TR-4955: Recuperación ante desastres con Azure NetApp Files (ANF) y Azure VMware Solution (AVS)

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/es-es/netapp-solutions-cloud/vmware/vmw-azure-avs-dro.html on August 18, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

TR-4955: Recuperación ante desastres con Azure NetApp Files (ANF) y Azure VMware Solution (AVS) 1
Descripción general 1
Prerrequisitos y recomendaciones generales 1
Empezando 2
Implementar la solución VMware de Azure 2
Aprovisionar y configurar Azure NetApp Files 2
Instalación de DRO 3
Configuración de DRO 4
Agrupaciones de recursos 7
Planes de replicación 8
Recuperación de ransomware 15
Conclusión 15
Dónde encontrar información adicional 15

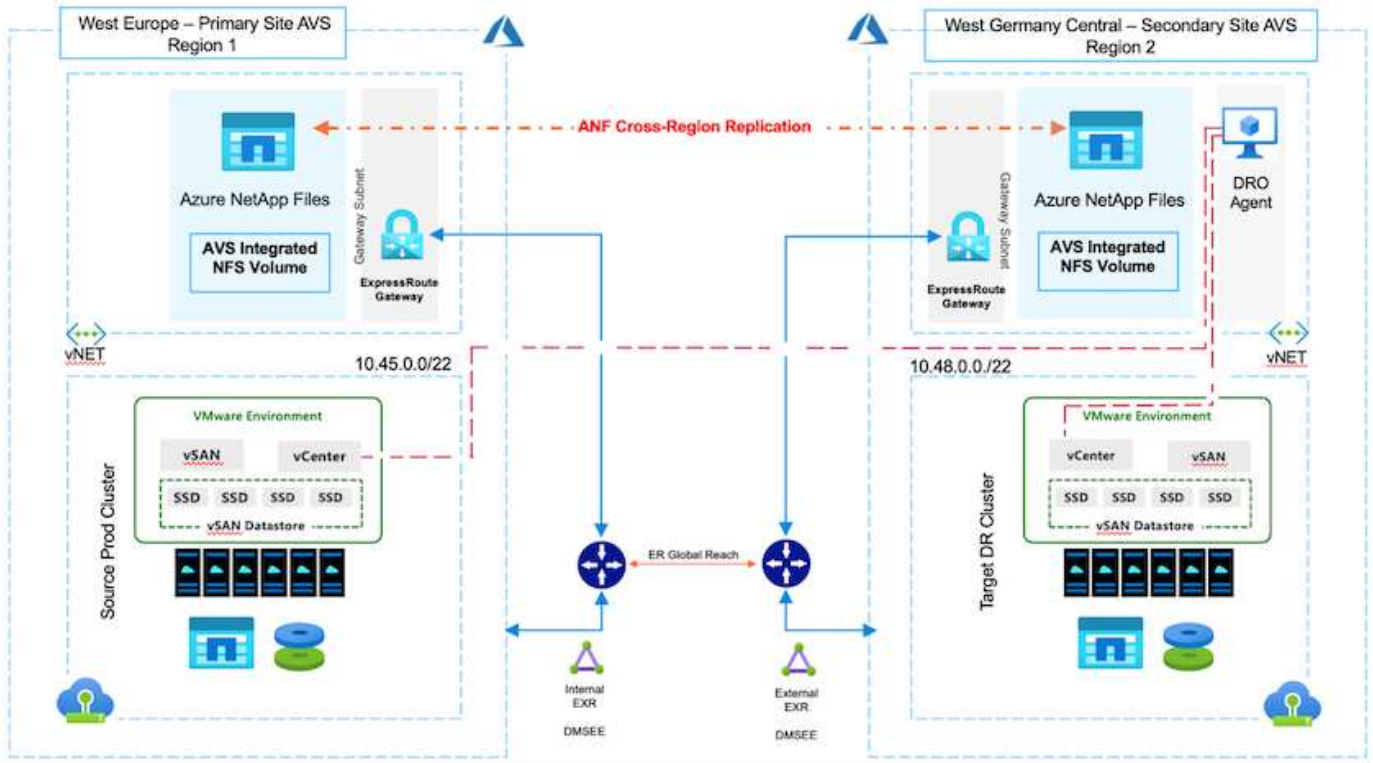
TR-4955: Recuperación ante desastres con Azure NetApp Files (ANF) y Azure VMware Solution (AVS)

La recuperación ante desastres mediante la replicación a nivel de bloques entre regiones dentro de la nube es una forma resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos de corrupción de datos (por ejemplo, ransomware).

Descripción general

Con la replicación de volúmenes entre regiones de archivos Azure NetApp (ANF), las cargas de trabajo de VMware que se ejecutan en un sitio SDDC de Azure VMware Solution (AVS) que usa volúmenes de archivos Azure NetApp como un almacén de datos NFS en el sitio AVS principal se pueden replicar en un sitio AVS secundario designado en la región de recuperación de destino.

Disaster Recovery Orchestrator (DRO) (una solución con script y una interfaz de usuario) se puede utilizar para recuperar sin problemas cargas de trabajo replicadas de un SDDC de AVS a otro. DRO automatiza la recuperación interrumpiendo el emparejamiento de replicación y luego montando el volumen de destino como un almacén de datos, a través del registro de VM en AVS, hasta asignaciones de red directamente en NSX-T (incluido con todas las nubes privadas de AVS).



Prerrequisitos y recomendaciones generales

- Verifique que haya habilitado la replicación entre regiones mediante la creación de un emparejamiento de replicación. Ver "Crear replicación de volumen para Azure NetApp Files" .

- Debe configurar ExpressRoute Global Reach entre las nubes privadas de Azure VMware Solution de origen y destino.
- Debe tener una entidad de servicio que pueda acceder a los recursos.
- Se admite la siguiente topología: sitio AVS principal a sitio AVS secundario.
- Configurar el "replicación" Programe cada volumen de manera adecuada según las necesidades del negocio y la tasa de cambio de datos.

No se admiten topologías en cascada ni de entrada y salida en abanico.

Empezando

Implementar la solución VMware de Azure

El "Solución VMware de Azure" (AVS) es un servicio de nube híbrida que proporciona SDDC de VMware completamente funcionales dentro de una nube pública de Microsoft Azure. AVS es una solución propia totalmente administrada y respaldada por Microsoft y verificada por VMware que utiliza la infraestructura de Azure. Por lo tanto, los clientes obtienen VMware ESXi para la virtualización informática, vSAN para el almacenamiento hiperconvergente y NSX para redes y seguridad, todo ello mientras aprovechan la presencia global de Microsoft Azure, las instalaciones de centros de datos líderes en su clase y la proximidad al rico ecosistema de servicios y soluciones nativos de Azure. Una combinación de Azure VMware Solution SDDC y Azure NetApp Files proporciona el mejor rendimiento con una latencia de red mínima.

Para configurar una nube privada de AVS en Azure, siga los pasos de este"enlace" para la documentación de NetApp y en este "enlace" para la documentación de Microsoft. Se puede utilizar un entorno de luz piloto configurado con una configuración mínima para fines de recuperación ante desastres. Esta configuración solo contiene componentes básicos para soportar aplicaciones críticas, y puede escalar y generar más hosts para asumir la mayor parte de la carga si ocurre una conmutación por error.

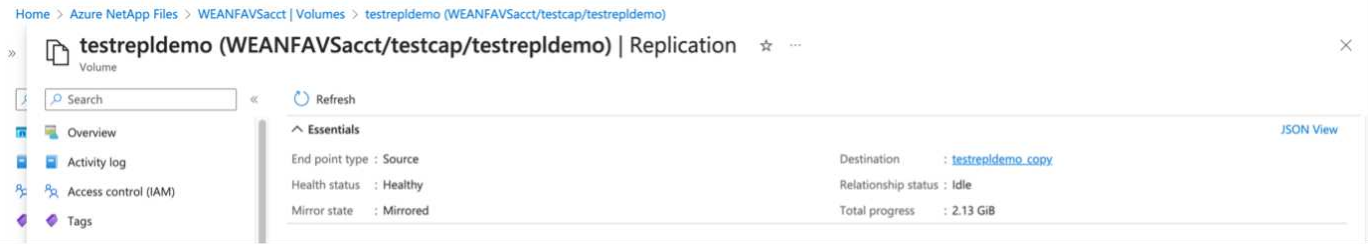
En la versión inicial, DRO admite un clúster SDDC de AVS existente. La creación de SDDC a pedido estará disponible en una próxima versión.

Aprovisionar y configurar Azure NetApp Files

"Azure NetApp Files"Es un servicio de almacenamiento de archivos medido, de clase empresarial y de alto rendimiento. Siga los pasos de este "enlace" para aprovisionar y configurar Azure NetApp Files como un almacén de datos NFS para optimizar las implementaciones de nube privada de AVS.

Crear replicación de volumen para volúmenes de almacén de datos con tecnología Azure NetApp Files

El primer paso es configurar la replicación entre regiones para los volúmenes de almacén de datos deseados desde el sitio principal de AVS al sitio secundario de AVS con las frecuencias y retenciones adecuadas.



Siga los pasos de este "enlace" para configurar la replicación entre regiones mediante la creación de un peering de replicación. El nivel de servicio del grupo de capacidad de destino puede coincidir con el del grupo de capacidad de origen. Sin embargo, para este caso de uso específico, puede seleccionar el nivel de servicio estándar y luego "modificar el nivel de servicio" en caso de un desastre real o simulaciones de DR.

> Una relación de replicación entre regiones es un requisito previo y debe crearse de antemano.

Instalación de DRO

Para comenzar a utilizar DRO, use el sistema operativo Ubuntu en la máquina virtual de Azure designada y asegúrese de cumplir con los requisitos previos. Luego instala el paquete.

Prerrequisitos:

- Principal de servicio que puede acceder a los recursos.
- Asegúrese de que exista conectividad adecuada con las instancias de SDDC y de Azure NetApp Files de origen y destino.
- La resolución de DNS debe estar implementada si está utilizando nombres DNS. De lo contrario, utilice direcciones IP para vCenter.

Requisitos del sistema operativo:

- Ubuntu Focal 20.04 (LTS)Los siguientes paquetes deben instalarse en la máquina virtual del agente designado:
- Docker
- Docker-componer
- JqChange `docker.sock` A este nuevo permiso: `sudo chmod 666 /var/run/docker.sock`.

> El `deploy.sh` El script ejecuta todos los requisitos previos necesarios.

Los pasos son los siguientes:

1. Descargue el paquete de instalación en la máquina virtual designada:

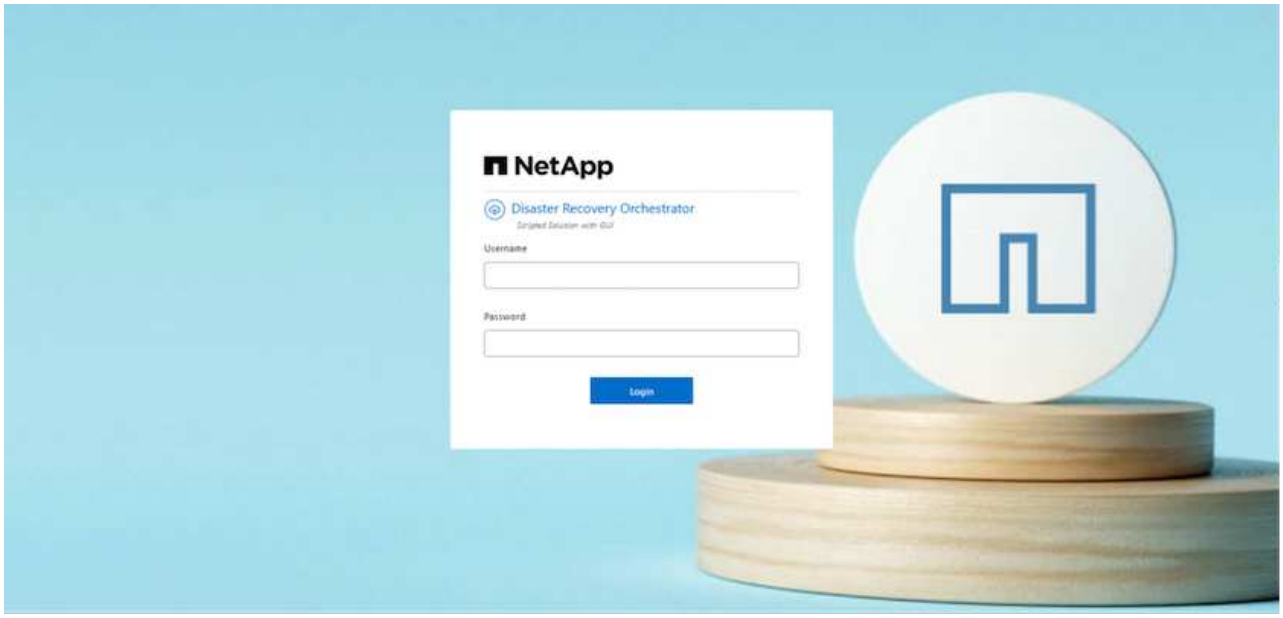
```
git clone https://github.com/NetApp/DRO-Azure.git
```

> El agente debe instalarse en la región del sitio AVS secundario o en la región del sitio AVS primario en una zona de disponibilidad (AZ) separada del SDDC.

2. Descomprima el paquete, ejecute el script de implementación e ingrese la IP del host (por ejemplo, `10.10.10.10`).

```
tar xvf draas_package.tar
Navigate to the directory and run the deploy script as below:
sudo sh deploy.sh
```

3. Acceda a la interfaz de usuario utilizando las siguientes credenciales:
    - Nombre de usuario: `admin`
    - Contraseña: `admin`



Configuración de DRO

Una vez que Azure NetApp Files y AVS se hayan configurado correctamente, puede comenzar a configurar DRO para automatizar la recuperación de cargas de trabajo desde el sitio de AVS principal al sitio de AVS secundario. NetApp recomienda implementar el agente DRO en el sitio AVS secundario y configurar la conexión de puerta de enlace de ExpressRoute para que el agente DRO pueda comunicarse a través de la red con los componentes AVS y Azure NetApp Files adecuados.

El primer paso es agregar credenciales. DRO requiere permiso para descubrir Azure NetApp Files y Azure VMware Solution. Puede otorgar los permisos necesarios a una cuenta de Azure creando y configurando una aplicación de Azure Active Directory (AD) y obteniendo las credenciales de Azure que DRO necesita. Debe vincular la entidad de servicio a su suscripción de Azure y asignarle un rol personalizado que tenga los permisos necesarios correspondientes. Cuando agrega entornos de origen y destino, se le solicita que seleccione las credenciales asociadas con la entidad de servicio. Debe agregar estas credenciales a DRO antes de poder hacer clic en Agregar nuevo sitio.

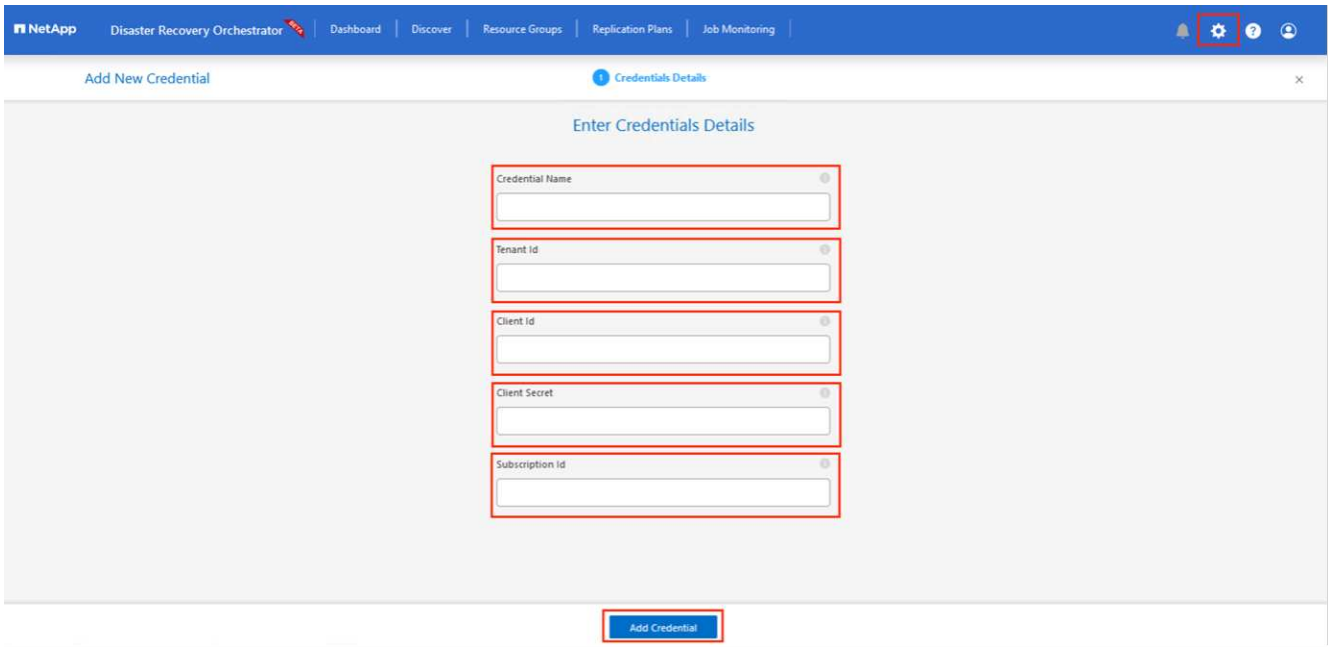
Para realizar esta operación, complete los siguientes pasos:

1. Abra DRO en un navegador compatible y use el nombre de usuario y la contraseña predeterminados/`admin`/`admin`). La contraseña se puede restablecer después del primer inicio de sesión utilizando la opción Cambiar contraseña.
2. En la parte superior derecha de la consola DRO, haga clic en el ícono **Configuración** y seleccione **Credenciales**.
3. Haga clic en Agregar nueva credencial y siga los pasos del asistente.
4. Para definir las credenciales, ingrese información sobre la entidad de servicio de Azure Active Directory que otorga los permisos necesarios:
    - Nombre de la credencial

- Identificación del inquilino
- ID de cliente
- Secreto del cliente
- ID de suscripción

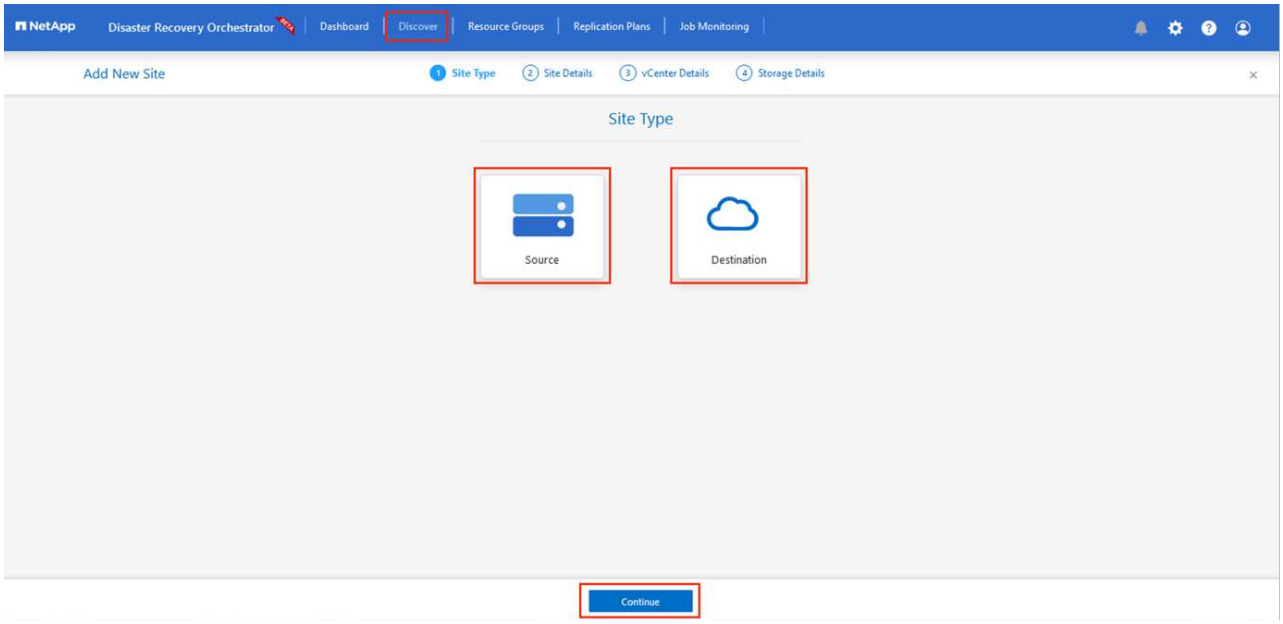
  Deberías haber capturado esta información cuando creaste la aplicación AD.

5. Confirme los detalles sobre las nuevas credenciales y haga clic en Agregar credencial.



Después de agregar las credenciales, es momento de descubrir y agregar los sitios AVS principales y secundarios (tanto vCenter como la cuenta de almacenamiento de archivos de Azure NetApp) a DRO. Para agregar el sitio de origen y destino, complete los siguientes pasos:

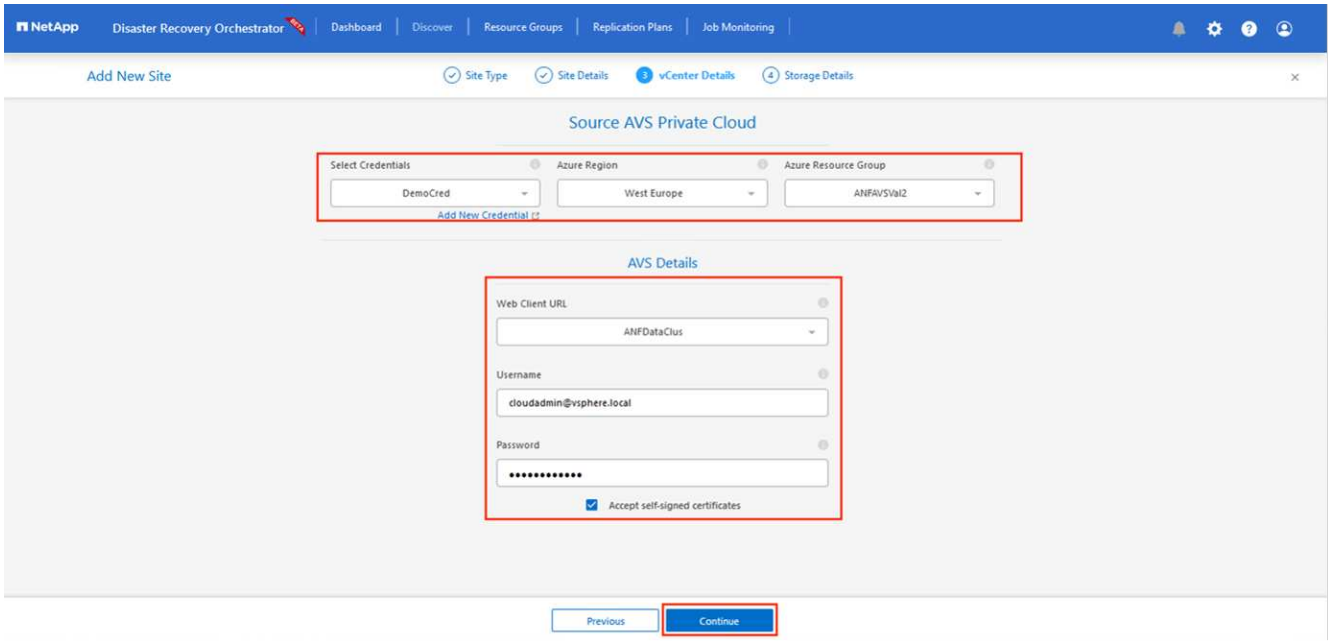
6. Vaya a la pestaña **Descubrir**.
7. Haga clic en **Agregar nuevo sitio**.
8. Agregue el siguiente sitio AVS principal (designado como **Fuente** en la consola).
   - vCenter de SDDC
   - Cuenta de almacenamiento de Azure NetApp Files
9. Agregue el siguiente sitio AVS secundario (designado como **Destino** en la consola).
   - vCenter de SDDC
   - Cuenta de almacenamiento de Azure NetApp Files



10. Agregue detalles del sitio haciendo clic en **Fuente**, ingresando un nombre de sitio descriptivo y seleccionando el conector. Luego haga clic en **Continuar**.

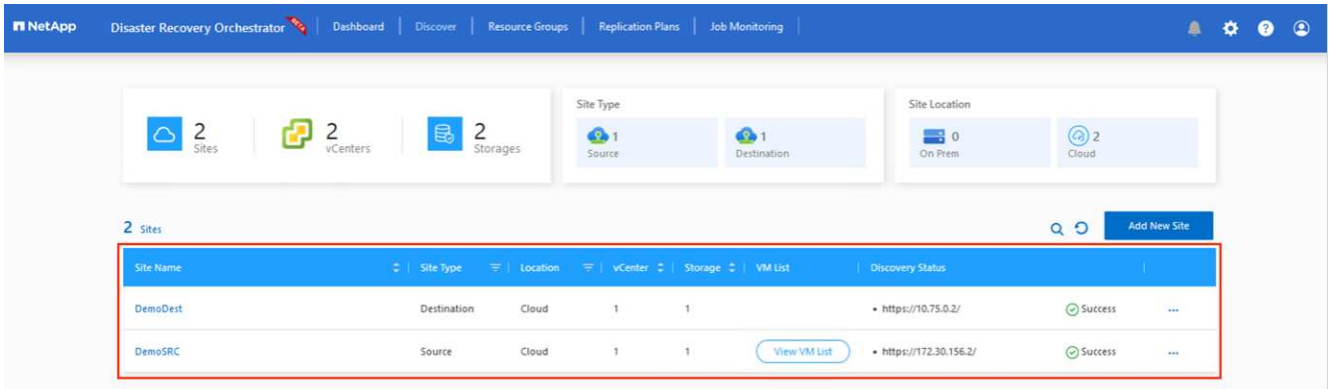
> Para fines de demostración, en este documento se explica cómo agregar un sitio de origen.

11. Actualice los detalles de vCenter. Para ello, seleccione las credenciales, la región de Azure y el grupo de recursos del menú desplegable para el SDDC de AVS principal.
12. DRO enumera todos los SDDC disponibles dentro de la región. Seleccione la URL de la nube privada designada en el menú desplegable.
13. Entrar en el `cloudadmin@vsphere.local` credenciales de usuario. Se puede acceder desde el Portal de Azure. Siga los pasos mencionados en este "enlace" . Una vez hecho esto, haga clic en **Continuar**.

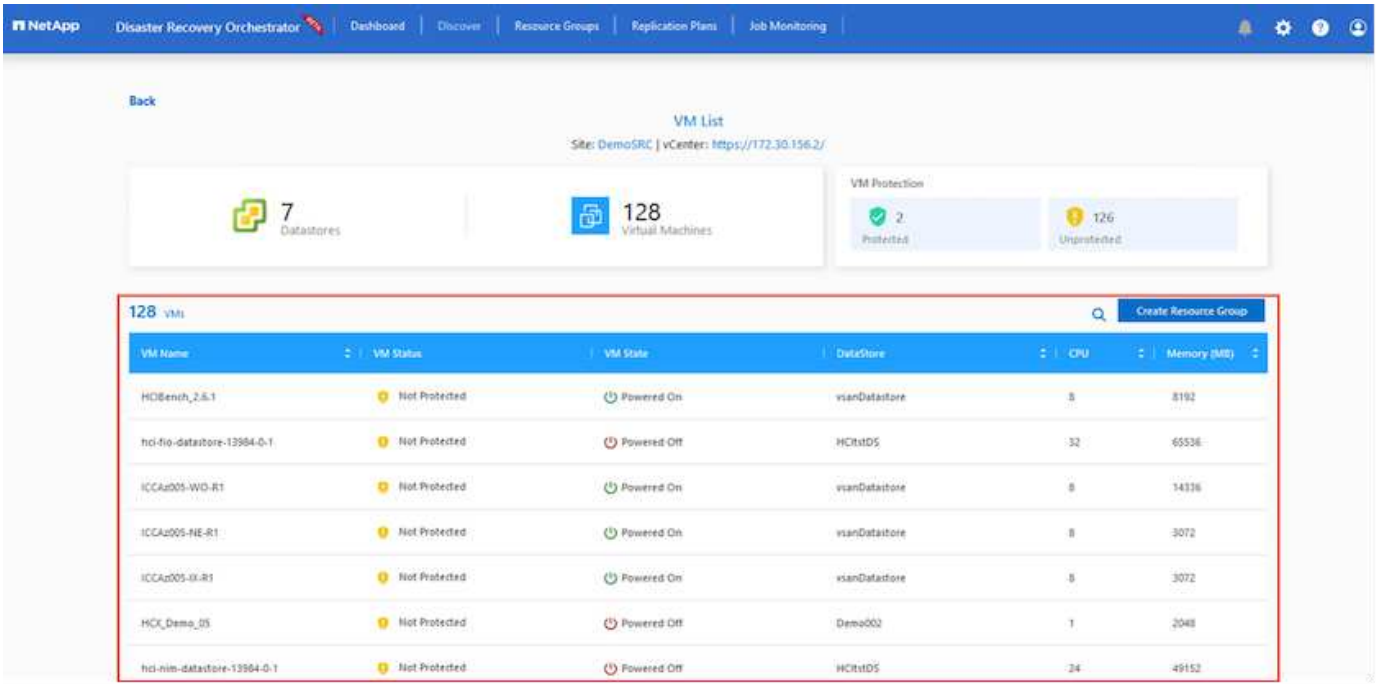


14. Seleccione los detalles del almacenamiento de origen (ANF) seleccionando el grupo de recursos de Azure y la cuenta de NetApp .

15. Haga clic en **Crear sitio**.



Una vez agregado, DRO realiza un descubrimiento automático y muestra las máquinas virtuales que tienen réplicas entre regiones correspondientes desde el sitio de origen al sitio de destino. DRO detecta automáticamente las redes y los segmentos utilizados por las máquinas virtuales y los completa.



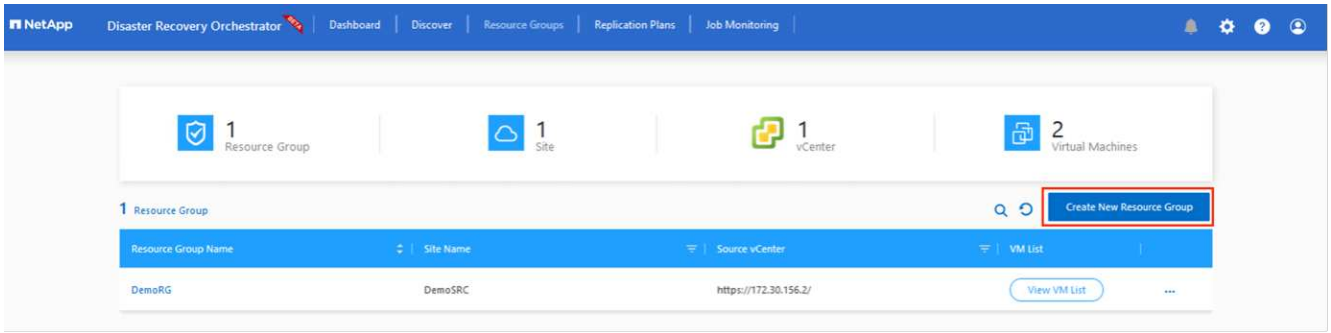
El siguiente paso es agrupar las máquinas virtuales necesarias en sus grupos funcionales como grupos de recursos.

Agrupaciones de recursos

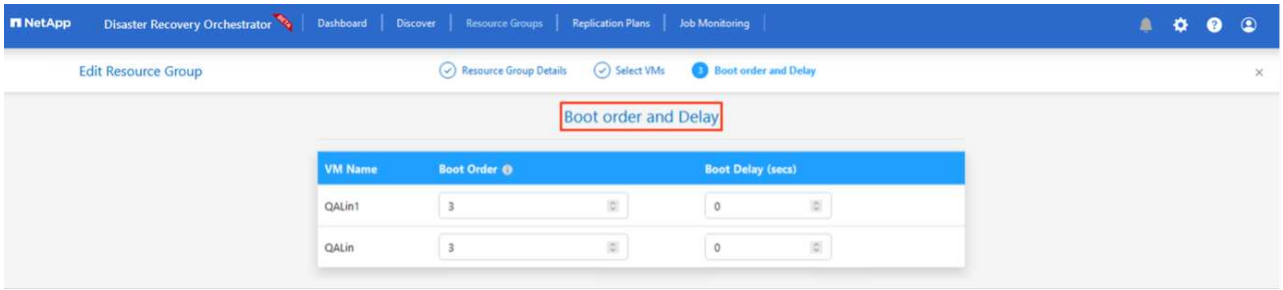
Una vez agregadas las plataformas, agrupe las máquinas virtuales que desea recuperar en grupos de recursos. Los grupos de recursos DRO le permiten agrupar un conjunto de máquinas virtuales dependientes en grupos lógicos que contienen sus órdenes de arranque, retrasos de arranque y validaciones de aplicaciones opcionales que se pueden ejecutar durante la recuperación.

Para comenzar a crear grupos de recursos, haga clic en el elemento de menú **Crear nuevo grupo de recursos**.

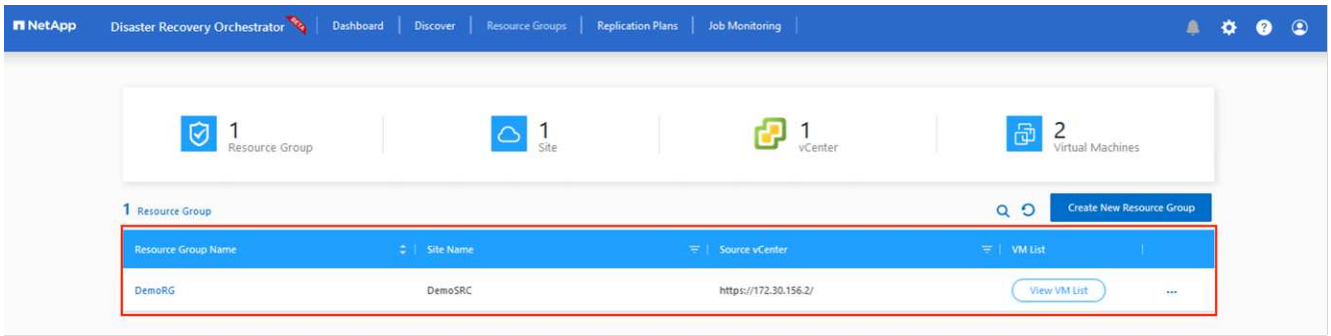
1. Acceda a **Grupos de recursos** y haga clic en **Crear nuevo grupo de recursos**.



2. En Nuevo grupo de recursos, seleccione el sitio de origen en el menú desplegable y haga clic en **Crear**.
3. Proporcione los detalles del grupo de recursos y haga clic en **Continuar**.
4. Seleccione las máquinas virtuales adecuadas mediante la opción de búsqueda.
5. Seleccione el **Orden de arranque** y el **Retraso de arranque** (segundos) para todas las máquinas virtuales seleccionadas. Establezca el orden de la secuencia de encendido seleccionando cada máquina virtual y configurando su prioridad. El valor predeterminado para todas las máquinas virtuales es 3. Las opciones son las siguientes:
   - La primera máquina virtual en encenderse
   - Por defecto
   - La última máquina virtual en encenderse



6. Haga clic en **Crear grupo de recursos**.

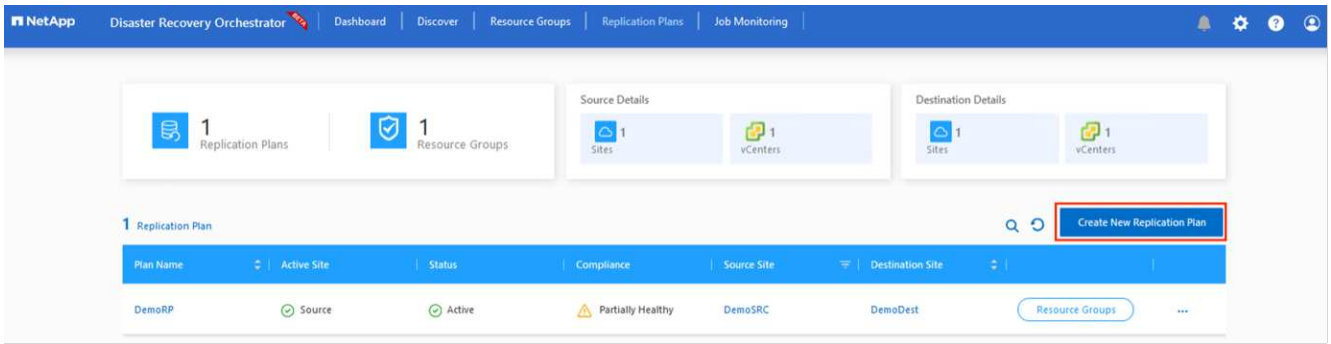


Planes de replicación

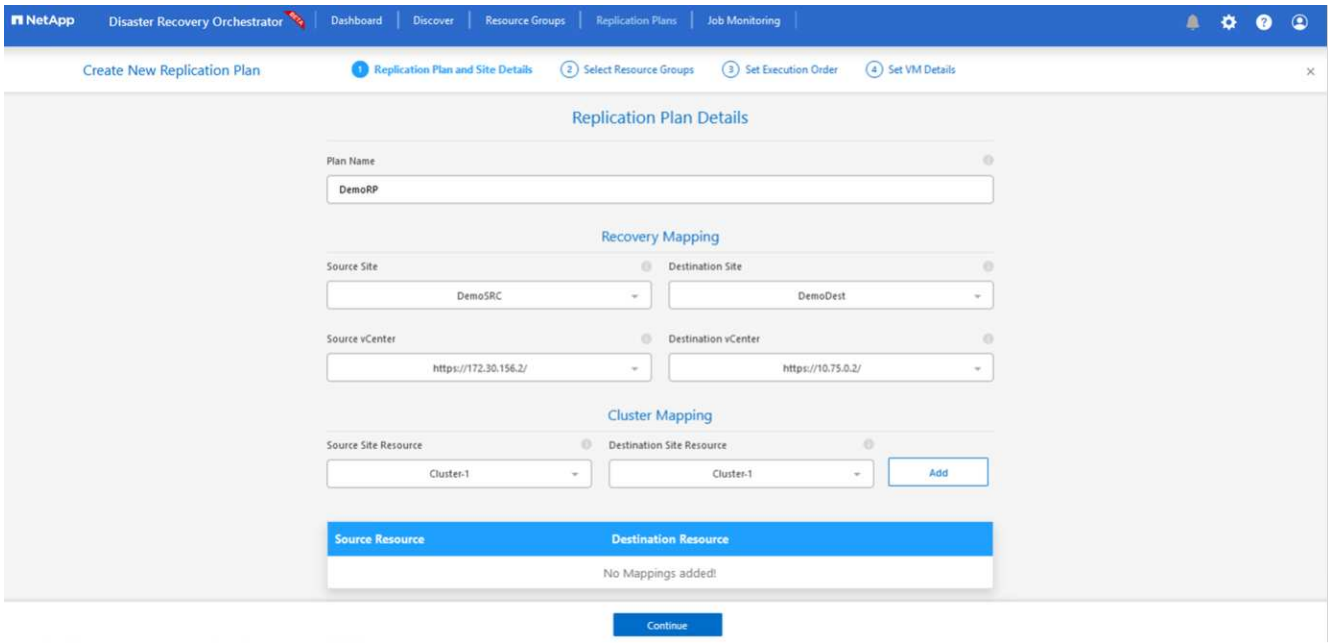
Debe tener un plan para recuperar aplicaciones en caso de desastre. Seleccione las plataformas de vCenter de origen y destino en el menú desplegable, elija los grupos de recursos que se incluirán en este plan y también incluya la agrupación de cómo se deben restaurar y encender las aplicaciones (por ejemplo, controladores de dominio, nivel 1, nivel 2, etc.). A los planes también se les suele llamar planos. Para definir el plan de recuperación, vaya a la pestaña Plan de replicación y haga clic en **Nuevo plan de replicación**.

Para comenzar a crear un plan de replicación, complete los siguientes pasos:

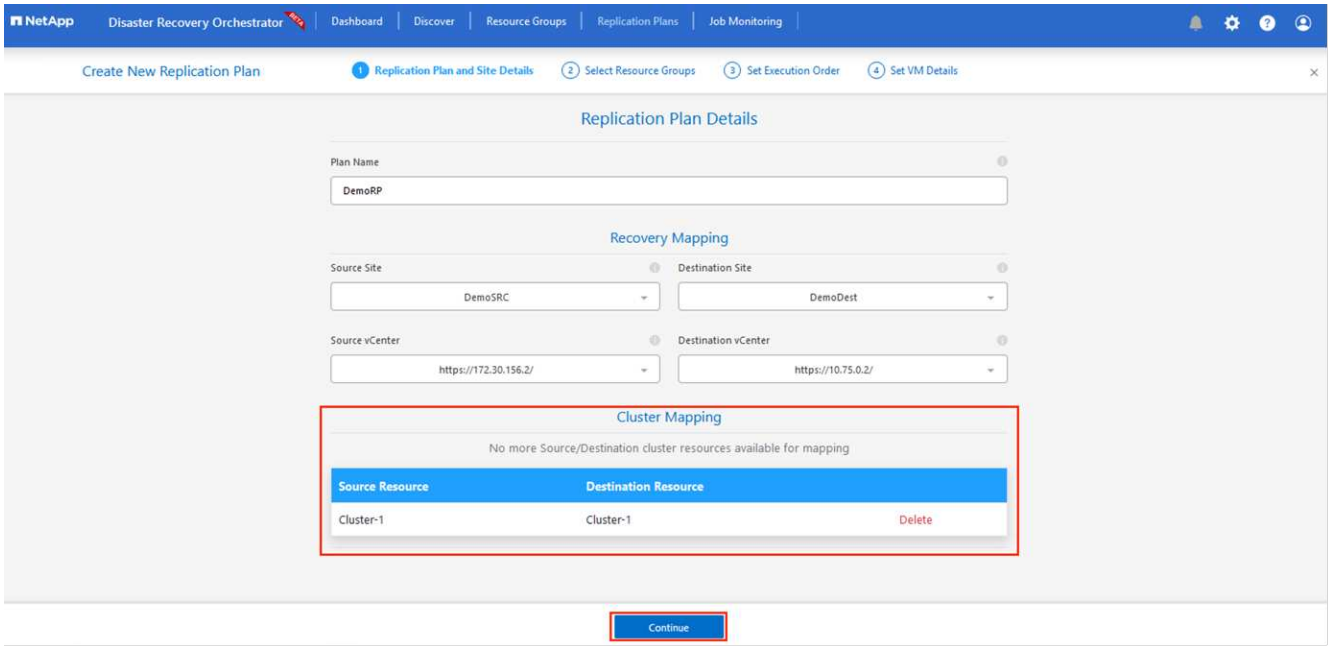
1. Vaya a **Planes de replicación** y haga clic en **Crear nuevo plan de replicación**.



2. En el **Nuevo plan de replicación**, proporcione un nombre para el plan y agregue asignaciones de recuperación seleccionando el Sitio de origen, el vCenter asociado, el Sitio de destino y el vCenter asociado.

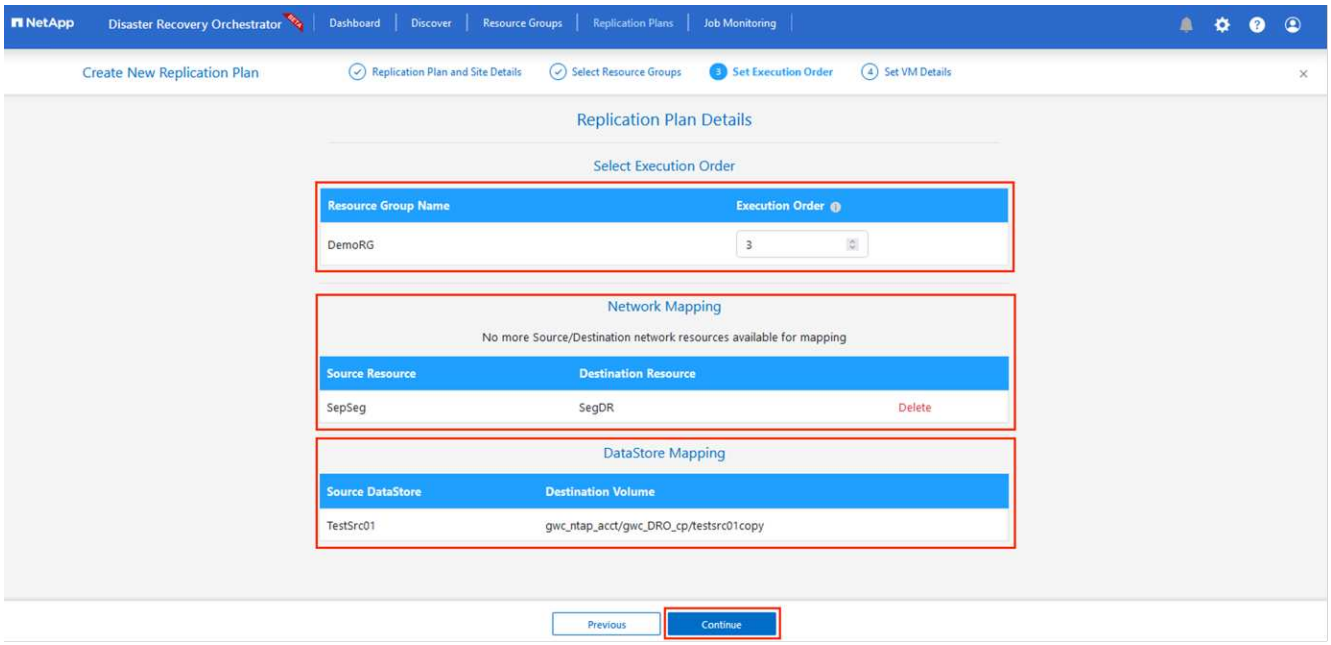


3. Una vez completado el mapeo de recuperación, seleccione **Mapeo de clúster**.

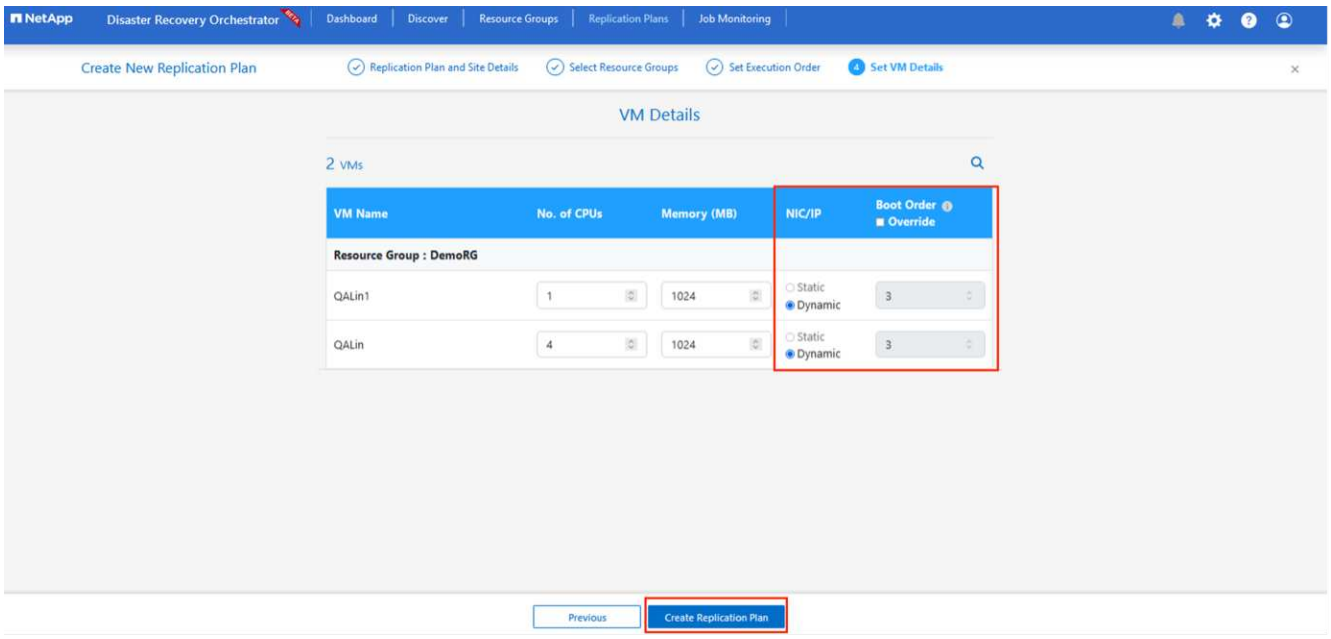


4. Seleccione **Detalles del grupo de recursos** y haga clic en **Continuar**.
5. Establecer el orden de ejecución para el grupo de recursos. Esta opción le permite seleccionar la secuencia de operaciones cuando existen múltiples grupos de recursos.
6. Una vez hecho esto, configure la asignación de red en el segmento apropiado. Los segmentos ya deben estar aprovisionados en el clúster AVS secundario y, para asignar las máquinas virtuales a ellos, seleccione el segmento apropiado.
7. Las asignaciones de almacenes de datos se seleccionan automáticamente en función de la selección de máquinas virtuales.

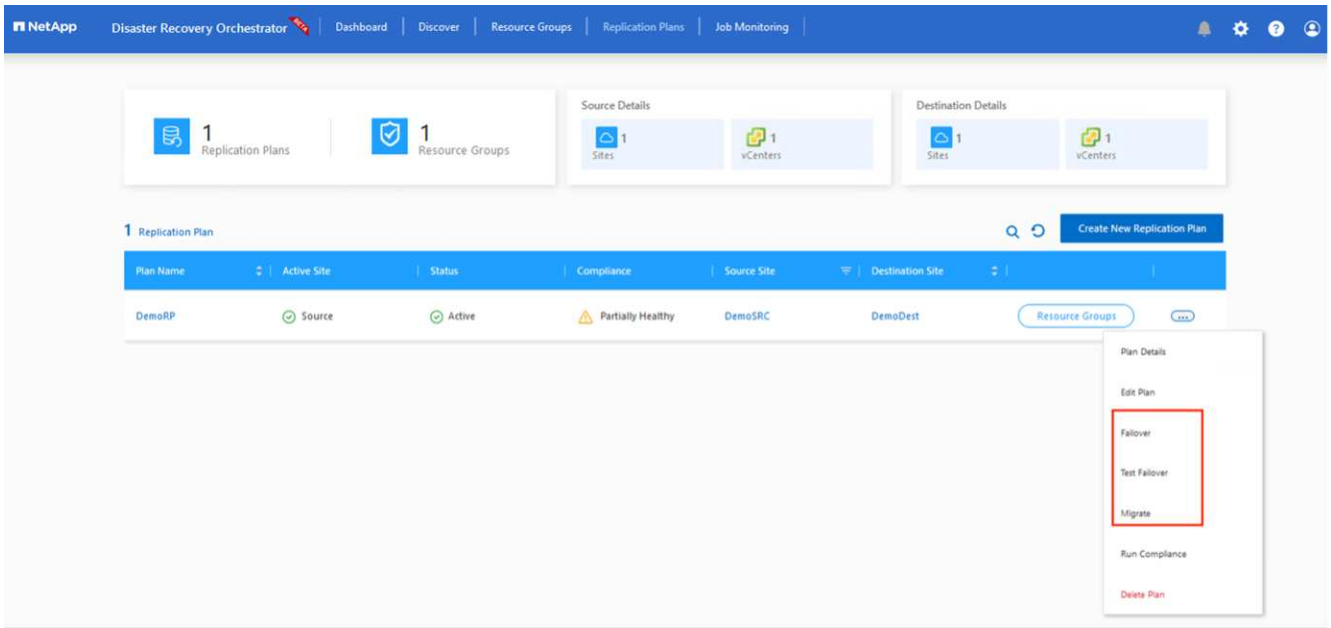
> La replicación entre regiones (CRR) se produce a nivel de volumen. Por lo tanto, todas las máquinas virtuales que residen en el volumen respectivo se replican en el destino CRR. Asegúrese de seleccionar todas las máquinas virtuales que forman parte del almacén de datos, porque solo se procesan las máquinas virtuales que forman parte del plan de replicación.



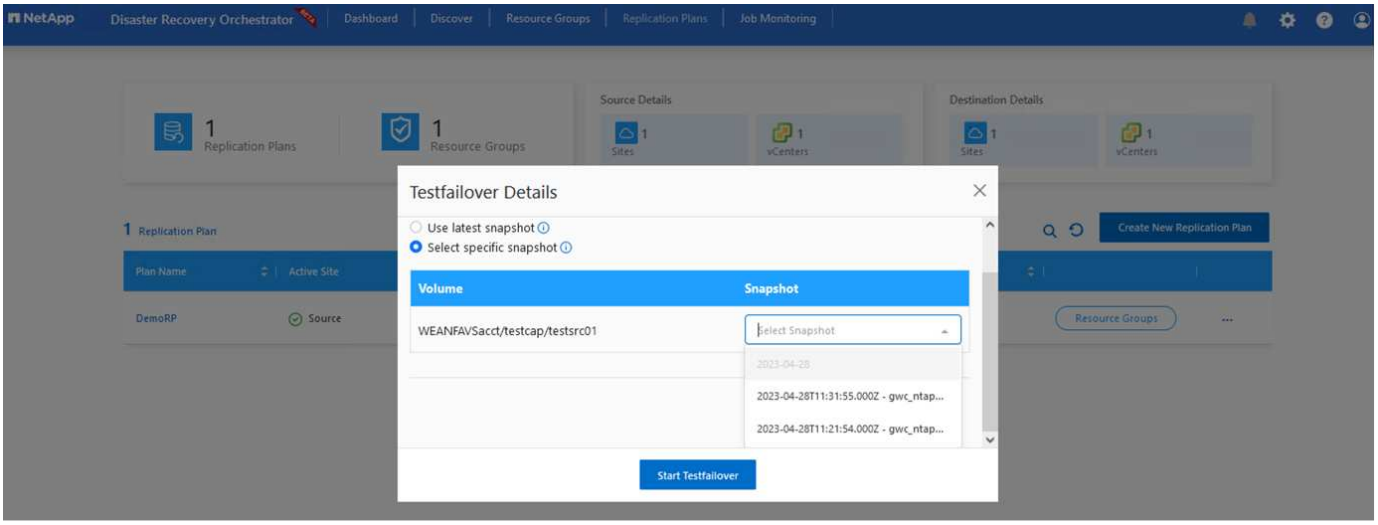
8. En Detalles de la máquina virtual, puede modificar opcionalmente el tamaño de los parámetros de CPU y RAM de la máquina virtual. Esto puede ser muy útil cuando se recuperan entornos grandes en clústeres de destino más pequeños o cuando se realizan pruebas de recuperación ante desastres sin tener que aprovisionar una infraestructura física VMware uno a uno. Además, modifique el orden de arranque y el retraso de arranque (segundos) para todas las máquinas virtuales seleccionadas en los grupos de recursos. Hay una opción adicional para modificar el orden de arranque si se requieren cambios respecto de lo seleccionado durante la selección del orden de arranque del grupo de recursos. De forma predeterminada, se utiliza el orden de arranque seleccionado durante la selección del grupo de recursos, sin embargo, cualquier modificación se puede realizar en esta etapa.



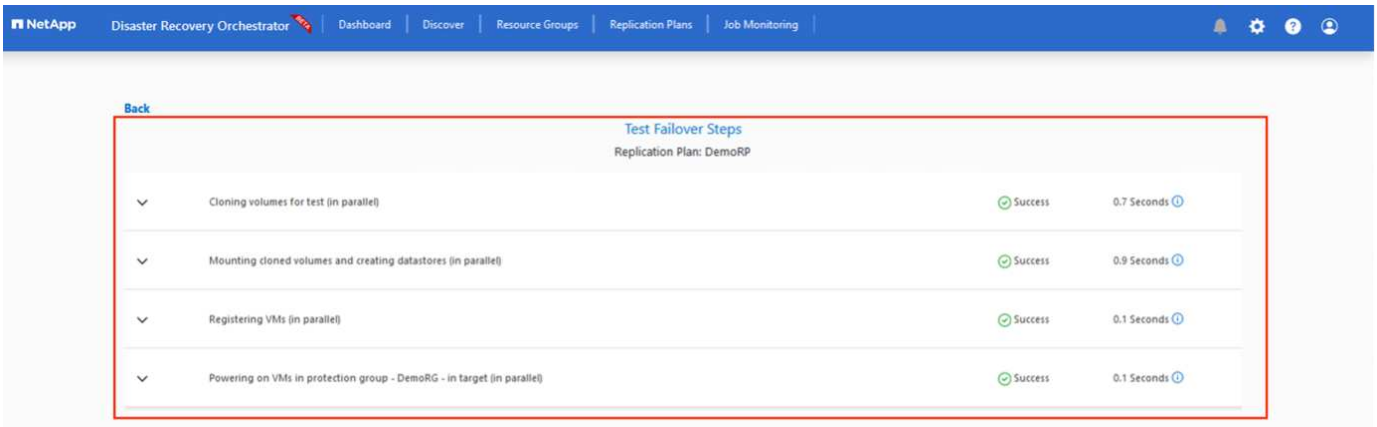
9. Haga clic en **Crear plan de replicación**. Una vez creado el plan de replicación, puede ejecutar las opciones de conmutación por error, conmutación por error de prueba o migración según sus requisitos.



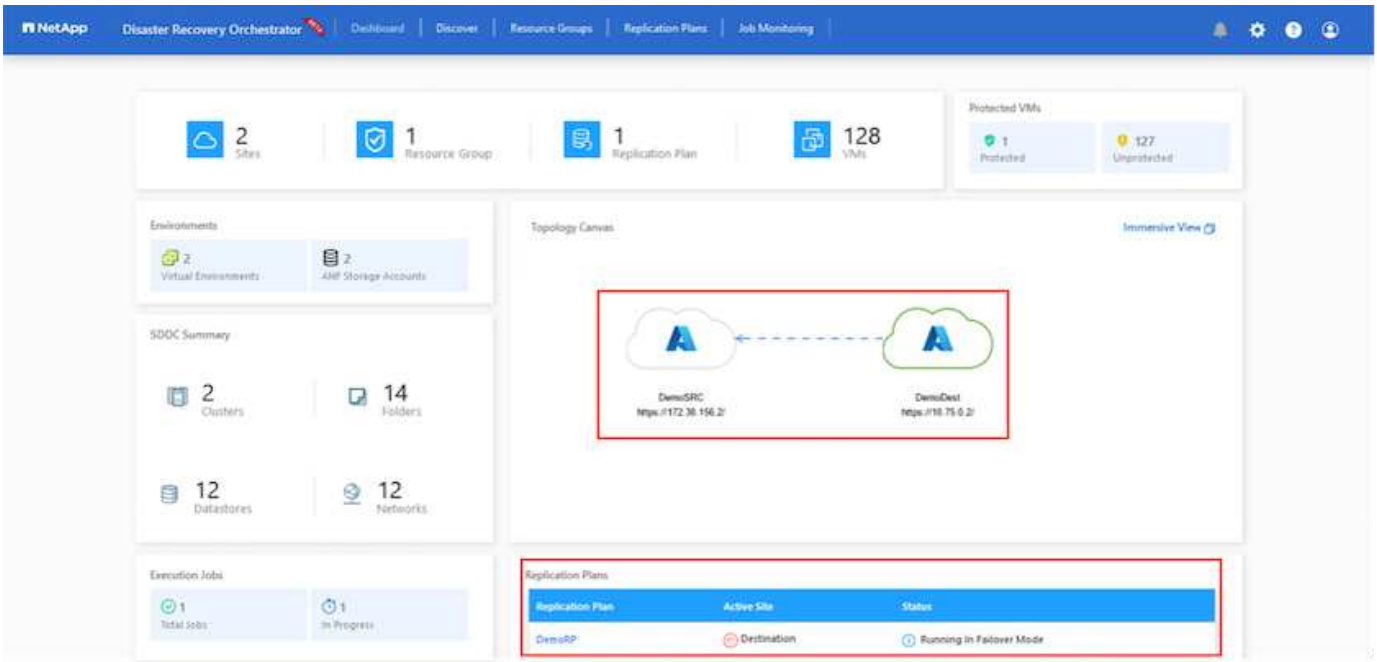
Durante las opciones de conmutación por error y conmutación por error de prueba, se utiliza la instantánea más reciente o se puede seleccionar una instantánea específica de una instantánea de un momento determinado. La opción de punto en el tiempo puede ser muy beneficiosa si se enfrenta a un evento de corrupción como ransomware, donde las réplicas más recientes ya están comprometidas o cifradas. DRO muestra todos los puntos de tiempo disponibles.



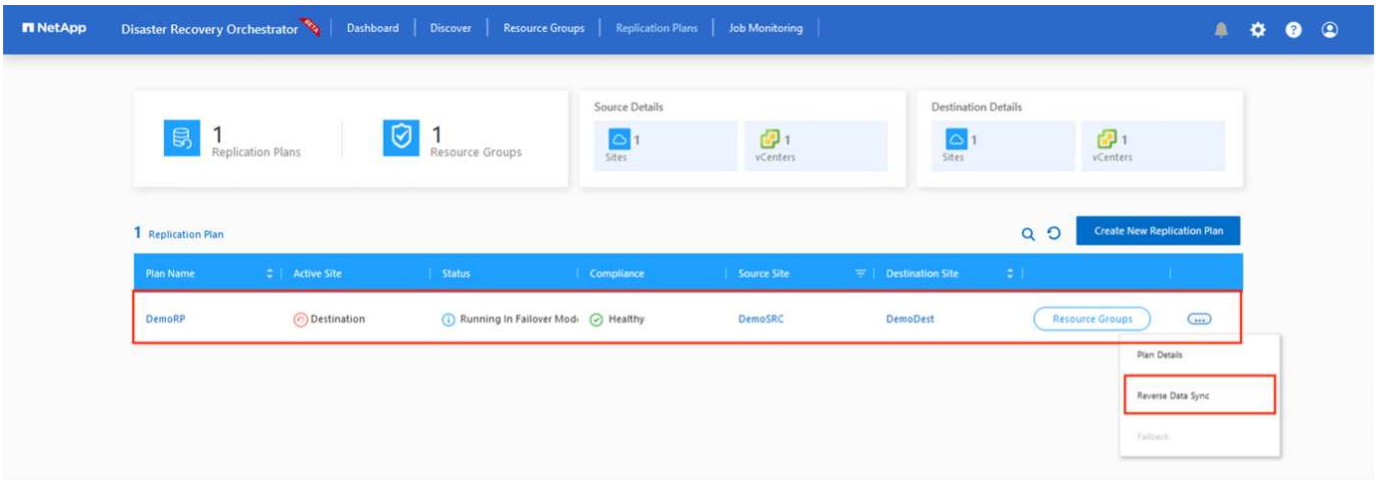
Para activar o probar la conmutación por error con la configuración especificada en el plan de replicación, puede hacer clic en **Conmutación por error** o **Probar conmutación por error**. Puede supervisar el plan de replicación en el menú de tareas.



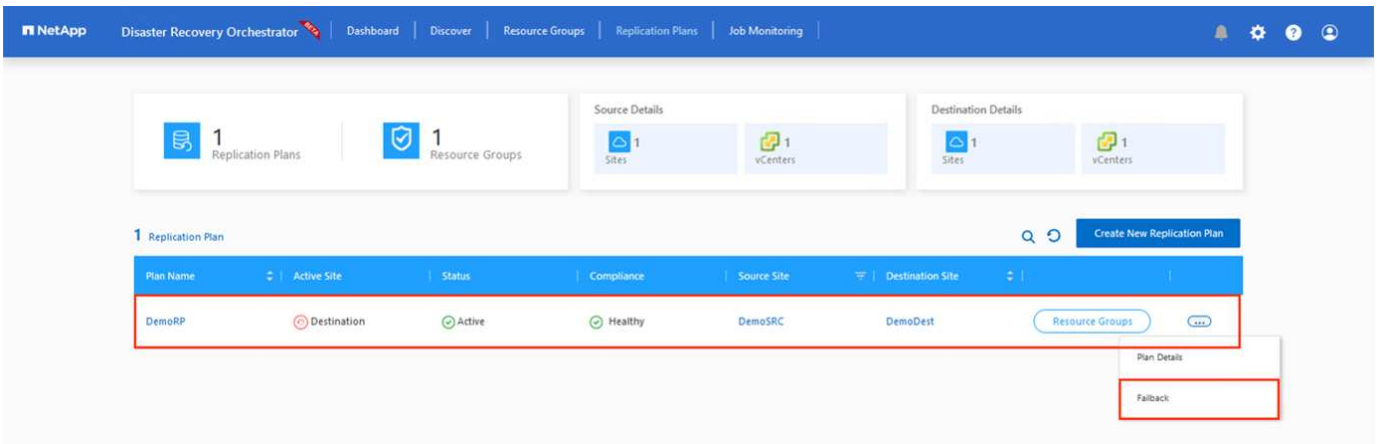
Una vez activada la conmutación por error, los elementos recuperados se pueden ver en el vCenter del SDDC de AVS del sitio secundario (máquinas virtuales, redes y almacenes de datos). De forma predeterminada, las máquinas virtuales se recuperan en la carpeta de carga de trabajo.

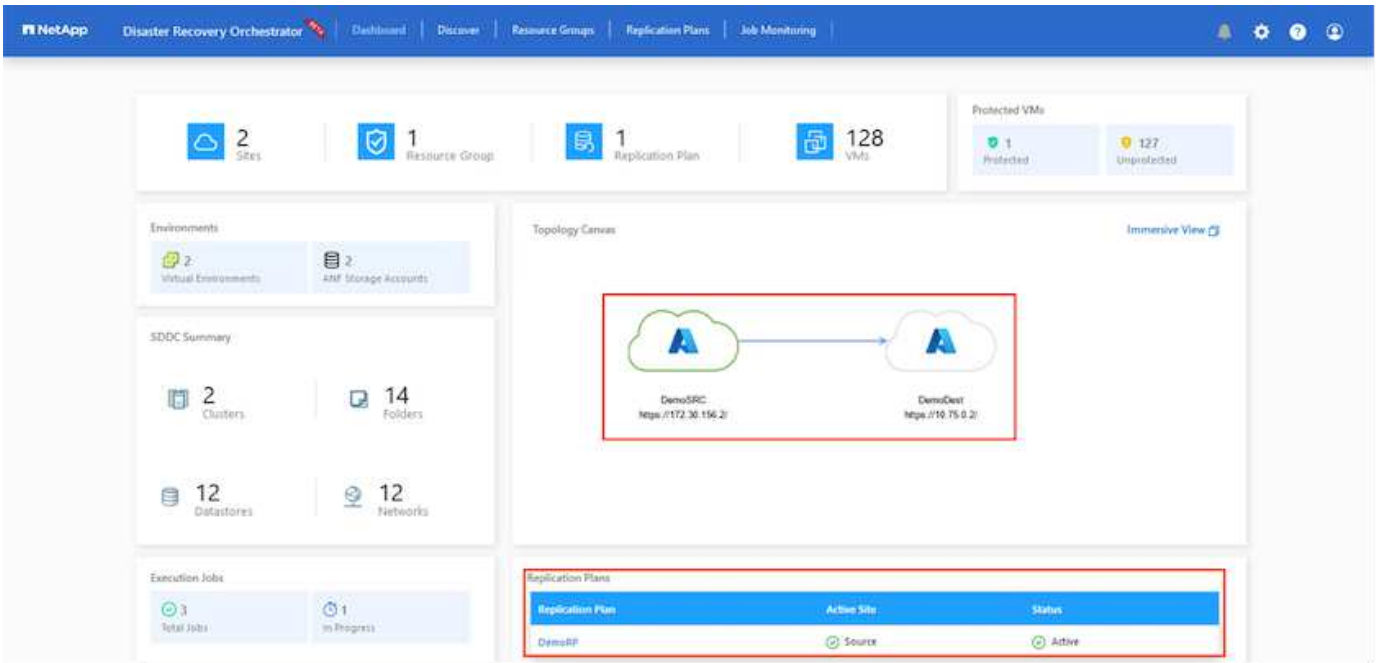


La conmutación por recuperación se puede activar en el nivel del plan de replicación. En caso de una conmutación por error de prueba, se puede utilizar la opción de desmantelamiento para revertir los cambios y eliminar el volumen recién creado. Las recuperaciones relacionadas con la conmutación por error son un proceso de dos pasos. Seleccione el plan de replicación y seleccione **Sincronización inversa de datos**.



Una vez completado este paso, active la conmutación por error para regresar al sitio AVS principal.





Desde el portal de Azure, podemos ver que se ha interrumpido el estado de la replicación para los volúmenes adecuados que se asignaron al SDDC de AVS del sitio secundario como volúmenes de lectura y escritura. Durante la conmutación por error de prueba, DRO no asigna el volumen de destino ni de réplica. En lugar de

ello, crea un nuevo volumen de la instantánea de replicación entre regiones requerida y expone el volumen como un almacén de datos, lo que consume capacidad física adicional del grupo de capacidad y garantiza que el volumen de origen no se modifique. En particular, los trabajos de replicación pueden continuar durante las pruebas de recuperación ante desastres o los flujos de trabajo de clasificación. Además, este proceso garantiza que la recuperación se pueda limpiar sin el riesgo de que la réplica se destruya si ocurren errores o se recuperan datos dañados.

Recuperación de ransomware

Recuperarse de un ransomware puede ser una tarea abrumadora. En concreto, puede resultar difícil para las organizaciones de TI determinar cuál es el punto de retorno seguro y, una vez determinado, cómo garantizar que las cargas de trabajo recuperadas estén protegidas de ataques recurrentes (por ejemplo, de malware inactivo o de aplicaciones vulnerables).

DRO aborda estas preocupaciones al permitir que las organizaciones se recuperen desde cualquier momento disponible. Las cargas de trabajo luego se recuperan en redes funcionales pero aisladas, de modo que las aplicaciones puedan funcionar y comunicarse entre sí pero no queden expuestas a ningún tráfico norte-sur. Este proceso brinda a los equipos de seguridad un lugar seguro para realizar análisis forenses e identificar cualquier malware oculto o inactivo.

Conclusión

La solución de recuperación ante desastres de Azure NetApp Files y Azure VMware le brindan los siguientes beneficios:

- Aproveche la replicación entre regiones eficiente y resistente de Azure NetApp Files .
- Recupere cualquier punto en el tiempo disponible con retención de instantáneas.
- Automatice completamente todos los pasos necesarios para recuperar cientos a miles de máquinas virtuales de los pasos de almacenamiento, computación, red y validación de aplicaciones.
- La recuperación de carga de trabajo aprovecha el proceso "Crear nuevos volúmenes a partir de las instantáneas más recientes", que no manipula el volumen replicado.
- Evite cualquier riesgo de corrupción de datos en los volúmenes o instantáneas.
- Evite interrupciones de replicación durante los flujos de trabajo de pruebas de DR.
- Aproveche los datos de DR y los recursos de computación en la nube para flujos de trabajo más allá de DR, como desarrollo y prueba, pruebas de seguridad, pruebas de parches y actualizaciones, y pruebas de remediación.
- La optimización de la CPU y la RAM puede ayudar a reducir los costos de la nube al permitir la recuperación a clústeres de cómputo más pequeños.

Dónde encontrar información adicional

Para obtener más información sobre la información que se describe en este documento, revise los siguientes documentos y/o sitios web:

- Crear replicación de volumen para Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Replicación entre regiones de volúmenes de Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-

level-objectives"

- "Solución VMware de Azure"

  "https://learn.microsoft.com/en-us/azure/azure-vmware/introduction"

- Implementar y configurar el entorno de virtualización en Azure

  "Configurar AVS en Azure"

- Implementar y configurar Azure VMware Solution

  https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal

Información de copyright

Copyright © 2025 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.