NetApp para GCP/GCVE

NetApp Solutions

NetApp
December 19, 2024

Tabla de contenidos

NetApp para GCP/GCVE

Funcionalidades de NetApp para Google Cloud Platform GCVE

Obtén más información sobre las funcionalidades que NetApp aporta a Google Cloud Platform (GCP) Google Cloud VMware Engine (GCVE), desde NetApp como dispositivo de almacenamiento conectado invitado o un almacén de datos NFS complementario para migrar flujos de trabajo, extender/irrumpir a la nube, backup/restauración y recuperación ante desastres.

Para ir a la sección del contenido deseado, seleccione una de las siguientes opciones:

- "Configuración de GCVE en GCP"
- "Opciones de almacenamiento de NetApp para GCVE"
- "Soluciones cloud de NetApp/VMware"

Configuración de GCVE en GCP

Al igual que en las instalaciones, la planificación de un entorno de virtualización basado en cloud es crucial para tener un entorno preparado para la producción con éxito a la hora de crear equipos virtuales y migración.

En esta sección se describe cómo configurar y gestionar GCVE y cómo utilizarlo junto con las opciones disponibles para conectar el almacenamiento de NetApp.

> El almacenamiento en invitado es el único método compatible para conectar volúmenes de Cloud Volumes ONTAP y Google Cloud NetApp a GCVE.

El proceso de configuración puede dividirse en los siguientes pasos:

- Implementar y configurar GCVE
- Active el acceso privado a GCVE

Vea el detalles "Pasos de configuración para GCVE".

Opciones de almacenamiento de NetApp para GCVE

El almacenamiento de NetApp se puede utilizar de varias maneras, ya sea como adivinar conectado o como un almacén de datos NFS complementario, en GCP GCVE.

Visite "Opciones de almacenamiento de NetApp admitidas" si quiere más información.

Google Cloud es compatible con almacenamiento de NetApp en las siguientes configuraciones:

- Cloud Volumes ONTAP (CVO) como almacenamiento conectado como invitado
- Google Cloud NetApp Volumes (NetApp Volumes) como almacenamiento conectado de invitado
- Google Cloud NetApp Volumes (NetApp Volumes) como almacén de datos NFS complementario

Ver los detalles "Opciones de almacenamiento de Guest Connect para GCVE". Ver los detalles "Opciones

complementarias de almacén de datos NFS para GCVE".

Lea más "Compatibilidad con el almacén de datos de NetApp Volumes de Google Cloud para VMware Engine de Google Cloud (blog de NetApp)"sobre o. "Cómo usar volúmenes de NetApp de Google Cloud como almacenes de datos para el motor de VMware de Google Cloud (blog de Google)"

Casos de uso de soluciones

Con las soluciones cloud de NetApp y VMware, la puesta en marcha en Azure AVS resulta sencilla en muchos casos de uso. Los casos de ingenieros de sistemas se definen para cada una de las áreas cloud definidas de VMware:

- Protect (incluye recuperación ante desastres y backup/restauración)
- Extender
- Migración

"Consulte las soluciones de NetApp para Google Cloud GCVE"

Protección de cargas de trabajo en GCP / GCVE

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

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.

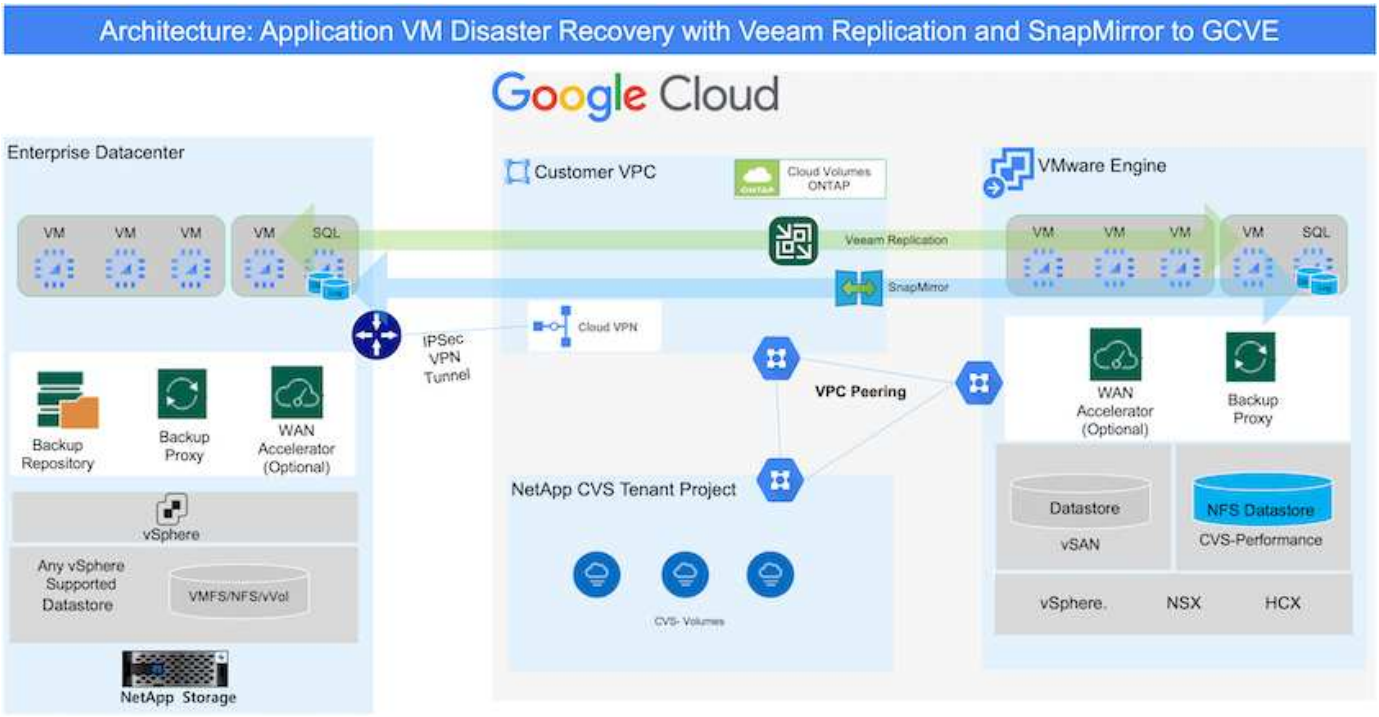
Autores: Suresh Thoppay, NetApp

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

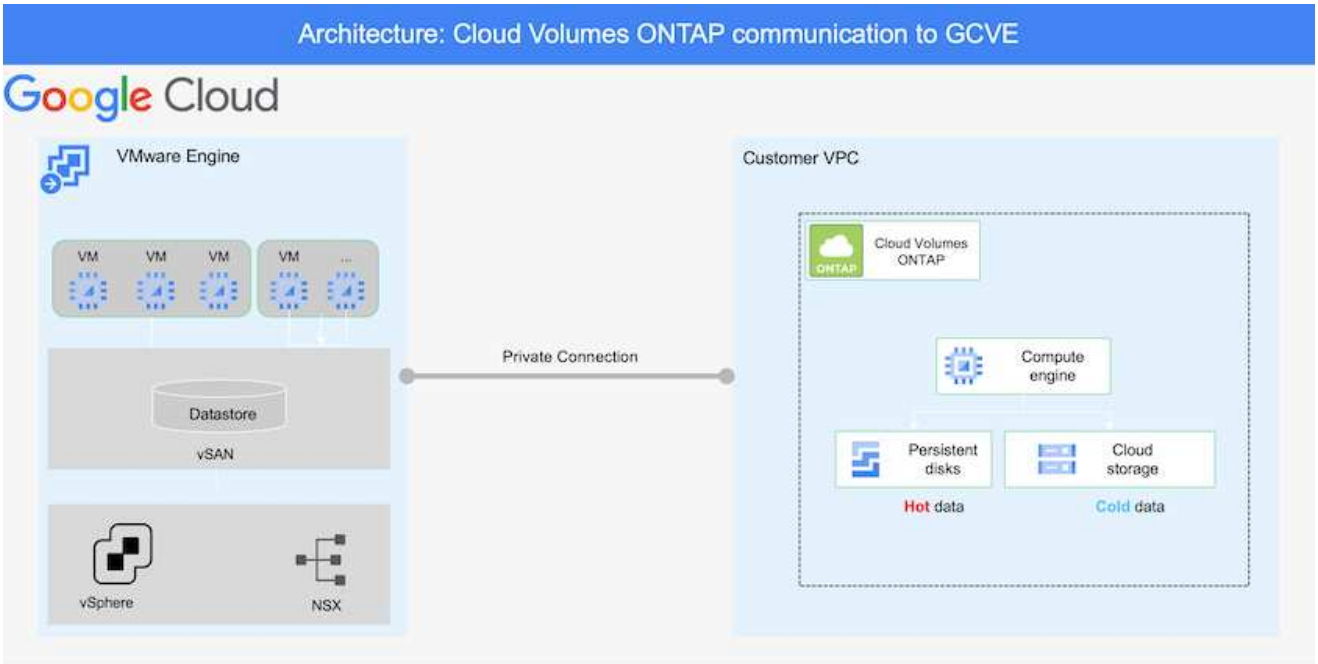
1. Asegúrese de que se realiza el backup de los datos de la aplicación mediante SnapCenter con los requisitos de punto de recuperación necesarios.
2. Aprovisiona Cloud Volumes ONTAP con el tamaño de instancia correcto mediante BlueXP en la suscripción y la red virtual adecuadas.
   a. Configurar SnapMirror 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 es 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"

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 almacén de datos y el registro de Google Cloud NetApp Volumes para NFS y Cloud Volumes ONTAP para SQL pueden implementarse en cualquier VPC y GCVE deben tener conexión privada con ese VPC para montar un almacén de datos NFS y tener conexión de máquinas virtuales a LUN 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

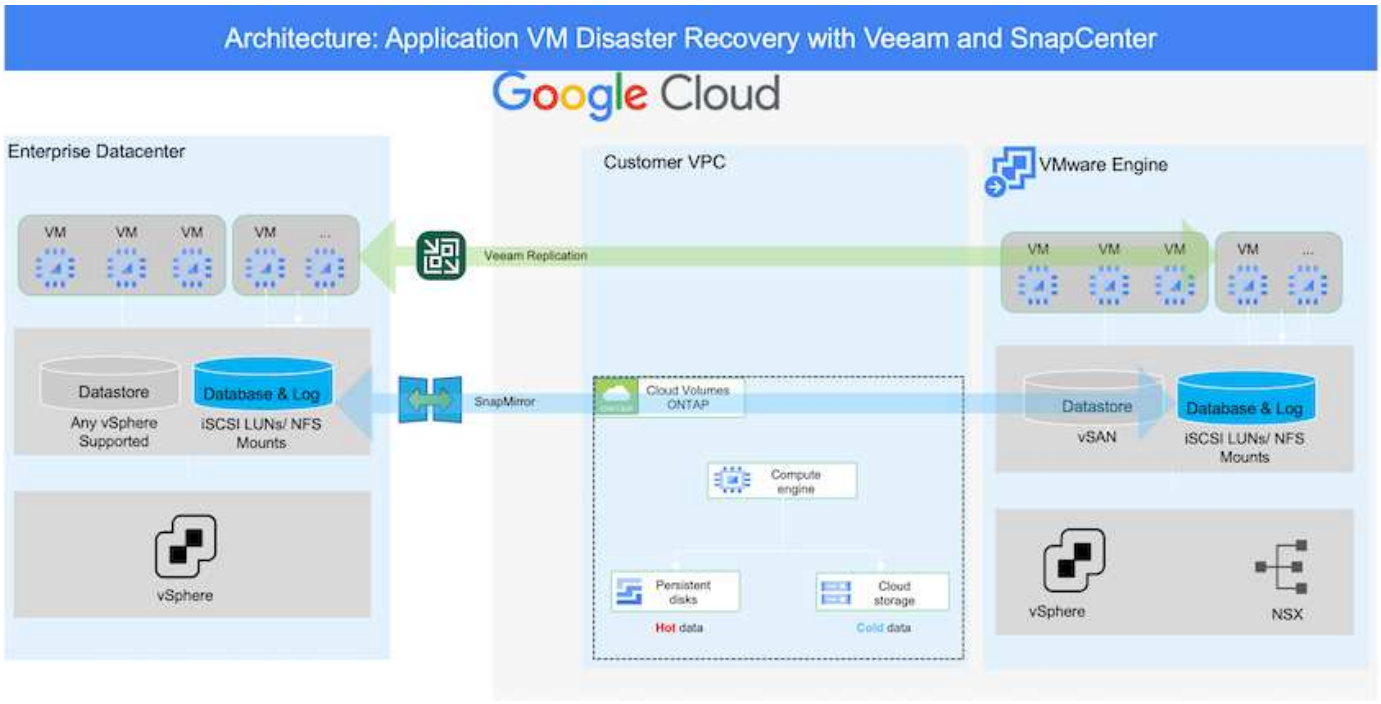
La recuperación ante desastres en el cloud es un método resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos dañados por datos como ransomware. Con SnapMirror de NetApp, las cargas de trabajo de VMware en las instalaciones que utilizan el almacenamiento conectado a invitado se pueden replicar a Cloud Volumes ONTAP de NetApp que se ejecuta en Google Cloud.

Autores: Suresh Thoppay, NetApp

Descripción general

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

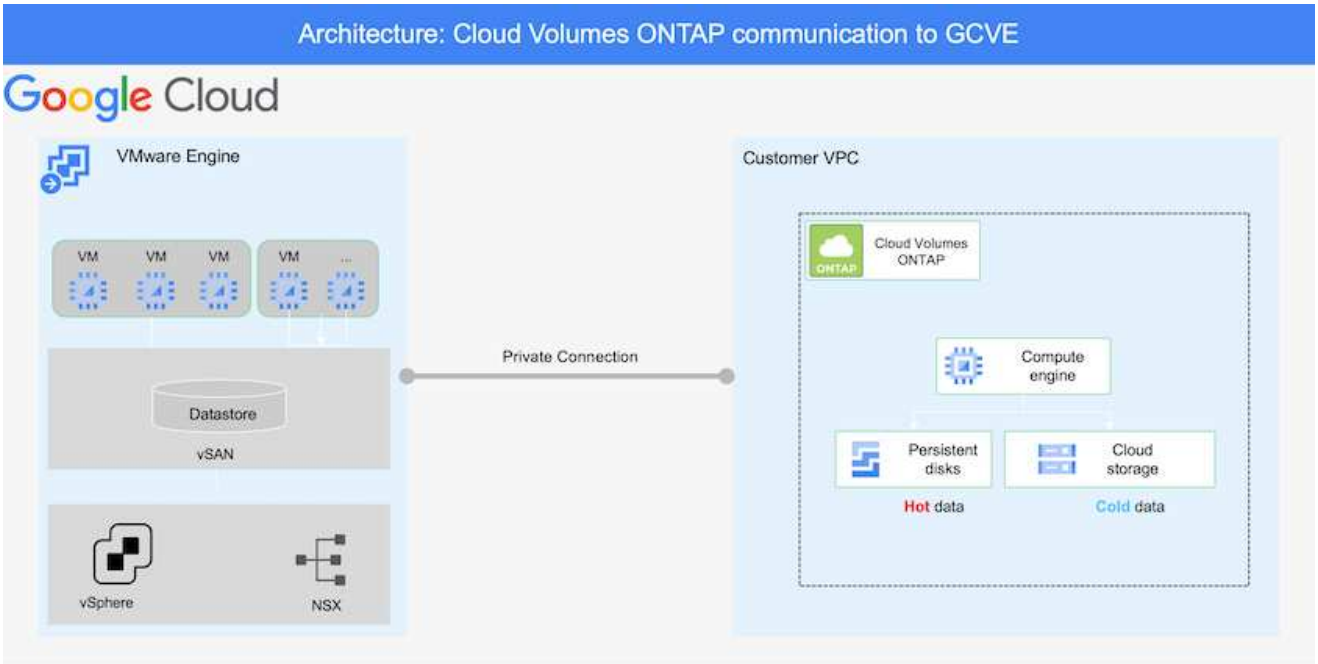
1. Asegúrese de que se realiza el backup de los datos de la aplicación mediante SnapCenter con los requisitos de punto de recuperación necesarios.
2. Aprovisione Cloud Volumes ONTAP con el tamaño de instancia correcto usando Cloud Manager dentro de la suscripción y la red virtual adecuadas.
   a. Configurar 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 es 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.

Usar la replicación de Veeam y el almacén de datos de NetApp Volumes de Google Cloud para la recuperación ante desastres en Google Cloud VMware Engine

Disponer de un completo plan de recuperación ante desastres es crítico para las empresas en momentos de crisis. Muchas organizaciones aprovechan el cloud computing para las operaciones diarias y la recuperación ante desastres. Este enfoque proactivo puede reducir o eliminar costosas interrupciones del negocio.

En este artículo se describe cómo usar el complemento de backup y replicación de Veeam para configurar la recuperación ante desastres para máquinas virtuales VMware locales en Google Cloud VMware Engine (GCVE) con Google Cloud NetApp Volumes (NetApp Volumes).

Descripción general

Google Cloud NetApp Volumes es un servicio de almacenamiento de Google y NetApp que está disponible para Google Cloud. El servicio de volúmenes de NetApp proporciona almacenamiento NFS/SMB de alto rendimiento. El almacenamiento NFS de NetApp Volumes con certificación de VMware se puede usar como almacén de datos externo para hosts ESXi en GCVE. Los usuarios deben establecer una conexión entre iguales entre su cloud privado de GCVE y el proyecto de NetApp Volumes. No hay cargos de red derivados del acceso al almacenamiento dentro de una región. Los usuarios pueden crear volúmenes de NetApp en la consola de Google Cloud y habilitar la protección de eliminación antes de montar volúmenes como almacenes de datos en sus hosts ESXi.

Los almacenes de datos NFS basados en NetApp Volumes pueden usarse para replicar datos desde las instalaciones mediante cualquier solución de terceros validada que ofrezca la funcionalidad de replicación de máquinas virtuales. Al añadir almacenes de datos de NetApp Volumes, permite una implementación optimizada de costos en lugar de crear un SDDC basado en Google Cloud VMware Engine (GCVE) con un gran número de hosts ESXi para acomodar el almacenamiento. Este enfoque se llama un “Clúster de Luz Piloto”. Un clúster ligero piloto es una configuración de host mínima de GCVE (3 hosts ESXi de GCVE) junto con la capacidad de los almacenes de datos de NetApp Volumes para permitir un escalado independiente que cumpla con los requisitos de capacidad.

El objetivo es mantener una infraestructura rentable con solo los componentes principales para gestionar una recuperación tras fallos. Un clúster piloto ligero puede expandir y agregar más hosts de GCVE en caso de una conmutación por error. Una vez resuelta la conmutación por error y se reanudan las operaciones normales, el grupo piloto ligero puede reducir su escala, volviendo a un modo operativo de bajo coste.

Objetivos de este documento

En este artículo se describe cómo usar un almacén de datos de NetApp Volumes de Google Cloud con Veeam

Backup & Replication para configurar la recuperación ante desastres para máquinas virtuales VMware locales en GCVE mediante la funcionalidad de software de replicación de Veeam VM.

Veeam Backup & Replication es una aplicación de backup y replicación para entornos virtuales. Cuando se replican las máquinas virtuales, Veeam Backup & Replication creará una copia exacta de las máquinas virtuales en el formato nativo de VMware vSphere en el clúster SDDC de GCVE de destino. Veeam Backup & Replication mantendrá la copia sincronizada con la máquina virtual original. La replicación proporciona el mejor objetivo de tiempo de recuperación (RTO) dado que hay una copia montada de un equipo virtual en el sitio de recuperación de desastres en estado listo para el inicio.

Este mecanismo de replicación garantiza que las cargas de trabajo puedan iniciarse rápidamente en GCVE en caso de un evento de desastre. El software Veeam Backup & Replication también optimiza la transmisión del tráfico para la replicación a través de WAN y conexiones lentas. Además, también filtra los bloques de datos duplicados, cero bloques de datos, archivos de intercambio y «archivos excluidos del SO invitado del equipo virtual». El software también comprimirá el tráfico de réplica. Para evitar que los trabajos de replicación consuman todo el ancho de banda de la red, se pueden utilizar aceleradores WAN y reglas de limitación de red.

El proceso de replicación en Veeam Backup & Replication está controlado por tareas, lo que significa que la replicación se realiza mediante la configuración de trabajos de replicación. En caso de desastre, se puede activar la conmutación al respaldo para recuperar las máquinas virtuales conmutando por error a su copia replicada. Cuando se realiza una conmutación por error, una máquina virtual replicada asume el rol de la máquina virtual original. La conmutación por error se puede realizar al estado más reciente de una réplica o a cualquiera de sus puntos de restauración en buen estado conocidos. Esto permite la recuperación frente al ransomware o las pruebas aisladas según sea necesario. Veeam Backup & Replication ofrece múltiples opciones para gestionar diferentes escenarios de recuperación ante desastres.

Descripción general de la solución

Esta solución cubre los siguientes pasos generales:

1. Crea un volumen NFS mediante Google Cloud NetApp Volumes
2. Siga el proceso de GCP para crear un almacén de datos de GCVE a partir del volumen NFS de NetApp Volumes.
3. Configure un trabajo de replicación para crear réplicas de máquinas virtuales con Veeam Backup & Replication.
4. Cree un plan de recuperación tras fallos y realice una recuperación tras fallos.
5. Vuelva a los equipos virtuales de producción una vez que el evento de desastre haya finalizado y el sitio principal esté activo.

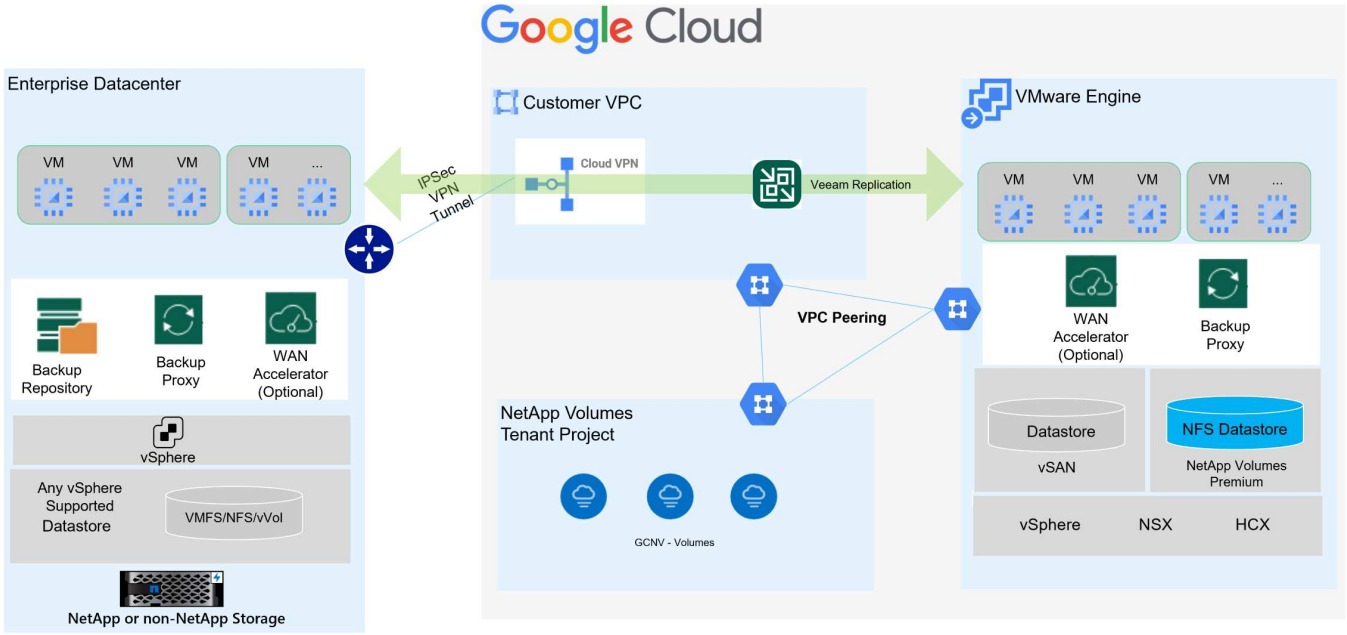
> Al crear un volumen en volúmenes de NetApp, para usarlo como almacén de datos GCVE, solo se admite NFS v3.

Para obtener más información sobre el uso de volúmenes NFS de NetApp Volumes como almacenes de datos de GCVE, consulte "Usar un volumen NFS como almacén de datos de vSphere alojado por Google Cloud NetApp Volumes" .

Arquitectura

El siguiente diagrama muestra la arquitectura de la solución presentada en esta documentación. Una práctica recomendada es tener un servidor Veeam Backup & Replication ubicado tanto en el sitio local como en el SDDC de GCVE. El servidor de Veeam en las instalaciones realiza y gestiona la copia de seguridad y la

recuperación, y el servidor de Veeam gestiona la replicación en el SDDC de GCVE. Esta arquitectura proporciona la máxima disponibilidad cuando se produce un fallo en el centro de datos primario.



Requisitos previos para la replicación de Veeam en almacenes de datos de GCVE y NetApp Volumes

Esta solución requiere los siguientes componentes y configuraciones:

1. Los volúmenes NetApp tienen un pool de almacenamiento disponible con capacidad libre suficiente para acomodar el volumen NFS que se va a crear.
2. El software Veeam Backup and Replication se ejecuta en un entorno local con la conectividad de red adecuada.
3. Asegúrese de que la máquina virtual de backup de Veeam Backup & Replication está conectada al origen y a los clústeres de SDDC GCVE de destino.
4. Asegúrese de que la máquina virtual de copia de seguridad de Veeam Backup & Replication está conectada a las máquinas virtuales del servidor proxy de Veeam tanto en los clústeres de GCVE de origen como de destino.
5. El servidor de copia de seguridad debe ser capaz de resolver nombres cortos y conectarse a vCenters de origen y destino.

Los usuarios deben establecer una conexión de interconexión entre la nube privada de GCVE y el proyecto de volúmenes de NetApp mediante las páginas de interconexión de red de VPC o conexiones privadas dentro de la interfaz de usuario de la consola de VMware Engine Cloud.

Veeam requiere una cuenta de usuario de la solución GCVE con Privileges elevado al agregar el servidor de vCenter de GCVE al inventario de Veeam Backup and Replication. Para obtener más información, consulte la documentación de Google Cloud Platform (GCP), "Elevación de VMware Engine Privileges".

Para obtener información adicional, consulte "Consideraciones y limitaciones" en la documentación de Veeam Backup & Replication.

Pasos de la implementación

Las siguientes secciones describen los pasos de implementación para crear y montar un almacén de datos NFS con volúmenes de NetApp de Google Cloud, y usar el backup y la replicación de Veeam para implementar una solución completa de recuperación ante desastres entre un centro de datos on-premises y el motor de VMware de Google Cloud.

Crear volumen y almacén de datos de NetApp Volumes NFS para GCVE

Consulte "Usar un volumen NFS como almacén de datos de vSphere alojado por Google Cloud NetApp Volumes" para ver información general sobre cómo usar Google Cloud NetApp Volumes como almacén de datos para GCVE.

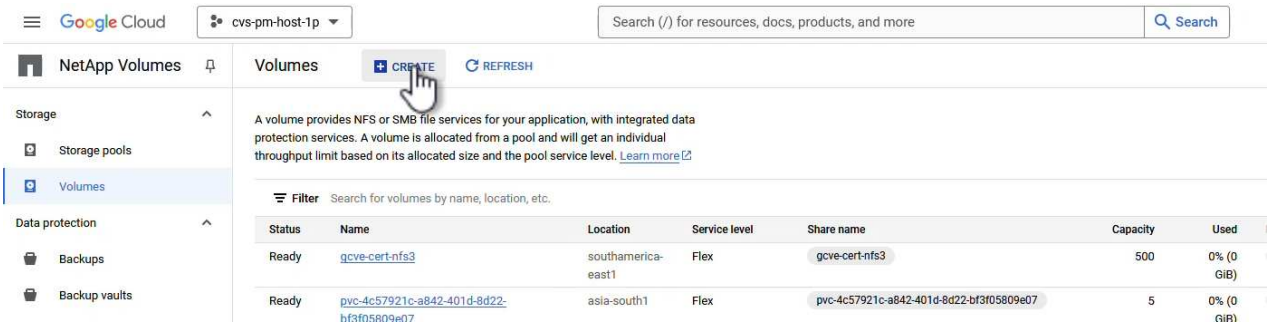
Complete los siguientes pasos para crear y utilizar un almacén de datos NFS para GCVE mediante volúmenes de NetApp:

Cree un volumen de NetApp Volumes NFS

Para acceder a Google Cloud NetApp Volumes desde la consola de Google Cloud Platform (GCP).

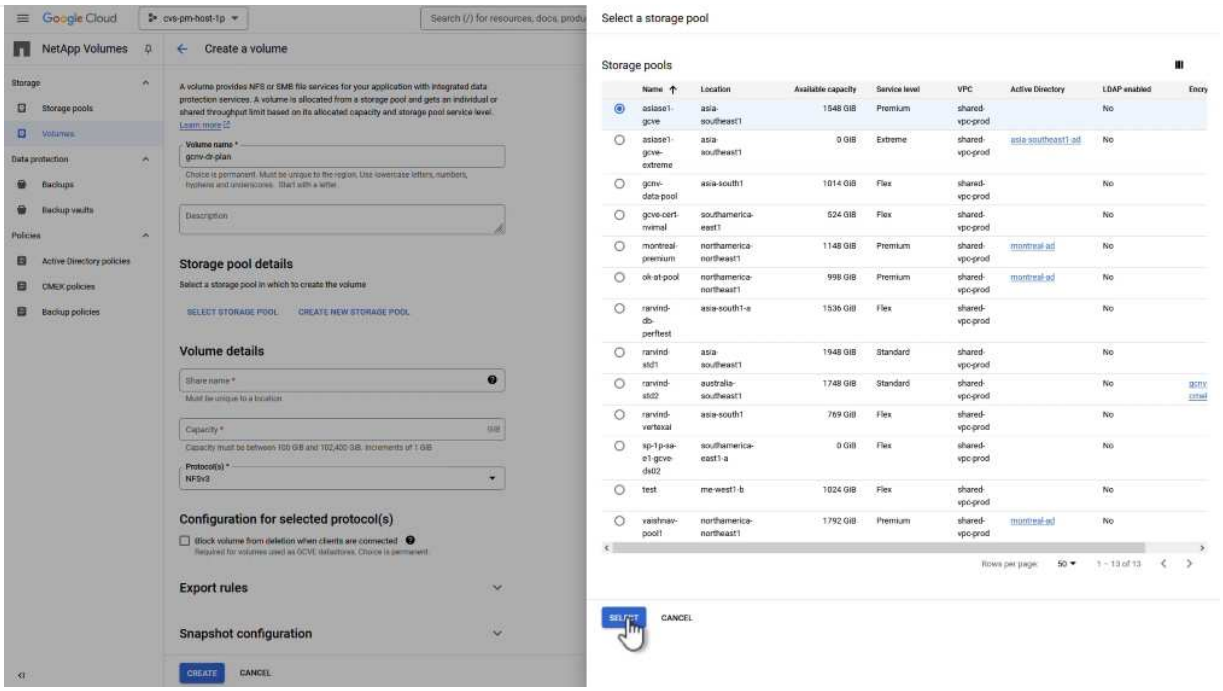
Consulte "Cree un volumen" en la documentación de Google Cloud NetApp Volumes para obtener información más detallada sobre este paso.

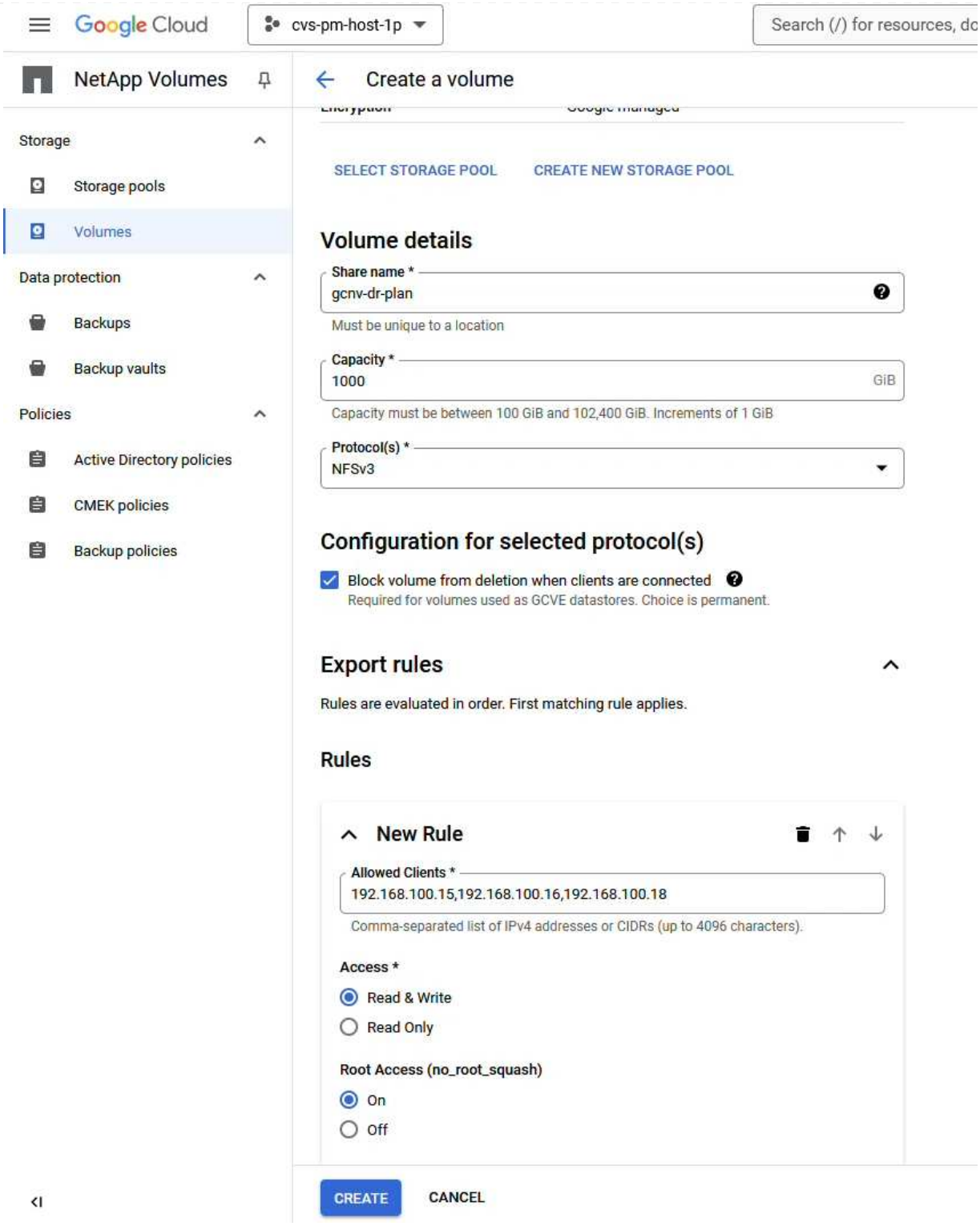
1. En un navegador web, navega https://console.cloud.google.com/ e inicia sesión en tu consola de GCP. Busque **NetApp Volumes** para comenzar.
2. En la interfaz de administración de **NetApp Volumes**, haz clic en **Crear** para comenzar a crear un volumen NFS.



3. En el asistente de **Crear un volumen**, complete toda la información requerida:
   - Un nombre del volumen.
   - El pool de almacenamiento en el que se crea el volumen.
   - Nombre de recurso compartido que se utiliza para montar el volumen de NFS.
   - La capacidad del volumen en GiB.
   - El protocolo de almacenamiento que se va a utilizar.
   - Marque la casilla para **Bloquear el volumen de la eliminación cuando los clientes están conectados** (requerido por GCVE al montarlo como un almacén de datos).
   - Las reglas de exportación para acceder al volumen. Estas son las direcciones IP de los adaptadores de ESXi en la red NFS.
   - Una programación Snapshot que se utiliza para proteger el volumen con Snapshot locales.
   - De manera opcional, elija realizar un backup del volumen y/o crear etiquetas para el volumen.

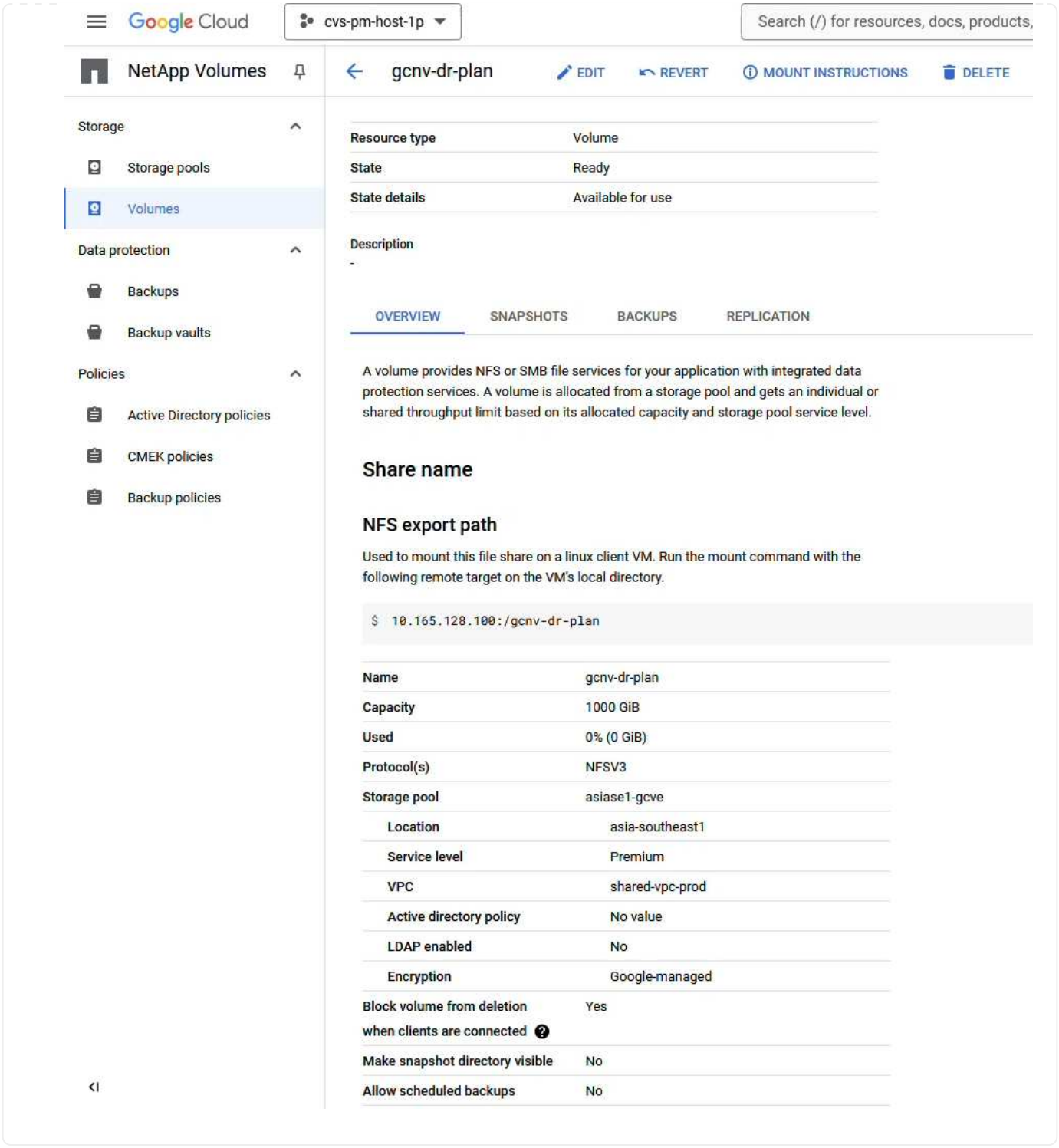
> Al crear un volumen en volúmenes de NetApp, para usarlo como almacén de datos GCVE, solo se admite NFS v3.


Google Cloud
cvs-pm-host-1p
Search (/) for resources, docs, produ
NetApp Volumes
Create a volume
Storage
Storage pools
Volumes
Data protection
Backups
Backup vaults
Policies
Active Directory policies
CMEK policies
Backup policies
A volume provides NFS or SMB file services for your application with integrated data protection services. A volume is allocated from a storage pool and gets an individual or shared throughput limit based on its allocated capacity and storage pool service level.
Learn more
Volume name *
gcnv-dr-plan
Choice is permanent. Must be unique to the region. Use lowercase letters, numbers, hyphens and underscores. Start with a letter.
Description
Storage pool details
Select a storage pool in which to create the volume
SELECT STORAGE POOL
CREATE NEW STORAGE POOL
Volume details
Share name *
Must be unique to a location
Capacity *
GiB
Capacity must be between 100 GiB and 102,400 GiB. Increments of 1 GiB
Protocol(s) *
NFSv3
Configuration for selected protocol(s)
Block volume from deletion when clients are connected
Required for volumes used as OCVE datastores. Choice is permanent.
Export rules
Snapshot configuration
CREATE
CANCEL
Select a storage pool
Storage pools
Name
Location
Available capacity
Service level
VPC
Active Directory
LDAP enabled
Encry
asiase1-gcve
asia-southeast1
1548 GiB
Premium
shared-vpc-prod
No
asiase1-gcve-extreme
asia-southeast1
0 GiB
Extreme
shared-vpc-prod
asia-southeast1-ad
No
gcnv-data-pool
asia-south1
1014 GiB
Flex
shared-vpc-prod
No
gcve-cert-nvimal
southamerica-east1
524 GiB
Flex
shared-vpc-prod
No
montreal-premium
northamerica-northeast1
1148 GiB
Premium
shared-vpc-prod
montreal-ad
No
ok-at-pool
northamerica-northeast1
998 GiB
Premium
shared-vpc-prod
montreal-ad
No
ranvind-db-perftest
asia-south1-a
1536 GiB
Flex
shared-vpc-prod
No
ranvind-std1
asia-southeast1
1948 GiB
Standard
shared-vpc-prod
No
ranvind-std2
australia-southeast1
1748 GiB
Standard
shared-vpc-prod
No
gcnv cmek
ranvind-vertexai
asia-south1
769 GiB
Flex
shared-vpc-prod
No
sp-1p-sa-e1-gcve-ds02
southamerica-east1-a
0 GiB
Flex
shared-vpc-prod
No
test
me-west1-b
1024 GiB
Flex
shared-vpc-prod
No
vaishnav-pool1
northamerica-northeast1
1792 GiB
Premium
shared-vpc-prod
montreal-ad
No
Rows per page: 50
1 – 13 of 13
SELECT
CANCEL



Haga clic en **Crear** para terminar de crear el volumen.

4. Una vez que se ha creado el volumen, la ruta de exportación NFS necesaria para montar el volumen puede visualizarse desde la página de propiedades del volumen.



Monte el almacén de datos NFS en GCVE

En el momento de escribir esto, el proceso para montar un almacén de datos en GCVE requiere abrir un ticket de soporte de GCP para que el volumen se monte como almacén de datos NFS.

Consulte "Usar un volumen NFS como almacén de datos de vSphere alojado por Google Cloud NetApp Volumes" si desea obtener más información.

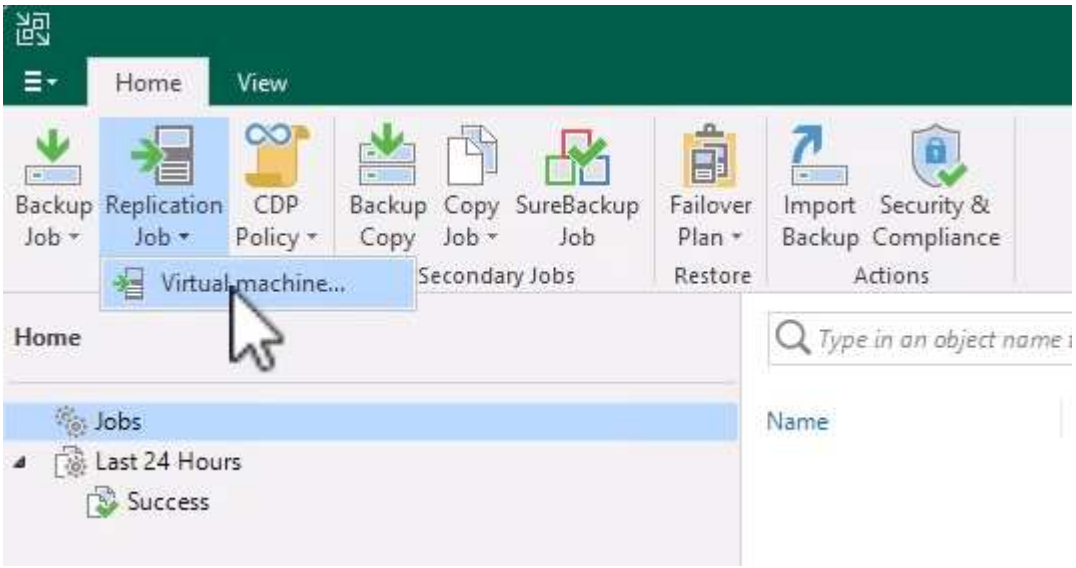
Replica las máquinas virtuales en GCVE y ejecuta el plan de conmutación al nodo de respaldo y la conmutación de retorno tras recuperación

Replicar máquinas virtuales en un almacén de datos NFS en GCVE

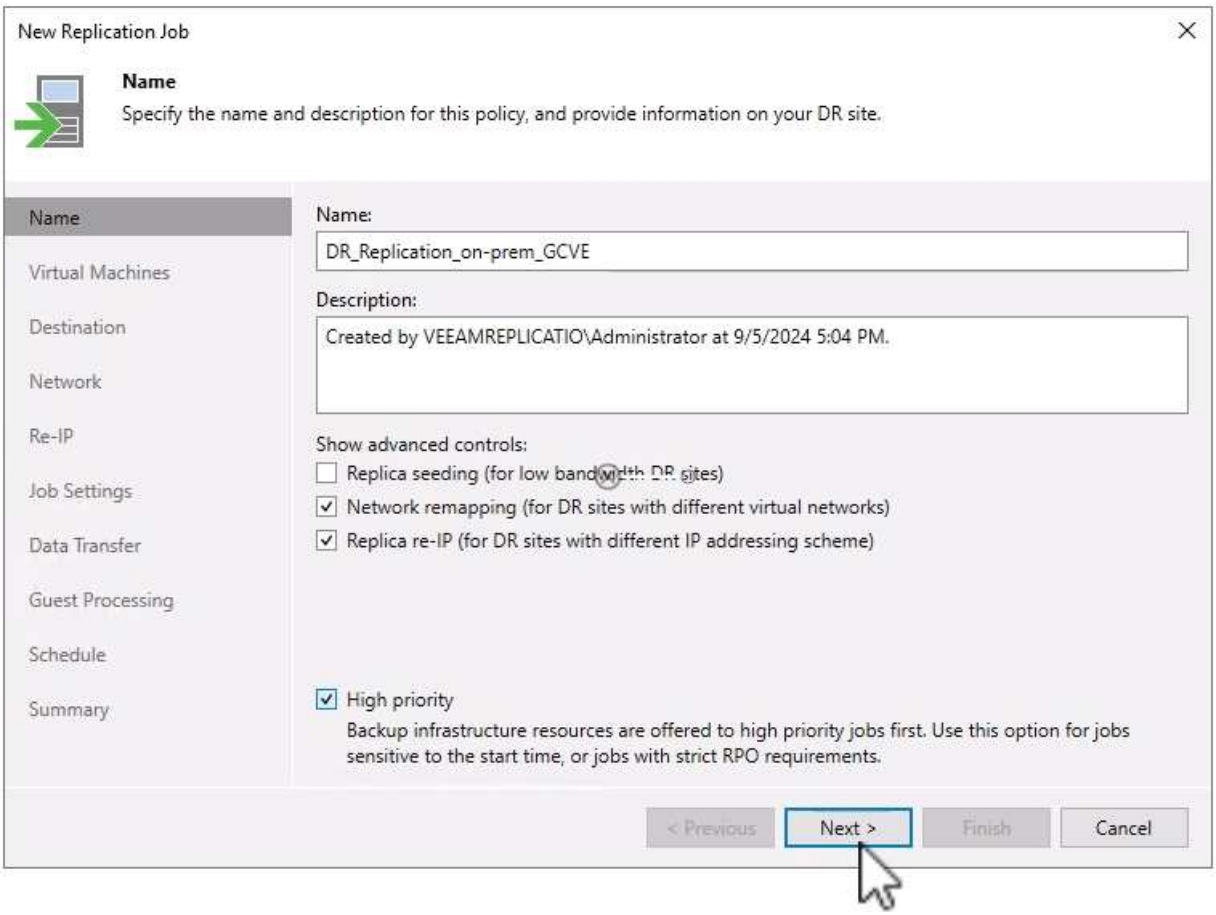
Veeam Backup & Replication aprovecha las funcionalidades Snapshot de VMware vSphere durante la replicación, Veeam Backup & Replication solicita a VMware vSphere para crear una snapshot de máquina virtual. La snapshot de la máquina virtual es la copia de un momento específico de una máquina virtual que incluye discos virtuales, estado del sistema, configuración y metadatos. Veeam Backup & Replication utiliza la snapshot como fuente de datos para la replicación.

Para replicar equipos virtuales, complete los siguientes pasos:

1. Abra Veeam Backup & Replication Console.
2. En la pestaña **Inicio**, haga clic en **Trabajo de replicación > Máquina virtual…**

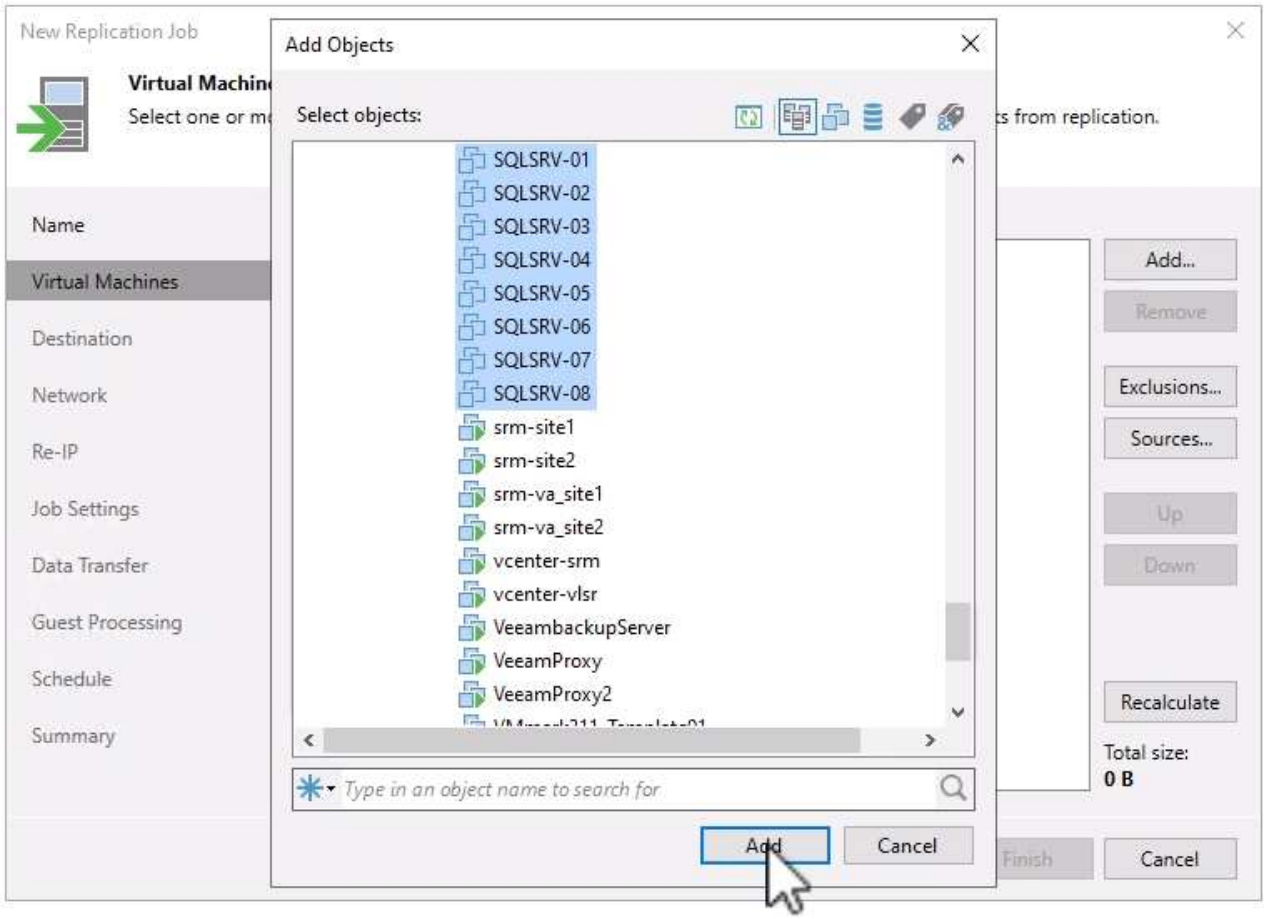


3. En la página **Name** del asistente **New Replication Job**, especifique un nombre de trabajo y seleccione las casillas de control avanzadas apropiadas.
   - Active la casilla de verificación Replica seeding si la conectividad entre las instalaciones y GCP tiene ancho de banda restringido.
   - Active la casilla de verificación Reasignación de red (para sitios SDDC de GCVE con redes diferentes) si los segmentos de la SDDC de GCVE no coinciden con los de las redes del sitio local.
   - Active la casilla de verificación Replica Re-IP (para sitios DR con un esquema de direcciones IP diferente) si el esquema de direcciones IP en el sitio de producción local difiere del esquema en el sitio de GCVE de destino.

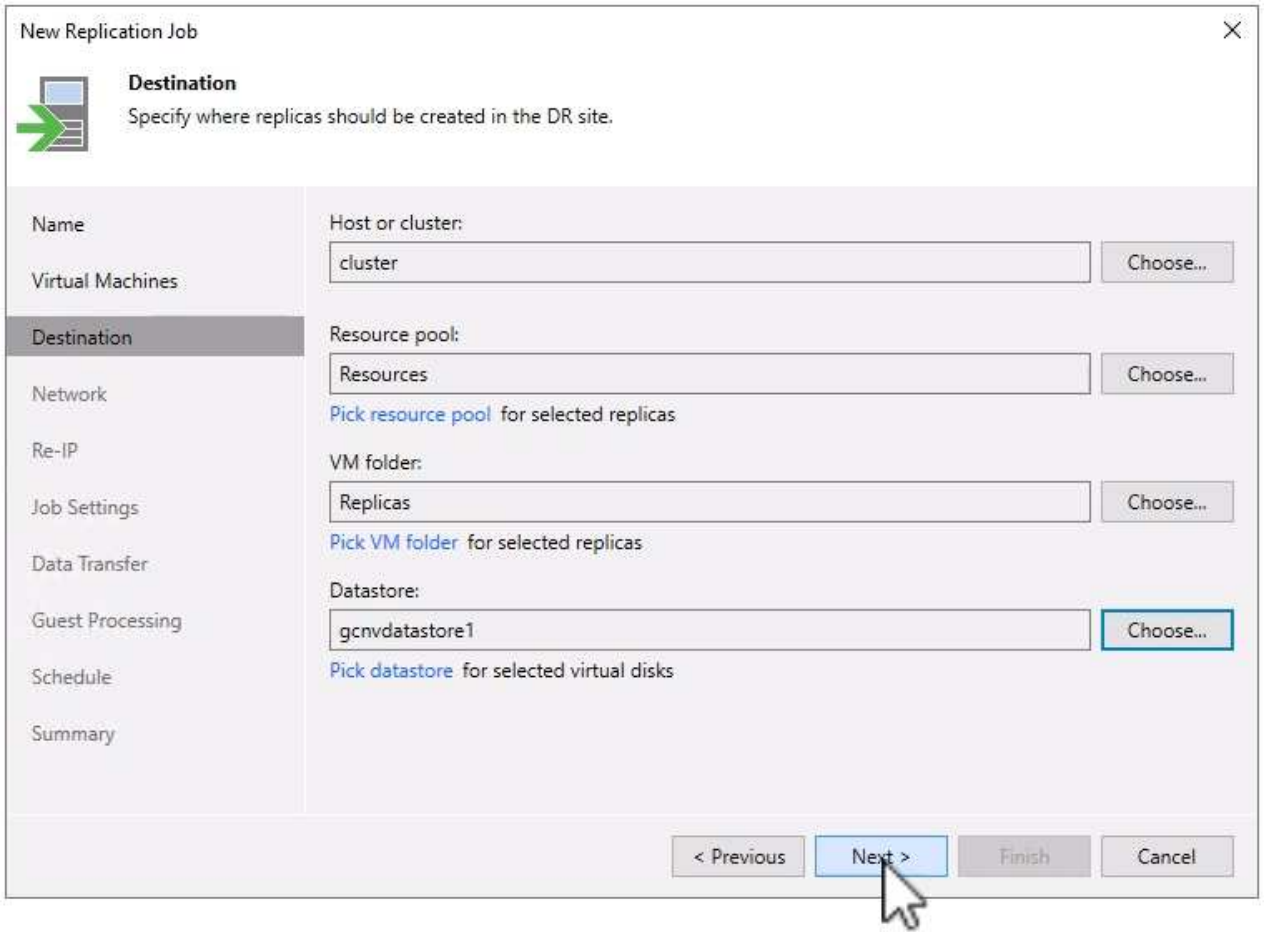


4. En la página **Virtual Machines**, seleccione las máquinas virtuales que se van a replicar en el almacén de datos de NetApp Volumes conectado a un SDDC de GCVE. Haga clic en **Agregar**, luego en la ventana **Agregar Objeto** seleccione las VM o contenedores de VM necesarios y haga clic en **Agregar**. Haga clic en **Siguiente**.

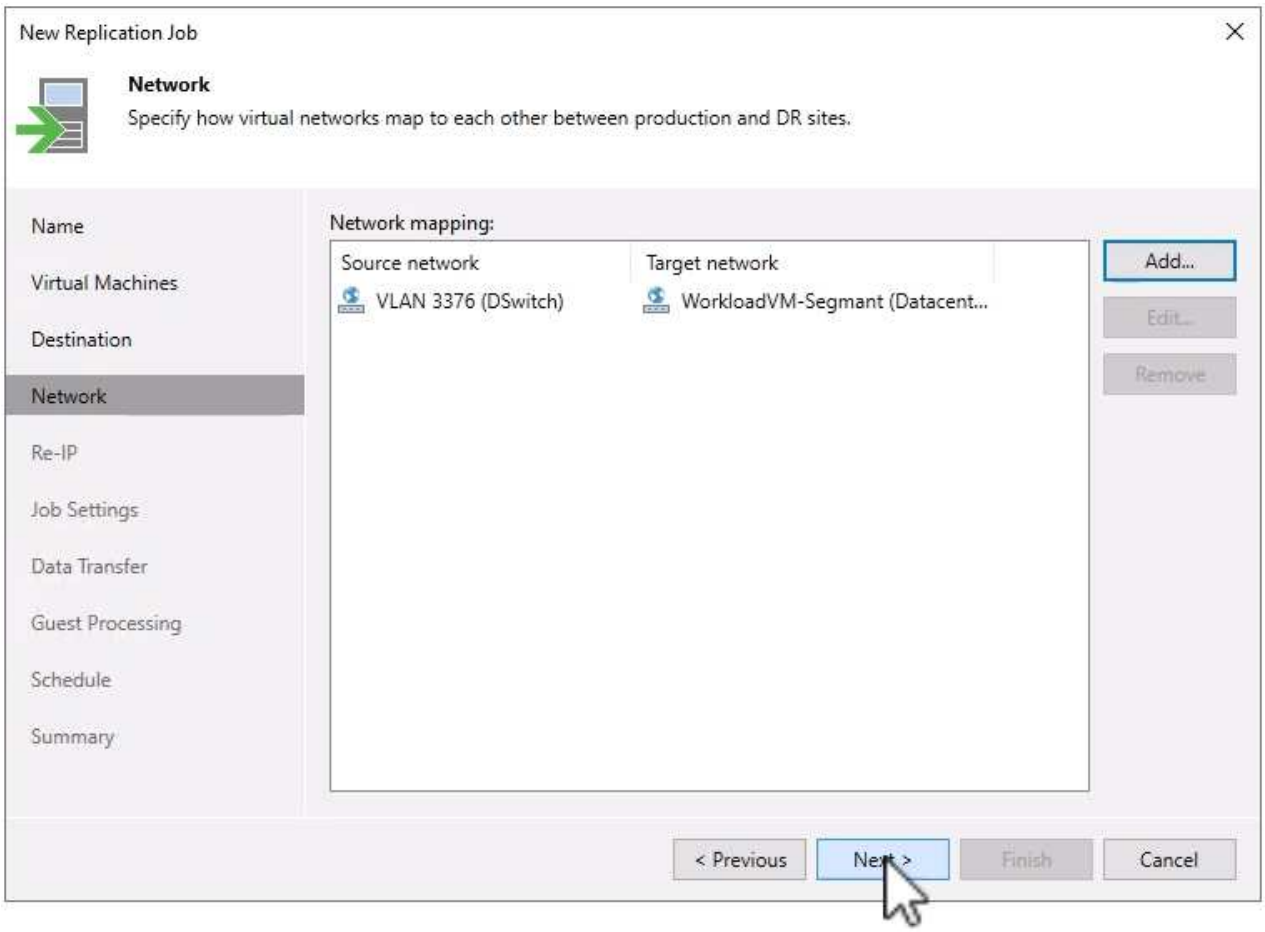
> ⓘ Las máquinas virtuales se pueden colocar en vSAN para llenar la capacidad de almacenes de datos vSAN disponible. En un clúster piloto ligero, la capacidad utilizable de un clúster vSAN de 3 nodos será limitada. El resto de datos puede colocarse fácilmente en almacenes de datos de Google Cloud NetApp Volumes para que las máquinas virtuales se puedan recuperar, y el clúster más adelante se pueda expandir para cumplir los requisitos de CPU/mem.



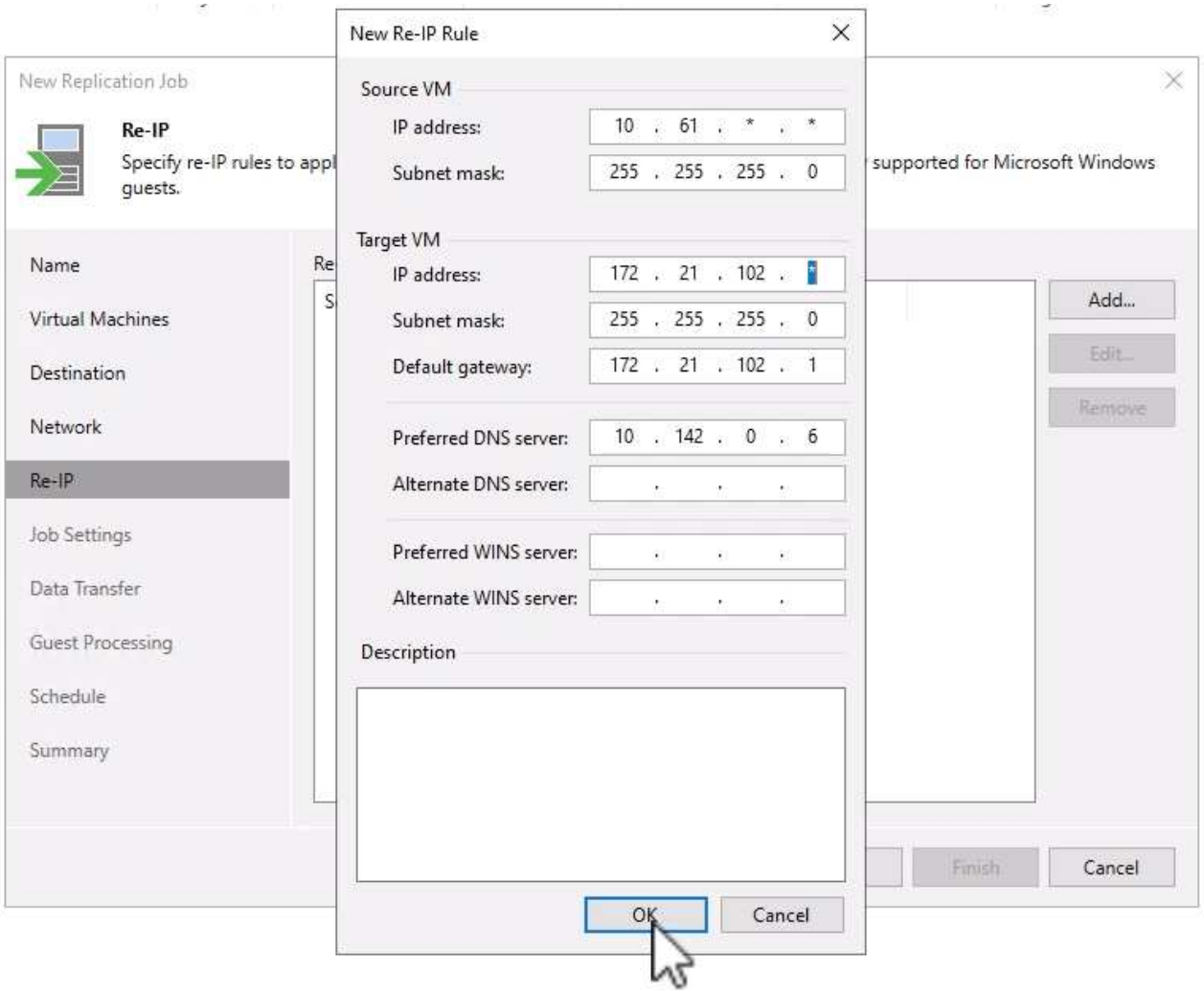
5. En la página **Destination**, seleccione el destino como cluster/hosts de SDDC de GCVE y el conjunto de recursos adecuado, la carpeta de VM y el almacén de datos de volúmenes de NetApp para las réplicas de VM. Haga clic en **Siguiente** para continuar.



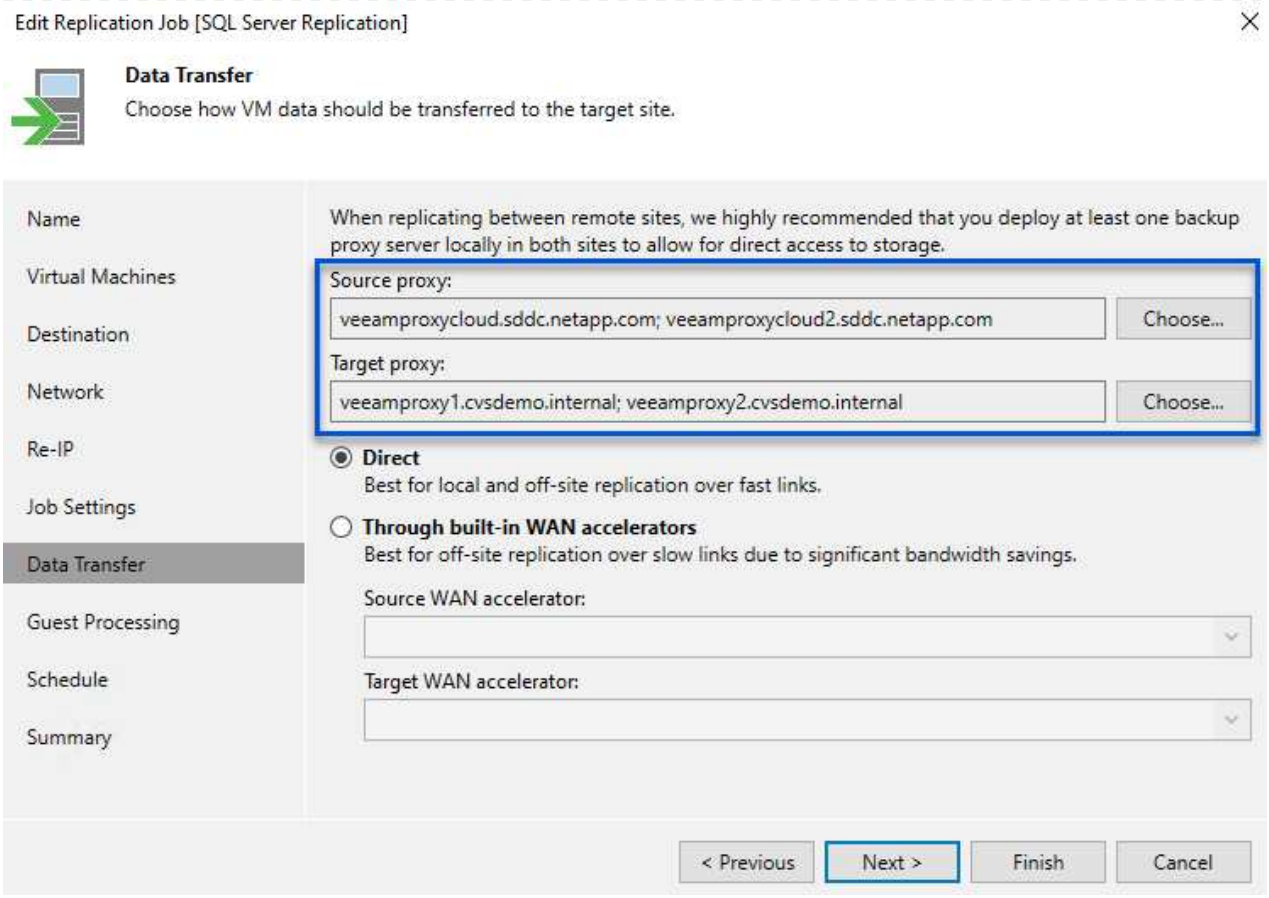
6. En la página **Red**, cree la asignación entre las redes virtuales de origen y de destino según sea necesario. Haga clic en **Siguiente** para continuar.



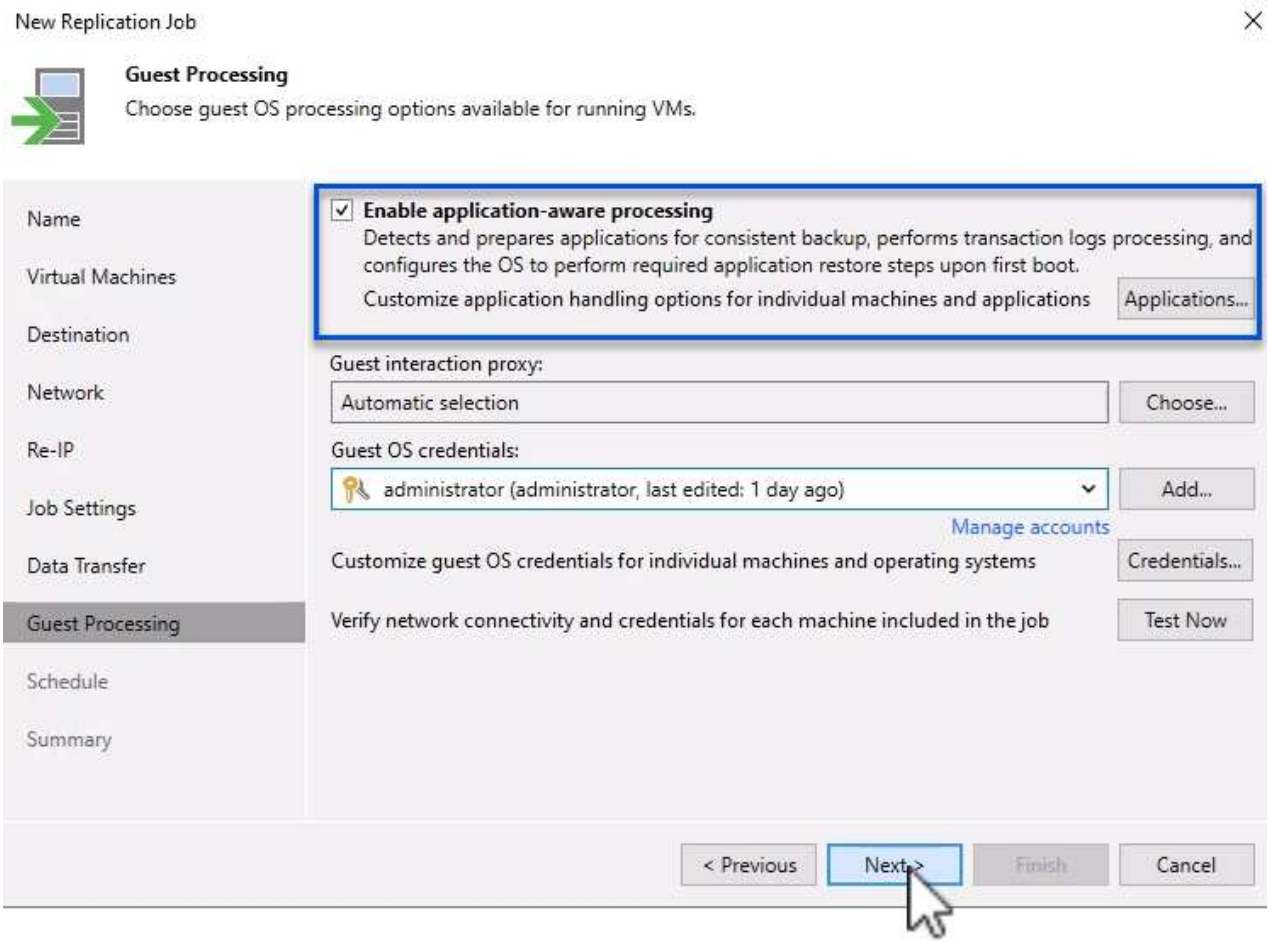
7. En la página **RE-IP**, haga clic en el botón **Add…** para agregar una nueva regla de RE-ip. Rellene los rangos de ip de la VM de origen y de destino para especificar la red que se aplicará a las VM de origen en caso de una conmutación por error. Utilice asteriscos para especificar un rango de direcciones indicado para ese octeto. Haga clic en **Siguiente** para continuar.



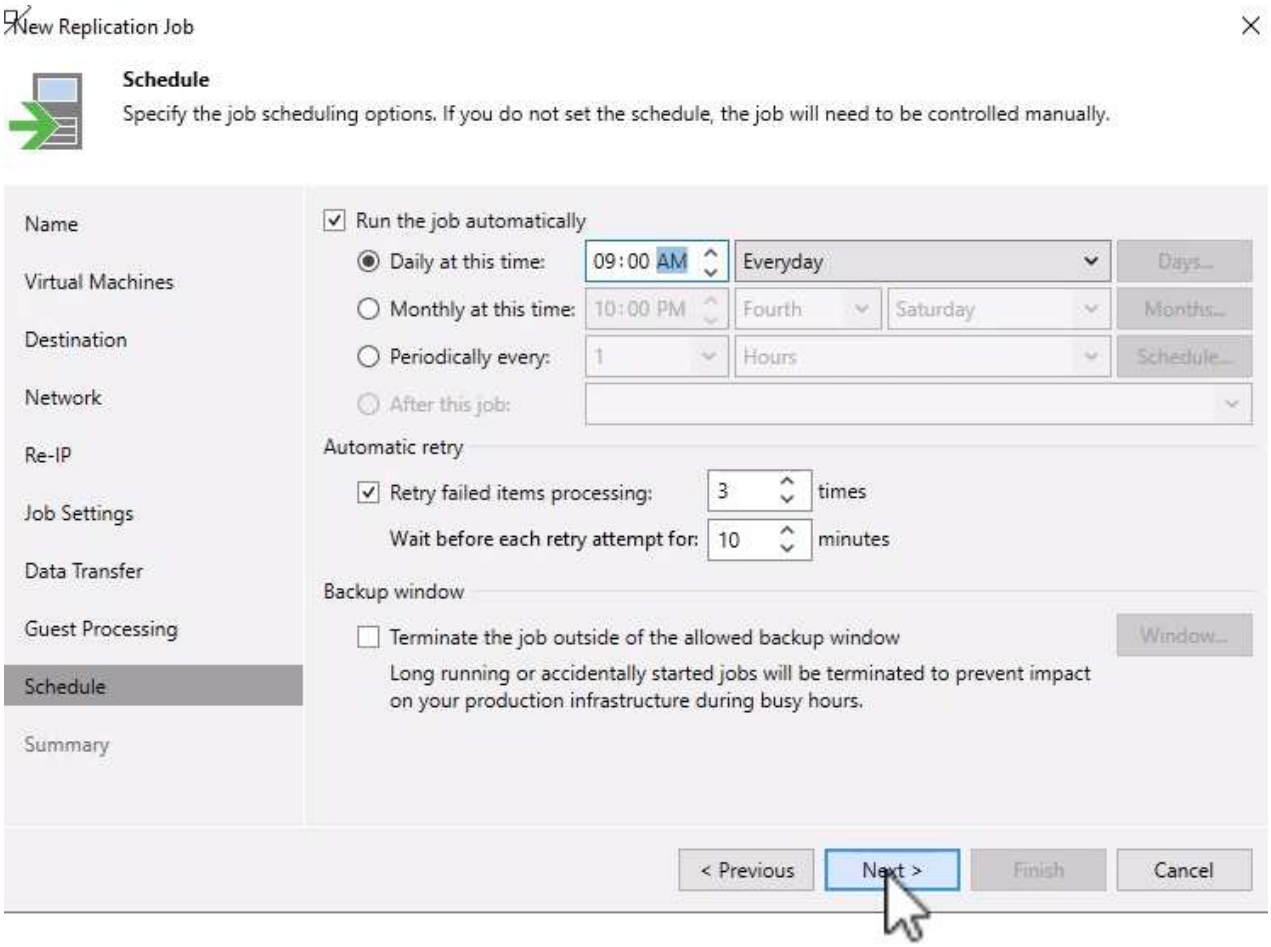
8. En la página **Configuración de trabajo**, especifique el repositorio de copia de seguridad que almacenará metadatos para las réplicas de VM, la política de retención y seleccione el botón en la parte inferior para el botón **Avanzado…** en la parte inferior para la configuración adicional del trabajo. Haga clic en **Siguiente** para continuar.
9. En **Data Transfer**, seleccione los servidores proxy que residen en los sitios de origen y destino, y mantenga seleccionada la opción Direct. Los aceleradores WAN también se pueden seleccionar aquí, si están configurados. Haga clic en **Siguiente** para continuar.



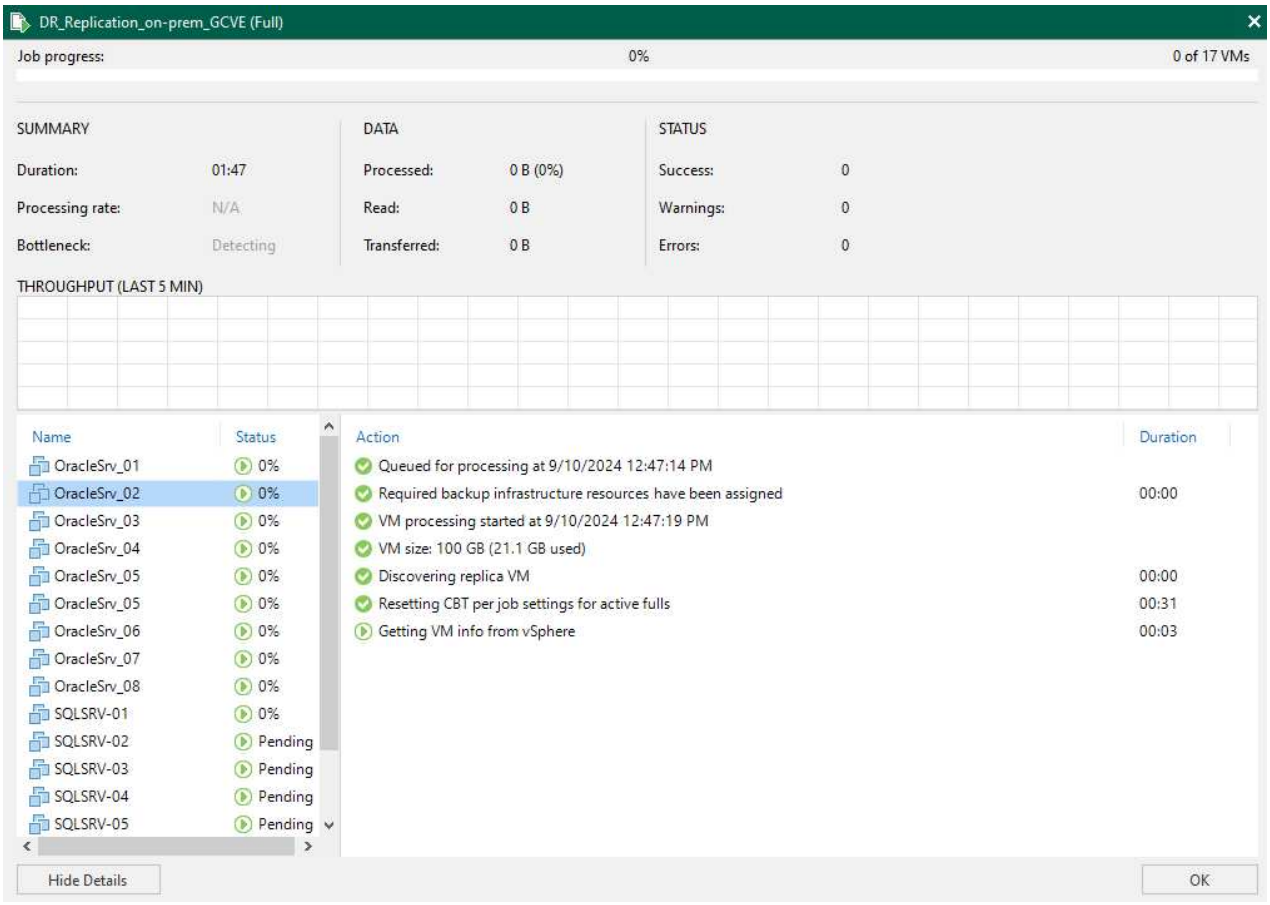
10. En la página **Guest Processing**, marque la casilla **Enable application-aware processing** según sea necesario y seleccione **Guest OS credentials**. Haga clic en **Siguiente** para continuar.



11. En la página **Schedule**, defina las horas y la frecuencia con la que se ejecutará el trabajo de replicación. Haga clic en **Siguiente** para continuar.



12. Por último, revise la configuración del trabajo en la página **Resumen**. Marque la casilla para **Ejecutar el trabajo cuando haga clic en Finalizar**, y haga clic en **Finalizar** para completar la creación del trabajo de replicación.
13. Una vez ejecutado, el trabajo de replicación se puede ver en la ventana de estado del trabajo.



Para obtener más información sobre la replicación de Veeam, consulte "Funcionamiento de la replicación"

Cree un plan de recuperación tras fallos

Una vez finalizada la replicación inicial o la propagación, cree el plan de conmutación por error. El plan de conmutación por error ayuda a realizar la conmutación por error de los equipos virtuales dependientes uno por uno o como grupo automáticamente. El plan de conmutación por error es el plan del orden en el que se procesan los equipos virtuales, incluidos los retrasos en el inicio. El plan de conmutación por error también ayuda a garantizar que los equipos virtuales dependientes cruciales ya se estén ejecutando.

Después de completar la replicación inicial o la propagación, cree un plan de conmutación por error. Este plan sirve como guía estratégica para orquestar la conmutación por error de máquinas virtuales dependientes, ya sea de forma individual o en grupo. Define el orden de procesamiento de los equipos virtuales, incorpora los retrasos de arranque necesarios y garantiza que los equipos virtuales dependientes de la importancia crítica funcionen antes que los demás. Al implementar un plan de recuperación tras fallos bien estructurado, las organizaciones pueden agilizar su proceso de recuperación ante desastres, lo que minimiza el tiempo de inactividad y mantiene la integridad de los sistemas interdependientes durante un evento de recuperación tras fallos.

Al crear el plan, Veeam Backup & Replication identifica y utiliza automáticamente los puntos de restauración más recientes para iniciar las réplicas de VM.

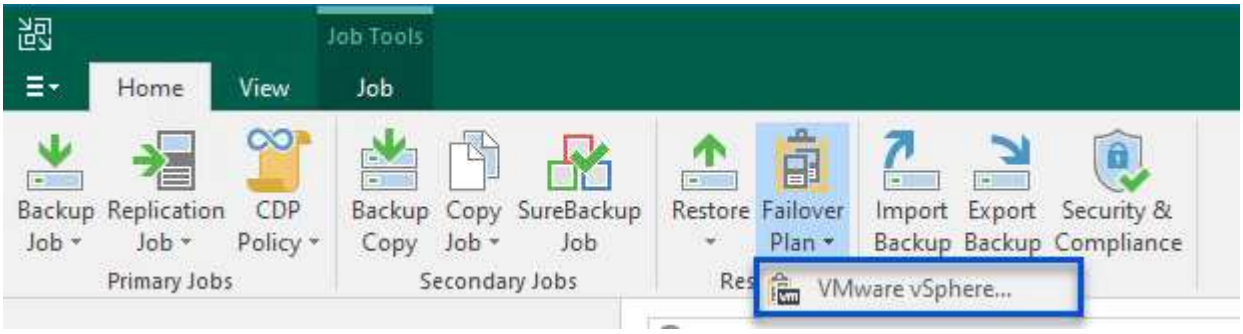
> El plan de conmutación por error solo se puede crear una vez que se haya completado la replicación inicial y las réplicas de las máquinas virtuales estén en estado Listo.

> El número máximo de equipos virtuales que se pueden iniciar simultáneamente cuando se ejecuta un plan de conmutación al nodo de respaldo es de 10.

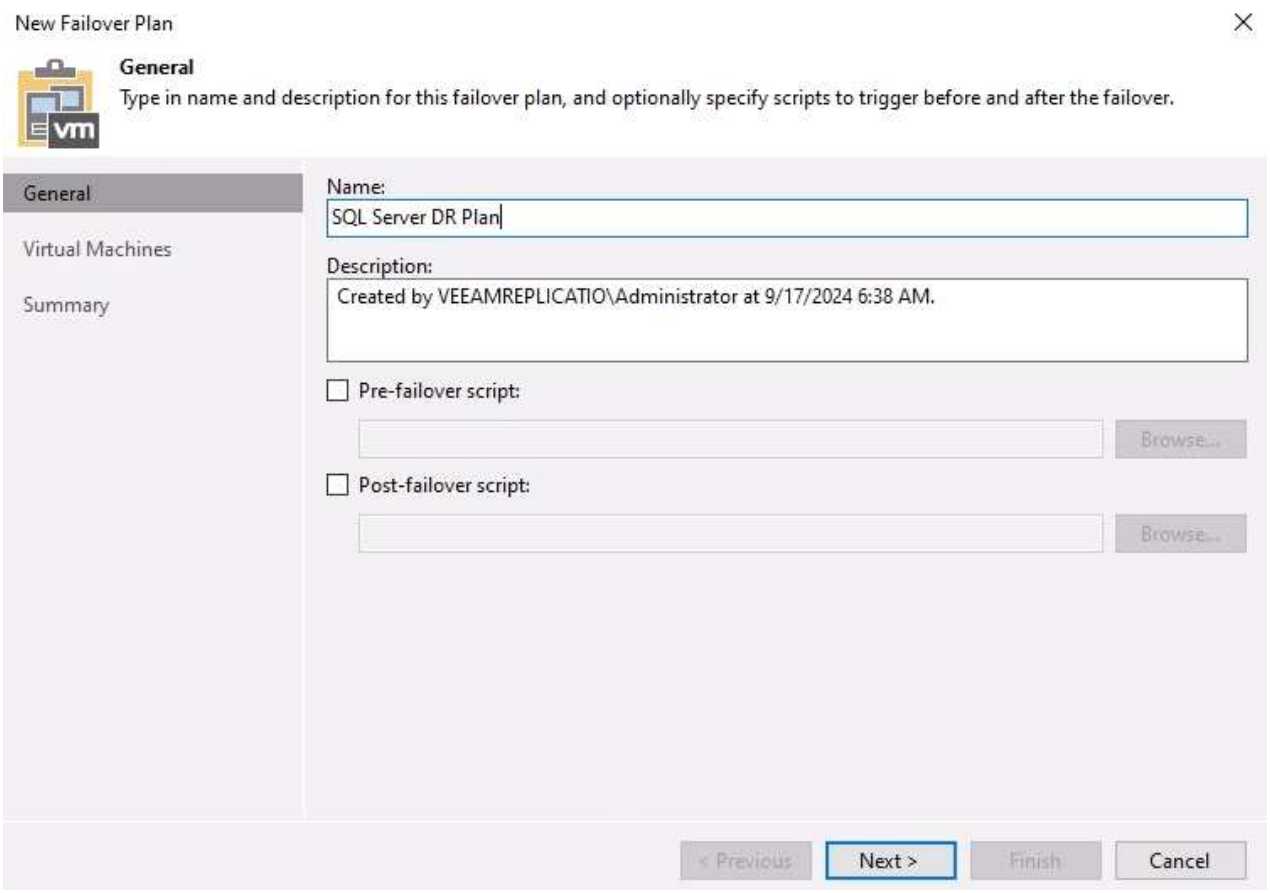
> Durante el proceso de conmutación al nodo de respaldo, los equipos virtuales de origen no se apagarán.

Para crear el **Failover Plan**, complete los siguientes pasos:

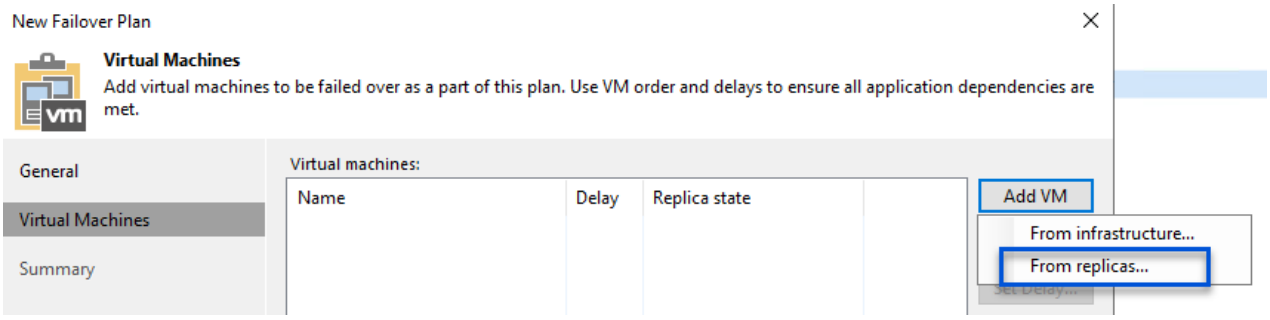
1. En la vista **Home**, haga clic en el botón **Failover Plan** en la sección **Restore**. En el menú desplegable, seleccione **VMware vSphere…**

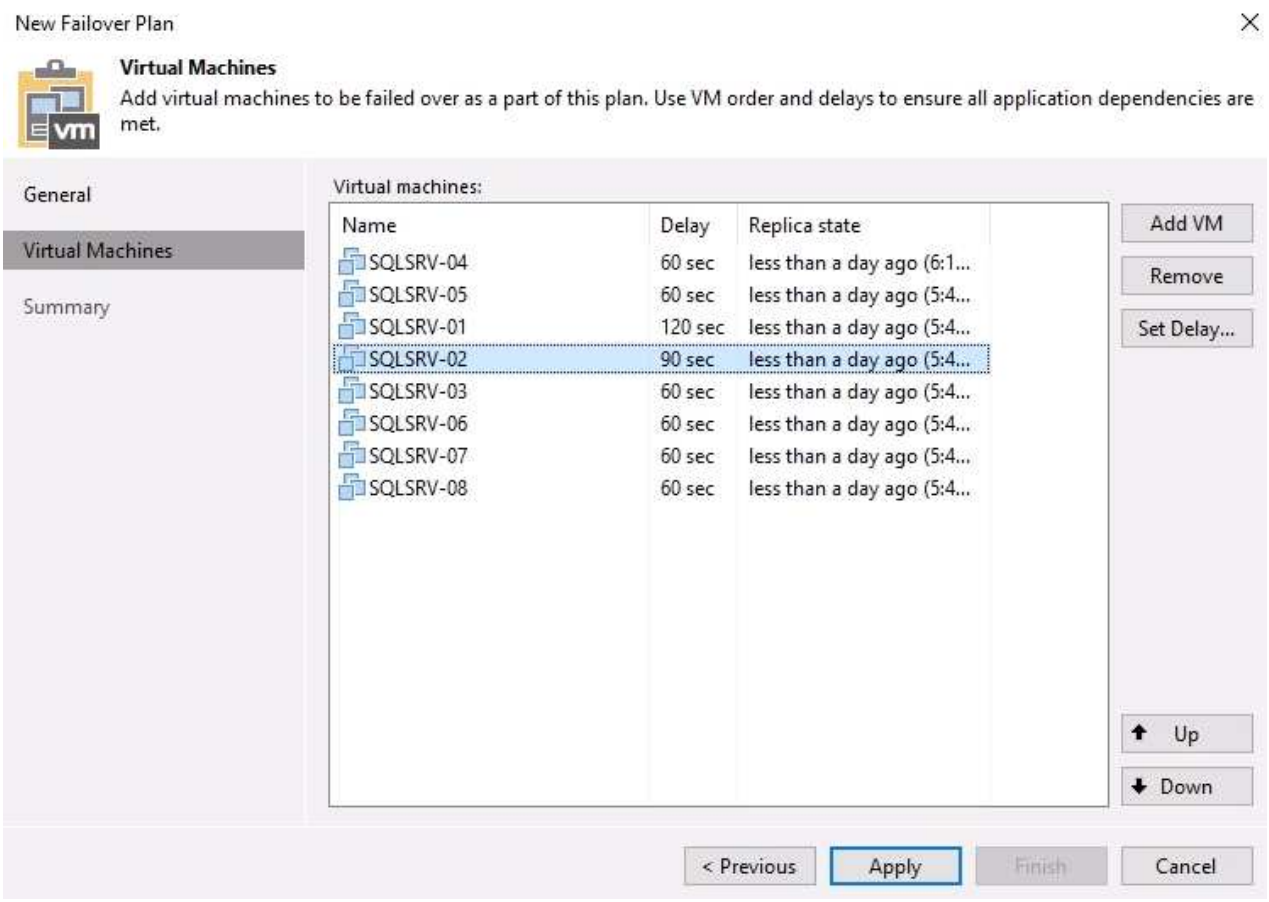


2. En la página **General** del asistente **New Failover Plan**, proporcione un nombre y una descripción al plan. Los scripts previos y posteriores a la conmutación al nodo de respaldo se pueden agregar según sea necesario. Por ejemplo, ejecute un script para cerrar los equipos virtuales antes de iniciar los equipos virtuales replicados.



3. En la página **Máquinas virtuales**, haz clic en el botón para **Agregar VM** y selecciona **De las réplicas…**. Seleccione las máquinas virtuales que formarán parte del plan de conmutación al nodo de respaldo y, a continuación, modifique el orden de arranque de las máquinas virtuales y los retrasos de arranque necesarios para cumplir con las dependencias de las aplicaciones.





Haga clic en **Aplicar** para continuar.

4. Finalmente revise toda la configuración del plan de failover y haga clic en **Finish** para crear el plan de failover.

Para obtener más información sobre la creación de trabajos de replicación, consulte "Creación de trabajos de replicación".

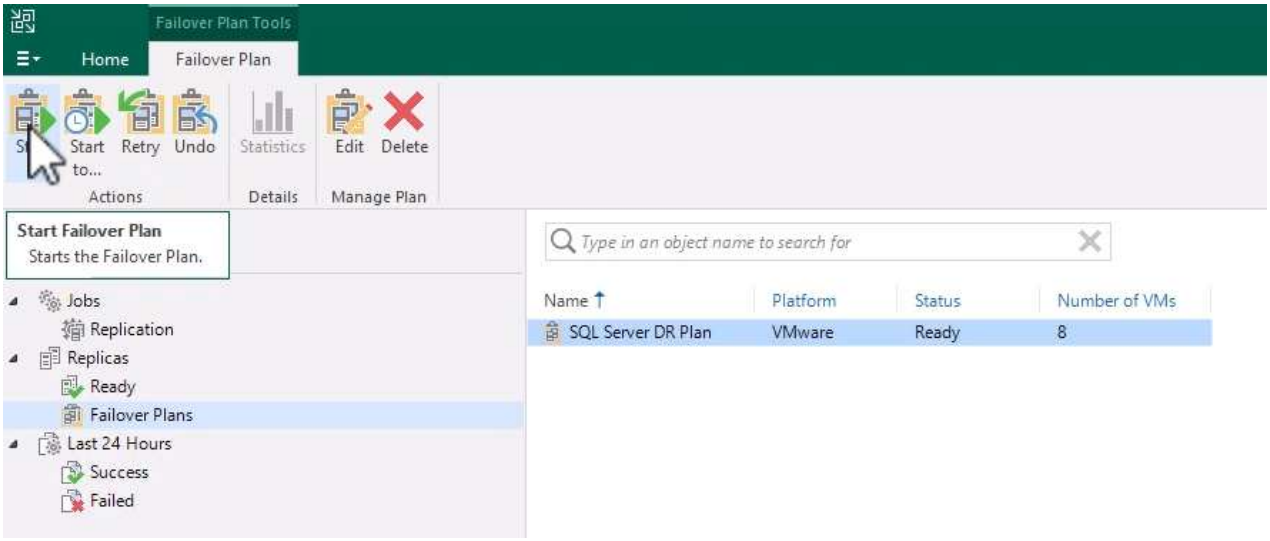
Ejecute el plan de failover

En el caso de la conmutación por error, la máquina virtual de origen del sitio de producción cambia a la réplica en el sitio de recuperación de desastres. Como parte del proceso, Veeam Backup & Replication restaura la réplica de la máquina virtual al punto de restauración requerido y transfiere todas las actividades de I/O del equipo virtual de origen a su réplica. Las réplicas no solo sirven para desastres reales, sino también para simular simulacros de recuperación ante desastres. En la simulación de recuperación tras fallos, la máquina virtual de origen sigue ejecutándose. Una vez finalizadas las pruebas necesarias, la conmutación por error puede deshacerse y devolver las operaciones a la normalidad.

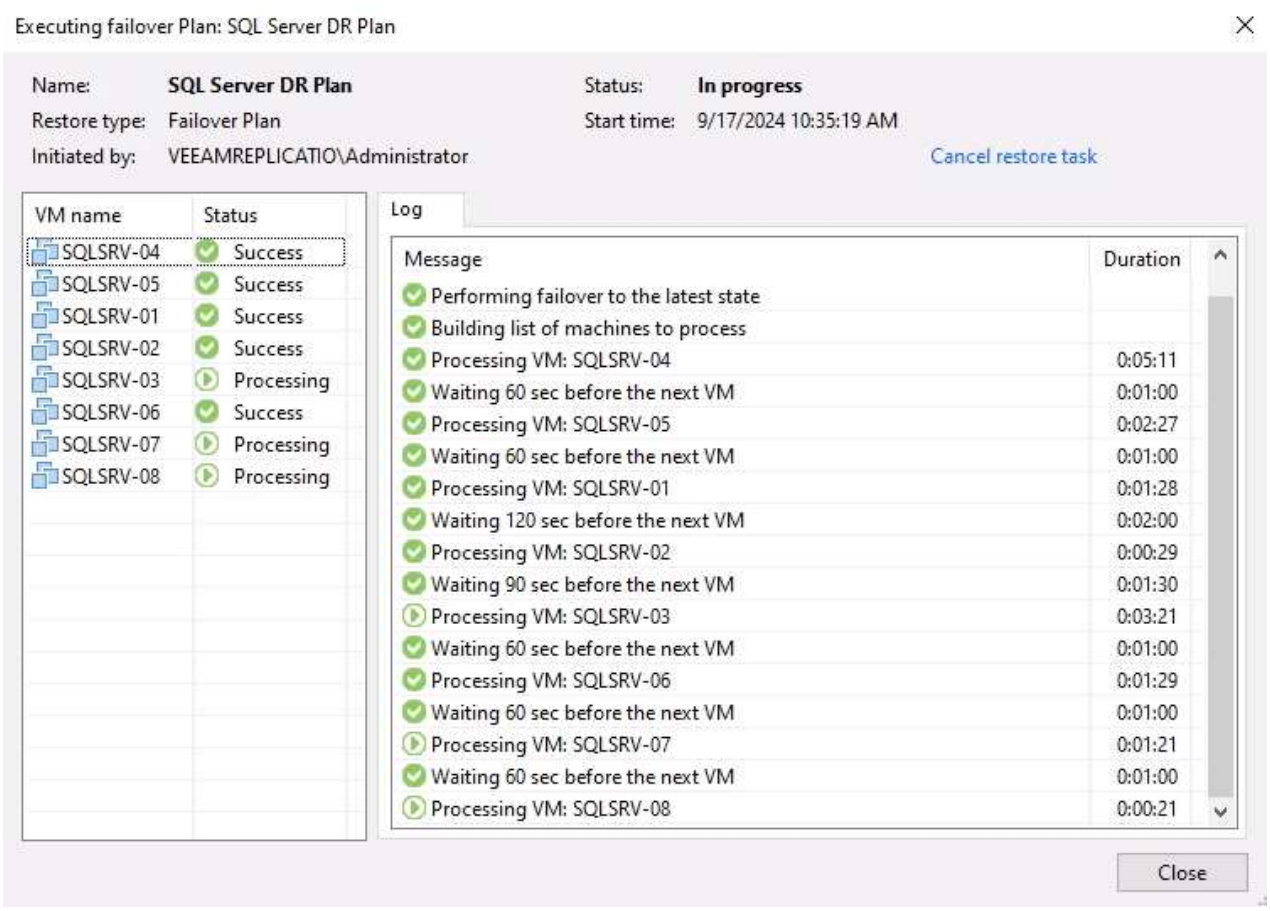
Asegúrese de que la segmentación de la red está en su lugar para evitar conflictos de IP durante la conmutación por error.

Realice los siguientes pasos para iniciar el plan de failover:

1. Para empezar, en la vista **Home**, haz clic en **replicas > Failover Plans** en el menú de la izquierda y luego en el botón **Start**. Alternativamente, el botón **Start To…** se puede utilizar para conmutar por error a un punto de restauración anterior.



2. Supervise el progreso de la conmutación por error en la ventana **Ejecución del plan de conmutación por error**.



Veeam Backup & Replication detiene todas las actividades de replicación de la máquina virtual de origen hasta que su réplica vuelve al estado Ready.

Para obtener información detallada sobre los planes de conmutación por error, consulte "Planes de conmutación al respaldo".

Conmutación tras recuperación en el sitio de producción

La realización de una recuperación tras fallos se considera un paso intermedio y debe finalizarse de acuerdo con los requisitos. Las opciones incluyen las siguientes:

- **Failback to Production** - Vuelva a la VM original y sincronice todas las modificaciones realizadas durante el período activo de la réplica de vuelta a la VM de origen.

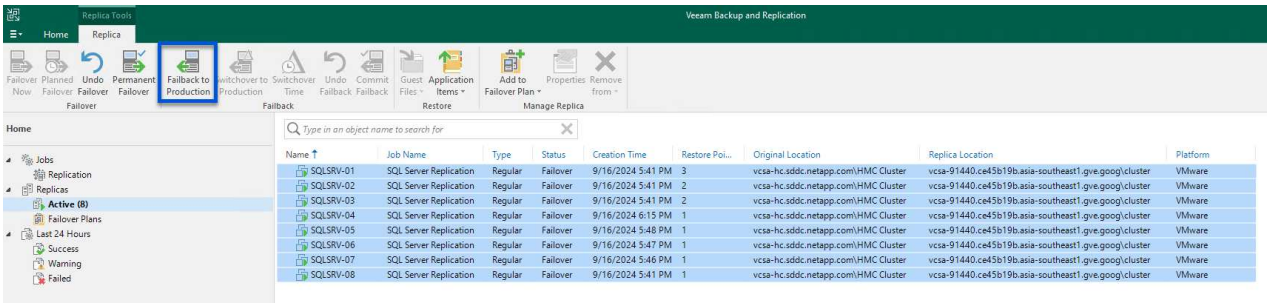
> ⓘ Durante la conmutación de retorno tras recuperación, los cambios se transfieren, pero no se aplican de inmediato. Seleccione **COMMIT failback** una vez que se verifique la funcionalidad de la VM original. Alternativamente, elija **Deshacer failback** para revertir a la réplica de VM si la VM original muestra un comportamiento inesperado.

- **Deshacer failover** - Revertir a la VM original, descartando todos los cambios realizados en la réplica de VM durante su período operativo.
- **Failover permanente** - Cambie permanentemente de la VM original a su réplica, estableciendo la réplica como la nueva VM primaria para las operaciones en curso.

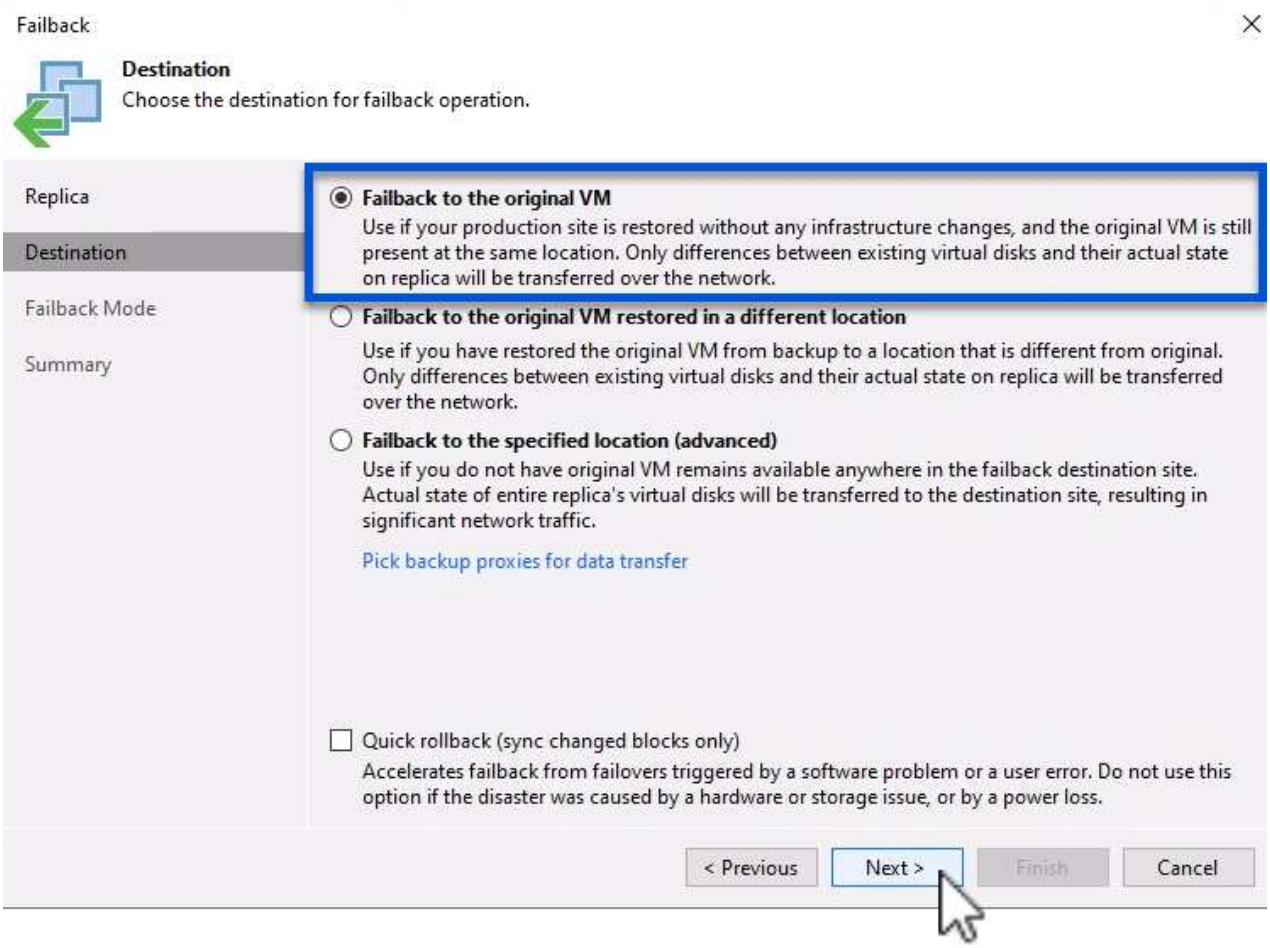
En este escenario, se ha seleccionado la opción «failback to production».

Lleve a cabo los siguientes pasos para realizar una conmutación por recuperación en el sitio de producción:

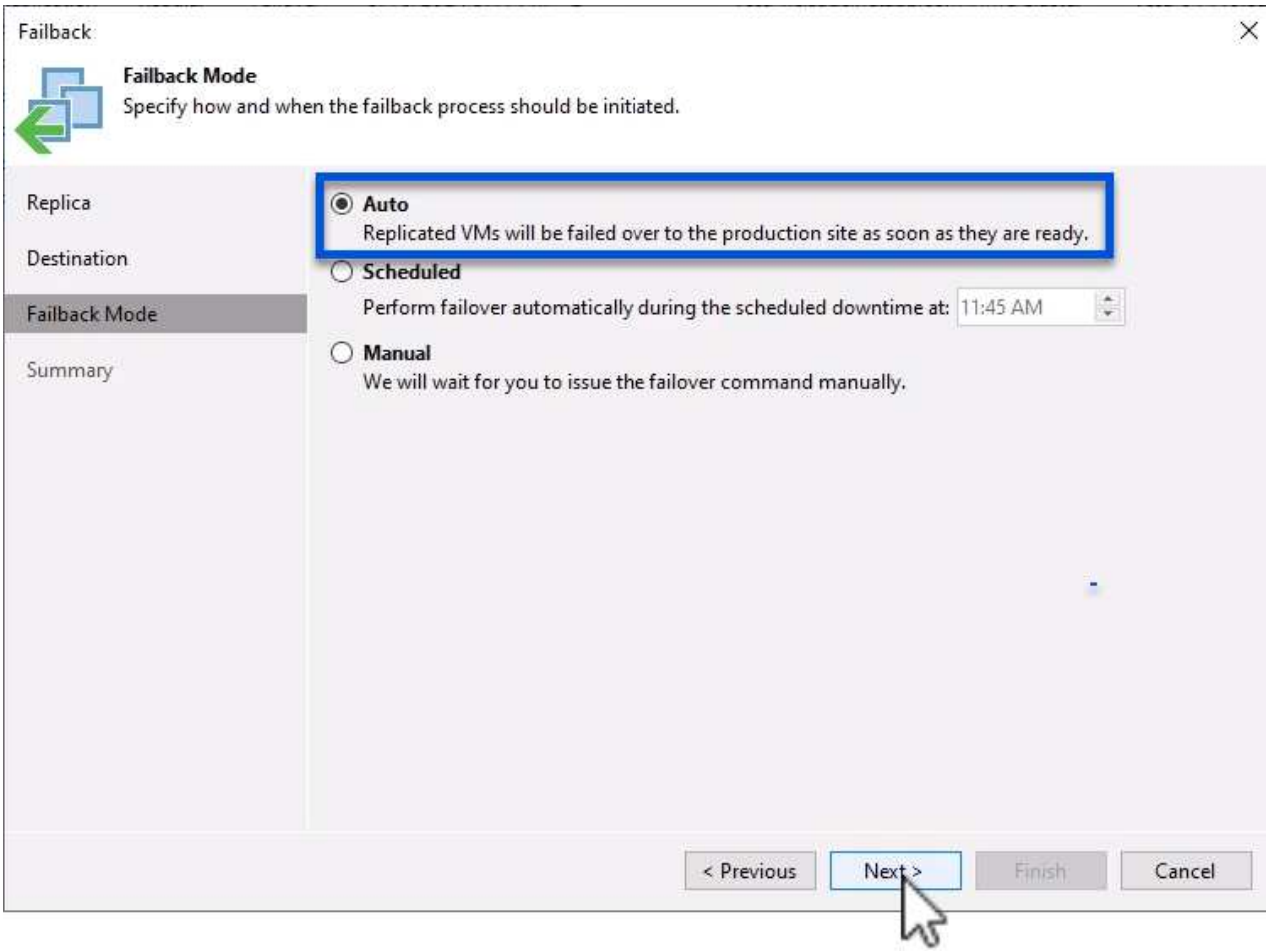
1. En la vista **Home**, haz clic en **replicas > Active** en el menú de la izquierda. Seleccione las VMs que se incluirán y haga clic en el botón **failback to production** en el menú superior.



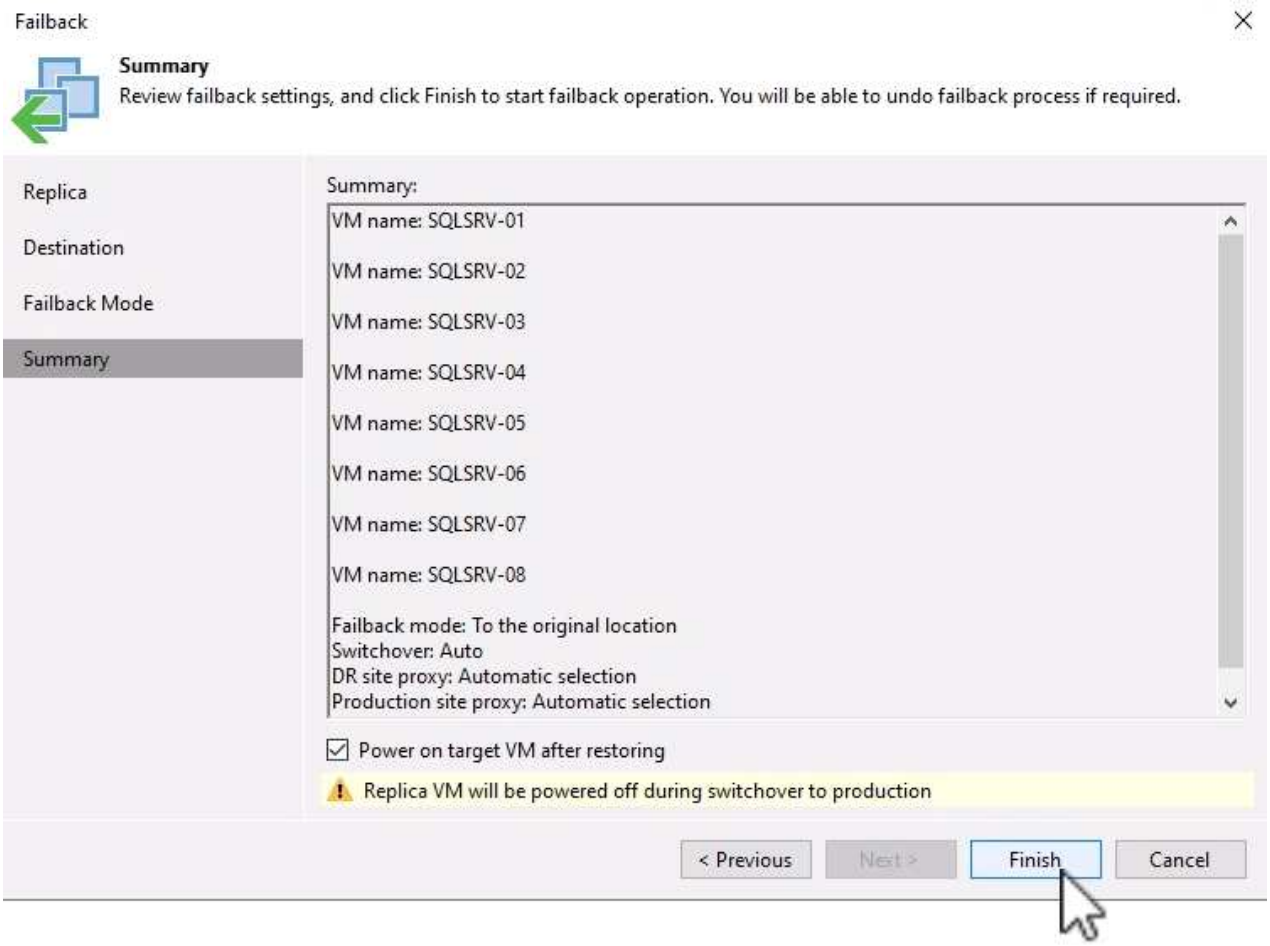
2. En la página **Replica** del asistente **failback**, seleccione las réplicas que desea incluir en el trabajo de failback.
3. En la página **Destino**, seleccione **failback to the original VM** y haga clic en **Siguiente** para continuar.



4. En la página **failback Mode**, selecciona **Auto** para iniciar el failback tan pronto como sea posible.

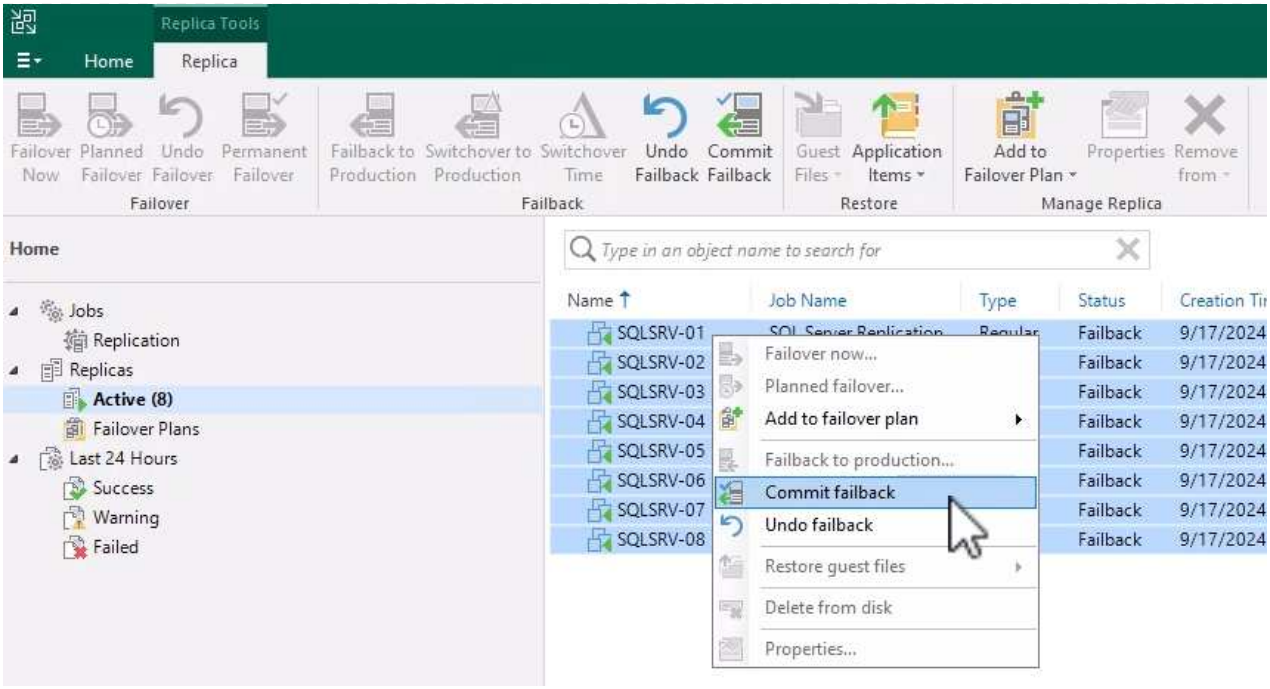


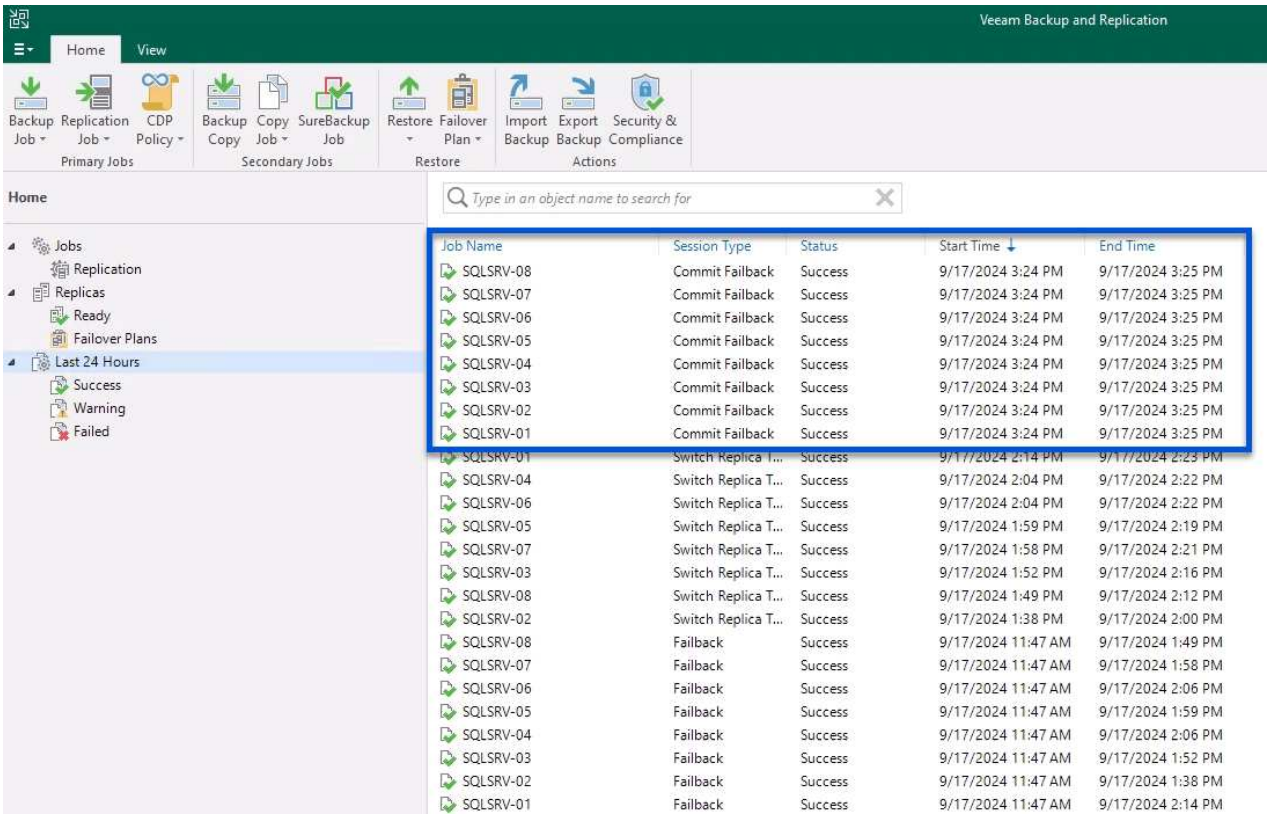
5. En la página **Resumen**, elija si desea **Encender en la VM de destino después de la restauración** y luego haga clic en Finalizar para iniciar el trabajo de conmutación por error.



La confirmación de failback finaliza la operación de failback, confirmando la integración correcta de los cambios en la VM de producción. Tras la asignación, Veeam Backup & Replication reanuda las actividades regulares de replicación para el equipo virtual de producción restaurado. Esto cambia el estado de la réplica restaurada de *failback* a *Ready*.

1. Para confirmar la conmutación por recuperación, navegue a **replicas > Active**, seleccione las VM que se van a confirmar, haga clic con el botón derecho y seleccione **commit failback**.





Una vez que la conmutación de retorno tras recuperación a producción se ha realizado correctamente, todas las máquinas virtuales se restauran al sitio de producción original.

Para obtener información detallada sobre el proceso de conmutación por recuperación, consulte la documentación de Veeam para "Conmutación al nodo de respaldo y conmutación de retorno tras recuperación para replicación".

Conclusión

La funcionalidad de almacén de datos de Google Cloud NetApp Volumes permite a Veeam y otras herramientas validadas de terceros ofrecer soluciones rentables de recuperación ante desastres. Al utilizar clústeres ligeros de Pilot en lugar de grandes clústeres dedicados para réplicas de VM, las organizaciones pueden reducir significativamente los gastos. Este enfoque permite estrategias de recuperación ante desastres personalizadas que aprovechan las soluciones de backup internas existentes para la recuperación ante desastres basada en el cloud, lo que elimina la necesidad de contar con más centros de datos en las instalaciones. En caso de desastre, la recuperación tras fallos puede iniciarse con un solo clic o configurarse para que se produzca automáticamente, lo que garantiza la continuidad del negocio con un tiempo de inactividad mínimo.

Para obtener más información sobre este proceso, puede seguir el vídeo detallado del tutorial.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=b2fb8597-c3fe-49e2-8a84-b1f10118db6d

Migrar cargas de trabajo en GCP / GCVE

Migre cargas de trabajo a Google Cloud NetApp Volumes datastore en Google Cloud VMware Engine mediante VMware HCX: Guía de inicio rápido

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.

Autores: Ingeniería de soluciones de NetApp

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

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

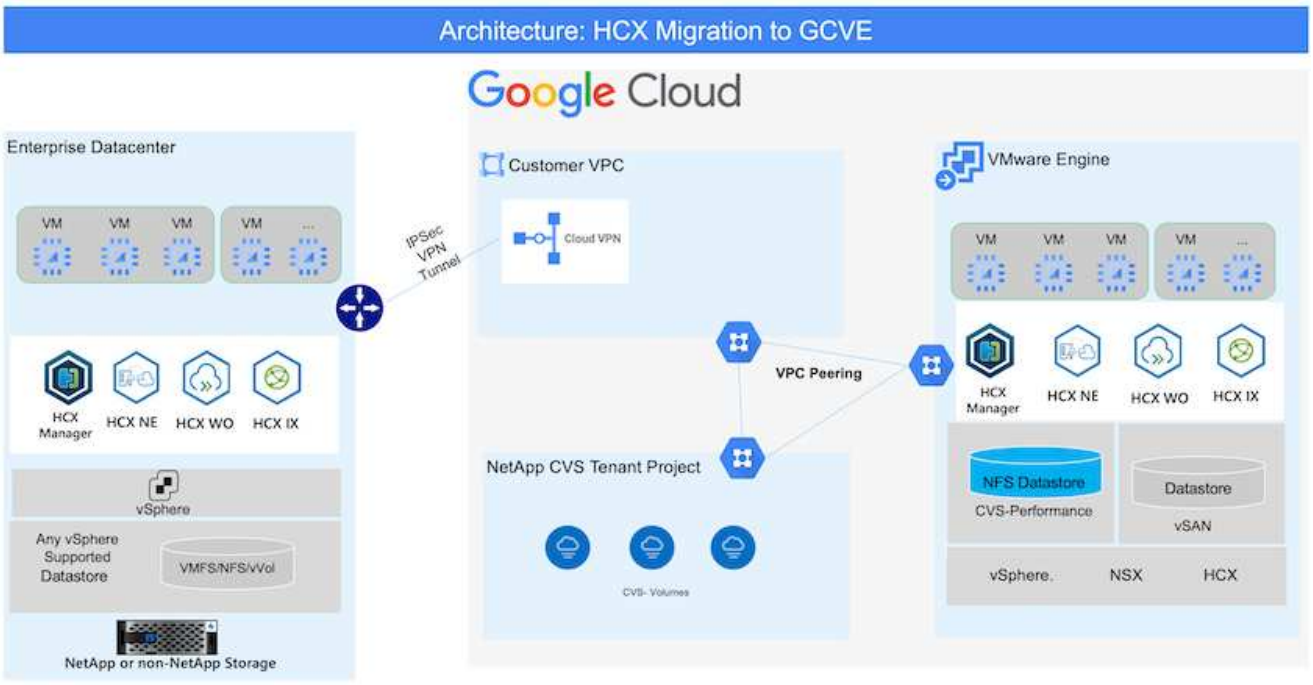
Antes de empezar, asegúrese de que se cumplan los siguientes requisitos previos. Para obtener más información, consulte este tema "enlace". Una vez que se hayan establecido los requisitos previos, incluida la conectividad, descargue la clave de licencia de HCX del portal Google Cloud VMware Engine. Después 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 más información sobre el uso de VMware HCX con Google, consulte "Enlace de VMware"

Puesta en marcha de la solución

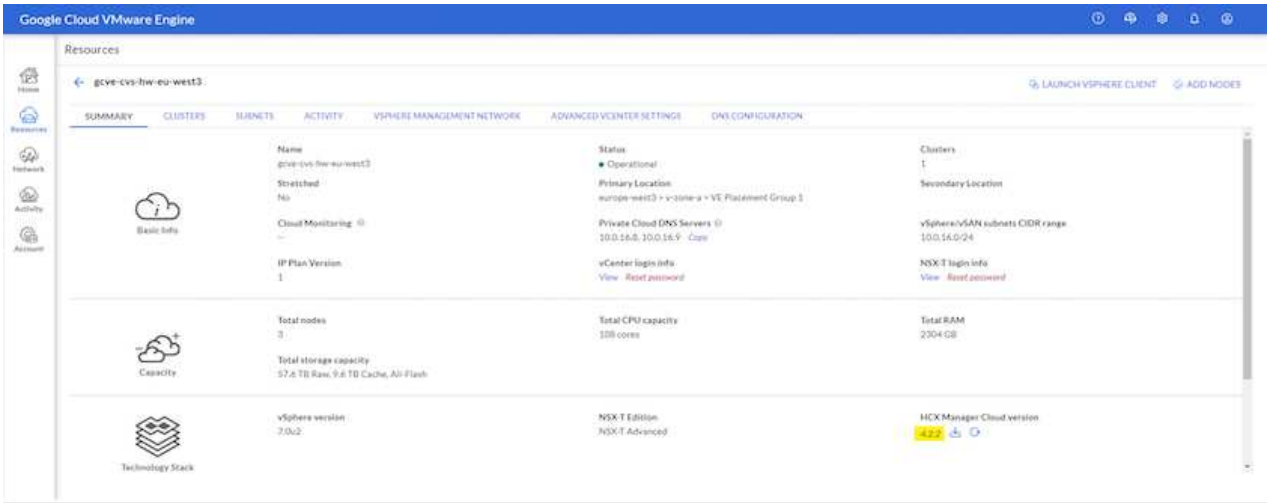
Siga la serie de pasos para completar la implementación de esta solución:

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

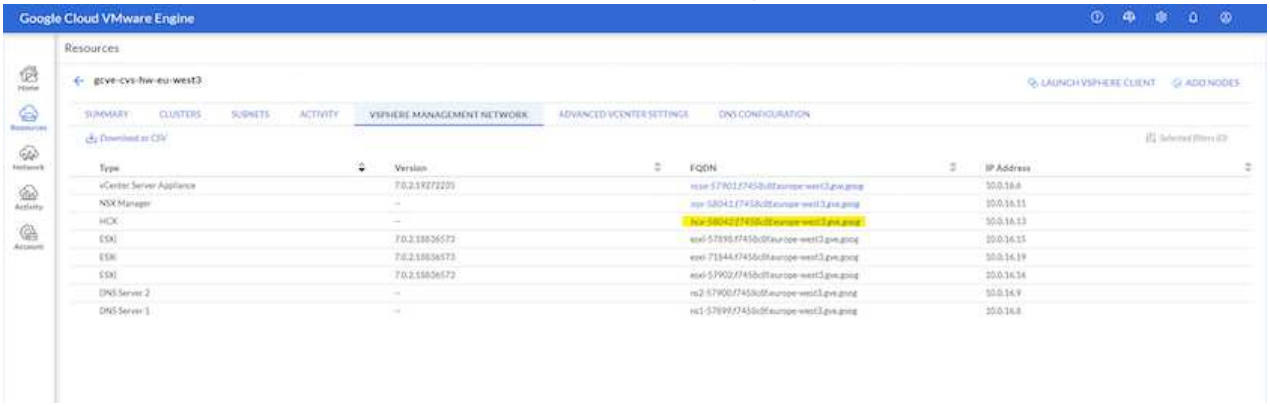
El componente DE HCX Cloud Manager se instala automáticamente a medida que aprovisiona el cloud privado con VMware Engine. Para preparar el emparejamiento de sitios, lleve a cabo los siguientes pasos:

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

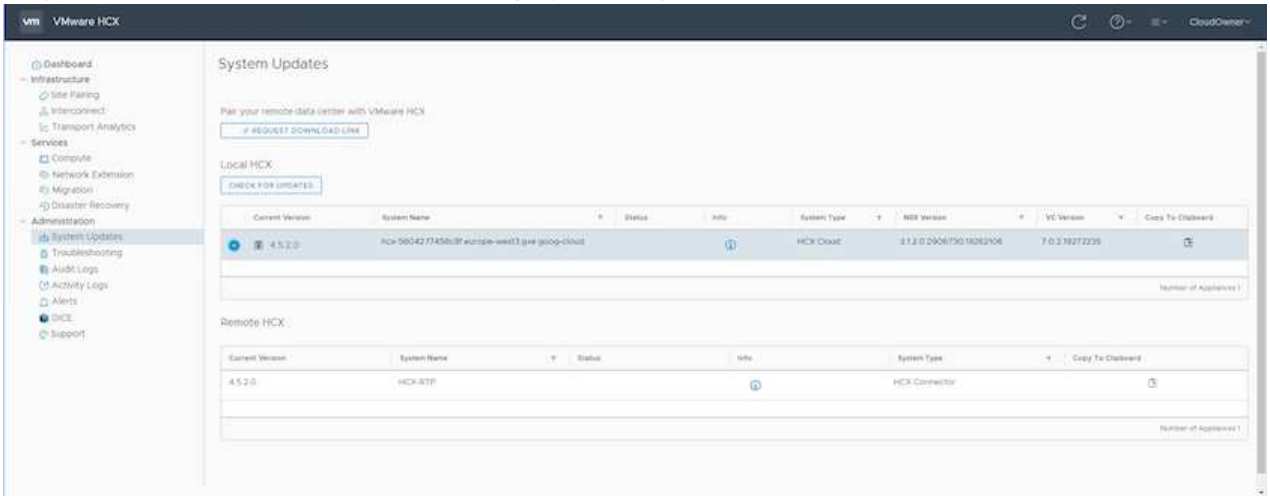
   Puede iniciar sesión en HCX Console haciendo clic en el enlace de la versión de HCX



   o haciendo 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.



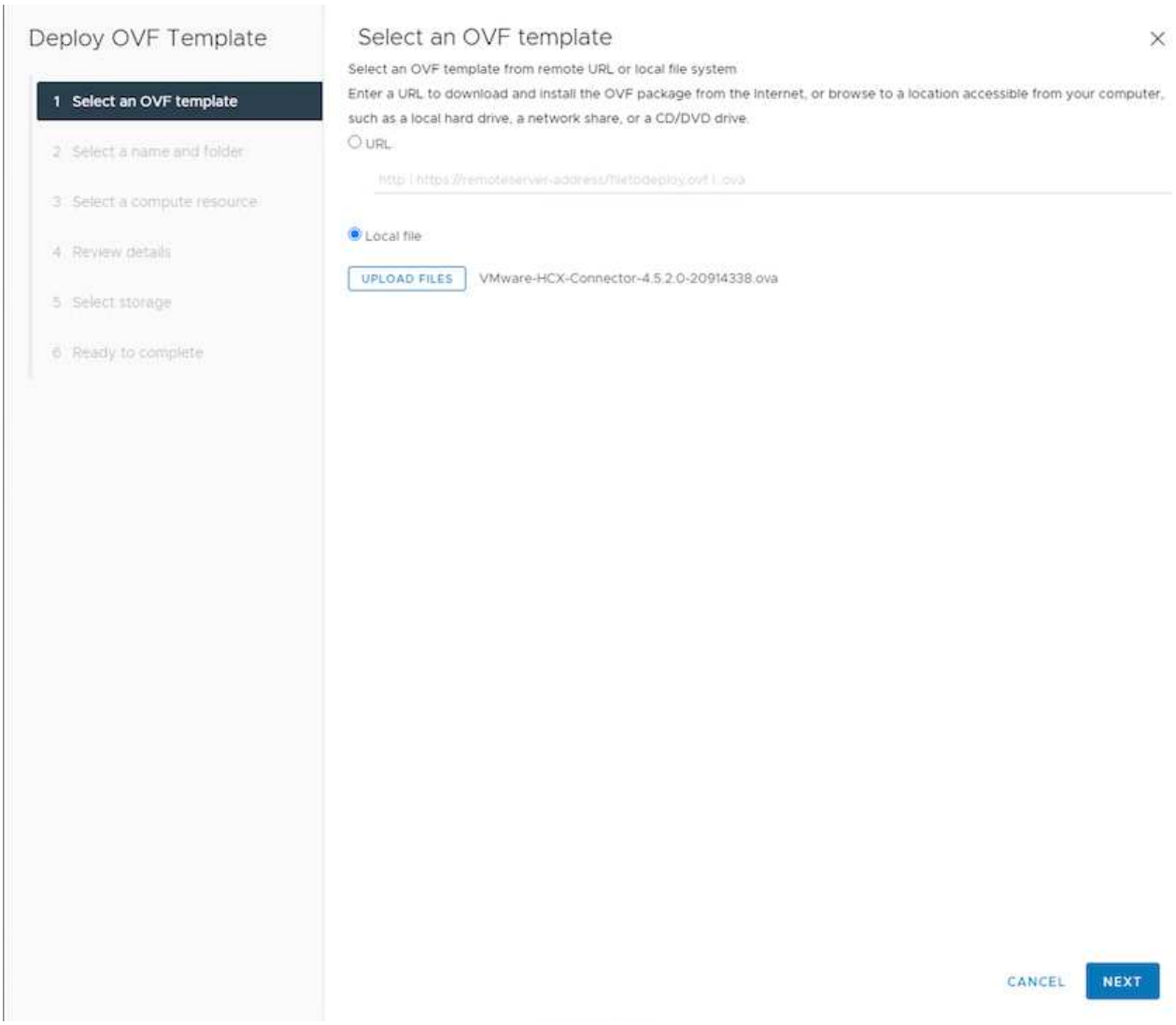
4. Actualice HCX Cloud Manager a la última versión disponible desde la interfaz de usuario de HCX Cloud Manager.

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.

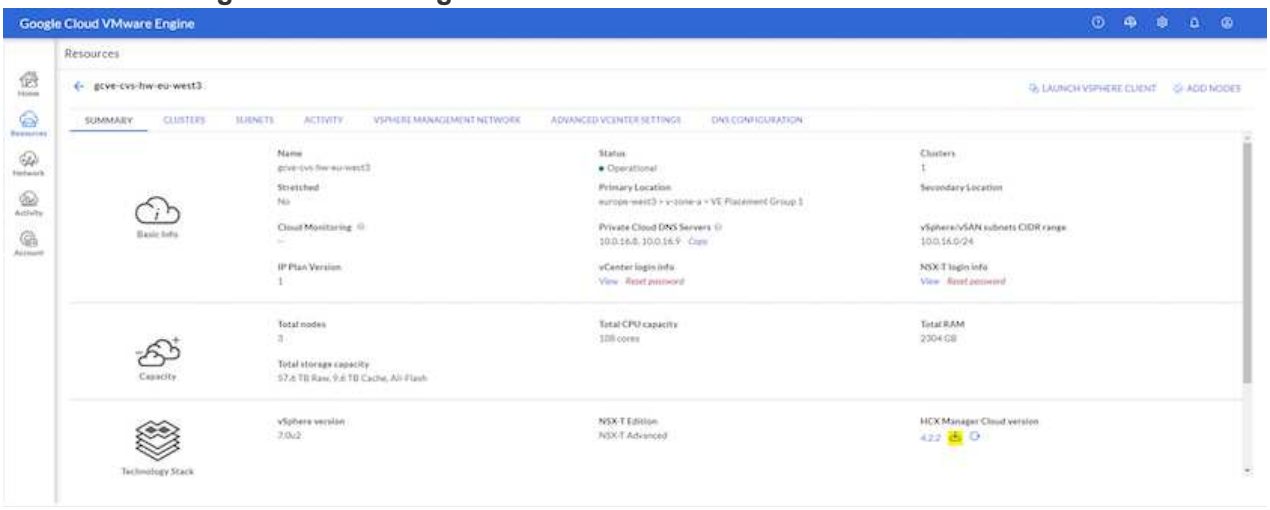
Encienda el dispositivo virtual manualmente.

Para obtener instrucciones paso a paso, consulte la "Documentación de Google 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 clave 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.

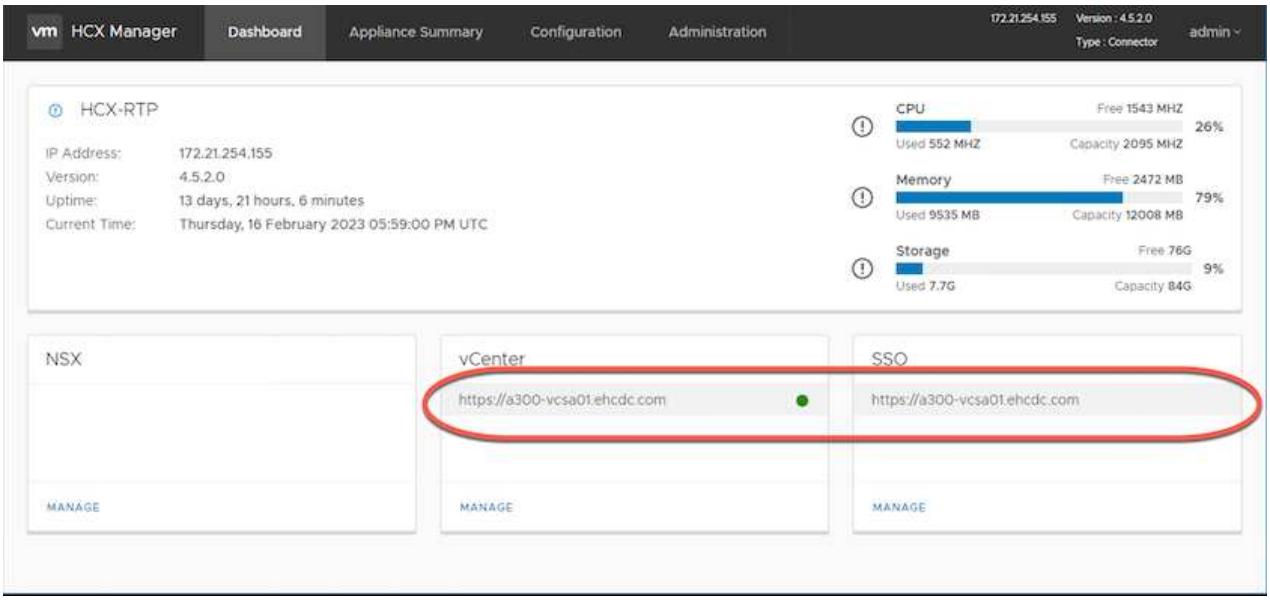
8. En **Configurar SSO/PSC**, proporcione el FQDN o la dirección IP del controlador de servicios de plataforma (PSC) y haga clic en **continuar**.

   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.

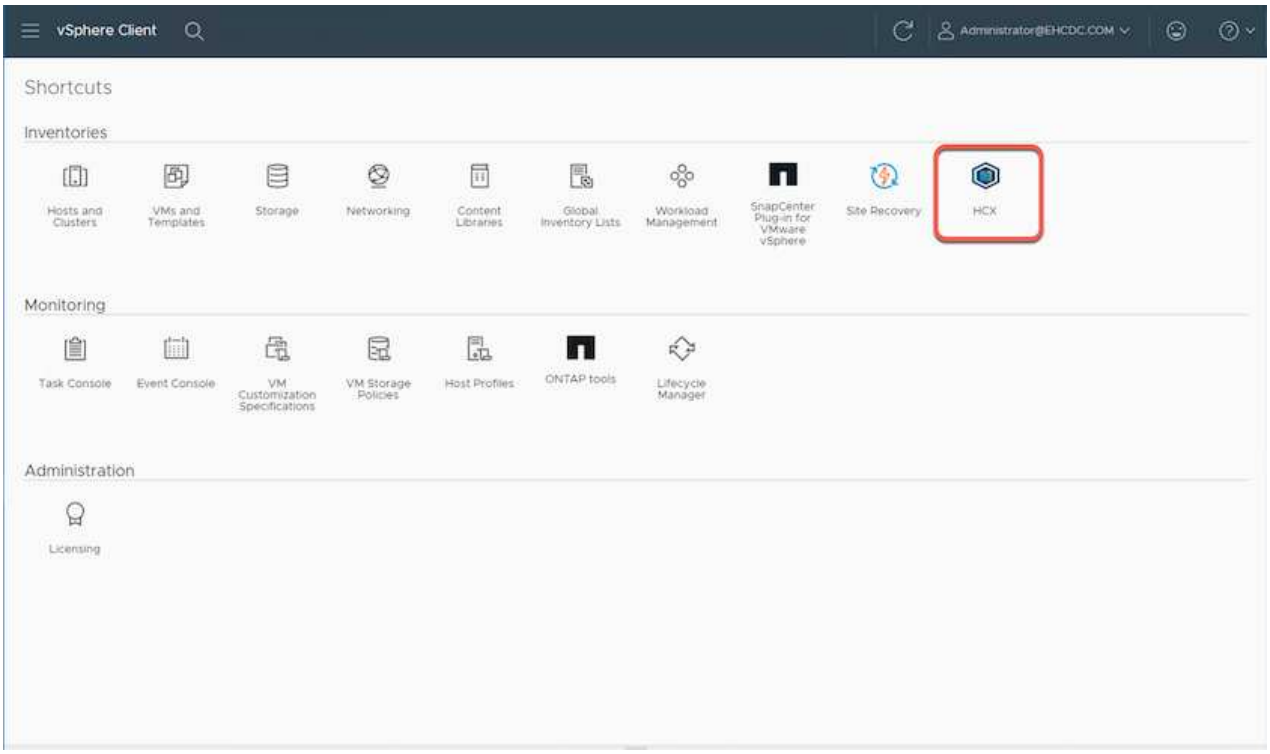
Este proceso debe tardar aproximadamente de 10 a 20 minutos y el plugin se añadirá a vCenter Server.



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

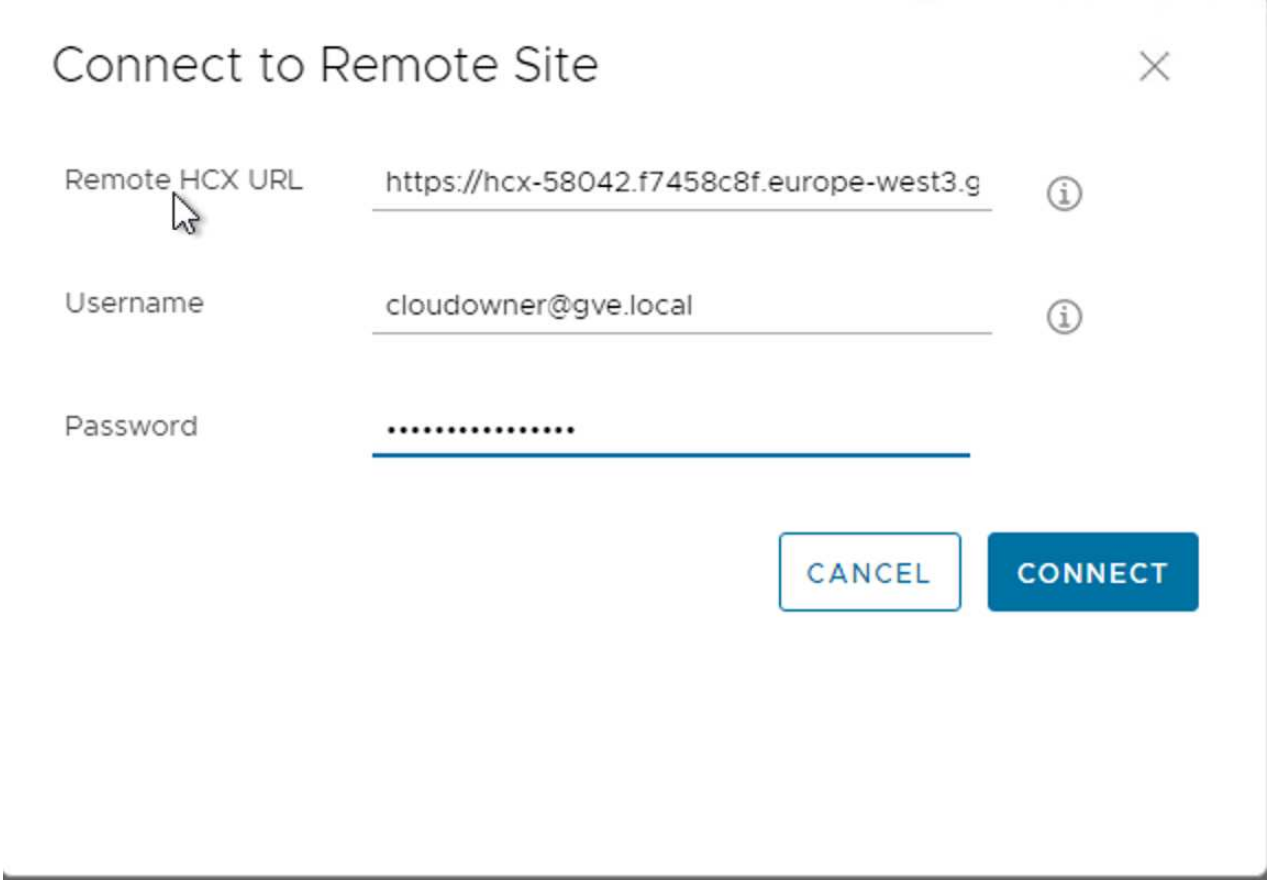
Después de implementar y configurar el conector HCX en el vCenter local, establezca la conexión con Cloud Manager añadiendo el emparejamiento. Para configurar el emparejamiento de sitios, lleve a cabo los siguientes pasos:

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**.

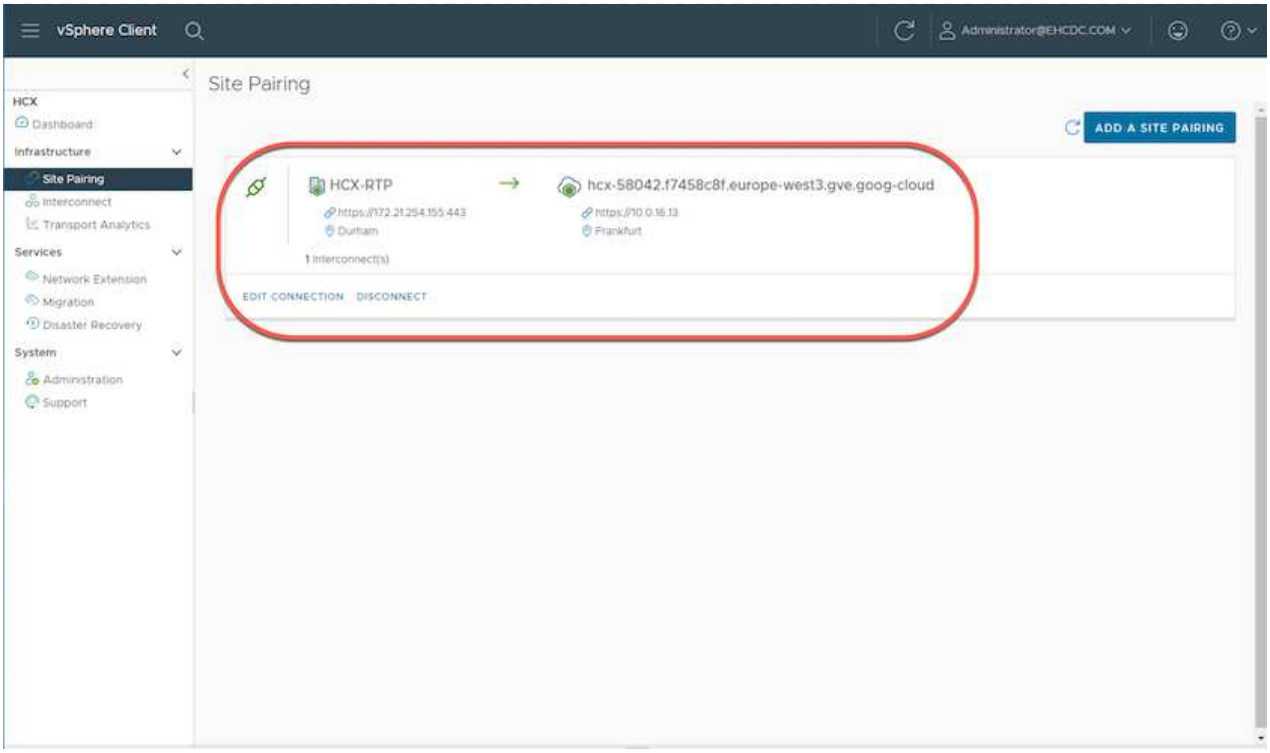
Introduzca la dirección URL o dirección IP de HCX Cloud Manager de Google Cloud Engine y las credenciales para el usuario con privilegios de rol de propietario de cloud para acceder al cloud privado.



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.

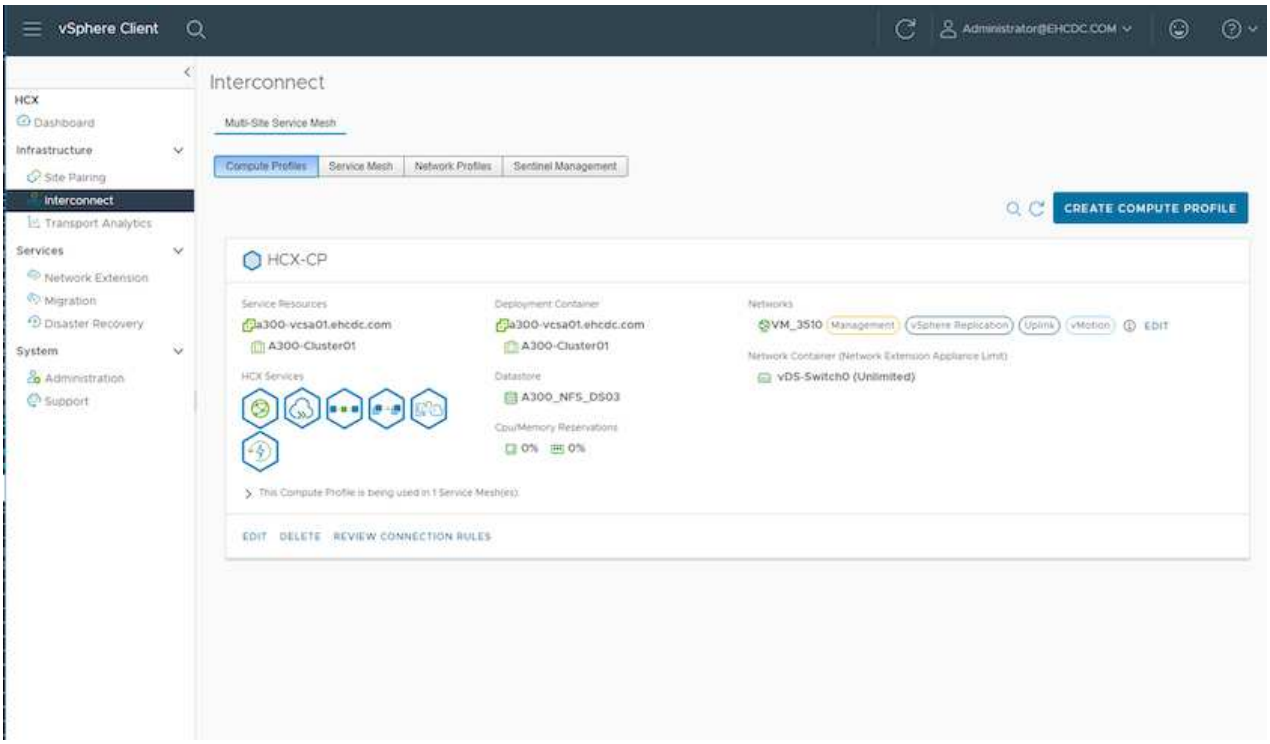

vSphere Client
Administrator@EHCDC.COM
HCX
Dashboard
Infrastructure
Site Pairing
Interconnect
Transport Analytics
Services
Network Extension
Migration
Disaster Recovery
System
Administration
Support
Site Pairing
ADD A SITE PAIRING
HCX-RTP
https://172.21.254.155:443
Durham
hcx-58042.f7458c8f.europe-west3.gve.goog-cloud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

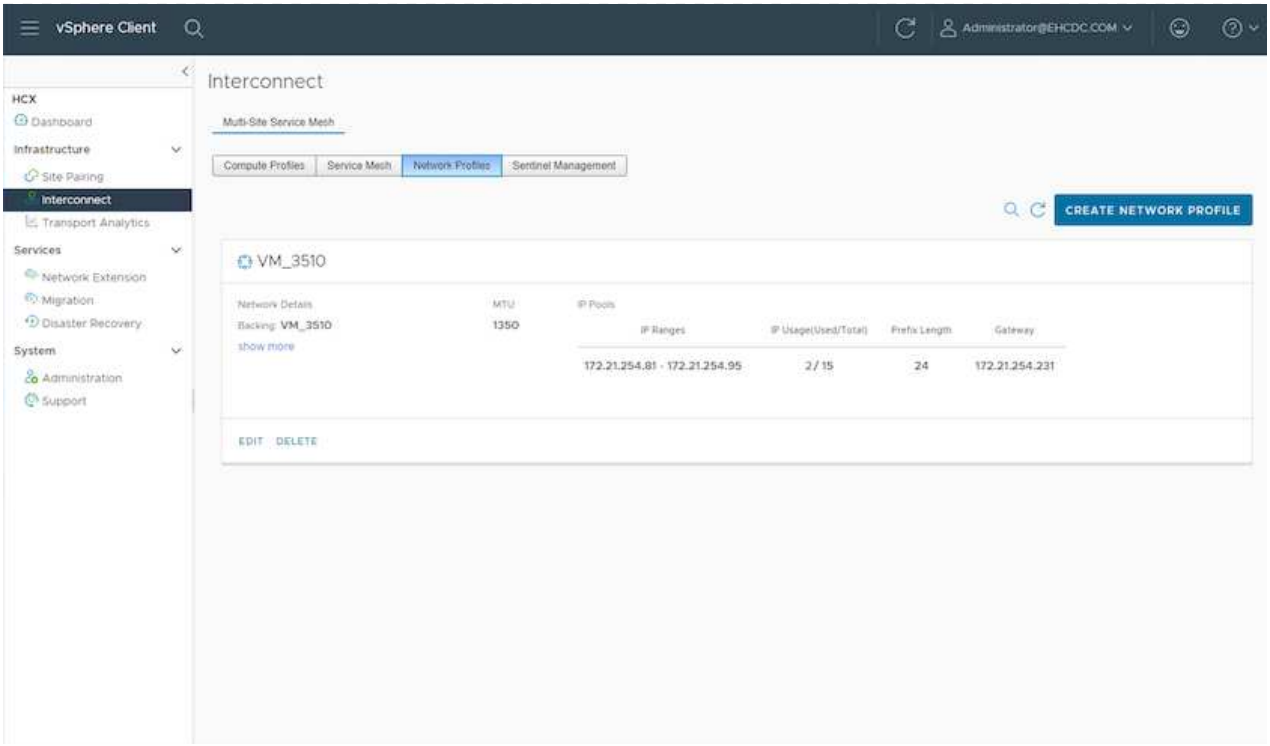
   Los perfiles informáticos definen los parámetros de implementación, incluidos los dispositivos que se implementan y qué parte del centro de datos de VMware puede acceder al servicio HCX.



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**.

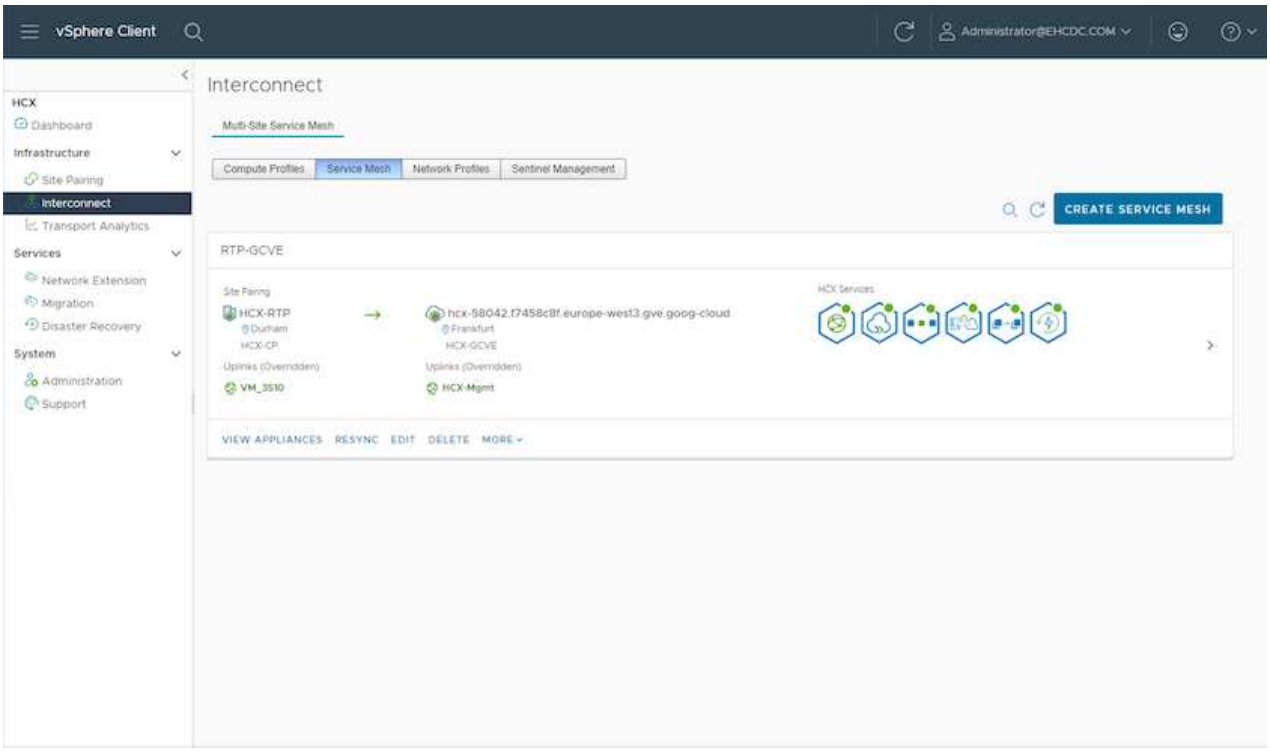
   El perfil de red define un rango de direcciones IP y redes que utiliza HCX para sus dispositivos virtuales.

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

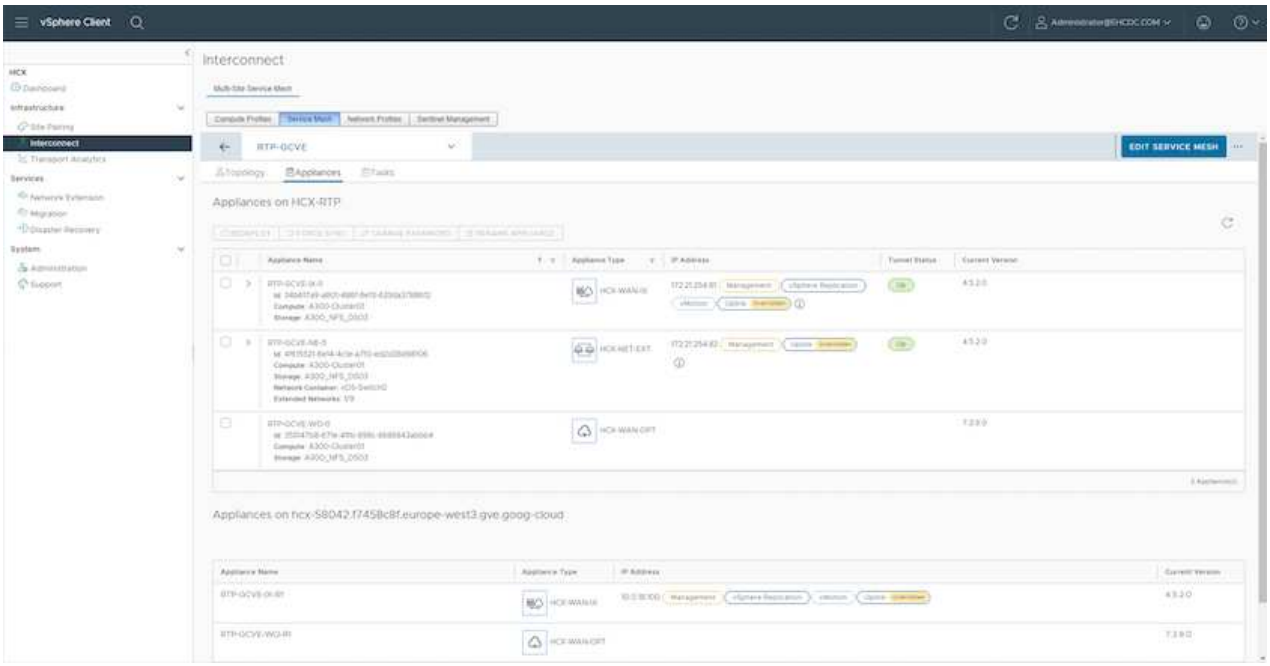


3. En este momento, se han creado correctamente los perfiles de computación y red.
4. Cree la malla de servicio seleccionando la pestaña **malla de servicio** en la opción **interconexión** y seleccione los sitios SDDC en las instalaciones y GCVE.
5. La malla de servicio especifica una pareja de perfiles 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 "Migración de máquinas virtuales de VMware con documentación de VMware HCX".

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

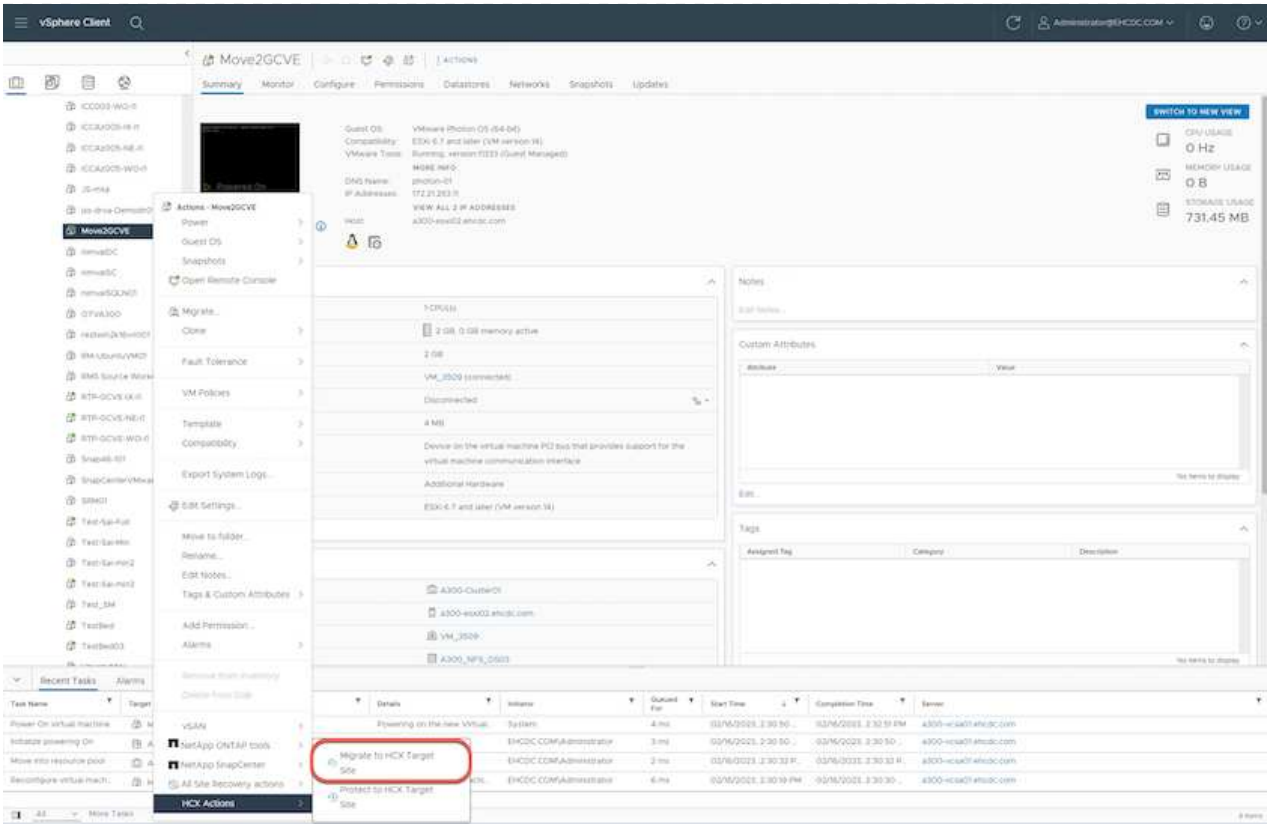
> El dispositivo HCX-IX agrega el servicio Mobility Agent como un objeto host en vCenter Server. El procesador, la memoria, los recursos de almacenamiento y redes que se muestran en este objeto no representan el consumo real en el hipervisor físico que aloja el dispositivo IX.

HCX vMotion

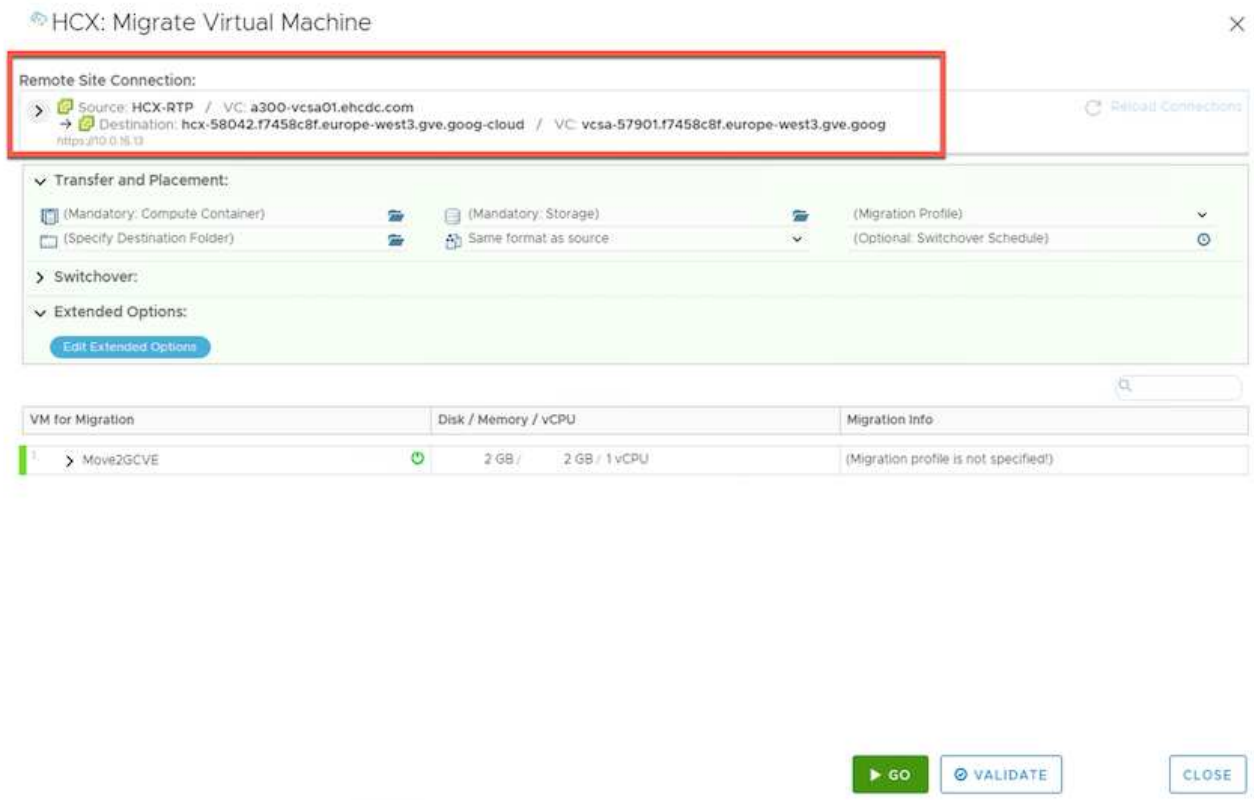
En esta sección se describe el mecanismo HCX vMotion. Esta tecnología de migración utiliza el protocolo VMware vMotion para migrar un equipo virtual a GCVE. La opción de migración de vMotion se utiliza para migrar el estado de las máquinas virtuales de una única máquina virtual a la vez. No se produce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

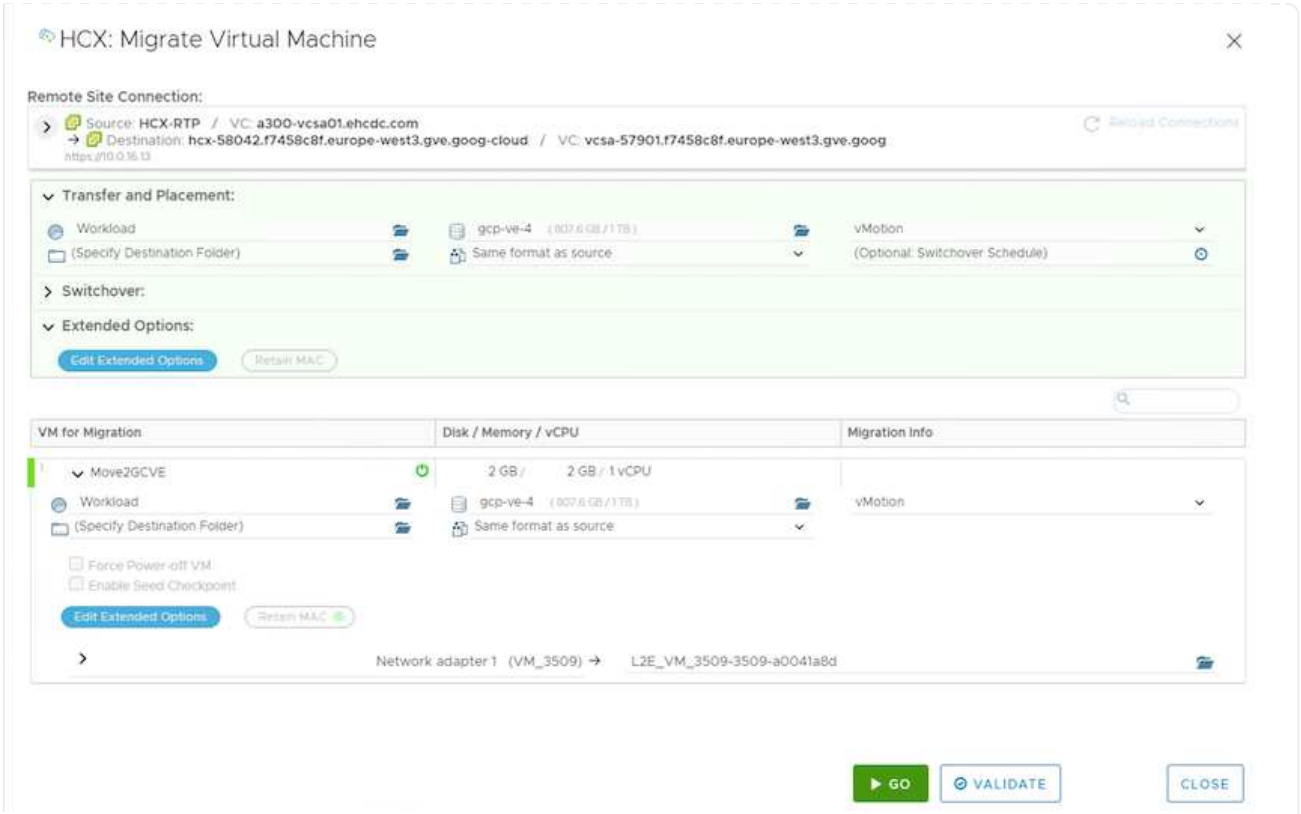
1. Desde el cliente vSphere local, vaya a Inventory, haga clic con el botón derecho en la máquina virtual que se va a migrar y seleccione HCX Actions > Migrate to HCX Target Site.



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



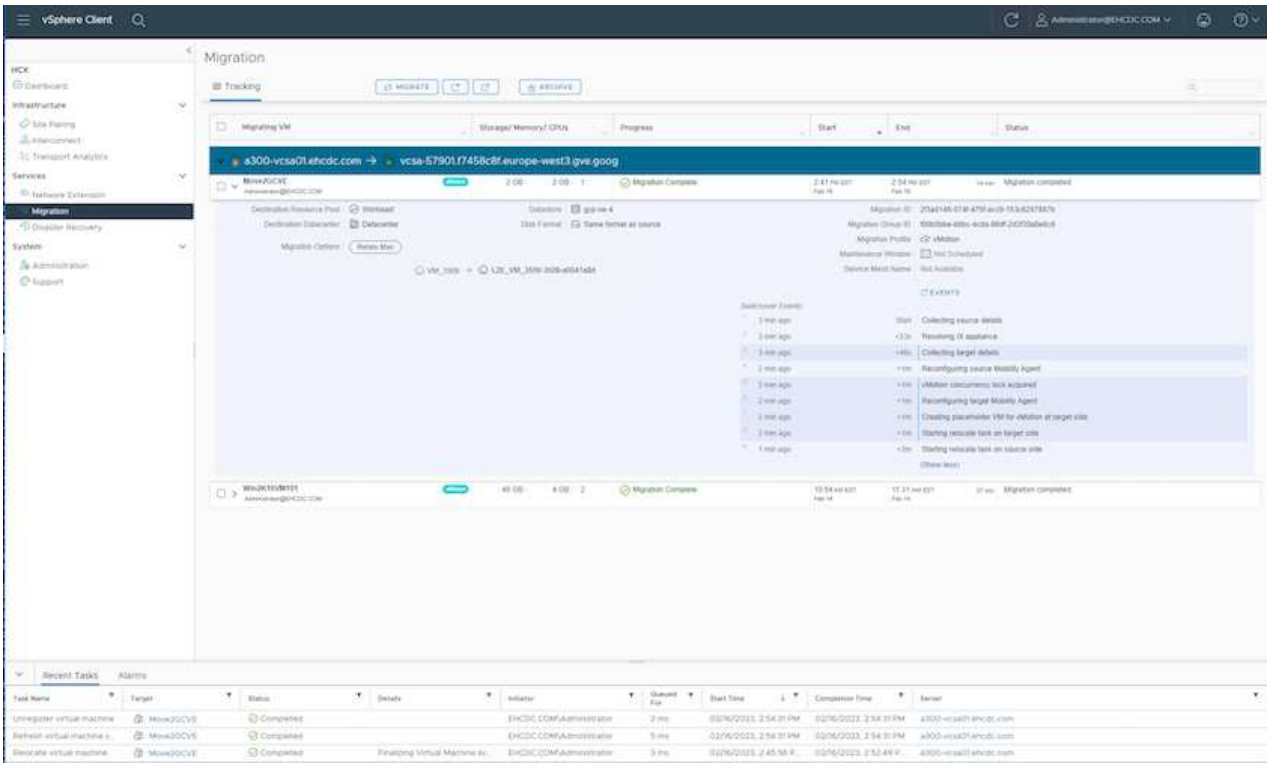
3. Actualice los campos obligatorios (clúster, almacenamiento y red de destino), haga clic en Validate.



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 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 NFS de Google Cloud NetApp Volumes (NetApp Volumes) de destino debe tener espacio suficiente para gestionar 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 Google Cloud NetApp Volumes NFS Datastore en Google Cloud VMware Engine mediante la función de replicación de Veeam

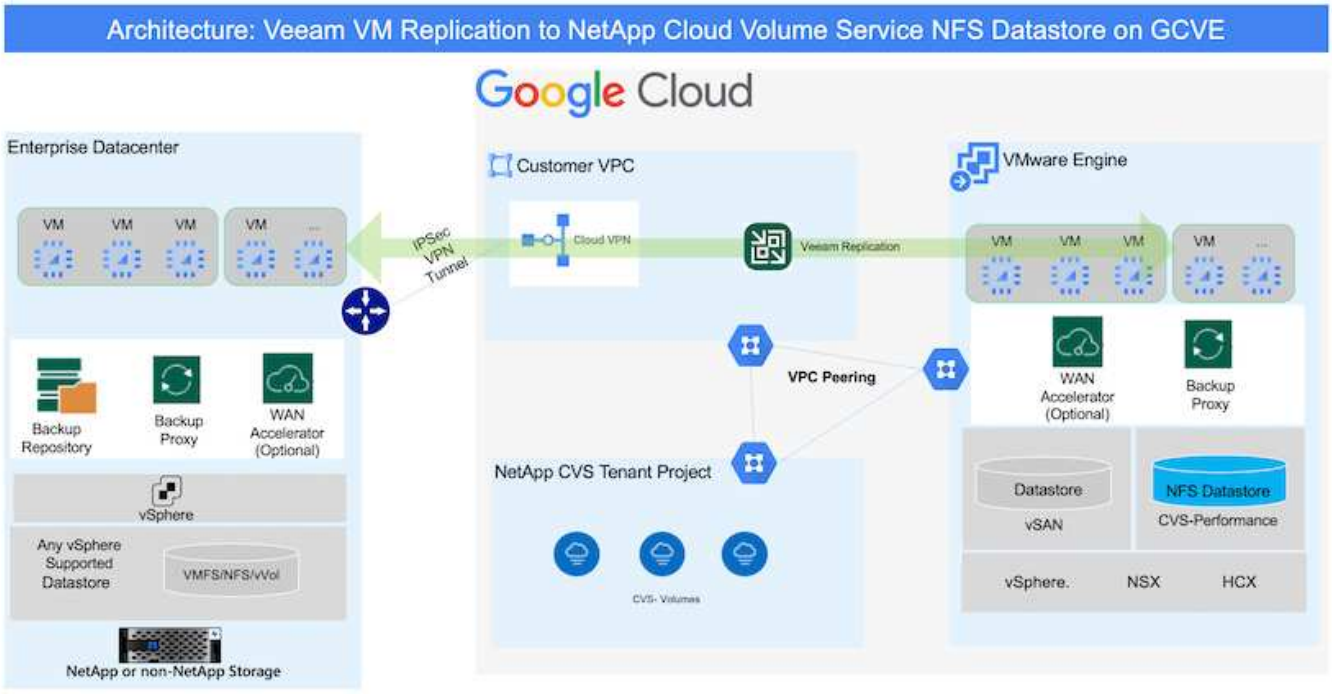
Los clientes que actualmente utilizan Veeam para sus requisitos de protección de datos continúan usando esa solución para migrar las cargas de trabajo a GCVE y disfrutar de las ventajas de los almacenes de datos de NetApp Volumes NFS de Google Cloud.

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 Google Cloud NetApp Volumes, Veeam y Google Cloud VMware Engine (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 de Google Cloud NetApp Volumes está 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 de Google Cloud NetApp Volumes está 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 volúmenes NetApp 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)

Obtén más información sobre el soporte de región global para GCP, GCVE y NetApp Volumes.

> El almacén de datos NFS estará disponible en las regiones en las que ambos servicios (GCVE y NetApp Volumes Performance) estén disponibles.

El almacén de datos NFS complementario para GCVE es compatible con volúmenes de NetApp de Google Cloud.

Solo se pueden utilizar volúmenes de NetApp Volumes-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 Cloud NetApp Volumes (NetApp Volumes) 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.