descifrado.

**Cargar el blob de transferencia de claves para importar la clave de HSM**

El cliente transfiere el archivo Blob de transferencia de claves (archivo ".byok") a una estación de trabajo en línea y, a continuación, ejecuta un comando az keyvault key import para importar este blob como una nueva clave respaldada por HSM en Key Vault.

**Habilitar el cifrado doble en el nivel de infraestructura de Azure Storage**

Azure Storage cifra de forma automática todos los datos de una cuenta de almacenamiento en el nivel de servicio mediante el cifrado AES de 256 bits, uno de los cifrados de bloques más sólidos que hay disponibles y compatible con FIPS 140-2. Los clientes que necesiten más seguridad para que sus datos estén seguros también pueden habilitar el cifrado AES de 256 bits en el nivel de infraestructura de Azure Storage para el cifrado doble. El doble cifrado de los datos de Azure Storage sirve de protección en caso de que uno de los algoritmos de cifrado o las claves puedan estar en peligro. En este escenario, la capa adicional de cifrado también protege los datos.

El cifrado de infraestructura se puede habilitar para toda la cuenta de almacenamiento o para un ámbito de cifrado dentro de una cuenta. Cuando se habilita el cifrado de infraestructura para una cuenta de almacenamiento o un ámbito de cifrado, los datos se cifran dos veces (una vez en el nivel de servicio y otra en el nivel de infraestructura) con dos algoritmos de cifrado y dos claves diferentes.

El cifrado de nivel de servicio permite usar claves administradas por Microsoft o claves administradas por el cliente con Azure Key Vault o el modelo de seguridad de hardware (HSM) administrado de Key Vault. El cifrado en el nivel de infraestructura se basa en las claves administradas por Microsoft y siempre usa una clave independiente.

Para cifrar dos veces los datos, primero debe crear una cuenta de almacenamiento o un ámbito de cifrado que estén configurados para el cifrado de infraestructura.

*El cifrado de infraestructura se recomienda en escenarios en los que es necesario cifrar los datos doblemente debido a los requisitos de cumplimiento. En la mayoría de los demás escenarios, el cifrado de Azure Storage proporciona un algoritmo de cifrado lo suficientemente eficaz y es poco probable que presente alguna ventaja con respecto al uso del cifrado de infraestructura.*

**Creación de una cuenta con el cifrado de infraestructura habilitado**

Para habilitar el cifrado de infraestructura para una cuenta de almacenamiento, debe configurar la cuenta de almacenamiento para que use el cifrado de infraestructura en el momento de crear la cuenta. Una vez que la cuenta se ha creado, no se puede habilitar o deshabilitar el cifrado de infraestructura. La cuenta de almacenamiento debe ser de tipo blob en bloques prémium o de uso general v2.

Para usar Azure Portal con el fin de crear una cuenta de almacenamiento con el cifrado de infraestructura habilitado, siga estos pasos:

1. En Azure Portal, vaya a la página **Cuentas de almacenamiento**.
2. Elija el botón **Agregar** para agregar una cuenta de almacenamiento de blob en bloques prémium o de uso general v2.
3. En la pestaña **Cifrar**, busque **Habilitar cifrado de infraestructura** y seleccione **Habilitado**.
4. Seleccione **Revisar y crear** para terminar de crear la cuenta de almacenamiento.

Para comprobar que el cifrado de infraestructura está habilitado para una cuenta de almacenamiento con Azure Portal, siga estos pasos:

1. Vaya a la cuenta de almacenamiento en Azure Portal.
2. En **Configuración**, elija **Cifrado**.

Azure Policy proporciona una directiva integrada para requerir que el cifrado de infraestructura esté habilitado para una cuenta de almacenamiento.

**Creación de un ámbito de cifrado con el cifrado de infraestructura habilitado**

Si el cifrado de infraestructura está habilitado para una cuenta, cualquier ámbito de cifrado creado en esa cuenta usa automáticamente el cifrado de infraestructura. Si el cifrado de infraestructura no está habilitado en el nivel de cuenta, tiene la opción de habilitarlo para un ámbito de cifrado en el momento de crear el ámbito. La configuración de cifrado de infraestructura para un ámbito de cifrado no se puede cambiar después de crear el ámbito.

**Prueba de conocimientos**

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

**Comprobación de conocimientos**

Principio del formulario

**1. ¿Cuál es la manera recomendada de administrar y rotar las claves de acceso de la cuenta de almacenamiento de Azure?**

1. Use Azure Key Vault para administrar y rotar las claves
2. Guardar las claves de acceso en texto sin formato accesible para otros usuarios
3. Claves de acceso de codificación rígida en el código de la aplicación

**2. ¿Cuál es el propósito de usar Azure Key Vault para administrar las claves de acceso de la cuenta de almacenamiento?**

1. Limitar el acceso a los datos almacenados en la cuenta de almacenamiento
2. Generar nuevas claves de acceso para cada cuenta de almacenamiento
3. Administrar y rotar las claves de acceso existentes de forma segura

**3. ¿Cuál es la manera recomendada de autorizar el acceso a los datos en Azure Storage?**

1. Uso de Microsoft Entra ID o una firma de acceso compartido SAS
2. Uso de la autorización de clave compartida
3. Uso de claves de acceso y cadenas de conexión para todas las aplicaciones que acceden a datos confidenciales o de producción

**4. ¿Cuál es el propósito de autorizar el acceso a los recursos de Azure Storage?**

1. Restringir el acceso solo a los recursos a los usuarios con autorización de Microsoft Entra Domain Services
2. Hacer que los recursos sean públicos y accesibles para cualquier usuario
3. Garantizar que solo se pueda acceder a los recursos cuando esté autorizado y únicamente a aquellos usuarios o aplicaciones a los que se haya concedido acceso

**5. ¿Cuál es el propósito de Bring Your Own Key (BYOK) en Azure Key Vault?**

1. Para transferir una clave de Azure Key Vault a un módulo de seguridad de hardware (HSM) local
2. Para transferir de forma segura una clave desde un módulo de seguridad de hardware (HSM) local fuera de Azure, en el HSM que respalda Azure Key Vault
3. Para generar una nueva clave en Azure Key Vault para su uso en un HSM local
4. A
5. C
6. A
7. C
8. B

Final del formulario

**Resumen**

En este módulo, ha aprendido a planear e implementar medidas de seguridad completas para los recursos de Azure Storage, incluida la configuración del control de acceso para las cuentas de almacenamiento, la administración de claves de acceso, la selección y configuración de los métodos adecuados para acceder a varios servicios de almacenamiento de Azure, la protección frente a amenazas de seguridad de datos mediante técnicas como la eliminación temporal, las copias de seguridad, el control de versiones e inmutables, y la mejora del cifrado de datos con Bring Your Own Key (BYOK) y el cifrado doble en el nivel de infraestructura de Azure Storage.