Implementación de la seguridad de almacenamiento

Definición de la soberanía de datos

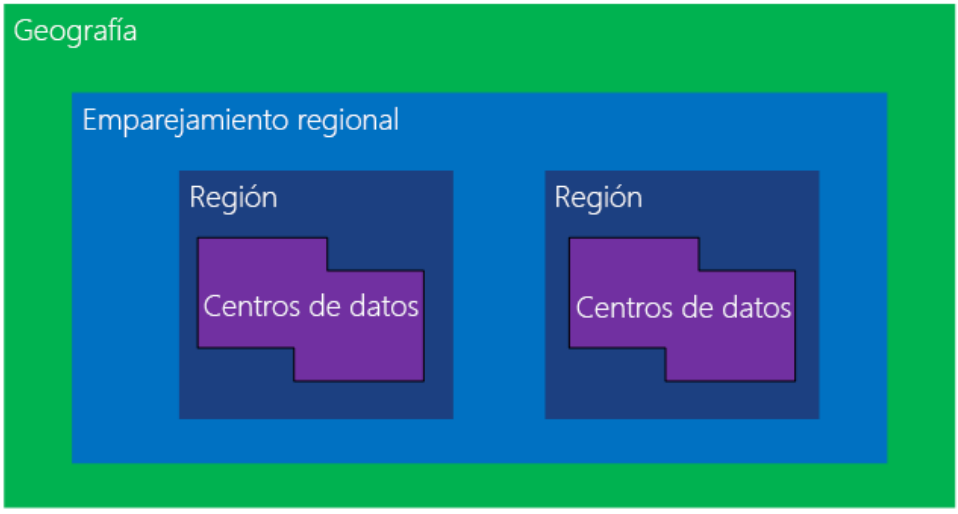
¿Qué es la soberanía de datos? - La soberanía de datos es el concepto de que la información, que se ha convertido y almacenado en formato digital binario, está sujeta a las leyes del país o región en el que se encuentra. Muchas de las preocupaciones en torno a la soberanía de datos tienen que ver con el cumplimiento de las regulaciones de privacidad y los esfuerzos por evitar que los datos almacenados en un país o región extranjeros sean requeridos mediante citación por el gobierno del país o la región anfitriones.

En Azure, los datos de los clientes se pueden replicar dentro de un área geográfica seleccionada para mejorar la durabilidad de los datos durante un desastre importante del centro de datos y, en algunos casos, no se replicarán fuera de él.

Regiones emparejadas

Azure funciona en varias ubicaciones geográficas del mundo. Una ubicación geográfica de Azure es un área definida del mundo que contiene al menos una región de Azure. Una región de Azure es un área dentro de una ubicación geográfica que contiene uno o varios centros de datos.

Cada región de Azure se empareja con otra región de la misma zona geográfica, conformando lo que se denomina par de regiones. La excepción es el Sur de Brasil, ya que se trata de una región emparejada con otra que se encuentra fuera de su ubicación geográfica. En los pares de regiones, Azure serializa las actualizaciones de la plataforma (o el mantenimiento planeado), de forma que solo se actualiza una región emparejada de cada vez. Si se produce una interrupción que afecta a varias regiones, se dará prioridad a la recuperación de una de las regiones de cada par.



Se recomienda configurar la continuidad empresarial y recuperación ante desastres entre los pares de regiones para beneficiarse de las directivas de máquina virtual y aislamiento de Azure.

Para aplicaciones que admiten varias regiones activas, recomendamos utilizar, siempre que sea posible, ambas regiones en un par de regiones. El hecho de que haya varias regiones asegurará una disponibilidad óptima de las aplicaciones y minimizará el tiempo de recuperación en caso de desastre.

Ventajas de las regiones emparejadas de Azure

- **Aislamiento físico: cuando es posible, los servicios de Azure prefieren un mínimo de 482 km (300 millas) de separación entre los centros de datos de un emparejamiento regional, aunque una distancia más larga no será práctico o posible en todo el mundo. La separación del centro de datos físico reduce la probabilidad de que ambas regiones se vean afectadas a la vez por desastres naturales, disturbios civiles, cortes del suministro eléctrico o interrupciones de la red física. El aislamiento está sujeto a las restricciones geográficas (como el tamaño de la ubicación geográfica, la disponibilidad de la infraestructura de red y de energía y las normativas).**
- **Replicación proporcionada por la plataforma: algunos servicios, como el almacenamiento con redundancia geográfica, ofrecen replicación automática en la región emparejada.**
- **Orden de recuperación de región: si se produce una interrupción amplia, tiene prioridad la recuperación de una región por cada par. Se garantiza que, si las aplicaciones se implementan en regiones emparejadas, se dará prioridad a la recuperación de una de las regiones. Si una aplicación se implementa en regiones que no están emparejadas, es posible que la recuperación se demore. En el peor de los casos, puede que las regiones elegidas sean las dos últimas que se van a recuperar.**
- **Actualizaciones en secuencia: las actualizaciones del sistema de Azure que estén previstas se implementan en las regiones emparejadas de forma secuencial, no a la vez. Una implementación por fases ayuda a minimizar el tiempo de inactividad, el efecto de los errores y los errores lógicos en el caso excepcional de una mala actualización.**
- **Residencia de datos: para cumplir los requisitos de residencia de datos con fines de jurisdicción de impuestos y aplicación de la ley, una región reside en la misma ubicación geográfica que su par (a excepción del Sur de Brasil).**

Microsoft también cumple las leyes internacionales de protección de datos en relación con las transferencias de datos de clientes a través de fronteras. Por ejemplo, para dar cabida al flujo continuo de información necesario en el comercio internacional (incluidas las transferencias de datos personales que atraviesan fronteras), muchos servicios de Microsoft Business Cloud ofrecen a los clientes cláusulas del modelo de Unión Europea que proporcionan más garantías contractuales en relación con las transferencias de datos personales en los servicios de nube en ámbito. Las autoridades de protección de datos de la Unión Europea han validado la implementación de Microsoft de las cláusulas del modelo de la UE como acordes con los rigurosos estándares de privacidad que regulan las transferencias de datos internacionales por parte de las empresas que operan en sus estados miembros.

Además de nuestros compromisos en virtud de las cláusulas contractuales estándar y otros contratos de modelo, Microsoft está certificado para el marco del Escudo de Privacidad de la UE-EE. UU. según lo establecido por el Departamento de Comercio de EE. UU. con respecto a la recopilación, el uso y la retención de información personal transferida desde la Unión Europea a Estados Unidos. La participación de Microsoft en el Escudo de Privacidad de la UE-EE. UU. se aplica a todos los datos personales que están sujetos a la Declaración de privacidad de Microsoft y que proceden de la Unión Europea, el Espacio Económico Europeo y Suiza. Microsoft también respeta la ley de protección de datos de Suiza en lo referente al procesamiento de datos personales procedentes del Espacio Económico Europeo y Suiza.

Microsoft no transferirá a ningún tercero (ni siquiera con fines de almacenamiento) los datos que facilite a Microsoft mediante el uso de nuestros servicios de nube de empresariales, y que se rigen por los Términos de los Servicios en Línea de Microsoft.

Nota Con independencia de dónde se almacenen los datos del cliente, Microsoft no controla ni limita las ubicaciones desde las que los clientes o sus usuarios finales pueden acceder a los datos.

Configuración del acceso a Azure Storage

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.

Entre las opciones para autorizar solicitudes a Azure Storage, se incluyen las siguientes:

- **Azure AD**: Azure Storage proporciona integración con Azure Active Directory (Azure AD) para la autorización basada en identidades de las solicitudes a Blob Services y Queue Services. Con Azure AD, puede usar el control de acceso basado en rol (RBAC) para conceder acceso a los recursos de blobs y colas a usuarios, grupos o aplicaciones. Puede conceder permisos que tengan como ámbito el nivel de un contenedor o cola individuales. La autorización del acceso a los datos de blobs y colas con Azure AD proporciona mayor seguridad y facilidad de uso con respecto a otras opciones de autorización. Cuando se usa Azure AD para autorizar las solicitudes que se realizan desde las aplicaciones, se 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 Azure AD siempre que sea posible.
- **Autorización de Azure Active Directory Domain Services (Azure AD DS)** para Azure Files. Azure Files admite la autorización basada en identidad sobre Bloque de mensajes del servidor(SMB) mediante Azure AD DS. Puede usar RBAC para un control más preciso sobre el acceso de un cliente a los recursos de Azure Files de una cuenta de almacenamiento.

- **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 a través de la solicitud en el encabezado de autorización.
- **Firmas de acceso compartido**: una firma de acceso compartido (SAS) es un URI que concede derechos de acceso restringidos a recursos de Azure Storage. Puede proporcionar una firma de acceso compartido a los clientes que no deben ser de confianza con la clave de la cuenta de almacenamiento, pero a los que sí quiere delegar acceso a determinados recursos de la cuenta de almacenamiento. Mediante la distribución de un URI de firma de acceso compartido a estos clientes, puede concederles acceso a un recurso durante un período de tiempo especificado y con un conjunto de permisos concreto. Los parámetros de consulta del URI que comprenden el token de SAS incorporan toda la información necesaria para conceder acceso controlado a un recurso de almacenamiento. Un cliente que esté en posesión de la SAS puede realizar una solicitud en Azure Storage solo con el URI de SAS, y la información contenida en el token de SAS se usará para autorizar la solicitud.
- **Acceso anónimo a contenedores y blobs**: puede habilitar el acceso de lectura anónimo y público a un contenedor y sus blobs en Azure Blob Storage. Al hacerlo, puede conceder acceso de solo lectura a estos recursos sin compartir la clave de cuenta y sin necesidad de una firma de acceso compartido (SAS). El acceso de lectura público es mejor para escenarios en los que desea que determinados blobs estén siempre disponibles para el acceso de lectura anónimo. Para un control más detallado, busque el uso de la firma de acceso compartido, descrita anteriormente.

La autenticación y autorización del acceso a los datos de blobs y colas con Azure AD proporciona mayor seguridad y facilidad de uso con respecto a otras opciones de autorización. Por ejemplo, al usar Azure AD, 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 Azure AD 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 Azure AD ofrece capacidades similares sin necesidad de administrar tokens de SAS ni preocuparse sobre cómo revocar una SAS en peligro.

Importante

Siempre que sea posible, utilice aplicaciones de autorización que accedan a Azure Storage mediante Azure AD. Esto proporciona una mayor seguridad y facilidad de uso con respecto a otras opciones de autorización.

Implementación de firmas de acceso compartido

Se recomienda no compartir claves de cuenta de almacenamiento con aplicaciones de terceros externas. Si estas aplicaciones necesitan acceso a los datos, debe proteger sus conexiones sin usar claves de cuenta de almacenamiento.

En el caso de los clientes que no son de confianza, use una **firma de acceso compartido** (SAS). Una firma de acceso compartido es una cadena que contiene un token de seguridad que se puede asociar a un URI. Use una firma de acceso compartido para delegar el acceso a objetos de almacenamiento y especificar restricciones, como los permisos y el intervalo de tiempo de acceso.

Puede dar a un cliente un token de firma de acceso compartido, por ejemplo, para que pueda cargar imágenes en un sistema de archivos en Blob Storage. Por otro lado, puede dar permiso a una aplicación web para que lea esas imágenes. En ambos casos, solo permite el acceso que la aplicación necesita para realizar la tarea.

Tipos de firmas de acceso compartido

- Puede usar una firma de acceso compartido de **nivel de servicio** para permitir el acceso a recursos específicos de una cuenta de almacenamiento. Este tipo de firma de acceso compartido se usaría, por ejemplo, para permitir que una aplicación recuperara una lista de archivos de un sistema de archivos o para descargar un archivo.
- Use una firma de acceso compartido de **nivel de cuenta** para permitir el acceso a todo lo que puede permitir una firma de acceso compartido de nivel de servicio, además de a otros recursos y capacidades. Por ejemplo, puede usar una firma de acceso compartido de nivel de cuenta para permitir la creación de sistemas de archivos.
- Una **SAS de delegación de usuarios**, introducida con la versión 2018-11-09. Una SAS de delegación de usuarios se protege con credenciales de Azure AD. Este tipo de SAS solo se admite para Blob service y se puede usar para conceder acceso a contenedores y blobs.

Además, una SAS de servicio puede hacer referencia a una directiva de acceso almacenada que proporcione un nivel de control adicional sobre un conjunto de firmas, incluida la capacidad de modificar o revocar el acceso al recurso en caso necesario.

Normalmente, se usaría una firma de acceso compartido para un servicio en el que los usuarios leyeran y escribieran sus datos en la cuenta de almacenamiento. Las cuentas que almacenan datos de usuario tienen dos diseños típicos:

- Los clientes cargan y descargan datos mediante un servicio de proxy de front-end que realiza la autenticación. Este servicio de proxy de front-end tiene la ventaja de permitir la validación de reglas de negocio. Pero si el servicio debe controlar grandes cantidades de datos o transacciones de gran volumen, es posible que le resulte complicado o costoso

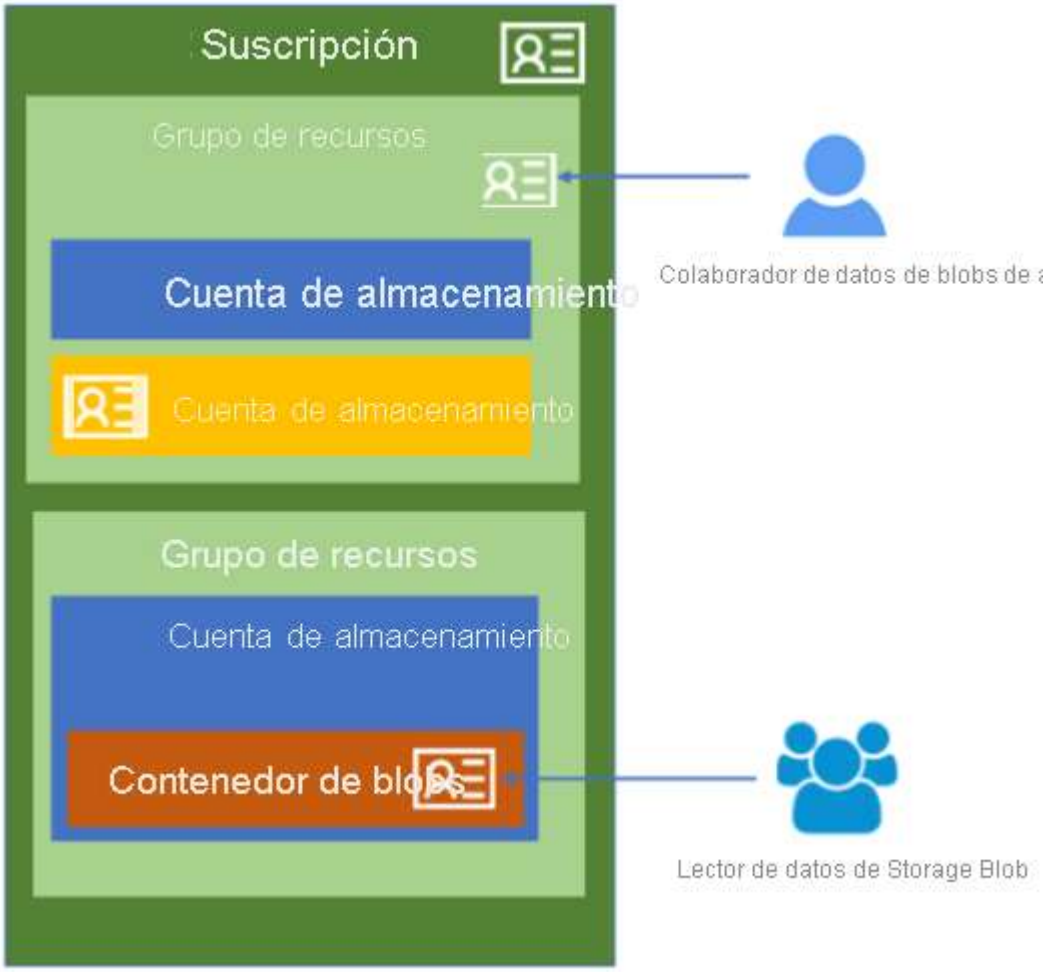
escalarlo para satisfacer la demanda.

- Un servicio ligero autentica al cliente según necesidad. Luego genera una firma de acceso compartido. Después de recibir la firma de acceso compartido, el cliente puede acceder a los recursos de la cuenta de almacenamiento directamente. La firma de acceso compartido define los permisos y el intervalo de acceso del cliente. La firma de acceso compartido reduce la necesidad de enrutar todos los datos a través del servicio de proxy de front-end.

Administración de la autenticación de almacenamiento de Azure AD

Además de la clave compartida y las firmas de acceso compartido, Almacenamiento de Azure admite el uso de Azure Active Directory (Azure AD) para autorizar las solicitudes a datos blob. Con Azure AD, 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. Azure AD 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 de solicitudes en Azure Storage con Azure AD proporciona seguridad superior y facilidad de uso sobre la autorización de clave compartida. Microsoft recomienda usar la autorización de Azure AD con las aplicaciones de blobs cuando sea posible para garantizar el acceso con los privilegios mínimos necesarios.
- La autorización con credenciales de Azure AD 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 Azure AD.
- Blob Storage admite de forma adicional la creación de firmas de acceso compartido (SAS) firmadas con credenciales de Azure AD.



Algunos detalles más

Cuando una entidad de seguridad (un usuario, un grupo o una aplicación) intenta acceder a un recurso de cola, la solicitud debe estar autorizada. Con Azure AD, 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 Queue 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 colas.

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 cola. Los roles que se asignan a una entidad de seguridad determinan los permisos que tiene esa entidad de seguridad. Para saber más sobre la asignación de roles de Azure para el acceso a la cola.

Las aplicaciones nativas y las aplicaciones web que realizan solicitudes a Queue service de Azure también pueden autorizar el acceso con Azure AD. Para obtener información sobre cómo solicitar un token de acceso y usarlo para autorizar solicitudes

Implementación del cifrado del servicio de almacenamiento

La **seguridad de Azure Storage** es una parte clave para la defensa en profundidad. Azure Storage proporciona un completo conjunto de funcionalidades de seguridad que, conjuntamente, permiten a los desarrolladores compilar aplicaciones seguras:

- Todos los datos (incluidos los metadatos) escritos en Azure Storage se cifran automáticamente con Storage Service Encryption (SSE).
- Azure Active Directory (Azure AD) y el control de acceso basado en rol (RBAC) son compatibles con Azure Storage para las operaciones de administración de recursos y las operaciones de datos, como se indica a continuación:
    - Puede asignar roles de RBAC en el ámbito de la cuenta de almacenamiento para las entidades de seguridad y utilizar Azure AD para autorizar las operaciones de administración de recursos, como la administración de claves.
    - La integración con Azure AD se admite para las operaciones de datos de cola y blob. Puede asignar roles de RBAC en el ámbito de una suscripción, un grupo de recursos, una cuenta de almacenamiento, un contenedor individual o una cola a una entidad de seguridad o identidad administrada para los recursos de Azure.
- Los datos se pueden proteger en tránsito entre una aplicación y Azure usando cifrado de cliente, HTTPS o SMB 3.0.
- Se puede establecer el cifrado de los discos de datos y del sistema operativo utilizados por Azure Virtual Machines mediante Azure Disk Encryption.
- Se puede conceder acceso delegado a los objetos de datos de Azure Storage mediante las firmas de acceso compartido.

Cifrado de Azure Storage para datos en reposo

Azure Storage cifra automáticamente los datos al guardarlos en la nube. Mediante el cifrado, se protegen los datos y es más fácil cumplir los compromisos de cumplimiento y seguridad de la organización. Los datos de Azure Storage se cifran y descifran de forma transparente mediante el cifrado AES de 256 bits, uno de los cifrados de bloques más sólidos que hay disponibles, y son compatibles con FIPS 140-2. El cifrado de Azure Storage es similar al cifrado de BitLocker en Windows.

El cifrado de Azure Storage está habilitado para todas las cuentas de almacenamiento nuevas y existentes, y no se puede deshabilitar. Como los datos están protegidos de forma predeterminada, no es necesario modificar el código o las aplicaciones para aprovechar el cifrado de Azure Storage.

Las cuentas de almacenamiento se cifran independientemente de su nivel de rendimiento (Estándar o Premium) o del modelo de implementación (Azure Resource Manager o clásico). Todas las opciones de redundancia de Azure Storage admiten el cifrado y se cifran todas las copias de una cuenta de almacenamiento. Se cifran todos los recursos de Azure Storage, incluidos los blobs, los discos, los archivos, las colas y las tablas. También se cifran todos los metadatos de objetos.

El cifrado no afecta al rendimiento de Azure Storage. No hay ningún costo adicional para el cifrado de Azure Storage.

Administración de claves de cifrado

Puede confiar en las claves administradas por Microsoft para el cifrado de la cuenta de almacenamiento, o puede administrar el cifrado con sus propias claves. Si opta por administrar el cifrado con sus propias claves, tiene dos opciones:

- Puede especificar una clave *administrada por el cliente* que se use para cifrar y descifrar todos los datos de la cuenta de almacenamiento. Una clave administrada por el cliente se usa para cifrar todos los datos de todos los servicios de la cuenta de almacenamiento.
- Puede especificar una clave *proporcionada por el cliente* en las operaciones de Blob Storage. Un cliente que realiza una solicitud de lectura o escritura en el almacenamiento de blobs puede incluir una clave de cifrado en la solicitud para tener un control detallado sobre el cifrado y el descifrado de los datos de blob.

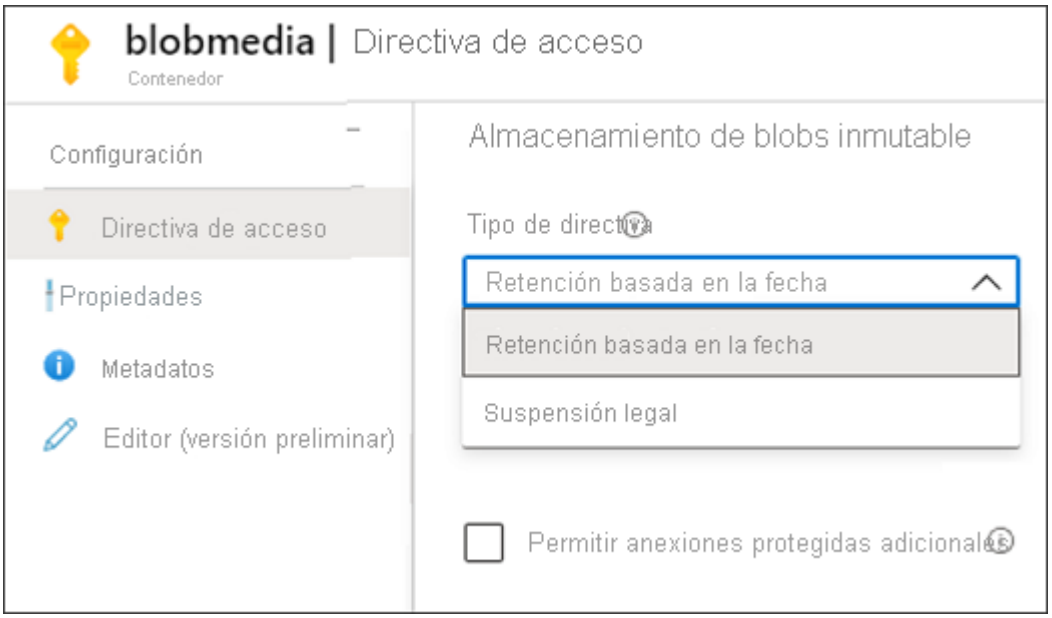
En la tabla siguiente se comparan las opciones de administración de claves para el cifrado de Azure Storage.

	Claves administradas por Microsoft	Claves administradas por el cliente	Claves proporcionadas por el cliente
Operaciones de cifrado y descifrado	Azure	Azure	Azure
Servicios de Azure Storage admitidos	All	Blob Storage, Azure Files	Blob Storage
Almacenamiento de claves	Almacén de claves de Microsoft	Azure Key Vault	Azure Key Vault o cualquier otro almacén de claves
Responsabilidad de la rotación de claves	Microsoft	Customer	Customer
Uso de las claves	Microsoft	Azure Portal, API REST del proveedor de recursos de almacenamiento, bibliotecas de administración de Azure Storage, PowerShell, CLI	API REST de Azure Storage (Blob Storage), bibliotecas de cliente de Azure Storage
Acceso a la clave	Solo Microsoft	Microsoft, cliente	Solo el cliente

Configuración de directivas de retención de datos de blobs

El almacenamiento inmutable para Azure Blob Storage permite a los usuarios almacenar objetos de datos críticos para la empresa en un estado WORM (escribir una vez, leer muchas). En este estado, los usuarios no pueden borrar ni modificar los datos durante el intervalo de tiempo especificado por el usuario. Mientras dure el intervalo de retención, se pueden crear y leer blobs, pero no modificar ni eliminar. El almacenamiento inmutable está disponible en las cuentas de uso general v2 y en las cuentas de Blob Storage de todas las regiones de Azure.

Directivas de retención basadas en el tiempo frente a directivas de retención legales



- **Compatibilidad con directivas de retención con duración definida** : los usuarios pueden establecer directivas para almacenar datos durante un intervalo especificado. Cuando se establece una directiva de retención con duración definida, se pueden crear y leer blobs, pero no se pueden modificar ni eliminar. Una vez transcurrido el período de retención, los blobs se pueden eliminar pero no sobrescribir. Cuando se aplica una directiva de retención con duración definida a un contenedor, todos los blobs de este permanecen en estado inmutable durante el período de retención en vigor. El período de retención efectivo para los blobs es igual a la diferencia entre la hora de creación del blob y el intervalo de retención especificado por el usuario. Como los usuarios pueden ampliar el intervalo de retención, el almacenamiento inmutable utiliza el valor más reciente del intervalo de retención especificado por el usuario para calcular el período de retención vigente.
- **Compatibilidad con directivas de suspensión legal** : si el intervalo de retención no se conoce, los usuarios pueden establecer suspensiones legales para almacenar los datos inmutables hasta que estas desaparezcan. Cuando se establece una directiva de suspensión legal, se pueden crear y leer blobs, pero no se pueden modificar ni eliminar. Cada suspensión legal está asociada a una etiqueta alfanumérica definida por el usuario que se usa como una cadena de identificación (por ejemplo, un identificador de caso, un nombre de evento, etc.). Las suspensiones legales son suspensiones temporales que se pueden usar con fines de investigación legal o directivas de protección general. Cada directiva de suspensión legal debe estar asociada a una o varias etiquetas. Las etiquetas se usan como un identificador con nombre, como un identificador de caso o un evento, para categorizar y describir el propósito de la suspensión.

Otras características de almacenamiento inmutables

- **Compatibilidad con todos los niveles de blobs:** las directivas WORM son independientes del nivel de Azure Blob Storage y se aplican a todos los niveles: de archivo, frecuente y esporádico. Los usuarios pueden transferir sus datos al nivel que les ofrezca la mayor

optimización de costos de acuerdo con sus cargas de trabajo sin alterar la inmutabilidad de los datos.

- **Configuración en el nivel de contenedor**: los usuarios pueden configurar las directivas de retención con duración definida y las etiquetas de suspensión legal a nivel del contenedor. Mediante valores de configuración sencillos en el nivel de contenedor, los usuarios pueden crear y bloquear las directivas de retención con duración definida, ampliar los intervalos de retención, establecer y eliminar suspensiones legales, etc. Estas directivas se aplican a todos los blobs del contenedor, tanto a los nuevos como a los existentes.
- **Compatibilidad con el registro de auditoría**: todos los contenedores incluyen un registro de auditoría de directiva. En él se muestran hasta siete comandos de retención con duración definida para las directivas de retención con duración definida bloqueadas y contiene el identificador de usuario, el tipo de comando, las marcas de tiempo y el intervalo de retención. En el caso de las suspensiones legales, el registro contiene el identificador del usuario, el tipo de comando, las marcas de tiempo y las etiquetas de suspensión legal. Este registro se conserva mientras dure la directiva, de acuerdo con las directrices de regulación SEC 17a-4(f). El registro de actividad de Azure muestra un registro más completo de todas las actividades del plano de control, mientras que al habilitar los registros de recursos de Azure se conservan y se muestran las operaciones del plano de datos. Es responsabilidad del usuario almacenar dichos registros de forma persistente, ya que podría ser obligatorio por ley o por otros fines.

Configuración de la autenticación de Azure Files

Azure Files admite la autenticación basada en identidades a través del Bloque de mensajes del servidor (SMB) mediante Active Directory Domain Services (AD DS) local y Azure Active Directory Domain Services (Azure AD DS). En este artículo se describe la forma en que los recursos compartido de archivos de Azure pueden usar los servicios de dominio, ya sea de forma local o en Azure, para admitir el acceso basado en identidad a los recursos compartidos de archivos de Azure a través de SMB. La habilitación del acceso basado en identidad de los recursos compartidos de archivos de Azure permite reemplazar los servidores de archivos existentes por recursos compartidos de archivos de Azure sin reemplazar el servicio de directorio existente, con lo que se mantiene el acceso sin problemas de los usuarios a los recursos compartidos.

Azure Files aplica la autorización en el acceso del usuario tanto al recurso compartido como a los niveles de directorio o archivo. La asignación de permisos de nivel de recurso compartido se puede realizar en usuarios o grupos administrados de Azure Active Directory (Azure AD) mediante el modelo de control de acceso basado en rol (RBAC). Con RBAC, las credenciales que se usan para el acceso a archivos deben estar disponibles o sincronizadas con Azure AD. Puede asignar roles de RBAC integrados como el lector de recursos compartidos de SMB de datos de archivos de

almacenamiento a usuarios o grupos en Azure AD para conceder acceso de lectura a un recurso compartido de archivos de Azure.

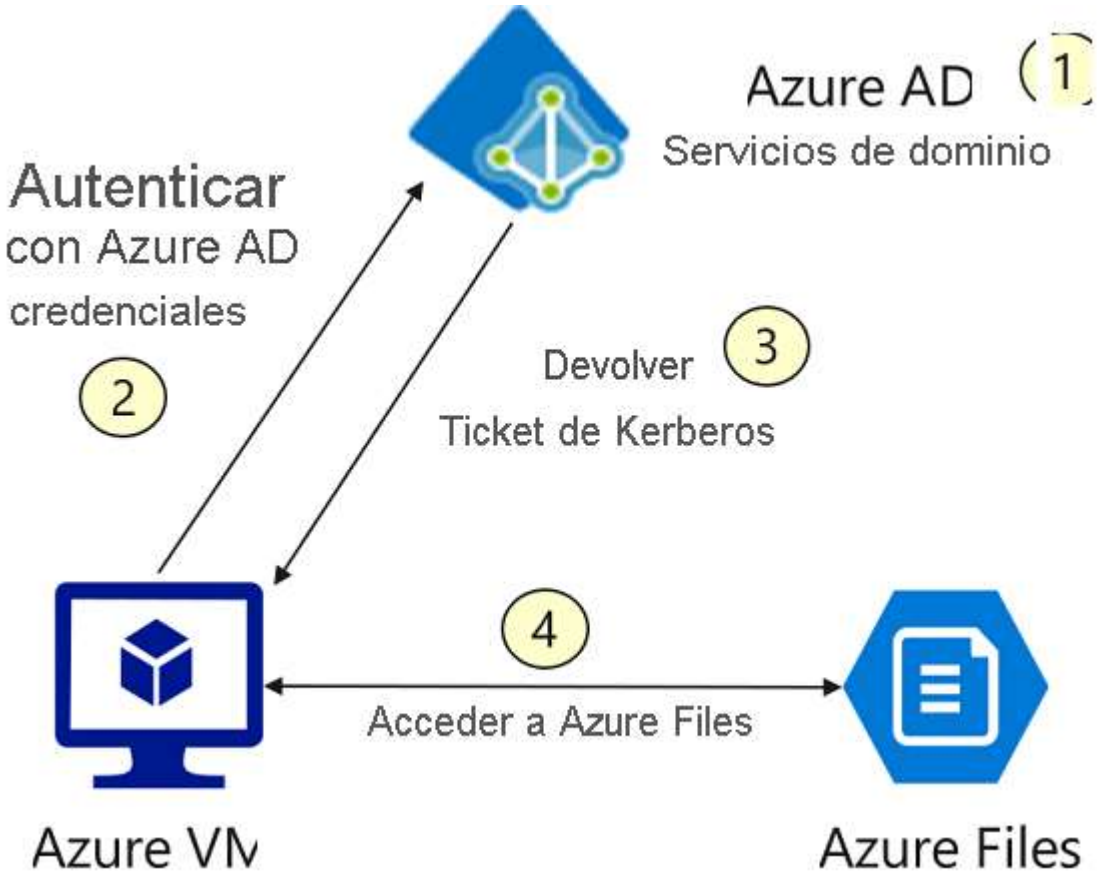
En el nivel de directorio o archivo, Azure Files admite la conservación, la herencia y la aplicación de DACL de Windows igual que cualquier servidor de archivos de Windows. Se puede optar por mantener las DACL de Windows al copiar datos a través de SMB entre el recurso compartido de archivos existente y los recursos compartidos de archivos de Azure. Independientemente de que se tenga previsto aplicar la autorización o no, se pueden usar los recursos compartidos de archivos de Azure para hacer copias de seguridad de las ACL junto con los datos.

Ventajas de la autenticación basadas en identidad

La autenticación basada en identidad para Azure Files ofrece varias ventajas respecto al uso de la autenticación de clave compartida:

- Amplíe la experiencia tradicional de acceso a recursos compartidos de archivos basado en identidades a la nube con AD DS local y Azure AD DS. Si tiene previsto realizar una migración "lift-and-shift" de su aplicación a la nube, mediante el reemplazo de los servidores de archivos tradicionales con recursos compartidos de archivos de Azure, tal vez quiera que la aplicación se autentique con las credenciales de AD DS local o Azure AD DS para acceder a los datos de los archivos. Azure Files admite el uso de credenciales de AD DS local y de Azure AD DS para tener acceso a los recursos compartidos de archivos de Azure a través de SMB desde VM unidas a un dominio de AD DS local o Azure AD DS.
- Aplique el control de acceso granular en recursos compartidos de archivos de Azure. Puede conceder permisos a una identidad específica en el nivel de recurso compartido, directorio o archivo. Por ejemplo, suponga que tiene varios equipos que utilizan un solo recurso compartido de archivos de Azure para la colaboración en proyectos. Puede conceder a todos los equipos acceso a directorios no confidenciales, al tiempo que limita el acceso a directorios que contienen datos financieros confidenciales únicamente a su equipo de financiero.
- Haga una copia de seguridad de las ACL de Windows (también conocidas como NTFS) junto con los datos. Puede usar recursos compartidos de archivos de Azure para realizar copias de seguridad de los recursos compartidos de archivos locales existentes. Azure Files conserva las listas de control de acceso junto con los datos cuando se hace una copia de seguridad de un recurso compartido de archivos en recursos compartidos de archivos de Azure sobre SMB.

Flujo de datos de autenticación basada en identidades



1. Antes de poder habilitar la autenticación en recursos compartidos de archivos de Azure, debe configurar el entorno del dominio. En el caso de la autenticación de Azure AD DS, debe habilitar Azure AD Domain Services y unir a un dominio las VM desde las que tiene pensado obtener acceso a los datos de los archivos. La VM unida a un dominio debe residir en la misma red virtual (Vnet) que la instancia de Azure AD DS. De forma similar, para la autenticación de AD DS local, debe configurar el controlador de dominio y la unión a un dominio de las máquinas o máquinas virtuales.
2. Cuando una identidad asociada con una aplicación que se ejecuta en una VM intenta acceder a los datos de recursos compartidos de archivos de Azure, la solicitud se envía a Azure AD DS para autenticar la identidad.
3. Si la autenticación es correcta, Azure AD DS devuelve un token de Kerberos.
4. La aplicación envía una solicitud que incluye el token de Kerberos, y los recursos compartidos de archivos de Azure usan ese token para autorizar la solicitud. Los recursos compartidos de archivos de Azure solo reciben el token y no conservan las credenciales de Azure AD DS.

Los recursos compartidos de archivos de Azure admiten la autenticación Kerberos para la integración con Azure AD DS o AD DS local. Antes de poder habilitar la autenticación en recursos compartidos de archivos de Azure, debe configurar el entorno del dominio. En el caso de la autenticación de Azure AD DS, debe habilitar Azure AD Domain Services y unir a un dominio las

VM desde las que tiene pensado obtener acceso a los datos de los archivos. La VM unida a un dominio debe residir en la misma red virtual (Vnet) que la instancia de Azure AD DS. De forma similar, para la autenticación de AD DS local, debe configurar el controlador de dominio y la unión a un dominio de las máquinas o máquinas virtuales.

Cuando una identidad asociada con una aplicación que se ejecuta en una VM intenta acceder a los datos de recursos compartidos de archivos de Azure, la solicitud se envía a Azure AD DS para autenticar la identidad. Si la autenticación es correcta, Azure AD DS devuelve un token de Kerberos. La aplicación envía una solicitud que incluye el token de Kerberos, y los recursos compartidos de archivos de Azure usan ese token para autorizar la solicitud. Los recursos compartidos de archivos de Azure solo reciben el token y no conservan las credenciales de Azure AD DS. La autenticación de AD DS local funciona de manera similar, donde AD DS proporciona el token de Kerberos.

Conservación de las listas de control de acceso de archivos y directorios al importar datos a recursos compartidos de archivos de Azure

Azure Files admite la conservación de las listas de control de acceso de directorios o archivos al copiar datos a recursos compartidos de archivos de Azure. Puede copiar listas de control de acceso de un directorio o archivo en recursos compartidos de archivos de Azure mediante Azure File Sync o conjuntos de herramientas comunes para mover archivos. Por ejemplo, puede usar robocopy con la marca /copy:s para copiar datos, así como ACL en un recurso compartido de archivos de Azure. Las listas de control de acceso se conservan de forma predeterminada, no es necesario habilitar la autenticación basada en identidad en la cuenta de almacenamiento para conservarlas.

Habilitación de la propiedad obligatoria de transferencia segura

Puede configurar la cuenta de almacenamiento para que acepte solicitudes de conexiones seguras solo si establece la propiedad Se requiere transferencia segura para la cuenta de almacenamiento. Cuando se requiere una transferencia segura, se rechazan todas las solicitudes que se originan en una conexión no segura. Microsoft recomienda que siempre se requiera una transferencia segura para todas las cuentas de almacenamiento.

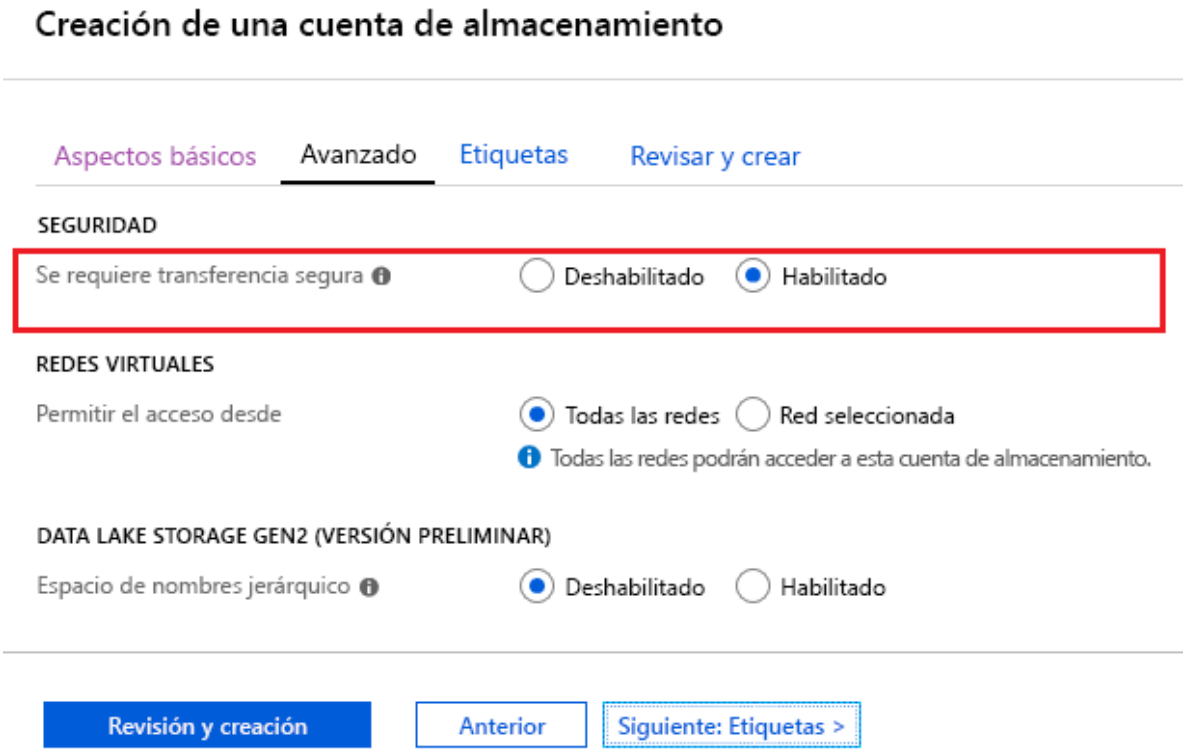
Cuando se requiere una transferencia segura, se debe realizar una llamada a una operación de API REST de Azure Storage a través de HTTPS. Se rechaza cualquier solicitud realizada a través de HTTP.

Se produce un error al establecer conexión con un recurso compartido de archivos de Azure a través de SMB sin cifrado cuando se requiere la transferencia segura para la cuenta de almacenamiento. Entre los ejemplos de conexiones no seguras se incluyen las realizadas a través de SMB 2.1, SMB 3.0 sin cifrado o algunas versiones del cliente SMB de Linux.

De forma predeterminada, la propiedad obligatoria de transferencia segura está habilitada al crear una cuenta de almacenamiento. Azure Storage no admite HTTPS para los **nombres de**

dominio personalizados. Esta opción no se puede aplicar cuando usa un nombre de dominio personalizado.

Solicitud de transferencia segura en una nueva cuenta de almacenamiento



Importante

Las conexiones de Azure Files requieren cifrado (SMB)