Protocolos NAS

NetApp Solutions

NetApp
April 25, 2024

Tabla de contenidos

Protocolos NAS

Información general sobre los protocolos NAS

Los protocolos NAS incluyen NFS (v3 y v4.1) y SMB/CIFS (2.x y 3.x). Estos protocolos son cómo CVS permite el acceso compartido a los datos entre varios clientes NAS. Además, Cloud Volumes Service puede proporcionar acceso a clientes NFS y SMB/CIFS simultáneamente (doble protocolo) a la vez que se respetan toda la configuración de identidades y permisos de los archivos y carpetas de los recursos compartidos NAS. Para mantener la seguridad de transferencia de datos más alta posible, Cloud Volumes Service admite el cifrado de protocolos en transferencia usando cifrado SMB y NFS Kerberos 5p.

El protocolo dual solo está disponible con CVS-Performance.

Conceptos básicos de los protocolos NAS

Los protocolos NAS representan formas en las que varios clientes de una red pueden acceder a los mismos datos en un sistema de almacenamiento, como Cloud Volumes Service en GCP. NFS y SMB son los protocolos NAS definidos y funcionan cliente/servidor donde Cloud Volumes Service actúa como servidor. Los clientes envían solicitudes de acceso, lectura y escritura al servidor y éste es responsable de coordinar los mecanismos de bloqueo de archivos, de almacenar permisos y de gestionar las solicitudes de identidad y autenticación.

Por ejemplo, se sigue el siguiente proceso general si un cliente NAS desea crear un nuevo archivo en una carpeta.

1. El cliente solicita al servidor información sobre el directorio (permisos, propietario, grupo, ID de archivo, espacio disponible, y así sucesivamente); el servidor responde con la información si el cliente y el usuario solicitante tienen los permisos necesarios en la carpeta principal.
2. Si los permisos del directorio permiten el acceso, el cliente le preguntará al servidor si el nombre de archivo que se está creando ya existe en el sistema de archivos. Si el nombre del archivo ya está en uso, se produce un error en la creación. Si el nombre del archivo no existe, el servidor hace saber al cliente que puede continuar.
3. El cliente realiza una llamada al servidor para crear el archivo con el identificador de directorio y el nombre de archivo y establece el acceso y las horas modificadas. El servidor emite un ID de archivo único al archivo para asegurarse de que no se crean otros archivos con el mismo ID de archivo.
4. El cliente envía una llamada para comprobar los atributos del archivo antes de la operación DE ESCRITURA. Si los permisos lo permiten, el cliente escribe el nuevo archivo. Si el protocolo/aplicación utiliza el bloqueo, el cliente solicita al servidor un bloqueo para evitar que otros clientes accedan al archivo mientras está bloqueado para evitar que se dañen los datos.

NFS

NFS es un protocolo de sistema de archivos distribuido que es un estándar abierto IETF

definido en solicitud de comentarios (RFC) que permite a cualquiera implementar el protocolo.

Los volúmenes de Cloud Volumes Service se comparten a los clientes NFS exportando una ruta a la que pueden acceder un cliente o un conjunto de clientes. Los permisos para montar estas exportaciones se definen mediante políticas y reglas de exportación, que los administradores de Cloud Volumes Service pueden configurar.

La implantación de NFS de NetApp se considera un estándar oro para el protocolo y se utiliza en innumerables entornos NAS empresariales. En las siguientes secciones se tratan el NFS y las características de seguridad específicas disponibles en Cloud Volumes Service y cómo se implementan.

Usuarios y grupos UNIX locales predeterminados

Cloud Volumes Service contiene varios usuarios y grupos UNIX predeterminados para varias funcionalidades básicas. Estos usuarios y grupos no se pueden modificar ni eliminar actualmente. No es posible agregar nuevos usuarios y grupos locales a Cloud Volumes Service en este momento. Los usuarios y grupos de UNIX fuera de los usuarios y grupos predeterminados deben ser proporcionados por un servicio de nombres LDAP externo.

En la siguiente tabla se muestran los usuarios y grupos predeterminados y sus correspondientes ID numéricos. NetApp recomienda no crear nuevos usuarios o grupos en LDAP o en los clientes locales que vuelvan a usar estos ID numéricos.

Usuarios predeterminados: ID numéricos	Grupos predeterminados: ID numéricos
• raíz:0 • pcuser:65534 • nadie:65535	• raíz:0 • daemon:1 • pcuser:65534 • nadie:65535

Cuando se utiliza NFSv4.1, el usuario raíz podría mostrarse como nadie cuando se ejecutan comandos de lista de directorios en clientes NFS. Esto se debe a la configuración de asignación de dominio de ID del cliente. Consulte la sección llamada NFSv4.1 y el usuario/grupo nadie para obtener detalles sobre esta edición y cómo resolverla.

El usuario raíz

En Linux, la cuenta raíz tiene acceso a todos los comandos, archivos y carpetas de un sistema de archivos basado en Linux. Debido a la eficacia de esta cuenta, las prácticas recomendadas de seguridad a menudo requieren que el usuario raíz se desactive o se restrinja de alguna manera. En las exportaciones NFS, la potencia que tienen los usuarios raíz sobre los archivos y carpetas se puede controlar en Cloud Volumes Service mediante las normas y políticas de exportación, y un concepto denominado squash raíz.

La función de ocupación de raíz garantiza que el usuario root que accede a un montaje NFS esté almacenado en la base del usuario numérico anónimo 65534 (consulte la sección “El usuario anónimo”) y actualmente sólo está disponible cuando se utiliza CVS-Performance seleccionando Off para acceso raíz durante la creación de reglas de política de exportación. Si el usuario root está almacenado en el nombre del usuario anónimo, ya no tiene acceso a ejecutar chown o. "comandos setuid/setgid (el bit de pegado)" En los archivos o carpetas del montaje NFS, y los archivos o carpetas creados por el usuario raíz muestran el UID anon como el propietario/grupo. Además, el usuario raíz no puede modificar las ACL de NFSv4. Sin embargo, el usuario raíz

todavía tiene acceso a chmod y archivos eliminados para los que no tiene permisos explícitos. Si desea limitar el acceso a los permisos de archivos y carpetas de un usuario raíz, considere la posibilidad de usar un volumen con ACL NTFS, creando un usuario de Windows con el nombre `root`y aplicar los permisos deseados a los archivos o carpetas.

El usuario anónimo

El ID de usuario anónimo (anon) especifica un ID de usuario o nombre de usuario de UNIX que se asigna a solicitudes de cliente que llegan sin credenciales de NFS válidas. Esto puede incluir al usuario root cuando se utiliza la función root squashing. El usuario anon en Cloud Volumes Service es 65534.

Este UID normalmente está asociado con el nombre de usuario `nobody` o. `nfsnobody` En entornos Linux. Cloud Volumes Service utiliza también 65534 como usuario local de UNIX' pcuser» (véase la sección "Usuarios y grupos UNIX locales predeterminados"), que también es el usuario de respaldo predeterminado para las asignaciones de nombres de Windows a UNIX cuando no se encuentra ningún usuario de UNIX válido coincidente en LDAP.

Debido a las diferencias en los nombres de usuario en Linux y Cloud Volumes Service para UID 65534, es posible que la cadena de nombre de los usuarios asignados a 65534 no coincida cuando se utiliza NFSv4.1. Como resultado, puede que vea `nobody` como usuario en algunos archivos y carpetas. Consulte la sección "NFSv4.1 y el usuario/grupo nadie" para obtener información sobre este problema y cómo resolverlo.

Control de accesos/exportaciones

El acceso inicial a las exportaciones y recursos compartidos para montajes NFS se controla mediante reglas de la política de exportación basadas en host contenidas en una política de exportación. Se define una IP de host, nombre de host, subred, netgroup o dominio para permitir el acceso al montaje del recurso compartido de NFS y el nivel de acceso permitido al host. Las opciones de configuración de las reglas de política de exportación dependen del nivel de Cloud Volumes Service.

Para CVS-SW, hay disponibles las siguientes opciones para la configuración de la política de exportación:

- **Coincidencia de cliente.** Lista de direcciones IP separadas por comas, lista separada por comas de nombres de host, subredes, grupos de red, nombres de dominio.
- **Reglas de acceso RO/RW.** Seleccione sólo lectura/escritura o lectura para controlar el nivel de acceso a la exportación.CVS-Performance ofrece las siguientes opciones:
- **Coincidencia de cliente.** Lista de direcciones IP separadas por comas, lista separada por comas de nombres de host, subredes, grupos de red, nombres de dominio.
- **Reglas de acceso RO/RW.** Seleccione sólo lectura/escritura o lectura para controlar el nivel de acceso a la exportación.
- **Acceso raíz (on/OFF).** configura el squash raíz (consulte la sección "El usuario raíz" para obtener más información).
- **Tipo de protocolo.** esto limita el acceso al montaje NFS a una versión específica del protocolo. Cuando se especifican NFSv3 y NFSv4.1 para el volumen, deje las dos casillas en blanco o marque ambas.
- **Nivel de seguridad de Kerberos (cuando se selecciona Enable Kerberos).** proporciona las opciones de krb5, krb5i y/o krb5p para acceso de solo lectura o de lectura/escritura.

Cambiar la propiedad (chown) y cambiar el grupo (chgrp)

NFS en Cloud Volumes Service sólo permite al usuario raíz ejecutar chown/chgrp en archivos y carpetas. Otros usuarios ven a. `Operation not permitted` error: incluso en los archivos que poseen. Si utiliza la

raíz de squash (como se describe en la sección “El usuario raíz”), la raíz está ocupada para un usuario que no es raíz y no se permite el acceso a chown y chgrp. Actualmente no hay soluciones alternativas en Cloud Volumes Service para permitir chown y chgrp para usuarios no raíz. Si se requieren cambios de propiedad, considere usar volúmenes de protocolo dual y establezca el estilo de seguridad en NTFS para controlar los permisos del lado de Windows.

Gestión de permisos

Cloud Volumes Service admite ambos bits de modo (como 644, 777, etc. para rwx) y ACL de NFSv4.1 para controlar los permisos de los clientes NFS de los volúmenes que utilicen el estilo de seguridad UNIX. La gestión de permisos estándar se utiliza para estos (como chmod, chown o nfs4_setfacl) y funciona con cualquier cliente Linux que los admita.

Además, cuando se usan volúmenes de protocolo dual establecidos en NTFS, los clientes NFS pueden aprovechar la asignación de nombres Cloud Volumes Service a usuarios de Windows, que se utilizan para resolver los permisos NTFS. Esto requiere una conexión LDAP a Cloud Volumes Service para proporcionar traducciones de ID-a-nombre de usuario numérico porque Cloud Volumes Service requiere un nombre de usuario UNIX válido para asignar correctamente a un nombre de usuario de Windows.

Proporcionar ACL granulares para NFSv3

Los permisos de bit de modo solo cubren al propietario, al grupo y a todos los demás en la semántica, lo que significa que no hay controles de acceso de usuario granulares disponibles para NFSv3 básico. Cloud Volumes Service no admite ACL de POSIX, ni atributos extendidos (como chattr), de modo que las listas de control de acceso granulares solo son posibles en los siguientes escenarios con NFSv3:

- Volúmenes de estilo de seguridad NTFS (servidor CIFS necesario) con asignaciones de usuarios de UNIX a Windows válidas.
- Las ACL de NFSv4.1 se aplican mediante el montaje de NFSv4.1 en un cliente de administrador para aplicar ACL.

Ambos métodos requieren una conexión LDAP para la administración de identidades de UNIX y una información de grupo y usuario de UNIX válida rellenada (consulte la sección ""LDAP"") Y sólo están disponibles con las instancias CVS-Performance. Para utilizar volúmenes de estilo de seguridad NTFS con NFS, debe utilizar el protocolo dual (SMB y NFSv3) o el protocolo doble (SMB y NFSv4.1), incluso si no se realiza ninguna conexión SMB. Para utilizar las ACL de NFSv4.1 con montajes NFSv3, debe seleccionar `Both (NFSv3/NFSv4.1)` como tipo de protocolo.

Los bits del modo UNIX normal no proporcionan el mismo nivel de granularidad en permisos que proporcionan las ACL de NTFS o NFSv4.x. En la siguiente tabla, se compara la granularidad de permisos entre bits del modo NFSv3 y ACL de NFSv4.1. Para obtener más información sobre las ACL de NFSv4.1, consulte "Nfs4_acl - Listas de control de acceso de NFSv4".

Bits del modo NFSv3	ACL de NFSv4.1
• Defina el ID de usuario en la ejecución • Establezca el ID de grupo en la ejecución • Guardar texto intercambiado (no definido en POSIX) • Permiso de lectura para el propietario • Permiso de escritura para el propietario • Ejecutar permiso para el propietario en un archivo; o buscar (buscar) permiso para el propietario en el directorio • Permiso de lectura para grupo • Permiso de escritura para grupo • Ejecutar permiso para grupo en un archivo o buscar (buscar) permiso para grupo en el directorio • Permiso de lectura para otros • Permiso de escritura para otros • Ejecutar permiso para otros usuarios en un archivo; o buscar (buscar) permiso para otros en el directorio	Tipos de entrada de control de acceso (ACE) (permitir/Denegar/Auditoría) * indicadores de herencia * directorio-heredar * archivo-heredar * no-propagar-heredar * heredar-sólo Permisos * datos de lectura (archivos) / directorio de lista (directorios) * escribir-datos (archivos) / crear-archivo (directorios) * anexar-datos (archivos) / subdirectorio de creación (directorios) * ejecutar (archivos) / cambiar-directorio (directorios) * eliminar * eliminar-hijo * atributos de lectura-escritura * escribir-atributos * atributos-ACL de lectura-escritura * Sincronizar-escritura-escritura-propietario * ACL

Por último, la pertenencia a grupos de NFS (tanto en NFSv3 COMO EN NFSV4.x) está limitada a un máximo predeterminado de 16 para AUTH_SYS según los límites de paquetes RPC. NFS Kerberos proporciona hasta 32 grupos y las ACL de NFSv4 eliminan la limitación a través de ACL granulares de usuarios y grupos (hasta 1024 entradas por ACE).

Además, Cloud Volumes Service ofrece compatibilidad ampliada con grupos para ampliar el número máximo de grupos admitidos hasta 32. Esto requiere una conexión LDAP a un servidor LDAP que contenga identidades de grupo y de usuario UNIX válidas. Para obtener más información acerca de cómo configurar esto, consulte "Crear y gestionar volúmenes de NFS" En la documentación de Google.

ID de usuario y grupo de NFSv3

Los ID de usuario y de grupo de NFSv3 se encuentran en el cable como identificadores numéricos en lugar de como nombres. Cloud Volumes Service no soluciona el nombre de usuario de estos ID numéricos con NFSv3, con los volúmenes de estilo de seguridad de UNIX que utilizan únicamente bits del modo. Cuando hay ACL de NFSv4.1, es necesario realizar una búsqueda de ID numéricos y/o una búsqueda de cadenas de nombre para resolver la ACL correctamente, incluso cuando se utiliza NFSv3. Con volúmenes de estilo de seguridad NTFS, Cloud Volumes Service debe resolver un ID numérico a un usuario UNIX válido y, a continuación, asignar a un usuario de Windows válido para negociar derechos de acceso.

Limitaciones de seguridad de los ID de usuario y de grupo de NFSv3

Con NFSv3, el cliente y el servidor nunca tienen que confirmar que el usuario que intenta leer o escribir con un ID numérico es un usuario válido; sólo es de confianza implícita. Esto abre el sistema de archivos hasta posibles infracciones simplemente falsificar cualquier ID numérico. Para evitar agujeros de seguridad como este, hay algunas opciones disponibles para Cloud Volumes Service.

- La implementación de Kerberos para NFS obliga a los usuarios a autenticarse con un nombre de usuario y contraseña o un archivo keytab a obtener un vale Kerberos para permitir el acceso a un montaje. Kerberos solo está disponible con las instancias CVS-Performance y con NFSv4.1.
- Limitar la lista de hosts de las reglas de la política de exportación los límites que los clientes NFSv3 tienen acceso al volumen de Cloud Volumes Service.
- El uso de volúmenes de protocolo doble y la aplicación de ACL NTFS a los volúmenes obliga a los clientes NFSv3 a resolver los ID numéricos a nombres de usuario de UNIX válidos para autenticar correctamente el acceso a los montajes. Esto requiere habilitar LDAP y configurar las identidades de usuarios y grupos de UNIX.
- Al SQUID el usuario raíz limita el daño que un usuario raíz puede hacer a un montaje NFS, pero no elimina por completo el riesgo. Para obtener más información, consulte la sección “El usuario raíz.”

En última instancia, la seguridad de NFS se limita a qué versión del protocolo utiliza que ofrece. NFSv3, aunque tiene un rendimiento general superior al de NFSv4.1, no proporciona el mismo nivel de seguridad.

NFSv4.1

NFSv4.1 proporciona una mayor seguridad y fiabilidad en comparación con NFSv3, por los siguientes motivos:

- Bloqueo integrado mediante un mecanismo basado en arrendamiento
- Sesiones con estado
- Todas las funciones de NFS en un único puerto (2049)
- Solo TCP
- Asignación de dominio de ID
- Integración de Kerberos (NFSv3 puede utilizar Kerberos, pero solo para NFS, no para protocolos auxiliares como NLM)

Dependencias de NFSv4.1

Debido a las funciones de seguridad adicionales de NFSv4.1, existen algunas dependencias externas implicadas que no fueron necesarias para utilizar NFSv3 (de forma similar a cómo requiere SMB dependencias como Active Directory).

ACL de NFSv4.1

Cloud Volumes Service ofrece compatibilidad con las ACL de NFSv4.x, las cuales proporcionan ventajas distintivas con respecto a los permisos de estilo POSIX normales, como las siguientes:

- Control granular del acceso de los usuarios a los archivos y directorios
- Mejor seguridad NFS
- Interoperabilidad mejorada con CIFS/SMB
- Eliminación de la limitación NFS de 16 grupos por usuario con seguridad AUTH_SYS
- Los ACL omiten la necesidad de resolución del identificador de grupo (GID), que elimina en realidad las ACL de GID limititNFSv4.1 se controlan desde clientes NFS, no desde Cloud Volumes Service. Para utilizar las ACL de NFSv4.1, asegúrese de que la versión de software de su cliente las admite y de que están instaladas las utilidades NFS adecuadas.

Compatibilidad entre las ACL de NFSv4.1 y los clientes de SMB

Las ACL de NFSv4 son distintas de las de ACL de nivel de archivo de Windows (ACL de NTFS), pero llevan funciones similares. Sin embargo, en los entornos NAS multiprotocolo, si hay ACL de NFSv4.1 y utiliza acceso de doble protocolo (NFS y SMB en los mismos conjuntos de datos), los clientes que utilicen SMB2.0 y versiones posteriores no podrán ver ni gestionar ACL desde pestañas de seguridad de Windows.

Cómo funcionan las ACL de NFSv4.1

Como referencia, se definen los siguientes términos:

- **Lista de control de acceso (ACL).** una lista de entradas de permisos.
- **Entrada de control de acceso (ACE).** Entrada de permiso en la lista.

Cuando un cliente establece una ACL de NFSv4.1 en un archivo durante una operación SETATTR, Cloud Volumes Service establece esa ACL en el objeto, por lo que se sustituye cualquier ACL existente. Si no hay ACL en un archivo, los permisos de modo en el archivo se calculan a partir de OWNER@, GROUP@ y EVERYONE@. Si hay algún bit SUID/SGID/STICKY existente en el archivo, no se verán afectados.

Cuando un cliente obtiene una ACL de NFSv4.1 en un archivo durante UNA operación GETATTR, Cloud Volumes Service lee la ACL de NFSv4.1 asociada con el objeto, construye una lista de ACE y devuelve la lista al cliente. Si el archivo tiene una ACL de NT o bits de modo, se crea una ACL a partir de bits de modo y se devuelve al cliente.

Se deniega el acceso si EXISTE UNA ACE DENEGADA en la ACL; el acceso se concede si existe una ACE DE PERMISO. Sin embargo, también se deniega el acceso si ninguno de los ACE está presente en el ACL.

Un descriptor de seguridad consiste en una ACL de seguridad (SACL) y una ACL discrecional (DACL). Cuando NFSv4.1 interactúa con CIFS/SMB, el DACL se asigna de uno a uno con NFSv4 y CIFS. El DACL consta de LOS ACs PERMITIR Y DENEGAR.

Si es un básico `chmod` Se ejecuta en un archivo o carpeta con conjuntos de ACL de NFSv4.1, se conservan las ACL de usuario y grupo existentes, pero se modifican las ACL de PROPIETARIO@, GRUPO@ y TODOS@ predeterminadas.

Un cliente que utilice las ACL de NFSv4.1 puede definir y ver ACL de archivos y directorios en el sistema. Cuando se crea un archivo o subdirectorio nuevo en un directorio que tiene una ACL, ese objeto hereda todos los ACE de la ACL que se han etiquetado con el correspondiente "indicadores de herencia".

Si un archivo o directorio tiene una ACL de NFSv4.1, esa ACL se utiliza para controlar el acceso, independientemente de qué protocolo se utilice para acceder al archivo o directorio.

Los archivos y directorios heredan los ACE de las ACL de NFSv4 en directorios principales (posiblemente con las modificaciones adecuadas) siempre que se hayan etiquetado los ACE con las marcas de herencia correctas.

Cuando se crea un archivo o directorio como resultado de una solicitud de NFSv4, la ACL del archivo o directorio resultante depende de si la solicitud de creación de archivos incluye una ACL o solo permisos de acceso estándar a archivos UNIX. La ACL también depende de si el directorio primario tiene una ACL.

- Si la solicitud incluye una ACL, se utiliza esa ACL.
- Si la solicitud incluye sólo permisos de acceso estándar a archivos UNIX y el directorio principal no tiene una ACL, el modo de archivo de cliente se utiliza para establecer permisos de acceso estándar a archivos UNIX.

- Si la solicitud incluye sólo permisos de acceso estándar a archivos UNIX y el directorio primario tiene una ACL no heredable, se establece una ACL predeterminada basada en los bits de modo pasados a la solicitud en el nuevo objeto.
- Si la solicitud incluye sólo permisos de acceso estándar a archivos UNIX pero el directorio principal tiene una ACL, el archivo o directorio nuevos heredan los ACE de la ACL del directorio principal siempre que se hayan etiquetado los ACE con los indicadores de herencia correspondientes.

Permisos ACE

Los permisos de ACL de NFSv4.1 utilizan una serie de valores de letras mayúsculas y minúsculas (como `rxtncy`) para controlar el acceso. Para obtener más información acerca de estos valores de letra, consulte "CÓMO: Utilizar NFSv4 ACL".

Comportamiento de ACL de NFSv4.1 con herencia umask y ACL

"Las ACL de NFSv4 proporcionan la capacidad de ofrecer herencia de ACL". La herencia de ACL significa que los archivos o carpetas creados debajo de los objetos con conjuntos de ACL de NFSv4.1 pueden heredar las ACL según la configuración de "Indicador de herencia de ACL".

"Umask" se utiliza para controlar el nivel de permisos en el que se crean archivos y carpetas en un directorio sin interacción del administrador. De forma predeterminada, Cloud Volumes Service permite a umask reemplazar las ACL heredadas, que es el comportamiento esperado según "RFC 5661".

Formato de ACL

Las ACL de NFSv4.1 tienen formato específico. El ejemplo siguiente es un conjunto ACE en un archivo:

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

El ejemplo anterior sigue las directrices de formato ACL de:

```
type:flags:principal:permissions
```

Tipo de `A` significa “permitir”. Los indicadores heredar no se establecen en este caso, porque el principal no es un grupo y no incluye la herencia. Además, como ACE no es una entrada DE AUDITORÍA, no es necesario establecer los indicadores de auditoría. Para obtener más información sobre las ACL de NFSv4.1, consulte "http://linux.die.net/man/5/nfs4_acl".

Si la ACL de NFSv4.1 no se establece correctamente (o el cliente y el servidor no pueden resolver una cadena de nombre), es posible que la ACL no se comporte como se espera o que el cambio de ACL no se pueda aplicar y generar un error.

Los errores de muestra son los siguientes:

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

RECHAZO explícito

Los permisos de NFSv4.1 pueden incluir atributos DE DENEGACIÓN explícitos para EL PROPIETARIO, EL GRUPO Y TODOS. Esto se debe a que las ACL de NFSv4.1 son denegadas por defecto, lo que significa que si un ACE no concede explícitamente una ACL, se deniega. Los atributos DE DENEGACIÓN explícita anulan cualquier ACE de ACCESO, explícita o no.

DENEGAR ACE se establece con una etiqueta de atributo de `D`.

En el siguiente ejemplo, SE permite a GROUP@ todos los permisos de lectura y ejecución, pero se le deniega todo el acceso de escritura.

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

DENEGAR ACs debe evitarse siempre que sea posible porque pueden ser confusos y complicados; PERMITIR que las ACL que no están definidas explícitamente se deniegan implícitamente. Cuando SE establecen LAS ACE DENEGADAS, es posible que se deniegue el acceso a los usuarios cuando esperan que se les conceda el acceso.

El conjunto anterior de ACE es equivalente a 755 bits de modo, lo que significa:

- El propietario tiene derechos completos.
- Los grupos tienen sólo lectura.
- Otros sólo han leído.

Sin embargo, incluso si los permisos se ajustan al equivalente de 775, se puede denegar el acceso debido a LA DENEGACIÓN explícita establecida en TODOS.

Dependencias de asignación de dominio de ID de NFSv4.1

NFSv4.1 aprovecha la lógica de asignación de dominio de ID como capa de seguridad para ayudar a verificar que un usuario que intenta acceder a un montaje de NFSv4.1 es realmente lo que afirman que es. En estos casos, el nombre de usuario y el nombre del grupo que provienen del cliente NFSv4.1 anexa una cadena de nombres y la envía a la instancia de Cloud Volumes Service. Si esa combinación de nombre de usuario/grupo y cadena de ID no coincide, el usuario y/o grupo se utiliza en la función no se define ningún usuario por defecto en la `/etc/idmapd.conf` archivo en el cliente.

Esta cadena de ID es un requisito para la observancia correcta de los permisos, especialmente cuando se utilizan las ACL de NFSv4.1 y/o Kerberos. Como resultado, las dependencias del servidor del servicio de nombres, como los servidores LDAP, son necesarias para garantizar la coherencia entre los clientes y la Cloud Volumes Service con el fin de resolver correctamente la identidad de nombres de usuario y grupo.

Cloud Volumes Service utiliza un valor de nombre de dominio de ID predeterminado estático de `defaultv4iddomain.com`. Los clientes NFS utilizan de forma predeterminada el nombre de dominio DNS

para la configuración de nombre de dominio ID, pero puede ajustar manualmente el nombre de dominio ID en `/etc/idmapd.conf`.

Si LDAP está habilitado en Cloud Volumes Service, Cloud Volumes Service automatiza el dominio de identificador de NFS para cambiar a lo que está configurado para el dominio de búsqueda en DNS y los clientes no tendrán que modificarse a menos que utilicen nombres de búsqueda de dominio DNS diferentes.

Cuando Cloud Volumes Service puede resolver un nombre de usuario o de grupo en archivos locales o LDAP, se utiliza la cadena de dominio y los ID de dominio no coincidentes no se pueden squash a nadie. Si Cloud Volumes Service no puede encontrar un nombre de usuario o nombre de grupo en los archivos locales o LDAP, se utiliza el valor de ID numérico y el cliente NFS resuelve el nombre correctamente (esto es similar al comportamiento de NFSv3).

Sin cambiar el dominio de Id. De NFSv4.1 del cliente para que coincida con el uso del volumen de Cloud Volumes Service, verá el siguiente comportamiento:

- Los usuarios y grupos UNIX con entradas locales en Cloud Volumes Service (como root, tal como se define en los usuarios y grupos locales de UNIX) se utilizan en el valor nobody.
- Los usuarios y grupos de UNIX con entradas en LDAP (si Cloud Volumes Service está configurado para usar LDAP) no se conectan a nadie si los dominios DNS son diferentes entre los clientes NFS y Cloud Volumes Service.
- Los usuarios y grupos de UNIX que no tienen entradas locales ni entradas LDAP utilizan el valor de ID numérico y resuelven el nombre especificado en el cliente NFS. Si no existe ningún nombre en el cliente, sólo se muestra el ID numérico.

A continuación se muestran los resultados de la situación anterior:

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835   9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

Cuando los dominios de ID de cliente y servidor coinciden, así es como el mismo aspecto del listado de archivos:

```
# ls -la
total 8
drwxr-xr-x 2 root   root         4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root         4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835         9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache apache-group    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root            0 Feb  3 12:06 root-user-file
```

Para obtener más información acerca de este problema y cómo resolverlo, consulte la sección “NFSv4.1 y el usuario/grupo nadie.”

Dependencias de Kerberos

Si va a utilizar Kerberos con NFS, debe tener lo siguiente con Cloud Volumes Service:

- Dominio de Active Directory para servicios del centro de distribución Kerberos (KDC)
- Dominio de Active Directory con atributos de usuario y grupo rellenados con información de UNIX para la funcionalidad LDAP (NFS Kerberos en Cloud Volumes Service requiere un SPN de usuario a la asignación de usuarios UNIX para una funcionalidad adecuada).
- LDAP habilitado en la instancia de Cloud Volumes Service
- Dominio de Active Directory para servicios DNS

NFSv4.1 y el usuario/grupo nadie

Uno de los problemas más comunes que se ven con una configuración de NFSv4.1 es cuando se muestra un archivo o una carpeta en un listado mediante `ls` como propiedad de la `user:group` combinación de `nobody:nobody`.

Por ejemplo:

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

Y el ID numérico es `99`.

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

En algunos casos, es posible que el archivo muestre el propietario correcto pero `nobody` como grupo.

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

¿Quién no es nadie?

La `nobody` El usuario de NFSv4.1 es diferente del `nfsnobody` usuario. Puede ver cómo un cliente NFS ve cada usuario ejecutando el `id` comando:

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

Con NFSv4.1, el `nobody` user es el usuario predeterminado definido por `idmapd.conf` file y puede definirse como cualquier usuario que desee utilizar.

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

¿Por qué sucede esto?

Puesto que la seguridad mediante la asignación de cadenas de nombres es un conjunto de claves de las operaciones de NFSv4.1, el comportamiento predeterminado cuando una cadena de nombres no coincide correctamente es squash a ese usuario con uno que normalmente no tendrá acceso a los archivos y carpetas que pertenecen a usuarios y grupos.

Cuando vea `nobody` Para el usuario o el grupo de los listados de archivos, esto generalmente significa que hay algo configurado para NFSv4.1. Aquí puede entrar en juego la sensibilidad del caso.

Por ejemplo, si usuario1@CVSDEMO.LOLARL (uid 1234, gid 1234) está accediendo a una exportación, entonces Cloud Volumes Service debe ser capaz de encontrar usuario1@CVSDEMO.LOLARL (uid 1234, gid 1234). Si el usuario en Cloud Volumes Service es USER1@CVSDEMO.LLOLex, entonces no coincidiría (USUARIO1 en mayúscula frente al usuario en minúscula 1). En muchos casos, puede ver lo siguiente en el archivo de mensajes del cliente:

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDEMO.LOCAL'
```

Tanto el cliente como el servidor deben estar de acuerdo en que un usuario es realmente quien afirma que es, por lo que debe comprobar lo siguiente para asegurarse de que el usuario que ve el cliente tiene la misma información que el usuario que ve Cloud Volumes Service.

- **Dominio de ID NFSv4.x.** Cliente: `idmapd.conf` Archivo; utiliza Cloud Volumes Service `defaultv4iddomain.com` y no se puede cambiar manualmente. Si se utiliza LDAP con NFSv4.1, Cloud Volumes Service cambia el dominio de ID por lo que utiliza el dominio de búsqueda DNS, que es el mismo que el dominio de AD.
- **Nombre de usuario e ID numéricos.** esto determina dónde busca el cliente los nombres de usuario y aprovecha la configuración del conmutador de servicio de nombres—cliente: `nsswitch.conf` Y/o archivos locales passwd y group; Cloud Volumes Service no permite modificaciones a esto pero agrega automáticamente LDAP a la configuración cuando está habilitado.
- **Nombre del grupo e ID numéricos.** esto determina dónde está buscando el cliente los nombres de grupo y aprovecha la configuración del conmutador de servicio de nombres—cliente: `nsswitch.conf` Y/o archivos locales passwd y group; Cloud Volumes Service no permite modificaciones a esto pero agrega automáticamente LDAP a la configuración cuando está habilitado.

En casi todos los casos, si ve `nobody` En las listas de usuarios y grupos de clientes, el problema es la traducción de ID de dominio de nombre de usuario o grupo entre Cloud Volumes Service y el cliente NFS. Para evitar esta situación, use LDAP para resolver la información de usuario y grupo entre los clientes y Cloud Volumes Service.

Ver cadenas de ID de nombres para NFSv4.1 en clientes

Si utiliza NFSv4.1, hay una asignación de cadena de nombre que se realiza durante las operaciones de NFS, como se ha descrito anteriormente.

Además de utilizar `/var/log/messages` Para encontrar un problema con los ID de NFSv4, puede utilizar la "nfsidmap -l" Comando en el cliente NFS para ver los nombres de usuario que se han asignado correctamente al dominio de NFSv4.

Por ejemplo, se trata del resultado del comando después de que un usuario que puede encontrar el cliente y Cloud Volumes Service accede a un montaje NFSv4.x:

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

Cuando un usuario que no se asigna correctamente al dominio de ID de NFSv4.1 (en este caso, `netapp-user`) intenta acceder al mismo montaje y toca un archivo, están asignados `nobody:nobody`, según lo esperado.

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root   root   4096 Jan 14 17:13 .
drwxr-xr-x. 8 root   root     81 Jan 14 10:02 ..
-rw-r--r--  1 nobody nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root   root   4096 Jan 13 13:20 qtree1
drwxrwxrwx  2 root   root   4096 Jan 13 13:13 qtree2
drwxr-xr-x  2 nfs4   daemon 4096 Jan 11 14:30 testdir
```

La `nfsidmap -l` salida muestra al usuario `pcuser` en la pantalla pero no `netapp-user`; éste es el usuario anónimo en nuestra regla de política de exportación (`65534`).

```
# nfsidmap -l
6 .id_resolver keys found:
  gid:pcuser@CVSDEMO.LOCAL
  uid:pcuser@CVSDEMO.LOCAL
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

SMB

"SMB" Es un protocolo de uso compartido de archivos de red desarrollado por Microsoft que proporciona autenticación centralizada de usuarios/grupos, permisos, bloqueo y uso compartido de archivos a varios clientes SMB a través de una red Ethernet. Los archivos y carpetas se presentan a los clientes mediante recursos compartidos, que pueden configurarse con diversas propiedades de recursos compartidos y ofrecen control de acceso mediante permisos de nivel de recursos compartidos. SMB puede presentarse a cualquier cliente que ofrezca compatibilidad con el protocolo, incluidos clientes de Windows, Apple y Linux.

Cloud Volumes Service es compatible con las versiones SMB 2.1 y 3.x del protocolo.

Control de acceso/recursos compartidos de SMB

- Cuando un nombre de usuario de Windows solicita acceso al volumen Cloud Volumes Service, Cloud Volumes Service busca un nombre de usuario UNIX utilizando los métodos configurados por los administradores de Cloud Volumes Service.
- Si se configura un proveedor de identidad UNIX externo (LDAP) y los nombres de usuario de Windows/UNIX son idénticos, entonces los nombres de usuario de Windows asignarán 1:1 a nombres de usuario de UNIX sin necesidad de ninguna configuración adicional. Cuando LDAP está habilitado, Active Directory se utiliza para alojar esos atributos UNIX para objetos de grupo y usuario.
- Si los nombres de Windows y UNIX no coinciden de la misma manera, se debe configurar LDAP para permitir que Cloud Volumes Service utilice la configuración de asignación de nombres LDAP (consulte la sección ""Utilizar LDAP para asignar nombres asimétricos"").
- Si LDAP no está en uso, los usuarios SMB de Windows se asignan a un usuario UNIX local predeterminado denominado `pcuser` En Cloud Volumes Service. Esto significa que los usuarios que se asignan a los archivos escritos en Windows `pcuser` Mostrar propiedad de UNIX como `pcuser` En entornos NAS multiprotocolo. `pcuser` aquí está efectivamente la `nobody` Usuario en entornos Linux (UID 65534).

En implementaciones con solo SMB, el `pcuser` La asignación se sigue produciendo, pero no importa, porque la propiedad de usuarios y grupos de Windows se muestra correctamente y no se permite el acceso NFS al volumen sólo para SMB. Además, los volúmenes solo para SMB no admiten la conversión a volúmenes de protocolo doble o NFS después de crearse.

Windows utiliza Kerberos para la autenticación de nombre de usuario con los controladores de dominio de Active Directory, que requiere un intercambio de nombre de usuario/contraseña con los DC de AD, que es

externo a la instancia de Cloud Volumes Service. La autenticación Kerberos se utiliza cuando el `\\SERVERNAME` Los clientes SMB utilizan la ruta UNC que es la siguiente:

- Existe una entrada DNS A/AAAA para SERVERNAME
- Existe un SPN válido para el acceso SMB/CIFS para SERVERNAME

Cuando se crea un volumen SMB de Cloud Volumes Service, se crea el nombre de la cuenta de la máquina, tal como se define en la sección ""Cómo aparece Cloud Volumes Service en Active Directory."" Ese nombre de cuenta de equipo también se convierte en la ruta de acceso a recursos compartidos SMB porque Cloud Volumes Service aprovecha DNS dinámico (DDNS) para crear las entradas A/AAAA y PTR necesarias en DNS y las entradas SPN necesarias en el principal de cuenta de máquina.

> Para crear entradas PTR, la zona de búsqueda inversa para la dirección IP de la instancia Cloud Volumes Service debe existir en el servidor DNS.

Por ejemplo, este volumen Cloud Volumes Service utiliza la siguiente ruta de uso compartido UNC: `\\cvs-east- 433d.cvsdemo.local`.

En Active Directory, estas son las entradas de SPN generadas por el servicio Cloud Volumes:

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

Este es el resultado de búsqueda directa/inversa de DNS:

```
PS C:\> nslookup CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    CVS-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

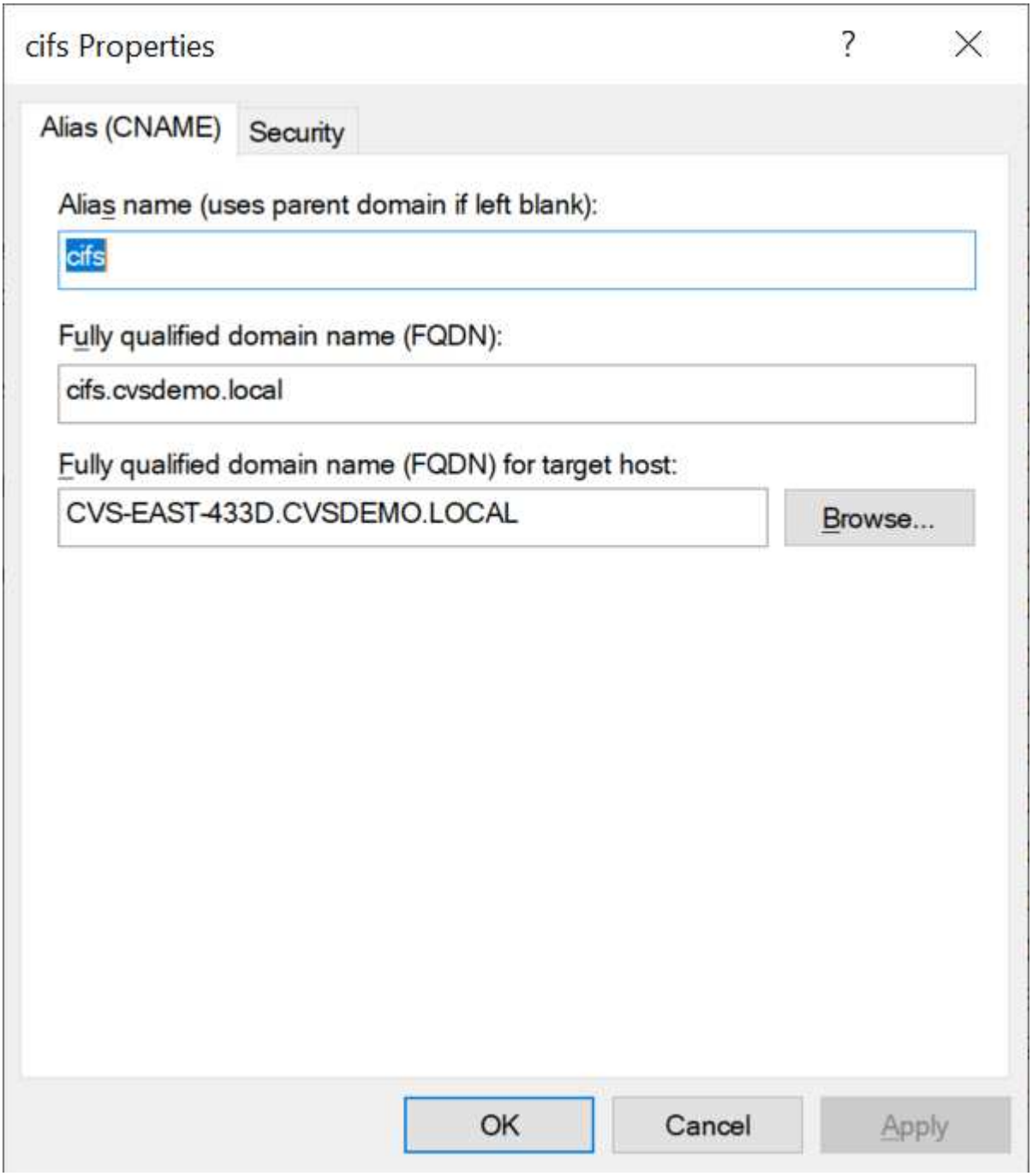
De manera opcional, se puede aplicar un mayor control de acceso al habilitar o requerir el cifrado SMB para recursos compartidos SMB en Cloud Volumes Service. Si uno de los extremos no admite el cifrado SMB, no se permite el acceso.

Usar alias de nombre de SMB

En algunos casos, podría ser una preocupación de seguridad para los usuarios finales saber el nombre de la cuenta de equipo que se está utilizando para Cloud Volumes Service. En otros casos, es posible que simplemente desee proporcionar una ruta de acceso más sencilla a sus usuarios finales. En esos casos, puede crear alias SMB.

Si desea crear alias para la ruta de acceso compartida SMB, puede aprovechar lo que se conoce como registro CNAME en DNS. Por ejemplo, si desea usar el nombre `\\CIFS` para acceder a los recursos

compartidos en lugar de `\\cvs-east- 433d.cvsdemo.local`, Pero todavía desea utilizar la autenticación Kerberos, un CNAME en DNS que señala al registro A/AAAA existente y un SPN adicional agregado a la cuenta de equipo existente proporciona acceso Kerberos.



Este es el resultado de búsqueda directa de DNS resultante después de agregar un CNAME:

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

Esta es la consulta SPN resultante tras agregar nuevos números de dominio:

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        cifs/cifs.cvsdemo.local
        cifs/cifs
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

En una captura de paquete, podemos ver la solicitud de configuración de sesión mediante el SPN vinculado al CNAME.

```
431 4.156722                                    SMB2    308 Negotiate Protocol Response
432 4.156785                                    SMB2    232 Negotiate Protocol Request
434 4.158108                                    SMB2    374 Negotiate Protocol Response
435 4.160977                                    SMB2   1978 Session Setup Request
437 4.166224                                    SMB2    322 Session Setup Response
438 4.166891                                    SMB2    152 Tree Connect Request Tree: \\cifs\IPC$
439 4.168063                                    SMB2    138 Tree Connect Response

        realm: CVSDEMO.LOCAL
      ⌄ sname
          name-type: kRB5-NT-SRV-INST (2)
        ⌄ sname-string: 2 items
            SNameString: cifs
            SNameString: cifs
      ⌄ enc-part
          etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

Dialectos de autenticación SMB

Cloud Volumes Service admite lo siguiente "dialectos" Para la autenticación SMB:

- LM
- NTLM
- NTLMv2
- Kerberos

La autenticación Kerberos para acceso a recursos compartidos SMB es el nivel de autenticación más seguro que puede utilizar. Con el cifrado AES y SMB habilitado, el nivel de seguridad aumenta aún más.

Cloud Volumes Service también admite compatibilidad con versiones anteriores de la autenticación LM y NTLM. Cuando Kerberos está mal configurado (como al crear alias SMB), el acceso al recurso compartido vuelve a los métodos de autenticación más débiles (como NTLMv2). Debido a que estos mecanismos son menos seguros, se desactivan en algunos entornos de Active Directory. Si los métodos de autenticación más débiles están desactivados y Kerberos no está configurado correctamente, el acceso al recurso compartido

falla porque no hay ningún método de autenticación válido al que recurrir.

Para obtener información acerca de cómo configurar o ver los niveles de autenticación compatibles en Active Directory, consulte "Seguridad de red: Nivel de autenticación de LAN Manager".

Modelos de permisos

Permisos NTFS/Archivo

Los permisos NTFS son los permisos aplicados a archivos y carpetas en sistemas de archivos que cumplen la lógica NTFS. Puede aplicar permisos NTFS en `Basic` o. `Advanced` y se puede establecer en `Allow` o. `Deny` para control de acceso.

Los permisos básicos incluyen los siguientes:

- Control total
- Modificar
- Lectura y ejecución
- Lea
- Escritura

Cuando establece permisos para un usuario o grupo, denominado ACE, reside en una ACL. Los permisos NTFS utilizan los mismos conceptos básicos de lectura/escritura/ejecución que los bits de modo UNIX, pero también pueden extenderse a controles de acceso más granulares y extendidos (también conocidos como permisos especiales), como tomar posesión, Crear carpetas/datos anexados, escribir atributos, etc.

Los bits de modo UNIX estándar no proporcionan el mismo nivel de granularidad que los permisos NTFS (como ser capaz de establecer permisos para objetos de usuario y grupo individuales en una ACL o establecer atributos extendidos). Sin embargo, las ACL de NFSv4.1 proporcionan la misma funcionalidad que las ACL de NTFS.

Los permisos NTFS son más específicos que los permisos de uso compartido y se pueden utilizar junto con los permisos de uso compartido. Con las estructuras de permisos NTFS, se aplica el más restrictivo. Como tal, las denegaciones explícitas a un usuario o grupo anulan incluso Control total al definir los derechos de acceso.

Los permisos NTFS se controlan desde clientes SMB de Windows.

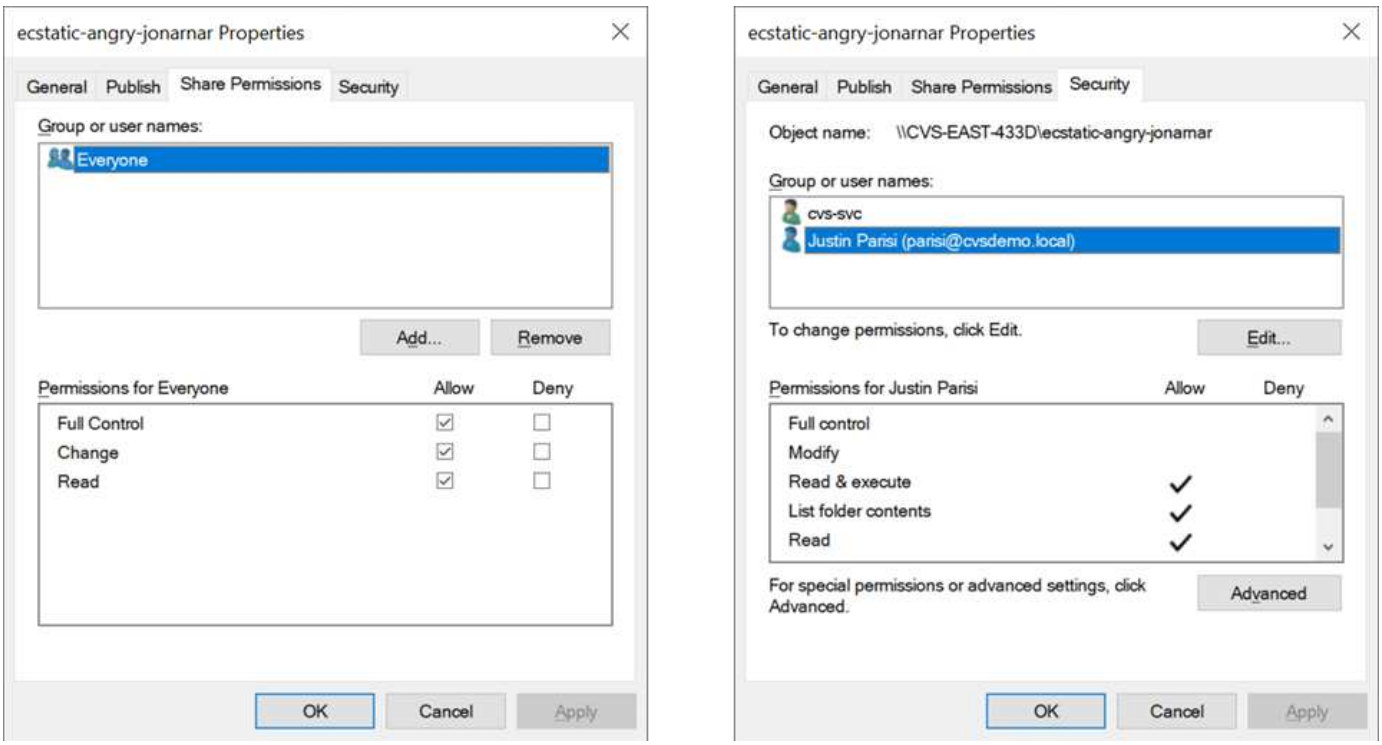
Comparta los permisos

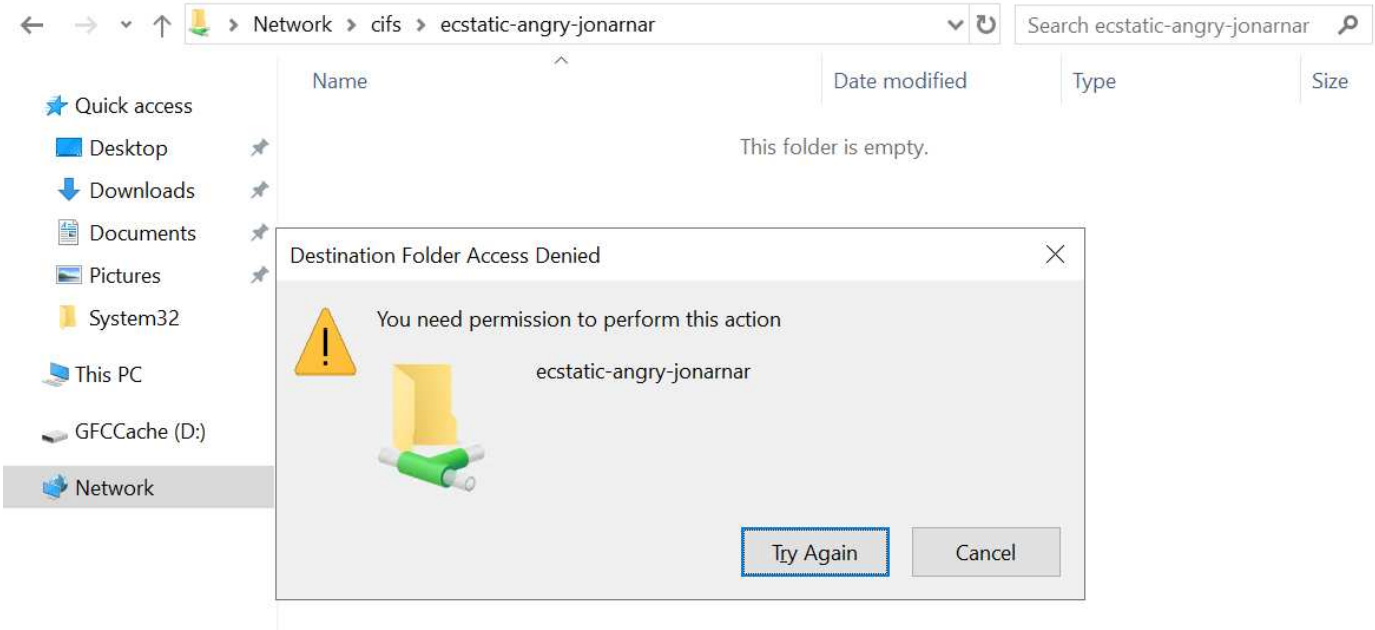
Los permisos de recursos compartidos son más generales que los permisos NTFS (sólo lectura/cambio/control total) y controlan la entrada inicial en un recurso compartido SMB, de forma similar a cómo funcionan las reglas de política de exportación NFS.

Si bien las reglas de política de exportación de NFS controlan el acceso mediante información basada en hosts, como direcciones IP o nombres de hosts, los permisos de uso compartido de SMB pueden controlar el acceso mediante ACE de usuario y de grupo en una ACL compartida. Puede configurar las ACL para compartir desde el cliente de Windows o desde la IU de gestión de Cloud Volumes Service.

De forma predeterminada, las ACL compartidas y las ACL de volumen inicial incluyen a todos los usuarios con control total. Las ACL de archivo se deben cambiar pero los permisos de uso compartido están anulados por los permisos de archivo de los objetos del recurso compartido.

Por ejemplo, si a un usuario solo se le permite acceso de lectura a la ACL del archivo de volumen Cloud Volumes Service, se les deniega el acceso para crear archivos y carpetas aunque la ACL de uso compartido esté establecida en todos los usuarios con control completo, como se muestra en la siguiente figura.





Para obtener los mejores resultados de seguridad, haga lo siguiente:

- Elimine a todos los usuarios de las ACL de uso compartido y de archivo y, en su lugar, establezca el acceso compartido para usuarios o grupos.
- Utilice grupos para controlar el acceso en lugar de usuarios individuales con el fin de facilitar la gestión y agilizar la incorporación/eliminación de usuarios para compartir ACL a través de la gestión de grupos.
- Permita un acceso compartido menos restrictivo y más general a los ACE en los permisos de uso compartido y bloquee el acceso a los usuarios y grupos con permisos de archivos para obtener un control

de acceso más granular.

- Evite el uso general de ACL de denegación explícita, ya que anulan permitir ACL. Limitar el uso de ACL de denegación explícita para usuarios o grupos que deben restringirse rápidamente del acceso a un sistema de archivos.
- Asegúrese de prestar atención al "Herencia de ACL" configuración al modificar los permisos; establecer el indicador de herencia en el nivel superior de un directorio o volumen con altos recuentos de archivos significa que cada archivo debajo de ese directorio o volumen ha heredado permisos que se le han agregado, que puede crear comportamientos no deseados como acceso no intencionado/denegación y pérdida prolongada de modificación de permisos a medida que se ajusta cada archivo.

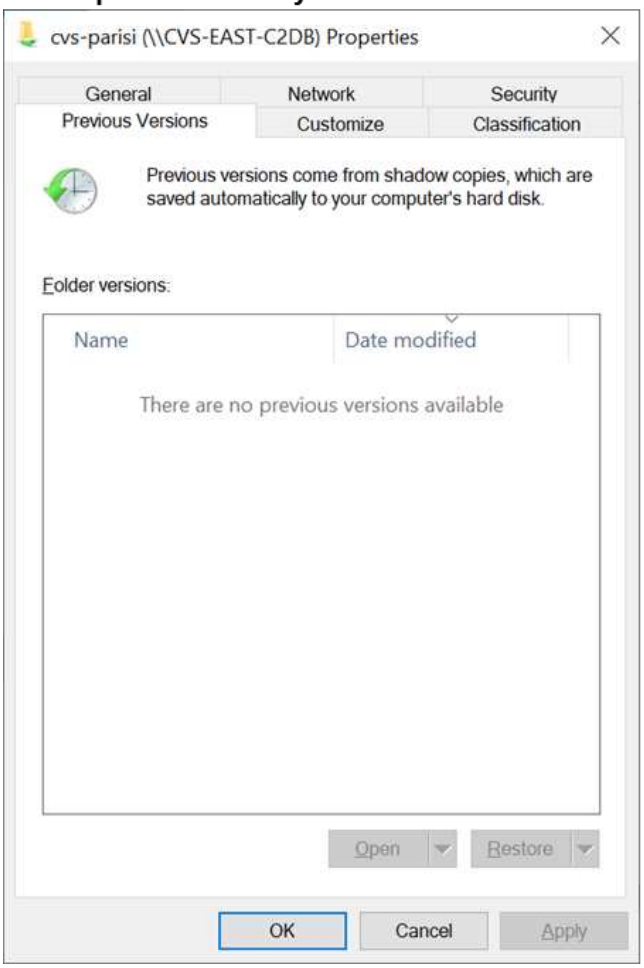
Funciones de seguridad para recursos compartidos de SMB

Cuando se crea por primera vez un volumen con acceso de SMB en Cloud Volumes Service, se presenta una serie de opciones para proteger ese volumen.

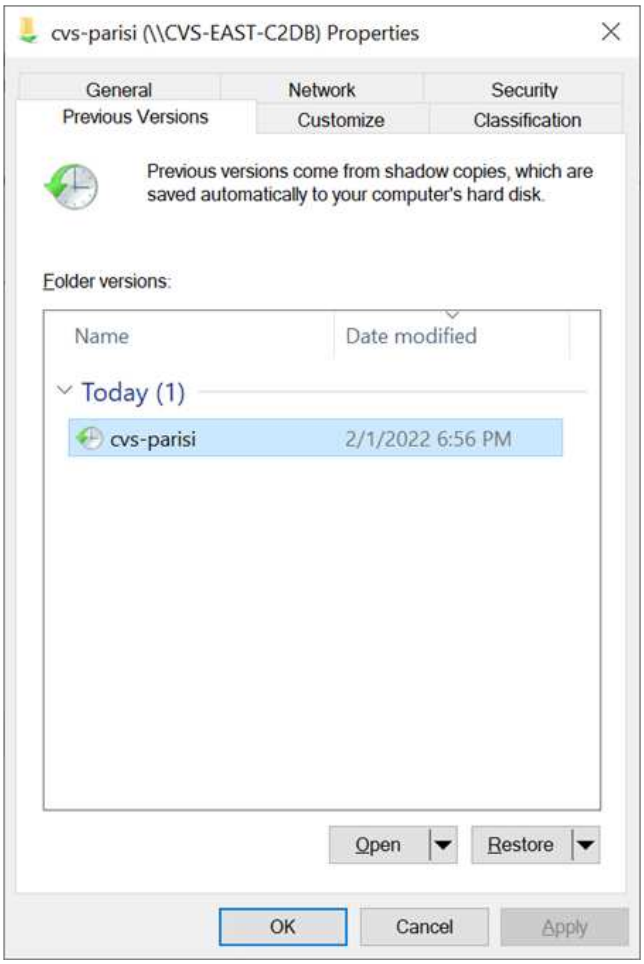
Algunas de estas opciones dependen del nivel de Cloud Volumes Service (rendimiento o software) y las opciones disponibles son:

- **Hacer visible el directorio de la instantánea (disponible tanto para CVS-Performance como para CVS-SW).** esta opción controla si los clientes de SMB pueden acceder al directorio de la instantánea en un recurso compartido de SMB (`\\server\share\~snapshot` Y/o la ficha versiones anteriores). La configuración predeterminada no está activada, lo que significa que el volumen se oculta y se despermite el acceso a la `~snapshot` y no aparecen copias Snapshot en la pestaña versiones anteriores del volumen.

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



Ocultar copias Snapshot de usuarios finales puede ser conveniente por motivos de seguridad, por motivos de rendimiento (ocultar estas carpetas de los análisis AV) o por preferencias. Las instantáneas Cloud Volumes Service son de sólo lectura, por lo que aunque estas Snapshots estén visibles, los usuarios finales no pueden eliminar ni modificar archivos en el directorio Snapshot. Se aplican permisos de archivo en los archivos o carpetas en el momento en que se realizó la copia snapshot. Si los permisos de un archivo o carpeta cambian entre copias Snapshot, los cambios también se aplican a los archivos o carpetas del directorio Snapshot. Los usuarios y grupos pueden obtener acceso a estos archivos o carpetas en función de los permisos. Aunque no es posible eliminar o modificar archivos del directorio Snapshot, es posible copiar archivos o carpetas fuera del directorio Snapshot.

- **Activar cifrado SMB (disponible tanto para CVS-Performance como para CVS-SW).** el cifrado SMB está desactivado en el recurso compartido SMB de forma predeterminada (sin seleccionar). Al activar la casilla se habilita el cifrado SMB, lo que significa que el tráfico entre el cliente SMB y el servidor se cifra en tránsito con los niveles de cifrado más altos admitidos negociados. Cloud Volumes Service admite hasta el cifrado AES-256 para SMB. La habilitación del cifrado SMB supone un detrimento del rendimiento que puede o no ser perceptible para sus clientes de SMB, aproximadamente en el rango de 10-20 %. NetApp recomienda encarecidamente realizar pruebas para ver si esa penalización en el rendimiento es aceptable.
- **Ocultar recurso compartido SMB (disponible tanto para CVS-Performance como para CVS-SW).** al establecer esta opción se oculta la ruta de acceso compartido SMB de la navegación normal. Esto significa que los clientes que no conocen la ruta de acceso al recurso compartido no pueden ver los recursos compartidos al acceder a la ruta UNC predeterminada (por ejemplo `\\CVS-SMB`). Cuando se selecciona la casilla de verificación, solo los clientes que conozcan explícitamente la ruta de acceso compartido SMB o que tengan la ruta de acceso de recurso compartido definida por un objeto de directiva

de grupo pueden tener acceso a ella (seguridad mediante ocultación).

- **Activar enumeración basada en acceso (ABE) (sólo CVS-SW).** esto es similar a ocultar el recurso compartido SMB, excepto que los recursos compartidos o archivos sólo están ocultos de usuarios o grupos que no tienen permisos para acceder a los objetos. Por ejemplo, si el usuario de Windows `joe` No se permite al menos acceso de lectura a través de los permisos, entonces el usuario de Windows `joe` No se pueden ver los archivos o recursos compartidos de SMB en absoluto. Esta opción está deshabilitada de forma predeterminada y puede habilitarla mediante la selección de la casilla de verificación. Para obtener más información sobre ABE, consulte el artículo de la base de conocimientos de NetApp "¿Cómo funciona la enumeración basada en acceso (ABE)?"
- **Activar soporte compartido de disponibilidad continua (CA) (CVS-Performance solamente).** "Recursos compartidos de SMB disponibles de forma continua" Proporcionar una forma de minimizar las interrupciones de aplicaciones durante eventos de conmutación por error mediante la replicación de estados de bloqueo entre nodos del sistema de entorno de administración de Cloud Volumes Service. Esta no es una función de seguridad, pero sí ofrece una mejor resiliencia general. Actualmente, sólo se admiten las aplicaciones SQL Server y FSLogix para esta funcionalidad.

Recursos compartidos ocultos predeterminados

Cuando se crea un servidor SMB en Cloud Volumes Service, existen "recursos compartidos administrativos ocultos" (Usa la convención de nomenclatura de $) que se crean además del recurso compartido de SMB del volumen de datos. Entre ellas se incluyen C$ (acceso al espacio de nombres) e IPC$ (uso compartido de canalizaciones con nombre para la comunicación entre programas, como las llamadas a procedimiento remoto (RPC) utilizadas para el acceso a Microsoft Management Console (MMC)).

El recurso compartido IPC$ no contiene ACL compartidos y no se puede modificar; se utiliza estrictamente para las llamadas RPC y. "Windows no permite el acceso anónimo a estos recursos compartidos de forma predeterminada".

El recurso compartido C$ permite el acceso BUILTIN/Administrators de forma predeterminada, pero la automatización Cloud Volumes Service elimina la ACL compartida y no permite el acceso a nadie porque el acceso al recurso compartido C$ permite la visibilidad de todos los volúmenes montados en los sistemas de archivos Cloud Volumes Service. Como resultado, intenta navegar a. `\\SERVER\C$` error.

Cuentas con derechos de administrador/copia de seguridad local/BUILTIN

Los servidores SMB de Cloud Volumes Service mantienen una funcionalidad similar a los servidores SMB de Windows regulares en el sentido de que hay grupos locales (como BUILTIN\Administrators) que aplican derechos de acceso a determinados usuarios y grupos de dominio.

Cuando se especifica un usuario que se va a agregar a los usuarios de copia de seguridad, el usuario se agrega al grupo BUILTIN\operadores de copia de seguridad en la instancia de Cloud Volumes Service que utiliza esa conexión de Active Directory, que a continuación obtiene la "SeBackupPrivilege y SeRestorePrivilege".

Cuando agrega un usuario a usuarios de privilegios de seguridad, se le da al usuario SeSecurityPrivilege, que es útil en algunos casos de uso de aplicaciones, como "SQL Server en recursos compartidos de SMB".

Backup Users

Provide a comma separated list of domain users or a domain group name that require elevated privileges to access volumes created by Cloud Volumes Service.

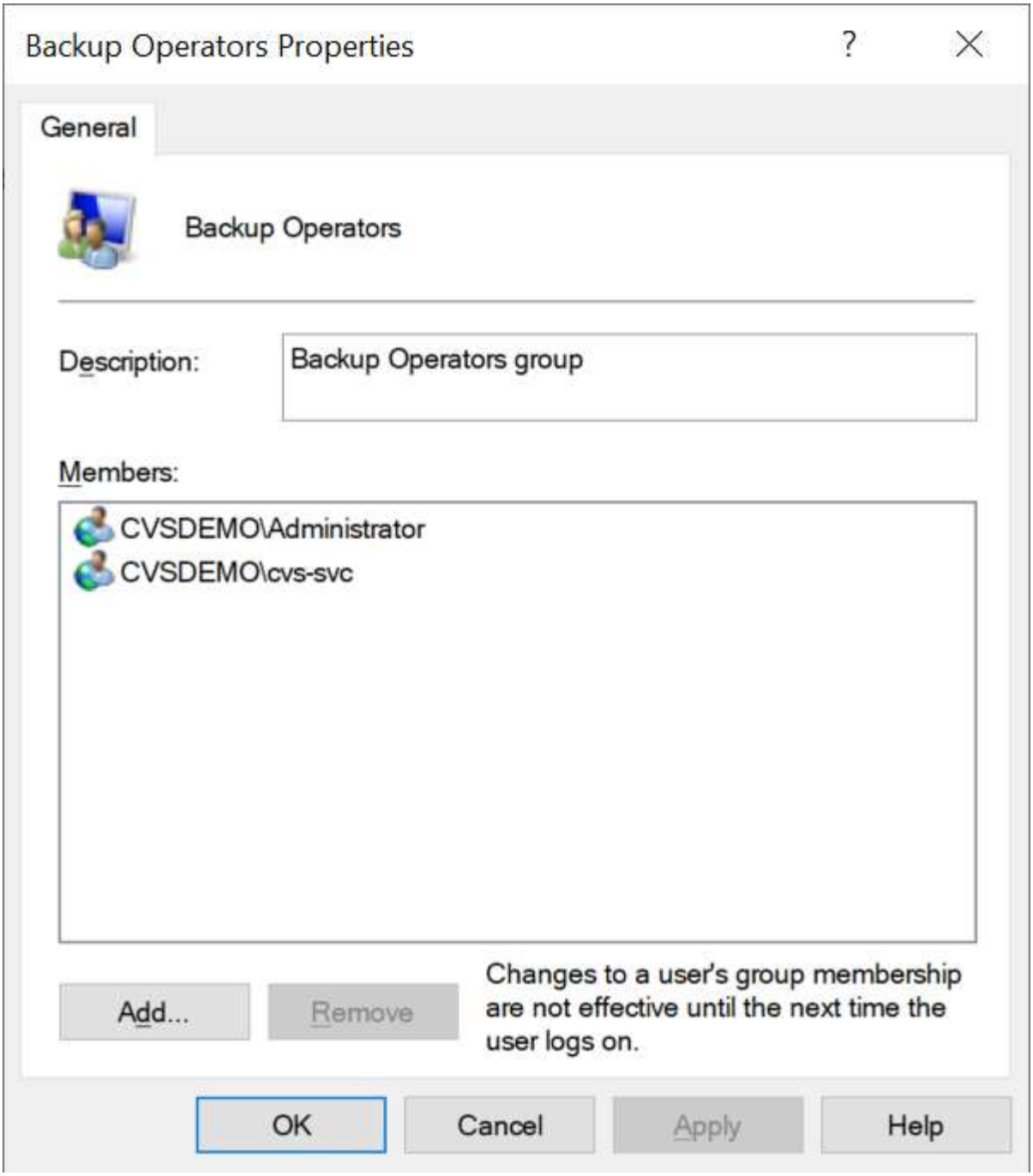
Accountnames
administrator,cvs-svc

Security Privilege Users

Provide a list of comma separated domain user accounts that require elevated privileges to manage security log for the Active Directory associated with Cloud Volumes Service.

Accountnames
administrator,cvs-svc

Puede ver las pertenencias a grupos locales de Cloud Volumes Service a través de MMC con los privilegios adecuados. La siguiente figura muestra los usuarios que se han agregado mediante la consola de Cloud Volumes Service.

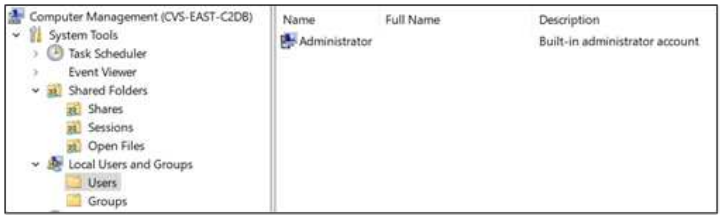


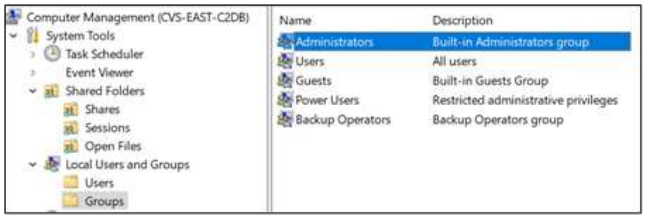
La siguiente tabla muestra la lista de grupos BUILTIN predeterminados y qué usuarios/grupos se agregan de forma predeterminada.

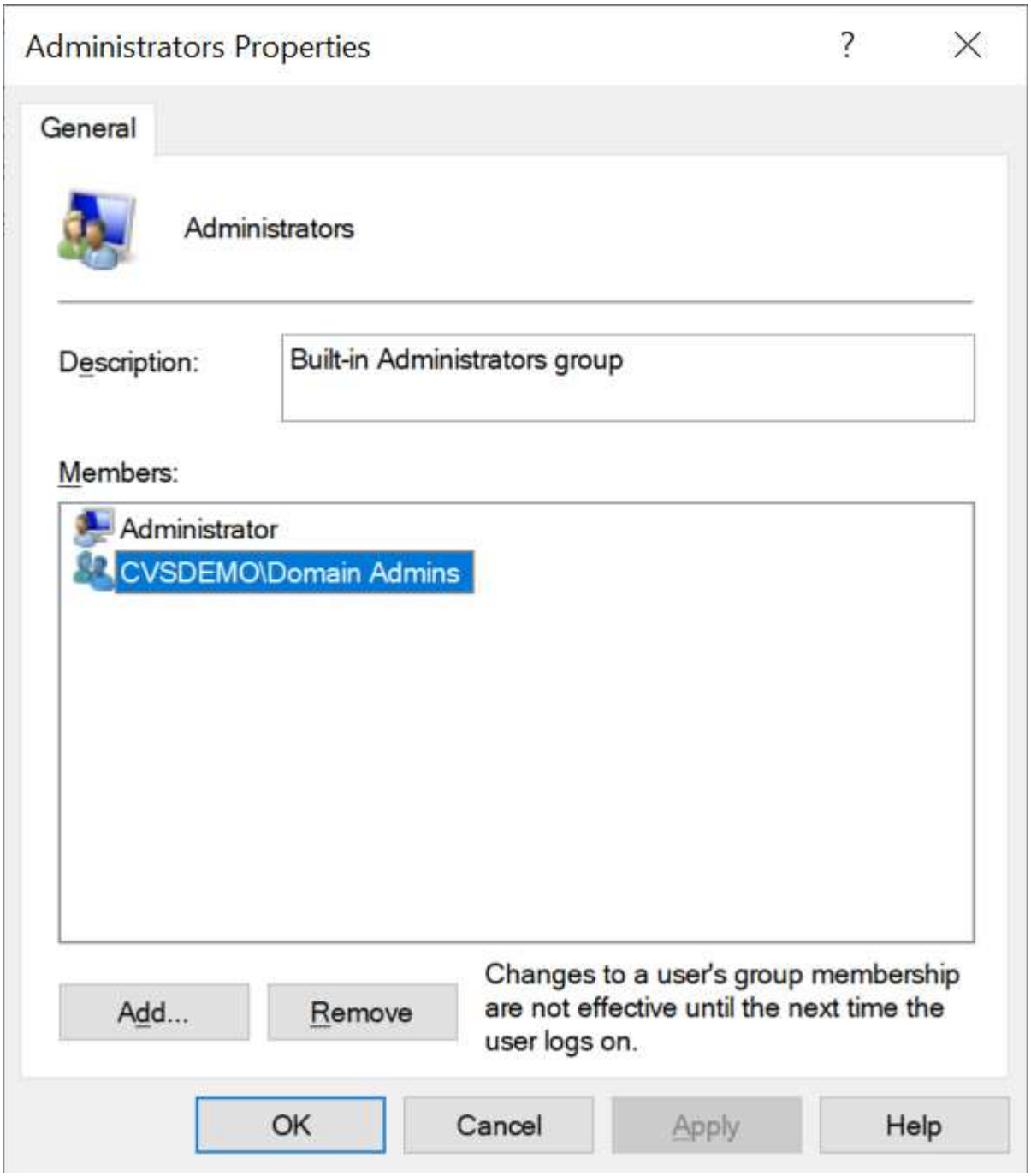
Grupo local/BUILTIN	Miembros predeterminados
BUILTIN\Administrators*	Dominio\Administradores de dominio
Operadores DE COPIAS DE seguridad/BUILTIN*	Ninguno
EDIFICIO\huéspedes	Dominio\invitados de dominio
Usuarios AVANZADOS\BUILTIN	Ninguno
USUARIOS DE BUILTIN\Domain	USUARIOS de DOMINIO/dominio

*Pertenencia a grupos controlada en la configuración de conexión de Cloud Volumes Service Active Directory.

Puede ver los usuarios y grupos locales (y los miembros del grupo) en la ventana MMC, pero no puede agregar ni eliminar objetos ni cambiar las pertenencias a grupos desde esta consola. De forma predeterminada, sólo el grupo Administradores de dominio y Administrador se agregan al grupo BUILTIN\Administradores de Cloud Volumes Service. Actualmente, no puede modificarlo.







Acceso a MMC/Computer Management

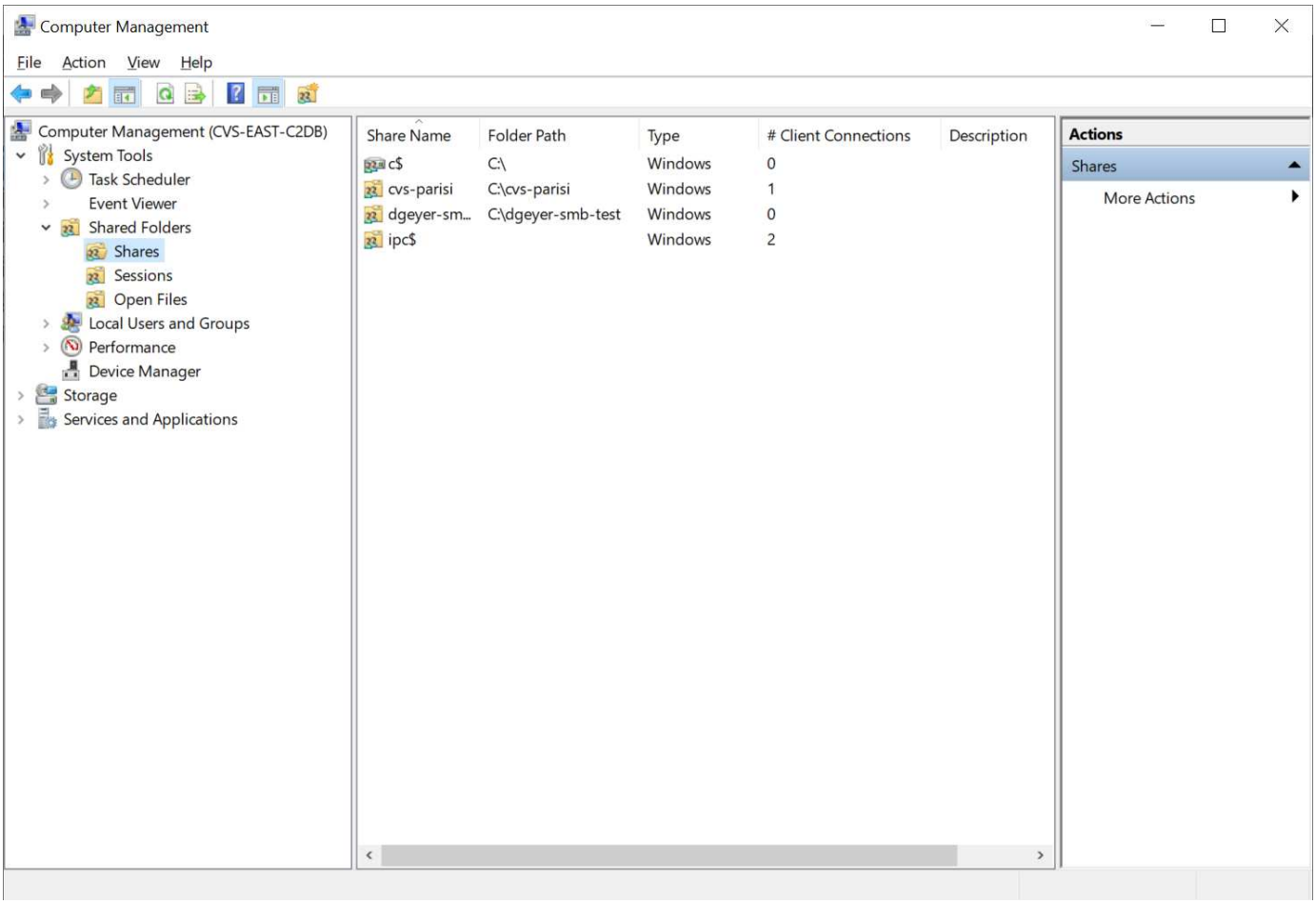
El acceso de SMB en Cloud Volumes Service proporciona conectividad a la MMC de gestión de equipos, que permite ver recursos compartidos, gestionar ACL de uso compartido, ver/gestionar sesiones de SMB y archivos abiertos.

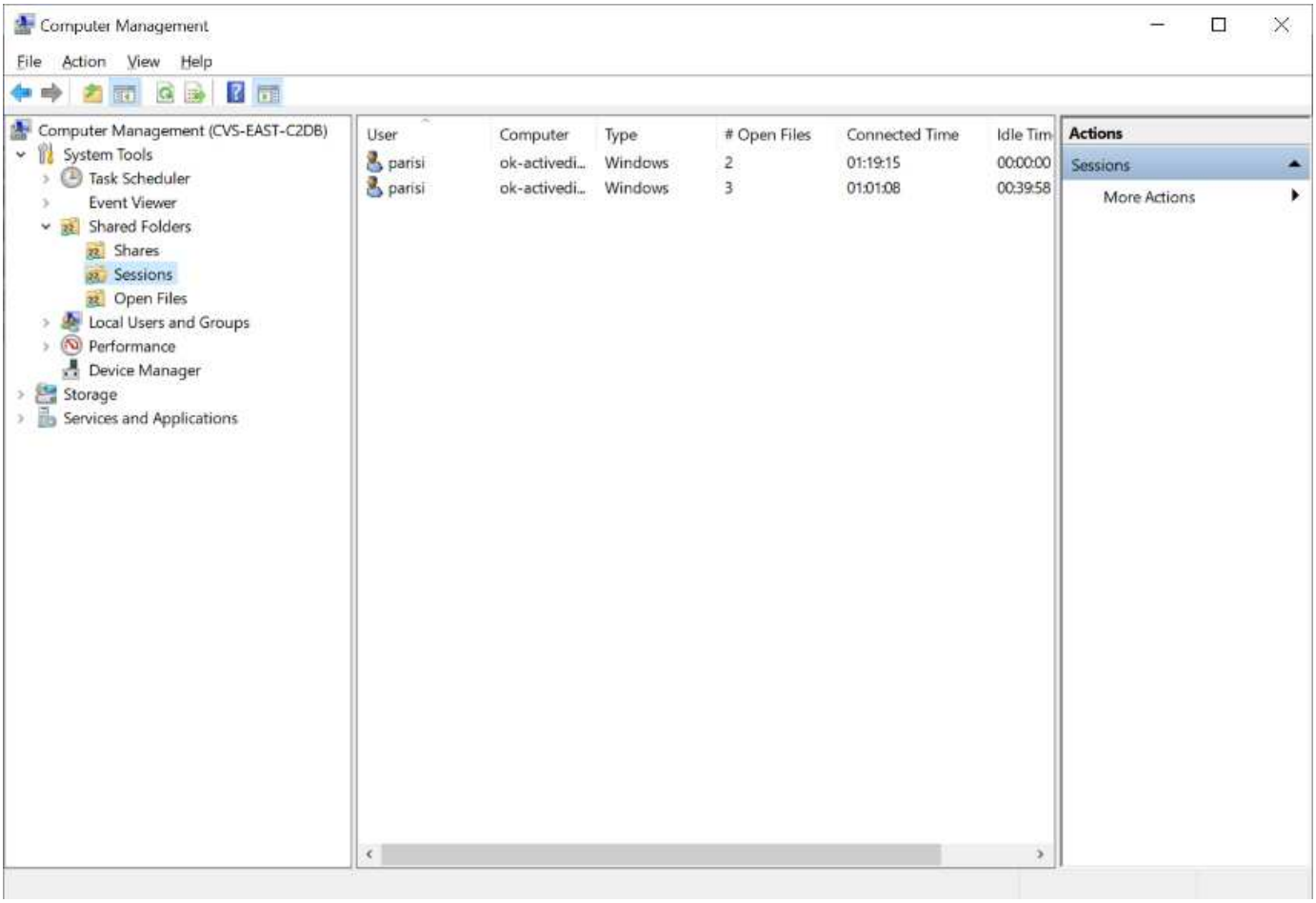
Para utilizar MMC para ver los recursos compartidos y las sesiones de SMB en Cloud Volumes Service, el usuario que ha iniciado sesión debe ser un administrador de dominio. A otros usuarios se les permite el acceso para ver o administrar el servidor SMB desde MMC y recibir un cuadro de diálogo no tiene permisos al intentar ver recursos compartidos o sesiones en la instancia del SMB de Cloud Volumes Service.

Para conectarse al servidor SMB, abra Administración de equipos, haga clic con el botón derecho en Administración de equipos y, a continuación, seleccione conectar a otro equipo. Con esto se abre el cuadro de diálogo Seleccionar equipo, donde puede introducir el nombre del servidor SMB (que se encuentra en la información del volumen Cloud Volumes Service).

Cuando se ven los recursos compartidos de SMB con los permisos adecuados, se ven todos los recursos compartidos disponibles en la instancia de Cloud Volumes Service que comparten la conexión de Active Directory. Para controlar este comportamiento, configure la opción Ocultar recursos compartidos de SMB en la instancia de volumen de Cloud Volumes Service.

Recuerde que sólo se permite una conexión de Active Directory por región.





En la siguiente tabla se muestra una lista de las funciones compatibles/no admitidas para MMC.

Funciones admitidas	Funciones no admitidas
• Ver recursos compartidos • Ver sesiones SMB activas • Ver archivos abiertos • Ver usuarios y grupos locales • Ver las membresías de grupo local • Enumera la lista de sesiones, archivos y conexiones de árbol del sistema • Cierre los archivos abiertos en el sistema • Cierre las sesiones abiertas • Cree/gestione recursos compartidos	• Creación de nuevos usuarios/grupos locales • Gestión/visualización de usuarios/grupos locales existentes • Ver eventos o registros de rendimiento • Gestionar el almacenamiento • Gestión de servicios y aplicaciones

Información de seguridad del servidor SMB

El servidor SMB en Cloud Volumes Service utiliza una serie de opciones que definen políticas de seguridad para las conexiones SMB, incluidos factores como la desviación del reloj de Kerberos, la antigüedad de los tickets, el cifrado, etc.

La siguiente tabla contiene una lista de esas opciones, qué hacen, las configuraciones predeterminadas y si se pueden modificar con Cloud Volumes Service. Algunas opciones no se aplican a Cloud Volumes Service.

Opción de seguridad	Qué hace	Valor predeterminado	¿Puede cambiar?
Sesgo de reloj Kerberos máximo (minutos)	Desfase de tiempo máximo entre Cloud Volumes Service y controladoras de dominio. Si la desviación de tiempo supera los 5 minutos, la autenticación de Kerberos fallará. Se establece en el valor predeterminado de Active Directory.	5	No
Duración de la entrada de Kerberos (horas)	Tiempo máximo que un ticket de Kerberos permanece válido antes de requerir una renovación. Si no se produce ninguna renovación antes de las 10 horas, debe obtener un boleto nuevo. Cloud Volumes Service realiza estas renovaciones automáticamente. 10 horas es el valor predeterminado de Active Directory.	10	No
Renovación máxima de entradas Kerberos (días)	Número máximo de días que se puede renovar un billete Kerberos antes de que se necesite una nueva solicitud de autorización. Cloud Volumes Service renueva automáticamente los boletos para las conexiones SMB. Seven Days es el valor predeterminado de Active Directory.	7	No
Tiempo de espera de conexión Kerberos KDC (segundos)	Número de segundos antes de que se agote el tiempo de espera de una conexión KDC.	3	No

Opción de seguridad	Qué hace	Valor predeterminado	¿Puede cambiar?
Es necesario firmar para tráfico entrante del bloque de mensajes del servidor	Configuración para requerir la firma para el tráfico SMB. Si se establece en true, los clientes que no admiten la conectividad de firma fallan.	Falso	
Requerir complejidad de contraseña para cuentas de usuario locales	Se usa para las contraseñas en usuarios SMB locales. Cloud Volumes Service no admite la creación de usuarios locales, por lo que esta opción no se aplica a Cloud Volumes Service.	Verdadero	No
Utilice START_tls para conexiones LDAP de Active Directory	Se utiliza para habilitar conexiones TLS de inicio para LDAP de Active Directory. Cloud Volumes Service no admite habilitar esto actualmente.	Falso	No
Es el cifrado AES-128 y AES-256 para Kerberos habilitado	Esto controla si el cifrado AES se utiliza para conexiones de Active Directory y se controla con la opción Activar cifrado AES para autenticación de Active Directory al crear o modificar la conexión de Active Directory.	Falso	Sí
Nivel de compatibilidad LM	Nivel de dialectos de autenticación compatibles para conexiones de Active Directory. Consulte la sección “Dialectos de autenticación SMB” para más información.	ntlmv2-krb	No
Se requiere cifrado SMB para el tráfico CIFS entrante	Requiere cifrado SMB para todos los recursos compartidos. Cloud Volumes Service no lo utiliza; en su lugar, establezca el cifrado por volumen (consulte la sección “Funciones de seguridad para recursos compartidos de SMB”).	Falso	No

Opción de seguridad	Qué hace	Valor predeterminado	¿Puede cambiar?
Seguridad de sesión de cliente	Establece la firma y/o el sellado para la comunicación LDAP. Esto no está establecido actualmente en Cloud Volumes Service, pero podría ser necesario en futuras versiones para abordar . La solución de problemas de autenticación LDAP debidos a la revisión de Windows se trata en la sección ""Enlace del canal LDAP"."".	Ninguno	No
Activación de SMB2 para conexiones de CC	Utiliza SMB2 para conexiones de CC. Activado de forma predeterminada.	Valor predeterminado del sistema	No
Especificación de referencia LDAP	Al usar varios servidores LDAP, la búsqueda de referencias permite al cliente consultar otros servidores LDAP de la lista cuando no se encuentra una entrada en el primer servidor. Actualmente, Cloud Volumes Service no admite esta operación.	Falso	No
Utilice LDAPS para conexiones seguras de Active Directory	Permite el uso de LDAP sobre SSL. Actualmente no es compatible con Cloud Volumes Service.	Falso	No
Se requiere cifrado para la conexión de CC	Requiere cifrado para conexiones DC correctas. Deshabilitado de forma predeterminada en Cloud Volumes Service.	Falso	No

Protocolo doble/multiprotocolo

Cloud Volumes Service permite compartir los mismos conjuntos de datos tanto con clientes SMB como NFS, a la vez que mantiene los permisos de acceso adecuados ("protocolo dual"). Esto se realiza coordinando la asignación de identidades entre protocolos y utilizando un servidor LDAP de backend centralizado para proporcionar las identidades de UNIX a Cloud Volumes Service. Puede utilizar Windows Active Directory para proporcionar facilidad de uso a los usuarios de Windows y UNIX.

Control de acceso

- **Controles de acceso compartido.** determine qué clientes y/o usuarios y grupos pueden acceder a un recurso compartido NAS. Para NFS, las reglas y políticas de exportación controlan el acceso del cliente a las exportaciones. Las exportaciones NFS se gestionan desde la instancia de Cloud Volumes Service. SMB utiliza recursos compartidos de CIFS/SMB y ACL de uso compartido para proporcionar un control más granular a nivel de usuarios y grupos. Solo puede configurar las ACL a nivel de uso compartido desde clientes de SMB mediante "Administración de MMC/Computer" Con una cuenta que tiene derechos de administrador en la instancia de Cloud Volumes Service (consulte la sección ""Cuentas con derechos de administrador/copia de seguridad local/BUILTIN."").
- **Controles de acceso a archivos.** Controle los permisos a nivel de archivo o carpeta y siempre se administran desde el cliente NAS. Los clientes NFS pueden utilizar bits de modo tradicional (rwx) o ACL de NFSv4. Los clientes de SMB aprovechan los permisos NTFS.

El control de acceso de los volúmenes que sirven datos tanto a NFS como a SMB depende del protocolo en uso. Para obtener información sobre los permisos con protocolo dual, consulte la sección "Modelo de permisos."

Asignación de usuarios

Cuando un cliente accede a un volumen, Cloud Volumes Service intenta asignar el usuario entrante a un usuario válido en la dirección opuesta. Esto es necesario para que se determine el acceso adecuado a través de los protocolos y para garantizar que el usuario que solicita acceso sea realmente lo que afirma ser.

Por ejemplo, si un usuario de Windows llamado `joe` Intenta acceder a un volumen con permisos UNIX a través del bloque de mensajes del servidor y, a continuación, Cloud Volumes Service realiza una búsqueda para encontrar el usuario UNIX correspondiente llamado `joe`. Si existe, los archivos que se escriben en un recurso compartido SMB como usuario de Windows `joe` Aparece como usuario UNIX `joe` De clientes NFS.

Como alternativa, si un usuario de UNIX llamado `joe` Intenta acceder al volumen Cloud Volumes Service con permisos de Windows y el usuario UNIX debe poder asignarlo a un usuario de Windows válido. De lo contrario, se deniega el acceso al volumen.

Actualmente, sólo se admite Active Directory para la gestión de identidades de UNIX externas con LDAP. Para obtener más información acerca de cómo configurar el acceso a este servicio, consulte "Creación de una conexión AD".

Modelo de permisos

Cuando se utilizan configuraciones de protocolo dual, Cloud Volumes Service utiliza estilos de seguridad para volúmenes para determinar el tipo de ACL. Estos estilos de seguridad se establecen en función de la especificación del protocolo NAS, o en el caso del protocolo dual, es la opción elegida en el momento de la creación del volumen de Cloud Volumes Service.

- Si solo utiliza NFS, los volúmenes de Cloud Volumes Service utilizan permisos de UNIX.
- Si solo utiliza SMB, los volúmenes de Cloud Volumes Service utilizan permisos NTFS.

Si se crea un volumen de protocolo doble, se puede elegir el estilo de ACL al crear un volumen. Esta decisión debe tomarse en función de la administración de permisos deseada. Si los usuarios gestionan permisos desde clientes de Windows/SMB, seleccione NTFS. Si sus usuarios prefieren usar clientes NFS y chmod/chown, utilice los estilos de seguridad de UNIX.

Consideraciones para crear conexiones de Active Directory

Cloud Volumes Service permite conectar la instancia de Cloud Volumes Service a un servidor de Active Directory externo para la gestión de identidades tanto para usuarios de SMB como UNIX. Se requiere crear una conexión de Active Directory para utilizar SMB en Cloud Volumes Service.

La configuración para esto ofrece varias opciones que requieren cierta consideración para la seguridad. El servidor de Active Directory externo puede ser una instancia de las instalaciones o una nativa del cloud. Si utiliza un servidor de Active Directory en las instalaciones, no exponga el dominio a la red externa (como con una DMZ o una dirección IP externa). En su lugar, utilice túneles privados seguros o VPN, fideicomisos forestales de un solo sentido o conexiones de red dedicadas a las redes locales con "Acceso privado a Google". Consulte la documentación de Google Cloud para obtener más información acerca de "Prácticas recomendadas con Active Directory en Google Cloud".

> CVS-SW requiere que los servidores de Active Directory se encuentren en la misma región. Si se intenta una conexión de CC en CVS-SW a otra región, el intento falla. Cuando utilice CVS-SW, asegúrese de crear sitios de Active Directory que incluyan los DC de Active Directory y, a continuación, especifique los sitios en Cloud Volumes Service para evitar intentos de conexión de DC entre regiones.

Credenciales de Active Directory

Cuando se habilita SMB o LDAP para NFS, Cloud Volumes Service interactúa con los controladores de Active Directory para crear un objeto de cuenta de máquina que se usará para la autenticación. Esto no difiere del modo en que un cliente SMB de Windows se une a un dominio y requiere los mismos derechos de acceso a las unidades organizativas (OU) de Active Directory.

En muchos casos, los grupos de seguridad no permiten el uso de una cuenta de administrador de Windows en servidores externos como Cloud Volumes Service. En algunos casos, el usuario Administrador de Windows está completamente deshabilitado como una práctica recomendada de seguridad.

Permisos necesarios para crear cuentas de máquina SMB

Para agregar objetos de máquina Cloud Volumes Service a un Active Directory, una cuenta que tenga derechos administrativos en el dominio o tiene "permisos delegados para crear y modificar objetos de cuenta de equipo" A una unidad organizativa especificada es necesaria. Puede hacerlo con el Asistente para delegación de control de Active Directory creando una tarea personalizada que proporcione a un usuario acceso a la creación o eliminación de objetos del equipo con los siguientes permisos de acceso proporcionados:

- Lectura/Escritura
- Crear/eliminar todos los objetos secundarios
- Todas las propiedades de lectura y escritura
- Cambiar/restablecer contraseña

Al hacerlo, se agrega automáticamente una ACL de seguridad para el usuario definido a la unidad organizativa de Active Directory y se minimiza el acceso al entorno de Active Directory. Una vez delegado un usuario, ese nombre de usuario y la contraseña se pueden proporcionar como credenciales de Active Directory en esta ventana.

> El nombre de usuario y la contraseña que se pasan al dominio de Active Directory aprovechan el cifrado Kerberos durante la consulta del objeto de cuenta de equipo y la creación para mayor seguridad.

Detalles de conexión de Active Directory

La "Detalles de conexión de Active Directory" Proporcione campos para que los administradores proporcionen información específica del esquema de Active Directory para la colocación de la cuenta de la máquina, como los siguientes:

- **Tipo de conexión de Active Directory.** se utiliza para especificar si la conexión de Active Directory en una región se utiliza para volúmenes de tipo de servicio Cloud Volumes Service o CVS-Performance. Si se establece de forma incorrecta en una conexión existente, es posible que no funcione correctamente cuando se utilice o edite.
- **Dominio.** el nombre de dominio de Active Directory.
- **Sitio.** limita los servidores de Active Directory a un sitio específico para seguridad y rendimiento "consideraciones". Esto es necesario cuando varios servidores de Active Directory abarcan regiones porque Cloud Volumes Service no admite actualmente la activación de solicitudes de autenticación de Active Directory a servidores de Active Directory en una región diferente a la instancia de Cloud Volumes Service. (Por ejemplo, el controlador de dominio de Active Directory se encuentra en una región que sólo soporta CVS-Performance pero desea un recurso compartido SMB en una instancia CVS-SW.)
- **Servidores DNS.** servidores DNS para utilizar en búsquedas de nombre.
- **Nombre NetBIOS (opcional).** Si lo desea, el nombre NetBIOS del servidor. Esto se utiliza cuando se crean cuentas de equipo nuevas mediante la conexión de Active Directory. Por ejemplo, si el nombre NetBIOS se establece en CVS-EAST, los nombres de la cuenta de la máquina serán CVS-EAST-{1234}. Consulte la sección "Cómo se muestra Cloud Volumes Service en Active Directory" si quiere más información.
- **Unidad organizativa (OU).** la unidad organizativa específica para crear la cuenta de equipo. Esto resulta útil si va a delegar el control a un usuario para las cuentas de equipo a una unidad organizativa específica.
- **Cifrado AES.** también puede activar o desactivar la casilla de verificación Activar cifrado AES para autenticación AD. Habilitar el cifrado AES para la autenticación de Active Directory proporciona seguridad adicional para la comunicación de Cloud Volumes Service a Active Directory durante las búsquedas de usuarios y grupos. Antes de habilitar esta opción, consulte con el administrador de dominio para confirmar que los controladores de dominio de Active Directory admiten la autenticación AES.

> De forma predeterminada, la mayoría de los servidores Windows no desactivan los cifrados más débiles (COMO DES o RC4-HMAC), pero si decide deshabilitar los cifrados más débiles, confirme que la conexión a Active Directory de Cloud Volumes Service se ha configurado para habilitar AES. De lo contrario, se producen fallos de autenticación. Al habilitar el cifrado AES, no se deshabilitan las cifrados, sino que se añade compatibilidad con AES a la cuenta de equipo SMB de Cloud Volumes Service.

Detalles del dominio de Kerberos

Esta opción no se aplica a los servidores SMB. En su lugar, se utiliza al configurar NFS Kerberos para el sistema Cloud Volumes Service. Cuando se rellenan estos detalles, el Reino de Kerberos de NFS se configura (similar al archivo krb5.conf en Linux) y se utiliza cuando se especifica NFS Kerberos en la creación de volúmenes de Cloud Volumes Service, ya que la conexión de Active Directory actúa como el Centro de distribución de Kerberos de NFS (KDC).

Actualmente no se admiten los KDC que no son de Windows para su uso con Cloud Volumes Service.

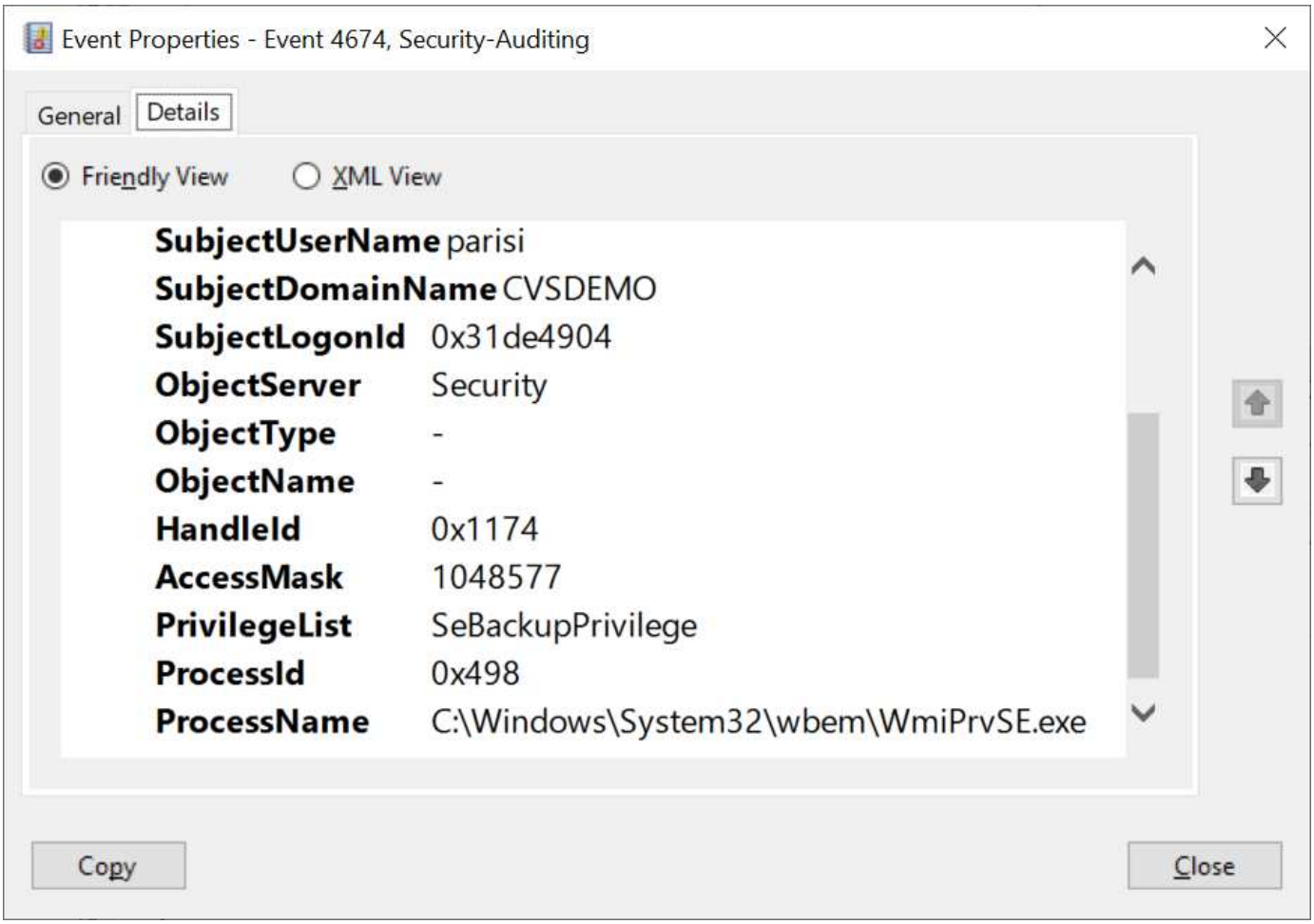
Región

Una región le permite especificar la ubicación donde reside la conexión de Active Directory. Esta región debe ser la misma región que el volumen Cloud Volumes Service.

- **Usuarios NFS locales con LDAP.** en esta sección también hay una opción para permitir usuarios NFS locales con LDAP. Esta opción debe dejarse sin seleccionar si desea ampliar la compatibilidad con la pertenencia a grupos de usuarios UNIX más allá de la limitación de 16 grupos de NFS (grupos extendidos). Sin embargo, el uso de grupos extendidos requiere un servidor LDAP configurado para identidades UNIX. Si no tiene un servidor LDAP, deje esta opción sin seleccionar. Si tiene un servidor LDAP y desea utilizar usuarios UNIX locales (como root), seleccione esta opción.

Usuarios de backup

Esta opción permite especificar usuarios de Windows que tienen permisos de backup en el volumen de Cloud Volumes Service. Los privilegios de backup (SeBackupPrivilege) son necesarios para que algunas aplicaciones puedan realizar backups y restaurar correctamente los datos en los volúmenes NAS. Este usuario tiene un alto nivel de acceso a los datos del volumen, por lo que debe tenerse en cuenta "habilitar la auditoría del acceso de ese usuario". Una vez habilitado, los eventos de auditoría aparecen en el Visor de sucesos > registros de Windows > Seguridad.



Usuarios con privilegios de seguridad

Esta opción permite especificar usuarios de Windows que tienen permisos de modificación de seguridad en el volumen de Cloud Volumes Service. Los privilegios de seguridad (SeSecurityPrivilege) son necesarios para algunas aplicaciones ("Como SQL Server") para establecer correctamente los permisos durante la instalación. Este privilegio se necesita para gestionar el registro de seguridad. Aunque este privilegio no es tan potente como SeBackupPrivilege, NetApp recomienda "auditar el acceso de los usuarios" con este nivel de privilegio, si es necesario.

Para obtener más información, consulte "Privilegios especiales asignados al nuevo inicio de sesión".

Cómo se muestra Cloud Volumes Service en Active Directory

Cloud Volumes Service aparece en Active Directory como un objeto de cuenta de equipo normal. Las convenciones de nomenclatura son las siguientes.

- CIFS/SMB y NFS Kerberos crean objetos de cuentas de equipo independientes.
- NFS con LDAP habilitado crea una cuenta de máquina en Active Directory para vínculos LDAP de Kerberos.
- Los volúmenes dobles de protocolo con LDAP comparten la cuenta de máquina CIFS/SMB para LDAP y SMB.
- Las cuentas de máquina de CIFS/SMB utilizan una convención de nomenclatura del NOMBRE-1234 (ID de cuatro dígitos aleatorio con un guión anexado al nombre de <10 caracteres) para la cuenta de la máquina. Puede definir EL NOMBRE mediante el valor de nombre NetBIOS en la conexión de Active Directory (consulte la sección “Detalles de conexión de Active Directory”).
- NFS Kerberos utiliza NFS-NAME-1234 como convención de nomenclatura (hasta 15 caracteres). Si se utilizan más de 15 caracteres, el nombre es NFS-TRUNCADO-NAME-1234.
- Las instancias de CVS-Performance de NFS solo con LDAP habilitado crean una cuenta de máquina SMB para enlazar al servidor LDAP con la misma convención de nomenclatura que las instancias de CIFS/SMB.
- Cuando se crea una cuenta de máquina SMB, los recursos compartidos admin ocultos predeterminados (consulte la sección ""Recursos compartidos ocultos predeterminados"") También se crean (c$, admin$, ipc$), pero esos recursos compartidos no tienen ACL asignados y son inaccesibles.
- Los objetos de cuenta de equipo se colocan de forma predeterminada en CN=Computers, pero a puede especificar una unidad organizativa diferente cuando sea necesario. Consulte la sección “Permisos necesarios para crear cuentas de máquina SMB” Para obtener información sobre los derechos de acceso necesarios para agregar/eliminar objetos de cuenta de máquina para Cloud Volumes Service.

Cuando Cloud Volumes Service agrega la cuenta de la máquina SMB a Active Directory, se rellenan los siguientes campos:

- cn (con el nombre del servidor SMB especificado)
- DNSHostName (con SMBserver.domain.com)
- MSDS-SupportedEncryptionTypes (permite DES_CBC_MD5, RC4_HMAC_MD5 si el cifrado AES no está habilitado; si el cifrado AES está habilitado, SE permite EL intercambio DE la cuenta DES_CBC_MD5, RC4_HMAC_MD5, AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_HMAC_96 con la cuenta SMB)
- Nombre (con el nombre del servidor SMB)
- SAMAccountName (con smbServer$)

- ServicePrincipalName (con host/smbserver.domain.com y host/smbServer SPN para Kerberos)

Si desea deshabilitar los tipos de cifrado Kerberos más débiles (enctype) en la cuenta de la máquina, puede cambiar el valor MSDS-SupportedEncryptionTypes de la cuenta de la máquina a uno de los valores de la tabla siguiente para permitir sólo AES.

MSDS-SupportedEncryptionTypes de valor	Enctype activado
2	DES_CBC_MD5
4	RC4_HMAC
8	SÓLO AES128_CTS_HMAC_SHA1_96
16	SÓLO AES256_CTS_HMAC_SHA1_96
24	AES128_CTS_HMAC_SHA1_96 Y AES256_CTS_HMAC_SHA1_96
30	DES_CBC_MD5, RC4_HMAC, AES128_CTS_HMAC_SHA1_96 Y AES256_CTS_HMAC_SHA1_96

Para habilitar el cifrado AES para cuentas de equipo SMB, haga clic en Activar cifrado AES para autenticación AD al crear la conexión de Active Directory.

Para habilitar el cifrado AES para Kerberos de NFS, "Consulte la documentación de Cloud Volumes Service".

Otras dependencias de servicios de infraestructura NAS (KDC, LDAP y DNS)

Cuando se utiliza Cloud Volumes Service para recursos compartidos NAS, es posible que sea necesario tener dependencias externas para disponer de una funcionalidad adecuada. Estas dependencias están en juego en circunstancias específicas. En la siguiente tabla se muestran diversas opciones de configuración y qué dependencias, si las hay, son necesarias.

Configuración	Dependencias necesarias
Solo NFSv3	Ninguno
Solo Kerberos para NFSv3	Active Directory de Windows: * KDC * DNS * LDAP
Solo NFSv4.1	Configuración de asignación de ID de cliente (/etc/idmap.conf)
Solo NFSv4.1 Kerberos	• Configuración de asignación de ID de cliente (/etc/idmap.conf) • Active Directory de Windows: LDAP de DNS de KDC
Solo SMB	Active Directory: * KDC * DNS

Configuración	Dependencias necesarias
NAS multiprotocolo (NFS y SMB)	• Configuración de asignación de ID de cliente (solo NFSv4.1; /etc/idmap.conf) • Active Directory de Windows: LDAP de DNS de KDC

Kerberos keytab rotation/password restablecerse para objetos de cuenta de equipo

Con las cuentas de máquina SMB, Cloud Volumes Service programa reinicios periódicos de contraseñas para la cuenta de la máquina SMB. Estos restablecimientos de contraseña se producen utilizando el cifrado Kerberos y funcionan según una programación de cada cuarto domingo a una hora aleatoria entre LAS 11:00 y LAS 01:00. Estos restablecimientos de contraseña cambian las versiones de clave Kerberos, giran las pestañas clave almacenadas en el sistema Cloud Volumes Service y ayudan a mantener un mayor nivel de seguridad para los servidores SMB que se ejecutan en Cloud Volumes Service. Las contraseñas de las cuentas de equipo son aleatorias y no son conocidas por los administradores.

Para las cuentas de máquina NFS Kerberos, los restablecimientos de contraseña sólo tienen lugar cuando se crea o se intercambia una nueva keytab con el KDC. Actualmente, no es posible hacerlo en Cloud Volumes Service.

Puertos de red para su uso con LDAP y Kerberos

Cuando se utilizan LDAP y Kerberos, debe determinar los puertos de red que utilizan estos servicios. En el, puede encontrar una lista completa de los puertos que utiliza Cloud Volumes Service "Documentación de Cloud Volumes Service sobre consideraciones de seguridad".

LDAP

Cloud Volumes Service actúa como un cliente LDAP y utiliza consultas de búsqueda LDAP estándar para búsquedas de usuarios y grupos de identidades de UNIX. LDAP es necesario si tiene la intención de utilizar usuarios y grupos fuera de los usuarios predeterminados estándar proporcionados por Cloud Volumes Service. LDAP también es necesario si tiene previsto utilizar NFS Kerberos con directores de usuario (como user1@domain.com). Actualmente, sólo LDAP con Microsoft Active Directory es compatible.

Para utilizar Active Directory como servidor LDAP de UNIX, debe rellenar los atributos UNIX necesarios en los usuarios y grupos que desee utilizar para las identidades de UNIX. Cloud Volumes Service utiliza una plantilla de esquema LDAP predeterminada en la que consulta atributos basados "RFC-2307-bis". Como resultado, en la siguiente tabla se muestran los atributos de Active Directory mínimos necesarios que se deben rellenar para los usuarios y grupos y para qué se utiliza cada atributo.

Para obtener más información acerca de la configuración de atributos LDAP en Active Directory, consulte "Gestión del acceso de doble protocolo."

Atributo	Qué hace
uid*	Especifica el nombre de usuario UNIX
UidNumber*	Especifica el ID numérico del usuario UNIX
GidNumber*	Especifica el identificador numérico del grupo principal del usuario UNIX

Atributo	Qué hace
ObjectClass*	Especifica qué tipo de objeto se está utilizando; Cloud Volumes Service requiere que “user” se incluya en la lista de clases de objeto (se incluye de forma predeterminada en la mayoría de implementaciones de Active Directory).
nombre	Información general sobre la cuenta (nombre real, número de teléfono, etc., también conocido como gecos)
UnixUserPassword	No es necesario configurar esto; no se utiliza en las búsquedas de identidad de UNIX para la autenticación NAS. Al establecer esta opción, el valor de unixUserPassword configurado se coloca en texto sin formato.
UnixHomeDirectory	Define la ruta a los directorios iniciales de UNIX cuando un usuario autentica con LDAP desde un cliente Linux. Establezca esta opción si desea utilizar la funcionalidad de directorio raíz de LDAP para UNIX.
LoginShell	Define la ruta al shell bash/profile para clientes Linux cuando un usuario autentica de acuerdo con LDAP.

*Denota atributo es necesario para una funcionalidad adecuada con Cloud Volumes Service. Los atributos restantes son para uso exclusivo del cliente.

Atributo	Qué hace
cn*	Especifica el nombre del grupo UNIX. Cuando se utiliza Active Directory para LDAP, se establece cuando se crea el objeto por primera vez, pero se puede cambiar más tarde. Este nombre no puede ser el mismo que el de otros objetos. Por ejemplo, si su usuario UNIX denominado user1 pertenece a un grupo denominado user1 en su cliente Linux, Windows no permite dos objetos con el mismo atributo cn. Para evitar esto, cambie el nombre del usuario de Windows por un nombre único (como user1-UNIX); LDAP en Cloud Volumes Service utiliza el atributo uid para los nombres de usuario de UNIX.
GidNumber*	Especifica el identificador numérico del grupo UNIX.
ObjectClass*	Especifica qué tipo de objeto se está utilizando; Cloud Volumes Service requiere que se incluya un grupo en la lista de clases de objeto (este atributo se incluye de forma predeterminada en la mayoría de las implementaciones de Active Directory).

Atributo	Qué hace
MemberUid	Especifica qué usuarios UNIX son miembros del grupo UNIX. Con LDAP de Active Directory en Cloud Volumes Service, este campo no es necesario. El esquema LDAP de Cloud Volumes Service utiliza el campo Miembro para las pertenencias a grupos.
Miembro*	Necesario para grupos de miembros/grupos UNIX secundarios. Para rellenar este campo, agregue usuarios de Windows a grupos de Windows. Sin embargo, si los grupos de Windows no tienen atributos UNIX rellenados, no se incluyen en las listas de miembros de grupo del usuario UNIX. Todos los grupos que tengan que estar disponibles en NFS deben rellenar los atributos de grupo UNIX necesarios que aparecen en esta tabla.

*Denota atributo es necesario para una funcionalidad adecuada con Cloud Volumes Service. Los atributos restantes son para uso exclusivo del cliente.

Información de enlace LDAP

Para consultar a los usuarios en LDAP, Cloud Volumes Service debe enlazar (iniciar sesión) con el servicio LDAP. Este inicio de sesión tiene permisos de sólo lectura y se utiliza para consultar atributos UNIX LDAP para búsquedas de directorios. Actualmente, los vínculos LDAP sólo son posibles mediante una cuenta de máquina SMB.

Solo puede habilitar LDAP para `CVS-Performance` Y utilícelo para NFSv3, NFSv4.1 o volúmenes de protocolo doble. Debe establecerse una conexión de Active Directory en la misma región que el volumen de Cloud Volumes Service para implementar correctamente el volumen habilitado para LDAP.

Cuando LDAP está habilitado, lo siguiente se produce en situaciones específicas.

- Si solo se utilizan NFSv3 o NFSv4.1 para el proyecto de Cloud Volumes Service, se crea una nueva cuenta de máquina en la controladora de dominio de Active Directory y el cliente LDAP de Cloud Volumes Service se enlaza a Active Directory mediante las credenciales de la cuenta del equipo. No se crean recursos compartidos de SMB para el volumen NFS ni los recursos compartidos administrativos ocultos predeterminados (consulte la sección ""Recursos compartidos ocultos predeterminados"") Se han eliminado las ACL compartidas.
- Si se utilizan volúmenes de protocolo doble para el proyecto Cloud Volumes Service, solo se utiliza la cuenta de máquina única creada para el acceso SMB para vincular el cliente LDAP en Cloud Volumes Service a Active Directory. No se crean cuentas de equipo adicionales.
- Si los volúmenes SMB dedicados se crean por separado (antes o después de que se habilitaron los volúmenes NFS con LDAP), la cuenta de máquina para los vínculos LDAP se comparte con la cuenta de la máquina SMB.
- Si también está habilitado NFS Kerberos, se crean dos cuentas de máquina: Una para recursos compartidos SMB y/o enlaces LDAP y una para autenticación Kerberos NFS.

Consultas LDAP

Aunque los vínculos LDAP están cifrados, las consultas LDAP se pasan por el cable en texto sin formato utilizando el puerto LDAP 389 común. Este puerto conocido no se puede cambiar actualmente en Cloud

Volumes Service. Como resultado, alguien con acceso al rastreo de paquetes en la red puede ver nombres de usuarios y grupos, identificadores numéricos y pertenencias a grupos.

Sin embargo, las máquinas virtuales de Google Cloud no pueden snifar el tráfico unicast de otras máquinas virtuales. Solo las máquinas virtuales que participan activamente en el tráfico LDAP (es decir, que se pueden enlazar) pueden ver tráfico del servidor LDAP. Para obtener más información sobre el rastreo de paquetes en Cloud Volumes Service, consulte la sección "“Consideraciones sobre rastreo y rastreo de paquetes”."

Valores predeterminados de la configuración del cliente LDAP

Cuando se habilita LDAP en una instancia de Cloud Volumes Service, se crea una configuración de cliente LDAP con detalles de configuración específicos de forma predeterminada. En algunos casos, las opciones no se aplican a Cloud Volumes Service (no se admiten) o no son configurables.

Opción de cliente LDAP	Qué hace	Valor predeterminado	¿Puede cambiar?
Lista de servidores LDAP	Establece los nombres de servidor LDAP o las direcciones IP que se utilizarán para las consultas. Esto no se utiliza para Cloud Volumes Service. En su lugar, el dominio de Active Directory se utiliza para definir servidores LDAP.	No configurado	No
Dominio de Active Directory	Establece el dominio de Active Directory que se utilizará para consultas LDAP. Cloud Volumes Service aprovecha los registros SRV para LDAP en DNS para buscar servidores LDAP en el dominio.	Establezca el dominio de Active Directory especificado en la conexión de Active Directory.	No
Servidores de Active Directory preferidos	Establece los servidores de Active Directory preferidos que se utilizarán para LDAP. Que Cloud Volumes Service no admite. En su lugar, utilice los sitios de Active Directory para controlar la selección del servidor LDAP.	No configurado.	No
Enlazar mediante credenciales de SMB Server	Enlaza a LDAP mediante la cuenta de máquina SMB. Actualmente, el único método de enlace LDAP admitido en Cloud Volumes Service.	Verdadero	No

Opción de cliente LDAP	Qué hace	Valor predeterminado	¿Puede cambiar?
Plantilla de esquema	La plantilla de esquema utilizada para consultas LDAP.	MS-AD-BIS	No
Puerto del servidor LDAP	El número de puerto utilizado para consultas LDAP. Cloud Volumes Service utiliza actualmente sólo el puerto LDAP estándar 389. LDAPS/el puerto 636 actualmente no es compatible.	389	No
LDAPS habilitado	Controla si se utiliza LDAP sobre Secure Sockets Layer (SSL) para consultas y vínculos. Actualmente no es compatible con Cloud Volumes Service.	Falso	No
Tiempo de espera de consulta (s)	Tiempo de espera para consultas. Si las consultas tardan más tiempo que el valor especificado, las consultas no se pueden realizar.	3	No
Nivel de autenticación de enlace mínimo	El nivel de enlace mínimo admitido. Dado que Cloud Volumes Service utiliza cuentas de equipo para los vínculos LDAP y Active Directory no admite enlaces anónimos de forma predeterminada, esta opción no entra en juego para la seguridad.	Anónimo	No
Enlazar DN	El nombre de usuario/distintivo (DN) utilizado para los vínculos cuando se utiliza el enlace simple. Cloud Volumes Service utiliza cuentas de equipo para enlaces LDAP y actualmente no admite autenticación de enlace simple.	No configurado	No

Opción de cliente LDAP	Qué hace	Valor predeterminado	¿Puede cambiar?
DN base	El DN base que se utiliza para las búsquedas LDAP.	El dominio de Windows se utiliza para la conexión de Active Directory, en formato DN (es decir, DC=dominio, DC=local).	No
Ámbito de búsqueda base	El ámbito de búsqueda para las búsquedas de DN base. Los valores pueden incluir base, onelevel o subárbol. Cloud Volumes Service sólo admite búsquedas en subárboles.	Subárbol	No
DN de usuario	Define el DN en el que se inician las búsquedas del usuario para las consultas LDAP. Actualmente no es compatible con Cloud Volumes Service, por lo que todas las búsquedas de usuarios comienzan en el DN base.	No configurado	No
Ámbito de búsqueda de usuarios	El ámbito de búsqueda para las búsquedas de DN de usuario. Los valores pueden incluir base, onelevel o subárbol. Cloud Volumes Service no admite la configuración del ámbito de búsqueda de usuarios.	Subárbol	No
DN de grupo	Define el DN donde comienzan las búsquedas de grupo para consultas LDAP. Actualmente no es compatible con Cloud Volumes Service, por lo que todas las búsquedas de grupo comienzan en el DN base.	No configurado	No
Ámbito de búsqueda de grupos	El ámbito de búsqueda para las búsquedas de DN de grupo. Los valores pueden incluir base, onelevel o subárbol. Cloud Volumes Service no admite la configuración del ámbito de búsqueda de grupos.	Subárbol	No

Opción de cliente LDAP	Qué hace	Valor predeterminado	¿Puede cambiar?
DN de grupo de red	Define el DN donde comienzan las búsquedas de netgroup para las consultas LDAP. Actualmente no es compatible con Cloud Volumes Service, por lo que todas las búsquedas de netgroup comienzan en el DN base.	No configurado	No
Ámbito de búsqueda de grupos de red	El ámbito de búsqueda para las búsquedas de DN de grupo de red. Los valores pueden incluir base, onelevel o subárbol. Cloud Volumes Service no admite la configuración del ámbito de búsqueda de netgroup.	Subárbol	No
Utilice start_tls sobre LDAP	Aprovecha Start TLS para conexiones LDAP basadas en certificados a través del puerto 389. Actualmente no es compatible con Cloud Volumes Service.	Falso	No
Habilite la búsqueda de netgroup-by-host	Habilita búsquedas de netgroup por nombre de host en lugar de expandir grupos de red para enumerar todos los miembros. Actualmente no es compatible con Cloud Volumes Service.	Falso	No
DN de netgroup por host	Define el DN donde comienzan las búsquedas netgroup-by-host para las consultas LDAP. Actualmente, netgroup-by-host no es compatible con Cloud Volumes Service.	No configurado	No
Ámbito de búsqueda netgroup-by-host	El ámbito de búsqueda para las búsquedas DN de netgroup-by-host. Los valores pueden incluir base, onelevel o subárbol. Actualmente, netgroup-by-host no es compatible con Cloud Volumes Service.	Subárbol	No

Opción de cliente LDAP	Qué hace	Valor predeterminado	¿Puede cambiar?
Seguridad de sesión de cliente	Define qué nivel de seguridad de sesión utiliza LDAP (firma, sello o ninguno). La firma LDAP es compatible con CVS-Performance, si es solicitada por Active Directory. CVS-SW no admite la firma LDAP. En ambos tipos de servicio, el sellado no es compatible actualmente.	Ninguno	No
Búsqueda de referencias LDAP	Al usar varios servidores LDAP, la búsqueda de referencias permite al cliente consultar otros servidores LDAP de la lista cuando no se encuentra una entrada en el primer servidor. Actualmente, Cloud Volumes Service no admite esta operación.	Falso	No
Filtro de pertenencia a grupos	Proporciona un filtro de búsqueda LDAP personalizado que se utilizará al buscar miembros de grupo desde un servidor LDAP. Actualmente no es compatible con Cloud Volumes Service.	No configurado	No

Se utiliza LDAP para la asignación de nombres asimétricos

Cloud Volumes Service, de forma predeterminada, asigna usuarios de Windows y usuarios UNIX con nombres de usuario idénticos de manera bidireccional sin configuración especial. Siempre que Cloud Volumes Service pueda encontrar un usuario UNIX válido (con LDAP), se producirá una asignación de nombre 1:1. Por ejemplo, si el usuario de Windows `johnsmith` Se utiliza, entonces, si Cloud Volumes Service puede encontrar un usuario UNIX llamado `johnsmith` En LDAP, la asignación de nombres se realiza correctamente para ese usuario, todos los archivos/carpetas creados por `johnsmith` Mostrar la propiedad de usuario correcta y todas las ACL que afectan `johnsmith` Sean honrados independientemente del protocolo NAS que se utilice. Esto se conoce como asignación simétrica de nombres.

La asignación de nombres asimétricos se produce cuando la identidad del usuario de Windows y de UNIX no coinciden. Por ejemplo, si el usuario de Windows `johnsmith` Tiene una identidad UNIX de `jsmith`, Cloud Volumes Service necesita una manera de ser contada acerca de la variación. Puesto que Cloud Volumes Service no admite actualmente la creación de reglas estáticas de asignación de nombres, se debe utilizar LDAP para buscar la identidad de los usuarios tanto para las identidades de Windows como UNIX para garantizar la propiedad correcta de los archivos y carpetas y los permisos esperados.

De forma predeterminada, Cloud Volumes Service incluye `LDAP` En el switch ns de la instancia de la base de datos de asignación de nombres, de modo que para proporcionar la funcionalidad de asignación de nombres mediante el uso de LDAP para nombres asimétricos, sólo es necesario modificar algunos de los atributos de usuario/grupo para reflejar lo que busca Cloud Volumes Service.

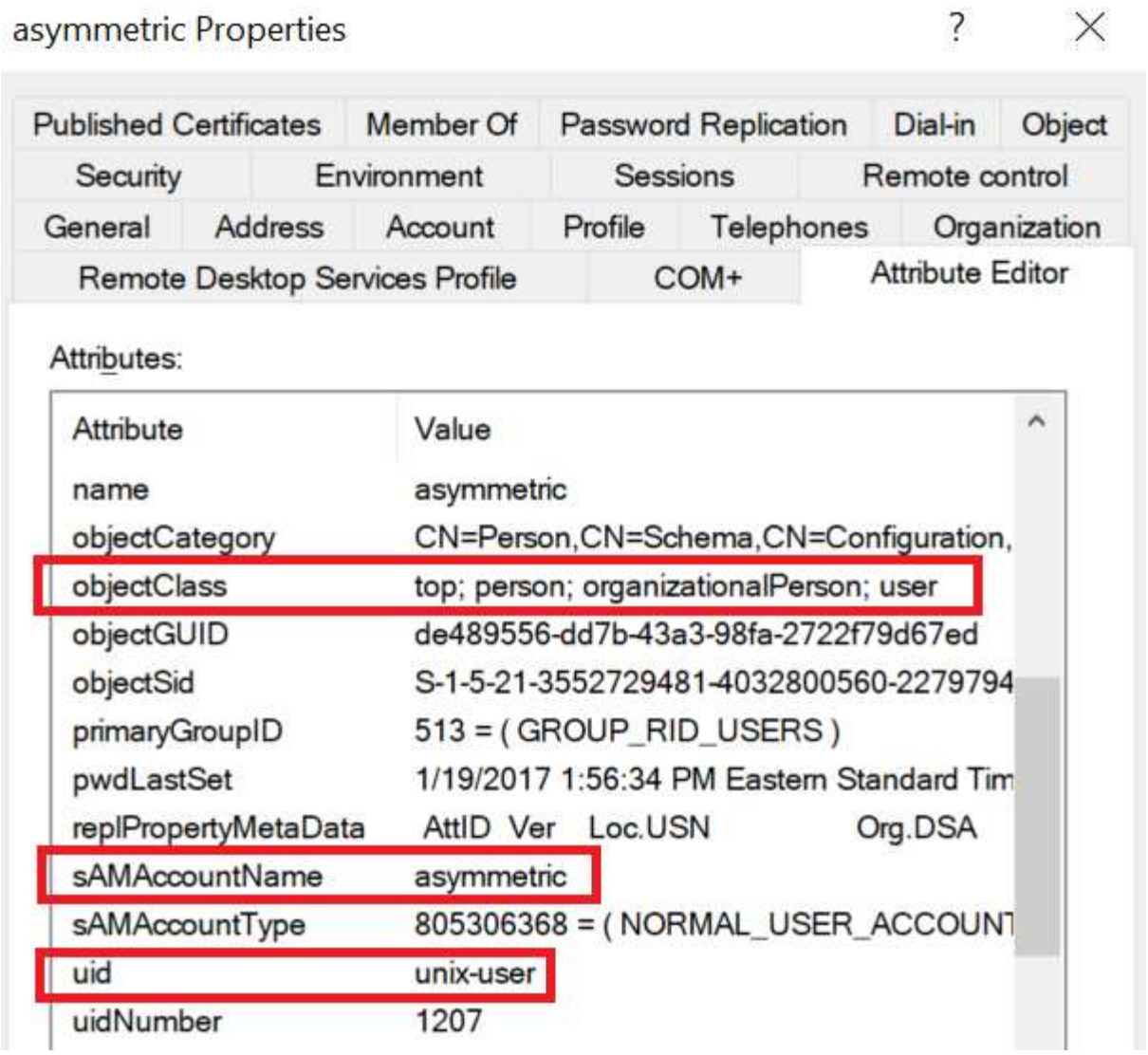
En la siguiente tabla se muestran los atributos que se deben rellenar en LDAP para la funcionalidad de asignación de nombres asimétrica. En la mayoría de los casos, Active Directory ya está configurado para hacerlo.

Atributo Cloud Volumes Service	**Qué hace**	**Valor que utiliza Cloud Volumes Service para la asignación de nombres**
Clase de objetos de Windows a UNIX	Especifica el tipo de objeto que se está utilizando. (Es decir, usuario, grupo, posixcuenta, etc.)	Debe incluir al usuario (puede contener varios otros valores, si lo desea).
Atributo de Windows a UNIX	Que define el nombre de usuario de Windows en el momento de su creación. Cloud Volumes Service lo utiliza para búsquedas de Windows a UNIX.	No se necesita ningún cambio aquí; sAMAccountName es igual que el nombre de inicio de sesión de Windows.
UID	Define el nombre de usuario UNIX.	Nombre de usuario UNIX deseado.

Cloud Volumes Service actualmente no utiliza prefijos de dominio en las búsquedas LDAP, de modo que varios entornos LDAP de dominio no funcionan correctamente con las búsquedas del mapa de nombres LDAP.

En el ejemplo siguiente se muestra un usuario con el nombre de Windows `asymmetric`, El nombre UNIX `unix-user`, Y el comportamiento que sigue al escribir archivos tanto de SMB como de NFS.

La figura siguiente muestra el aspecto de los atributos LDAP desde el servidor Windows.



Desde un cliente NFS, puede consultar el nombre de UNIX, pero no el nombre de Windows:

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

Cuando se escribe un archivo desde NFS AS `unix-user`, El siguiente es el resultado del cliente NFS:

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx------  1 unix-user sharedgroup     0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

Desde un cliente Windows, puede ver que el propietario del archivo está establecido en el usuario de Windows correcto:

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

Por el contrario, los archivos creados por el usuario de Windows `asymmetric` Desde un cliente SMB, se muestra el propietario UNIX correcto, tal y como se muestra en el texto siguiente.

SMB:

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS:

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx------  1 unix-user         sharedgroup   14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

Enlace de canal LDAP

Debido a una vulnerabilidad en los controladores de dominio de Windows Active Directory, "Aviso de seguridad de Microsoft ADV190023" Cambia la forma en que los DC permiten el enlace LDAP.

El impacto para Cloud Volumes Service es el mismo que para cualquier cliente LDAP. Cloud Volumes Service no admite actualmente el enlace de canal. Dado que Cloud Volumes Service admite la firma LDAP de forma predeterminada a través de la negociación, el enlace al canal LDAP no debe ser un problema. Si tiene problemas con la vinculación a LDAP con el enlace de canal activado, siga los pasos de corrección de ADV190023 para permitir que los enlaces LDAP de Cloud Volumes Service tengan éxito.

DNS

Active Directory y Kerberos tienen dependencias en DNS para el nombre de host a IP/IP para la resolución de nombres de host. DNS requiere que el puerto 53 esté abierto. Cloud Volumes Service no realiza modificaciones en los registros DNS ni admite actualmente el uso de "DNS dinámico" en las interfaces de red.

Puede configurar el DNS de Active Directory para restringir qué servidores pueden actualizar los registros DNS. Para obtener más información, consulte "Proteja el DNS de Windows".

Tenga en cuenta que los recursos de un proyecto de Google utilizan de forma predeterminada Google Cloud DNS, que no está conectado con Active Directory DNS. Los clientes que utilizan DNS cloud no pueden resolver las rutas UNC que devuelve Cloud Volumes Service. Los clientes de Windows Unidos al dominio de Active Directory están configurados para usar DNS de Active Directory y pueden resolver dichas rutas UNC.

Para unirse a un cliente a Active Directory, debe configurar su configuración DNS para utilizar el DNS de Active Directory. Opcionalmente, puede configurar Cloud DNS para reenviar solicitudes a Active Directory DNS. Consulte "¿Por qué mi cliente no puede resolver el nombre NetBIOS de SMB?"si quiere más información.

> Cloud Volumes Service no admite actualmente las consultas DNSSEC y las consultas DNS se realizan en texto sin formato.

Auditoría de acceso a los archivos

Actualmente no es compatible con Cloud Volumes Service.

Protección antivirus

Debe realizar análisis antivirus en Cloud Volumes Service en el cliente para un recurso compartido NAS. Actualmente no existe ninguna integración antivirus nativa con Cloud Volumes Service.