NetApp para GCP/GCVE

NetApp Solutions

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/es-es/netapp-solutions/ehc/gcp-app-dr-sc-cvs-veeam.html on April 24, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Multicloud híbrido de NetApp con soluciones de VMware 1
Protección de cargas de trabajo en GCP / GCVE 1
Migrar cargas de trabajo en GCP / GCVE 9
Disponibilidad de región – almacén de datos NFS complementario para Google Cloud Platform (GCP) . . . 29
Descripción general de la seguridad: Cloud Volumes Service de NetApp (CVS) en Google Cloud 31

Multicloud híbrido de NetApp con soluciones de VMware

Protección de cargas de trabajo en GCP / GCVE

Recuperación ante desastres coherente con las aplicaciones con NetApp SnapCenter y replicación de Veeam

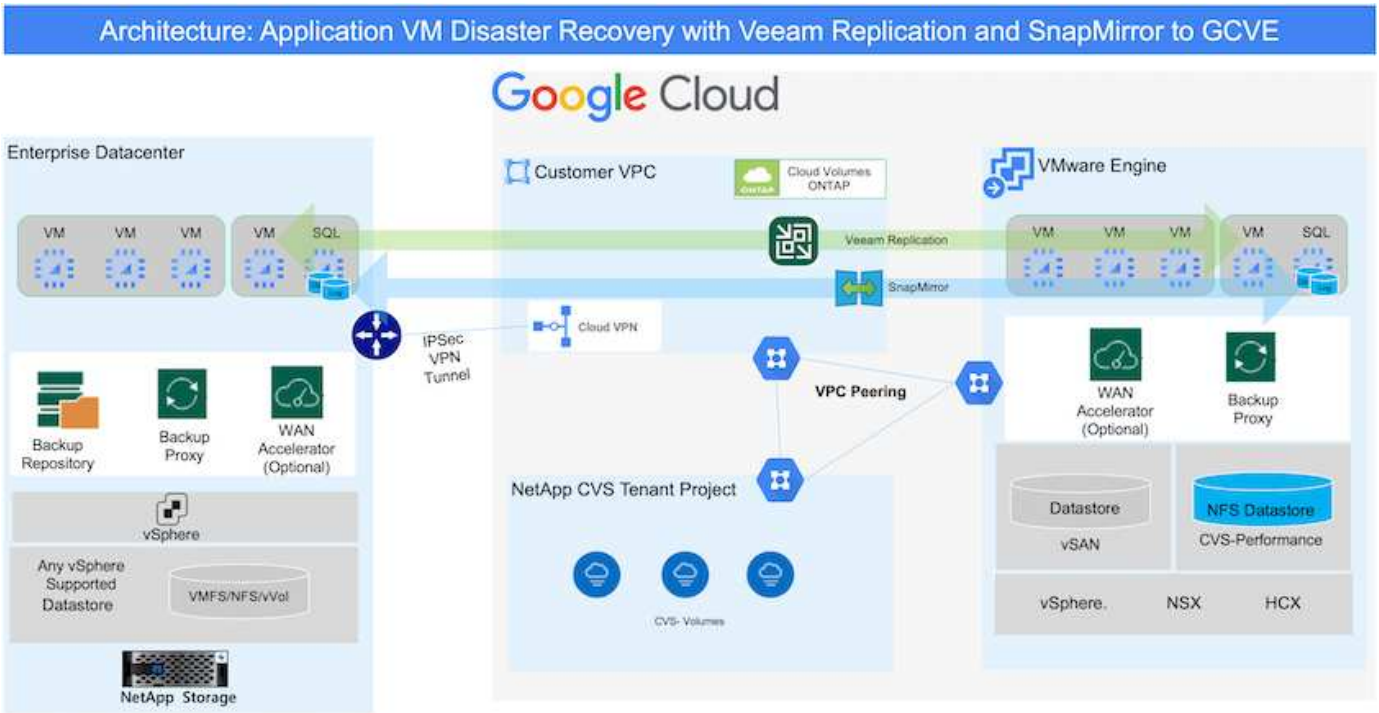
Autores: Suresh Thoppay, NetApp

Descripción general

Muchos clientes están buscando una solución de recuperación ante desastres eficaz para sus VM de aplicaciones alojadas en VMware vSphere. Muchos de ellos utilizan su solución de backup existente para realizar la recuperación durante el diaster.
Muchas veces esa solución aumenta el objetivo de tiempo de recuperación y no cumple con sus expectativas. Para reducir el objetivo de punto de recuperación y el objetivo de tiempo de recuperación, la replicación de Veeam VM se puede utilizar incluso desde on-premises a GCVE, siempre y cuando la conectividad de red y el entorno con los permisos adecuados estén disponibles.
NOTA: Veeam VM Replication no protege los dispositivos de almacenamiento conectados a invitados de VM como montajes iSCSI o NFS dentro de la VM invitada. Necesidad de protegerlos por separado.

Para la replicación consistente de las aplicaciones para SQL VM y para reducir el RTO, utilizamos SnapCenter para orquestar las operaciones de snapmirror de volúmenes de bases de datos y registros de SQL.

Este documento proporciona un enfoque paso a paso para configurar y realizar la recuperación ante desastres que utiliza SnapMirror, Veeam y Google Cloud VMware Engine (GCVE) de NetApp.



Supuestos

Este documento se centra en el almacenamiento invitado para datos de aplicaciones (también conocido como «guest» conectado) y asumimos que el entorno local utiliza SnapCenter para realizar backups coherentes con las aplicaciones.

> Este documento es aplicable a cualquier solución de backup o recuperación de terceros. Dependiendo de la solución utilizada en el entorno, siga las prácticas recomendadas para crear normativas de backup que cumplan los acuerdos de nivel de servicio de la organización.

Para la conectividad entre el entorno local y la red de Google Cloud, utilice las opciones de conectividad como interconexión dedicada o VPN en la nube. Los segmentos se deben crear en función del diseño VLAN en las instalaciones.

> Existen múltiples opciones para conectar los centros de datos en las instalaciones a Google Cloud, lo que nos impide esbozar un flujo de trabajo específico en este documento. Consulte la documentación de Google Cloud para conocer el método de conectividad apropiado de las instalaciones a Google.

Implementar la solución DR

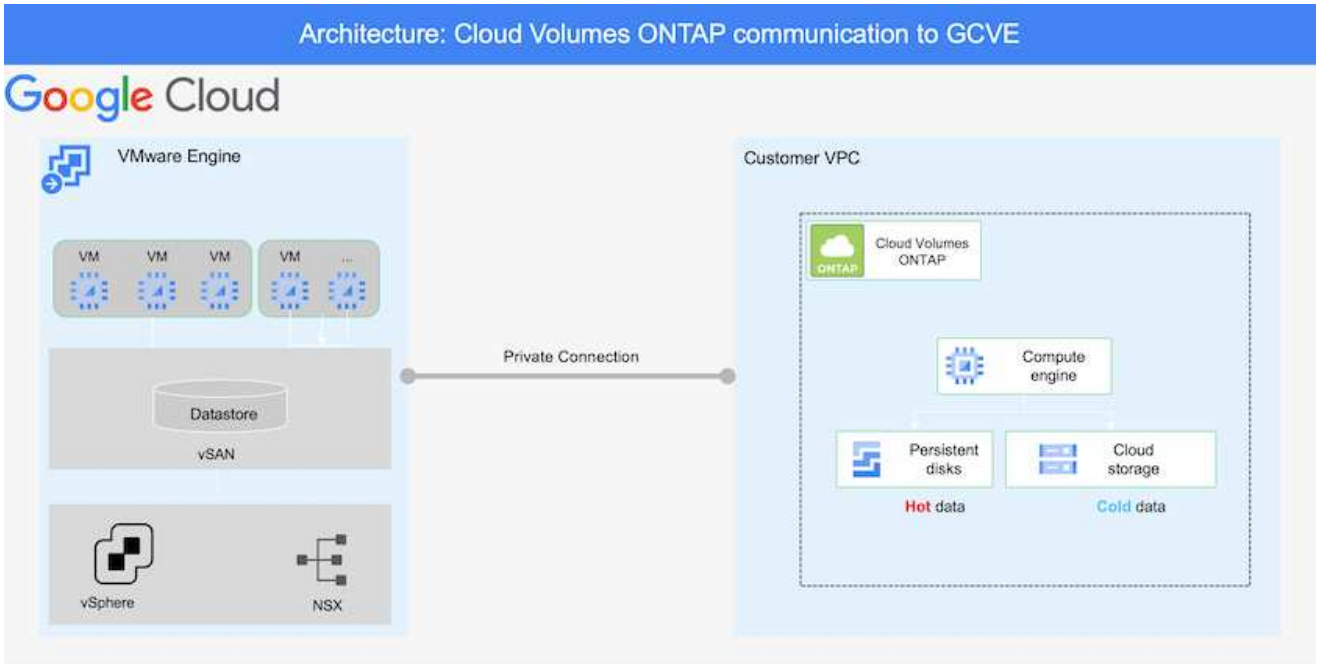
Descripción general de la puesta en marcha de soluciones

1. Asegúrese de que se realiza el backup de los datos de la aplicación mediante SnapCenter con los requisitos de punto de recuperación necesarios.
2. Aprovisiona Cloud Volumes ONTAP con el tamaño de instancia correcto mediante BlueXP en la suscripción y la red virtual adecuadas.
   a. Configurar SnapMirror para los volúmenes correspondientes de las aplicaciones.
   b. Actualice las políticas de backup en SnapCenter para activar actualizaciones de SnapMirror después de los trabajos programados.
3. Instale el software Veeam y empiece a replicar máquinas virtuales a la instancia de Google Cloud VMware Engine.
4. Durante un desastre, interrumpa la relación de SnapMirror mediante BlueXP y activa la conmutación al nodo de respaldo de máquinas virtuales con Veeam.
   a. Vuelva a conectar las LUN ISCSI y los montajes NFS para los equipos virtuales de la aplicación.
   b. Ponga en marcha aplicaciones en línea.
5. Invoque la conmutación tras recuperación al sitio protegido mediante la resincronización inversa de SnapMirror una vez que se haya recuperado el sitio principal.

Detalles de la implementación

Configurar CVO en Google Cloud y replicar volúmenes a CVO

El primer paso consiste en configurar Cloud Volumes ONTAP en Google Cloud ("cvo") Y replicar los volúmenes deseados en Cloud Volumes ONTAP con las frecuencias y retentions de instantánea deseadas.



Para obtener una muestra de instrucciones paso a paso acerca de la configuración de SnapCenter y la replicación de los datos, consulte "Configurar la replicación con SnapCenter"

Revisión de la protección de SQL VM con SnapCenter

Configurar los hosts GCVE y el acceso a datos CVO

Dos factores importantes que se deben tener en cuenta al implementar un SDDC son el tamaño del clúster SDDC en la solución GCVE y durante cuánto tiempo mantener el SDDC en servicio. Estas dos consideraciones clave para una solución de recuperación ante desastres ayudan a reducir los costes operativos generales. SDDC puede ser de tan solo tres hosts, hasta un clúster de varios hosts en una puesta en marcha a escala completa.

El servicio Cloud Volume de NetApp para almacén de datos NFS y las bases de datos y el registro Cloud Volumes ONTAP para SQL pueden implementarse en cualquier VPC y GCVE deben tener conexión privada con ese VPC para montar almacén de datos NFS y tener conexión de máquinas virtuales a LUN de iSCSI.

Para configurar GCVE SDDC, consulte "Poner en marcha y configurar el entorno de virtualización en Google Cloud Platform (GCP)". Como requisito previo, compruebe que los equipos virtuales invitados que residen en los hosts GCVE pueden consumir datos de Cloud Volumes ONTAP una vez establecida la conectividad.

Una vez que Cloud Volumes ONTAP y GCVE se hayan configurado correctamente, comience a configurar Veeam para automatizar la recuperación de las cargas de trabajo en las instalaciones en GCVE (máquinas virtuales con VMDK de aplicación y máquinas virtuales con almacenamiento en invitado) mediante la función Veeam Replication y aprovechando SnapMirror para las copias de los volúmenes de aplicación en Cloud Volumes ONTAP.

Instale Veeam Components

Según el escenario de implementación, se debe poner en marcha el servidor de backup de Veeam, el repositorio de backup y el proxy de backup. En este caso de uso, no es necesario poner en marcha el almacén de objetos para Veeam y tampoco se requiere ningún repositorio de escalado horizontal.
"Consulte la documentación de Veeam para conocer el procedimiento de instalación"
Para obtener más información, consulte "Migración con Veeam Replication"

Configure la replicación de VM con Veeam

Tanto el vCenter en las instalaciones como el vCenter de GCVE deben registrarse con Veeam.
"Configure el trabajo de replicación de máquina virtual de vSphere" En el asistente Guest Processing, seleccione Desactivar el procesamiento de aplicaciones, ya que utilizará SnapCenter para los procesos de backup y recuperación con reconocimiento de aplicaciones.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

Conmutación al nodo de respaldo de Microsoft SQL Server VM

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

Ventajas de esta solución

- Usa la replicación eficiente y resiliente de SnapMirror.

- Recupera a cualquier punto disponible en el tiempo con la retención de copias Snapshot de ONTAP.
- Existe una automatización completa a disposición de todos los pasos necesarios para recuperar de cientos a miles de VM, desde los pasos de almacenamiento, computación, red y validación de aplicaciones.
- SnapCenter utiliza mecanismos de clonado que no cambian el volumen replicado.
  - Esto evita el riesgo de daños en los datos de los volúmenes y las Snapshot.
  - Evita interrupciones de replicación durante los flujos de trabajo de pruebas de recuperación ante desastres.
  - Aprovecha los datos de recuperación ante desastres para flujos de trabajo que van más allá de la recuperación ante desastres, como las fases de desarrollo y pruebas, pruebas de seguridad, pruebas de parches y actualizaciones, y pruebas para solucionar problemas.
- La replicación de Veeam permite cambiar las direcciones IP de las máquinas virtuales en el sitio de recuperación ante desastres.

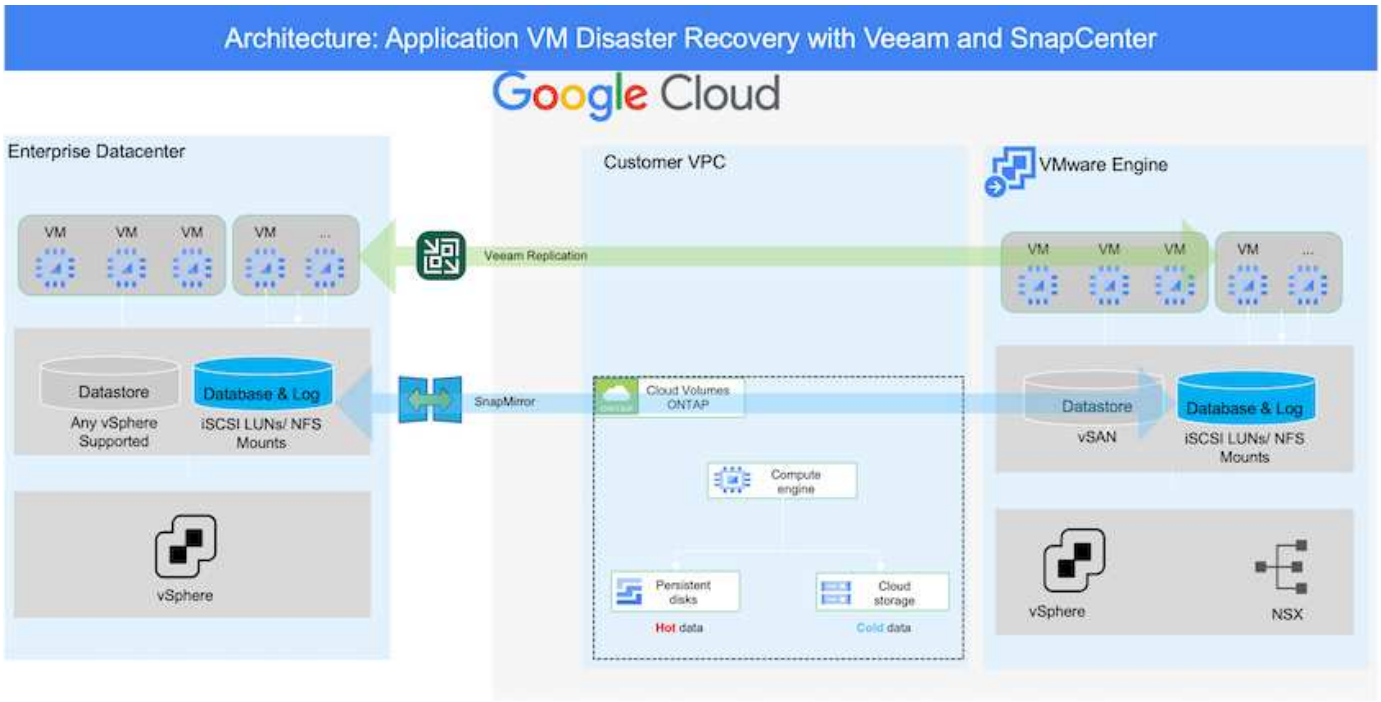
Recuperación ante desastres de aplicaciones con replicación de SnapCenter, Cloud Volumes ONTAP y Veeam

Autores: Suresh Thoppay, NetApp

Descripción general

La recuperación ante desastres en el cloud es un método resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos dañados por datos como ransomware. Con SnapMirror de NetApp, las cargas de trabajo de VMware en las instalaciones que utilizan el almacenamiento conectado a invitado se pueden replicar a Cloud Volumes ONTAP de NetApp que se ejecuta en Google Cloud. Así se tratan los datos de aplicaciones; sin embargo, ¿qué ocurre con los equipos virtuales mismos? La recuperación ante desastres debería cubrir todos los componentes dependientes, incluidos equipos virtuales, VMDK, datos de aplicaciones, etc. Para ello, se puede utilizar SnapMirror y Veeam para recuperar sin problemas cargas de trabajo replicadas de las instalaciones a Cloud Volumes ONTAP a la vez que se utiliza almacenamiento VSAN para VMDK de máquinas virtuales.

Este documento proporciona un enfoque paso a paso para configurar y realizar la recuperación ante desastres que utiliza SnapMirror, Veeam y Google Cloud VMware Engine (GCVE) de NetApp.



Supuestos

Este documento se centra en el almacenamiento invitado para datos de aplicaciones (también conocido como «guest» conectado) y asumimos que el entorno local utiliza SnapCenter para realizar backups coherentes con las aplicaciones.

> Este documento es aplicable a cualquier solución de backup o recuperación de terceros. Dependiendo de la solución utilizada en el entorno, siga las prácticas recomendadas para crear normativas de backup que cumplan los acuerdos de nivel de servicio de la organización.

Para la conectividad entre el entorno local y la red de Google Cloud, utilice las opciones de conectividad como interconexión dedicada o VPN en la nube. Los segmentos se deben crear en función del diseño VLAN en las instalaciones.

> Existen múltiples opciones para conectar los centros de datos en las instalaciones a Google Cloud, lo que nos impide esbozar un flujo de trabajo específico en este documento. Consulte la documentación de Google Cloud para conocer el método de conectividad apropiado de las instalaciones a Google.

Implementar la solución DR

Descripción general de la puesta en marcha de soluciones

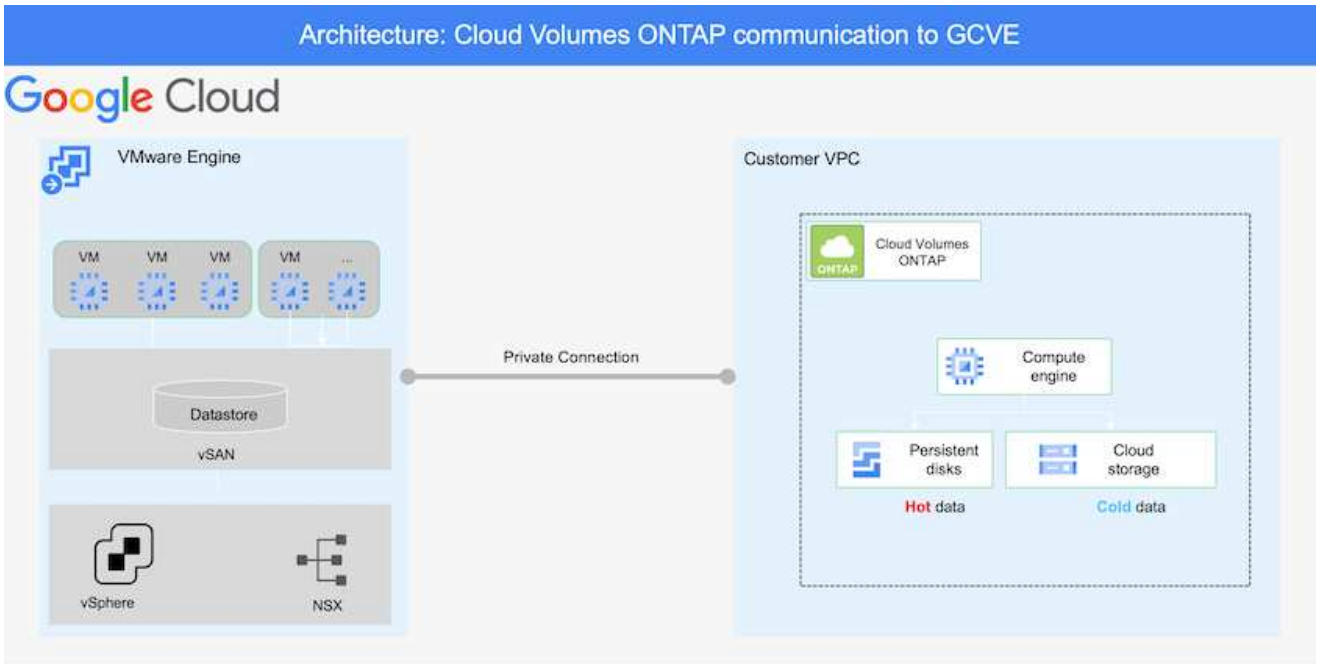
1. Asegúrese de que se realiza el backup de los datos de la aplicación mediante SnapCenter con los requisitos de punto de recuperación necesarios.
2. Aprovisione Cloud Volumes ONTAP con el tamaño de instancia correcto usando Cloud Manager dentro de la suscripción y la red virtual adecuadas.
   a. Configurar SnapMirror para los volúmenes correspondientes de las aplicaciones.
   b. Actualice las políticas de backup en SnapCenter para activar actualizaciones de SnapMirror después de los trabajos programados.

3. Instale el software Veeam y empiece a replicar máquinas virtuales a la instancia de Google Cloud VMware Engine.
4. Durante un evento de desastre, rompa la relación de SnapMirror mediante Cloud Manager y active la conmutación al nodo de respaldo de máquinas virtuales con Veeam.
   a. Vuelva a conectar las LUN ISCSI y los montajes NFS para los equipos virtuales de la aplicación.
   b. Ponga en marcha aplicaciones en línea.
5. Invoque la conmutación tras recuperación al sitio protegido mediante la resincronización inversa de SnapMirror una vez que se haya recuperado el sitio principal.

Detalles de la implementación

Configurar CVO en Google Cloud y replicar volúmenes a CVO

El primer paso consiste en configurar Cloud Volumes ONTAP en Google Cloud ("cvo") Y replicar los volúmenes deseados en Cloud Volumes ONTAP con las frecuencias y retentions de instantánea deseadas.



Para obtener instrucciones paso a paso de ejemplo sobre la configuración de SnapCenter y la replicación de datos, consulte "Configurar la replicación con SnapCenter"

Configurar la replicación con SnapCenter

Configurar los hosts GCVE y el acceso a datos CVO

Dos factores importantes que se deben tener en cuenta al implementar un SDDC son el tamaño del clúster SDDC en la solución GCVE y durante cuánto tiempo mantener el SDDC en servicio. Estas dos consideraciones clave para una solución de recuperación ante desastres ayudan a reducir los costes operativos generales. SDDC puede ser de tan solo tres hosts, hasta un clúster de varios hosts en una puesta en marcha a escala completa.

Cloud Volumes ONTAP se puede implementar en cualquier VPC y GCVE debe tener una conexión privada a ese VPC para que la máquina virtual se conecte a los LUN de iSCSI.

Para configurar GCVE SDDC, consulte "Poner en marcha y configurar el entorno de virtualización en Google Cloud Platform (GCP)". Como requisito previo, compruebe que los equipos virtuales invitados que residen en los hosts GCVE pueden consumir datos de Cloud Volumes ONTAP una vez establecida la conectividad.

Una vez que Cloud Volumes ONTAP y GCVE se hayan configurado correctamente, comience a configurar Veeam para automatizar la recuperación de las cargas de trabajo en las instalaciones en GCVE (máquinas virtuales con VMDK de aplicación y máquinas virtuales con almacenamiento en invitado) mediante la función Veeam Replication y aprovechando SnapMirror para las copias de los volúmenes de aplicación en Cloud Volumes ONTAP.

Instale Veeam Components

Según el escenario de implementación, se debe poner en marcha el servidor de backup de Veeam, el repositorio de backup y el proxy de backup. En este caso de uso, no es necesario poner en marcha el almacén de objetos para Veeam y tampoco se requiere ningún repositorio de escalado horizontal.https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["Consulte la documentación de Veeam para conocer el procedimiento de instalación"]

Configure la replicación de VM con Veeam

Tanto el vCenter en las instalaciones como el vCenter de GCVE deben registrarse con Veeam. "Configure el trabajo de replicación de máquina virtual de vSphere" En el asistente Guest Processing, seleccione Desactivar el procesamiento de aplicaciones, ya que utilizará SnapCenter para los procesos de backup y recuperación con reconocimiento de aplicaciones.

Configure el trabajo de replicación de máquina virtual de vSphere

Conmutación al nodo de respaldo de Microsoft SQL Server VM

Conmutación al nodo de respaldo de Microsoft SQL Server VM

Ventajas de esta solución

- Usa la replicación eficiente y resiliente de SnapMirror.
- Recupera a cualquier punto disponible en el tiempo con la retención de copias Snapshot de ONTAP.
- Existe una automatización completa a disposición de todos los pasos necesarios para recuperar de cientos a miles de VM, desde los pasos de almacenamiento, computación, red y validación de

aplicaciones.

- SnapCenter utiliza mecanismos de clonado que no cambian el volumen replicado.
  - Esto evita el riesgo de daños en los datos de los volúmenes y las Snapshot.
  - Evita interrupciones de replicación durante los flujos de trabajo de pruebas de recuperación ante desastres.
  - Aprovecha los datos de recuperación ante desastres para flujos de trabajo que van más allá de la recuperación ante desastres, como las fases de desarrollo y pruebas, pruebas de seguridad, pruebas de parches y actualizaciones, y pruebas para solucionar problemas.
- La replicación de Veeam permite cambiar las direcciones IP de las máquinas virtuales en el sitio de recuperación ante desastres.

Migrar cargas de trabajo en GCP / GCVE

Migre cargas de trabajo al almacén de datos de Cloud Volume Service de NetApp en Google Cloud VMware Engine mediante la guía de inicio rápido de VMware HCX

Autores: Ingeniería de soluciones de NetApp

Descripción general: Migrar máquinas virtuales con VMware HCX, almacenes de datos de Cloud Volume Service de NetApp y Google Cloud VMware Engine (GCVE)

Uno de los casos de uso más comunes de los almacenes de datos de Google Cloud VMware Engine y Cloud Volume Service es la migración de las cargas de trabajo de VMware. HCX de VMware es la opción preferida y ofrece diversos mecanismos de migración para mover las máquinas virtuales (VM) locales y sus datos a los almacenes de datos NFS de Cloud Volume Service.

VMware HCX es principalmente una plataforma de migración diseñada para simplificar la migración de aplicaciones, el reequilibrado de las cargas de trabajo e incluso la continuidad de negocio entre clouds. Se incluye como parte de Google Cloud VMware Engine Private Cloud y ofrece muchas formas de migrar cargas de trabajo y se puede utilizar para operaciones de recuperación ante desastres.

Este documento proporciona orientación paso a paso para aprovisionar el almacén de datos de Cloud Volume Service seguido de la descarga, la puesta en marcha y la configuración de VMware HCX, incluidos todos sus componentes principales en las instalaciones y Google Cloud VMware Engine, que incluye interconexión, extensión de red y optimización de WAN para habilitar diversos mecanismos de migración de máquinas virtuales.

> VMware HCX funciona con cualquier tipo de almacén de datos, ya que la migración se realiza a nivel de equipo virtual. Por lo tanto, este documento es aplicable a clientes existentes de NetApp y clientes que no son de NetApp que planeen poner en marcha Cloud Volume Service con Google Cloud VMware Engine para una puesta en marcha de cloud VMware rentable.

Escalones de alto nivel

Esta lista contiene los pasos de alto nivel necesarios para emparejar y migrar las máquinas virtuales a HCX Cloud Manager en el lado de Google Cloud VMware Engine desde HCX Connector on-premises:

1. Prepare HCX a través del portal Google VMware Engine.
2. Descargue e implemente el instalador de HCX Connector Open Virtualization Appliance (OVA) en VMware vCenter Server en las instalaciones.
3. Active HCX con la clave de licencia.
4. Empareje el conector VMware HCX en las instalaciones con Google Cloud VMware Engine HCX Cloud Manager.
5. Configure el perfil de red, el perfil de computación y la malla de servicio.
6. (Opcional) lleve a cabo la extensión de red para evitar la reIP durante las migraciones.
7. Valide el estado del dispositivo y asegúrese de que la migración sea posible.
8. Migrar las cargas de trabajo de la máquina virtual.

Requisitos previos

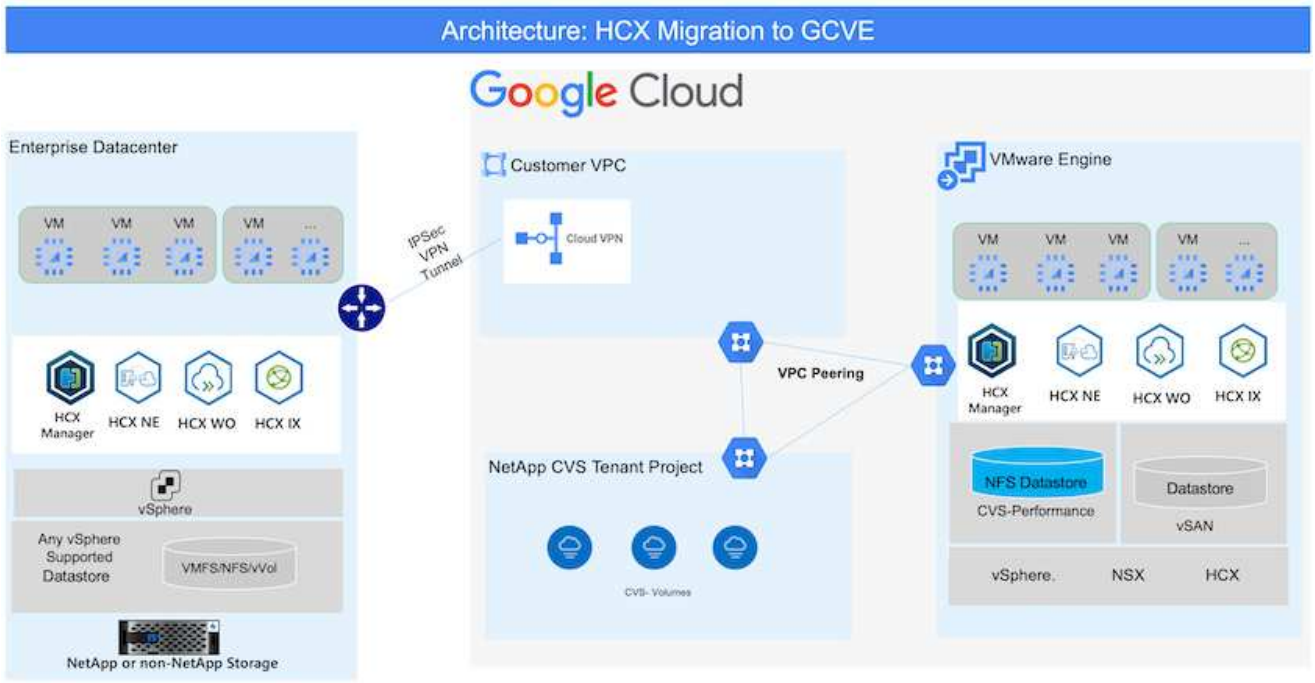
Antes de empezar, asegúrese de que se cumplan los siguientes requisitos previos. Para obtener más información, consulte este tema "enlace". Una vez que se hayan establecido los requisitos previos, incluida la conectividad, descargue la clave de licencia de HCX del portal Google Cloud VMware Engine. Después de descargar el instalador de OVA, continúe con el proceso de instalación como se describe a continuación.

> HCX Advanced es la opción predeterminada y VMware HCX Enterprise Edition también está disponible a través de un ticket de soporte y se admite sin coste adicional. Consulte "este enlace"

- Utilice un centro de datos definido por software (SDDC) de Google Cloud VMware Engine o cree un cloud privado utilizando este método "Enlace a NetApp" o esto "Vínculo de Google".
- La migración de equipos virtuales y datos asociados desde el centro de datos integrado con VMware vSphere en las instalaciones requiere conectividad de red del centro de datos al entorno SDDC. Antes de migrar cargas de trabajo, "Configure una conexión de Cloud VPN o de Cloud Interconnect" entre el entorno local y el cloud privado correspondiente.
- La ruta de red desde el entorno local de VMware vCenter Server al cloud privado de Google Cloud VMware Engine debe admitir la migración de las máquinas virtuales mediante vMotion.
- Asegúrese de que es necesario "reglas y puertos del firewall" Se permiten para el tráfico de vMotion entre la instancia local de vCenter Server y SDDC vCenter.
- El volumen de NFS de Cloud Volume Service debe montarse como un almacén de datos en Google Cloud VMware Engine. Siga los pasos detallados en este documento "enlace" Para conectar almacenes de datos de Cloud Volume Service a los hosts de Google Cloud VMware Engines.

Arquitectura de alto nivel

Para realizar las pruebas, el entorno de laboratorio de las instalaciones que se emplean para esta validación se conectó a través de una VPN de cloud que permite la conectividad local con Google Cloud VPC.



Para obtener un diagrama más detallado del HCX, consulte "Enlace de VMware"

Puesta en marcha de la solución

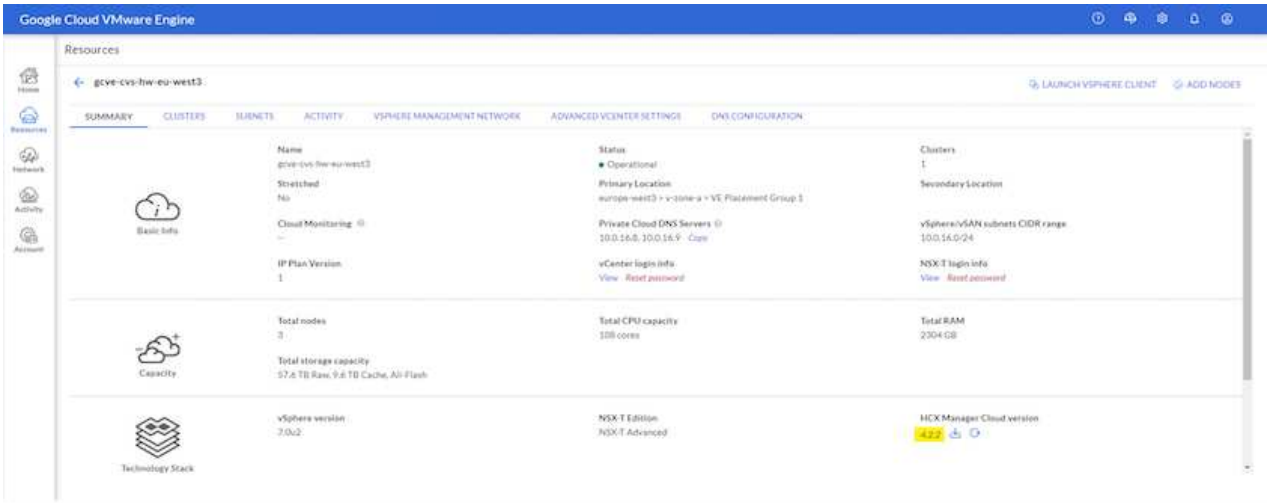
Siga la serie de pasos para completar la implementación de esta solución:

Paso 1: Preparación del HCX a través del portal Google VMware Engine

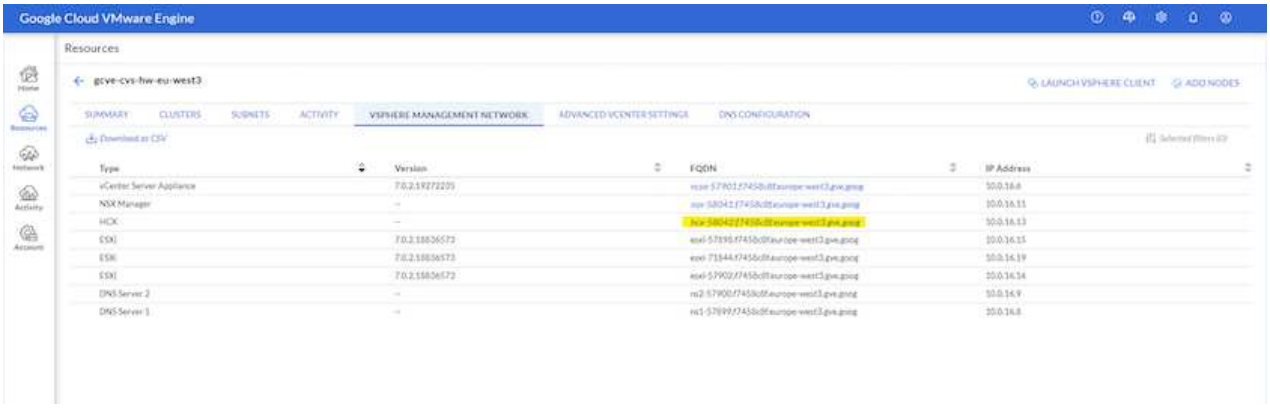
El componente DE HCX Cloud Manager se instala automáticamente a medida que aprovisiona el cloud privado con VMware Engine. Para preparar el emparejamiento de sitios, lleve a cabo los siguientes pasos:

1. Inicie sesión en el portal Google VMware Engine e inicie sesión en HCX Cloud Manager.

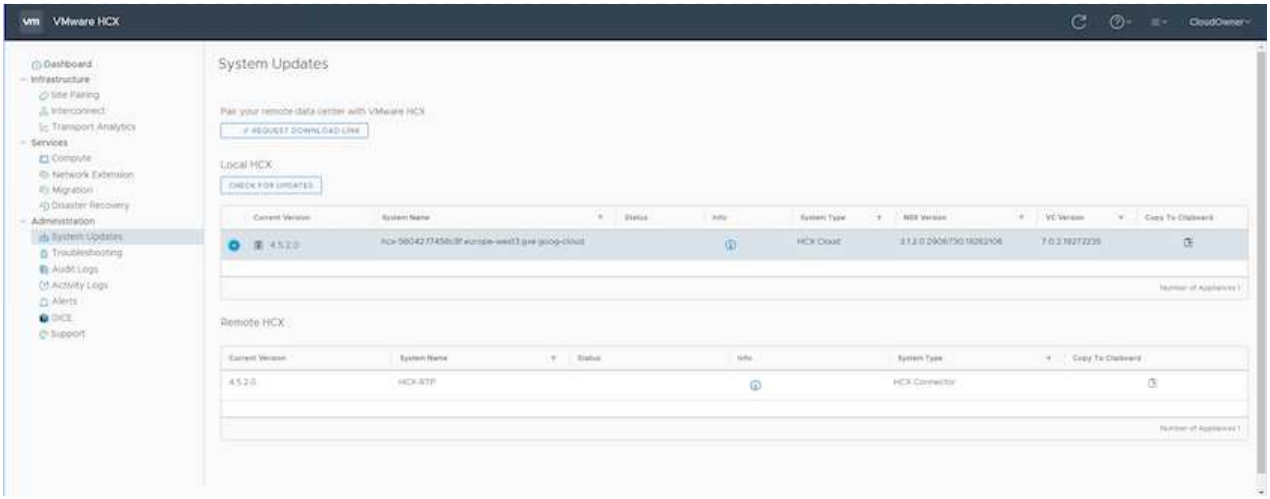
   Puede iniciar sesión en la consola HCX haciendo clic en el enlace de la versión HCX

   O bien, haga clic en HCX FQDN en la pestaña vSphere Management Network.

2. En HCX Cloud Manager, vaya a **Administración > actualizaciones del sistema**.
3. Haga clic en **solicitar enlace de descarga** y descargue el archivo OVA.



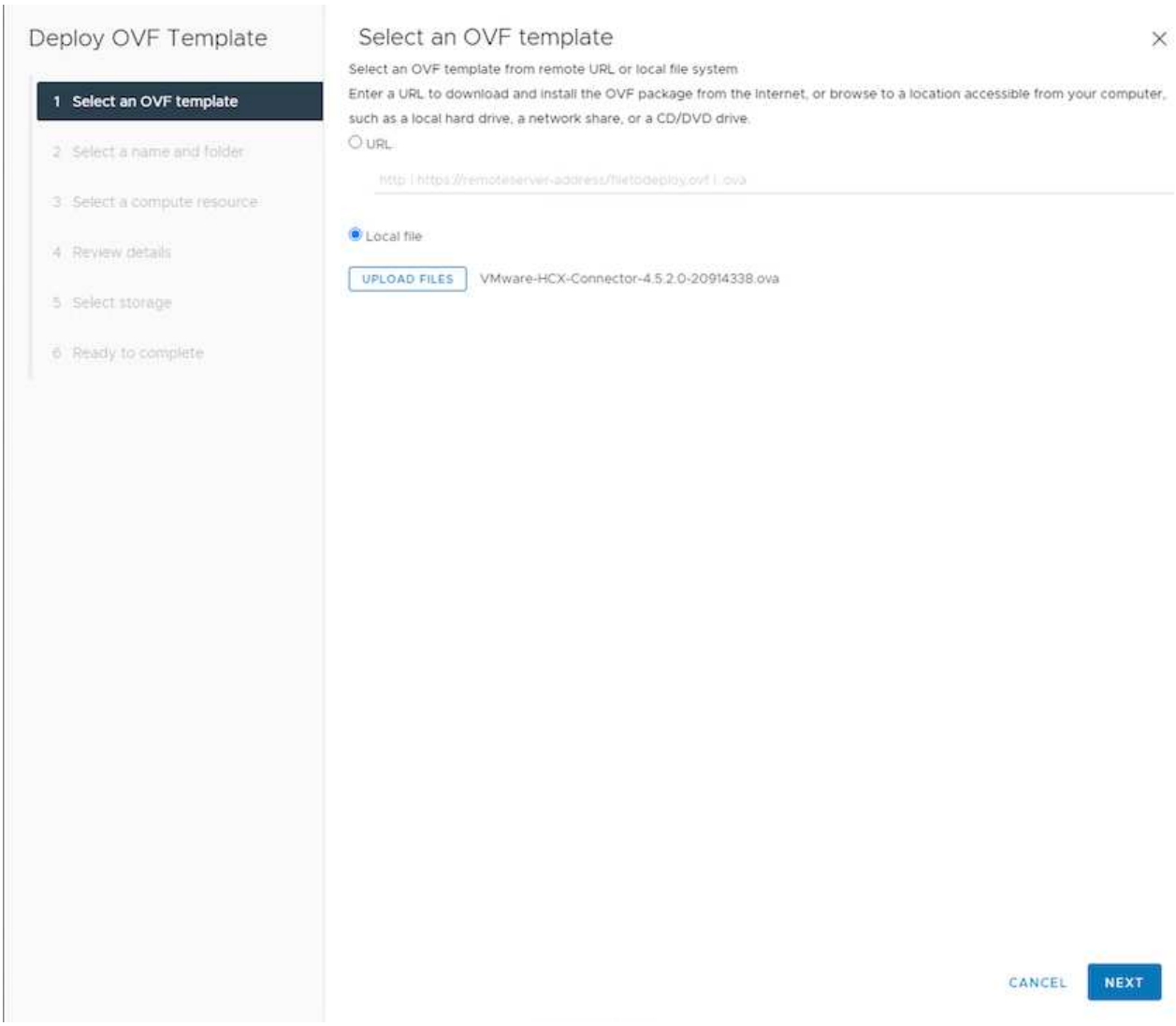
4. Actualice HCX Cloud Manager a la última versión disponible desde la interfaz de usuario de HCX Cloud Manager.

Paso 2: Ponga en marcha el OVA del instalador en la instancia local de vCenter Server

Para que el conector local se conecte al HCX Manager en Google Cloud VMware Engine, asegúrese de que los puertos de firewall adecuados están abiertos en el entorno local.

Para descargar e instalar el conector HCX en el vCenter Server local, complete los siguientes pasos:

1. Haga que la ova se descargue de la consola HCX en Google Cloud VMware Engine como se indica en el paso anterior.
2. Una vez descargado el OVA, póngalo en marcha en el entorno local de VMware vSphere mediante la opción **implementar plantilla OVF**.



3. Introduzca toda la información necesaria para la implementación de OVA, haga clic en **Siguiente** y, a continuación, haga clic en **Finalizar** para implementar el OVA del conector HCX de VMware.

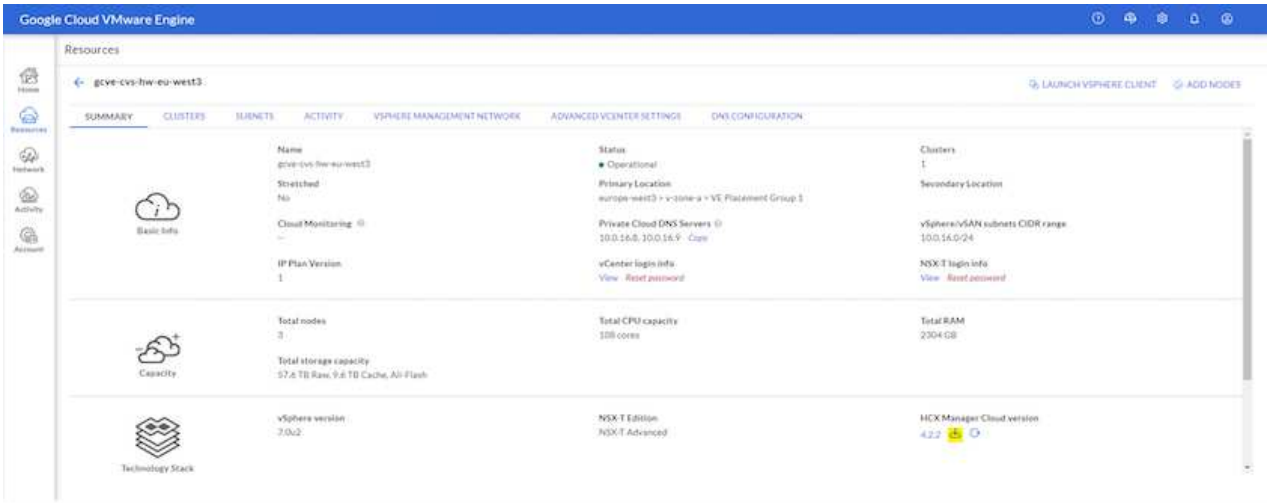
> Encienda el dispositivo virtual manualmente.

Para obtener instrucciones paso a paso, consulte "Guía del usuario de VMware HCX".

Paso 3: Active el conector HCX con la clave de licencia

Después de implementar el OVA del conector HCX de VMware en las instalaciones e iniciar el dispositivo, lleve a cabo los siguientes pasos para activar el conector HCX. Genere la clave de licencia desde el portal Google Cloud VMware Engine y actívela en VMware HCX Manager.

1. En el portal VMware Engine, haga clic en Resources, seleccione la nube privada y **haga clic en el icono de descarga en HCX Manager Cloud Version**
.



Abra el archivo descargado y copie la cadena de claves de licencia.

2. Inicie sesión en el VMware HCX Manager local en "https://hcxmanagerIP:9443" uso de las credenciales de administrador.

> Utilice hcxmanagerIP y la contraseña definidos durante la implementación de OVA.

3. En la licencia, introduzca la clave copiada del paso 3 y haga clic en **Activar**.

> El conector HCX de las instalaciones debe tener acceso a Internet.

4. En **Datacenter Location**, proporcione la ubicación más cercana para instalar el VMware HCX Manager en las instalaciones. Haga clic en **continuar**.
5. En **Nombre del sistema**, actualice el nombre y haga clic en **continuar**.
6. Haga clic en **Sí, continuar**.
7. En **Conecte su vCenter**, proporcione el nombre de dominio completo (FQDN) o la dirección IP de vCenter Server y las credenciales adecuadas, y haga clic en **continuar**.

> Utilice el FQDN para evitar problemas de conectividad más adelante.

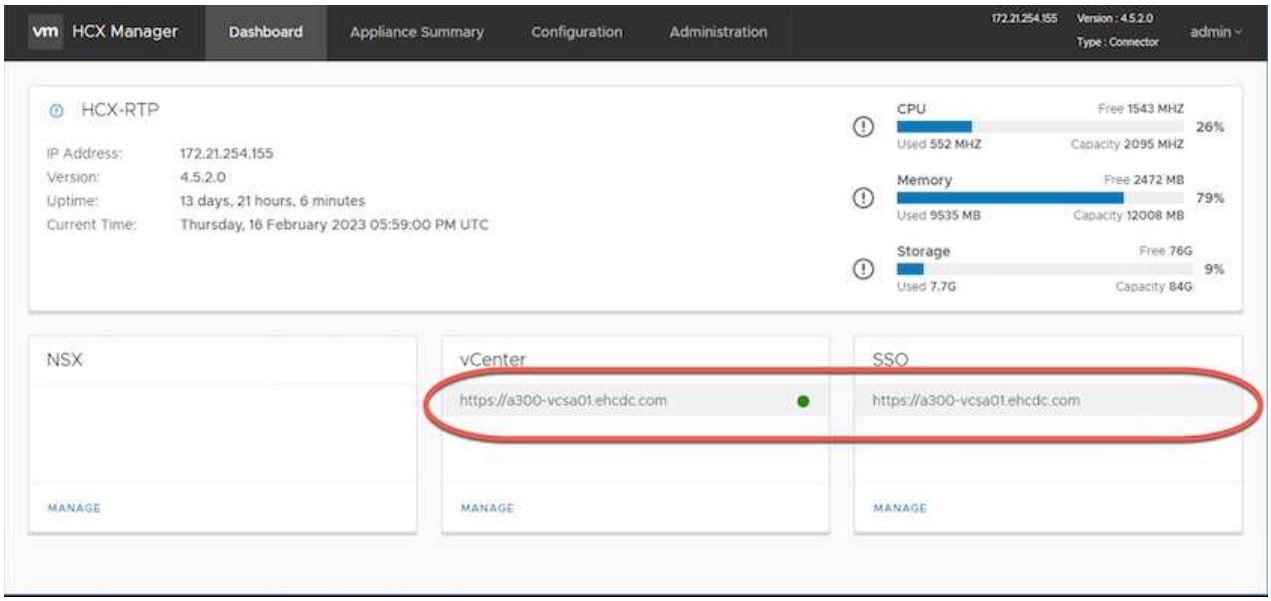
8. En **Configurar SSO/PSC**, proporcione el FQDN o la dirección IP del controlador de servicios de plataforma (PSC) y haga clic en **continuar**.

> Para el PSC integrado, introduzca el FQDN de VMware vCenter Server o la dirección IP.

9. Compruebe que la información introducida es correcta y haga clic en **Reiniciar**.

10. Después de reiniciar los servicios, vCenter Server se muestra como verde en la página que aparece. Tanto vCenter Server como SSO deben tener los parámetros de configuración adecuados, que deben ser los mismos que los de la página anterior.

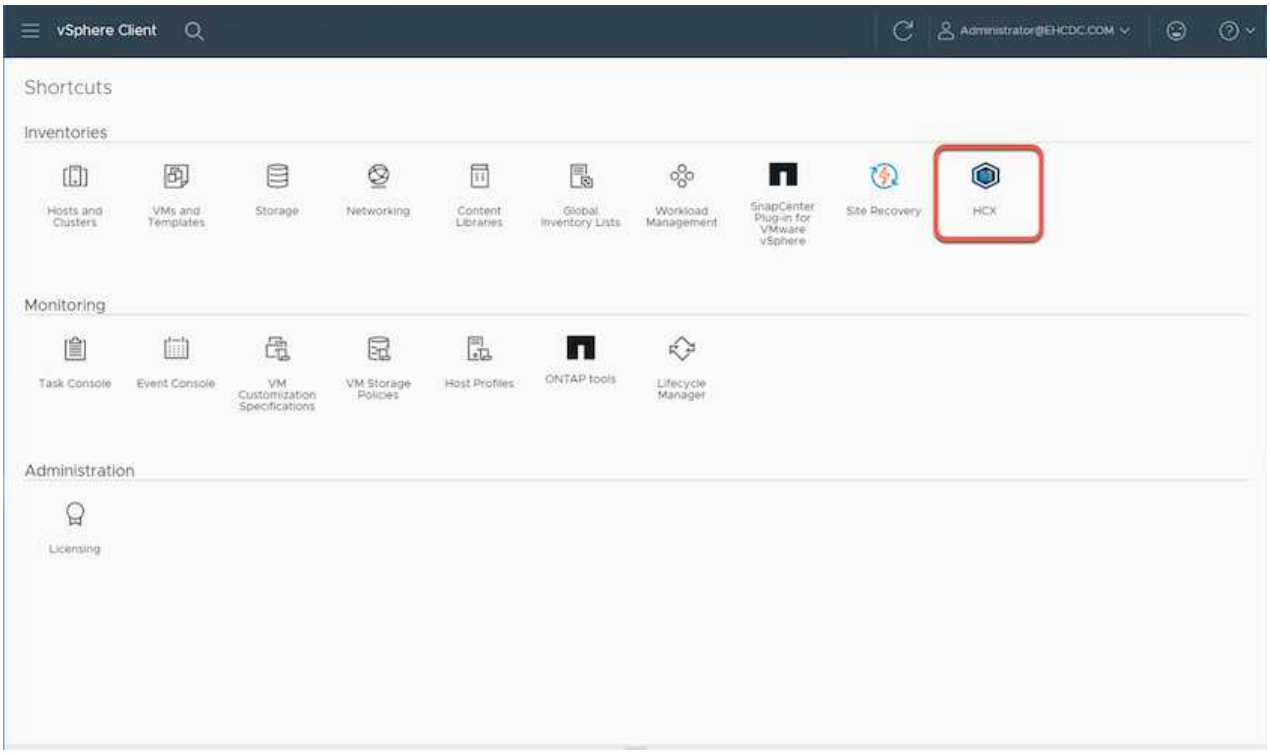
> Este proceso debe tardar aproximadamente de 10 a 20 minutos y el plugin se añadirá a vCenter Server.



Paso 4: Emparejar el conector VMware HCX en las instalaciones con Google Cloud VMware Engine HCX Cloud Manager

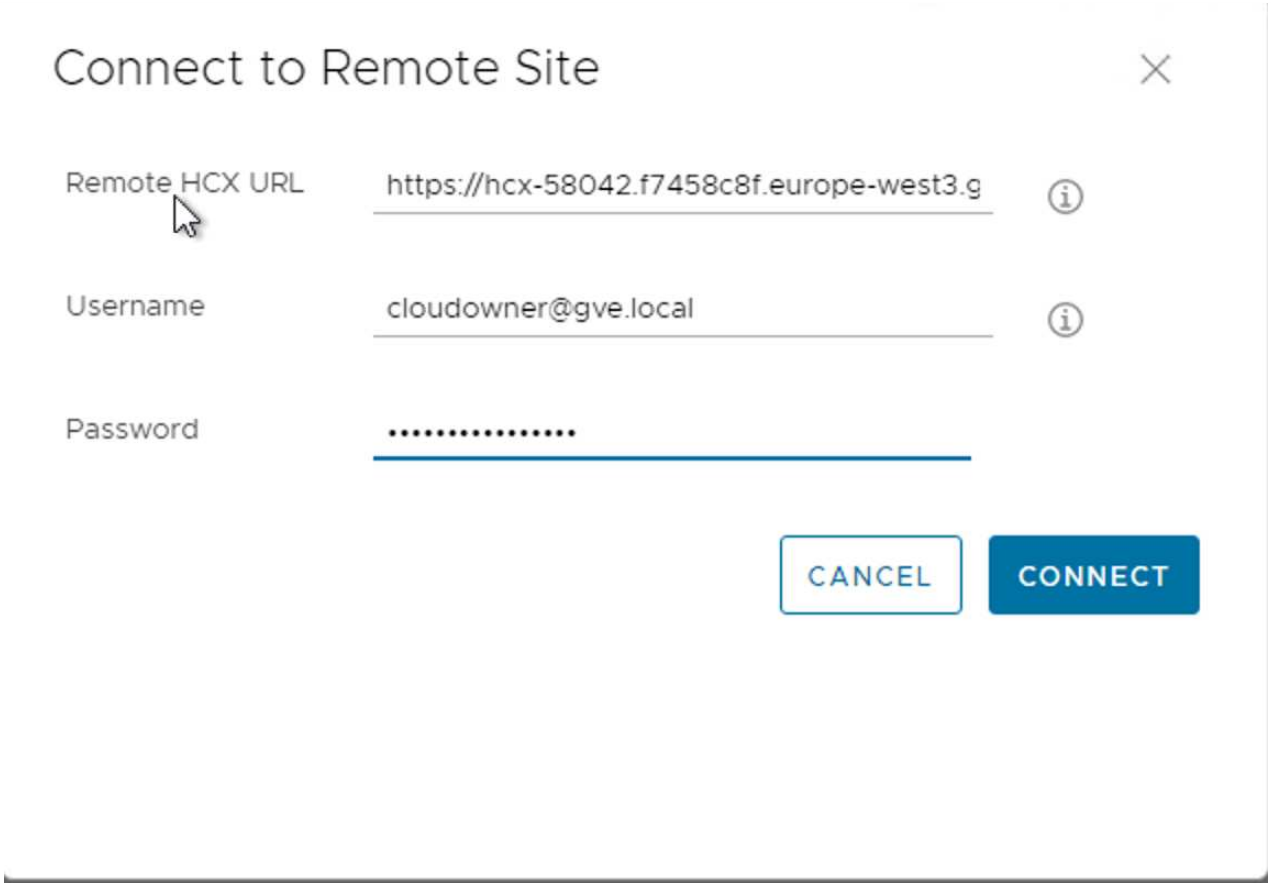
Después de implementar y configurar el conector HCX en el vCenter local, establezca la conexión con Cloud Manager añadiendo el emparejamiento. Para configurar el emparejamiento de sitios, lleve a cabo los siguientes pasos:

1. Para crear una pareja de sitios entre el entorno local de vCenter y el motor SDDC de Google Cloud VMware, inicie sesión en la instancia local de vCenter Server y acceda al nuevo complemento HCX vSphere Web Client.



2. En Infraestructura, haga clic en **Agregar un emparejamiento de sitios**.

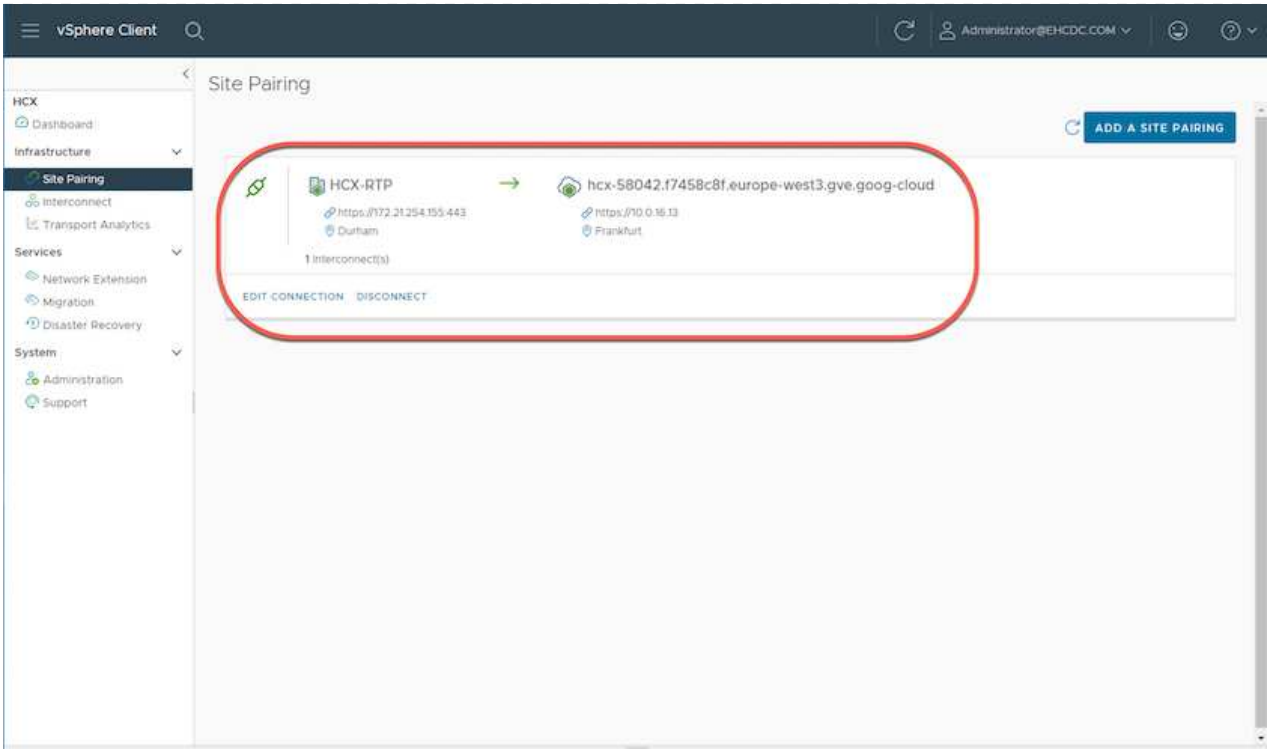
> Introduzca la dirección URL o dirección IP de HCX Cloud Manager de Google Cloud Engine y las credenciales para el usuario con privilegios de rol de propietario de cloud para acceder al cloud privado.



3. Haga clic en **conectar**.

> El conector HCX de VMware debe poder enrutar a HCX Cloud Manager IP a través del puerto 443.

4. Una vez creado el emparejamiento, el emparejamiento de sitios recién configurado está disponible en el panel de HCX.

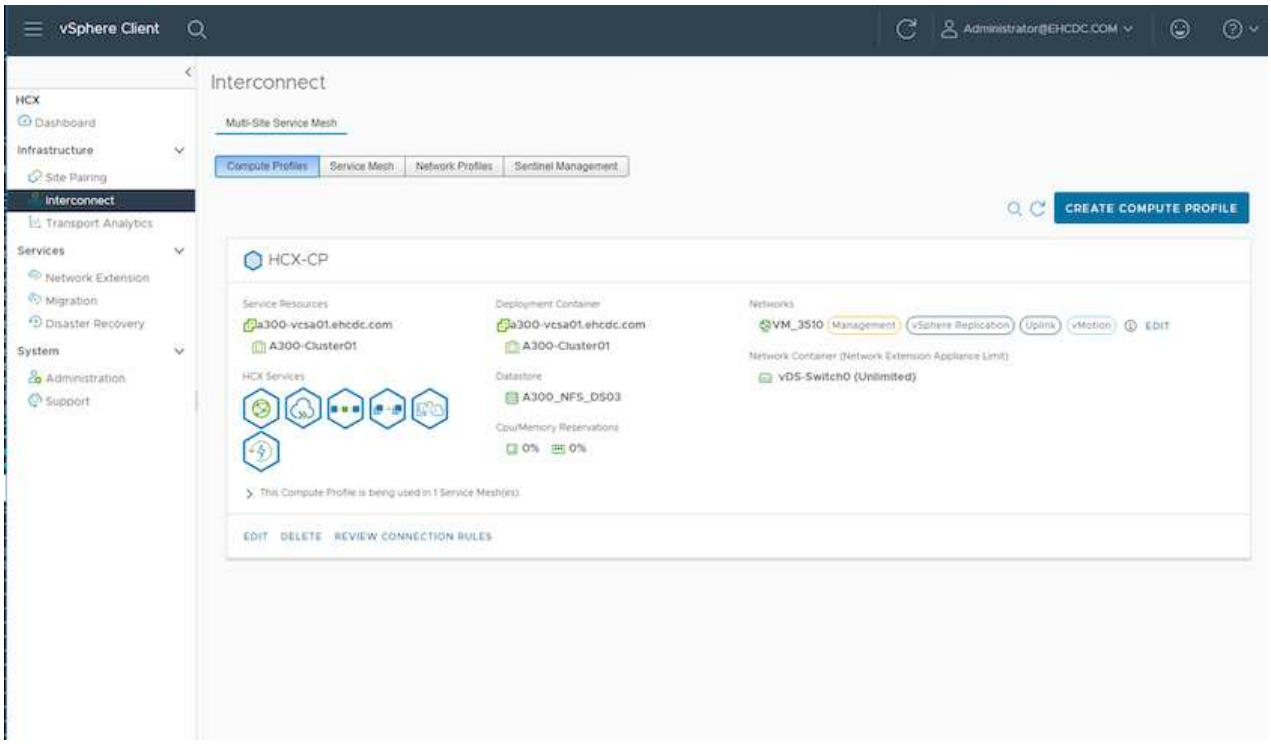

vSphere Client
Administrator@EHCDC.COM
HCX
Dashboard
Infrastructure
Site Pairing
Interconnect
Transport Analytics
Services
Network Extension
Migration
Disaster Recovery
System
Administration
Support
Site Pairing
ADD A SITE PAIRING
HCX-RTP
https://172.21.254.155:443
Durham
1 Interconnect(s)
hcx-58042.f7458c8f.europe-west3.gve.goog-cloud
https://10.0.16.13
Frankfurt
EDIT CONNECTION
DISCONNECT

Paso 5: Configure el perfil de red, el perfil de computación y la malla de servicio

El dispositivo de servicio VMware HCX Interconnect proporciona funcionalidades de replicación y migración basada en vMotion a través de Internet y conexiones privadas al sitio de destino. La interconexión ofrece cifrado, ingeniería de tráfico y movilidad de máquinas virtuales. Para crear un dispositivo de servicio de interconexión, lleve a cabo los siguientes pasos:

1. En Infraestructura, seleccione **interconexión > malla de servicio multisitio > Perfiles de computación > Crear perfil de computación**.

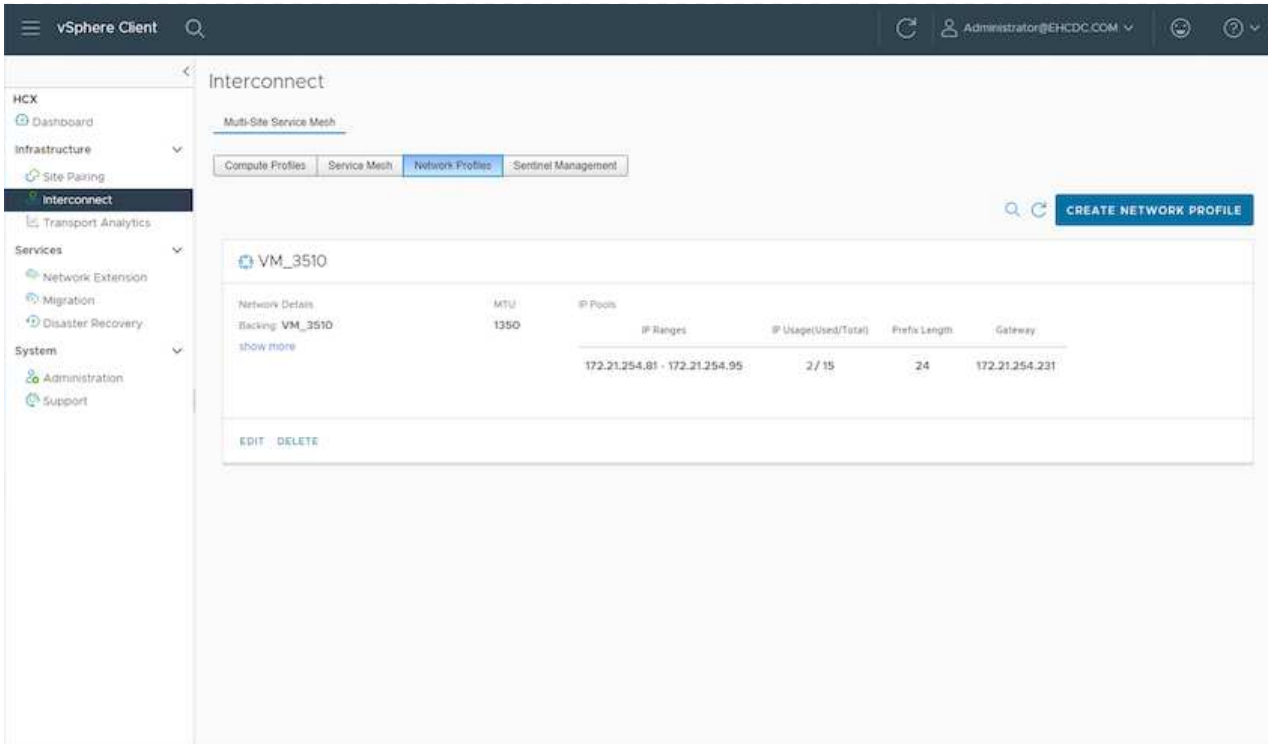
   Los perfiles informáticos definen los parámetros de implementación, incluidos los dispositivos que se implementan y qué parte del centro de datos de VMware puede acceder al servicio HCX.



2. Después de crear el perfil de computación, cree los perfiles de red seleccionando **malla de servicio multisitio > Perfiles de red > Crear perfil de red**.

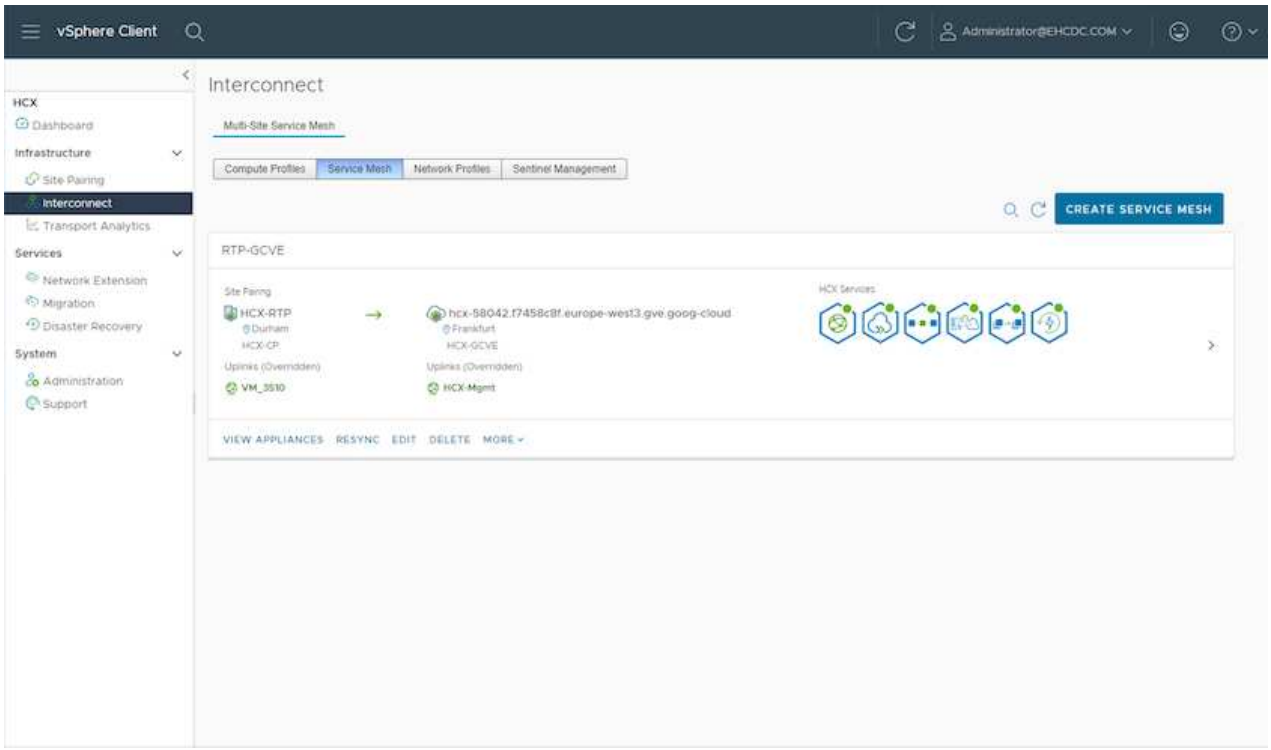
   El perfil de red define un rango de direcciones IP y redes que utiliza HCX para sus dispositivos virtuales.

   Este paso requiere dos o más direcciones IP. Estas direcciones IP se asignan desde la red de gestión a los dispositivos de interconexión.

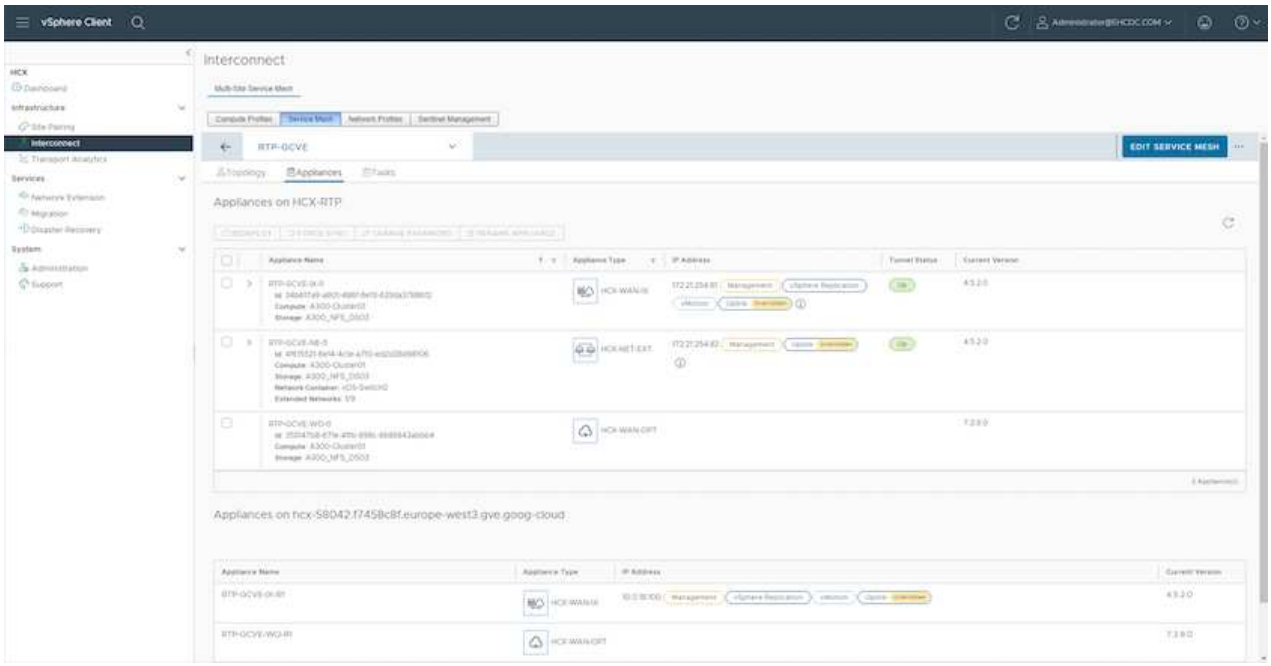


3. En este momento, se han creado correctamente los perfiles de computación y red.
4. Cree la malla de servicio seleccionando la pestaña **malla de servicio** en la opción **interconexión** y seleccione los sitios SDDC en las instalaciones y GCVE.
5. La malla de servicio especifica una pareja de perfiles de red y de computación local y remota.

> Como parte de este proceso, los dispositivos HCX se implementan y se configuran automáticamente tanto en los sitios de origen como en los de destino con el fin de crear una estructura de transporte segura.



6. Este es el paso final de la configuración. Esta operación debería tardar cerca de 30 minutos en completar la puesta en marcha. Una vez configurada la malla de servicio, el entorno está preparado con los túneles IPsec creados correctamente para migrar las VM de carga de trabajo.



Paso 6: Migrar cargas de trabajo

Las cargas de trabajo se pueden migrar de manera bidireccional entre los centros de datos de GCVE y sus instalaciones mediante diversas tecnologías de migración de VMware HCX. Los equipos virtuales se pueden mover hacia y desde entidades activadas por HCX de VMware mediante varias tecnologías de migración, como la migración masiva de HCX, HCX vMotion, migración en frío de HCX, el asistente de replicación de HCX vMotion (disponible con la edición de HCX Enterprise) y la migración asistida por SO HCX (disponible con la edición de HCX Enterprise).

Para obtener más información sobre varios mecanismos de migración de HCX, consulte "Tipos de migración HCX de VMware".

El dispositivo HCX-IX utiliza el servicio de agente de movilidad para realizar migraciones vMotion, de frío y de replicación asistida (RAV).

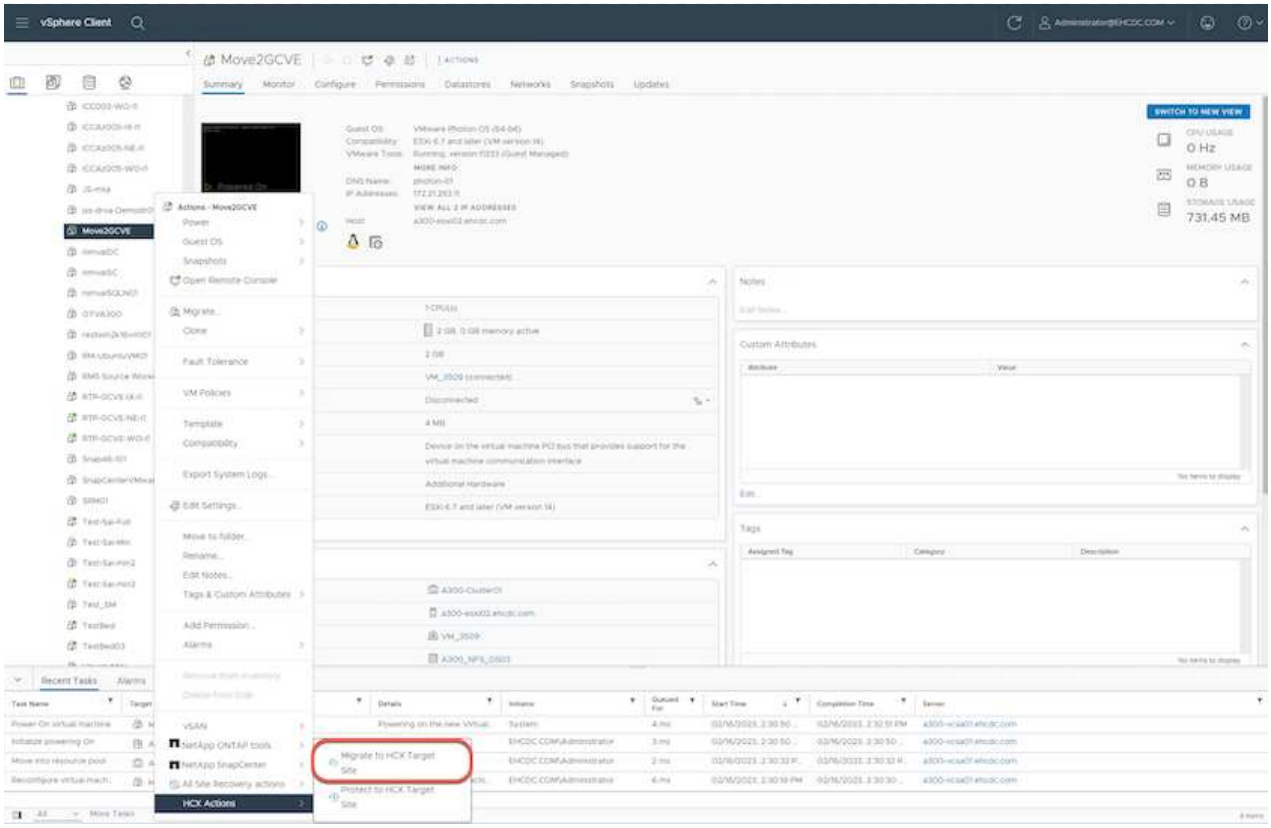
> El dispositivo HCX-IX agrega el servicio Mobility Agent como un objeto host en vCenter Server. El procesador, la memoria, los recursos de almacenamiento y redes que se muestran en este objeto no representan el consumo real en el hipervisor físico que aloja el dispositivo IX.

HCX vMotion

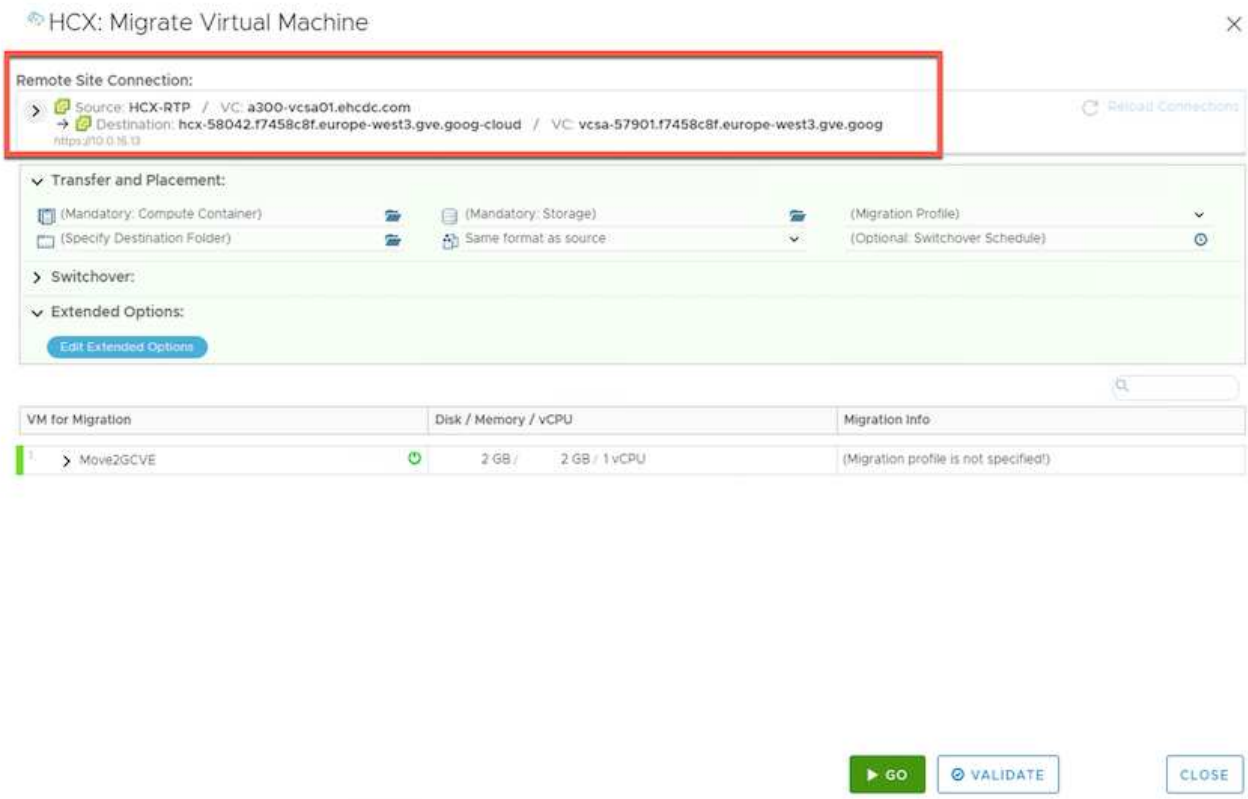
En esta sección se describe el mecanismo HCX vMotion. Esta tecnología de migración utiliza el protocolo VMware vMotion para migrar un equipo virtual a GCVE. La opción de migración de vMotion se utiliza para migrar el estado de las máquinas virtuales de una única máquina virtual a la vez. No se produce ninguna interrupción del servicio durante este método de migración.

> La extensión de red debe estar en su lugar (para el grupo de puertos en el que está conectada la máquina virtual) para migrar la máquina virtual sin necesidad de modificar la dirección IP.

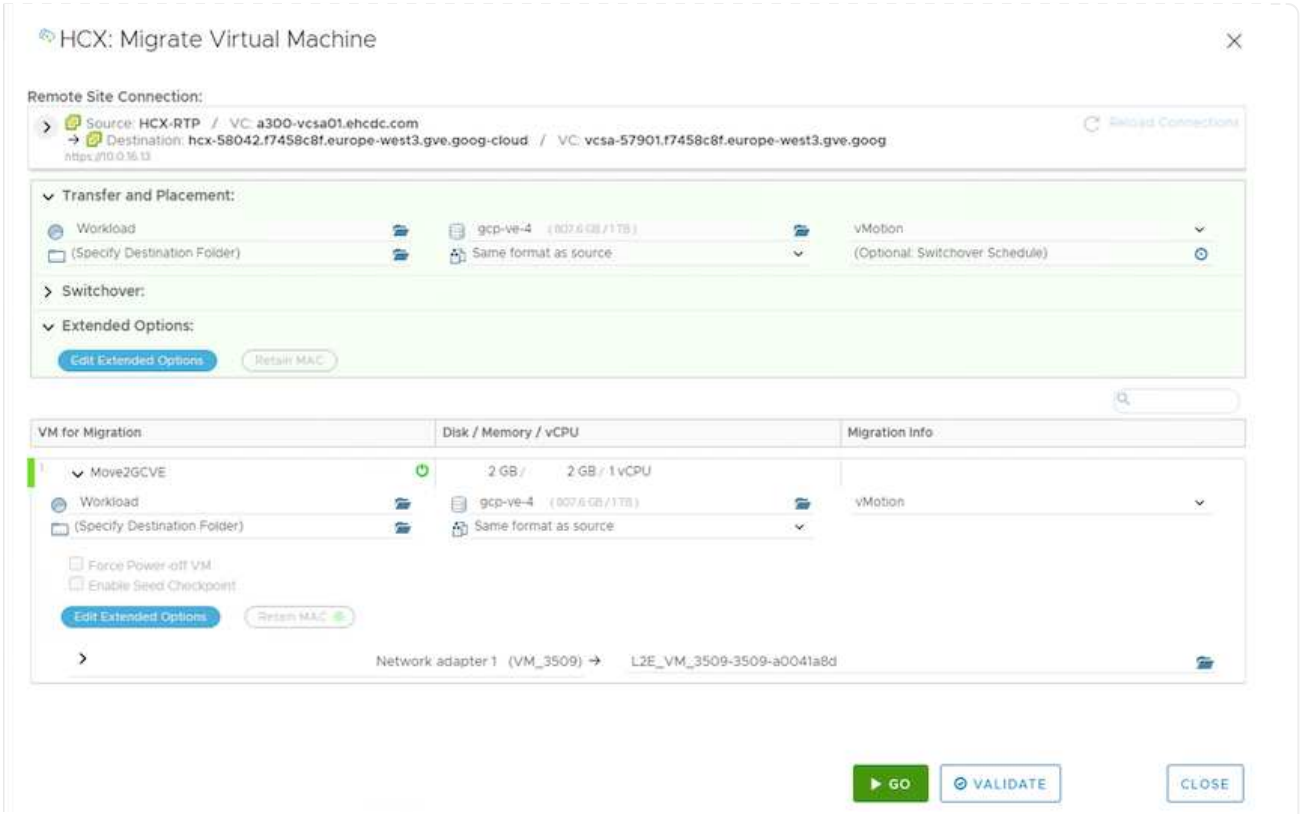
1. Desde el cliente vSphere local, vaya a Inventory, haga clic con el botón derecho en la máquina virtual que se va a migrar y seleccione HCX Actions > Migrate to HCX Target Site.



2. En el asistente Migrate Virtual Machine, seleccione Remote Site Connection (GCVE de destino).



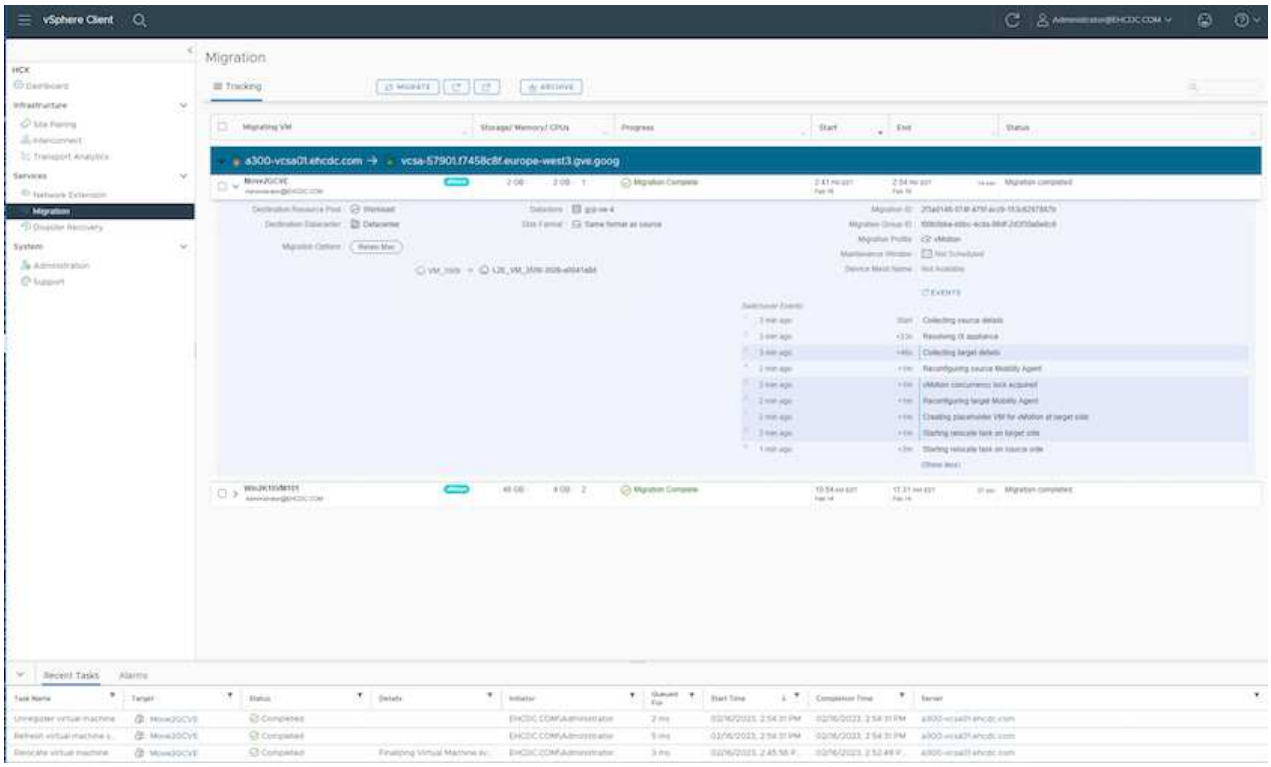
3. Actualice los campos obligatorios (clúster, almacenamiento y red de destino), haga clic en Validate.



4. Una vez finalizadas las comprobaciones de validación, haga clic en Ir para iniciar la migración.

> La transferencia de vMotion captura la memoria activa de la máquina virtual, su estado de ejecución, su dirección IP y su dirección MAC. Para obtener más información sobre los requisitos y las limitaciones de HCX vMotion, consulte "Comprender vMotion y la migración de datos fríos de VMware HCX".

5. Es posible supervisar el progreso y la finalización de vMotion desde el panel HCX > Migration.



El almacén de datos CVS NFS de destino debe tener espacio suficiente para manejar la migración.

Conclusión

Tanto si su objetivo es el cloud híbrido como el cloud, y los datos residen en un almacenamiento de cualquier tipo o proveedor en las instalaciones, Cloud Volume Service y HCX proporcionan opciones excelentes para poner en marcha y migrar las cargas de trabajo de las aplicaciones, a la vez que reduce el TCO porque los requisitos de datos se adaptan perfectamente a la capa de la aplicación. Sea cual sea el caso práctico, elija Google Cloud VMware Engine junto con Cloud Volume Service para obtener rápidamente las ventajas del cloud, una infraestructura consistente y operaciones en las instalaciones y en varios clouds, portabilidad bidireccional de cargas de trabajo, y capacidad y rendimiento de clase empresarial. Se trata del mismo proceso y procedimientos que ya conoce que se utiliza para conectar el almacenamiento y migrar máquinas virtuales mediante la replicación de VMware vSphere, VMware vMotion o incluso la copia de archivos de red (NFC).

Puntos

Los puntos clave de este documento son:

- Ahora puede usar Cloud Volume Service como almacén de datos en Google Cloud VMware Engine SDDC.
- Puede migrar datos fácilmente desde las instalaciones a un almacén de datos de Cloud Volume Service.
- Puede ampliar y reducir fácilmente el almacén de datos de Cloud Volume Service para satisfacer los requisitos de capacidad y rendimiento durante la actividad de migración.

Vídeos de Google y VMware como referencia

De Google

- "Despliegue el conector HCX con GCVE"
- "Configure HCX ServiceMesh con GCVE"
- "Migrar VM con HCX a GCVE"

De VMware

- "Despliegue del conector HCX para GCVE"
- "Configuración DE ServiceMesh DE HCX para GCVE"
- "Migración de carga de trabajo HCX a GCVE"

Dónde encontrar información adicional

Si quiere más información sobre la información descrita en este documento, consulte los siguientes enlaces a sitios web:

- Documentación de Google Cloud VMware Engine

  "https://cloud.google.com/vmware-engine/docs/overview"

- Documentación de Cloud Volume Service

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes"

- Guía del usuario de VMware HCX

  "https://docs.vmware.com/en/VMware-HCX/index.html"

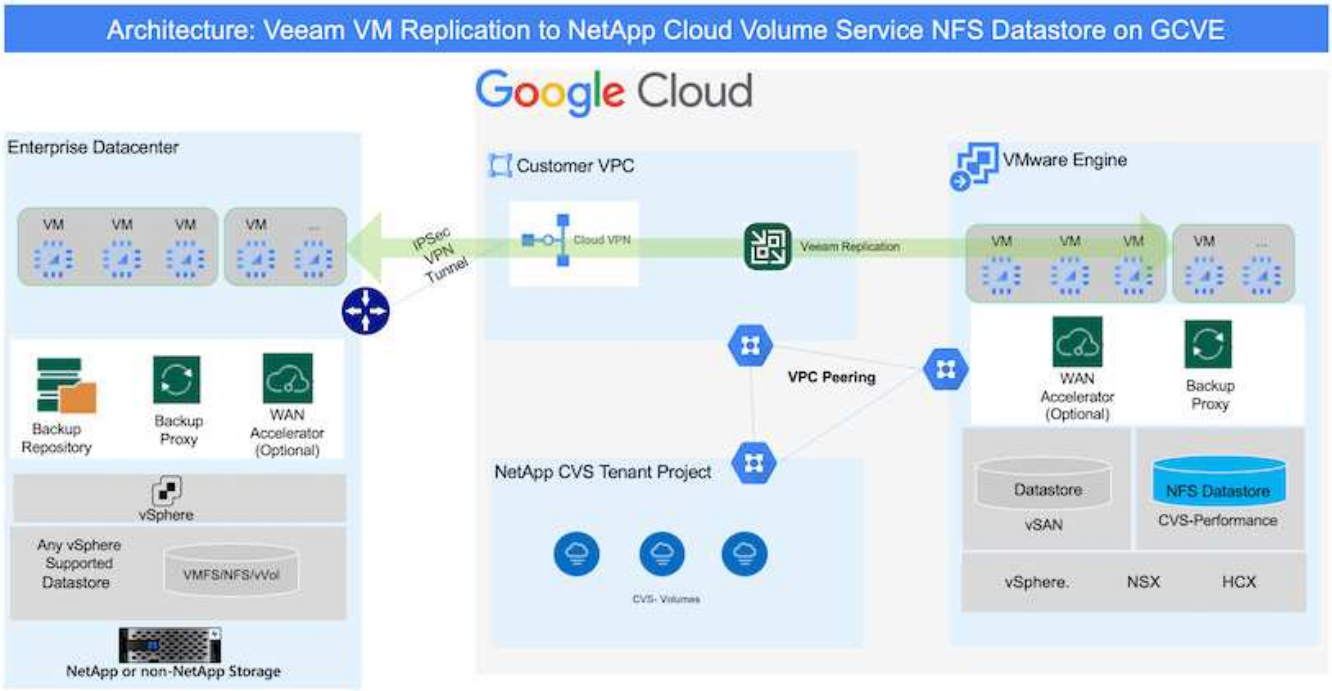
Migración de máquinas virtuales a NetApp Cloud Volume Service NFS Datastore en Google Cloud VMware Engine mediante la función de replicación de Veeam

Descripción general

Autores: Suresh Thoppay, NetApp

Las cargas de trabajo de máquinas virtuales que se ejecutan en VMware vSphere se pueden migrar a Google Cloud VMware Engine (GCVE) mediante la función de replicación de Veeam.

Este documento proporciona un enfoque paso a paso para configurar y realizar la migración de VM que utiliza el servicio Cloud Volume de NetApp, Veeam y el motor de VMware de Google Cloud (GCVE).



Supuestos

En este documento se asume que tiene Google Cloud VPN o Cloud Interconnect u otra opción de red para establecer la conectividad de red desde los servidores vSphere existentes a Google Cloud VMware Engine.

> Existen múltiples opciones para conectar los centros de datos en las instalaciones a Google Cloud, lo que nos impide esbozar un flujo de trabajo específico en este documento.
> Consulte la "Documentación de Google Cloud" Para el método de conectividad de on-premises a Google adecuado.

Puesta en marcha de la solución de migración

Descripción general de la puesta en marcha de soluciones

1. Asegúrese de que el almacén de datos NFS del servicio NetApp Cloud Volume esté montado en GCVE vCenter.
2. Compruebe que Veeam Backup Recovery se implementa en el entorno de VMware vSphere existente
3. Crear trabajo de replicación para iniciar la replicación de máquinas virtuales en la instancia de Google Cloud VMware Engine.
4. Realizar failover del trabajo de replicación de Veeam.
5. Realice failover permanente en Veeam.

Detalles de la implementación

Asegúrese de que el almacén de datos NFS del servicio NetApp Cloud Volume esté montado en GCVE vCenter

Inicie sesión en GCVE vCenter y asegúrese de que el almacén de datos NFS tenga espacio suficiente disponible.
Si no es así, consulte "Monte NetApp CVS como almacén de datos NFS en GCVE"

Compruebe que Veeam Backup Recovery se implementa en el entorno de VMware vSphere existente

Consulte "Componentes de replicación de Veeam" documentación para instalar los componentes requeridos.

Crear trabajo de replicación para iniciar la replicación de máquinas virtuales en la instancia de Google Cloud VMware Engine.

Tanto el vCenter en las instalaciones como el vCenter de GCVE deben registrarse con Veeam. "Configure el trabajo de replicación de máquina virtual de vSphere"
Aquí hay un video que explica cómo hacerlo
"Configurar trabajo de replicación".

> La VM de réplica puede tener una IP diferente a la VM de origen y también puede conectarse a un grupo de puertos diferente. Para obtener más detalles, consulte el vídeo de arriba.

Realizar failover del trabajo de replicación de Veeam

Para migrar máquinas virtuales, ejecute el "Realice el failover"

Realice failover permanente en Veeam.

Para tratar a GCVE como su nuevo entorno de origen, realice "Recuperación tras fallos permanente"

Ventajas de esta solución

- La infraestructura existente de backup de Veeam puede utilizarse para la migración.
- Veeam Replication permite cambiar las direcciones IP de VM en el sitio de destino.
- Tiene la capacidad de reasignar los datos existentes replicados fuera de Veeam (como los datos replicados de BlueXP)
- Tiene capacidad para especificar diferentes grupos de puertos de red en el sitio de destino.
- Puede especificar el orden de encendido de las máquinas virtuales.
- Utiliza VMware Change Block Tracking para minimizar la cantidad de datos que se deben enviar a través de la WAN.
- Capacidad para ejecutar scripts previos y posteriores para la replicación.
- Capacidad para ejecutar scripts previos y posteriores para instantáneas.

Disponibilidad de región – almacén de datos NFS complementario para Google Cloud Platform (GCP)

El almacén de datos NFS complementario para GCVE es compatible con el servicio de volúmenes de cloud de NetApp.

> Solo se pueden usar volúmenes de CVS-Performance para el almacén de datos NFS de GCVE. Para conocer la ubicación disponible, consulte "Mapa de región global"

Google Cloud VMware Engine está disponible en las siguientes ubicaciones

asia-northeast1 > v-zone-a > VE Placement Group 1
asia-northeast1 > v-zone-a > VE Placement Group 2
asia-south1 > v-zone-a > VE Placement Group 2
asia-south1 > v-zone-a > VE Placement Group 1
asia-southeast1 > v-zone-a > VE Placement Group 1
asia-southeast1 > v-zone-a > VE Placement Group 2
australia-southeast1 > v-zone-b > VE Placement Group 1
australia-southeast1 > v-zone-a > VE Placement Group 1
australia-southeast1 > v-zone-b > VE Placement Group 2
australia-southeast1 > v-zone-a > VE Placement Group 2
europe-west2 > v-zone-a > VE Placement Group 2
europe-west2 > v-zone-a > VE Placement Group 1
europe-west3 > v-zone-b > VE Placement Group 2
europe-west3 > v-zone-a > VE Placement Group 3
europe-west3 > v-zone-a > VE Placement Group 4
europe-west3 > v-zone-b > VE Placement Group 1
europe-west3 > v-zone-a > VE Placement Group 2
europe-west3 > v-zone-a > VE Placement Group 1
europe-west4 > v-zone-a > VE Placement Group 2
europe-west4 > v-zone-a > VE Placement Group 1
europe-west6 > v-zone-a > VE Placement Group 1
europe-west8 > v-zone-a > VE Placement Group 1
northamerica-northeast1 > v-zone-a > VE Placement Group 1
northamerica-northeast1 > v-zone-a > VE Placement Group 2
northamerica-northeast2 > v-zone-a > VE Placement Group 2
northamerica-northeast2 > v-zone-a > VE Placement Group 1
southamerica-east1 > v-zone-a > VE Placement Group 1
southamerica-east1 > v-zone-a > VE Placement Group 2
us-central1 > v-zone-a > VE Placement Group 2
us-central1 > v-zone-a > VE Placement Group 5
us-central1 > v-zone-a > VE Placement Group 1
us-central1 > v-zone-a > VE Placement Group 3
us-east4 > v-zone-a > VE Placement Group 5
us-east4 > v-zone-a > VE Placement Group 10
us-east4 > v-zone-a > VE Placement Group 6
us-east4 > v-zone-a > VE Placement Group 3
us-east4 > v-zone-b > VE Placement Group 5
us-east4 > v-zone-a > VE Placement Group 1
us-east4 > v-zone-b > VE Placement Group 1
us-east4 > v-zone-a > VE Placement Group 4
us-east4 > v-zone-b > VE Placement Group 6
us-east4 > v-zone-a > VE Placement Group 2
us-west2 > v-zone-a > VE Placement Group 3
us-west2 > v-zone-a > VE Placement Group 4
us-west2 > v-zone-a > VE Placement Group 5
us-west2 > v-zone-a > VE Placement Group 2
us-west2 > v-zone-a > VE Placement Group 1
us-west2 > v-zone-a > VE Placement Group 6

Para minimizar la latencia, NetApp CVS Volume y GCVE, donde se intenta montar el volumen, deben estar en la misma zona de disponibilidad.
Trabaja con Google y NetApp Solution Architects para obtener optimizaciones de TCO y disponibilidad.

Descripción general de la seguridad: Cloud Volumes Service de NetApp (CVS) en Google Cloud

TR-4918: Descripción general de la seguridad: Cloud Volumes Service de NetApp en Google Cloud

Oliver Krause, Justin Parisi, NetApp

Alcance del documento

La seguridad, especialmente en el cloud, donde la infraestructura se encuentra fuera del control de los administradores de almacenamiento, es primordial para confiar en sus datos para ofrecer servicios ofrecidos por los proveedores de cloud. Este documento ofrece una visión general de las ofertas de seguridad de NetApp "Cloud Volumes Service proporciona en Google Cloud".

Audiencia de destino

La audiencia de destino de este documento incluye, entre otros, los siguientes roles:

- Proveedores de cloud
- Administradores de almacenamiento
- Arquitectos de almacenamiento
- Recursos sobre el terreno
- Responsables de la toma de decisiones empresariales

Si tiene alguna pregunta sobre el contenido de este informe técnico, consulte la sección "“Contacto”."

Abreviatura	Definición
CVS-SW	Cloud Volumes Service, tipo de servicio CVS
CVS-Performance	Cloud Volume Service, tipo de servicio CVS-Performance
SAL	

Cómo Cloud Volumes Service en Google Cloud protege sus datos

Cloud Volumes Service en Google Cloud ofrece múltiples formas de proteger sus datos de forma nativa.

Arquitectura segura y modelo de multi-tenancy

Cloud Volumes Service proporciona una arquitectura segura en Google Cloud al segmentar la gestión de servicios (plano de control) y el acceso a los datos (plano de datos) en diferentes extremos, de modo que ninguno de ellos puede afectar al otro (consulte la sección "“Arquitectura Cloud Volumes Service”"). Utiliza Google’s. "acceso a servicios privados" (PSA) marco para prestar el servicio. Este marco distingue entre el

productor de servicios, que ofrece NetApp y está gestionado por este, y el consumidor de servicios, que es un cloud privado virtual (VPC) en un proyecto de cliente, alojando los clientes que deseen acceder a recursos compartidos de archivos de Cloud Volumes Service.

En esta arquitectura, los clientes (consulte la sección ""Modelo de soporte"") Se definen como proyectos de Google Cloud que están completamente aislados entre sí a menos que el usuario lo conecte explícitamente. Los clientes permiten el aislamiento completo de volúmenes de datos, servicios de nombres externos y otras piezas esenciales de la solución de otros clientes con la plataforma de volúmenes de Cloud Volumes Service. Dado que la plataforma Cloud Volumes Service se conecta a través de la agrupación VPC, ese aislamiento también se aplica a ella. Para habilitar el uso compartido de volúmenes de Cloud Volumes Service entre varios proyectos, utilice un VPC compartido (consulte la sección ""VPC compartidos""). Puede aplicar controles de acceso a recursos compartidos de SMB y exportaciones de NFS para limitar quién o qué puede ver o modificar conjuntos de datos.

Gestión de identidades sólida para el plano de control

En el plano de control en el que se lleva a cabo la configuración de Cloud Volumes Service, la gestión de identidades se gestiona mediante "Gestión de acceso a identidades (IAM)". IAM es un servicio estándar que permite controlar la autenticación (inicios de sesión) y la autorización (permisos) de las instancias de proyectos de Google Cloud. Toda la configuración se realiza con las API de Cloud Volumes Service mediante un transporte HTTPS seguro con cifrado TLS 1.2 y la autenticación se realiza mediante tokens JWT para mayor seguridad. La interfaz de usuario de la consola de Google para Cloud Volumes Service convierte las entradas del usuario en llamadas a la API de Cloud Volumes Service.

Seguridad reforzada: Limitar las superficies de ataque

Parte de la seguridad efectiva está limitando el número de superficies de ataque disponibles en un servicio. Las superficies de ataque pueden incluir diversas cosas, como datos en reposo, transferencias en tránsito, inicios de sesión y los propios conjuntos de datos.

Un servicio gestionado elimina algunas de las superficies de ataque de forma inherente en su diseño. Gestión de infraestructuras, como se describe en la sección ""Funcionamiento de servicio"," es manejado por un equipo específico y es automatizado para reducir el número de veces que un ser humano realmente toca configuraciones, lo que ayuda a reducir el número de errores intencionales y no intencionales. La conexión de red está cerrada de modo que solo los servicios necesarios puedan acceder los unos a los otros. El cifrado se lleva a cabo en el almacenamiento de datos, y solo el plano de datos necesita atención de seguridad de los administradores de Cloud Volumes Service. Al ocultar la mayor parte de la gestión de una interfaz API, la seguridad se logra limitando las superficies de ataque.

Modelo de confianza cero

Históricamente, la filosofía de seguridad DE TI ha sido confiar pero verificar, y se ha manifestado basándose únicamente en mecanismos externos (como firewalls y sistemas de detección de intrusiones) para mitigar las amenazas. Sin embargo, los ataques y las infracciones evolucionaron para evitar la verificación en entornos mediante el phishing, la ingeniería social, las amenazas internas y otros métodos que proporcionan la verificación para entrar en redes y causar estragos.

Zero Trust se ha convertido en una nueva metodología en seguridad, con el mantra actual “confiar en nada mientras sigue verificando todo”. Por lo tanto, no se permite el acceso predeterminado a nada. Este mantra se aplica de diversas maneras, incluidos los cortafuegos estándar y los sistemas de detección de intrusiones (IDS) y también con los siguientes métodos:

- Métodos de autenticación sólidos (como Kerberos con cifrado AES o tokens JWT)
- Fuentes sólidas de identidades únicas (como Windows Active Directory, Lightweight Directory Access

Protocol (LDAP) y Google IAM)

- Segmentación de red y multi-tenancy seguro (solo se permite el acceso de forma predeterminada a los inquilinos)
- Controles de acceso granular con políticas de acceso con privilegios mínimos
- Listas exclusivas pequeñas de administradores dedicados y de confianza con auditorías digitales y pistas en papel

La ejecución de Cloud Volumes Service en Google Cloud cumple con el modelo Zero Trust, al implementar la postura "no confiar en nada, verificar todo".

Cifrado

Cifrar datos en reposo (consulte la sección ""Cifrado de datos en reposo"") Mediante el uso de cifrados XTS-AES-256 con el cifrado de volúmenes de NetApp (NVE) y en tránsito con ""Cifrado SMB"" O soporte para NFS Kerberos 5p. Las transferencias de replicación entre regiones con REST sencilla están protegidas con cifrado TLS 1.2 (consulte la sección ""Replicación entre regiones""). Además, Google Networking también proporciona comunicaciones cifradas (consulte la sección ""Cifrado de datos en tránsito"") para una capa adicional de protección contra ataques. Para obtener más información sobre el cifrado de transporte, consulte la sección ""Red de Google Cloud"".

Protección de datos y backups

La seguridad no se trata sólo de la prevención de ataques. También se trata de cómo recuperamos los ataques cuando se producen. Esta estrategia incluye protección de datos y backups. Cloud Volumes Service proporciona métodos para replicar en otras regiones en caso de interrupciones del servicio (consulte la sección ""Replicación entre regiones"") o si un conjunto de datos se ve afectado por un ataque de ransomware. También puede realizar backups asíncronos de datos en ubicaciones externas a la instancia de Cloud Volumes Service mediante el uso de "Backup de Cloud Volumes Service". Con los backups periódicos, la mitigación de los eventos de seguridad puede llevar menos tiempo y ahorrar dinero y angustia para los administradores.

Mitigación de ransomware rápida con copias Snapshot líderes en el sector

Además de la protección de datos y los backups, Cloud Volumes Service ofrece compatibilidad con copias Snapshot inalterables (consulte la sección ""Copias Snapshot inmutables"") de volúmenes que permiten la recuperación de ataques de ransomware (consulte la sección ""Funcionamiento de servicio"") en cuestión de segundos de descubrir el problema y con una interrupción mínima. El tiempo y los efectos de la recuperación dependen de la programación de la copia Snapshot, pero puede crear copias de SnapVault que proporcionen deltas de solo una hora en ataques de ransomware. Las copias Snapshot afectan al rendimiento y al uso de la capacidad y son un enfoque de bajo riesgo y gran recompensa para proteger sus conjuntos de datos.

Consideraciones de seguridad y superficies de ataque

El primer paso para comprender cómo proteger los datos es identificar los riesgos y las posibles superficies de ataque.

Estos incluyen (pero no se limitan a) lo siguiente:

- Administración y inicios de sesión
- Datos en reposo
- Datos en movimiento

- Red y firewalls
- Ransomware, malware y virus

Comprender las superficies de ataque puede ayudarle a proteger mejor sus entornos. Cloud Volumes Service en Google Cloud ya considera muchos de estos temas e implementa la funcionalidad de seguridad de forma predeterminada, sin ninguna interacción administrativa.

Garantizar inicios de sesión seguros

Al proteger los componentes esenciales de su infraestructura, es fundamental asegurarse de que solo los usuarios aprobados puedan iniciar sesión y gestionar sus entornos. Si los agentes erróneos infringen sus credenciales administrativas, tienen las claves para el castillo y pueden hacer lo que quieran: Cambiar configuraciones, eliminar volúmenes y backups, crear puertas traseras o deshabilitar las programaciones de Snapshot.

Cloud Volumes Service para Google Cloud proporciona protección contra accesos administrativos no autorizados a través de la confusión del almacenamiento como servicio (StaaS). Cloud Volumes Service está completamente mantenido por el proveedor de cloud sin disponibilidad para iniciar sesión externamente. Todas las operaciones de configuración y configuración se automatizan por completo, por lo que un administrador humano nunca tiene que interactuar con los sistemas excepto en circunstancias muy raras.

Si se requiere inicio de sesión, Cloud Volumes Service en Google Cloud asegura los inicios de sesión manteniendo una lista muy corta de administradores de confianza que tienen acceso para iniciar sesión en los sistemas. Este método de gatekeeping ayuda a reducir el número de posibles malos actores con acceso. Además, la red de Google Cloud oculta los sistemas tras capas de seguridad de la red y sólo expone lo que se necesita al mundo exterior. Si quiere más información sobre la arquitectura de Google Cloud y Cloud Volumes Service, consulte la sección "“Arquitectura de Cloud Volumes Service”."

Administración de clústeres y actualizaciones

Dos áreas con riesgos potenciales de seguridad incluyen la administración de clústeres (lo que ocurre si un actor defectuoso tiene acceso de administrador) y las actualizaciones (lo que ocurre si una imagen de software está comprometida).

Protección en la administración del almacenamiento

El almacenamiento proporcionado como servicio elimina el riesgo añadido de exposición a los administradores al eliminar ese acceso a los usuarios finales fuera del centro de datos de cloud. En su lugar, la única configuración que se realiza es para el plano de acceso a los datos por parte de los clientes. Cada inquilino gestiona sus propios volúmenes y ningún inquilino puede llegar a otras instancias de Cloud Volumes Service. El servicio se gestiona mediante automatización, con una pequeña lista de administradores de confianza a los que se les da acceso a los sistemas a través de los procesos que se tratan en la sección "“Funcionamiento de servicio”."

El tipo de servicio CVS-Performance ofrece replicación entre regiones como una opción para proporcionar protección de datos a otra región en caso de un fallo en una región. En esos casos, Cloud Volumes Service puede realizar una conmutación por error a la región no afectada para mantener el acceso a los datos.

Actualizaciones de servicios

Las actualizaciones ayudan a proteger los sistemas vulnerables. Cada actualización proporciona mejoras de seguridad y correcciones de errores que minimizan las superficies de ataque. Las actualizaciones de software se descargan desde repositorios centralizados y se validan antes de permitir que las actualizaciones verifiquen que las imágenes oficiales se utilizan y que las actualizaciones no se ven comprometidas por

actores defectuosos.

Con Cloud Volumes Service, los equipos del proveedor de cloud se encargan de gestionar las actualizaciones, lo que elimina la exposición al riesgo para los equipos de administrador, al proporcionar a los expertos conocedor de la configuración y las actualizaciones, que han automatizado y probado totalmente el proceso. Las actualizaciones no son disruptivas, y Cloud Volumes Service mantiene las últimas actualizaciones para obtener los mejores resultados generales.

Para obtener información acerca del equipo de administrador que realiza estas actualizaciones de servicio, consulte la sección "“Funcionamiento de servicio”."

Protección de datos en reposo

El cifrado de datos en reposo es importante para proteger los datos confidenciales en caso de robo, devolución o reasignación de un disco. Los datos de Cloud Volumes Service se protegen en reposo mediante el cifrado basado en software.

- Las claves generadas por Google se utilizan para CVS-SW.
- Para CVS-Performance, las claves por volumen se almacenan en un gestor de claves incorporado en Cloud Volumes Service, que usa CryptoMod de ONTAP de NetApp para generar claves de cifrado AES-256. CryptoMod aparece en la lista CMVP de módulos validados FIPS 140-2-2. Consulte "FIPS 140-2 certificado n.o 4144".

A partir de noviembre de 2021, se empezó a disponer de la funcionalidad de cifrado gestionado por el cliente (CMEK) para CVS-Performance. Esta funcionalidad le permite cifrar las claves por volumen con claves maestras por proyecto y región alojadas en Google Key Management Service (KMS). KMS le permite asociar gestores de claves externos.

Para obtener detalles sobre cómo configurar KMS para CVS-Performance, "Consulte la documentación de Cloud Volumes Service".

Para obtener más información acerca de la arquitectura, consulte la sección "“Arquitectura de Cloud Volumes Service”."

Protección de datos en tránsito

Además de proteger los datos en reposo, también debe ser capaz de proteger los datos cuando están en tránsito entre la instancia de Cloud Volumes Service y un destino de cliente o replicación. Cloud Volumes Service proporciona cifrado para los datos en tránsito en protocolos NAS mediante métodos de cifrado como el cifrado SMB mediante Kerberos, la firma/sellado de paquetes y NFS Kerberos 5p para el cifrado integral de transferencias de datos.

La replicación de volúmenes de Cloud Volumes Service utiliza TLS 1.2, que aprovecha los métodos de cifrado AES-GCM.

Los protocolos en vuelo más inseguros, como telnet, NDMP, etc., están desactivados de forma predeterminada. Sin embargo, DNS no está encriptado por Cloud Volumes Service (no admite segundos DNS) y debe ser encriptada usando cifrado de red externa cuando sea posible. Consulte la sección "“Cifrado de datos en tránsito”" para obtener más información sobre cómo proteger los datos en movimiento.

Para obtener información acerca del cifrado del protocolo NAS, consulte la sección "“Protocolos NAS”."

Usuarios y grupos para permisos NAS

Parte de la protección de datos en el cloud implica una autenticación de usuarios y grupos adecuada, en la que se comprueban los usuarios que acceden a los datos como usuarios reales del entorno y los grupos contienen usuarios válidos. Estos usuarios y grupos proporcionan acceso inicial al recurso compartido y a la exportación, así como validación de permisos para archivos y carpetas en el sistema de almacenamiento.

Cloud Volumes Service utiliza la autenticación estándar de grupos y usuarios de Windows basada en Active Directory para recursos compartidos de SMB y permisos de estilo Windows. El servicio también puede aprovechar proveedores de identidad UNIX, como LDAP para usuarios y grupos de UNIX para exportaciones NFS, validación de ID de NFSv4, autenticación Kerberos y ACL de NFSv4.

> Actualmente sólo el LDAP de Active Directory es compatible con Cloud Volumes Service para la funcionalidad LDAP.

Detección, prevención y mitigación de ransomware, malware y virus

El ransomware, el malware y los virus representan una amenaza persistente para los administradores, y la detección, prevención y mitigación de esas amenazas son siempre una prioridad para las organizaciones empresariales. Un solo evento de ransomware en un conjunto de datos crucial puede costar potencialmente millones de dólares, por lo que es beneficioso hacer lo que puede minimizar el riesgo.

Aunque Cloud Volumes Service no incluye actualmente medidas de detección o prevención nativas, como la protección antivirus o "detección automática de ransomware", Hay formas de recuperarse rápidamente de un evento de ransomware mediante la habilitación de horarios habituales de copias Snapshot. Las copias Snapshot no modificables y de solo lectura hacen referencia a los bloques modificados del sistema de ficheros, son casi instantáneas, tienen un impacto mínimo en el rendimiento y solo utilizan espacio cuando se modifican o eliminan datos. Puede configurar programaciones para copias Snapshot de acuerdo con el objetivo de punto de recuperación (RPO)/objetivo de tiempo de recuperación (RTO) que desee y puede conservar hasta 1,024 copias Snapshot por volumen.

El soporte de copias Snapshot se incluye sin coste adicional (además de los cargos en el almacenamiento de datos correspondientes a los bloques/datos modificados que conservan las copias Snapshot) con Cloud Volumes Service y, en el caso de un ataque de ransomware, se puede usar para revertir a una copia Snapshot antes de que se produjera el ataque. Las restauraciones Snapshot se realizan en cuestión de segundos y, a continuación, puede volver a servir datos de forma normal. Para obtener más información, consulte "La solución de NetApp para ransomware".

Para evitar que el ransomware afecte a su negocio es necesario un enfoque multicapa que incluya una o varias de las siguientes opciones:

- Protección de terminales
- Protección contra amenazas externas a través de firewalls de red
- Detección de anomalías de datos
- Múltiples backups (in situ y fuera de ellas) de conjuntos de datos cruciales
- Pruebas de restauración de backups periódicas
- Copias Snapshot de NetApp de solo lectura inalterables
- Autenticación multifactor para la infraestructura crucial
- Auditorías de seguridad de inicios de sesión del sistema

Esta lista dista mucho de ser exhaustiva, pero es un buen proyecto a seguir cuando se trata del potencial de

ataques de ransomware. Cloud Volumes Service en Google Cloud proporciona varias formas de protegerse contra eventos de ransomware y reducir sus efectos.

Copias Snapshot modificables

De forma nativa, Cloud Volumes Service proporciona copias Snapshot inmutables de solo lectura que se utilizan en una programación personalizable para una recuperación rápida de un momento específico en caso de eliminación de datos o si un volumen completo ha sido victimizado por un ataque de ransomware. Las restauraciones de Snapshot a copias Snapshot en buenas condiciones anteriores son rápidas y minimizan la pérdida de datos en función del período de retención de sus programaciones de Snapshot, y de objetivos de tiempo y de punto de recuperación. El efecto que tiene la tecnología Snapshot en el rendimiento es mínimo.

Como las copias snapshot de Cloud Volumes Service son de solo lectura, no pueden infectarse con el ransomware a menos que el ransomware haya proliferado en el conjunto de datos inadvertido y las copias snapshot se han tomado de los datos infectados por el ransomware. Por este motivo, también debe considerar la detección de ransomware basada en anomalías de los datos. Cloud Volumes Service no ofrece actualmente una detección de forma nativa, pero puede utilizar un software de supervisión externo.

Backups y restauraciones

Cloud Volumes Service proporciona funcionalidades de backup de clientes NAS estándar (como backups a través de NFS o SMB).

- CVS-Performance ofrece replicación de volúmenes entre regiones a otros volúmenes CVS-Performance. Para obtener más información, consulte "replicación de volúmenes" En la documentación de Cloud Volumes Service.
- CVS-SW ofrece funcionalidades de backup y restauración de volúmenes nativas del servicio. Para obtener más información, consulte "backup en el cloud" En la documentación de Cloud Volumes Service.

La replicación de volúmenes proporciona una copia exacta del volumen de origen para una conmutación por error rápida en caso de un desastre, incluidos los eventos de ransomware.

Replicación entre regiones

CVS-Performance le permite replicar de forma segura volúmenes en las regiones de Google Cloud para la protección de datos y casos de uso de archivado mediante el cifrado TLS1.2 AES 256 GCM en una red de servicios de back-end controlada por NetApp mediante interfaces específicas que se utilizan para la replicación que se ejecuta en la red de Google. Un volumen primario (origen) contiene los datos de producción activos y se replica en un volumen secundario (destino) para proporcionar una réplica exacta del conjunto de datos primario.

La replicación inicial transfiere todos los bloques, pero las actualizaciones solo transmiten los bloques cambiados de un volumen primario. Por ejemplo, si una base de datos de 1 TB que reside en un volumen primario se replica en el volumen secundario, se transfiere 1 TB de espacio en la replicación inicial. Si esa base de datos tiene unos pocos cientos de filas (hipotéticamente, unos pocos MB) que cambian entre la inicialización y la siguiente actualización, sólo los bloques con las filas modificadas se replican al secundario (unos pocos MB). Esto ayuda a garantizar que los tiempos de transferencia siguen siendo bajos y que los costes de replicación siguen bajos.

Todos los permisos de los archivos y carpetas se replican en el volumen secundario, pero los permisos de acceso al recurso compartido (como políticas y reglas de exportación o recursos compartidos de SMB y ACL compartidos) se deben gestionar por separado. En el caso de una conmutación por error del sitio, el sitio de destino debe aprovechar los mismos servicios de nombre y las conexiones de dominio de Active Directory para proporcionar un manejo coherente de identidades y permisos de usuarios y grupos. Puede usar un volumen secundario como destino de conmutación por error en caso de un desastre si se rompe la relación de

replicación, que convierte el volumen secundario en lectura/escritura.

Las réplicas de volúmenes son de solo lectura, lo que proporciona una copia inalterable de datos fuera de las instalaciones para una recuperación rápida de los datos en instancias donde un virus ha infectado los datos o ransomware ha cifrado el conjunto de datos principal. Los datos de solo lectura no se cifrarán, pero, si el volumen primario se ve afectado y se produce la replicación, los bloques infectados también se replican. Puede utilizar copias Snapshot antiguas no afectadas para la recuperación, pero es posible que los acuerdos de nivel de servicio no estén dentro del rango de objetivo de tiempo de recuperación/objetivo de punto de recuperación prometido en función de la rapidez con la que se detecte un ataque.

Además, puede evitar acciones administrativas maliciosas, como eliminaciones de volúmenes, eliminaciones de copias Snapshot o cambios de programación de Snapshot, con gestión de replicación entre regiones (CRR) en Google Cloud. Para ello, se crean funciones personalizadas que separan a los administradores de volúmenes, que pueden eliminar volúmenes de origen, pero no interrumpir las operaciones y, por lo tanto, no se pueden eliminar los volúmenes de destino, de los administradores de CRR, que no pueden realizar ninguna operación de volumen. Consulte "Consideraciones de seguridad" En la documentación de Cloud Volumes Service para los permisos que permite cada grupo de administradores.

Backup de Cloud Volumes Service

Aunque Cloud Volumes Service proporciona una gran durabilidad de los datos, los eventos externos pueden causar la pérdida de datos. En caso de producirse un evento de seguridad, como un virus o ransomware, los backups y las restauraciones se convierten en algo crucial para reanudar el acceso a los datos de forma puntual. Un administrador puede eliminar accidentalmente un volumen de Cloud Volumes Service. O los usuarios simplemente quieren conservar las versiones de backup de sus datos durante muchos meses y mantener el espacio adicional de copia Snapshot dentro del volumen supone un reto de costes. A pesar de que las copias Snapshot deberían ser la forma preferida de conservar las versiones de backup durante las últimas semanas para restaurar los datos perdidos de ellas, se encuentran dentro del volumen y se pierden si este desaparece.

Por todas estas razones, NetApp Cloud Volumes Service ofrece servicios de backup a través de "Backup de Cloud Volumes Service".

El backup de Cloud Volumes Service genera una copia del volumen en Google Cloud Storage (GCS). Solo realiza un backup de los datos reales almacenados en el volumen, no del espacio libre. Funciona como siempre incremental, lo que significa que transfiere el contenido del volumen una vez y desde allí sólo se realiza el backup de los datos modificados. En comparación con los conceptos clásicos de backup con varios backups completos, ahorrará una gran cantidad de almacenamiento de backup al reducir costes. Puesto que el precio mensual del espacio de backup es más bajo en comparación con un volumen, es el lugar ideal para mantener las versiones de backup por más tiempo.

Los usuarios pueden utilizar una copia de seguridad de Cloud Volumes Service para restaurar cualquier versión de copia de seguridad en el mismo volumen o en otro dentro de la misma región. Si el volumen de origen se elimina, se conservan los datos de backup y se debe gestionar (por ejemplo, se eliminan) de forma independiente.

Cloud Volumes Service backup está integrado en Cloud Volumes Service as Option. Los usuarios pueden decidir qué volúmenes proteger activando el backup de Cloud Volumes Service por volumen. Consulte "Documentación de backup de Cloud Volumes Service" para obtener información sobre los backups, el "número máximo de versiones de backup admitidas", programación, y. "precios".

Todos los datos de backup de un proyecto se almacenan en un bloque de GCS que gestiona el servicio y que el usuario no puede ver. Cada proyecto utiliza un bloque diferente. Actualmente, los bloques se encuentran en la misma región que los volúmenes Cloud Volumes Service, pero se están debatiendo más opciones. Consulte la documentación para obtener la información más reciente.

El transporte de datos desde un bloque de Cloud Volumes Service a GCS utiliza redes de Google internas en servicio con HTTPS y TLS1.2. Los datos se cifran en reposo con claves gestionadas por Google.

Para gestionar el backup de Cloud Volumes Service (crear, eliminar y restaurar backups), un usuario debe tener el "roles/netappcloudvolumes.admin" función.

Arquitectura

Descripción general

Parte de confiar en una solución cloud es comprender la arquitectura y el modo en el que se protege. En esta sección se presentan distintos aspectos de la arquitectura de Cloud Volumes Service en Google para ayudar a solucionar los posibles problemas relacionados con la seguridad de los datos, así como llamadas a áreas en las que se puedan necesitar pasos de configuración adicionales para obtener la puesta en marcha más segura.

La arquitectura general de Cloud Volumes Service se puede dividir en dos componentes principales: El plano de control y el plano de datos.

Plano de control

El plano de control en Cloud Volumes Service es la infraestructura de back-end gestionada por los administradores de Cloud Volumes Service y el software de automatización nativo de NetApp. Este plano es completamente transparente para los usuarios finales e incluye redes, hardware de almacenamiento, actualizaciones de software, etc. para ayudar a ofrecer valor a una solución residente en cloud como Cloud Volumes Service.

Plano de datos

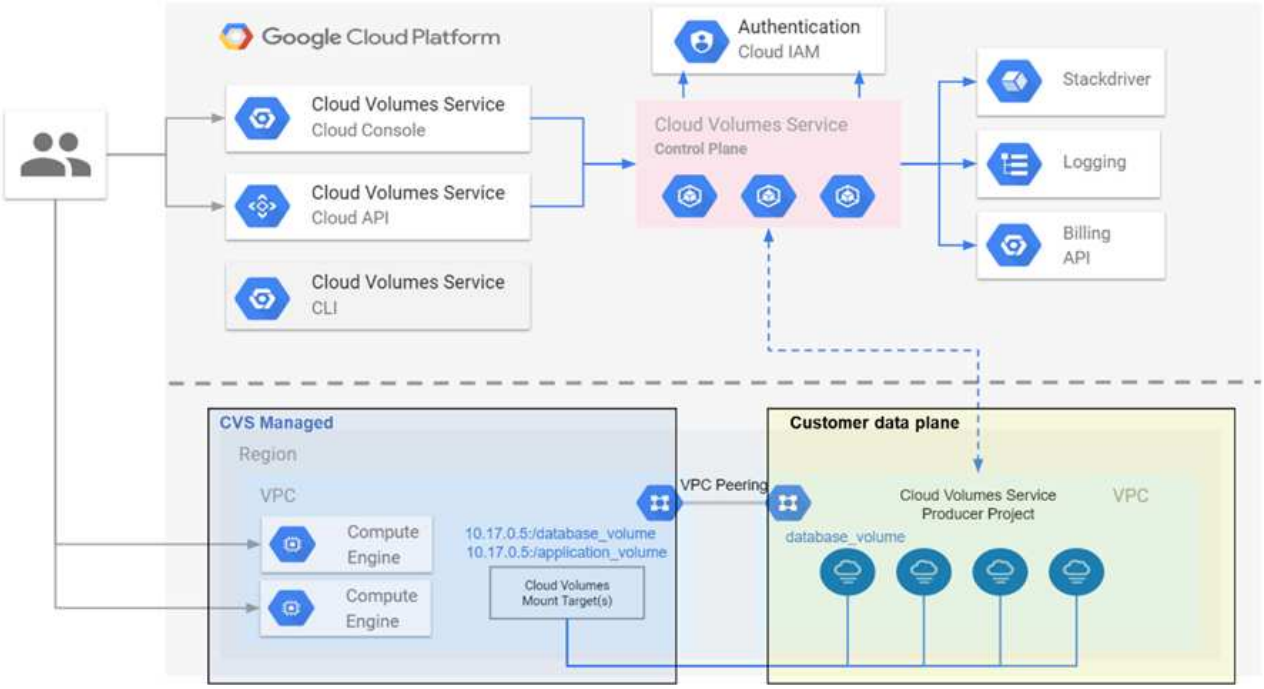
El plano de datos en Cloud Volumes Service incluye los volúmenes de datos reales y la configuración de Cloud Volumes Service general (como el control de acceso, la autenticación de Kerberos, etc.). El plano de datos está totalmente bajo el control de los usuarios finales y de los consumidores de la plataforma Cloud Volumes Service.

Existen diferencias distintas en cómo se asegura y gestiona cada plano. En las siguientes secciones se tratan estas diferencias, empezando por la descripción general de la arquitectura de Cloud Volumes Service.

Arquitectura Cloud Volumes Service

De forma similar a otros servicios nativos de Google Cloud como CloudSQL, Google Cloud VMware Engine (GCVE) y filestore, utiliza Cloud Volumes Service "Google PSA" para prestar el servicio. En PSA, los servicios se construyen dentro de un proyecto de productor de servicios, que utiliza "Agrupación de redes VPC" para conectarse con el consumidor de servicios. El productor de servicios lo proporciona y controla NetApp, y el consumidor de servicios es un VPC en un proyecto de cliente, que aloja a los clientes que desean acceder a recursos compartidos de archivos de Cloud Volumes Service.

La siguiente figura, a la que se hace referencia desde "sección de arquitectura" De la documentación de Cloud Volumes Service, muestra una vista de alto nivel.



La pieza situada encima de la línea de puntos muestra el plano de control del servicio, que controla el ciclo de vida del volumen. La pieza debajo de la línea de puntos muestra el plano de datos. El cuadro azul izquierdo muestra el VPC (consumidor de servicios) del usuario, el cuadro azul derecho es el productor de servicios que proporciona NetApp. Ambos se conectan mediante la agrupación de VPC.

Modelo de tenancy

En Cloud Volumes Service, los proyectos individuales se consideran inquilinos únicos. Esto significa que la manipulación de volúmenes, copias Snapshot, etc. se realiza por proyecto. En otras palabras, todos los volúmenes son propiedad del proyecto en el que se crearon y solo ese proyecto puede gestionar y acceder a los datos de su interior de forma predeterminada. Se considera la vista del plano de control del servicio.

VPC compartidos

En la vista del plano de datos, Cloud Volumes Service puede conectarse a un VPC compartido. Se pueden crear volúmenes en el proyecto de host o en uno de los proyectos de servicio conectados al VPC compartido. Todos los proyectos (host o servicio) conectados al VPC compartido pueden llegar a los volúmenes de la capa de red (TCP/IP). Debido a que todos los clientes con conectividad de red en el VPC compartido pueden acceder potencialmente a los datos mediante los protocolos NAS, se debe utilizar el control de acceso en el volumen individual (como las listas de control de acceso de usuarios/grupos (ACL) y los nombres de host/direcciones IP para las exportaciones de NFS para controlar quién puede acceder a los datos.

Puede conectar Cloud Volumes Service hasta a cinco VPC por proyecto de cliente. En el plano de control, el proyecto le permite gestionar todos los volúmenes creados, independientemente del VPC al que estén conectados. En el plano de datos, las PC están aisladas entre sí y cada volumen solo se puede conectar a un VPC.

El acceso a los volúmenes individuales está controlado por mecanismos de control de acceso específicos de los protocolos (NFS/SMB).

En otras palabras, en la capa de red, todos los proyectos conectados al VPC compartido pueden ver el volumen, mientras que, por el lado de la gestión, el plano de control solo permite que el proyecto del

propietario vea el volumen.

Controles de servicio VPC

Los controles de servicio VPC establecen un perímetro de control de acceso alrededor de los servicios de Google Cloud que están conectados a Internet y son accesibles en todo el mundo. Estos servicios proporcionan control de acceso a través de identidades de usuario, pero no pueden restringir desde qué solicitudes de ubicación de red se originan. Los controles de servicio VPC cierran esa brecha introduciendo las funcionalidades para restringir el acceso a las redes definidas.

El plano de datos Cloud Volumes Service no está conectado a Internet externo sino a ordenadores virtuales privados con límites de red bien definidos (perímetros). Dentro de esa red, cada volumen utiliza un control de acceso específico del protocolo. Los administradores de proyectos de Google Cloud crean explícitamente cualquier conectividad de red externa. Sin embargo, el plano de control no proporciona las mismas protecciones que el plano de datos y puede ser accesible por cualquier persona desde cualquier lugar con credenciales válidas ("Fichas JWT").

En resumen, el plano de datos Cloud Volumes Service proporciona la funcionalidad de control de acceso a la red, sin el requisito de admitir controles de servicio VPC y no utiliza de forma explícita los controles de servicio VPC.

Consideraciones sobre rastreo y rastreo de paquetes

Las capturas de paquetes pueden ser útiles para solucionar problemas de red u otros problemas (como permisos NAS, conectividad LDAP, etc.), pero también se pueden usar de forma malintencionada para obtener información sobre direcciones IP de red, direcciones MAC, nombres de usuarios y grupos, y sobre qué nivel de seguridad se está utilizando en los extremos. Debido a la forma en que se configuran las reglas de red, VPC y firewall de Google Cloud, el acceso no deseado a los paquetes de red debería ser difícil de obtener sin credenciales de inicio de sesión del usuario o "Fichas JWT" a las instancias de cloud. Las capturas de paquetes solo son posibles en extremos (como máquinas virtuales (VM)) y solo en extremos internos en el VPC, a menos que se utilice un VPC compartido o un reenvío de túnel/IP de red externo para permitir de forma explícita el tráfico externo a los extremos. No hay forma de sniff el tráfico fuera de los clientes.

Cuando se utilizan VPC compartidos, cifrado en tránsito con NFS Kerberos y/o. "Cifrado SMB" puede enmascarar gran parte de la información obtenida de las trazas. Sin embargo, cierto tráfico se sigue enviando en texto sin texto, como "DNS" y.. "Consultas LDAP". En la siguiente figura se muestra una captura de paquetes de una consulta LDAP de texto sin formato originada en Cloud Volumes Service y la información de identificación potencial que se expone. Las consultas LDAP en Cloud Volumes Service actualmente no admiten cifrado ni LDAP sobre SSL. CVS-Performance admite la firma LDAP, si es solicitada por Active Directory. CVS-SW no admite la firma LDAP.

IP addresses of the LDAP server and CVS instance

LDAP base DN and search type, search result

No.	Time	Source	Destination	Protocol	Length	Info
2320…	366.244071	10.194.0.6	10.10.0.11	LDAP	225	searchRequest(2) "DC=cvsdemo,DC=local" wholeSubtree
2320…	366.244381	10.10.0.11	10.194.0.6	LDAP	330	searchResRef(2) | searchResRef(2) | searchResRef(2) | searchResDone(2) success [0 results]

```
searchRequest
    baseObject: DC=cvsdemo,DC=local
    scope: wholeSubtree (2)
    derefAliases: neverDerefAliases (0)
    sizeLimit: 0
    timeLimit: 3
    typesOnly: False
    Filter: (&(objectClass=User)(uidNumber=1025))
      filter: and (0)
        and: (&(objectClass=User)(uidNumber=1025))
          and: 2 items
            Filter: (objectClass=User)
              and item: equalityMatch (3)
                equalityMatch
                    attributeDesc: objectClass
                    assertionValue: User
            Filter: (uidNumber=1025)
              and item: equalityMatch (3)
                equalityMatch
                    attributeDesc: uidNumber
                    assertionValue: 1025
    attributes: 7 items
        AttributeDescription: uid
        AttributeDescription: uidNumber
        AttributeDescription: gidNumber
        AttributeDescription: unixUserPassword
        AttributeDescription: name
        AttributeDescription: unixHomeDirectory
        AttributeDescription: loginShell
```

Filters used in the query
- Usernames
- Numeric IDs
- Group names
- Group IDs

Attributes queried

UnixUserPassword es consultada por LDAP y no se envía en texto sin formato sino en un hash salado. De forma predeterminada, LDAP de Windows no rellena los campos unixUserPassword. Este campo sólo es necesario si necesita aprovechar LDAP de Windows para inicios de sesión interactivos a través de LDAP a clientes. Cloud Volumes Service no admite inicios de sesión LDAP interactivos en las instancias.

En la siguiente figura se muestra una captura de paquetes desde una conversación Kerberos de NFS junto a una captura de NFS sobre AUTH_SYS. Tenga en cuenta que la información disponible en una traza difiere entre ambas y cómo habilitar el cifrado en tránsito ofrece una mayor seguridad general para el tráfico NAS.

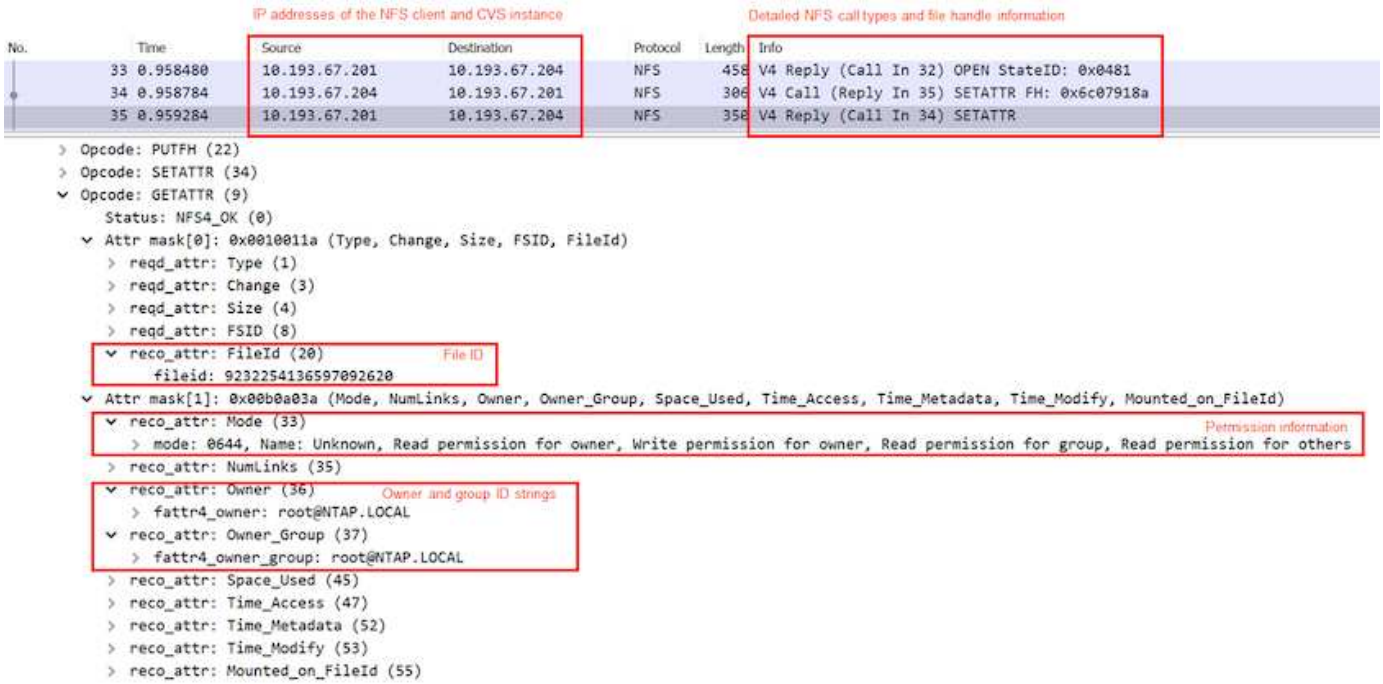
IP addresses of the NFS client and CVS instance

Genericized NFS call/reply

No.	Time	Source	Destination	Protocol	Length	Info
380	9.218014	10.193.67.225	10.193.67.219	NFS	346	V4 Call (Reply In 381)
381	9.218480	10.193.67.219	10.193.67.225	NFS	426	V4 Reply (Call In 380)
382	9.218641	10.193.67.225	10.193.67.219	NFS	370	V4 Call (Reply In 397)
397	9.369035	10.193.67.219	10.193.67.225	NFS	458	V4 Reply (Call In 382)

```
> Frame 381: 426 bytes on wire (3408 bits), 426 bytes captured (3408 bits)
> Ethernet II, Src: IntelCor_7f:da:bc (90:e2:ba:7f:da:bc), Dst: VMware_a0:2c:2d (00:50:56:a0:2c:2d)
> Internet Protocol Version 4, Src: 10.193.67.219, Dst: 10.193.67.225
> Transmission Control Protocol, Src Port: 2049, Dst Port: 738, Seq: 6305, Ack: 6569, Len: 360
> Remote Procedure Call, Type:Reply XID:0xef5e998d
v GSS-Wrap
    Length: 300
    GSS Data: 050407ff0000000000000000025913451ee1d43d298cf3031…
  > krb5_blob: 050407ff0000000000000000025913451ee1d43d298cf3031…
v Network File System
    [Program Version: 4]
    [V4 Procedure: COMPOUND (1)]
```

GSS wrapped NFS calls/replies with no other identifying information



Interfaces de red de equipos virtuales

Un truco que los atacantes podrían intentar es agregar una nueva tarjeta de interfaz de red (NIC) a una VM en "modo promiscuo" (Duplicación de puertos) o habilite el modo promiscuo en una NIC existente para sniff todo el tráfico. En Google Cloud, agregar una nueva NIC requiere que una máquina virtual se cierre por completo, lo que crea alertas, por lo que los atacantes no pueden pasar por alto.

Además, las NIC no se pueden establecer en modo promiscuo y activarán alertas en Google Cloud.

Arquitectura del plano de control

Todas las acciones de gestión a Cloud Volumes Service se realizan mediante API. La gestión de Cloud Volumes Service integrada en la consola cloud de GCP también utiliza la API de Cloud Volumes Service.

Gestión de acceso e identidad

Gestión de acceso e identidad ("IAM") Es un servicio estándar que le permite controlar la autenticación (inicios de sesión) y la autorización (permisos) a las instancias de proyecto de Google Cloud. Google IAM proporciona un registro de auditoría completo de la autorización y eliminación de permisos. Actualmente, Cloud Volumes Service no proporciona auditoría del plano de control.

Información general sobre autorización/permisos

IAM ofrece permisos granulares integrados para Cloud Volumes Service. Puede encontrar un "complete aquí la lista de permisos granulares".

IAM también ofrece dos roles predefinidos llamados `netappcloudvolumes.admin` y.. `netappcloudvolumes.viewer`. Estos roles pueden asignarse a usuarios o cuentas de servicio específicos.

Asigne roles y permisos adecuados para permitir que los usuarios de IAM gestionen Cloud Volumes Service.

Algunos ejemplos para el uso de permisos granulares son los siguientes:

- Cree una función personalizada con sólo permisos get/list/create/update para que los usuarios no puedan eliminar volúmenes.
- Use un rol personalizado con solo `snapshot.*` Permisos para crear una cuenta de servicio que se utilice para crear una integración de Snapshot coherente con las aplicaciones.
- Cree un rol personalizado para delegar `volumereplication.*` para usuarios específicos.

Cuentas de servicio

Para realizar llamadas a la API de Cloud Volumes Service a través de scripts o. "Terraform", debe crear una cuenta de servicio con `roles/netappcloudvolumes.admin` función. Puede utilizar esta cuenta de servicio para generar los tokens JWT necesarios para autenticar las solicitudes de API de Cloud Volumes Service de dos maneras diferentes:

- Genere una clave JSON y utilice las API de Google para obtener un token de JWT de él. Este es el método más sencillo, pero implica la gestión de secretos manuales (la clave JSON).
- Uso "Suplantación de cuentas de servicio" con `roles/iam.serviceAccountTokenCreator`. El código (script, Terraform, etc.) se ejecuta con "Credenciales predeterminadas de la aplicación" e representa a la cuenta de servicio para obtener sus permisos. Este enfoque refleja las mejores prácticas de seguridad de Google.

Consulte "Creación de la cuenta de servicio y la clave privada" Para obtener más información, consulte la documentación de cloud de Google.

API de Cloud Volumes Service

La API de Cloud Volumes Service utiliza una API basada en REST usando HTTPS (TLSv1.2) como transporte de red subyacente. Puede encontrar la definición de API más reciente "aquí" E información acerca de cómo utilizar la API en "API de Cloud Volumes en la documentación de Google Cloud".

NetApp utiliza y protege el extremo de la API mediante la funcionalidad estándar HTTPS (TLSv1.2).

Fichas JWT

La autenticación a la API se realiza con tokens JWT portadores ("RFC-7519"). Se deben obtener tokens JWT válidos mediante la autenticación de Google Cloud IAM. Para ello, debe obtener un token del IAM mediante la obtención de una clave JSON de la cuenta de servicio.

Registro de auditoría

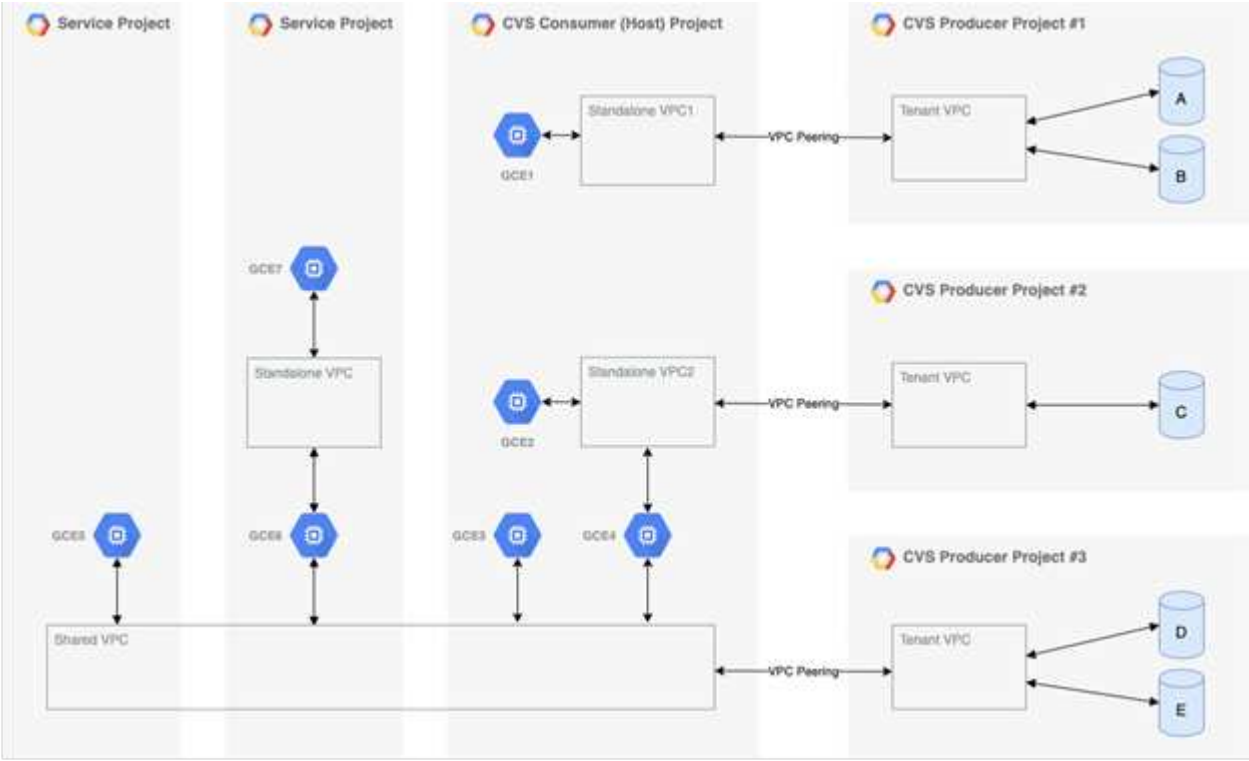
Actualmente, no hay registros de auditoría del plano de control a los que el usuario pueda acceder.

Arquitectura de plano de datos

Cloud Volumes Service para Google Cloud aprovecha Google Cloud "acceso a servicios privados" marco. En este marco, los usuarios pueden conectarse a Cloud Volumes Service. Este marco usa construcciones de paridad de Service Networking y VPC, al igual que otros servicios de Google Cloud, para garantizar un aislamiento completo entre clientes.

Para obtener información general sobre la arquitectura de Cloud Volumes Service para Google Cloud, consulte "Para Cloud Volumes Service".

Las VPC de usuario (independientes o compartidas) tienen una relación entre sí y las VPC dentro de los proyectos de arrendatarios administrados de Cloud Volumes Service, que alojan los volúmenes.



La figura anterior muestra un proyecto (el proyecto para consumidores CVS en el medio) con tres redes VPC conectadas a Cloud Volumes Service y a varios equipos virtuales de Compute Engine (GCE1-7) compartiendo volúmenes:

- VPC1 permite a GCE1 acceder a los volúmenes A y B.
- VPC2 permite a GCE2 y GCE4 acceder al volumen C.
- La tercera red VPC es un VPC compartido, compartido con dos proyectos de servicio. Permite a GCE3, GCE4, GCE5 y GCE6 acceder a los volúmenes D y E. Las redes VPC compartidas solo se admiten para volúmenes del tipo de servicio CVS-Performance.

GCE7 no puede acceder a ningún volumen.

Los datos se pueden cifrar tanto en tránsito (mediante Kerberos y/o cifrado SMB) como en reposo en Cloud Volumes Service.

Cifrado de datos en tránsito

Los datos en tránsito pueden cifrarse en la capa de protocolo NAS, y la propia red de Google Cloud está cifrada, tal y como se describe en las siguientes secciones.

Red de Google Cloud

Google Cloud cifra el tráfico en el nivel de la red, tal y como se describe en "Cifrado en tránsito" En la documentación de Google. Como se mencionó en la sección "Arquitectura de Cloud Volumes Services", Cloud Volumes Service se ofrece desde un proyecto de productor de PSA controlado por NetApp.

En caso de CVS-SW, el inquilino productor ejecuta las VM de Google para ofrecer el servicio. Google cifra

automáticamente el tráfico entre los equipos virtuales del usuario y los equipos virtuales de Cloud Volumes Service.

Aunque la ruta de datos para CVS-Performance no está completamente cifrada en la capa de red, NetApp y Google usan una combinación de ambos "De cifrado IEEE 802.1AE (MACSec)", "encapsulación" (Cifrado de datos) y redes con limitaciones físicas para proteger los datos en tránsito entre el tipo de servicio CVS-Performance de Cloud Volumes Service y Google Cloud.

Protocolos NAS

Los protocolos NFS y SMB NAS proporcionan un cifrado de transporte opcional en la capa del protocolo.

Cifrado SMB

"Cifrado SMB" Proporciona cifrado integral de datos SMB y protege los datos de espionaje en redes que no son de confianza. Puede habilitar el cifrado tanto para la conexión de datos de cliente/servidor (solo disponible para clientes compatibles con SMB3.x) como para la autenticación de la controladora de servidor/dominio.

Cuando el cifrado SMB está habilitado, los clientes que no admiten el cifrado no pueden acceder al recurso compartido.

Cloud Volumes Service admite cifrados de seguridad RC4-HMAC, AES-128-CTS-HMAC-SHA1 y AES-256-CTS-HMAC-SHA1 para el cifrado SMB. SMB negocia con el tipo de cifrado más alto admitido por el servidor.

NFSv4.1 Kerberos

Para NFSv4.1, CVS-Performance ofrece autenticación de Kerberos, tal como se describe en "RFC7530". Puede activar Kerberos por volumen.

El tipo de cifrado disponible más actual para Kerberos es AES-256-CTS-HMAC-SHA1. Cloud Volumes Service de NetApp es compatible con AES-256-CTS-HMAC-SHA1, AES-128-CTS-HMAC-SHA1, DES3 y DES para NFS. También admite ARCFOUR-HMAC (RC4) para el tráfico CIFS/SMB, pero no para NFS.

Kerberos proporciona tres niveles de seguridad distintos para montajes NFS que ofrecen opciones para la solidez de la seguridad de Kerberos.

Según RedHat's "Opciones de montaje comunes" documentación:

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to
authenticate users.
sec=krb5i uses Kerberos V5 for user authentication and performs integrity
checking of NFS operations using secure checksums to prevent data
tampering.
sec=krb5p uses Kerberos V5 for user authentication, integrity checking,
and encrypts NFS traffic to prevent traffic sniffing. This is the most
secure setting, but it also involves the most performance overhead.
```

Como regla general, cuanto mayor sea el nivel de seguridad de Kerberos, peor será el rendimiento, puesto que el cliente y el servidor pasan tiempo cifrando y descifrando las operaciones de NFS para cada paquete enviado. Muchos clientes y servidores NFS ofrecen soporte para la descarga de AES-ni a las CPU para una mejor experiencia general, pero el impacto en el rendimiento de Kerberos 5p (cifrado completo integral) es significativamente mayor que el impacto de Kerberos 5 (autenticación de usuario).

En la siguiente tabla se muestran las diferencias en el rendimiento y la seguridad de cada nivel.

Nivel de seguridad	Seguridad	Rendimiento
NFSv3: System	• Menos seguro; texto sin formato con ID de usuario/ID de grupo numéricos • Capaz de ver UID, GID, direcciones IP de cliente, rutas de exportación, nombres de archivos, permisos en capturas de paquetes	• Lo mejor para la mayoría de los casos
NFSv4.x: Sys	• Más seguro que NFSv3 (identificadores de cliente, coincidencia de cadena de nombre/cadena de dominio) pero texto sin formato • Se puede ver UID, GID, direcciones IP de cliente, cadenas de nombre, identificadores de dominio, rutas de exportación, nombres de archivo y permisos en capturas de paquetes	• Bueno para cargas de trabajo secuenciales (como equipos virtuales, bases de datos, archivos de gran tamaño) • Malo con un número elevado de archivos/metadatos altos (un 30-50% peor)
NFS: Krb5	• El cifrado Kerberos para credenciales en cada paquete NFS envuelve UID/GID de usuarios/grupos en llamadas RPC en el contenedor GSS • El usuario que solicita el acceso al montaje necesita un ticket Kerberos válido (ya sea mediante el nombre de usuario/contraseña o el cambio de tabulación manual); el ticket caduca después de un período de tiempo especificado y el usuario debe volver a autenticarse para el acceso • No existe cifrado para operaciones de NFS ni para protocolos auxiliares como Mount/portmapper/nlm (puede ver rutas de exportación, direcciones IP, identificadores de archivos, permisos, nombres de archivos, atime/mtime en capturas de paquetes)	• Mejor en la mayoría de los casos para Kerberos; peor que AUTH_SYS

Nivel de seguridad	Seguridad	Rendimiento
NFS: Krb5i	• El cifrado Kerberos para credenciales en cada paquete NFS envuelve UID/GID de usuarios/grupos en llamadas RPC en el contenedor GSS • El usuario que solicita el acceso al montaje necesita un ticket Kerberos válido (ya sea mediante el nombre de usuario/contraseña o el cambio de tabulación manual); el ticket caduca después de un período de tiempo especificado y el usuario debe volver a autenticarse para el acceso • No existe cifrado para operaciones de NFS ni para protocolos auxiliares como Mount/portmapper/nlm (puede ver rutas de exportación, direcciones IP, identificadores de archivos, permisos, nombres de archivos, atime/mtime en capturas de paquetes) • La suma de comprobación de Kerberos GSS se agrega a cada paquete para garantizar que nada intercepta los paquetes. Si coinciden sumas de comprobación, se permite la conversación.	• Mejor que krb5p porque la carga útil NFS no está cifrada; solo la sobrecarga añadida en comparación con krb5 es la suma de comprobación de integridad. El rendimiento del krb5i no será mucho peor que el krb5, pero sí que se verá algo de degradación.

Nivel de seguridad	Seguridad	Rendimiento
NFS: Krb5p	• El cifrado Kerberos para credenciales en cada paquete NFS envuelve UID/GID de usuarios/grupos en llamadas RPC en el contenedor GSS • El usuario que solicita acceso al montaje necesita un ticket Kerberos válido (ya sea mediante nombre de usuario/contraseña o cambio manual de keytab); el ticket caduca después del período de tiempo especificado y el usuario debe volver a autenticarse para acceder • Todas las cargas de paquetes NFS se cifran con el contenedor GSS (no se pueden ver los identificadores de archivos, permisos, nombres de archivos, atime/mtime en capturas de paquetes). • Incluye comprobación de integridad. • El tipo de operación NFS es visible (FSINFO, ACCESS, GETATTR, etc.). • Los protocolos auxiliares (Mount, portmap, nlm, etc.) no están cifrados (puede ver rutas de exportación, direcciones IP)	• El peor rendimiento de los niveles de seguridad; krb5p debe cifrar/descifrar más. • Mejor rendimiento que krb5p con NFSv4.x para cargas de trabajo con un gran número de archivos.

En Cloud Volumes Service, un servidor de Active Directory configurado se utiliza como servidor Kerberos y servidor LDAP (para buscar identidades de usuario desde un esquema compatible con RFC2307). No se admiten otros servidores Kerberos o LDAP. NetApp recomienda encarecidamente utilizar LDAP para la gestión de identidades en Cloud Volumes Service. Para obtener más información acerca de cómo se muestra NFS Kerberos en capturas de paquetes, consulte la sección ""Consideraciones sobre rastreo y rastreo de paquetes"."

Cifrado de datos en reposo

Todos los volúmenes de Cloud Volumes Service se cifran en reposo mediante el cifrado AES-256, lo que significa que todos los datos de usuario escritos en medios se cifran y solo se pueden descifrar con una clave por volumen.

- Para CVS-SW, se usan claves generadas por Google.
- Para CVS-Performance, las claves por volumen se almacenan en un gestor de claves incorporado en Cloud Volumes Service.

A partir de noviembre de 2021, ya estaba disponible la funcionalidad de obtener una vista previa de las claves de cifrado gestionadas por el cliente (CMEK). Esto permite cifrar las claves por volumen con una clave maestra por proyecto y por región alojada en "Servicio de administración de claves (KMS) de Google." KMS le permite asociar gestores de claves externos.

Para obtener información acerca de la configuración de KMS para CVS-Performance, consulte "Configurar las claves de cifrado gestionadas por el cliente".

Servidor de seguridad

Cloud Volumes Service expone varios puertos TCP para que sirvan a los recursos compartidos NFS y SMB:

- "Puertos necesarios para el acceso NFS"
- "Puertos necesarios para el acceso a SMB"

Además, SMB, NFS con LDAP incluido Kerberos y configuraciones de protocolo dual requieren acceso a un dominio de Windows Active Directory. Deben estar las conexiones de Active Directory "configurado" por región. Los controladores de dominio de Active Directory (DC) se identifican mediante el uso "Descubrimiento de DC basado en DNS" Utilizando los servidores DNS especificados. Se utiliza cualquiera de los DC devueltos. La lista de centros de datos elegibles se puede limitar especificando un sitio de Active Directory.

Cloud Volumes Service se dirige a través de direcciones IP del rango CIDR asignado con el `gcloud compute address` command mientras "Integración de Cloud Volumes Service". Puede utilizar este CIDR como direcciones de origen para configurar firewalls entrantes en los controladores de dominio de Active Directory.

Los controladores de dominio de Active Directory deben "Exponer los puertos a los CIDR de Cloud Volumes Service como se menciona aquí".

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:

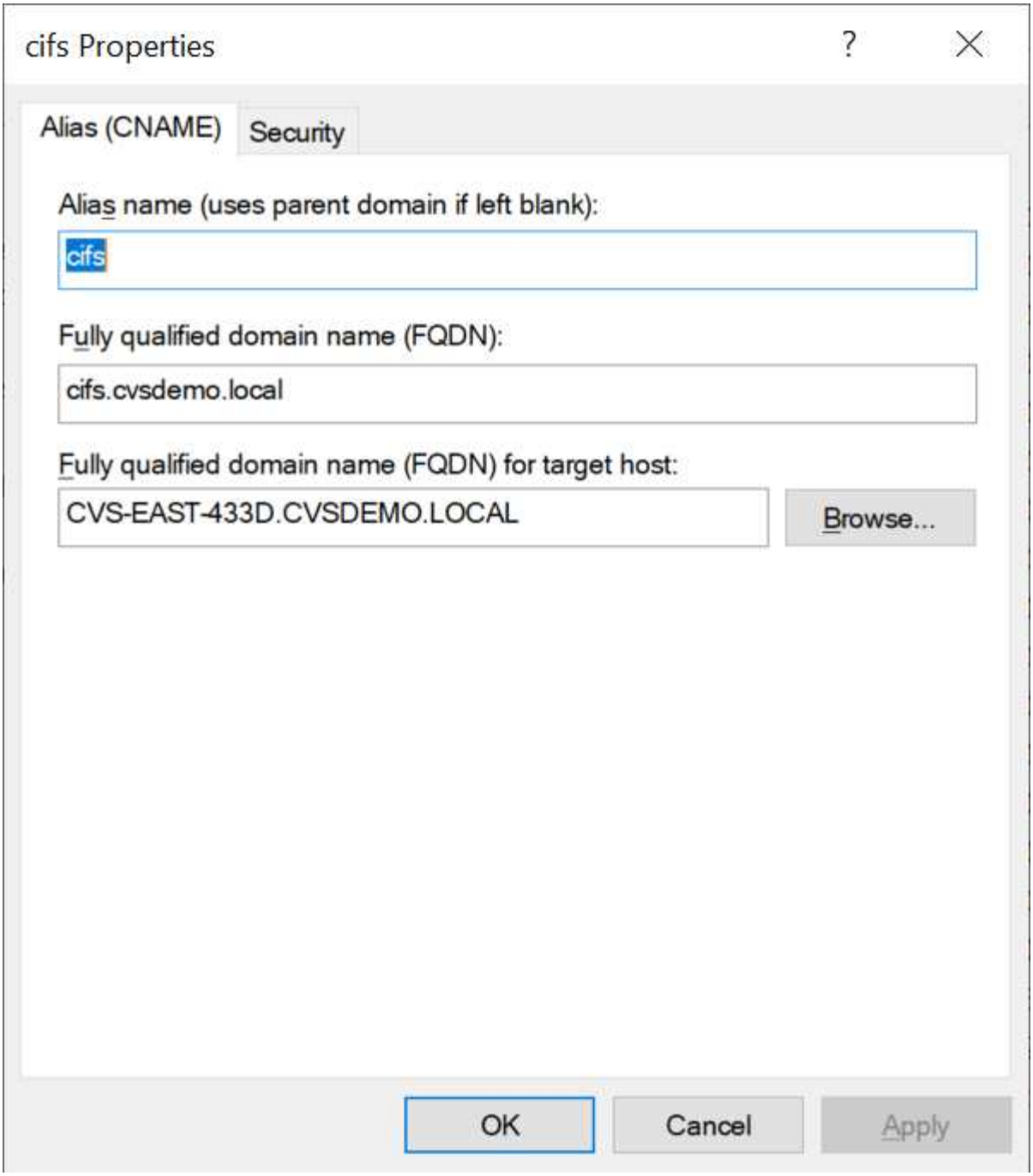
```
PS C:\> nslookup CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    CVS-EAST-433D.CVSDEMO.LOCAL
Address: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

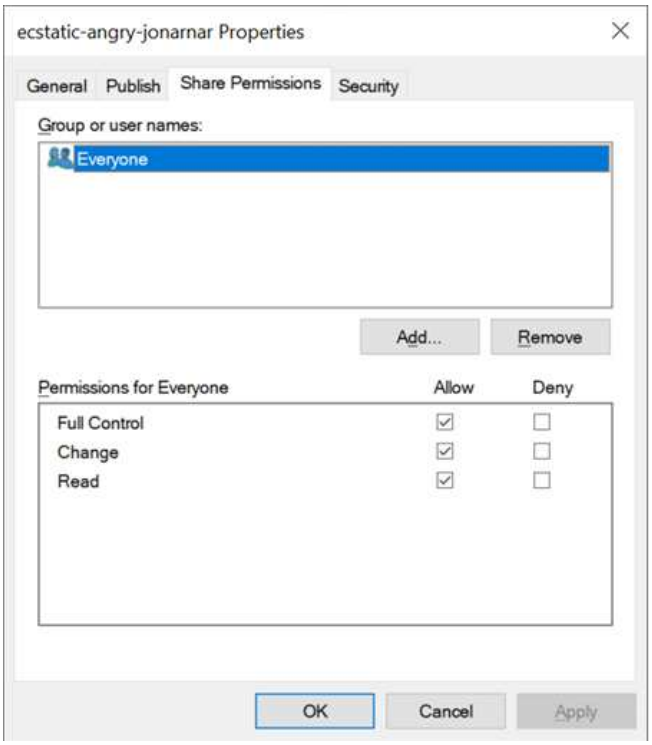
Comparta los permisos

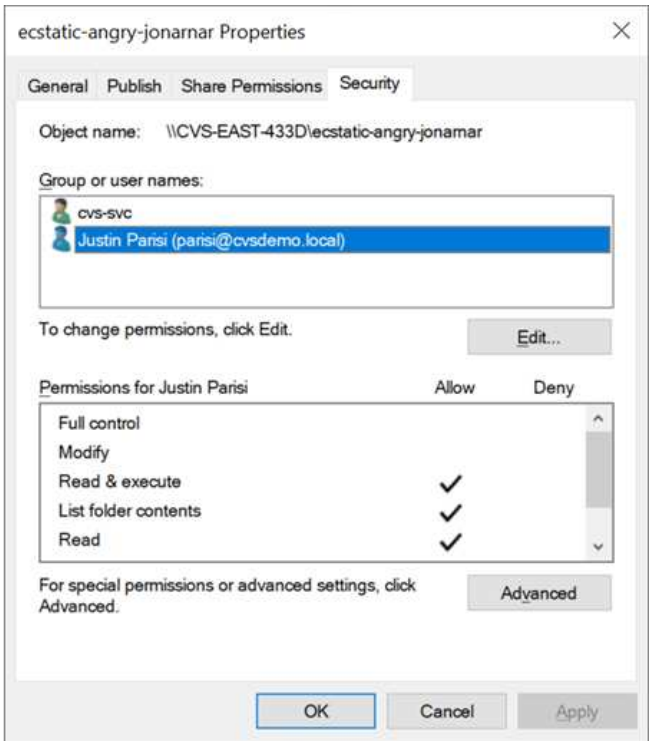
Los permisos de recursos compartidos son más generales que los permisos NTFS (sólo lectura/cambio/control total) y controlan la entrada inicial en un recurso compartido SMB, de forma similar a cómo funcionan las reglas de política de exportación NFS.

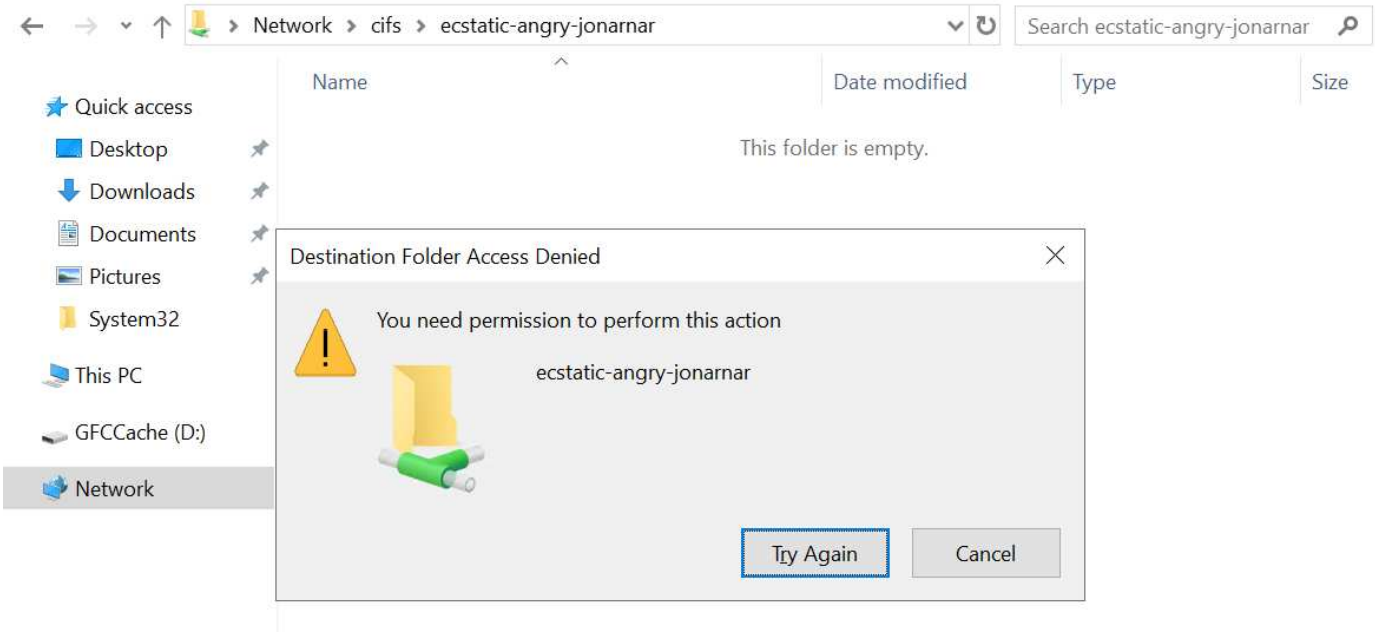
Si bien las reglas de política de exportación de NFS controlan el acceso mediante información basada en hosts, como direcciones IP o nombres de hosts, los permisos de uso compartido de SMB pueden controlar el acceso mediante ACE de usuario y de grupo en una ACL compartida. Puede configurar las ACL para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

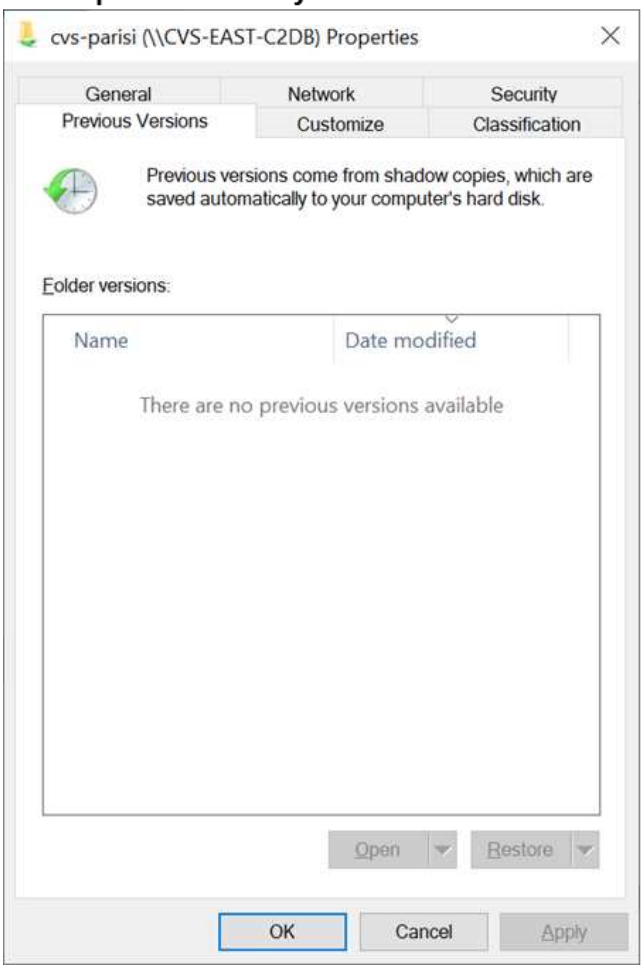
Funciones de seguridad para recursos compartidos de SMB

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.

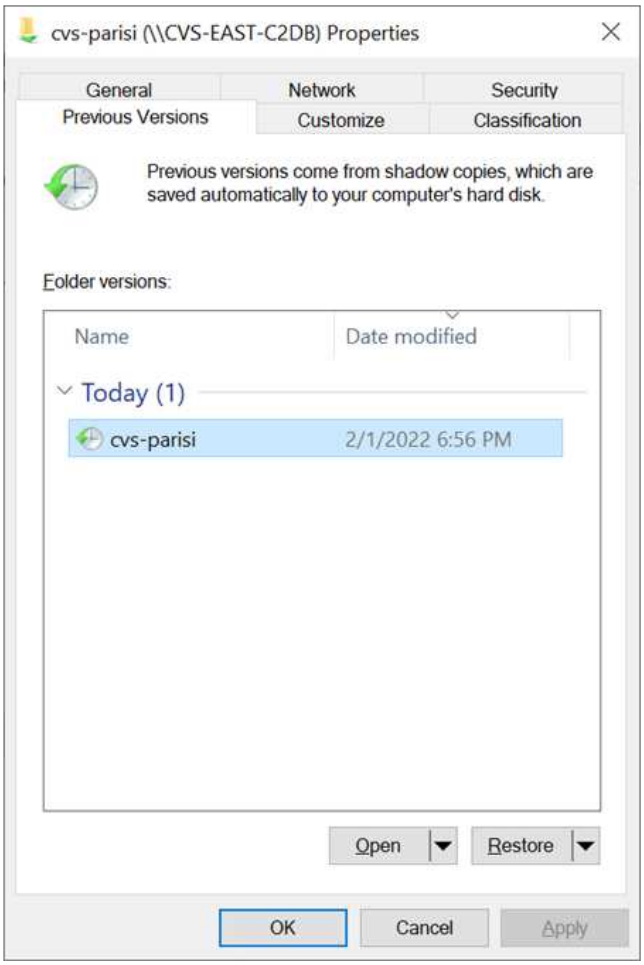
Algunas de estas opciones dependen del nivel de Cloud Volumes Service (rendimiento o software) y las opciones disponibles son:

- **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

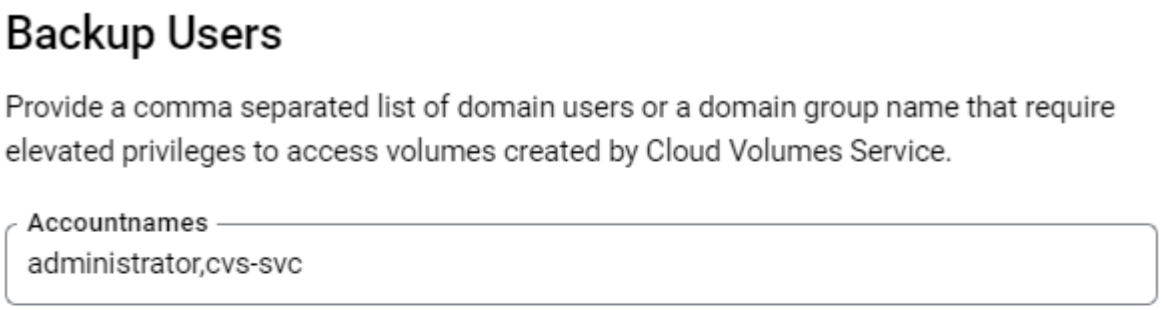
archivos Cloud Volumes Service. Como resultado, intenta navegar a. `\\SERVER\C$` error.

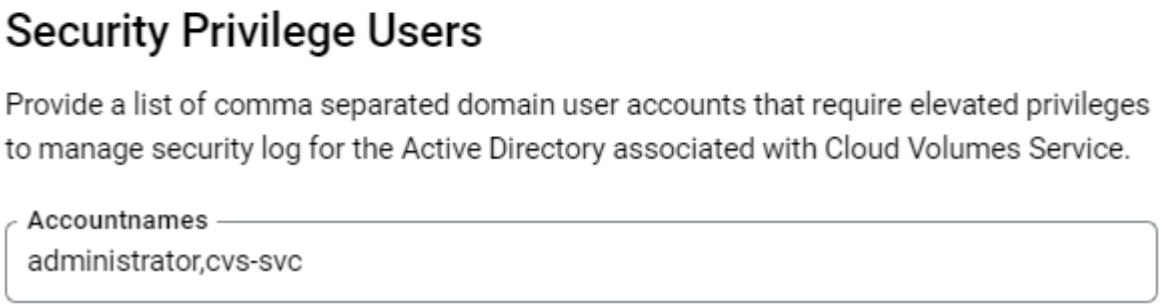
Cuentas con derechos de administrador/copia de seguridad local/BUILTIN

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.

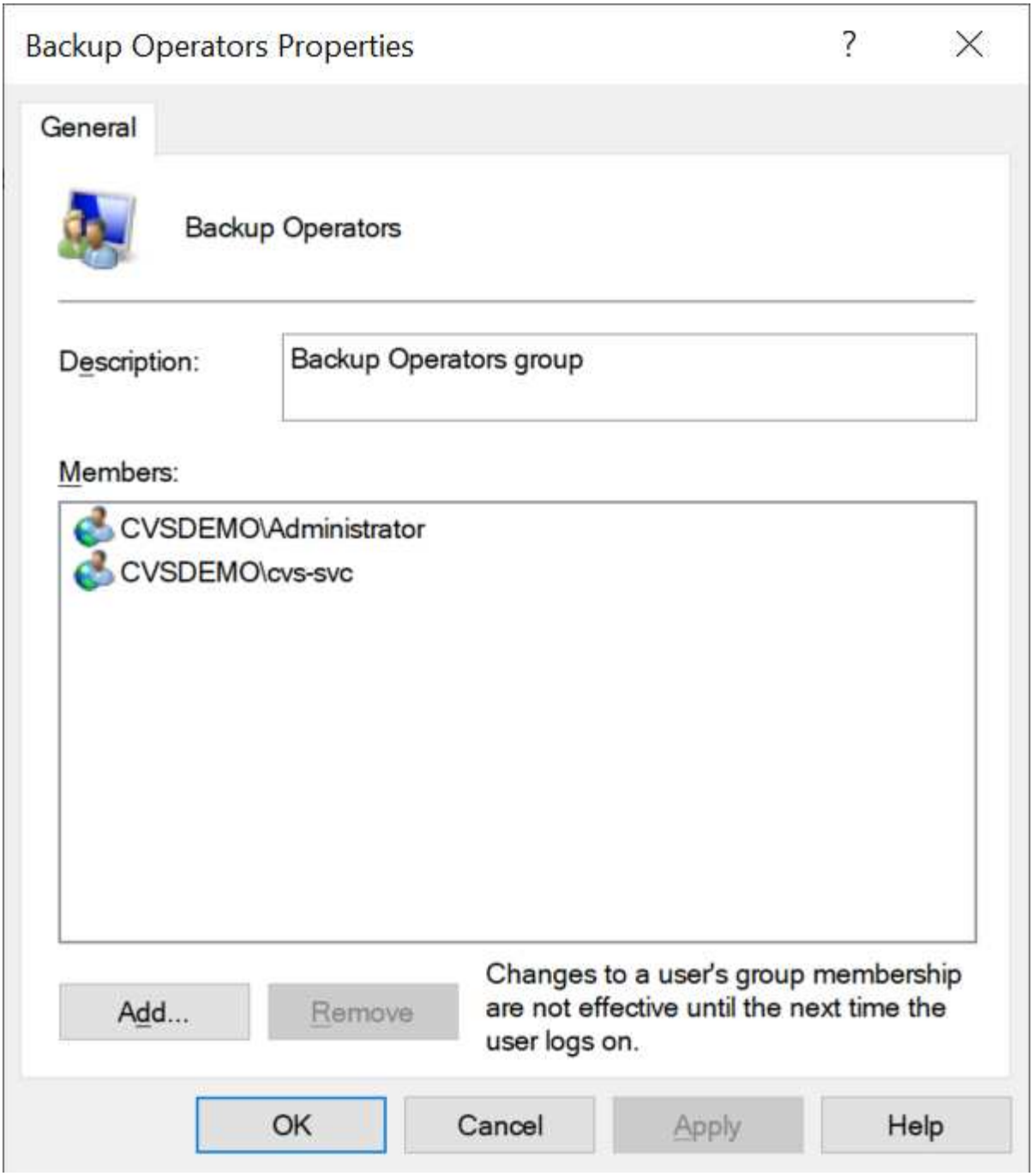
Cuando se especifica un usuario que se va a agregar a los usuarios de copia de seguridad, el usuario se agrega al grupo BUILTIN\operadores de copia de seguridad en la instancia de Cloud Volumes Service que utiliza esa conexión de Active Directory, que a continuación obtiene la "SeBackupPrivilege y SeRestorePrivilege".

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".





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.

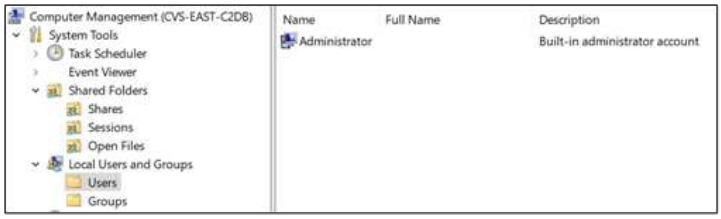


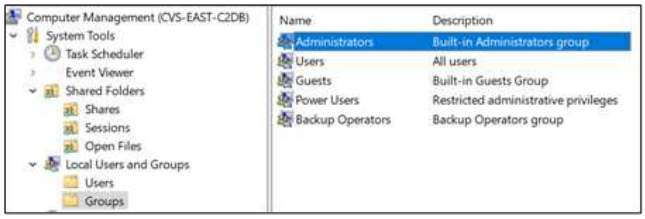
La siguiente tabla muestra la lista de grupos BUILTIN predeterminados y qué usuarios/grupos se agregan de forma predeterminada.

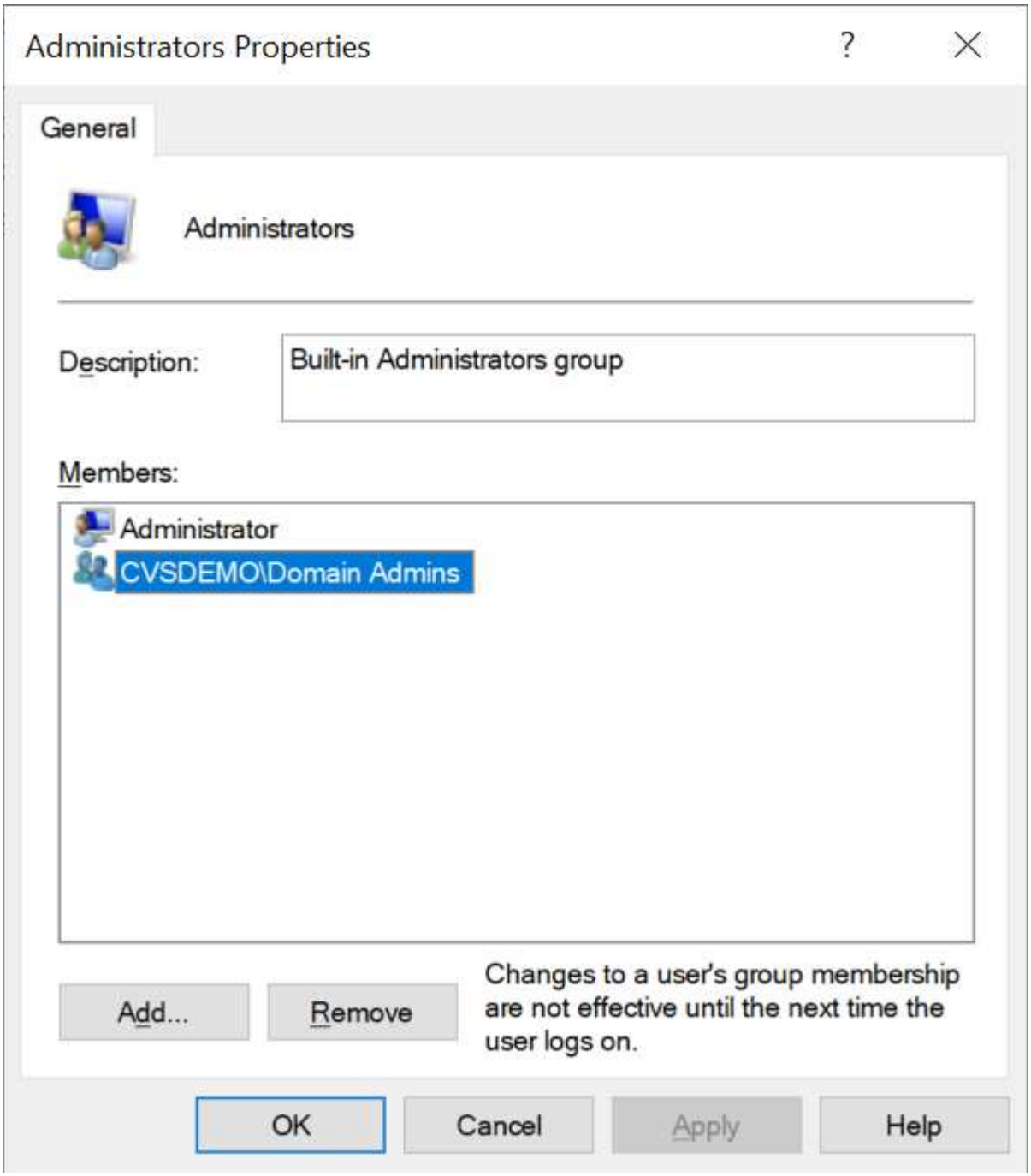
Grupo local/BUILTIN	Miembros predeterminados
BUILTIN\Administrators*	Dominio\Administradores de dominio
Operadores DE COPIAS DE seguridad/BUILTIN*	Ninguno
EDIFICIO\huéspedes	Dominio\invitados de dominio
Usuarios AVANZADOS\BUILTIN	Ninguno
USUARIOS DE BUILTIN\Domain	USUARIOS de DOMINIO/dominio

*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

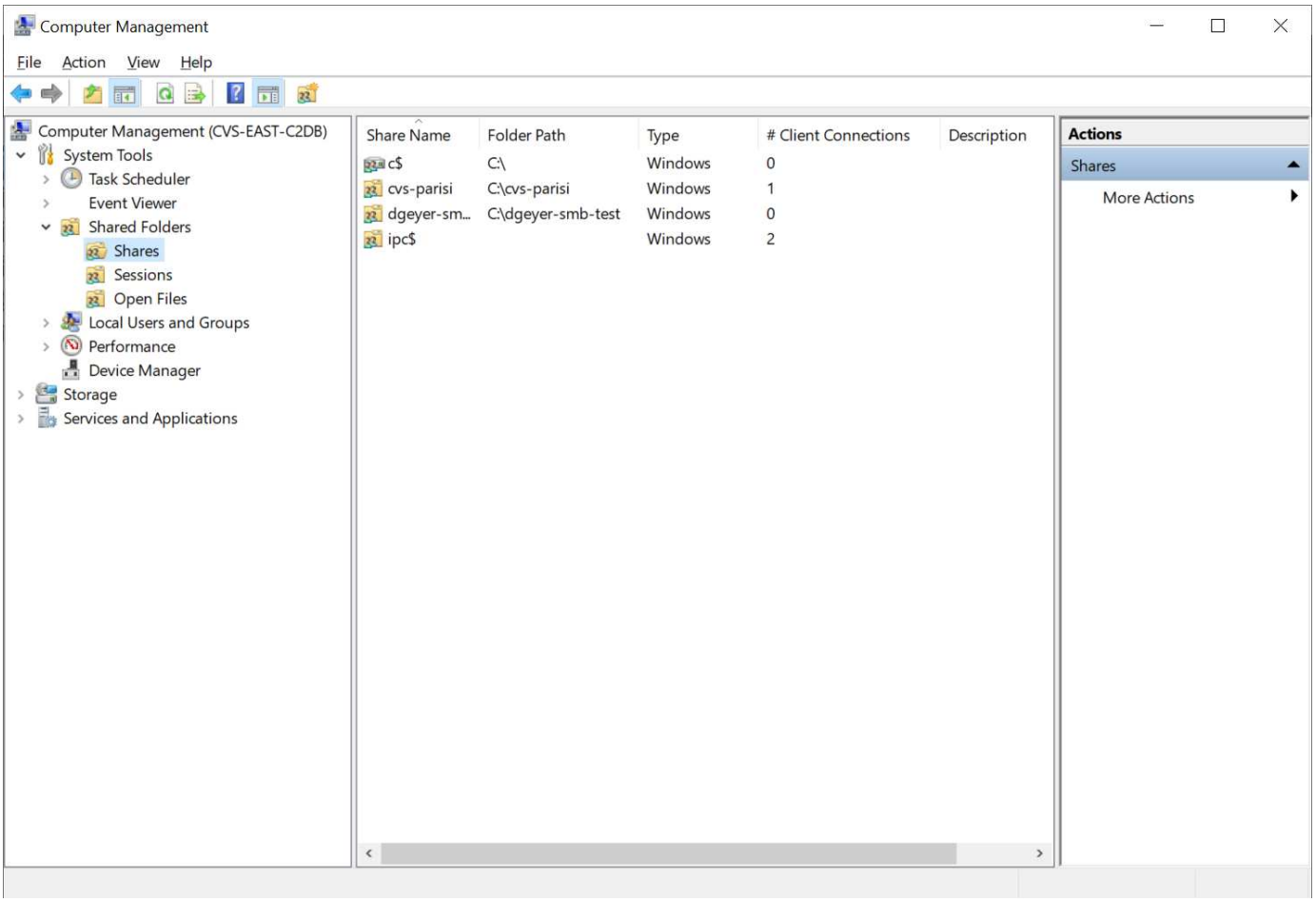
El acceso de SMB en Cloud Volumes Service proporciona conectividad a la MMC de gestión de equipos, que permite ver recursos compartidos, gestionar ACL de uso compartido, ver/gestionar sesiones de SMB y archivos abiertos.

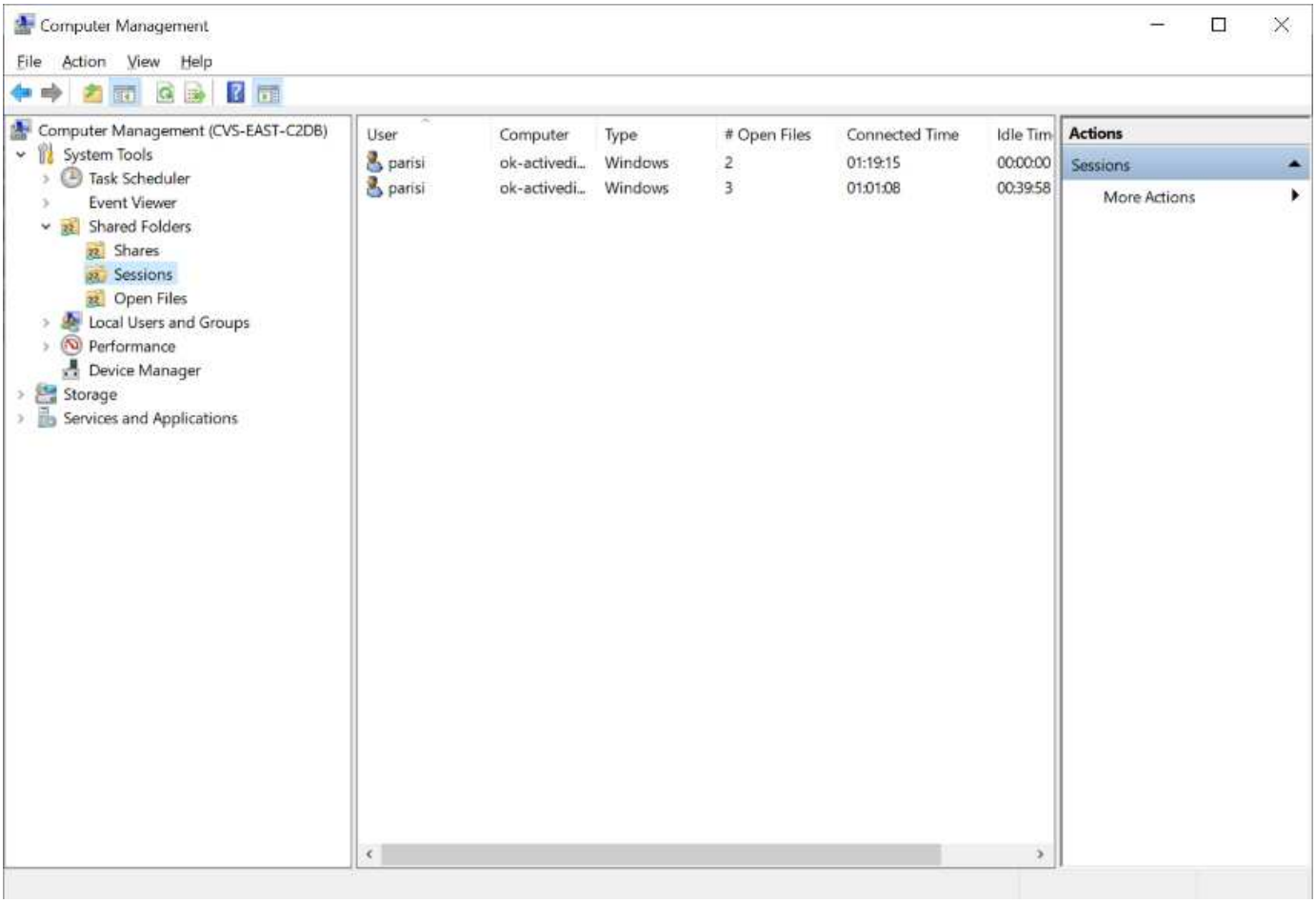
Para utilizar MMC para ver los recursos compartidos y las sesiones de SMB en Cloud Volumes Service, el usuario que ha iniciado sesión debe ser un administrador de dominio. A otros usuarios se les permite el acceso para ver o administrar el servidor SMB desde MMC y recibir un cuadro de diálogo no tiene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

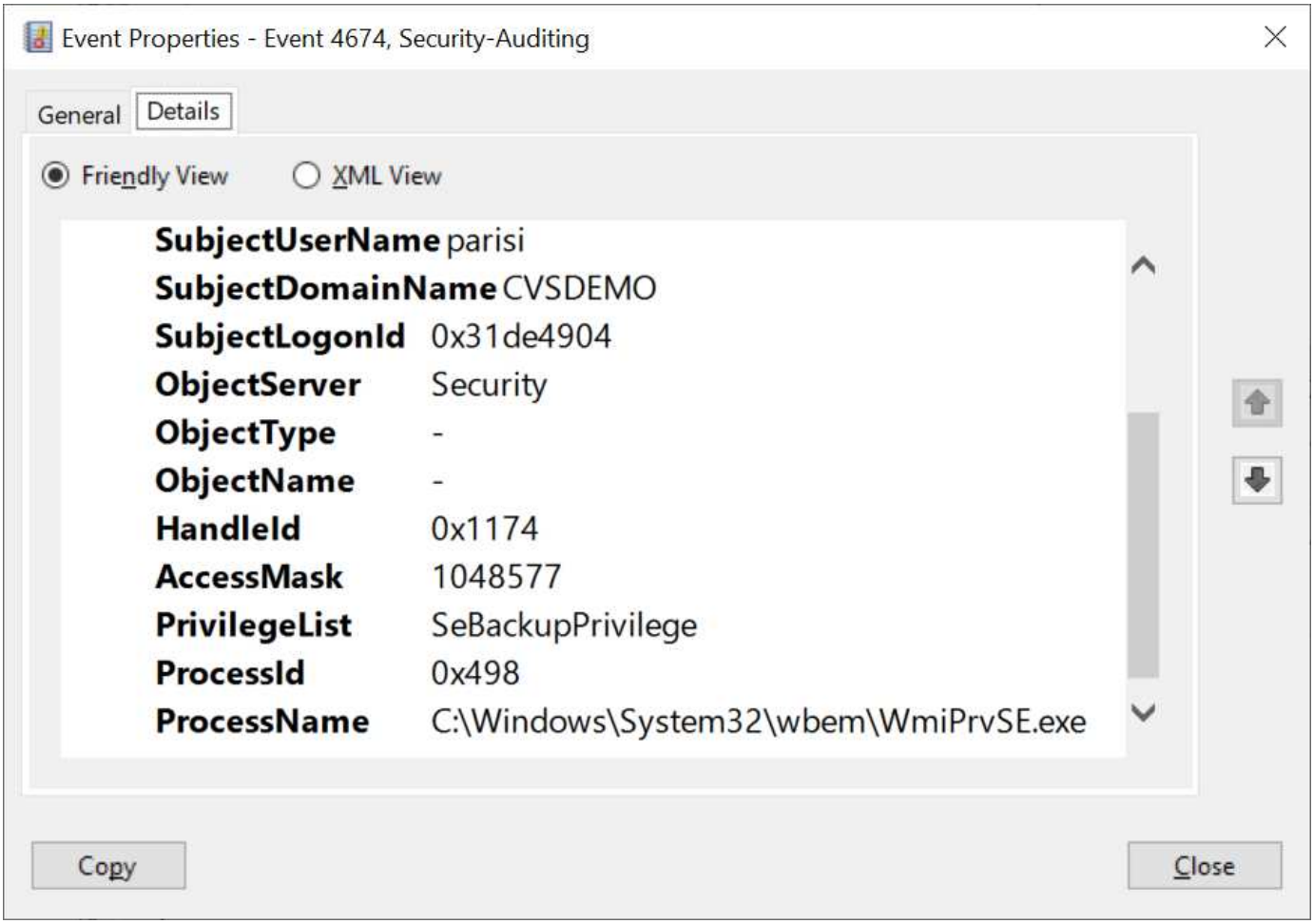
Región

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.

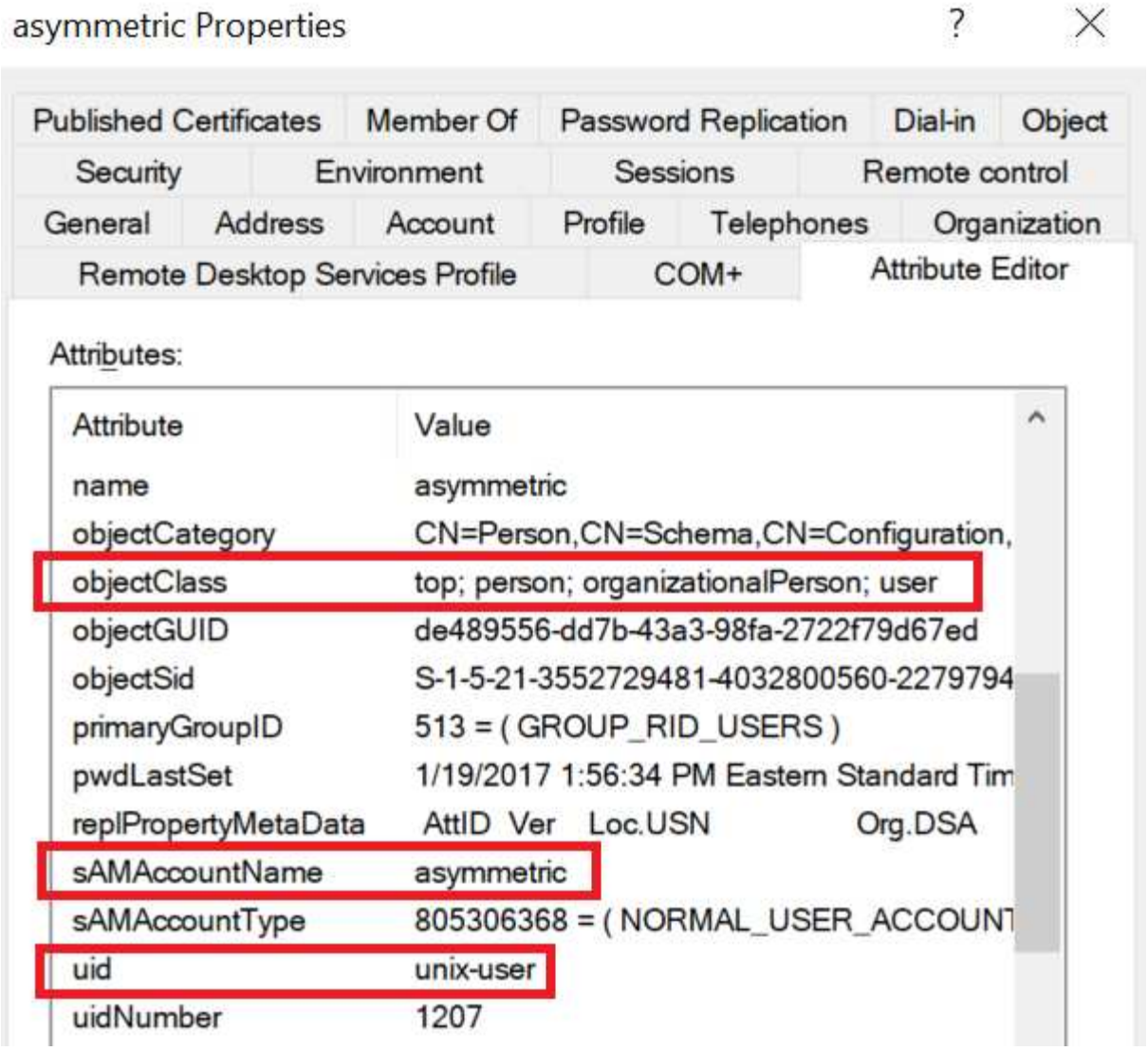
En la siguiente tabla se muestran los atributos que se deben rellenar en LDAP para la funcionalidad de asignación de nombres asimétrica. En la mayoría de los casos, Active Directory ya está configurado para hacerlo.

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.

Operación de servicio

El equipo de Cloud Volumes Service gestiona los servicios de back-end en Google Cloud y utiliza varias estrategias para proteger la plataforma y evitar el acceso no deseado.

Cada cliente obtiene su propia subred única, que tiene acceso acotado de forma predeterminada a otros clientes; cada cliente de Cloud Volumes Service obtiene su propio espacio de nombres y VLAN para aislar todos los datos. Una vez autenticado un usuario, el motor de entrega de servicios (SDE) sólo puede leer los datos de configuración específicos de ese arrendatario.

Seguridad física

Con la aprobación previa adecuada, solo los ingenieros in situ y los ingenieros de soporte de campo (FSE) con insignia de NetApp tienen acceso a la jaula y los racks para trabajar físicamente. La gestión de almacenamiento y redes no está permitida. Solo estos recursos in situ pueden realizar tareas de mantenimiento del hardware.

Para los ingenieros in situ, se crea un ticket para la descripción del trabajo (SOW, Stament ID) que incluye el identificador de rack y la ubicación del dispositivo (RU), y todos los demás detalles se incluyen en la incidencia. En el caso de los FSE de NetApp, es necesario elevar un ticket de visita a las instalaciones con LA COLOCACIÓN y el ticket incluye los detalles, la fecha y la hora del visitante a efectos de auditoría. La Descripción del Trabajo para el FSE se comunica internamente a NetApp.

Equipo de operaciones

El equipo de operaciones de Cloud Volumes Service consta de ingeniería de producción y un ingeniero de fiabilidad de sitio (SRE) para servicios de volumen de cloud, e ingenieros de soporte de campo y partners de NetApp para hardware. Todos los miembros del equipo de operaciones están acreditados por su trabajo en Google Cloud y se mantienen registros detallados del trabajo para cada ticket generado. Además, existe un estricto proceso de control y aprobación de cambios para garantizar que cada decisión sea examinada adecuadamente.

El equipo de SRE gestiona el plano de control y cómo se enrutan los datos desde las solicitudes de la interfaz de usuario al hardware y software de back-end en Cloud Volumes Service. El equipo de SRE también gestiona los recursos del sistema, como los máximos de volumen e inodo. Los SRE no pueden interactuar con los datos del cliente ni tener acceso a ellos. Los Sres también proporcionan coordinación con Autorizaciones de devolución de material (RMA), como solicitudes de sustitución de disco o memoria nuevas para el

hardware de backend.

Responsabilidades del Cliente

Los clientes de Cloud Volumes Service gestionan la administración de Active Directory y las funciones de usuario de su empresa, así como las operaciones de volumen y datos. Los clientes pueden tener roles administrativos y pueden delegar permisos en otros usuarios finales dentro del mismo proyecto de Google Cloud con las dos funciones predefinidas que proporcionan NetApp y Google Cloud (Administrador y Visor).

El administrador puede establecer la relación entre iguales de cualquier VPC del proyecto del cliente a Cloud Volumes Service que el cliente determine que es apropiado. Es responsabilidad del cliente gestionar el acceso a su suscripción a Google Cloud Marketplace y gestionar los ordenadores virtuales que tienen acceso al plano de datos.

Protección frente a SRE maliciosa

Una preocupación que podría surgir es cómo protege Cloud Volumes Service frente a situaciones en las que hay una SRE maliciosa o cuando se han comprometido las credenciales de SRE?

El acceso al entorno de producción es sólo con un número limitado de personas que reciben servicios de salud sexual y reproductiva. Los privilegios administrativos se limitan además a un puñado de administradores con experiencia. Todas las acciones realizadas por cualquier persona en el entorno de producción de Cloud Volumes Service se registran y cualquier anomalía en la línea de base o actividades sospechosas es detectada por nuestra plataforma de inteligencia de amenazas de gestión de eventos e información de seguridad (SIEM). Como resultado, se puede realizar un seguimiento y mitigar de acciones maliciosas antes de que se produzcan demasiados daños en el entorno de administración de Cloud Volumes Service.

Ciclo de vida de volumen

Cloud Volumes Service solo gestiona los objetos dentro del servicio, no los datos dentro de los volúmenes. Solo los clientes que acceden a los volúmenes pueden gestionar los datos, las ACL, los propietarios de archivos, etc. Los datos de estos volúmenes se cifran en reposo y el acceso se limita a los inquilinos de la instancia de Cloud Volumes Service.

El ciclo de vida del volumen para Cloud Volumes Service es create-update-delete. Los volúmenes conservan las copias Snapshot de los volúmenes hasta que se eliminan los volúmenes y solo los administradores de Cloud Volumes Service validados pueden eliminar volúmenes en Cloud Volumes Service. Cuando un administrador solicita la eliminación de un volumen, se necesita un paso adicional para introducir el nombre del volumen para verificar la eliminación. Una vez eliminado el volumen, este ya no se puede recuperar.

En los casos en que se termina un contrato de Cloud Volumes Service, NetApp Marca los volúmenes para su eliminación después de un período de tiempo específico. Antes de que caduque ese período de tiempo, puede recuperar volúmenes a petición del cliente.

Certificaciones

Cloud Volumes Services para Google Cloud está certificado actualmente para cumplir los estándares ISO/IEC 27001:2013 e ISO/IEC 27018:2019. El servicio también recibió recientemente su informe de certificación SOC2 de tipo I. Si desea obtener más información sobre el compromiso de NetApp con la privacidad y la seguridad de los datos, consulte "Cumplimiento de normativas: Seguridad y privacidad de los datos".

RGPD

Nuestros compromisos con respecto a la privacidad y el cumplimiento del RGPD están disponibles en diversos de nuestros "contratos con clientes", como nuestro "Adición al procesamiento de datos del cliente",

que incluye la "Cláusulas contractuales estándar" Proporcionado por la Comisión Europea. También asumimos estos compromisos en nuestra Política de privacidad, respaldada por los valores fundamentales establecidos en nuestro Código de conducta corporativo.

Información adicional e información de contacto

Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

- Documentación de Google Cloud para Cloud Volumes Service

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes/"

- Acceso a servicios privados de Google

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- Documentación de productos de NetApp

  "https://www.netapp.com/support-and-training/documentation/"

- Programa de módulos de validación criptográfico—NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- La solución de NetApp para ransomware

  https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

- TR-4616: Kerberos de NFS en ONTAP

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

Póngase en contacto con nosotros

Háganos saber cómo podemos mejorar este informe técnico.

Póngase en contacto con nosotros en correo electrónico: doccomments@netapp.com [doccomments@netapp.com]. Incluir EL INFORME TÉCNICO 4918 en el asunto.

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.