# Documentación de recuperación ante desastres de NetApp

## NetApp Disaster Recovery

NetApp
October 06, 2025

# Tabla de contenidos

# Documentación de recuperación ante desastres de NetApp

# Notas de la versión

## Novedades en NetApp Disaster Recovery

Descubra las novedades en NetApp Disaster Recovery.

### 6 de octubre de 2025

#### La BlueXP disaster recovery ahora es NetApp Disaster Recovery

La BlueXP disaster recovery ha pasado a llamarse Recuperación ante desastres de NetApp .

#### BlueXP ahora es NetApp Console

La consola NetApp , construida sobre la base BlueXP mejorada y reestructurada, proporciona una gestión centralizada del almacenamiento NetApp y de los servicios de datos NetApp en entornos locales y en la nube a nivel empresarial, brindando información en tiempo real, flujos de trabajo más rápidos y una administración simplificada, que es altamente segura y compatible.

Para obtener más detalles sobre lo que ha cambiado, consulte la"Notas de la versión de la consola de NetApp" .

#### Otras actualizaciones

- El soporte para Amazon Elastic VMware Service (EVS) con Amazon FSx for NetApp ONTAP estaba en una vista previa pública. Con este lanzamiento, ahora está disponible de forma generalizada. Para más detalles, consulte"Introducción de NetApp Disaster Recovery mediante Amazon Elastic VMware Service y Amazon FSx for NetApp ONTAP" .
- Mejoras en el descubrimiento de almacenamiento, incluidos tiempos de descubrimiento reducidos para implementaciones locales
- Compatibilidad con gestión de identidad y acceso (IAM), incluido el control de acceso basado en roles (RBAC) y permisos de usuario mejorados
- Compatibilidad de vista previa privada con la solución VMware de Azure y Cloud Volumes ONTAP. Con este soporte, ahora puede configurar la protección de recuperación ante desastres desde las instalaciones locales hasta la solución VMware de Azure mediante el almacenamiento de Cloud Volumes ONTAP .

### 04 de agosto de 2025

Versión 4.2.5P2

#### Actualizaciones de NetApp Disaster Recovery

Esta versión incluye las siguientes actualizaciones:

- Se mejoró la compatibilidad de VMFS para manejar el mismo LUN presentado desde múltiples máquinas virtuales de almacenamiento.
- Se mejoró la limpieza de desmontaje de prueba para controlar el almacén de datos que ya se está desmontando o eliminando.
- Se mejoró el mapeo de subredes para que ahora valide que la puerta de enlace ingresada esté contenida dentro de la red proporcionada.

- Se corrigió un problema que podía provocar que el plan de replicación fallara si el nombre de la máquina virtual contenía ".com".
- Se eliminó una restricción que impedía que el volumen de destino fuera el mismo que el volumen de origen al crear el volumen como parte de la creación del plan de replicación.
- Se agregó soporte para una suscripción de pago por uso (PAYGO) a NetApp Intelligent Services en Azure Marketplace y se agregó un vínculo a Azure Marketplace en el cuadro de diálogo de prueba gratuita.

  Para más detalles, véase "Licencias de recuperación ante desastres de NetApp" y "Configurar licencias para NetApp Disaster Recovery" .

## 14 de julio de 2025

Versión 4.2.5

### Roles de usuario en NetApp Disaster Recovery

NetApp Disaster Recovery ahora emplea roles para gobernar el acceso que tiene cada usuario a funciones y acciones específicas.

El servicio utiliza los siguientes roles que son específicos de NetApp Disaster Recovery.

- **Administrador de recuperación ante desastres**: realiza cualquier acción en NetApp Disaster Recovery.
- **Administrador de conmutación por error de recuperación ante desastres**: realiza acciones de conmutación por error y migración en NetApp Disaster Recovery.
- **Administrador de aplicaciones de recuperación ante desastres**: crear y modificar planes de replicación e iniciar conmutaciones por error de prueba.
- **Visor de recuperación ante desastres**: ve información en NetApp Disaster Recovery, pero no puede realizar ninguna acción.

Si hace clic en el servicio NetApp Disaster Recovery y lo configura por primera vez, debe tener el permiso **SnapCenterAdmin** o el rol **Organization Admin**.

Para obtener más información, consulte "Roles y permisos de usuario en NetApp Disaster Recovery" .

"Obtenga información sobre los roles de acceso para todos los servicios" .

### Otras actualizaciones en NetApp Disaster Recovery

- Descubrimiento de red mejorado
- Mejoras de escalabilidad:
  - Filtrado de los metadatos requeridos en lugar de todos los detalles
  - Mejoras en el descubrimiento para recuperar y actualizar recursos de máquinas virtuales más rápidamente
  - Optimización de la memoria y optimización del rendimiento para la recuperación y actualización de datos
  - Mejoras en la creación de clientes y la gestión de grupos de vCenter SDK
- Gestión de datos obsoletos en el próximo descubrimiento programado o manual:
  - Cuando se elimina una máquina virtual en vCenter, NetApp Disaster Recovery ahora la elimina

automáticamente del plan de replicación.

  - Cuando se elimina un almacén de datos o una red en vCenter, NetApp Disaster Recovery ahora lo elimina del plan de replicación y del grupo de recursos.
  - Cuando se elimina un clúster, un host o un centro de datos en vCenter, NetApp Disaster Recovery ahora lo elimina del plan de replicación y del grupo de recursos.

- Ahora puedes acceder a la documentación de Swagger en el modo de incógnito de tu navegador. Puede acceder a él desde NetApp Disaster Recovery desde la opción Configuración > Documentación de API o directamente en la siguiente URL en el modo incógnito de su navegador: "Documentación de Swagger" .
- En algunas situaciones, después de una operación de conmutación por error, el iGroup quedó abandonado una vez completada la operación. Esta actualización elimina el iGroup si está obsoleto.
- Si se utilizó el FQDN de NFS en el plan de replicación, NetApp Disaster Recovery ahora lo resuelve en una dirección IP. Esta actualización es útil si el FQDN no se puede resolver en el sitio de recuperación ante desastres.
- Mejoras en la alineación de la interfaz de usuario
- Mejoras en el registro para capturar los detalles de tamaño de vCenter después del descubrimiento exitoso

## 30 de junio de 2025

Versión 4.2.4P2

#### Mejoras en el descubrimiento

Esta actualización mejora el proceso de descubrimiento, lo que reduce el tiempo necesario para realizarlo.

## 23 de junio de 2025

Versión 4.2.4P1

#### Mejoras en el mapeo de subredes

Esta actualización mejora el cuadro de diálogo Agregar y editar mapeo de subred con una nueva funcionalidad de búsqueda. Ahora puede encontrar rápidamente subredes específicas ingresando términos de búsqueda, lo que facilita la administración de las asignaciones de subredes.

## 9 de junio de 2025

Versión 4.2.4

#### Compatibilidad con la solución de contraseña de administrador local de Windows (LAPS)

La Solución de contraseña de administrador local de Windows (Windows LAPS) es una función de Windows que administra y realiza copias de seguridad automáticamente de la contraseña de una cuenta de administrador local en Active Directory.

Ahora puede seleccionar las opciones de mapeo de subred y marcar la opción LAPS proporcionando los detalles del controlador de dominio. Al utilizar esta opción, no es necesario proporcionar una contraseña para cada una de sus máquinas virtuales.

Para más detalles, consulte "Crear un plan de replicación" .

## 13 de mayo de 2025

Versión 4.2.3

### Mapeo de subredes

Con esta versión, puede administrar direcciones IP en conmutación por error de una nueva manera mediante el mapeo de subredes, que le permite agregar subredes para cada vCenter. Al hacerlo, define el CIDR IPv4, la puerta de enlace predeterminada y el DNS para cada red virtual.

En caso de conmutación por error, NetApp Disaster Recovery determina la dirección IP adecuada de cada vNIC observando el CIDR proporcionado para la red virtual asignada y lo utiliza para derivar la nueva dirección IP.

Por ejemplo:

- RedA = 10.1.1.0/24
- RedB = 192.168.1.0/24

VM1 tiene una vNIC (10.1.1.50) que está conectada a NetworkA. La red A se asigna a la red B en la configuración del plan de replicación.

En caso de conmutación por error, NetApp Disaster Recovery reemplaza la parte de red de la dirección IP original (10.1.1) y conserva la dirección de host (.50) de la dirección IP original (10.1.1.50). Para VM1, NetApp Disaster Recovery analiza la configuración CIDR para NetworkB y utiliza la parte de red de NetworkB 192.168.1 mientras conserva la parte del host (.50) para crear la nueva dirección IP para VM1. La nueva IP pasa a ser 192.168.1.50.

En resumen, la dirección del host permanece igual, mientras que la dirección de red se reemplaza con la que esté configurada en la asignación de subred del sitio. Esto le permite administrar la reasignación de direcciones IP en caso de conmutación por error con mayor facilidad, especialmente si tiene cientos de redes y miles de máquinas virtuales para administrar.

Para obtener detalles sobre cómo incluir la asignación de subredes en sus sitios, consulte "Agregar sitios de servidor vCenter" .

### Protección contra saltos

Ahora puede omitir la protección para que el servicio no cree automáticamente una relación de protección inversa después de una conmutación por error del plan de replicación. Esto es útil si desea realizar operaciones adicionales en el sitio restaurado antes de volver a ponerlo en línea dentro de NetApp Disaster Recovery.

Cuando se inicia una conmutación por error, de manera predeterminada el servicio crea automáticamente una relación de protección inversa para cada volumen en el plan de replicación, si el sitio de origen original está en línea. Esto significa que el servicio crea una relación SnapMirror desde el sitio de destino hasta el sitio de origen. El servicio también revierte automáticamente la relación SnapMirror cuando se inicia una conmutación por recuperación.

Al iniciar una conmutación por error, ahora puede elegir la opción **Omitir protección**. Con esto, el servicio no revierte automáticamente la relación SnapMirror . En lugar de ello, deja el volumen escribible en ambos lados del plan de replicación.

Una vez que el sitio de origen original vuelva a estar en línea, puede establecer una protección inversa seleccionando **Proteger recursos** en el menú Acciones del plan de replicación. Esto intenta crear una

relación de replicación inversa para cada volumen del plan. Puede ejecutar este trabajo repetidamente hasta que se restablezca la protección. Cuando se restablezca la protección, puede iniciar una conmutación por error de la forma habitual.

Para obtener más detalles sobre cómo omitir la protección, consulte "Conmutar por error las aplicaciones a un sitio remoto" .

#### Actualizaciones de programación de SnapMirror en el plan de replicación

NetApp Disaster Recovery ahora admite el uso de soluciones de gestión de instantáneas externas, como el programador de políticas nativo ONTAP SnapMirror o integraciones de terceros con ONTAP. Si cada almacén de datos (volumen) en el plan de replicación ya tiene una relación SnapMirror que se administra en otro lugar, puede usar esas instantáneas como puntos de recuperación en NetApp Disaster Recovery.

Para configurar, en la sección Plan de replicación > Asignación de recursos, marque la casilla de verificación **Usar copias de seguridad administradas por la plataforma y programas de retención** al configurar la asignación de almacenes de datos.

Cuando se selecciona la opción, NetApp Disaster Recovery no configura una programación de respaldo. Sin embargo, aún es necesario configurar un programa de retención porque aún se podrían tomar instantáneas para operaciones de prueba, conmutación por error y recuperación.

Una vez configurado esto, el servicio no toma ninguna instantánea programada regularmente, sino que depende de la entidad externa para tomar y actualizar esas instantáneas.

Para obtener detalles sobre el uso de soluciones de instantáneas externas en el plan de replicación, consulte "Crear un plan de replicación" .

## 16 de abril de 2025

Versión 4.2.2

#### Descubrimiento programado para máquinas virtuales

NetApp Disaster Recovery realiza el descubrimiento una vez cada 24 horas. Con esta versión, ahora puede personalizar el programa de descubrimiento para satisfacer sus necesidades y reducir el impacto en el rendimiento cuando lo necesite. Por ejemplo, si tiene una gran cantidad de máquinas virtuales, puede configurar la programación de descubrimiento para que se ejecute cada 48 horas. Si tiene una pequeña cantidad de máquinas virtuales, puede configurar la programación de detección para que se ejecute cada 12 horas.

Si no desea programar el descubrimiento, puede deshabilitar la opción de descubrimiento programado y actualizar el descubrimiento manualmente en cualquier momento.

Para más detalles, consulte "Agregar sitios de servidor vCenter" .

#### Compatibilidad con almacenes de datos de grupos de recursos

Anteriormente, solo se podían crear grupos de recursos por máquinas virtuales. Con esta versión, puede crear un grupo de recursos por almacenes de datos. Cuando crea un plan de replicación y crea un grupo de recursos para ese plan, se enumerarán todas las máquinas virtuales en un almacén de datos. Esto es útil si tiene una gran cantidad de máquinas virtuales y desea agruparlas por almacén de datos.

Puede crear un grupo de recursos con un almacén de datos de las siguientes maneras:

- Cuando agrega un grupo de recursos mediante almacenes de datos, puede ver una lista de almacenes de datos. Puede seleccionar uno o más almacenes de datos para crear un grupo de recursos.
- Cuando crea un plan de replicación y crea un grupo de recursos dentro del plan, puede ver las máquinas virtuales en los almacenes de datos.

Para más detalles, consulte "Crear un plan de replicación" .

#### Notificaciones de prueba gratuita o vencimiento de licencia

Este comunicado proporciona notificaciones de que la prueba gratuita expirará en 60 días para garantizar que tenga tiempo de obtener una licencia. Esta versión también proporciona notificaciones el día en que vence la licencia.

#### Notificación de actualizaciones del servicio

Con esta versión, aparece un banner en la parte superior para indicar que los servicios se están actualizando y que el servicio se coloca en modo de mantenimiento. El banner aparece cuando se está actualizando el servicio y desaparece cuando se completa la actualización. Si bien puede continuar trabajando en la interfaz de usuario mientras la actualización está en progreso, no puede enviar nuevos trabajos. Los trabajos programados se ejecutarán después de que se complete la actualización y el servicio vuelva al modo de producción.

## 10 de marzo de 2025

Versión 4.2.1

#### Soporte de proxy inteligente

El agente de la consola de NetApp admite proxy inteligente. El proxy inteligente es una forma liviana, segura y eficiente de conectar su sistema local a NetApp Disaster Recovery. Proporciona una conexión segura entre su sistema y NetApp Disaster Recovery sin necesidad de una VPN o acceso directo a Internet. Esta implementación de proxy optimizada descarga el tráfico de API dentro de la red local.

Cuando se configura un proxy, NetApp Disaster Recovery intenta comunicarse directamente con VMware o ONTAP y utiliza el proxy configurado si falla la comunicación directa.

La implementación del proxy de recuperación ante desastres de NetApp requiere comunicación del puerto 443 entre el agente de la consola y cualquier servidor vCenter y matriz ONTAP que utilice un protocolo HTTPS. El agente de recuperación ante desastres de NetApp dentro del agente de consola se comunica directamente con VMware vSphere, VC u ONTAP cuando realiza cualquier acción.

Para obtener más información sobre el proxy inteligente para NetApp Disaster Recovery, consulte "Configure su infraestructura para NetApp Disaster Recovery" .

Para obtener más información sobre la configuración general del proxy en la consola de NetApp , consulte "Configurar el agente de la consola para utilizar un servidor proxy" .

#### Finaliza la prueba gratuita en cualquier momento

Puedes detener la prueba gratuita en cualquier momento o esperar hasta que caduque.

Ver "Finalizar la prueba gratuita" .

## 19 de febrero de 2025

Versión 4.2

### Compatibilidad de ASA r2 con máquinas virtuales y almacenes de datos en almacenamiento VMFS

Esta versión de NetApp Disaster Recovery proporciona soporte para ASA r2 para máquinas virtuales y almacenes de datos en almacenamiento VMFS. En un sistema ASA r2, el software ONTAP admite la funcionalidad SAN esencial y elimina funciones que no son compatibles con los entornos SAN.

Esta versión admite las siguientes funciones para ASA r2:

- Aprovisionamiento de grupo de consistencia para almacenamiento primario (solo grupo de consistencia plano, es decir, solo un nivel sin una estructura jerárquica)
- Operaciones de copia de seguridad (grupo de consistencia), incluida la automatización de SnapMirror

El soporte para ASA r2 en NetApp Disaster Recovery utiliza ONTAP 9.16.1.

Si bien los almacenes de datos se pueden montar en un volumen ONTAP o en una unidad de almacenamiento ASA r2, un grupo de recursos en NetApp Disaster Recovery no puede incluir un almacén de datos de ONTAP y uno de ASA r2. Puede seleccionar un almacén de datos de ONTAP o un almacén de datos de ASA r2 en un grupo de recursos.

## 30 de octubre de 2024

### Informes

Ahora puede generar y descargar informes que le ayudarán a analizar su panorama. Los informes prediseñados resumen las conmutaciones por error y por recuperación, muestran detalles de replicación en todos los sitios y muestran detalles de trabajos de los últimos siete días.

Referirse a "Crear informes de recuperación ante desastres" .

### Prueba gratuita de 30 días

Ahora puede registrarse para una prueba gratuita de 30 días de NetApp Disaster Recovery. Anteriormente, las pruebas gratuitas duraban 90 días.

Referirse a "Configurar licencias" .

### Deshabilitar y habilitar planes de replicación

Una versión anterior incluía actualizaciones a la estructura del cronograma de pruebas de conmutación por error, que era necesario para soportar cronogramas diarios y semanales. Esta actualización requiere que deshabilite y vuelva a habilitar todos los planes de replicación existentes para poder utilizar los nuevos programas de pruebas de conmutación por error diarios y semanales. Este es un requisito único.

Aquí te explicamos cómo:

1. Desde el menú, seleccione **Planes de replicación**.
2. Seleccione un plan y seleccione el ícono Acciones para mostrar el menú desplegable.
3. Seleccione **Deshabilitar**.

4. Después de unos minutos, seleccione **Habilitar**.

### Mapeo de carpetas

Cuando crea un plan de replicación y asigna recursos informáticos, ahora puede asignar carpetas para que las máquinas virtuales se recuperen en una carpeta que especifique para el centro de datos, el clúster y el host.

Para más detalles, consulte "Crear un plan de replicación" .

### Detalles de la máquina virtual disponibles para conmutación por error, recuperación y conmutación por error de prueba

Cuando ocurre una falla y usted está iniciando una conmutación por error, realizando una conmutación por recuperación o probando la conmutación por error, ahora puede ver los detalles de las máquinas virtuales e identificar cuáles no se reiniciaron.

Referirse a "Conmutar por error las aplicaciones a un sitio remoto" .

### Retraso en el arranque de la máquina virtual con secuencia de arranque ordenada

Al crear un plan de replicación, ahora puede establecer un retraso de arranque para cada máquina virtual en el plan. Esto le permite establecer una secuencia para que las máquinas virtuales se inicien a fin de garantizar que todas las máquinas virtuales de prioridad uno se estén ejecutando antes de que se inicien las máquinas virtuales de prioridad posterior.

Para más detalles, consulte "Crear un plan de replicación" .

### Información del sistema operativo de la máquina virtual

Al crear un plan de replicación, ahora puede ver el sistema operativo de cada máquina virtual en el plan. Esto es útil para decidir cómo agrupar las máquinas virtuales en un grupo de recursos.

Para más detalles, consulte "Crear un plan de replicación" .

### Alias de nombres de máquinas virtuales

Al crear un plan de replicación, ahora puede agregar un prefijo y un sufijo a los nombres de las máquinas virtuales en el sitio de recuperación ante desastres. Esto le permite utilizar un nombre más descriptivo para las máquinas virtuales en el plan.

Para más detalles, consulte "Crear un plan de replicación" .

### Limpiar instantáneas antiguas

Puede eliminar cualquier instantánea que ya no necesite más allá del recuento de retención especificado. Las instantáneas pueden acumularse con el tiempo cuando reduce el recuento de retención de instantáneas, y ahora puede eliminarlas para liberar espacio. Puede hacer esto en cualquier momento a pedido o cuando elimine un plan de replicación.

Para más detalles, consulte "Administrar sitios, grupos de recursos, planes de replicación, almacenes de datos e información de máquinas virtuales" .

### Conciliar instantáneas

Ahora puedes conciliar instantáneas que no están sincronizadas entre el origen y el destino. Esto podría ocurrir si se eliminan instantáneas en un destino fuera de NetApp Disaster Recovery. El servicio elimina la instantánea de la fuente automáticamente cada 24 horas. Sin embargo, puedes realizar esto bajo demanda. Esta función le permite garantizar que las instantáneas sean consistentes en todos los sitios.

Para más detalles, consulte "Administrar planes de replicación" .

## 20 de septiembre de 2024

### Compatibilidad con almacenes de datos VMware VMFS locales a locales

Esta versión incluye soporte para máquinas virtuales montadas en almacenes de datos del sistema de archivos de máquinas virtuales (VMFS) VMware vSphere para iSCSI y FC protegidos en almacenamiento local. Anteriormente, el servicio proporcionaba una *vista previa de tecnología* compatible con almacenes de datos VMFS para iSCSI y FC.

A continuación se presentan algunas consideraciones adicionales con respecto a los protocolos iSCSI y FC:

- El soporte de FC es para protocolos front-end del cliente, no para replicación.
- NetApp Disaster Recovery solo admite un único LUN por volumen ONTAP . El volumen no debe tener múltiples LUN.
- Para cualquier plan de replicación, el volumen ONTAP de destino debe utilizar los mismos protocolos que el volumen ONTAP de origen que aloja las máquinas virtuales protegidas. Por ejemplo, si el origen utiliza un protocolo FC, el destino también debe utilizar FC.

## 02 de agosto de 2024

### Compatibilidad con almacenes de datos VMware VMFS locales a locales para FC

Esta versión incluye una *vista previa tecnológica* de soporte para máquinas virtuales montadas en almacenes de datos del sistema de archivos de máquinas virtuales (VMFS) VMware vSphere para almacenamiento local protegido por FC. Anteriormente, el servicio proporcionaba una vista previa de la tecnología compatible con almacenes de datos VMFS para iSCSI.

NetApp no le cobrará por ninguna capacidad de carga de trabajo previsualizada.

### Cancelación de trabajo

Con esta versión, ahora puedes cancelar un trabajo en la interfaz de usuario del Monitor de trabajos.

Referirse a "Monitorear trabajos" .

## 17 de julio de 2024

### Programaciones de pruebas de conmutación por error

Esta versión incluye actualizaciones a la estructura del cronograma de pruebas de conmutación por error, que era necesario para soportar cronogramas diarios y semanales. Esta actualización requiere que deshabilite y vuelva a habilitar todos los planes de replicación existentes para poder utilizar los nuevos programas de pruebas de conmutación por error diarios y semanales. Este es un requisito único.

Aquí te explicamos cómo:

1. Desde el menú, seleccione **Planes de replicación**.
2. Seleccione un plan y seleccione el ícono Acciones para mostrar el menú desplegable.
3. Seleccione **Deshabilitar**.
4. Después de unos minutos, seleccione **Habilitar**.

#### Actualizaciones del plan de replicación

Esta versión incluye actualizaciones a los datos del plan de replicación, lo que resuelve un problema de "instantánea no encontrada". Esto requiere que cambie el recuento de retención en todos los planes de replicación a 1 e inicie una instantánea a pedido. Este proceso crea una nueva copia de seguridad y elimina todas las copias de seguridad anteriores.

Aquí te explicamos cómo:

1. Desde el menú, seleccione **Planes de replicación**.
2. Seleccione el plan de replicación, haga clic en la pestaña **Asignación de conmutación por error** y haga clic en el ícono de lápiz **Editar**.
3. Haga clic en la flecha **Almacenes de datos** para expandirla.
4. Tenga en cuenta el valor del recuento de retención en el plan de replicación. Necesitará restablecer este valor original cuando haya terminado con estos pasos.
5. Reduce el conteo a 1.
6. Inicie una instantánea a pedido. Para hacerlo, en la página del plan de replicación, seleccione el plan, haga clic en el ícono Acciones y seleccione **Tomar instantánea ahora**.
7. Una vez que el trabajo de instantánea se complete exitosamente, aumente el recuento en el plan de replicación a su valor original que anotó en el primer paso.
8. Repita estos pasos para todos los planes de replicación existentes.

## 05 de julio de 2024

Esta versión de NetApp Disaster Recovery incluye las siguientes actualizaciones:

#### Soporte para la serie AFF A

Esta versión es compatible con las plataformas de hardware NetApp AFF serie A.

#### Compatibilidad con almacenes de datos VMware VMFS locales a locales

Esta versión incluye una *vista previa tecnológica* de soporte para máquinas virtuales montadas en almacenes de datos del sistema de archivos de máquinas virtuales (VMFS) VMware vSphere protegidos en el almacenamiento local. Con esta versión, se admite la recuperación ante desastres en una vista previa de tecnología para cargas de trabajo de VMware locales en entornos de VMware locales con almacenes de datos VMFS.

NetApp no le cobrará por ninguna capacidad de carga de trabajo previsualizada.

### Actualizaciones del plan de replicación

Puede agregar un plan de replicación más fácilmente filtrando las máquinas virtuales por almacén de datos en la página Aplicaciones y seleccionando más detalles de destino en la página de mapeo de recursos. Referirse a "Crear un plan de replicación" .

### Editar planes de replicación

Con esta versión, se ha mejorado la página de asignaciones de conmutación por error para lograr mayor claridad.

Referirse a "Administrar planes" .

### Editar máquinas virtuales

Con esta versión, el proceso de edición de máquinas virtuales en el plan incluyó algunas mejoras menores en la interfaz de usuario.

Referirse a "Administrar máquinas virtuales" .

### Actualizaciones con conmutación por error

Antes de iniciar una conmutación por error, ahora puede determinar el estado de las máquinas virtuales y si están encendidas o apagadas. El proceso de conmutación por error ahora le permite tomar una instantánea ahora o elegir las instantáneas.

Referirse a "Conmutar por error las aplicaciones a un sitio remoto" .

### Programaciones de pruebas de conmutación por error

Ahora puede editar las pruebas de conmutación por error y establecer programaciones diarias, semanales y mensuales para las pruebas de conmutación por error.

Referirse a "Administrar planes" .

### Actualizaciones de la información de prerrequisitos

Se ha actualizado la información sobre los requisitos previos de NetApp Disaster Recovery.

Referirse a "Requisitos previos de NetApp Disaster Recovery" .

## 15 de mayo de 2024

Esta versión de NetApp Disaster Recovery incluye las siguientes actualizaciones:

### Replicación de cargas de trabajo de VMware desde un entorno local a otro local

Esta función ahora está disponible de forma general. Anteriormente era una versión preliminar de tecnología con funcionalidad limitada.

### Actualizaciones de licencias

Con NetApp Disaster Recovery, puede registrarse para una prueba gratuita de 90 días, comprar una suscripción de pago por uso (PAYGO) con Amazon Marketplace o traer su propia licencia (BYOL), que es un archivo de licencia de NetApp (NLF) que obtiene de su representante de ventas de NetApp o del sitio de

soporte de NetApp (NSS).

Para obtener detalles sobre la configuración de licencias para NetApp Disaster Recovery, consulte"Configurar licencias" .

"Obtenga más información sobre NetApp Disaster Recovery" .

## 05 de marzo de 2024

Esta es la versión de disponibilidad general de NetApp Disaster Recovery, que incluye las siguientes actualizaciones.

### Actualizaciones de licencias

Con NetApp Disaster Recovery, puede registrarse para una prueba gratuita de 90 días o traer su propia licencia (BYOL), que es un archivo de licencia de NetApp (NLF) que obtiene de su representante de ventas de NetApp . Puede utilizar el número de serie de la licencia para activar el BYOL en las suscripciones de la consola de NetApp . Los cargos de recuperación ante desastres de NetApp se basan en la capacidad aprovisionada de los almacenes de datos.

Para obtener detalles sobre la configuración de licencias para NetApp Disaster Recovery, consulte "Configurar licencias" .

Para obtener detalles sobre la administración de licencias para **todos** los servicios de datos de la consola de NetApp , consulte "Administrar licencias para todos los servicios de datos de la consola de NetApp" .

### Editar horarios

Con esta versión, ahora puede configurar cronogramas para probar pruebas de cumplimiento y conmutación por error para asegurarse de que funcionarán correctamente si las necesita.

Para más detalles, consulte "Crear el plan de replicación" .

## 01 de febrero de 2024

Esta versión preliminar de NetApp Disaster Recovery incluye las siguientes actualizaciones:

### Mejora de la red

Con esta versión, ahora puedes cambiar el tamaño de los valores de CPU y RAM de la máquina virtual. Ahora también puede seleccionar una red DHCP o una dirección IP estática para la VM.

- DHCP: si elige esta opción, proporcionará credenciales para la máquina virtual.
- IP estática: puede seleccionar la misma información o una diferente de la máquina virtual de origen. Si elige lo mismo que la fuente, no necesita ingresar credenciales. Por otro lado, si elige utilizar información diferente de la fuente, puede proporcionar las credenciales, la dirección IP, la máscara de subred, el DNS y la información de la puerta de enlace.

Para más detalles, consulte "Crear un plan de replicación" .

### Scripts personalizados

Ahora se pueden incluir como procesos posteriores a la conmutación por error. Con scripts personalizados, puede hacer que NetApp Disaster Recovery ejecute su script después de un proceso de conmutación por

error. Por ejemplo, puede utilizar un script personalizado para reanudar todas las transacciones de la base de datos una vez completada la conmutación por error.

Para más detalles, consulte "Conmutación por error a un sitio remoto" .

#### Relación de SnapMirror

Ahora puede crear una relación SnapMirror mientras desarrolla el plan de replicación. Anteriormente, era necesario crear la relación fuera de NetApp Disaster Recovery.

Para más detalles, consulte "Crear un plan de replicación" .

#### Grupos de consistencia

Al crear un plan de replicación, puede incluir máquinas virtuales de diferentes volúmenes y diferentes SVM. NetApp Disaster Recovery crea una instantánea de grupo de consistencia incluyendo todos los volúmenes y actualiza todas las ubicaciones secundarias.

Para más detalles, consulte "Crear un plan de replicación" .

#### Opción de retardo de encendido de la máquina virtual

Cuando crea un plan de replicación, puede agregar máquinas virtuales a un grupo de recursos. Con los grupos de recursos, puede establecer un retraso en cada máquina virtual para que se enciendan en una secuencia retrasada.

Para más detalles, consulte "Crear un plan de replicación" .

#### Copias de instantáneas consistentes con la aplicación

Puede especificar la creación de copias de instantáneas consistentes con la aplicación. El servicio inactivará la aplicación y luego tomará una instantánea para obtener un estado consistente de la aplicación.

Para más detalles, consulte "Crear un plan de replicación" .

## 11 de enero de 2024

Esta versión preliminar de NetApp Disaster Recovery incluye las siguientes actualizaciones:

#### Panel de control más rápido

Con esta versión, podrás acceder a la información de otras páginas desde el Panel de Control más rápidamente.

"Obtenga más información sobre la recuperación ante desastres de NetApp" .

## 20 de octubre de 2023

Esta versión preliminar de NetApp Disaster Recovery incluye las siguientes actualizaciones.

#### Proteja las cargas de trabajo de VMware locales basadas en NFS

Ahora, con NetApp Disaster Recovery, puede proteger sus cargas de trabajo VMware locales basadas en NFS contra desastres en otro entorno VMware local basado en NFS, además de la nube pública. NetApp Disaster

Recovery orquesta la finalización de los planes de recuperación ante desastres.

> Con esta oferta de vista previa, NetApp se reserva el derecho de modificar los detalles, el contenido y el cronograma de la oferta antes de la disponibilidad general.

"Obtenga más información sobre NetApp Disaster Recovery" .

## 27 de septiembre de 2023

Esta versión preliminar de NetApp Disaster Recovery incluye las siguientes actualizaciones:

### Actualizaciones del panel de control

Ahora puede hacer clic en las opciones del Panel de Control, lo que le permitirá revisar la información rápidamente con mayor facilidad. Además, el Panel de Control ahora muestra el estado de las conmutaciones por error y las migraciones.

Referirse a "Vea el estado de sus planes de recuperación ante desastres en el Panel de Control" .

### Actualizaciones del plan de replicación

- **RPO**: Ahora puede ingresar el Objetivo de punto de recuperación (RPO) y el recuento de retención en la sección Almacenes de datos del plan de replicación. Esto indica la cantidad de datos que deben existir que no sean más antiguos que el tiempo establecido. Si, por ejemplo, lo configura en 5 minutos, el sistema puede perder hasta 5 minutos de datos si ocurre un desastre sin afectar las necesidades críticas del negocio.

  Referirse a "Crear un plan de replicación" .

- **Mejoras de red**: al asignar redes entre ubicaciones de origen y destino en la sección de máquinas virtuales del plan de replicación, NetApp Disaster Recovery ahora ofrece dos opciones: DHCP o IP estática. Anteriormente solo se admitía DHCP. Para las direcciones IP estáticas, configure la subred, la puerta de enlace y los servidores DNS. Además, ahora puedes ingresar credenciales para máquinas virtuales.

  Referirse a "Crear un plan de replicación" .

- **Editar programaciones**: ahora puedes actualizar las programaciones del plan de replicación.

  Referirse a "Administrar recursos" .

- * Automatización de SnapMirror *: mientras crea el plan de replicación en esta versión, puede definir la relación de SnapMirror entre los volúmenes de origen y destino en una de las siguientes configuraciones:
  - 1 a 1
  - 1 a muchos en una arquitectura de abanico
  - Muchos a 1 como grupo de consistencia
  - Muchos a muchos

    Referirse a "Crear un plan de replicación" .

## 01 de agosto de 2023

### Vista previa de NetApp Disaster Recovery

La versión preliminar de NetApp Disaster Recovery es un servicio de recuperación ante desastres basado en la nube que automatiza los flujos de trabajo de recuperación ante desastres. Inicialmente, con la vista previa de NetApp Disaster Recovery, puede proteger sus cargas de trabajo VMware locales basadas en NFS que ejecutan almacenamiento NetApp en VMware Cloud (VMC) en AWS con Amazon FSx para ONTAP.

Con esta oferta de vista previa, NetApp se reserva el derecho de modificar los detalles, el contenido y el cronograma de la oferta antes de la disponibilidad general.

"Obtenga más información sobre NetApp Disaster Recovery" .

Esta versión incluye las siguientes actualizaciones:

### Actualización de los grupos de recursos para el orden de arranque

Cuando crea un plan de replicación o recuperación ante desastres, puede agregar máquinas virtuales a grupos de recursos funcionales. Los grupos de recursos le permiten colocar un conjunto de máquinas virtuales dependientes en grupos lógicos que cumplan con sus requisitos. Por ejemplo, los grupos podrían contener el orden de arranque que se puede ejecutar durante la recuperación. Con esta versión, cada grupo de recursos puede incluir una o más máquinas virtuales. Las máquinas virtuales se encenderán según la secuencia en que las incluya en el plan. Referirse a "Seleccionar aplicaciones para replicar y asignar grupos de recursos" .

### Verificación de replicación

Después de crear el plan de recuperación ante desastres o de replicación, identificar la recurrencia en el asistente e iniciar una replicación en un sitio de recuperación ante desastres, cada 30 minutos NetApp Disaster Recovery verifica que la replicación realmente se esté realizando de acuerdo con el plan. Puede supervisar el progreso en la página Monitor de trabajo. Consulte "Replicar aplicaciones a otro sitio" .

### El plan de replicación muestra los cronogramas de transferencia del objetivo del punto de recuperación (RPO)

Cuando crea un plan de replicación o recuperación ante desastres, selecciona las máquinas virtuales. En esta versión, ahora puede ver el SnapMirror asociado con cada uno de los volúmenes asociados con el almacén de datos o la máquina virtual. También puede ver los programas de transferencia de RPO que están asociados con el programa de SnapMirror . RPO le ayuda a determinar si su programa de copias de seguridad es suficiente para recuperarse después de un desastre. Referirse a "Crear un plan de replicación" .

### Actualización del monitor de trabajo

La página Monitor de trabajo ahora incluye una opción Actualizar para que pueda obtener un estado actualizado de las operaciones. Consulte "Supervisar trabajos de recuperación ante desastres" .

## 18 de mayo de 2023

Esta es la versión inicial de NetApp Disaster Recovery.

### Servicio de recuperación ante desastres basado en la nube

NetApp Disaster Recovery es un servicio de recuperación ante desastres basado en la nube que automatiza los flujos de trabajo de recuperación ante desastres. Inicialmente, con la vista previa de NetApp Disaster

Recovery, puede proteger sus cargas de trabajo VMware locales basadas en NFS que ejecutan almacenamiento NetApp en VMware Cloud (VMC) en AWS con Amazon FSx para ONTAP.

"Obtenga más información sobre NetApp Disaster Recovery" .

# Limitaciones en la recuperación ante desastres de NetApp

Las limitaciones conocidas identifican plataformas, dispositivos o funciones que no son compatibles con esta versión del servicio o que no interactúan correctamente con él.

## Espere hasta que se complete la conmutación por error antes de ejecutar el descubrimiento

Una vez finalizada una conmutación por error, no inicie la detección en el vCenter de origen manualmente. Espere hasta que finalice la conmutación por error y luego inicie la detección en el vCenter de origen.

## Es posible que la consola de NetApp no detecte Amazon FSx for NetApp ONTAP

A veces, la consola de NetApp no detecta Amazon FSx for NetApp ONTAP . Esto podría deberse a que las credenciales de FSx no eran correctas.

**Solución alternativa**: agregue el clúster Amazon FSx for NetApp ONTAP en la consola de NetApp y actualice periódicamente el clúster para mostrar cualquier cambio.

Si necesita eliminar el clúster ONTAP FSx de NetApp Disaster Recovery, complete los siguientes pasos:

1. En el agente de la consola de NetApp , use las opciones de conectividad de su proveedor de nube, conéctese a la máquina virtual Linux en la que se ejecuta el agente de la consola, reinicie el servicio "occm" usando el `docker restart occm` dominio.

Referirse a "Administrar agentes de consola existentes" .

1. En la página Sistemas de consola de NetApp , agregue nuevamente el sistema Amazon FSx para ONTAP y proporcione las credenciales de FSx.

   Referirse a "Cree un sistema de archivos Amazon FSx for NetApp ONTAP" .

2. Desde NetApp Disaster Recovery, seleccione **Sitios**, en la fila vCenter seleccione la opción **Acciones***  **y en el menú Acciones, seleccione *Actualizar** para actualizar la detección de FSx en NetApp Disaster Recovery.

   Esto redescubre el almacén de datos, sus máquinas virtuales y su relación de destino.

# Empezar

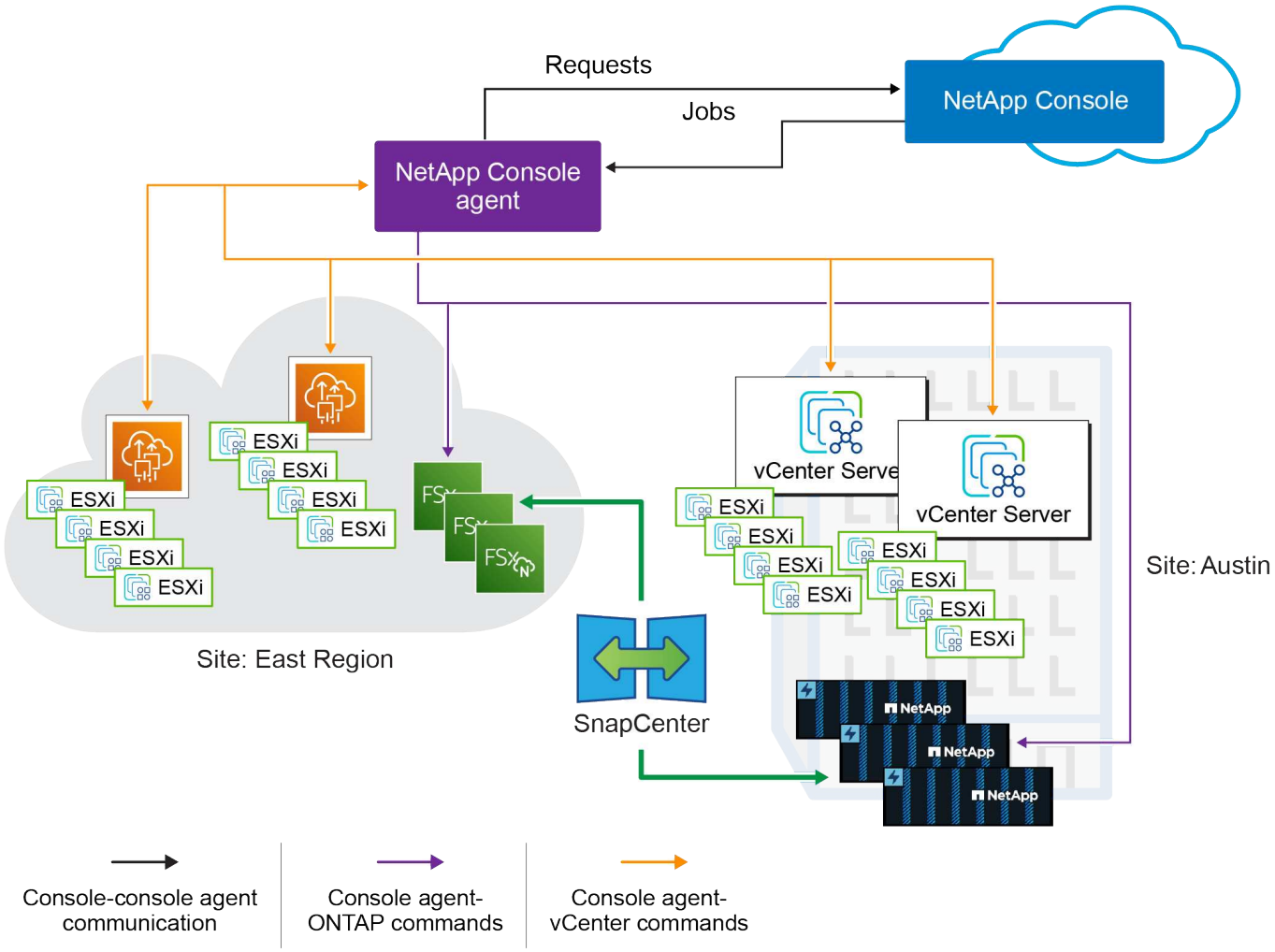
## Obtenga más información sobre NetApp Disaster Recovery para VMware

La recuperación ante desastres en la nube es una forma resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos de corrupción de datos. Con NetApp Disaster Recovery para VMware, puede replicar sus cargas de trabajo de almacén de datos o máquinas virtuales VMware locales que ejecutan almacenamiento ONTAP en un centro de datos definido por software VMware en una nube pública mediante almacenamiento en la nube de NetApp o en otro entorno VMware local con almacenamiento ONTAP como sitio de recuperación ante desastres. También puede utilizar Disaster Recovery para migrar cargas de trabajo de máquinas virtuales de un sitio a otro.

NetApp Disaster Recovery es un servicio de recuperación ante desastres basado en la nube que automatiza los flujos de trabajo de recuperación ante desastres. Con NetApp Disaster Recovery, puede proteger sus cargas de trabajo locales basadas en NFS y los almacenes de datos del sistema de archivos de máquina virtual (VMFS) VMware vSphere para iSCSI y FC que ejecutan almacenamiento NetApp en uno de los siguientes:

- VMware Cloud (VMC) en AWS con Amazon FSx for NetApp ONTAP
- Amazon Elastic VMware Service (EVS) con Amazon FSx for NetApp ONTAP Para obtener más detalles, consulte"Introducción de NetApp Disaster Recovery mediante Amazon Elastic VMware Service y Amazon FSx for NetApp ONTAP" .
- Azure VMware Solution (AVS) con NetApp Cloud Volumes ONTAP (iSCSI) (versión preliminar privada)
- Otro entorno VMware local basado en NFS y/o VMFS (iSCSI/FC) con almacenamiento ONTAP

NetApp Disaster Recovery utiliza la tecnología ONTAP SnapMirror con orquestación nativa VMware integrada para proteger las máquinas virtuales VMware y sus imágenes de sistema operativo en disco asociadas, al tiempo que conserva todos los beneficios de eficiencia de almacenamiento de ONTAP. La recuperación ante desastres utiliza estas tecnologías como transporte de replicación al sitio de recuperación ante desastres. Esto permite la mejor eficiencia de almacenamiento de la industria (compresión y deduplicación) en sitios primarios y secundarios.




## Consola de NetApp

Se puede acceder a NetApp Disaster Recovery a través de la consola de NetApp .

La consola de NetApp proporciona una gestión centralizada de los servicios de datos y almacenamiento de NetApp en entornos locales y en la nube a nivel empresarial. La consola es necesaria para acceder y utilizar los servicios de datos de NetApp . Como interfaz de administración, le permite administrar muchos recursos de almacenamiento desde una sola interfaz. Los administradores de la consola pueden controlar el acceso al almacenamiento y los servicios para todos los sistemas dentro de la empresa.

No necesita una licencia o suscripción para comenzar a usar NetApp Console y solo incurre en cargos cuando necesita implementar agentes de Console en su nube para garantizar la conectividad con sus sistemas de almacenamiento o servicios de datos de NetApp . Sin embargo, algunos servicios de datos de NetApp accesibles desde la consola requieren licencia o suscripción.

Obtenga más información sobre el "Consola de NetApp" .

## Beneficios de utilizar NetApp Disaster Recovery para VMware

NetApp Disaster Recovery ofrece los siguientes beneficios:

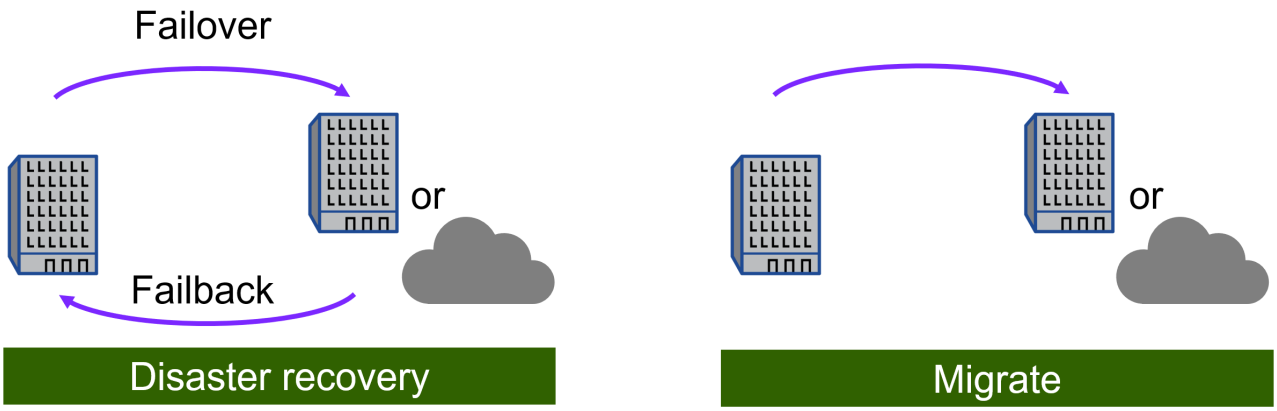
- Experiencia de usuario simplificada para el descubrimiento y la recuperación de aplicaciones de vCenter con múltiples operaciones de recuperación en puntos específicos del tiempo.

- Menor costo total de propiedad con menor costo de operaciones y capacidad de crear y ajustar planes de recuperación ante desastres con recursos mínimos.
- Preparación para la recuperación ante desastres continua con pruebas de conmutación por error virtual que no interrumpen las operaciones. Puede probar periódicamente sus planes de conmutación por error de DR sin afectar las cargas de trabajo de producción.
- Tiempos más rápidos para obtener valor con cambios dinámicos en su entorno de TI y capacidad de abordarlos en sus planes de recuperación ante desastres.
- Capacidad de administrar tanto las capas de almacenamiento como las virtuales a través de la orquestación de back-end de ONTAP y VMware al mismo tiempo sin la necesidad de contar con dispositivos de servidor virtuales (VSA) que deban implementarse y mantenerse.
- Las soluciones de recuperación ante desastres para VMware pueden consumir muchos recursos. Muchas soluciones de DR replican máquinas virtuales en la capa virtual de VMware mediante VSA, lo que puede consumir más recursos computacionales y perder la valiosa eficiencia de almacenamiento de ONTAP. Debido a que Disaster Recovery utiliza la tecnología ONTAP SnapMirror , puede replicar datos desde almacenes de datos de producción al sitio de DR utilizando nuestro modelo de replicación incremental permanente con todas las eficiencias de compresión y deduplicación de datos nativos de ONTAP.

## Qué puede hacer con NetApp Disaster Recovery para VMware

NetApp Disaster Recovery le proporciona el uso completo de varias tecnologías de NetApp para lograr los siguientes objetivos:

- Replique las aplicaciones de VMware en su sitio de producción local a un sitio remoto de recuperación ante desastres en la nube o en las instalaciones mediante la replicación SnapMirror .
- Migre cargas de trabajo de VMware desde su sitio original a otro sitio.
- Realizar una prueba de conmutación por error. Al hacer esto, el servicio crea máquinas virtuales temporales. Disaster Recovery crea un nuevo volumen FlexClone a partir de la instantánea seleccionada, y un almacén de datos temporal, respaldado por el volumen FlexClone , se asigna a los hosts ESXi. Este proceso no consume capacidad física adicional en el almacenamiento ONTAP local ni en FSx para el almacenamiento ONTAP de NetApp en AWS. El volumen de origen original no se modifica y los trabajos de réplica pueden continuar incluso durante la recuperación ante desastres.
- En caso de desastre, conmute su sitio principal a pedido al sitio de recuperación ante desastres, que puede ser VMware Cloud on AWS con Amazon FSx for NetApp ONTAP o un entorno VMware local con ONTAP.
- Una vez resuelto el desastre, se realiza un retorno a pedido desde el sitio de recuperación ante desastres al sitio principal.
- Agrupe máquinas virtuales o almacenes de datos en grupos de recursos lógicos para una gestión eficiente.




La configuración del servidor vSphere se realiza fuera de NetApp Disaster Recovery en vSphere Server.

## Costo

NetApp no le cobra por utilizar la versión de prueba de NetApp Disaster Recovery.

NetApp Disaster Recovery se puede utilizar con una licencia de NetApp o con un plan de suscripción anual a través de Amazon Web Services.

Algunos lanzamientos incluyen una vista previa de la tecnología. NetApp no le cobrará por ninguna capacidad de carga de trabajo previsualizada. Ver"Novedades en NetApp Disaster Recovery" para obtener información sobre los últimos avances tecnológicos.

## Licencias

Puede utilizar los siguientes tipos de licencia:

- Regístrese para una prueba gratuita de 30 días.
- Compre una suscripción de pago por uso (PAYGO) con Amazon Web Services (AWS) Marketplace o Microsoft Azure Marketplace. Esta licencia le permite adquirir una licencia de capacidad protegida fija sin ningún compromiso a largo plazo.
- Traiga su propia licencia (BYOL), que es un archivo de licencia de NetApp (NLF) que obtiene de su representante de ventas de NetApp . Puede utilizar el número de serie de la licencia para activar el BYOL en la consola de NetApp .

Las licencias para todos los servicios de datos de NetApp se administran a través de suscripciones en la consola de NetApp . Después de configurar su BYOL, podrá ver una licencia activa para el servicio en la Consola.

El servicio se licencia en función de la cantidad de datos alojados en volúmenes ONTAP protegidos. El servicio determina qué volúmenes se deben considerar para fines de licencia mediante la asignación de máquinas virtuales protegidas a sus almacenes de datos de vCenter. Cada almacén de datos está alojado en un volumen ONTAP o LUN. La capacidad utilizada informada por ONTAP para ese volumen o LUN se utiliza para determinaciones de licencias.

Los volúmenes protegidos pueden alojar muchas máquinas virtuales. Es posible que algunos no formen parte de un grupo de recursos de recuperación ante desastres de NetApp . De todos modos, el almacenamiento consumido por todas las máquinas virtuales en ese volumen o LUN se utiliza para la capacidad máxima de la licencia.

> Los cargos de recuperación ante desastres de NetApp se basan en la capacidad utilizada de los almacenes de datos en el sitio de origen cuando hay al menos una máquina virtual que tiene un plan de replicación. La capacidad para un almacén de datos conmutado por error no está incluida en la capacidad asignada. En el caso de un BYOL, si los datos exceden la capacidad permitida, las operaciones en el servicio estarán limitadas hasta que obtenga una licencia de capacidad adicional o actualice la licencia en la consola de NetApp .

Para obtener detalles sobre la configuración de licencias para NetApp Disaster Recovery, consulte"Configurar la licencia de NetApp Disaster Recovery" .

## Prueba gratuita de 30 días

Puede probar NetApp Disaster Recovery mediante una prueba gratuita de 30 días.

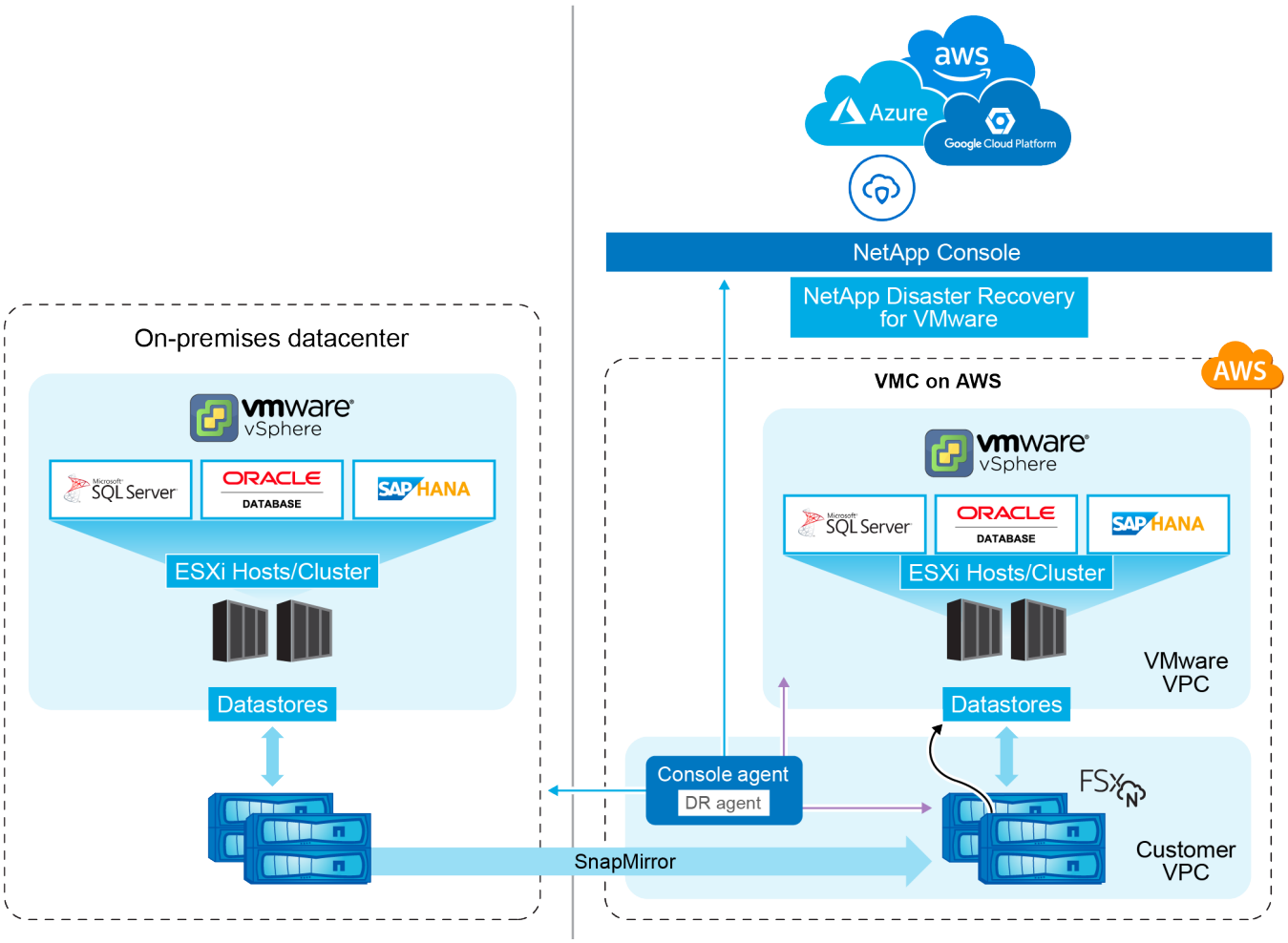
Para continuar después de la prueba de 30 días, deberá obtener una suscripción de pago por uso (PAYGO) de su proveedor de nube o comprar una licencia BYOL de NetApp.

Puede comprar una licencia en cualquier momento y no se le cobrará hasta que finalice el período de prueba de 30 días.

## Cómo funciona NetApp Disaster Recovery

NetApp Disaster Recovery es un servicio alojado dentro del entorno de software como servicio (SaaS) de NetApp Console. La recuperación ante desastres puede recuperar cargas de trabajo replicadas desde un sitio local a Amazon FSx para ONTAP o a otro sitio local. Este servicio automatiza la recuperación desde el nivel de SnapMirror , mediante el registro de máquinas virtuales en VMware Cloud on AWS y las asignaciones de red directamente en la plataforma de virtualización y seguridad de red de VMware, NSX-T. Esta función está incluida en todos los entornos de Virtual Machine Cloud.

NetApp Disaster Recovery utiliza la tecnología ONTAP SnapMirror , que proporciona una replicación altamente eficiente y preserva la eficiencia de las instantáneas incrementales de ONTAP para siempre. La replicación de SnapMirror garantiza que las copias de instantáneas consistentes con la aplicación estén siempre sincronizadas y que los datos se puedan utilizar inmediatamente después de una conmutación por error.




Cuando ocurre un desastre, este servicio le ayuda a recuperar máquinas virtuales en el otro entorno local de VMware o VMC rompiendo las relaciones de SnapMirror y activando el sitio de destino.

- El servicio también le permite revertir las máquinas virtuales a la ubicación de origen original.
- Puede probar el proceso de conmutación por error de recuperación ante desastres sin interrumpir las máquinas virtuales originales. La prueba recupera máquinas virtuales en una red aislada mediante la creación de un FlexClone del volumen.
- Para el proceso de conmutación por error o de prueba, puede elegir la instantánea más reciente (predeterminada) o seleccionada desde la cual recuperar su máquina virtual.

**Componentes de la recuperación ante desastres**

La recuperación ante desastres utiliza los siguientes componentes para proporcionar recuperación ante desastres para cargas de trabajo de VMware:

- *Consola NetApp *: la interfaz de usuario para administrar sus planes de recuperación ante desastres. Puede utilizar la consola de NetApp para crear y administrar planes de replicación, grupos de recursos y operaciones de conmutación por error en sus entornos locales y en la nube.
- **Agente de consola**: un componente de software liviano que se ejecuta en su red alojada en la nube o en su entorno VMware local. Se comunica con la consola de NetApp y administra la replicación de datos entre su entorno local y el sitio de recuperación ante desastres. El agente de consola se instala en una máquina virtual en su entorno VMware.

- * Clústeres de almacenamiento ONTAP *: Los clústeres de almacenamiento ONTAP son los sistemas de almacenamiento principales que alojan sus cargas de trabajo de VMware. Los clústeres de almacenamiento de ONTAP proporcionan la infraestructura de almacenamiento subyacente para sus planes de recuperación ante desastres. Disaster Recovery utiliza las API de almacenamiento de ONTAP para administrar clústeres de almacenamiento de ONTAP , como matrices locales y soluciones basadas en la nube, como Amazon FSx for NetApp ONTAP.
- **Servidores vCenter**: VMware vCenter es el servidor de administración para su entorno VMware. Administra los hosts ESXi y sus almacenes de datos asociados. El agente de consola se comunica con VMware vCenter para administrar la replicación de datos entre su entorno local y el sitio de recuperación ante desastres. Esto incluye registrar LUN y volúmenes de ONTAP como almacenes de datos, reconfigurar máquinas virtuales e iniciar y detener máquinas virtuales.

**El flujo de trabajo de protección de recuperación ante desastres**

Cuando se asigna un plan de replicación a un grupo de recursos, Disaster Recovery realiza una verificación de detección de todos los componentes del grupo de recursos y del plan para garantizar que el plan pueda activarse.

Si esta comprobación es exitosa, Disaster Recovery realiza los siguientes pasos de inicialización:

1. Para cada máquina virtual en el grupo de recursos de destino, identifique el almacén de datos VMware que lo aloja.
2. Para cada almacén de datos de VMware encontrado, identifique el volumen o LUN ONTAP FlexVol volume que lo aloja.
3. Para cada volumen ONTAP y LUN encontrado, determine si existe una relación SnapMirror entre los volúmenes de origen y un volumen de destino en el sitio de destino.
    a. Si no existe una relación SnapMirror preexistente, cree cualquier nuevo volumen de destino y cree una nueva relación SnapMirror entre cada volumen de origen no protegido.
    b. Si existe una relación SnapMirror preexistente, utilice esa relación para realizar todas las operaciones de replicación.

Después de que Disaster Recovery crea e inicializa todas las relaciones, en cada copia de seguridad programada, el servicio realiza los siguientes pasos de protección de datos:

1. Para cada máquina virtual marcada como “compatible con la aplicación”, utilice VMtools para colocar la aplicación compatible en un estado de respaldo.
2. Cree una nueva instantánea de todos los volúmenes ONTAP que alojan almacenes de datos VMware protegidos.
3. Realice una operación de actualización de SnapMirror para replicar esas instantáneas en el clúster ONTAP de destino.
4. Determine si la cantidad de instantáneas retenidas ha excedido la retención máxima de instantáneas definida en el plan de replicación y elimine cualquier instantánea extraña de los volúmenes de origen y destino.

## Objetivos de protección y tipos de almacén de datos admitidos

**Tipos de almacenes de datos compatibles** NetApp Disaster Recovery admite los siguientes tipos de almacenes de datos:

- Almacenes de datos NFS alojados en volúmenes ONTAP FlexVol que residen en clústeres ONTAP .

- Almacenes de datos del sistema de archivos de máquina virtual (VMFS) de VMware vSphere que utilizan el protocolo iSCSI o FC

**Objetivos de protección admitidos**

- VMware Cloud (VMC) en AWS con Amazon FSx for NetApp ONTAP
- Otro entorno VMware basado en NFS local con almacenamiento ONTAP o un VMSF FC/iSCSI local
- Servicio Amazon Elastic VMware
- Azure VMware Solution (AVS) con NetApp Cloud Volumes ONTAP (iSCSI) (versión preliminar privada)

### Términos que podrían ayudarle con NetApp Disaster Recovery

Podría resultarle beneficioso comprender algunos términos relacionados con la recuperación ante desastres.

- **Almacén de datos**: un contenedor de datos de VMware vCenter, que utiliza un sistema de archivos para almacenar archivos VMDK. Los tipos de almacenes de datos típicos son NFS, VMFS, vSAN o vVol. Disaster Recovery admite almacenes de datos NFS y VMFS. Cada almacén de datos de VMware está alojado en un único volumen o LUN de ONTAP . Disaster Recovery admite almacenes de datos NFS y VMFS alojados en volúmenes FlexVol que residen en clústeres ONTAP .
- **Plan de replicación**: un conjunto de reglas sobre la frecuencia con la que se realizan las copias de seguridad y cómo manejar eventos de conmutación por error. Los planes se asignan a uno o más grupos de recursos.
- **Objetivo de punto de recuperación (RPO)**: La cantidad máxima de pérdida de datos que es aceptable en caso de desastre. El RPO se define en la frecuencia de replicación de datos o en el cronograma de replicación del plan de replicación.
- **Objetivo de tiempo de recuperación (RTO)**: La cantidad máxima de tiempo que es aceptable para recuperarse de un desastre. El RTO se define en el plan de replicación y es el tiempo que lleva realizar una conmutación por error al sitio de recuperación ante desastres y reiniciar todas las máquinas virtuales.
- **Grupo de recursos**: un contenedor lógico que le permite administrar varias máquinas virtuales como una sola unidad. Una máquina virtual solo puede estar en un grupo de recursos a la vez. Puede crear un grupo de recursos para cada aplicación o carga de trabajo que desee proteger.
- **Sitio**: Un contenedor lógico generalmente asociado con un centro de datos físico o una ubicación en la nube que aloja uno o más clústeres de vCenter y almacenamiento ONTAP .

# Requisitos previos de NetApp Disaster Recovery

Antes de utilizar NetApp Disaster Recovery, debe asegurarse de que su entorno cumpla con los requisitos de almacenamiento de ONTAP , clúster VMware vCenter y consola de NetApp .

### Versiones de software

| Componente | Versión mínima |
|---|---|
| Software ONTAP | ONTAP 9.10.0 o posterior |
| VMware vCenter local | 7.0u3 o posterior |

| Componente | Versión mínima |
| --- | --- |
| VMware Cloud para AWS | Última versión disponible |
| Amazon FSx for NetApp ONTAP | Última versión disponible |

## Requisitos previos de almacenamiento de ONTAP

Estos requisitos previos se aplican a las instancias de ONTAP o Amazon FSX para NetApp ONTAP .

- Los clústeres de origen y destino deben tener una relación de pares.
- La SVM que alojará los volúmenes de recuperación ante desastres debe existir en el clúster de destino.
- El SVM de origen y el SVM de destino deben tener una relación de pares.
- Si se implementa con Amazon FSx for NetApp ONTAP, se aplica el siguiente requisito previo:
  - Debe existir una instancia de Amazon FSx for NetApp ONTAP para alojar almacenes de datos de VMware DR en su VPC. Consulte Amazon FSx para obtener documentación de ONTAP sobre "Cómo empezar" .

## Requisitos previos de los clústeres de VMware vCenter

Estos requisitos previos se aplican tanto a los clústeres de vCenter locales como al centro de datos definido por software (SDDC) de VMware Cloud para AWS.

- Revisar"Privilegios de vCenter" requerido para NetApp Disaster Recovery.
- Todos los clústeres de VMware que desea que NetApp Disaster Recovery administre utilizan volúmenes ONTAP para alojar cualquier máquina virtual que desee proteger.
- Todos los almacenes de datos de VMware que administrará NetApp Disaster Recovery deben utilizar uno de los siguientes protocolos:
  - Sistema Nacional de Archivos
  - VMFS utilizando el protocolo iSCSI o FC
- VMware vSphere versión 7.0 Actualización 3 (7.0v3) o posterior
- Si utiliza VMware Cloud SDDC, se aplican estos requisitos previos.
  - En VMware Cloud Console, utilice los roles de servicio de Administrador y Administrador de NSX Cloud. Utilice también el propietario de la organización para el rol de Organización. Referirse a "Uso de VMware Cloud Foundations con AWS FSx para la documentación de NetApp ONTAP" .
  - Vincule VMware Cloud SDDC con la instancia de Amazon FSx for NetApp ONTAP . Referirse a "Información sobre la integración de VMware Cloud on AWS con Amazon FSx for NetApp ONTAP" .

## Requisitos previos de la consola de NetApp

### Comience a utilizar la consola de NetApp

Si aún no lo has hecho, "Regístrese en la consola de NetApp y cree una organización" .

### Recopilar credenciales para ONTAP y VMware

- Las credenciales de Amazon FSx para ONTAP y AWS deben agregarse al sistema dentro del proyecto de consola de NetApp que se utilizará para administrar NetApp Disaster Recovery.
- NetApp Disaster Recovery requiere credenciales de vCenter. Ingresa las credenciales de vCenter cuando agrega un sitio en NetApp Disaster Recovery.

  Para obtener una lista de los privilegios de vCenter necesarios, consulte"Privilegios de vCenter necesarios para NetApp Disaster Recovery" . Para obtener instrucciones sobre cómo agregar un sitio, consulte"Agregar un sitio" .

### Crear el agente de la consola de NetApp

El agente de consola es un componente de software que permite que la consola se comunique con su almacenamiento ONTAP y los clústeres VMware vCenter. Es necesario para que la recuperación ante desastres funcione correctamente. El agente reside en su red privada (ya sea en un centro de datos local o en una VPC en la nube) y se comunica con sus instancias de almacenamiento de ONTAP y cualquier componente de servidor y aplicación adicional. Para la recuperación ante desastres, este es el acceso a sus clústeres de vCenter administrados.

Se debe configurar un agente de consola en la consola de NetApp . Cuando utilice el agente, incluirá las capacidades adecuadas para el servicio de recuperación ante desastres.

- NetApp Disaster Recovery solo funciona con la implementación del agente en modo estándar. Ver "Introducción a la consola de NetApp en modo estándar" .
- Asegúrese de que tanto el vCenter de origen como el de destino utilicen el mismo agente de consola.
- Tipo de agente de consola necesario:
  - **Recuperación ante desastres local a local**: instale el agente local de la consola en el sitio de recuperación ante desastres. Con este método, una falla del sitio principal no impide que el servicio reinicie sus recursos virtuales en el sitio de recuperación ante desastres. Referirse a "Instalar y configurar el agente de consola en las instalaciones" .
  - **En las instalaciones de AWS**: instale el agente de consola para AWS en su VPC de AWS. Referirse a "Opciones de instalación del agente de consola en AWS" .

    Para conexiones locales a locales, utilice el agente de consola local. Para las instalaciones locales en AWS, utilice el agente de la consola de AWS, que tiene acceso al vCenter local de origen y al vCenter local de destino.

  - El agente de consola instalado debe poder acceder a cualquier clúster de VMware que NetApp Disaster Recovery administrará.
- Todas las matrices ONTAP que serán administradas por NetApp Disaster Recovery deben agregarse a cualquier sistema dentro del proyecto de la Consola NetApp que se utilizará para administrar NetApp Disaster Recovery.

  Ver "Descubra los clústeres ONTAP locales" .
- Para obtener información sobre cómo configurar un proxy inteligente para NetApp Disaster Recovery, consulte"Configure su infraestructura para NetApp Disaster Recovery" .

### Requisitos previos de la carga de trabajo

Para garantizar que los procesos de coherencia de aplicaciones sean exitosos, aplique estos requisitos previos:

- Asegúrese de que las herramientas de VMware (o las herramientas de OpenVM) se estén ejecutando en las máquinas virtuales que estarán protegidas.
- Para las máquinas virtuales Windows que ejecutan Microsoft SQL Server u Oracle Database o ambos, las bases de datos deben tener sus escritores VSS habilitados.
- Las bases de datos Oracle que se ejecutan en un sistema operativo Linux deben tener la autenticación de usuario del sistema operativo habilitada para la función SYSDBA de la base de datos Oracle.

# Inicio rápido para NetApp Disaster Recovery

A continuación se muestra una descripción general de los pasos necesarios para comenzar a utilizar NetApp Disaster Recovery. Los enlaces dentro de cada paso lo llevarán a una página que proporciona más detalles.

**Revisar los prerrequisitos**

"Asegúrese de que su sistema cumpla estos requisitos" .

**Configurar NetApp Disaster Recovery**

- "Configurar la infraestructura para el servicio" .
- "Configurar licencias" .

**¿Que sigue?**

Después de configurar el servicio, esto es lo que puedes hacer a continuación.

- "Agregue sus sitios de vCenter a NetApp Disaster Recovery" .
- "Crea tu primer grupo de recursos" .
- "Crea tu primer plan de replicación" .
- "Replicar aplicaciones a otro sitio" .
- "Conmutar por error las aplicaciones a un sitio remoto" .
- "Regresar las aplicaciones al sitio de origen original" .
- "Administrar sitios, grupos de recursos y planes de replicación" .
- "Supervisar las operaciones de recuperación ante desastres" .

# Configure su infraestructura para NetApp Disaster Recovery

Para utilizar NetApp Disaster Recovery, realice algunos pasos para configurarlo tanto en

Amazon Web Services (AWS) como en la consola de NetApp .

Revisar"prerrequisitos" para garantizar que su sistema esté listo.

Puede utilizar NetApp Disaster Recovery en las siguientes infraestructuras:

- DR en nube híbrida que replica un centro de datos VMware plus ONTAP local a una infraestructura de DR de AWS basada en VMware Cloud on AWS y Amazon FSx for NetApp ONTAP.
- DR en nube privada que replica un VMware plus ONTAP vCenter local a otro VMware plus ONTAP vCenter local.

## Nube híbrida con VMware Cloud y Amazon FSx for NetApp ONTAP

Este método consiste en una infraestructura de vCenter de producción local que utiliza almacenes de datos alojados en volúmenes ONTAP FlexVol mediante un protocolo NFS. El sitio de DR consta de una o más instancias de VMware Cloud SDDC que utilizan almacenes de datos alojados en volúmenes FlexVol proporcionados por una o más instancias de FSx para ONTAP mediante un protocolo NFS.

Los sitios de producción y DR están conectados mediante una conexión segura compatible con AWS. Los tipos de conexión comunes son una VPN segura (privada o proporcionada por AWS), AWS Direct Connect u otros métodos de interconexión aprobados.

Para la recuperación ante desastres que involucra la infraestructura de nube de AWS, debe utilizar el agente de consola para AWS. El agente debe instalarse en la misma VPC que la instancia de FSx para ONTAP . Si se implementaron instancias adicionales de FSx para ONTAP en otras VPC, la VPC que aloja al agente debe tener acceso a las otras VPC.

### Zonas de disponibilidad de AWS

AWS admite la implementación de soluciones en una o más zonas de disponibilidad (AZ) dentro de una región determinada. La recuperación ante desastres utiliza dos servicios alojados en AWS: VMware Cloud para AWS y AWS FSx para NetApp ONTAP.

- **VMware Cloud para AWS**: admite la implementación en un entorno SDDC de clúster extendido de una sola AZ o de dos AZ. Disaster Recovery admite una implementación de SDDC de zona única solo para Amazon VMware Cloud para AWS.
- **AWS FSx para NetApp ONTAP**: cuando se implementa en una configuración de doble AZ, cada volumen es propiedad de un solo sistema FSx. Cada volumen es propiedad de un único sistema FSx. Los datos del volumen se reflejan en el segundo sistema FSx. Los sistemas FSx para ONTAP se pueden implementar en implementaciones de zona de disponibilidad única o doble. La recuperación ante desastres admite FSx de una o varias zonas de disponibilidad para implementaciones de FSx para ONTAP .

**MEJORES PRÁCTICAS**: Para la configuración del sitio de AWS DR, NetApp recomienda usar implementaciones de zona de disponibilidad única tanto para VMware Cloud como para AWS FSx para instancias de ONTAP . Dado que AWS se utiliza para recuperación ante desastres, no hay ninguna ventaja en introducir múltiples AZ. Las multi-AZ pueden aumentar los costos y la complejidad.

### Local a AWS

AWS proporciona los siguientes métodos para conectar centros de datos privados a la nube de AWS. Cada solución tiene sus beneficios y consideraciones de costos.

- **AWS Direct Connect**: se trata de una interconexión en la nube de AWS ubicada en la misma área

geográfica que su centro de datos privado y proporcionada por un socio de AWS. Esta solución proporciona una conexión segura y privada entre su centro de datos local y la nube de AWS sin la necesidad de una conexión a Internet pública. Este es el método de conexión más directo y eficiente que ofrece AWS.

- **AWS Internet Gateway**: Proporciona conectividad pública entre los recursos de la nube de AWS y los recursos informáticos externos. Este tipo de conexión se utiliza normalmente para ofrecer servicios a clientes externos, como el servicio HTTP/HTTPS donde la seguridad no es un requisito. No hay control de calidad de servicio, seguridad ni garantía de conectividad. Por este motivo, este método de conexión no se recomienda para conectar un centro de datos de producción a la nube.
- **AWS Site-Site VPN**: esta conexión de red privada virtual se puede utilizar para proporcionar conexiones de acceso seguro junto con un proveedor de servicios de Internet público. La VPN cifra y descifra todos los datos que viajan hacia y desde la nube de AWS. Las VPN pueden basarse en software o hardware. Para las aplicaciones empresariales, el proveedor de servicios de Internet (ISP) público debe ofrecer garantías de calidad de servicio para asegurar que se proporcione el ancho de banda y la latencia adecuados para la replicación de DR.

**MEJORES PRÁCTICAS**: Para la configuración del sitio de AWS DR, NetApp recomienda usar AWS Direct Connect. Esta solución proporciona el máximo rendimiento y seguridad para aplicaciones empresariales. Si no está disponible, se debe utilizar una conexión ISP pública de alto rendimiento junto con una VPN. Asegúrese de que el ISP ofrezca niveles de servicio QoS comerciales para garantizar un rendimiento adecuado de la red.

#### Interconexiones de VPC a VPC

AWS ofrece los siguientes tipos de interconexiones de VPC a VPC. Cada solución tiene sus beneficios y consideraciones de costos.

- **VPC Peering**: se trata de una conexión privada entre dos VPC. Es el método de conexión más directo y eficiente que ofrece AWS. El peering de VPC se puede utilizar para conectar VPC en la misma región de AWS o en diferentes.
- **AWS Internet Gateway**: normalmente se utiliza para proporcionar conexiones entre recursos de AWS VPC y recursos y puntos finales que no son de AWS. Todo el tráfico sigue una ruta de "horquilla" donde el tráfico de VPC destinado a otra VPC sale de la infraestructura de AWS a través de la puerta de enlace de Internet y regresa a la infraestructura de AWS a través de la misma puerta de enlace o de una diferente. Este no es un tipo de conexión VPC adecuado para soluciones VMware empresariales.
- **AWS Transit Gateway**: este es un tipo de conexión centralizada basada en enrutador que permite que cada VPC se conecte a una única puerta de enlace central, que actúa como un concentrador central para todo el tráfico de VPC a VPC. Esto también se puede conectar a su solución VPN para permitir que los recursos del centro de datos local accedan a los recursos alojados en AWS VPC. Este tipo de conexión generalmente requiere un costo adicional para implementarse.

**MEJORES PRÁCTICAS**: Para soluciones de recuperación ante desastres que involucran VMware Cloud y un solo FSx para ONTAP VPC, NetApp recomienda que utilice la conexión de pares de VPC. Si se implementan varias VPC de FSx para ONTAP , recomendamos utilizar AWS Transit Gateway para reducir la sobrecarga de administración de varias conexiones de pares de VPC.

### Prepárese para la protección local en la nube con AWS

Para configurar NetApp Disaster Recovery para la protección local en la nube mediante AWS, debe configurar lo siguiente:

- Configurar AWS FSx para NetApp ONTAP
- Configurar VMware Cloud en AWS SDDC

#### Configurar AWS FSx para NetApp ONTAP

- Cree un sistema de archivos Amazon FSx for NetApp ONTAP .
  - Aprovisionar y configurar FSx para ONTAP. Amazon FSx for NetApp ONTAP es un servicio completamente administrado que proporciona almacenamiento de archivos altamente confiable, escalable, de alto rendimiento y con gran cantidad de funciones, creado sobre el sistema de archivos NetApp ONTAP .
  - Siga los pasos en "Informe técnico 4938: Monte Amazon FSx ONTAP como un almacén de datos NFS con VMware Cloud en AWS" y "Inicio rápido de Amazon FSx for NetApp ONTAP" para aprovisionar y configurar FSx para ONTAP.
- Agregue Amazon FSx para ONTAP al sistema y agregue las credenciales de AWS para FSx para ONTAP.
- Cree o verifique su SVM ONTAP de destino en AWS FSx para la instancia de ONTAP .
- Configure la replicación entre su clúster ONTAP local de origen y su instancia de FSx para ONTAP en la consola de NetApp .

Referirse a "Cómo configurar un sistema FSx para ONTAP" para conocer los pasos detallados.

#### Configurar VMware Cloud en AWS SDDC

"VMware Cloud en AWS"Proporciona una experiencia nativa de la nube para cargas de trabajo basadas en VMware en el ecosistema de AWS. Cada centro de datos definido por software (SDDC) de VMware se ejecuta en una Amazon Virtual Private Cloud (VPC) y proporciona una pila VMware completa (incluido vCenter Server), redes definidas por software NSX-T, almacenamiento definido por software vSAN y uno o más hosts ESXi que proporcionan recursos de procesamiento y almacenamiento a las cargas de trabajo.

Para configurar un entorno de VMware Cloud en AWS, siga los pasos que se indican en "Implementar y configurar el entorno de virtualización en AWS" Un grupo de luces piloto también se puede utilizar para fines de recuperación ante desastres.

## Nube privada

Puede utilizar NetApp Disaster Recovery para proteger las máquinas virtuales VMware alojadas en uno o más clústeres de vCenter replicando los almacenes de datos de las máquinas virtuales en otro clúster de vCenter, ya sea en el mismo centro de datos privado o en un centro de datos remoto privado o ubicado en el mismo lugar.

Para situaciones locales a locales, instale el agente de consola en uno de los sitios físicos.

Disaster Recovery admite la replicación de sitio a sitio mediante Ethernet y TCP/IP. Asegúrese de que haya suficiente ancho de banda disponible para soportar las tasas de cambio de datos en las máquinas virtuales del sitio de producción, de modo que todos los cambios se puedan replicar en el sitio de recuperación ante desastres dentro del marco de tiempo del Objetivo de punto de recuperación (RPO).

### Prepárese para la protección local a local

Asegúrese de que se cumplan los siguientes requisitos antes de configurar NetApp Disaster Recovery para la protección local a local:

- Almacenamiento ONTAP
  - Asegúrese de tener las credenciales de ONTAP .
  - Cree o verifique su sitio de recuperación ante desastres.

- Cree o verifique su SVM ONTAP de destino.
- Asegúrese de que sus SVM ONTAP de origen y destino estén emparejados.

- Clústeres de vCenter
  - Asegúrese de que las máquinas virtuales que desea proteger estén alojadas en almacenes de datos NFS (utilizando volúmenes NFS de ONTAP ) o almacenes de datos VMFS (utilizando LUN iSCSI de NetApp ).
  - Revisar"Privilegios de vCenter" requerido para NetApp Disaster Recovery.
  - Cree una cuenta de usuario de recuperación ante desastres (no la cuenta de administrador de vCenter predeterminada) y asigne los privilegios de vCenter a la cuenta.

**Soporte de proxy inteligente**

El agente de la consola de NetApp admite proxy inteligente. El proxy inteligente es una forma liviana, segura y eficiente de conectar su entorno local a la consola de NetApp . Proporciona una conexión segura entre su sistema y el servicio de consola sin necesidad de una VPN o acceso directo a Internet. Esta implementación de proxy optimizada descarga el tráfico de API dentro de la red local.

Cuando se configura un proxy, NetApp Disaster Recovery intenta comunicarse directamente con VMware o ONTAP y utiliza el proxy configurado si falla la comunicación directa.

La implementación del proxy de recuperación ante desastres de NetApp requiere comunicación del puerto 443 entre el agente de la consola y cualquier servidor vCenter y matriz ONTAP que utilice un protocolo HTTPS. El agente de recuperación ante desastres de NetApp dentro del agente de consola se comunica directamente con VMware vSphere, VC u ONTAP cuando realiza cualquier acción.

Para obtener más información sobre la configuración general del proxy en la consola de NetApp , consulte "Configurar el agente de la consola para utilizar un servidor proxy" .

# Acceda a NetApp Disaster Recovery

## Utilice la consola de NetApp para iniciar sesión en el servicio de recuperación ante desastres de NetApp .

Para iniciar sesión, puede utilizar sus credenciales del sitio de soporte de NetApp o puede registrarse para iniciar sesión en la nube de NetApp usando su correo electrónico y una contraseña. "Obtenga más información sobre cómo iniciar sesión" .

Tareas específicas requieren roles de usuario específicos. "Obtenga información sobre los roles y permisos de usuario en NetApp Disaster Recovery" . "Obtenga información sobre los roles de acceso a la consola de NetApp para todos los servicios" .

**Pasos**

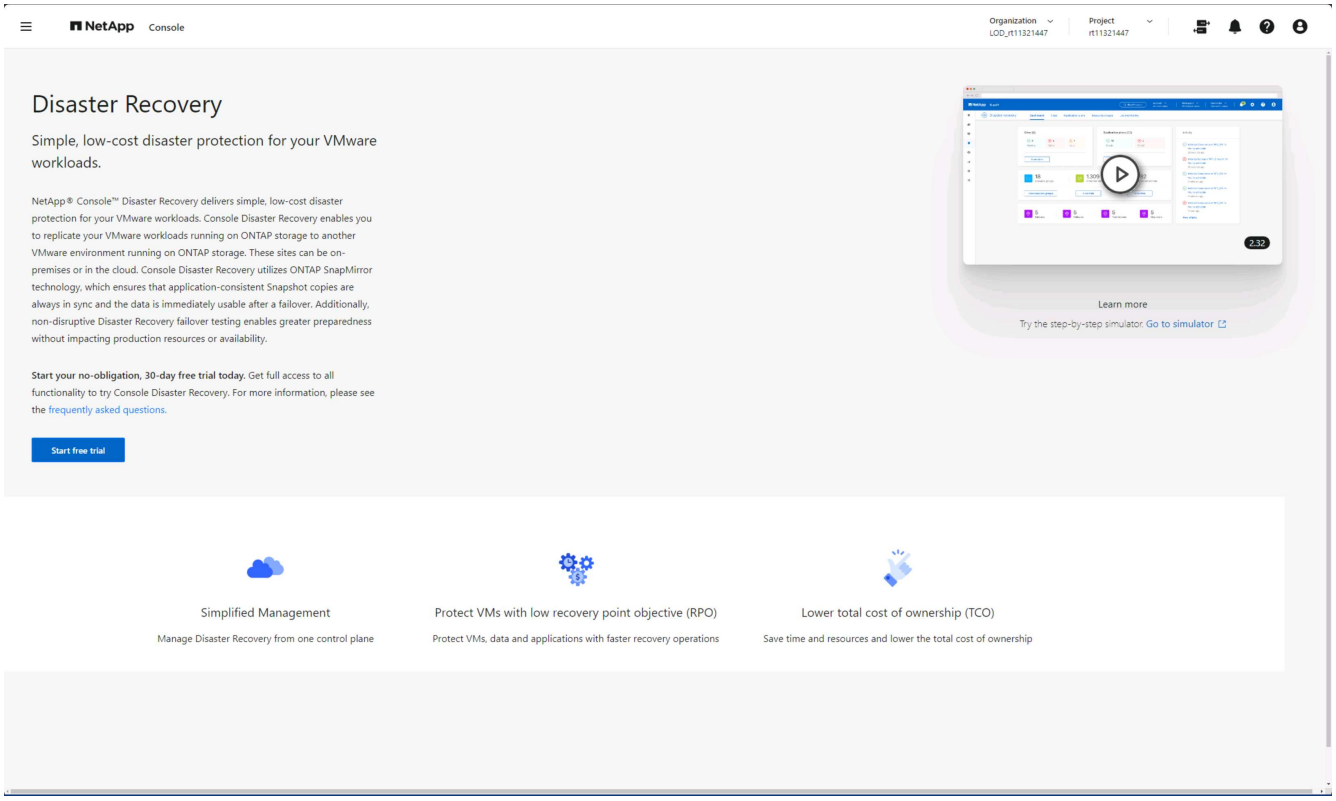
1. Abra un navegador web y vaya a "Consola de NetApp" .

   Aparece la página de inicio de sesión de la consola de NetApp .

2. Inicie sesión en la consola de NetApp .
3. Desde el panel de navegación izquierdo de la consola NetApp , seleccione **Protección** > **Recuperación ante desastres**.

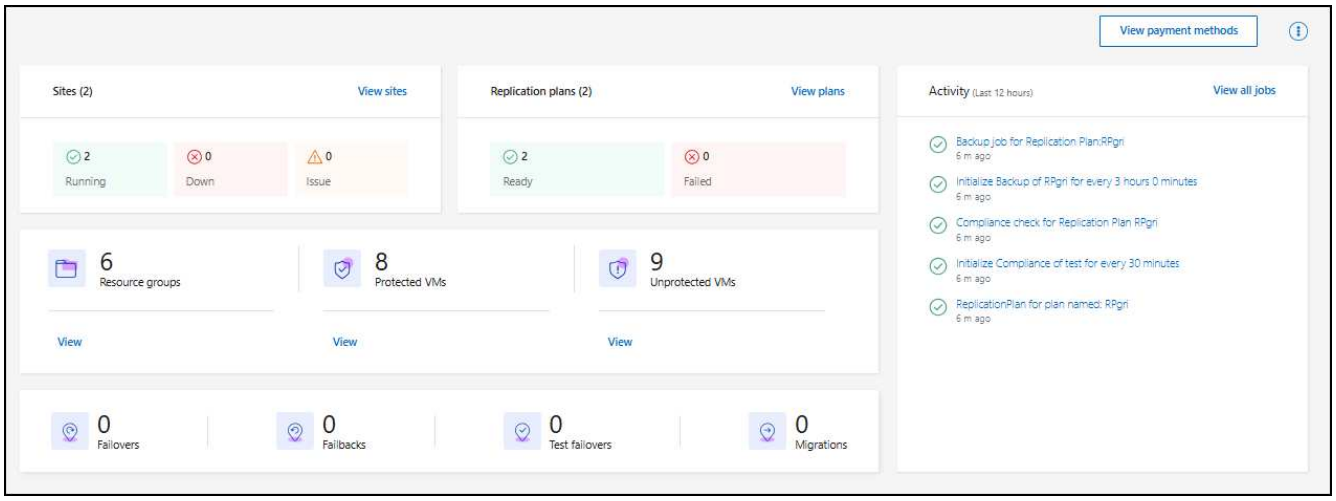
   Si es la primera vez que inicia sesión en este servicio, aparecerá la página de inicio y podrá registrarse

para una prueba gratuita.




De lo contrario, aparecerá el Panel de recuperación ante desastres de NetApp .

- Si aún no ha agregado un agente de consola de NetApp , deberá agregar uno. Para agregar el agente, consulte "Obtenga más información sobre los agentes de consola" .
- Si es un usuario de la consola de NetApp con un agente existente, cuando selecciona "Recuperación ante desastres", aparece un mensaje sobre cómo registrarse.
- Si ya está utilizando el servicio, cuando seleccione "Recuperación ante desastres", aparecerá el Panel de control.



# Configurar licencias para NetApp Disaster Recovery

Con NetApp Disaster Recovery, puede utilizar diferentes planes de licencia, incluida una prueba gratuita, una suscripción de pago por uso o traer su propia licencia.

**Rol de consola de NetApp requerido** Administrador de organización, Administrador de carpeta o proyecto, Administrador de recuperación ante desastres o Administrador de aplicación de recuperación ante desastres.

"Obtenga información sobre los roles y permisos de usuario en NetApp Disaster Recovery" . "Obtenga información sobre los roles de acceso para todos los servicios" .

**Opciones de licencia** Puede utilizar las siguientes opciones de licencia:

- Regístrese para una prueba gratuita de 30 días.
- Compre una suscripción de pago por uso (PAYGO) en Amazon Web Services (AWS) Marketplace o en Microsoft Azure Marketplace.
- Traiga su propia licencia (BYOL), que es un archivo de licencia de NetApp (NLF) que obtiene de su representante de ventas de NetApp . Puede utilizar el número de serie de la licencia para activar el BYOL en la consola de NetApp .

> Los cargos de recuperación ante desastres de NetApp se basan en la capacidad utilizada de los almacenes de datos en el sitio de origen cuando hay al menos una máquina virtual que tiene un plan de replicación. La capacidad para un almacén de datos conmutado por error no está incluida en la capacidad asignada. En el caso de un BYOL, si los datos exceden la capacidad permitida, las operaciones en el servicio estarán limitadas hasta que obtenga una licencia de capacidad adicional o actualice la licencia en la consola de NetApp .

"Obtenga más información sobre las suscripciones" .

Una vez finalizada la prueba gratuita o caducada la licencia, aún puedes hacer lo siguiente en el servicio:

- Ver cualquier recurso, como una carga de trabajo o un plan de replicación.
- Eliminar cualquier recurso, como una carga de trabajo o un plan de replicación.
- Ejecute todas las operaciones programadas que se crearon durante el período de prueba o bajo la licencia.

## Pruébelo utilizando una prueba gratuita de 30 días

Puede probar NetApp Disaster Recovery mediante una prueba gratuita de 30 días.

> No se aplican límites de capacidad durante la prueba.

Para continuar después de la prueba, deberá comprar una licencia BYOL o una suscripción PAYGO de AWS. Puede obtener una licencia en cualquier momento y no se le cobrará hasta que finalice el período de prueba.

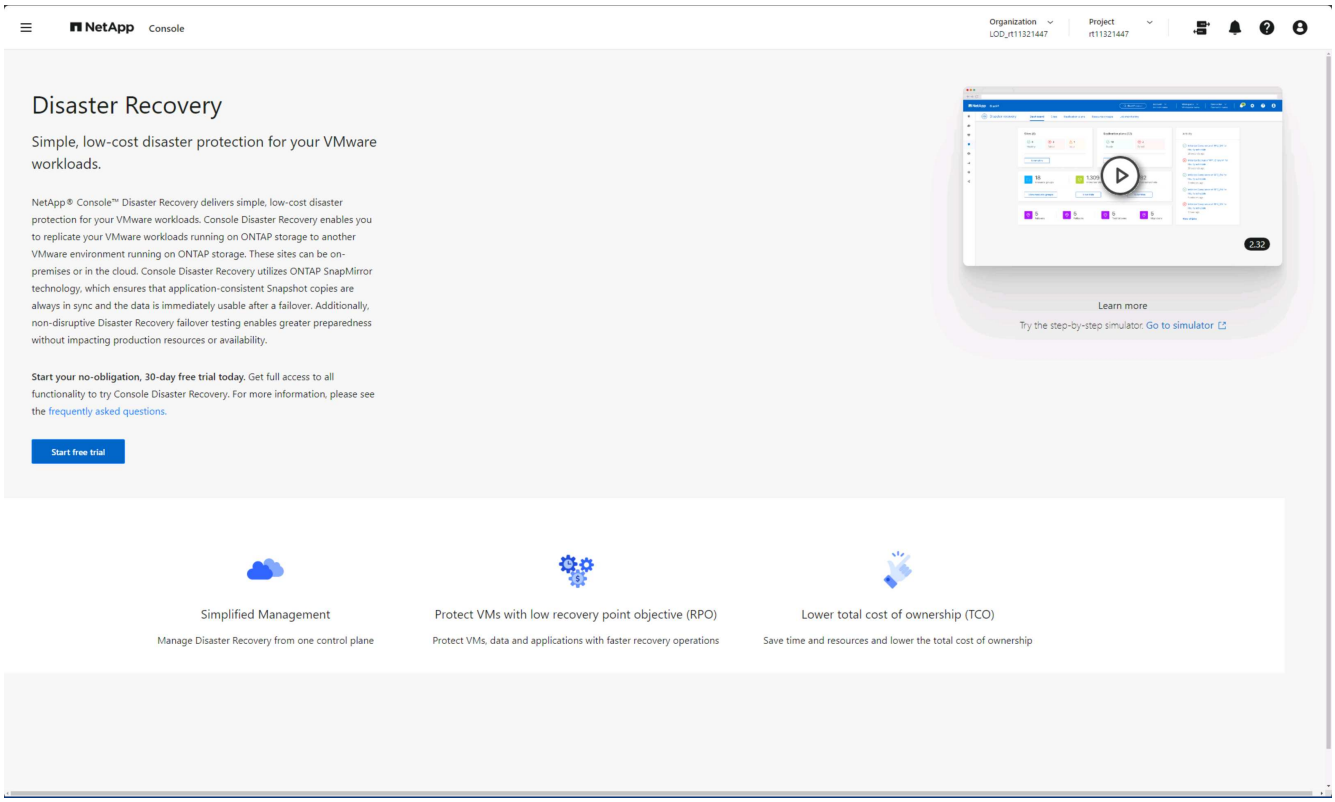
Durante la prueba, tendrás acceso a todas las funciones.

**Pasos**

1. Iniciar sesión en el "Consola de NetApp" .
2. Desde el panel de navegación izquierdo de la consola NetApp , seleccione **Protección** > **Recuperación**

**ante desastres**.

Si es la primera vez que inicia sesión en este servicio, aparecerá la página de destino.




3. Si aún no ha agregado un agente de consola para otros servicios, agregue uno.

   Para agregar un agente de consola, consulte "Obtenga más información sobre los agentes de consola" .

4. Después de configurar el agente, en la página de inicio de NetApp Disaster Recovery, el botón para agregar el agente cambia a un botón para iniciar una prueba gratuita. Seleccione **Iniciar prueba gratuita**.
5. Comience agregando vCenters.

   Para obtener más información, consulte "Agregar sitios de vCenter" .

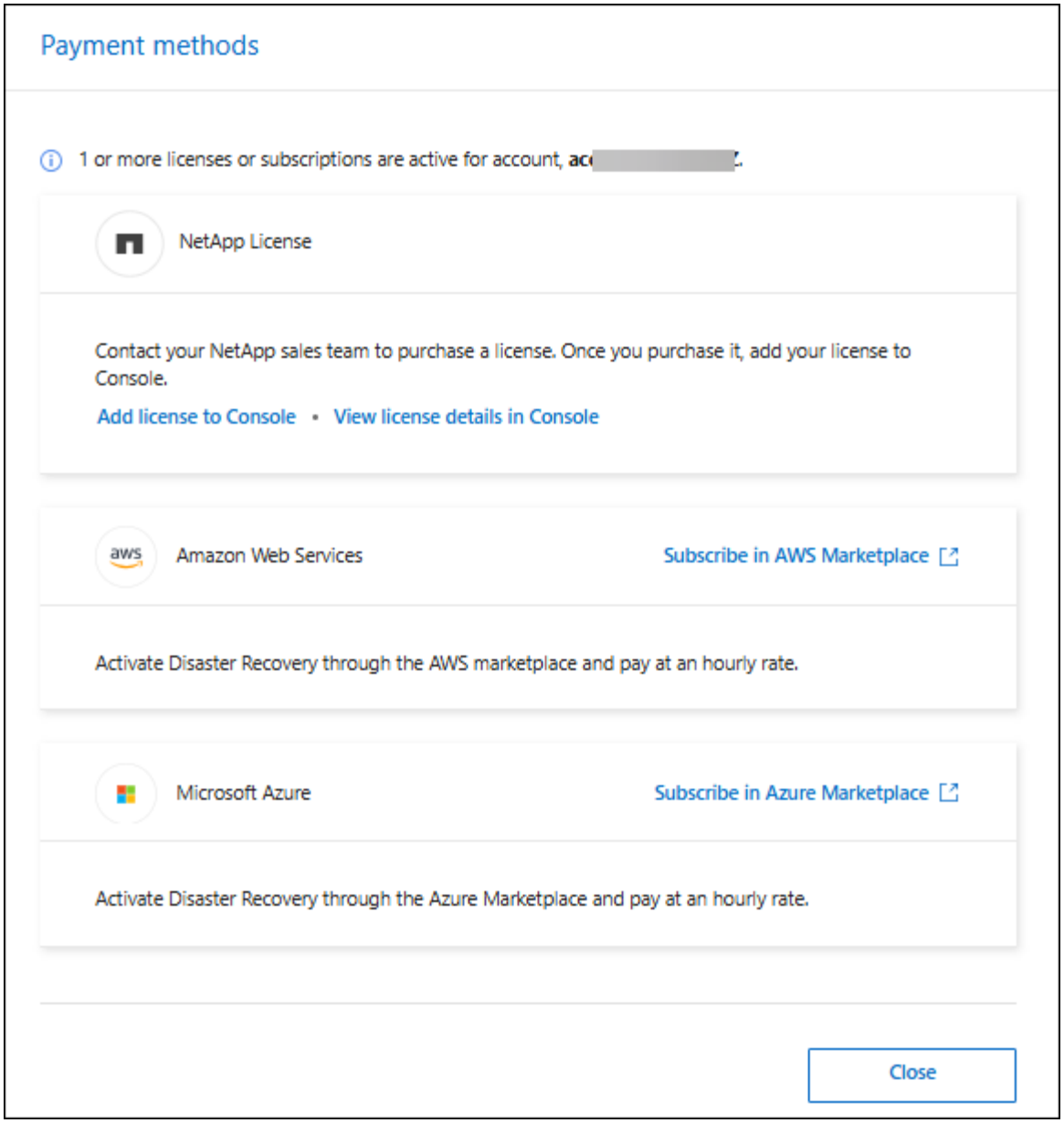
## Una vez finalizada la prueba, suscríbete a través de uno de los Marketplaces

Una vez finalizada la prueba gratuita, puede comprar una licencia de NetApp o suscribirse a través de AWS Marketplace o Microsoft Azure Marketplace. Este procedimiento proporciona una descripción general de alto nivel sobre cómo suscribirse directamente en uno de los Marketplaces.

**Pasos**

1. En NetApp Disaster Recovery, verá un mensaje que indica que la prueba gratuita está por vencer. En el mensaje, seleccione **Suscribirse o comprar una licencia**.

   O bien, desde , seleccione **Ver métodos de pago**.




2. Seleccione **Suscribirse en AWS Marketplace** o **Suscribirse en Azure Marketplace**.
3. Utilice AWS Marketplace o Microsoft Azure Marketplace para suscribirse a * NetApp Disaster Recovery*.
4. Cuando regrese a NetApp Disaster Recovery, aparecerá un mensaje que indica que está suscrito.

   Puede ver los detalles de la suscripción en la página de suscripción de la consola de NetApp . "Obtenga más información sobre cómo administrar suscripciones con la consola de NetApp" .

## Una vez finalizada la prueba, compre una licencia BYOL a través de NetApp

Una vez finalizada la prueba, puede comprar una licencia a través de su representante de ventas de NetApp .

Si trae su propia licencia (BYOL), la configuración incluye comprar la licencia, obtener el archivo de licencia de NetApp (NLF) y agregar la licencia a la consola de NetApp .

**Agregue la licencia a la consola de NetApp *** Después de haber comprado su licencia de recuperación ante desastres de NetApp a un representante de ventas de NetApp , puede administrar la licencia en la consola.

"Obtenga información sobre cómo agregar licencias con la consola de NetApp" .

## Actualice su licencia cuando expire

Si su período de licencia está cerca de la fecha de vencimiento o si su capacidad de licencia está alcanzando el límite, se le notificará en la interfaz de usuario de recuperación ante desastres de NetApp . Puede actualizar su licencia de NetApp Disaster Recovery antes de que caduque para que no haya interrupciones en su capacidad de acceder a los datos escaneados.

Este mensaje también aparece en la consola de NetApp y en "Notificaciones" .

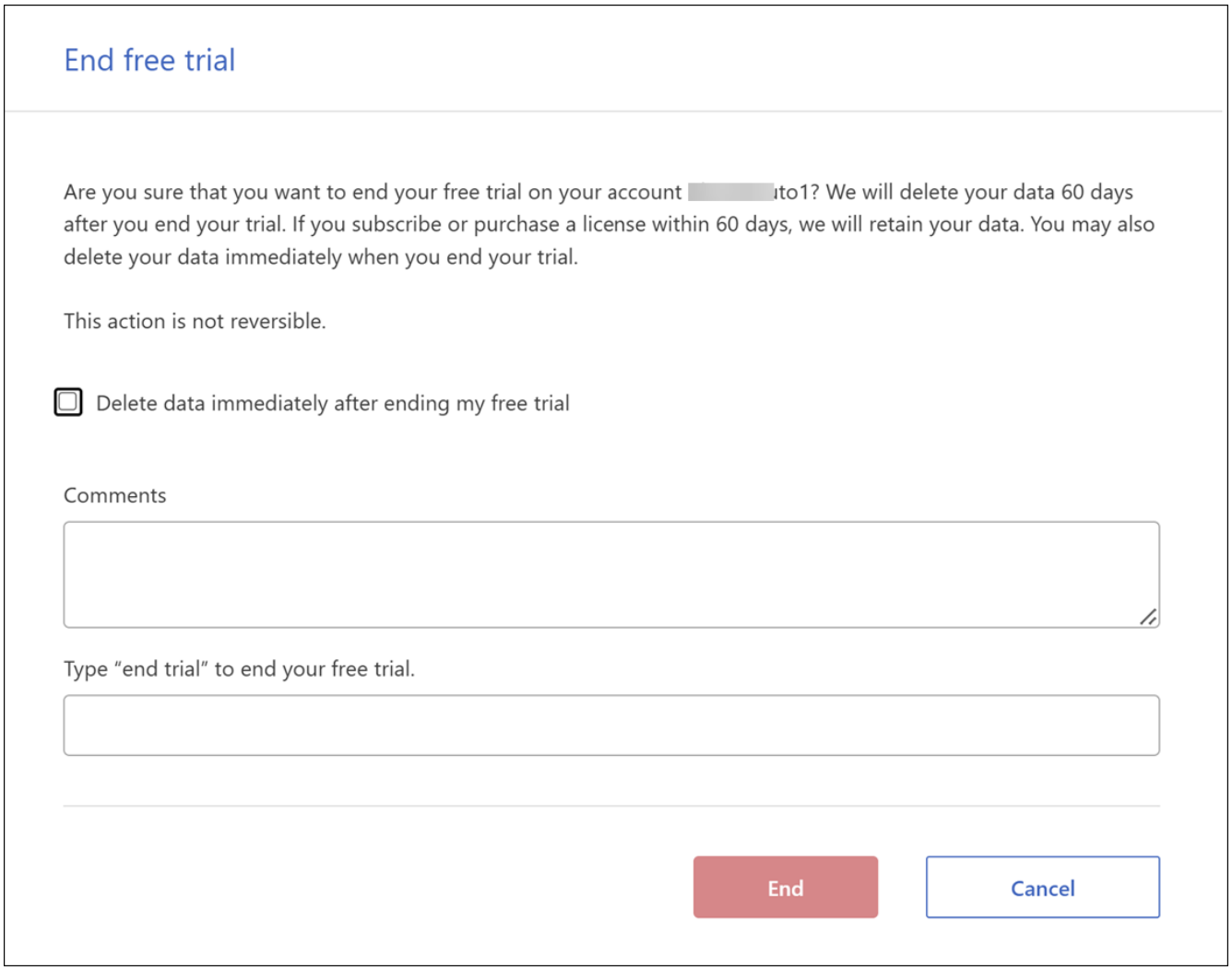
"Obtenga información sobre cómo actualizar licencias con la consola de NetApp" .

## Finalizar la prueba gratuita

Puedes detener la prueba gratuita en cualquier momento o esperar hasta que caduque.

**Pasos**

1. En NetApp Disaster Recovery, seleccione **Prueba gratuita - Ver detalles**.
2. En los detalles desplegables, seleccione **Finalizar prueba gratuita**.



3. Si desea eliminar todos los datos, marque **Eliminar datos inmediatamente después de finalizar mi prueba gratuita**.

   Esto elimina todas las programaciones, planes de replicación, grupos de recursos, vCenters y sitios. Los datos de auditoría, los registros de operaciones y el historial de trabajos se conservan hasta el final de la vida útil del producto.

   > Si finaliza la prueba gratuita, no solicitó la eliminación de datos y no compra una licencia o suscripción, NetApp Disaster Recovery eliminará todos sus datos 60 días después de que finalice la prueba gratuita.

4. Escriba "finalizar prueba" en el cuadro de texto.
5. Seleccione **Fin**.

# Utilice NetApp Disaster Recovery

## Descripción general del uso de NetApp Disaster Recovery

Con NetApp Disaster Recovery, puede lograr los siguientes objetivos:

- "Visualizar el estado de sus planes de recuperación ante desastres" .
- "Agregar sitios de vCenter" .
- "Crear grupos de recursos para organizar las máquinas virtuales juntas"
- "Crear un plan de recuperación ante desastres" .
- "Replicar aplicaciones de VMware"en su sitio principal a un sitio remoto de recuperación ante desastres en la nube mediante la replicación SnapMirror .
- "Migrar aplicaciones de VMware"de su sitio principal a otro sitio.
- "Probar la conmutación por error"sin interrumpir las máquinas virtuales originales.
- En caso de desastre,"conmutar por error su sitio principal" a VMware Cloud en AWS con FSx para NetApp ONTAP.
- Una vez resuelto el desastre,"recuperación por fallo" Desde el sitio de recuperación ante desastres hasta el sitio principal.
- "Supervisar las operaciones de recuperación ante desastres"en la página de Monitoreo de trabajos.

## Vea el estado de sus planes de recuperación ante desastres de NetApp en el Panel de control

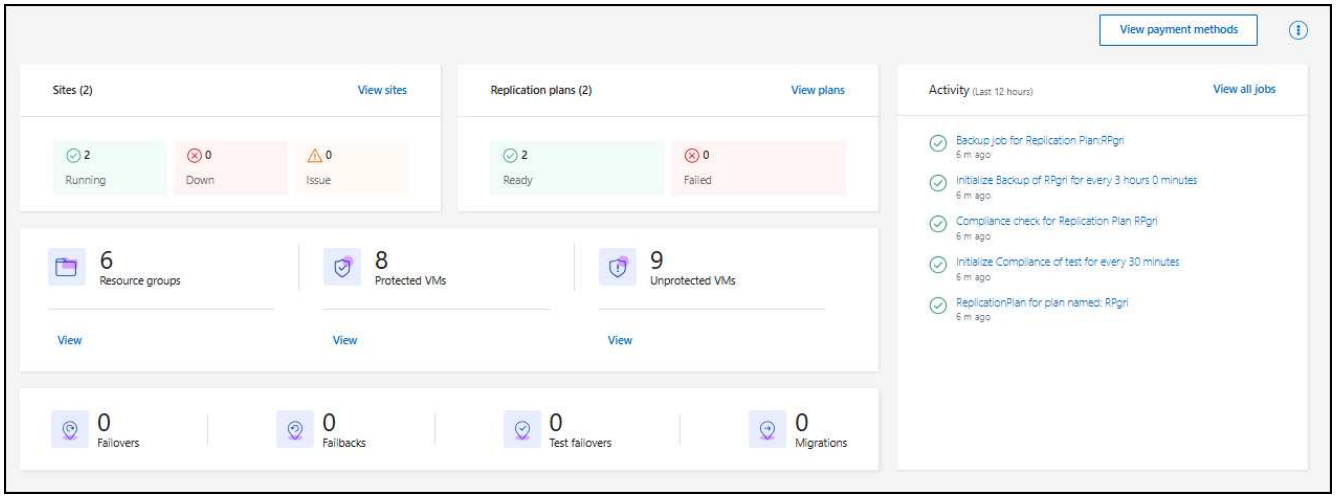
Con el panel de recuperación ante desastres de NetApp , puede determinar el estado de sus sitios de recuperación ante desastres y sus planes de replicación. Puede determinar rápidamente qué sitios y planes están en buen estado, desconectados o degradados.

**Rol de consola de NetApp requerido** Administrador de organización, Administrador de carpeta o proyecto, Administrador de recuperación ante desastres, Administrador de aplicaciones de recuperación ante desastres o Rol de visualizador de recuperación ante desastres.

"Obtenga información sobre los roles y permisos de usuario en NetApp Disaster Recovery" . "Obtenga información sobre los roles de acceso a la consola de NetApp para todos los servicios" .

**Pasos**

1. Iniciar sesión en el "Consola de NetApp" .
2. Desde el panel de navegación izquierdo de la consola NetApp , seleccione **Protección** > **Recuperación ante desastres**.
3. Desde el menú Recuperación ante desastres de NetApp , seleccione **Panel de control**.




4. Revise la siguiente información en el Tablero:
   - **Sitios**: vea el estado de sus sitios. Un sitio puede tener uno de los siguientes estados:
     - **En ejecución**: el vCenter está conectado, en buen estado y funcionando.
     - **Caído**: No se puede acceder al vCenter o hay problemas de conectividad.
     - **Problema**: No se puede acceder al vCenter o hay problemas de conectividad.

       Para ver los detalles del sitio, seleccione **Ver todo** para un estado o **Ver sitios** para verlos todos.
   - **Planes de replicación**: vea el estado de sus planes. Un plan puede tener uno de los siguientes estados:
     - **Listo**
     - **Fallido**

       Para revisar los detalles del plan de replicación, seleccione **Ver todo** para ver un estado o **Ver planes de replicación** para verlos todos.
   - **Grupos de recursos**: vea el estado de sus grupos de recursos. Un grupo de recursos puede tener uno de los siguientes estados:
   - **Máquinas virtuales protegidas**: Las máquinas virtuales son parte de un grupo de recursos.
   - **Máquinas virtuales no protegidas**: Las máquinas virtuales no son parte de un grupo de recursos.

     Para revisar los detalles, seleccione el enlace **Ver** debajo de cada uno.
   - El número de conmutaciones por error, conmutaciones por error de prueba y migraciones. Por ejemplo, si creó dos planes y migró a los destinos, el recuento de migración aparece como "2".
5. Revise todas las operaciones en el panel Actividad. Para ver todas las operaciones en el Monitor de trabajos, seleccione **Ver todos los trabajos**.

# Agregar vCenters a un sitio en NetApp Disaster Recovery

Antes de poder crear un plan de recuperación ante desastres, debe agregar un servidor vCenter principal a un sitio y un sitio de recuperación ante desastres vCenter de destino en la consola de NetApp .

Asegúrese de que tanto el vCenter de origen como el de destino utilicen el mismo agente de consola de NetApp .

Una vez agregados los vCenters, NetApp Disaster Recovery realiza un descubrimiento profundo de los entornos de vCenter, incluidos los clústeres de vCenter, los hosts ESXi, los almacenes de datos, la superficie de almacenamiento, los detalles de las máquinas virtuales, las réplicas de SnapMirror y las redes de máquinas virtuales.

**Rol de consola de NetApp requerido** Administrador de organización, administrador de carpeta o proyecto, o administrador de recuperación ante desastres.

"Obtenga información sobre los roles y permisos de usuario en NetApp Disaster Recovery" . "Obtenga información sobre los roles de acceso a la consola de NetApp para todos los servicios" .

**Acerca de esta tarea**

Si agregó vCenters en versiones anteriores y desea personalizar la programación de detección, debe editar el sitio del servidor vCenter y configurar la programación.

NetApp Disaster Recovery realiza el descubrimiento una vez cada 24 horas. Después de configurar un sitio, puede editar más tarde el vCenter para personalizar la programación de detección que satisfaga sus necesidades. Por ejemplo, si tiene una gran cantidad de máquinas virtuales, puede configurar la programación de descubrimiento para que se ejecute cada 23 horas y 59 minutos. Si tiene una pequeña cantidad de máquinas virtuales, puede configurar la programación de detección para que se ejecute cada 12 horas. El intervalo mínimo es de 30 minutos y el máximo de 24 horas.

Primero debe realizar algunos descubrimientos manuales para obtener la información más actualizada sobre su entorno. Después de esto, puedes configurar el cronograma para que se ejecute automáticamente.

Si tiene vCenters de versiones anteriores y desea cambiar cuándo se ejecuta la detección, edite el sitio del servidor vCenter y configure la programación.

Las máquinas virtuales recién agregadas o eliminadas se reconocen en la próxima detección programada o durante una detección manual inmediata.

Las máquinas virtuales solo se pueden proteger si el plan de replicación se encuentra en uno de los siguientes estados:

- Listo
- Conmutación por recuperación comprometida
- Prueba de conmutación por error confirmada

**Clústeres de vCenter en un sitio** Cada sitio contiene uno o más vCenters. Estos vCenters utilizan uno o más clústeres de almacenamiento ONTAP para alojar almacenes de datos NFS o VMFS.

Un clúster de vCenter puede residir en un solo sitio. Necesita la siguiente información para agregar un clúster de vCenter a un sitio:

- La dirección IP o FQDN de administración de vCenter
- Credenciales para una cuenta de vCenter con los privilegios necesarios para realizar operaciones. Ver "privilegios de vCenter requeridos" Para más información.

- Para los sitios VMware alojados en la nube, las claves de acceso a la nube necesarias
- Un certificado de seguridad para acceder a su vCenter.

> El servicio admite certificados de seguridad autofirmados o certificados de una autoridad de certificación (CA) central.

**Pasos**

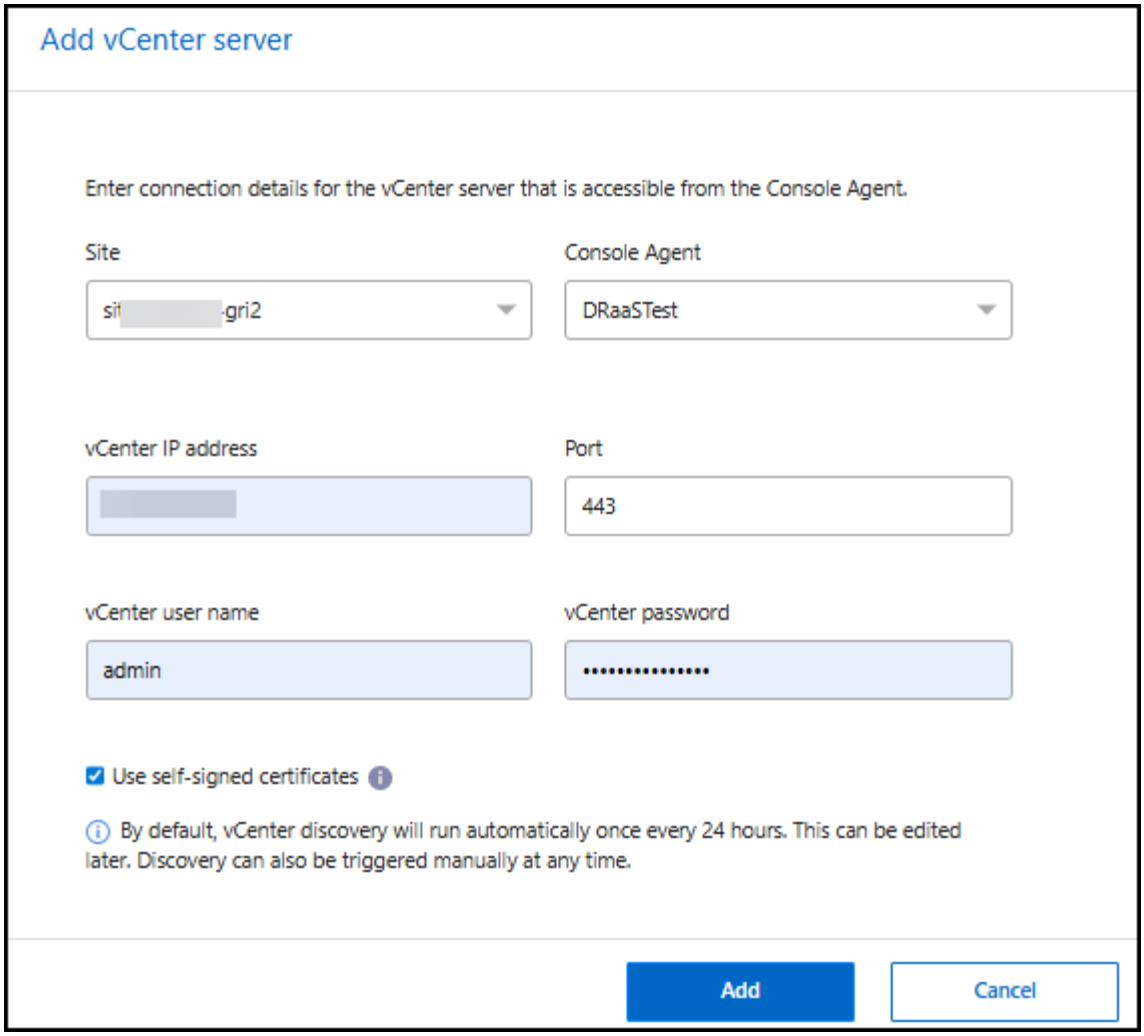
1. Iniciar sesión en el "Consola de NetApp" .
2. Desde el panel de navegación izquierdo de la consola NetApp , seleccione **Protección** > **Recuperación ante desastres**.

   Accederá a la página del Panel de recuperación ante desastres de NetApp . Cuando comience a utilizar el servicio, deberá agregar información de vCenter. Más tarde, el Panel de control muestra datos sobre sus sitios y planes de replicación.

   > Aparecen diferentes campos según el tipo de sitio que esté agregando.

3. Si ya existen algunos sitios de vCenter y desea agregar más, en el menú, seleccione **Sitios** y luego seleccione **Agregar**.
4. En la página Sitios, seleccione el sitio y seleccione **Agregar vCenter**.
5. **Fuente**: seleccione **Descubrir servidores vCenter** para ingresar información sobre el sitio vCenter de origen.

   > Si ya existen algunos sitios de vCenter y desea agregar más, en el menú superior, seleccione **Sitios** y luego seleccione **Agregar**.




- Seleccione un sitio, seleccione el agente de consola de NetApp y proporcione las credenciales de vCenter.
- (Se aplica solo a sitios locales) Para aceptar certificados autofirmados para el vCenter de origen, marque la casilla.

> Los certificados autofirmados no son tan seguros como otros certificados. Si su vCenter **NO** está configurado con certificados de autoridad de certificación (CA), debe marcar esta casilla; de lo contrario, la conexión al vCenter no funcionará.

6. Seleccione **Agregar**.

   A continuación, agregará un vCenter de destino.

7. Agregue nuevamente un sitio para el vCenter de destino.
8. Nuevamente, seleccione **Agregar vCenter** y agregue la información del vCenter de destino.
9. **Objetivo**:

   a. Elija el sitio de destino y la ubicación. Si el destino es la nube, seleccione **AWS**.

      - (Se aplica solo a sitios en la nube) **Token API**: Ingrese el token API para autorizar el acceso al servicio para su organización. Cree el token API proporcionando roles de organización y servicio específicos.

- (Se aplica solo a sitios en la nube) **ID de organización larga**: Ingrese la ID única de la organización. Puede identificar esta ID haciendo clic en el nombre de usuario en la sección Cuenta de la Consola de NetApp .

b. Seleccione **Agregar**.

Los vCenters de origen y destino aparecen en la lista de sitios.


10. Para ver el progreso de la operación, desde el menú, seleccione **Monitoreo de trabajos**.

## Agregar asignación de subred para un sitio de vCenter

Puede administrar direcciones IP en operaciones de conmutación por error mediante la asignación de subredes, lo que le permite agregar subredes para cada vCenter. Al hacerlo, define el CIDR IPv4, la puerta de enlace predeterminada y el DNS para cada red virtual.

En caso de conmutación por error, NetApp Disaster Recovery utiliza el CIDR de la red asignada para asignar a cada vNIC una nueva dirección IP.

Por ejemplo:

- RedA = 10.1.1.0/24
- RedB = 192.168.1.0/24

VM1 tiene una vNIC (10.1.1.50) que está conectada a NetworkA. La red A se asigna a la red B en la configuración del plan de replicación.

En caso de conmutación por error, NetApp Disaster Recovery reemplaza la parte de red de la dirección IP original (10.1.1) y conserva la dirección de host (.50) de la dirección IP original (10.1.1.50). Para VM1, NetApp Disaster Recovery analiza la configuración CIDR para NetworkB y utiliza la parte de red de NetworkB 192.168.1 mientras conserva la parte del host (.50) para crear la nueva dirección IP para VM1. La nueva IP pasa a ser 192.168.1.50.

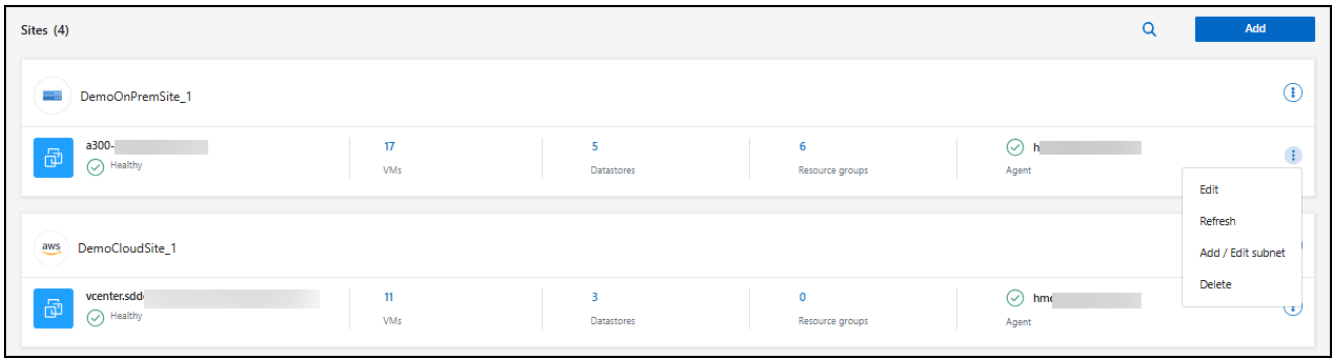
En resumen, la dirección del host permanece igual, mientras que la dirección de red se reemplaza con la que esté configurada en la asignación de subred del sitio. Esto le permite administrar la reasignación de direcciones IP en caso de conmutación por error con mayor facilidad, especialmente si tiene cientos de redes y miles de máquinas virtuales para administrar.

El uso del mapeo de subredes es un proceso opcional de dos pasos:

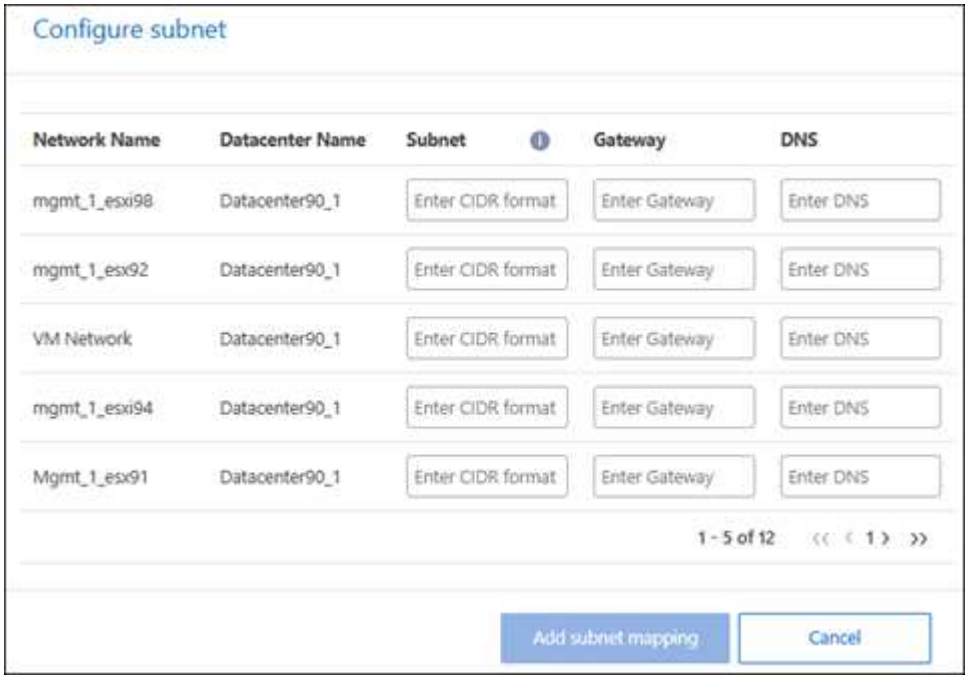
- Primero, agregue la asignación de subred para cada sitio de vCenter.
- En segundo lugar, en el plan de replicación, indique que desea utilizar la asignación de subred en la pestaña Máquinas virtuales y en el campo IP de destino.

**Pasos**

1. En el menú Recuperación ante desastres de NetApp , seleccione **Sitios**.
2. De las acciones Icono de la derecha, seleccione **Agregar subred**.




Aparece la página Configurar subred:




3. En la página Configurar subred, ingrese la siguiente información:
   a. Subred: ingrese el CIDR IPv4 para la subred hasta /32.

   La notación CIDR es un método para especificar direcciones IP y sus máscaras de red. El /24 denota la máscara de red. El número consta de una dirección IP con el número después del "/" indicando cuántos bits de la dirección IP denotan la red. Por ejemplo, 192.168.0.50/24, la dirección IP es 192.168.0.50 y el número total de bits en la dirección de red es 24. 192.168.0.50 255.255.255.0 se convierte en 192.168.0.0/24.

   b. Puerta de enlace: introduzca la puerta de enlace predeterminada para la subred.
   c. DNS: Ingrese el DNS para la subred.
4. Seleccione **Agregar mapeo de subred**.

### Seleccionar la asignación de subred para un plan de replicación

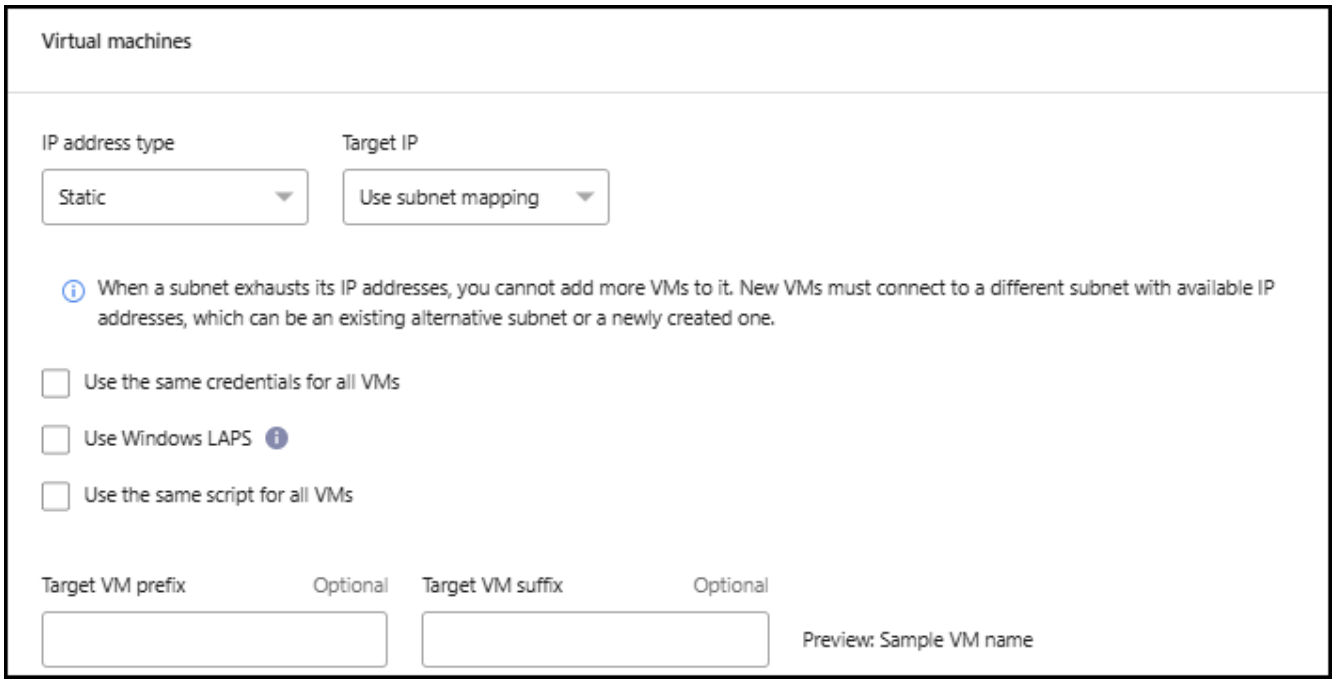
Al crear un plan de replicación, puede seleccionar la asignación de subred para el plan de replicación.

El uso del mapeo de subredes es un proceso opcional de dos pasos:

- Primero, agregue la asignación de subred para cada sitio de vCenter.
- En segundo lugar, en el plan de replicación, indique que desea utilizar la asignación de subred.

**Pasos**

1. En el menú NetApp Disaster Recovery, seleccione **Planes de replicación**.
2. Seleccione **Agregar** para agregar un plan de replicación.
3. Complete los campos de la forma habitual agregando los servidores vCenter, seleccionando los grupos de recursos o aplicaciones y completando las asignaciones.
4. En la página Plan de replicación > Asignación de recursos, seleccione la sección **Máquinas virtuales**.




5. En el campo **IP de destino**, seleccione **Usar asignación de subred** de la lista desplegable.

> Si hay dos máquinas virtuales (por ejemplo, una es Linux y la otra es Windows), las credenciales solo se necesitan para Windows.

6. Continúe con la creación del plan de replicación.

## Edite el sitio del servidor vCenter y personalice la programación de detección

Puede editar el sitio del servidor vCenter para personalizar la programación de detección. Por ejemplo, si tiene una gran cantidad de máquinas virtuales, puede configurar la programación de descubrimiento para que se ejecute cada 23 horas y 59 minutos. Si tiene una pequeña cantidad de máquinas virtuales, puede configurar la programación de detección para que se ejecute cada 12 horas.

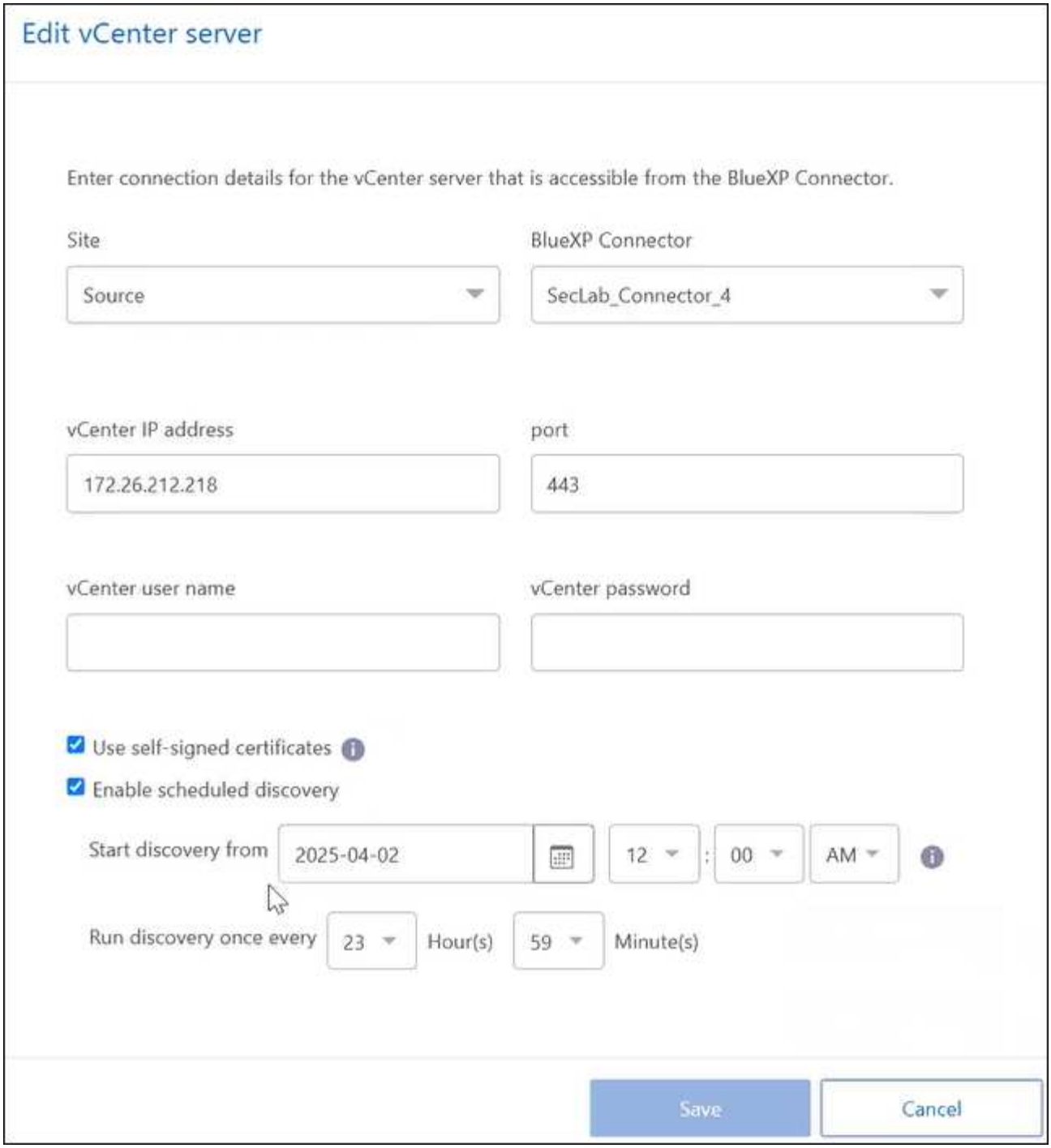
Si tiene vCenters de versiones anteriores y desea cambiar cuándo se ejecuta la detección, edite el sitio del

servidor vCenter y configure la programación.

Si no desea programar la detección, puede deshabilitar la opción de detección programada y actualizar la detección manualmente en cualquier momento.

**Pasos**

1. En el menú Recuperación ante desastres de NetApp , seleccione **Sitios**.
2. Seleccione el sitio que desea editar.
3. Seleccione las acciones  icono de la derecha y seleccione **Editar**.
4. En la página Editar servidor vCenter, edite los campos según sea necesario.
5. Para personalizar la programación de descubrimiento, marque la casilla **Habilitar descubrimiento programado** y seleccione el intervalo de fecha y hora que desee.




6. Seleccione **Guardar**.

## Actualizar el descubrimiento manualmente

Puede actualizar el descubrimiento manualmente en cualquier momento. Esto es útil si ha agregado o eliminado máquinas virtuales y desea actualizar la información en NetApp Disaster Recovery.

**Pasos**

1. En el menú Recuperación ante desastres de NetApp , seleccione **Sitios**.
2. Seleccione el sitio que desea actualizar.
3.

Seleccione las acciones  icono a la derecha y seleccione **Actualizar**.

# Cree un grupo de recursos para organizar las máquinas virtuales juntas en NetApp Disaster Recovery

Después de agregar sitios de vCenter, puede crear grupos de recursos para proteger las máquinas virtuales por máquina virtual o almacén de datos como una sola unidad. Los grupos de recursos le permiten organizar un conjunto de máquinas virtuales dependientes en grupos lógicos que satisfacen sus requisitos. Por ejemplo, puede agrupar máquinas virtuales asociadas con una aplicación o puede agrupar aplicaciones que tengan niveles similares. Como otro ejemplo, los grupos podrían contener órdenes de arranque retrasadas que se puedan ejecutar durante la recuperación.

**Rol de consola de NetApp requerido** Administrador de organización, Administrador de carpeta o proyecto, Administrador de recuperación ante desastres o Administrador de aplicación de recuperación ante desastres.

"Obtenga información sobre los roles y permisos de usuario en NetApp Disaster Recovery" . "Obtenga información sobre los roles de acceso a la consola de NetApp para todos los servicios" .

### Acerca de esta tarea

Puede agrupar las máquinas virtuales en sí o las máquinas virtuales en almacenes de datos.

Puede crear grupos de recursos utilizando los siguientes métodos:

- Desde la opción Grupos de recursos
- Mientras crea un plan de recuperación ante desastres o *replicación*. Si tiene muchas máquinas virtuales alojadas en un clúster de vCenter de origen, puede que le resulte más fácil crear los grupos de recursos mientras crea el plan de replicación. Para obtener instrucciones sobre cómo crear grupos de recursos mientras crea un plan de replicación, consulte"Crear un plan de replicación" .

Cada grupo de recursos puede incluir una o más máquinas virtuales o almacenes de datos. Las máquinas virtuales se encenderán según la secuencia en que las incluya en el plan de replicación. Puede cambiar el orden arrastrando las máquinas virtuales o los almacenes de datos hacia arriba o hacia abajo en la lista del grupo de recursos.

### Acerca de los grupos de recursos

Los grupos de recursos le permiten combinar máquinas virtuales o almacenes de datos como una sola unidad.

Por ejemplo, una aplicación de punto de venta podría utilizar varias máquinas virtuales para bases de datos, lógica empresarial y tiendas. Puede administrar todas estas máquinas virtuales con un solo grupo de recursos. Configure grupos de recursos para aplicar reglas de plan de replicación para el orden de inicio de las máquinas virtuales, la conexión de red y la recuperación de todas las máquinas virtuales necesarias para la aplicación.

### ¿Cómo funciona?

NetApp Disaster Recovery protege las máquinas virtuales al replicar los volúmenes ONTAP y los LUN subyacentes que alojan las máquinas virtuales en el grupo de recursos. Para ello, el sistema consulta a vCenter el nombre de cada almacén de datos que aloja máquinas virtuales en un grupo de recursos. Luego, NetApp Disaster Recovery identifica el volumen ONTAP o LUN de origen que aloja ese almacén de datos.

Toda la protección se realiza a nivel de volumen ONTAP mediante la replicación SnapMirror .

Si las máquinas virtuales del grupo de recursos están alojadas en diferentes almacenes de datos, NetApp Disaster Recovery utiliza uno de los siguientes métodos para crear una instantánea coherente con los datos de los volúmenes o LUN de ONTAP .

| **Ubicación relativa de los volúmenes FlexVol** | **Proceso de réplica de instantánea** |
|---|---|
| Múltiples almacenes de datos: volúmenes FlexVol en el **mismo SVM** | • Se creó un grupo de consistencia ONTAP<br>• Instantáneas del grupo de consistencia tomadas<br>• Se realizó la replicación de SnapMirror con alcance de volumen |
| Múltiples almacenes de datos: volúmenes FlexVol en **múltiples SVM** | • API de ONTAP : `cg_start` . Pone en pausa todos los volúmenes para que se puedan tomar instantáneas e inicia instantáneas de alcance de volumen de todos los volúmenes del grupo de recursos.<br>• API de ONTAP : `cg_end` . Reanuda la E/S en todos los volúmenes y habilita la replicación de SnapMirror en todo el volumen después de tomar instantáneas. |

Al crear grupos de recursos, tenga en cuenta las siguientes cuestiones:

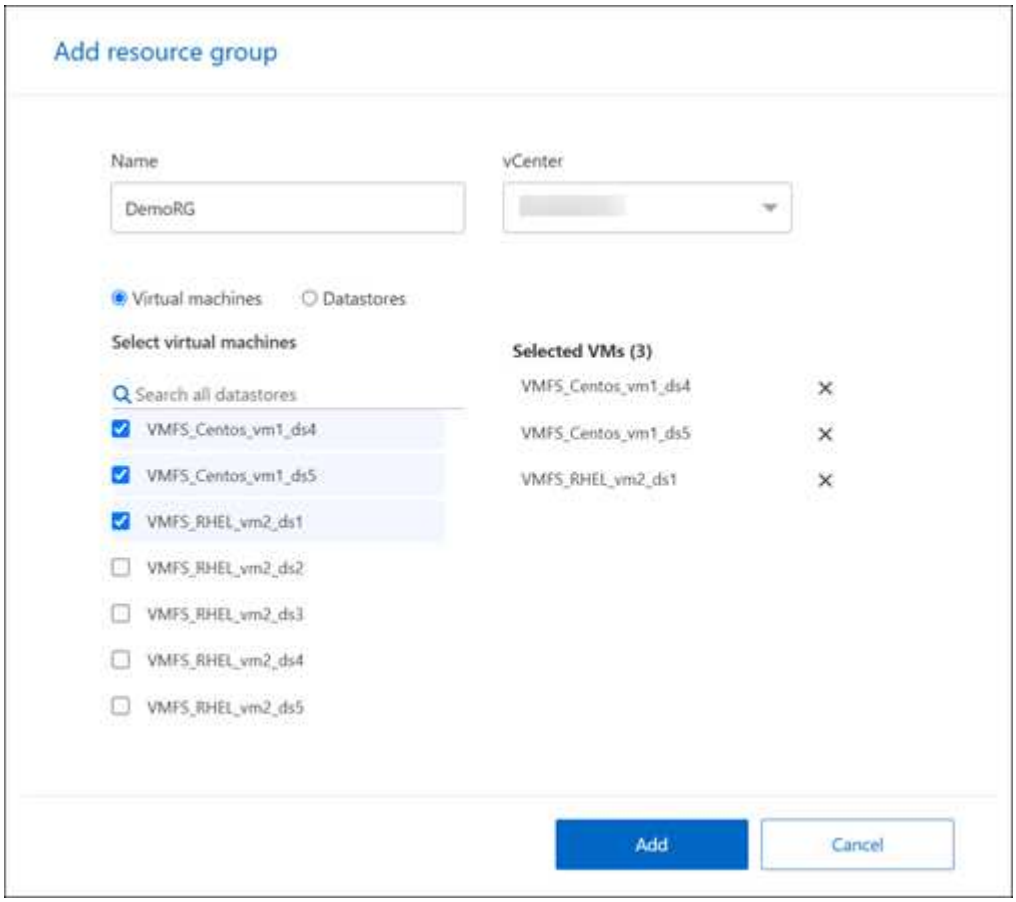
- Antes de agregar almacenes de datos a grupos de recursos, inicie primero un descubrimiento manual o un descubrimiento programado de las máquinas virtuales. Esto garantiza que las máquinas virtuales se detecten y se incluyan en el grupo de recursos. Si no inicia un descubrimiento manual, es posible que las máquinas virtuales no aparezcan en el grupo de recursos.
- Asegúrese de que haya al menos una máquina virtual en el almacén de datos. Si no hay máquinas virtuales en el almacén de datos, Disaster Recovery no descubre el almacén de datos.
- Un único almacén de datos no debe alojar máquinas virtuales protegidas por más de un plan de replicación.
- No aloje máquinas virtuales protegidas y no protegidas en el mismo almacén de datos. Si las máquinas virtuales protegidas y no protegidas están alojadas en el mismo almacén de datos, podrían surgir los siguientes problemas:
  - Debido a que NetApp Disaster Recovery utiliza SnapMirror y el sistema replica volúmenes ONTAP completos, la capacidad utilizada de ese volumen se utiliza para consideraciones de licencia. En este caso, el espacio de volumen consumido por las máquinas virtuales protegidas y no protegidas se incluiría en este cálculo.
  - Si el grupo de recursos y sus almacenes de datos asociados deben conmutarse por error al sitio de recuperación ante desastres, todas las máquinas virtuales desprotegidas (máquinas virtuales que no forman parte del grupo de recursos, pero que están alojadas en el volumen de ONTAP ) ya no existirán en el sitio de origen debido al proceso de conmutación por error, lo que provocará una falla de las máquinas virtuales desprotegidas en el sitio de origen. Además, NetApp Disaster Recovery no iniciará aquellas máquinas virtuales desprotegidas en el sitio de vCenter de conmutación por error.
- Para que una VM esté protegida, debe estar incluida en un grupo de recursos.

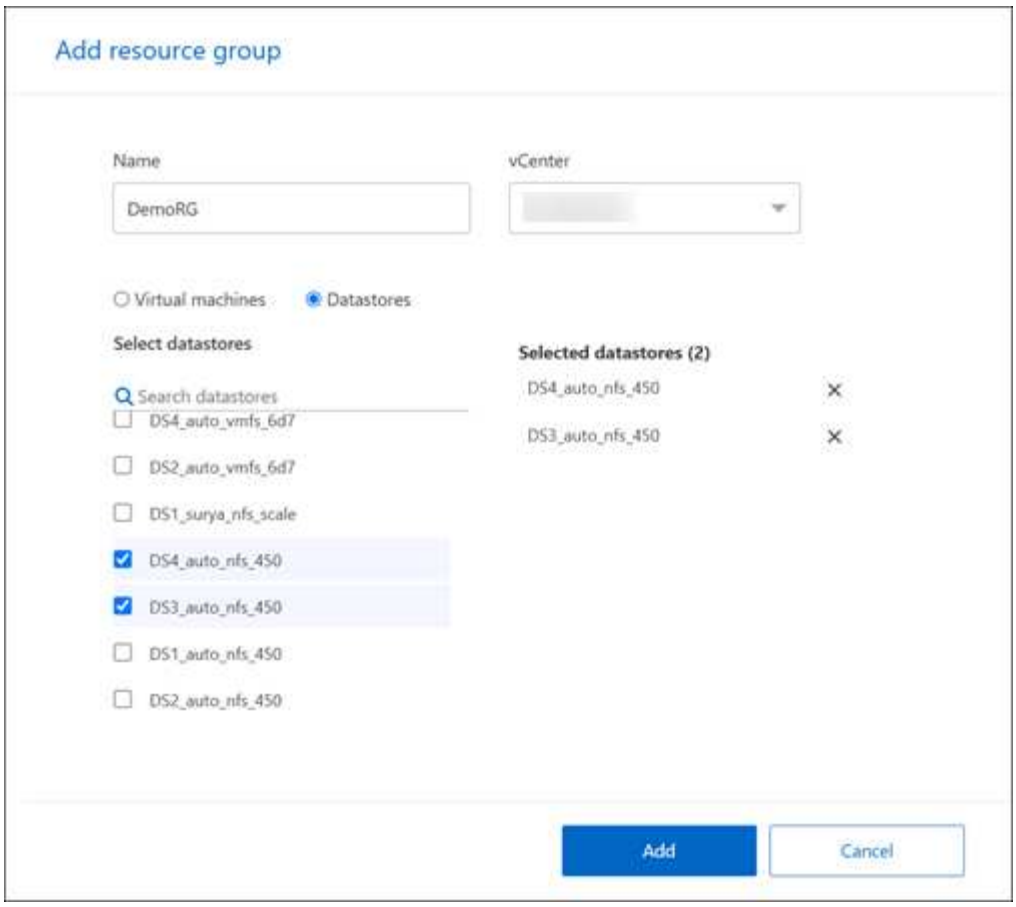
**MEJORES PRÁCTICAS**: Organice sus máquinas virtuales antes de implementar NetApp Disaster Recovery para minimizar la “expansión del almacén de datos”. Coloque las máquinas virtuales que necesitan protección en un subconjunto de almacenes de datos y coloque las máquinas virtuales que no van a estar protegidas en un subconjunto diferente de almacenes de datos. Asegúrese de que las máquinas virtuales en un almacén de

datos determinado no estén protegidas por diferentes planes de replicación.

**Pasos**

1. Iniciar sesión en el "Consola de NetApp" .
2. Desde el panel de navegación izquierdo de la consola NetApp , seleccione **Protección** > **Recuperación ante desastres**.
3. En el menú NetApp Disaster Recovery, seleccione **Grupos de recursos**.
4. Seleccione **Agregar**.
5. Introduzca un nombre para el grupo de recursos.
6. Seleccione el clúster vCenter de origen donde se encuentran las máquinas virtuales.
7. Seleccione **Máquinas virtuales** o **Almacenes de datos** según cómo desee buscar.
8. Seleccione la pestaña **Agregar grupos de recursos**. El sistema enumera todos los almacenes de datos o máquinas virtuales en el clúster de vCenter seleccionado. Si seleccionó **Almacenes de datos**, el sistema enumera todos los almacenes de datos en el clúster de vCenter seleccionado. Si seleccionó **Máquinas virtuales**, el sistema enumera todas las máquinas virtuales en el clúster vCenter seleccionado.
9. En el lado izquierdo de la página Agregar grupos de recursos, seleccione las máquinas virtuales que desea proteger.






10. Opcionalmente, cambie el orden de las máquinas virtuales a la derecha arrastrando cada máquina virtual hacia arriba o hacia abajo en la lista. Las máquinas virtuales se encenderán según la secuencia en que las incluya.
11. Seleccione **Agregar**.

# Crear un plan de replicación en NetApp Disaster Recovery

Una vez que haya agregado sitios de vCenter, estará listo para crear un plan de recuperación ante desastres o *replicación*. Los planes de replicación administran la protección de datos de la infraestructura de VMware. Seleccione los vCenters de origen y destino, elija los grupos de recursos y agrupe cómo se deben restaurar y encender las aplicaciones. Por ejemplo, puede agrupar máquinas virtuales (VM) asociadas con una aplicación o puede agrupar aplicaciones que tengan niveles similares. A estos planes a veces se les llama "proyectos".

**Rol de consola de NetApp requerido** Administrador de organización, Administrador de carpeta o proyecto, Administrador de recuperación ante desastres, Administrador de conmutación por error de recuperación ante desastres o Administrador de aplicación de recuperación ante desastres.

"Obtenga información sobre los roles y permisos de usuario en NetApp Disaster Recovery" . "Obtenga información sobre los roles de acceso a la consola de NetApp para todos los servicios" .

**Acerca de esta tarea**

Puede crear un plan de replicación y también editar cronogramas para cumplimiento y pruebas. Ejecute

conmutaciones por error de prueba de máquinas virtuales sin afectar las cargas de trabajo de producción.

Puede proteger varias máquinas virtuales en varios almacenes de datos. NetApp Disaster Recovery crea grupos de consistencia ONTAP para todos los volúmenes ONTAP que alojan almacenes de datos de máquinas virtuales protegidos.

Las máquinas virtuales solo se pueden proteger si el plan de replicación se encuentra en uno de los siguientes estados:

- Listo
- Conmutación por recuperación comprometida
- Prueba de conmutación por error confirmada

**Instantáneas del plan de replicación**

La recuperación ante desastres mantiene la misma cantidad de instantáneas en los clústeres de origen y destino. De forma predeterminada, el servicio realiza un proceso de conciliación de instantáneas cada 24 horas para garantizar que la cantidad de instantáneas en los clústeres de origen y destino sea la misma.

Las siguientes situaciones pueden provocar que la cantidad de instantáneas varíe entre los clústeres de origen y destino:

- Algunas situaciones pueden provocar que las operaciones de ONTAP fuera de la recuperación ante desastres agreguen o eliminen instantáneas del volumen:
  - Si faltan instantáneas en el sitio de origen, es posible que se eliminen las instantáneas correspondientes en el sitio de destino, según la política de SnapMirror predeterminada para la relación.
  - Si faltan instantáneas en el sitio de destino, el servicio podría eliminar las instantáneas correspondientes en el sitio de origen durante el próximo proceso de conciliación de instantáneas programado, según la política SnapMirror predeterminada para la relación.
- Una reducción en el recuento de retención de instantáneas del plan de replicación puede provocar que el servicio elimine las instantáneas más antiguas tanto en el sitio de origen como en el de destino para cumplir con el número de retención recientemente reducido.

En estos casos, Disaster Recovery elimina instantáneas más antiguas de los clústeres de origen y destino en la siguiente verificación de consistencia. O bien, el administrador puede realizar una limpieza de instantáneas inmediata seleccionando **Acciones*** ••• **icono en el plan de replicación y seleccionando *Limpiar instantáneas**.

El servicio realiza comprobaciones de simetría de instantáneas cada 24 horas.

**Antes de empezar**

Antes de crear una relación SnapMirror , configure el clúster y el emparejamiento SVM fuera de Disaster Recovery.

**MEJORES PRÁCTICAS**: Organice sus máquinas virtuales antes de implementar NetApp Disaster Recovery para minimizar la “expansión del almacén de datos”. Coloque las máquinas virtuales que necesitan protección en un subconjunto de almacenes de datos y coloque las máquinas virtuales que no van a estar protegidas en un subconjunto diferente de almacenes de datos. Utilice protección basada en almacén de datos para garantizar que las máquinas virtuales en cualquier almacén de datos determinado estén protegidas.

## Crear el plan

Un asistente le guiará a través de estos pasos:

- Seleccione servidores vCenter.
- Seleccione las máquinas virtuales o los almacenes de datos que desea replicar y asigne grupos de recursos.
- Mapee cómo los recursos del entorno de origen se asignan al destino.
- Establezca la frecuencia con la que se ejecuta el plan, ejecute un script alojado por el invitado, establezca el orden de arranque y seleccione el objetivo del punto de recuperación.
- Revisar el plan.

Al crear el plan, debes seguir estas pautas:

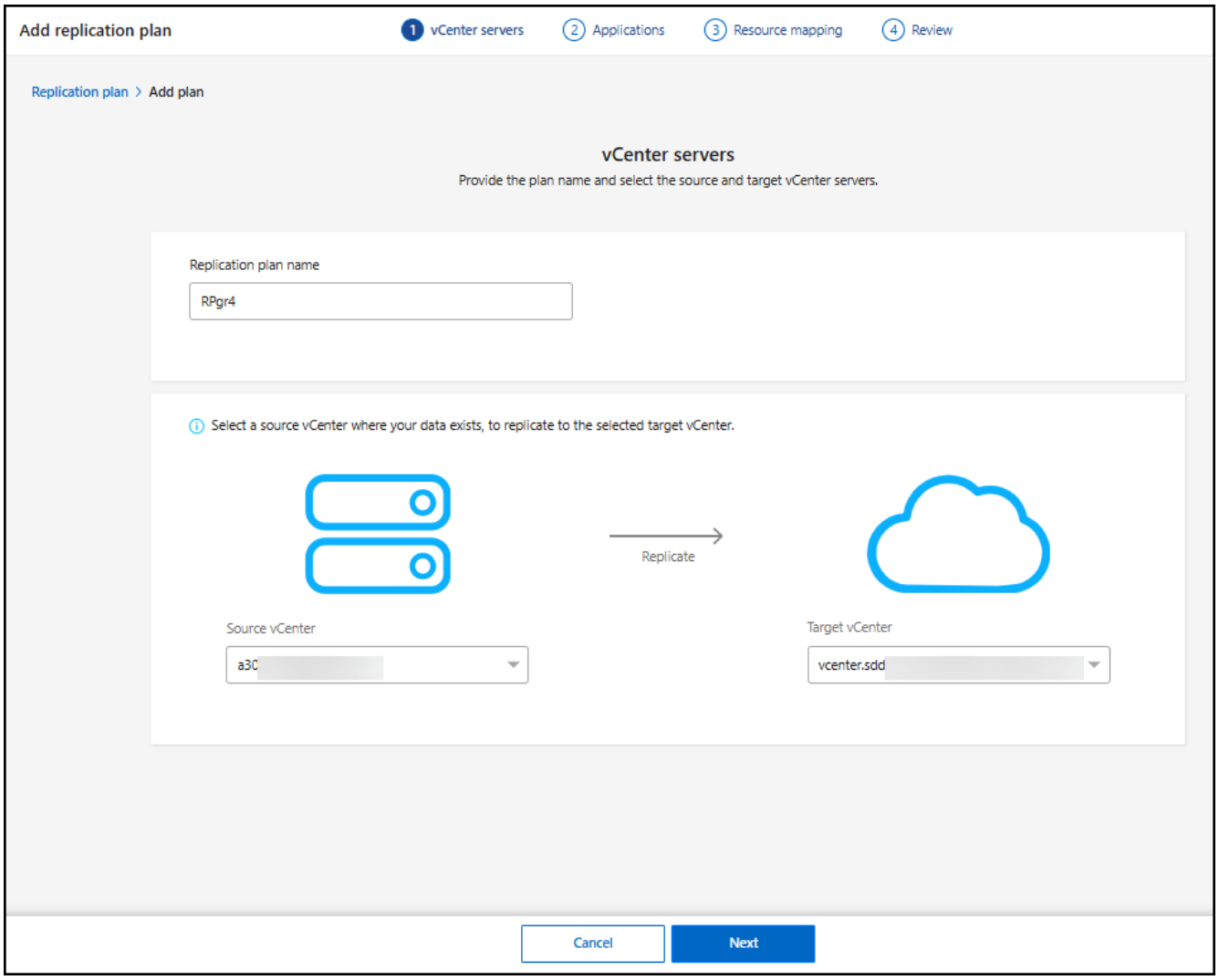
- Utilice las mismas credenciales para todas las máquinas virtuales del plan.
- Utilice el mismo script para todas las máquinas virtuales del plan.
- Utilice la misma subred, DNS y puerta de enlace para todas las máquinas virtuales del plan.

### Seleccionar servidores vCenter

Primero, seleccione el vCenter de origen y luego seleccione el vCenter de destino.

**Pasos**

1. Iniciar sesión en el "Consola de NetApp" .
2. Desde el panel de navegación izquierdo de la consola NetApp , seleccione **Protección** > **Recuperación ante desastres**.
3. En el menú NetApp Disaster Recovery, seleccione **Planes de replicación** y seleccione **Agregar**. O bien, si recién está comenzando a utilizar el servicio, desde el Panel de control, seleccione **Agregar plan de replicación**.




4. Crea un nombre para el plan de replicación.
5. Seleccione los vCenters de origen y de destino de las listas vCenters de origen y de destino.
6. Seleccione **Siguiente**.

### Seleccionar aplicaciones para replicar y asignar grupos de recursos

El siguiente paso es agrupar las máquinas virtuales o los almacenes de datos necesarios en grupos de recursos funcionales. Los grupos de recursos le permiten proteger un conjunto de máquinas virtuales o almacenes de datos con una instantánea común.

Al seleccionar aplicaciones en el plan de replicación, puede ver el sistema operativo de cada máquina virtual o almacén de datos en el plan. Esto es útil para decidir cómo agrupar máquinas virtuales o almacenes de datos en un grupo de recursos.

Cada grupo de recursos puede incluir una o más máquinas virtuales o almacenes de datos.

Al crear grupos de recursos, tenga en cuenta las siguientes cuestiones:

- Antes de agregar almacenes de datos a grupos de recursos, inicie primero un descubrimiento manual o un descubrimiento programado de las máquinas virtuales. Esto garantiza que las máquinas virtuales se detecten y se incluyan en el grupo de recursos. Si no activa un descubrimiento manual, es posible que las

máquinas virtuales no aparezcan en el grupo de recursos.

- Asegúrese de que haya al menos una máquina virtual en el almacén de datos. Si no hay máquinas virtuales en el almacén de datos, este no se descubrirá.
- Un único almacén de datos no debe alojar máquinas virtuales protegidas por más de un plan de replicación.
- No aloje máquinas virtuales protegidas y no protegidas en el mismo almacén de datos. Si las máquinas virtuales protegidas y no protegidas están alojadas en el mismo almacén de datos, podrían surgir los siguientes problemas:
  - Debido a que NetApp Disaster Recovery utiliza SnapMirror y el sistema replica volúmenes ONTAP completos, la capacidad utilizada de ese volumen se utiliza para consideraciones de licencia. En este caso, el espacio de volumen consumido por las máquinas virtuales protegidas y no protegidas se incluiría en este cálculo.
  - Si el grupo de recursos y sus almacenes de datos asociados deben conmutarse por error al sitio de recuperación ante desastres, todas las máquinas virtuales desprotegidas (máquinas virtuales que no forman parte del grupo de recursos, pero que están alojadas en el volumen de ONTAP ) ya no existirán en el sitio de origen debido al proceso de conmutación por error, lo que provocará una falla de las máquinas virtuales desprotegidas en el sitio de origen. Además, NetApp Disaster Recovery no iniciará aquellas máquinas virtuales desprotegidas en el sitio de vCenter de conmutación por error.
- Para que una VM esté protegida, debe estar incluida en un grupo de recursos.

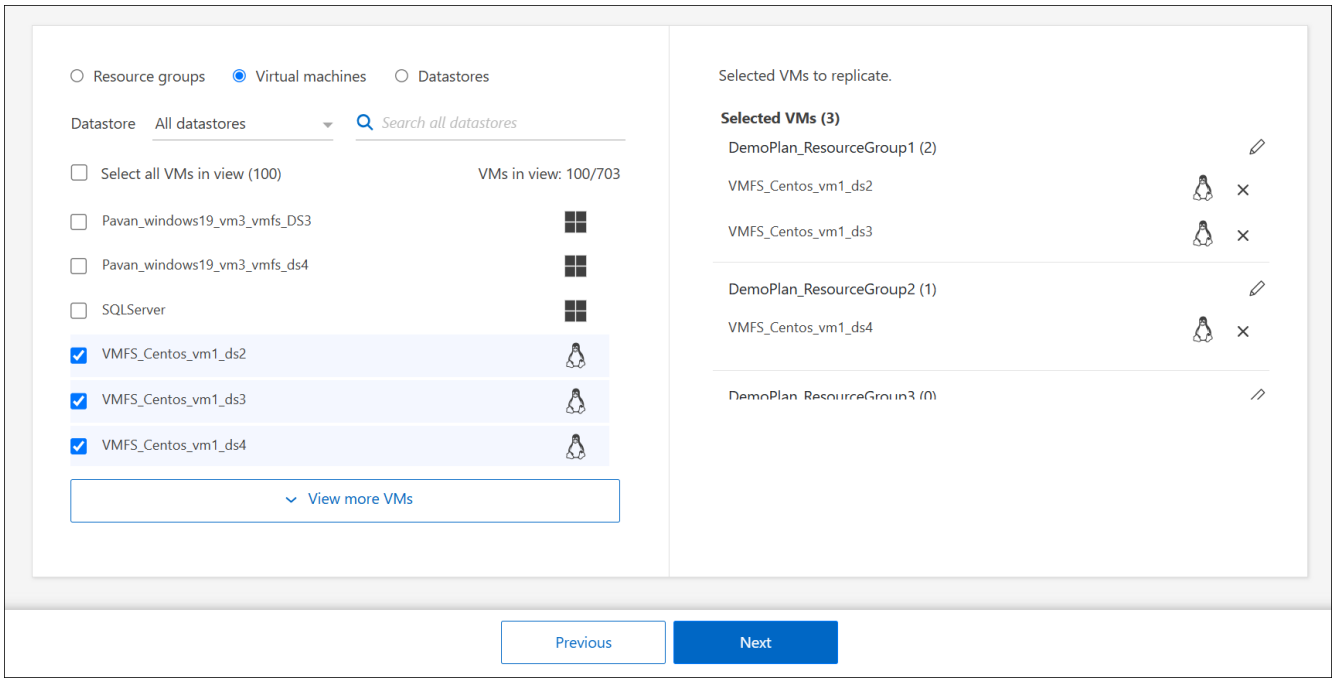
**MEJOR PRÁCTICA**: Cree un conjunto dedicado e independiente de asignaciones para sus pruebas de conmutación por error para evitar que las máquinas virtuales se conecten a redes de producción utilizando las mismas direcciones IP.

**Pasos**

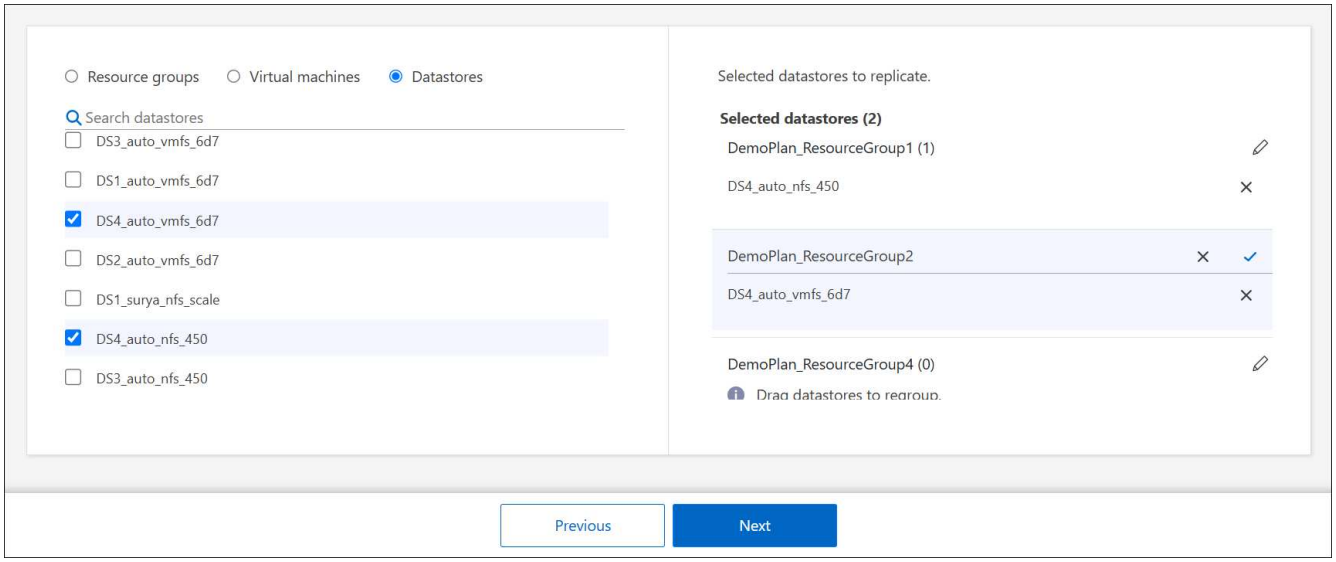
1. Seleccione **Máquinas virtuales** o **Almacenes de datos**.
2. Opcionalmente, busque una máquina virtual o un almacén de datos específico por nombre.
3. En el lado izquierdo de la página Aplicaciones, seleccione las máquinas virtuales o los almacenes de datos que desea proteger y asígnelos al grupo seleccionado.

   El vCenter de origen debe residir en el vCenter local. El vCenter de destino puede ser un segundo vCenter local en el mismo sitio o un sitio remoto, o un centro de datos definido por software (SDDC) basado en la nube, como VMware Cloud on AWS. Ambos vCenters ya deberían estar agregados a su entorno de trabajo de BlueXP disaster recovery .

   El recurso seleccionado se agrega automáticamente al grupo 1 y se inicia un nuevo grupo 2. Cada vez que se agrega un recurso al último grupo, se agrega otro grupo.




O, para almacenes de datos:




4. Opcionalmente, realice cualquiera de las siguientes acciones:
   - Para cambiar el nombre del grupo, haga clic en el grupo *Editar* icono.
   - Para eliminar un recurso de un grupo, seleccione **X** junto al recurso.
   - Para mover un recurso a un grupo diferente, arrástrelo y suéltelo en el nuevo grupo.

> Para mover un almacén de datos a un grupo de recursos diferente, anule la selección del almacén de datos no deseado y envíe el plan de replicación. Luego, cree o edite el otro plan de replicación y vuelva a seleccionar el almacén de datos.

5. Seleccione **Siguiente**.

### Asignar recursos de origen al destino

En el paso de mapeo de recursos, especifique cómo deben mapearse los recursos del entorno de origen al destino. Al crear un plan de replicación, puede establecer un retraso y un orden de arranque para cada máquina virtual en el plan. Esto le permite establecer una secuencia para que se inicien las máquinas virtuales.

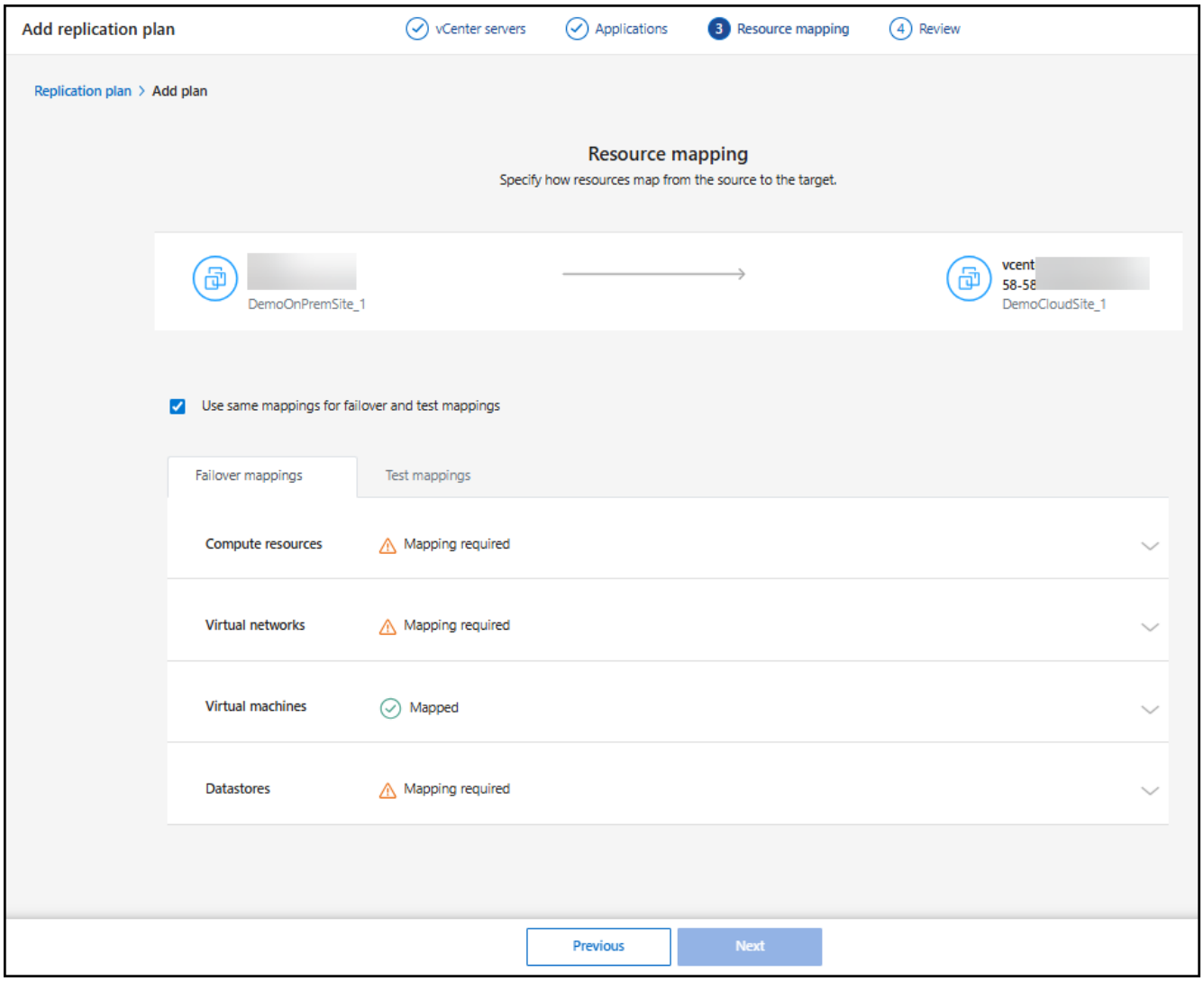
Si planea realizar conmutaciones por error de prueba como parte de su plan de recuperación ante desastres, debe proporcionar un conjunto de asignaciones de conmutación por error de prueba para garantizar que las máquinas virtuales iniciadas durante la prueba de conmutación por error no interfieran con las máquinas virtuales de producción. Puede lograr esto proporcionando a las máquinas virtuales de prueba direcciones IP diferentes o asignando las NIC virtuales de las máquinas virtuales de prueba a una red diferente que esté aislada de la producción pero que tenga la misma configuración IP (conocida como *burbuja* o *red de prueba*).

#### Antes de empezar

Si desea crear una relación SnapMirror en este servicio, el clúster y su emparejamiento SVM ya deben haberse configurado fuera de NetApp Disaster Recovery.

#### Pasos

1. En la página de mapeo de recursos, para usar las mismas asignaciones para las operaciones de prueba y conmutación por error, marque la casilla.



2. En la pestaña Asignaciones de conmutación por error, seleccione la flecha hacia abajo a la derecha de cada recurso y asigne los recursos en cada sección:
    - Recursos computacionales
    - Redes virtuales
    - Máquinas virtuales
    - Almacenes de datos

**Recursos de mapas > Sección de recursos informáticos**

La sección Recursos de cómputo define dónde se restaurarán las máquinas virtuales después de una conmutación por error. Asigne el centro de datos y el clúster de vCenter de origen a un centro de datos y un clúster de destino.

Opcionalmente, las máquinas virtuales se pueden reiniciar en un host vCenter ESXi específico. Si VMWare DRS está habilitado, puede mover la VM a un host alternativo automáticamente si es necesario para cumplir con la política de DR configurada.

Opcionalmente, puede colocar todas las máquinas virtuales en este plan de replicación en una carpeta única con vCenter. Esto proporciona una forma sencilla de organizar rápidamente las máquinas virtuales conmutadas por error dentro del vCenter.

Seleccione la flecha hacia abajo junto a **Recursos informáticos**.

- **Centros de datos de origen y destino**
- **Clúster objetivo**
- **Host de destino** (opcional): después de seleccionar el clúster, puede configurar esta información.

Si un vCenter tiene un Programador de recursos distribuidos (DRS) configurado para administrar varios hosts en un clúster, no es necesario seleccionar un host. Si selecciona un host, NetApp Disaster Recovery colocará todas las máquinas virtuales en el host seleccionado. * **Carpeta de máquina virtual de destino** (opcional): crea una nueva carpeta raíz para almacenar las máquinas virtuales seleccionadas.

**Recursos cartográficos > Sección de redes virtuales**

Las máquinas virtuales utilizan NIC virtuales conectadas a redes virtuales. En el proceso de conmutación por error, el servicio conecta estas NIC virtuales a redes virtuales definidas en el entorno VMware de destino. Para cada red virtual de origen utilizada por las máquinas virtuales en el grupo de recursos, el servicio requiere una asignación de red virtual de destino.

Puede asignar varias redes virtuales de origen a la misma red virtual de destino. Sin embargo, esto podría crear conflictos de configuración de red IP. Puede asignar varias redes de origen a una única red de destino para garantizar que todas las redes de origen tengan la misma configuración.

En la pestaña Mapeos de conmutación por error, seleccione la flecha hacia abajo junto a **Redes virtuales**. Seleccione la LAN virtual de origen y la LAN virtual de destino.

Seleccione la asignación de red a la LAN virtual adecuada. Las LAN virtuales ya deberían estar aprovisionadas, así que seleccione la LAN virtual adecuada para asignar la VM.

**Recursos de mapas > Sección de máquinas virtuales**

Puede configurar cada máquina virtual en el grupo de recursos protegido por el plan de replicación para que se adapte al entorno virtual de vCenter de destino configurando cualquiera de las siguientes opciones:

- El número de CPU virtuales
- La cantidad de DRAM virtual
- La configuración de la dirección IP
- La capacidad de ejecutar scripts de shell del sistema operativo invitado como parte del proceso de conmutación por error
- La capacidad de cambiar los nombres de las máquinas virtuales conmutadas por error mediante un prefijo y un sufijo únicos
- La capacidad de establecer el orden de reinicio durante la conmutación por error de la máquina virtual

En la pestaña Mapeos de conmutación por error, seleccione la flecha hacia abajo junto a **Máquinas virtuales**.

El valor predeterminado para las máquinas virtuales está asignado. La asignación predeterminada utiliza las mismas configuraciones que usan las máquinas virtuales en el entorno de producción (misma dirección IP, máscara de subred y puerta de enlace).

Si realiza algún cambio en la configuración predeterminada, deberá cambiar el campo IP de destino a "Diferente de la fuente".

Si cambia la configuración a "Diferente de la fuente", deberá proporcionar las credenciales del sistema operativo invitado de la máquina virtual.

Esta sección puede mostrar diferentes campos dependiendo de su selección.

Puede aumentar o disminuir la cantidad de CPU virtuales asignadas a cada máquina virtual conmutada por error. Sin embargo, cada VM requiere al menos una CPU virtual. Puede cambiar la cantidad de CPU virtuales y DRAM virtuales asignadas a cada VM. El motivo más común por el que podría querer cambiar la configuración predeterminada de CPU virtual y DRAM virtual es si los nodos del clúster vCenter de destino no tienen tantos recursos disponibles como el clúster vCenter de origen.

**Configuración de red** Disaster Recovery admite un amplio conjunto de opciones de configuración para redes de máquinas virtuales. Es posible que sea necesario cambiarlos si el sitio de destino tiene redes virtuales que usan configuraciones TCP/IP diferentes a las redes virtuales de producción en el sitio de origen.

En el nivel más básico (y predeterminado), la configuración simplemente utiliza la misma configuración de red TCP/IP para cada VM en el sitio de destino que la utilizada en el sitio de origen. Esto requiere que configure los mismos ajustes TCP/IP en las redes virtuales de origen y destino.

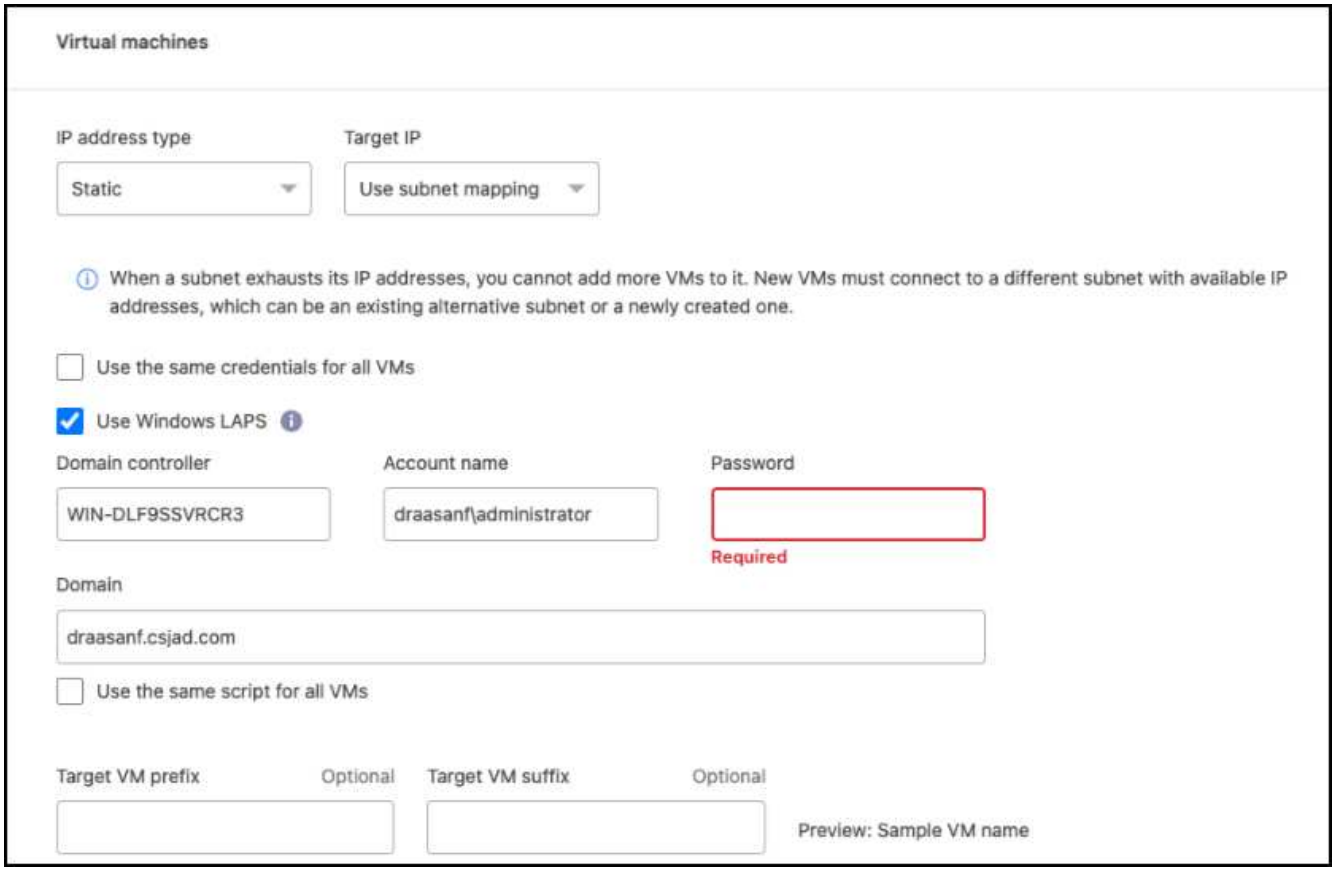
El servicio admite configuraciones de red de IP estática o de protocolo de configuración dinámica de host (DHCP) para máquinas virtuales. DHCP proporciona un método basado en estándares para configurar dinámicamente los parámetros TCP/IP de un puerto de red host. DHCP debe proporcionar, como mínimo, una dirección TCP/IP y también puede proporcionar una dirección de puerta de enlace predeterminada (para enrutar a una conexión a Internet externa), una máscara de subred y una dirección de servidor DNS. El DHCP se utiliza comúnmente para dispositivos informáticos de usuarios finales, como computadoras de escritorio, portátiles y conexiones de teléfonos móviles de empleados, aunque también se puede utilizar para cualquier dispositivo informático en red, como servidores.

- Opción **Usar la misma máscara de subred, DNS y configuración de puerta de enlace**: debido a que

estas configuraciones suelen ser las mismas para todas las máquinas virtuales conectadas a las mismas redes virtuales, es posible que le resulte más fácil configurarlas una vez y dejar que Disaster Recovery use las configuraciones para todas las máquinas virtuales en el grupo de recursos protegido por el plan de replicación. Si algunas máquinas virtuales usan configuraciones diferentes, deberá desmarcar esta casilla y proporcionar esas configuraciones para cada máquina virtual.

- **Tipo de dirección IP**: reconfigura la configuración de las máquinas virtuales para que coincida con los requisitos de la red virtual de destino. NetApp Disaster Recovery ofrece dos opciones: DHCP o IP estática. Para direcciones IP estáticas, configure la máscara de subred, la puerta de enlace y los servidores DNS. Además, ingrese las credenciales para las máquinas virtuales.
  - **DHCP**: seleccione esta configuración si desea que sus máquinas virtuales obtengan información de configuración de red de un servidor DHCP. Si elige esta opción, proporcionará únicamente las credenciales para la máquina virtual.
  - **IP estática**: seleccione esta configuración si desea especificar la información de configuración de IP manualmente. Puede seleccionar una de las siguientes opciones: igual que la fuente, diferente de la fuente o asignación de subred. Si elige lo mismo que la fuente, no necesita ingresar credenciales. Por otro lado, si elige utilizar información diferente de la fuente, puede proporcionar las credenciales, la dirección IP de la VM, la máscara de subred, el DNS y la información de la puerta de enlace. Las credenciales del sistema operativo invitado de la máquina virtual se deben proporcionar al nivel global o a cada nivel de la máquina virtual.

    Esto puede ser muy útil al recuperar entornos grandes en clústeres de destino más pequeños o para realizar pruebas de recuperación ante desastres sin tener que aprovisionar una infraestructura VMware física uno a uno.




- **Scripts**: puede incluir scripts personalizados alojados en el sistema operativo invitado en formato .sh, .bat o .ps1 como procesos posteriores. Con scripts personalizados, la BlueXP disaster recovery puede ejecutar su script después de una conmutación por error, una recuperación y procesos de migración. Por ejemplo,

puede utilizar un script personalizado para reanudar todas las transacciones de la base de datos una vez completada la conmutación por error. El servicio puede ejecutar scripts dentro de máquinas virtuales que ejecutan Microsoft Windows o cualquier variante de Linux compatible con parámetros de línea de comandos admitidos. Puede asignar un script a máquinas virtuales individuales o a todas las máquinas virtuales en el plan de replicación.

Para habilitar la ejecución de scripts con el sistema operativo invitado de la máquina virtual, se deben cumplir las siguientes condiciones:

- VMware Tools debe estar instalado en la máquina virtual.
- Se deben proporcionar credenciales de usuario apropiadas con privilegios de sistema operativo invitado adecuados para ejecutar el script.
- Opcionalmente, incluya un valor de tiempo de espera en segundos para el script.

  **Máquinas virtuales que ejecutan Microsoft Windows**: pueden ejecutar scripts por lotes de Windows (.bat) o de PowerShell (ps1). Los scripts de Windows pueden utilizar argumentos de línea de comandos. Formatear cada argumento en el `arg_name$value` formato, donde `arg_name` es el nombre del argumento y `$value` es el valor del argumento y un punto y coma separa cada uno `argument$value` par.

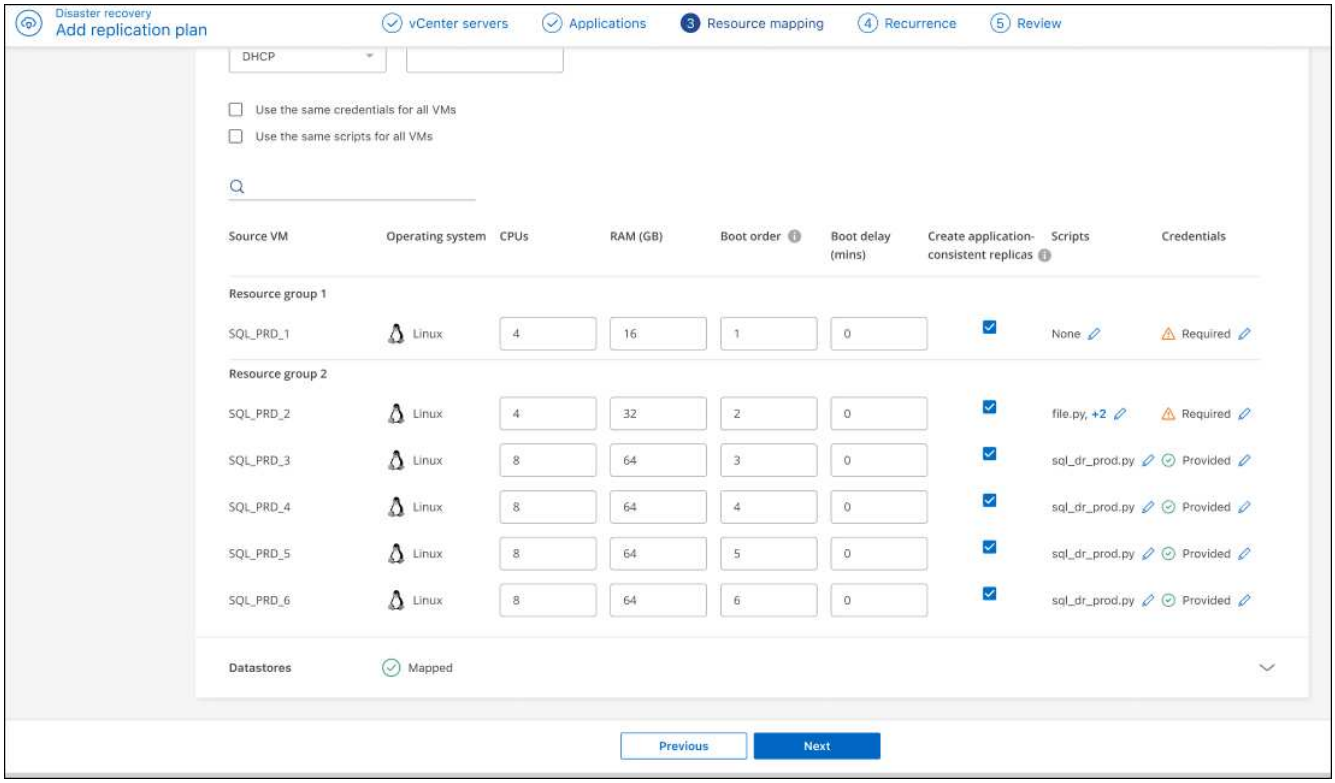
**Máquinas virtuales que ejecutan Linux**: pueden ejecutar cualquier script de shell (.sh) compatible con la versión de Linux utilizada por la máquina virtual. Los scripts de Linux pueden utilizar argumentos de línea de comandos. Proporcione argumentos en una lista de valores separados por punto y coma. No se admiten argumentos con nombre. Añade cada argumento a la `Arg[x]` lista de argumentos y hacer referencia a cada valor mediante un puntero a la `Arg[x]` matriz, por ejemplo, `value1;value2;value3` .

- **Prefijo y sufijo de la máquina virtual de destino**: en los detalles de las máquinas virtuales, puede agregar opcionalmente un prefijo y un sufijo a cada nombre de máquina virtual conmutada por error. Esto puede resultar útil para diferenciar las máquinas virtuales conmutadas por error de las máquinas virtuales de producción que se ejecutan en el mismo clúster de vCenter. Por ejemplo, puede agregar un prefijo "DR-" y un sufijo "-failover" al nombre de la VM. Algunas personas agregan un segundo vCenter de producción para alojar máquinas virtuales temporalmente en un sitio diferente en caso de desastre. Agregar un prefijo o sufijo puede ayudarle a identificar rápidamente las máquinas virtuales conmutadas por error. También puedes usar el prefijo o sufijo en scripts personalizados.

  Puede utilizar el método alternativo para configurar la carpeta de la máquina virtual de destino en la sección Recursos de cómputo.

- **CPU y RAM de la máquina virtual de origen**: en los detalles de las máquinas virtuales, puede cambiar opcionalmente el tamaño de los parámetros de CPU y RAM de la máquina virtual.

  Puede configurar la DRAM en gigabytes (GiB) o megabytes (MiB). Si bien cada VM requiere al menos un MiB de RAM, la cantidad real debe garantizar que el sistema operativo invitado de la VM y cualquier aplicación en ejecución puedan funcionar de manera eficiente.




- **Orden de arranque**: puede modificar el orden de arranque después de una conmutación por error para todas las máquinas virtuales seleccionadas en los grupos de recursos. De forma predeterminada, todas las máquinas virtuales arrancan juntas en paralelo; sin embargo, puedes realizar cambios en esta etapa. Esto es útil para garantizar que todas las máquinas virtuales de prioridad uno se estén ejecutando antes de que se inicien las máquinas virtuales de prioridad posterior.

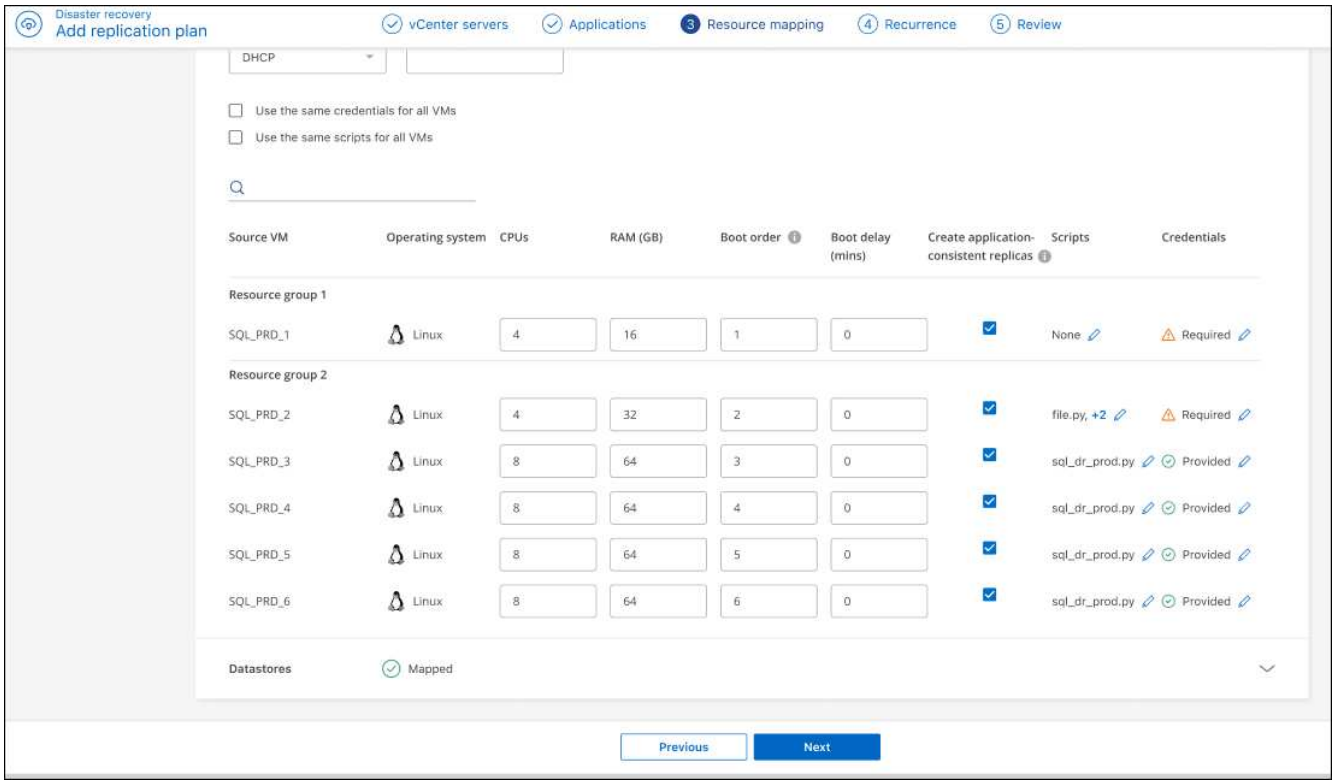
  La BlueXP disaster recovery inicia cualquier máquina virtual con el mismo número de orden de inicio en paralelo.

  - Arranque secuencial: asigna a cada VM un número único para arrancar en el orden asignado, por ejemplo, 1, 2, 3, 4, 5.
  - Arranque simultáneo: asigne el mismo número a todas las máquinas virtuales para iniciarlas al mismo tiempo, por ejemplo, 1,1,1,1,2,2,3,4,4.
- **Retraso de arranque**: ajusta el retraso en minutos de la acción de arranque, indicando la cantidad de tiempo que la VM esperará antes de iniciar el proceso de encendido. Introduzca un valor de 0 a 10 minutos.

> Para restablecer el orden de arranque al predeterminado, seleccione **Restablecer configuración de VM a predeterminada** y luego elija qué configuración desea cambiar a la predeterminada.

- **Crear réplicas consistentes con la aplicación**: indica si se deben crear copias de instantáneas consistentes con la aplicación. El servicio inactivará la aplicación y luego tomará una instantánea para obtener un estado consistente de la aplicación. Esta función es compatible con Oracle ejecutándose en Windows y Linux y con SQL Server ejecutándose en Windows. Ver más detalles a continuación.
- **Usar Windows LAPS**: si está utilizando la Solución de contraseña de administrador local de Windows (Windows LAPS), marque esta casilla. Esta opción solo está disponible si ha seleccionado la opción **IP estática**. Al marcar esta casilla, no es necesario que proporcione una contraseña para cada una de sus máquinas virtuales. En su lugar, proporciona los detalles del controlador de dominio.

Si no utiliza Windows LAPS, entonces la VM es una VM de Windows y la opción de credenciales en la fila de VM está habilitada. Puede proporcionar las credenciales para la VM.




**Crear réplicas consistentes con la aplicación**

Muchas máquinas virtuales alojan servidores de bases de datos como Oracle o Microsoft SQL Server. Estos servidores de bases de datos requieren instantáneas consistentes con la aplicación para garantizar que la base de datos esté en un estado consistente cuando se toma la instantánea.

Las instantáneas consistentes con la aplicación garantizan que la base de datos esté en un estado consistente cuando se toma la instantánea. Esto es importante porque garantiza que la base de datos pueda restaurarse a un estado consistente después de una operación de conmutación por error o recuperación.

Los datos administrados por el servidor de base de datos pueden estar alojados en el mismo almacén de datos que la máquina virtual que aloja el servidor de base de datos o pueden estar alojados en un almacén de datos diferente. La siguiente tabla muestra las configuraciones admitidas para instantáneas consistentes con la aplicación en recuperación ante desastres:

| Ubicación de los datos | Apoyado | Notas |
|---|---|---|
| Dentro del mismo almacén de datos de vCenter que la máquina virtual | Sí | Debido a que el servidor de base de datos y la base de datos residen en el mismo almacén de datos, tanto el servidor como los datos estarán sincronizados en caso de conmutación por error. |

| Ubicación de los datos | Apoyado | Notas |
| --- | --- | --- |
| Dentro de un almacén de datos de vCenter diferente al de la máquina virtual | No | La recuperación ante desastres no puede identificar cuándo los datos de un servidor de base de datos están en un almacén de datos de vCenter diferente. El servicio no puede replicar los datos, pero puede replicar la máquina virtual del servidor de base de datos.<br><br>Si bien los datos de la base de datos no se pueden replicar, el servicio garantiza que el servidor de la base de datos realice todos los pasos necesarios para garantizar que la base de datos esté inactiva en el momento de la copia de seguridad de la máquina virtual. |
| Dentro de una fuente de datos externa | No | Si los datos residen en un LUN o recurso compartido NFS montado por el invitado, Disaster Recovery no puede replicar los datos, pero puede replicar la máquina virtual del servidor de base de datos.<br><br>Si bien los datos de la base de datos no se pueden replicar, el servicio garantiza que el servidor de la base de datos realice todos los pasos necesarios para garantizar que la base de datos esté inactiva en el momento de la copia de seguridad de la máquina virtual. |

Durante una copia de seguridad programada, Disaster Recovery inactiva el servidor de base de datos y luego toma una instantánea de la máquina virtual que aloja el servidor de base de datos. Esto garantiza que la base de datos esté en un estado consistente cuando se toma la instantánea.

- Para las máquinas virtuales de Windows, el servicio utiliza el Servicio de instantáneas de volumen (VSS) de Microsoft para coordinarse con cualquiera de los servidores de base de datos.
- Para las máquinas virtuales Linux, el servicio utiliza un conjunto de scripts para colocar el servidor Oracle en modo de respaldo.

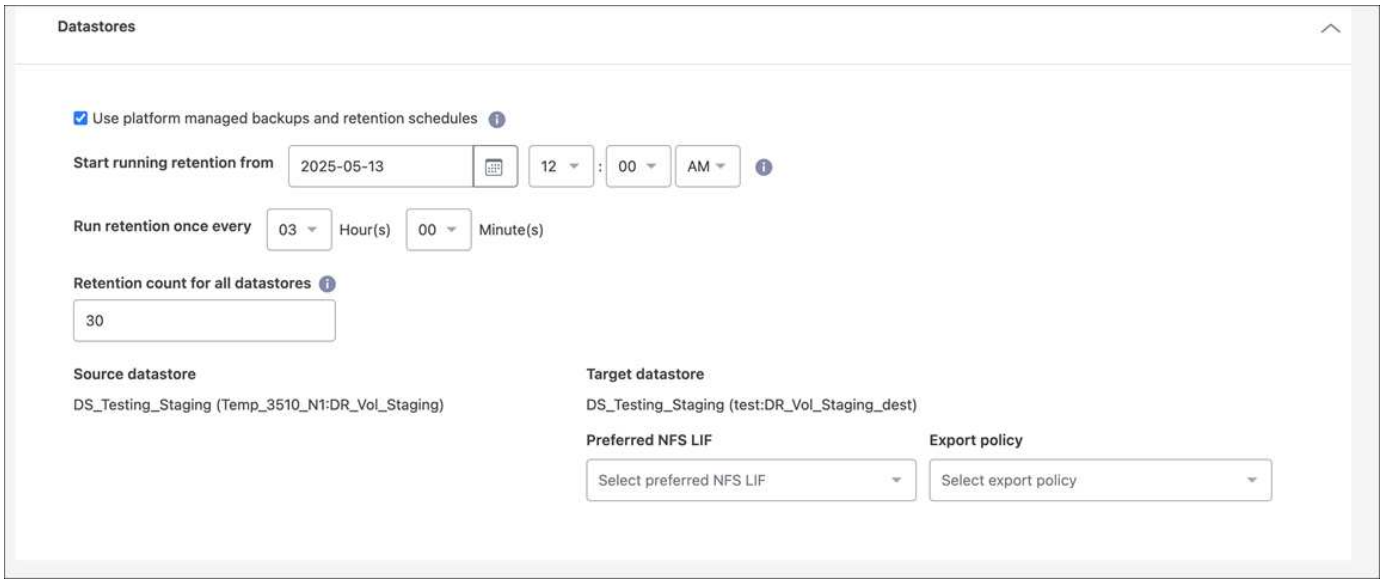
Para habilitar réplicas consistentes con la aplicación de las máquinas virtuales y sus almacenes de datos de alojamiento, marque la casilla junto a **Crear réplicas consistentes con la aplicación** para cada máquina virtual y proporcione credenciales de inicio de sesión de invitado con los privilegios adecuados.

**Recursos de mapas > Sección Almacenes de datos**

Los almacenes de datos de VMware están alojados en volúmenes ONTAP FlexVol o LUN iSCSI o FC de ONTAP mediante VMware VMFS. Utilice la sección Almacenes de datos para definir el clúster ONTAP de destino, la máquina virtual de almacenamiento (SVM) y el volumen o LUN para replicar los datos del disco al destino.

Seleccione la flecha hacia abajo junto a **Almacenes de datos**. Según la selección de máquinas virtuales, las asignaciones de almacenes de datos se seleccionan automáticamente.

Esta sección puede estar habilitada o deshabilitada según su selección.




- **Utilizar copias de seguridad administradas por la plataforma y programas de retención**: si está utilizando una solución de administración de instantáneas externa, marque esta casilla. NetApp Disaster Recovery admite el uso de soluciones de gestión de instantáneas externas, como el programador de políticas nativo ONTAP SnapMirror o integraciones de terceros. Si cada almacén de datos (volumen) en el plan de replicación ya tiene una relación SnapMirror que se administra en otro lugar, puede usar esas instantáneas como puntos de recuperación en NetApp Disaster Recovery.

  Cuando se selecciona esta opción, NetApp Disaster Recovery no configura una programación de respaldo. Sin embargo, aún es necesario configurar un programa de retención porque aún se podrían tomar instantáneas para operaciones de prueba, conmutación por error y recuperación.

  Una vez configurado esto, el servicio no toma ninguna instantánea programada regularmente, sino que depende de la entidad externa para tomar y actualizar esas instantáneas.

- **Hora de inicio**: Ingrese la fecha y la hora en que desea que comiencen a ejecutarse las copias de seguridad y la retención.
- **Intervalo de ejecución**: Ingrese el intervalo de tiempo en horas y minutos. Por ejemplo, si ingresa 1 hora, el servicio tomará una instantánea cada hora.
- **Recuento de retención**: Ingrese la cantidad de instantáneas que desea conservar.

  La cantidad de instantáneas retenidas junto con la tasa de cambio de datos entre cada instantánea determina la cantidad de espacio de almacenamiento consumido tanto en el origen como en el destino. Cuanto más instantáneas conserve, más espacio de almacenamiento se consumirá.

- **Almacenes de datos de origen y destino**: si existen múltiples relaciones SnapMirror (de distribución), puede seleccionar el destino que desea utilizar. Si un volumen ya tiene una relación SnapMirror establecida, aparecen los almacenes de datos de origen y destino correspondientes. Si un volumen no tiene una relación SnapMirror , puede crear uno ahora seleccionando un clúster de destino, seleccionando un SVM de destino y proporcionando un nombre de volumen. El servicio creará el volumen y la relación SnapMirror .

  Si desea crear una relación SnapMirror en este servicio, el clúster y su emparejamiento SVM ya deben haberse configurado fuera de NetApp Disaster Recovery.

- Si las máquinas virtuales son del mismo volumen y del mismo SVM, el servicio realiza una instantánea de ONTAP estándar y actualiza los destinos secundarios.
- Si las máquinas virtuales son de diferentes volúmenes y del mismo SVM, el servicio crea una instantánea del grupo de consistencia incluyendo todos los volúmenes y actualiza los destinos secundarios.
- Si las máquinas virtuales son de diferentes volúmenes y diferentes SVM, el servicio realiza una instantánea de la fase de inicio y la fase de confirmación del grupo de consistencia incluyendo todos los volúmenes en el mismo clúster o en uno diferente y actualiza los destinos secundarios.
- Durante la conmutación por error, puede seleccionar cualquier instantánea. Si selecciona la última instantánea, el servicio crea una copia de seguridad a pedido, actualiza el destino y utiliza esa instantánea para la conmutación por error.

- **LIF NFS preferido** y **Política de exportación**: normalmente, deje que el servicio seleccione el LIF NFS preferido y la política de exportación. Si desea utilizar una política de exportación o LIF de NFS específica, seleccione la flecha hacia abajo junto a cada campo y seleccione la opción adecuada.

  Opcionalmente, puede utilizar interfaces de datos específicas (LIF) para un volumen después de un evento de conmutación por error. Esto es útil para equilibrar el tráfico de datos si el SVM de destino tiene múltiples LIF.

  Para un control adicional sobre la seguridad del acceso a los datos del NAS, el servicio puede asignar políticas de exportación de NAS específicas a diferentes volúmenes de almacenamiento de datos. Las políticas de exportación definen las reglas de control de acceso para los clientes NFS que acceden a los volúmenes del almacén de datos. Si no especifica una política de exportación, el servicio utiliza la política de exportación predeterminada para SVM.

**MEJORES PRÁCTICAS**: Le recomendamos encarecidamente que cree una política de exportación dedicada que limite el acceso al volumen únicamente a los hosts vCenter ESXi de origen y destino que alojarán las máquinas virtuales protegidas. Esto ayuda a garantizar que las entidades externas no puedan acceder a la exportación NFS.

### Agregar asignaciones de conmutación por error de prueba

**Pasos**

1. Para configurar diferentes asignaciones para el entorno de prueba, desmarque la casilla y seleccione la pestaña **Asignaciones de prueba**.
2. Revise cada pestaña como antes, pero esta vez para el entorno de prueba.

   En la pestaña Asignaciones de prueba, las asignaciones de máquinas virtuales y almacenes de datos están deshabilitadas.

   Podrás probar el plan completo más tarde. En este momento, estás configurando las asignaciones para el entorno de prueba.

### Revisar el plan de replicación

Por último, tómese unos momentos para revisar el plan de replicación.

Posteriormente podrá deshabilitar o eliminar el plan de replicación.

**Pasos**

1. Revise la información en cada pestaña: Detalles del plan, Mapeo de conmutación por error y Máquinas virtuales.
2. Seleccione **Agregar plan**.

   El plan se agrega a la lista de planes.

## Edite los cronogramas para probar el cumplimiento y garantizar que las pruebas de conmutación por error funcionen

Es posible que desees configurar cronogramas para probar pruebas de cumplimiento y conmutación por error para asegurarte de que funcionarán correctamente si las necesitas.

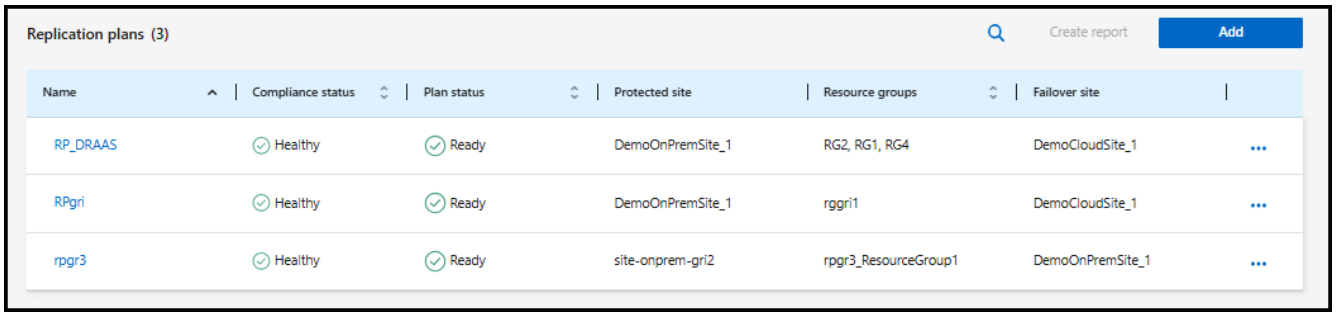
- **Impacto en el tiempo de cumplimiento**: cuando se crea un plan de replicación, el servicio crea un programa de cumplimiento de forma predeterminada. El tiempo de cumplimiento predeterminado es de 30 minutos. Para cambiar este tiempo, puede editar la programación en el plan de replicación.
- **Impacto de la conmutación por error de prueba**: puede probar un proceso de conmutación por error a pedido o según un cronograma. Esto le permite probar la conmutación por error de máquinas virtuales a un destino especificado en un plan de replicación.

  Una conmutación por error de prueba crea un volumen FlexClone , monta el almacén de datos y mueve la carga de trabajo en ese almacén de datos. Una operación de conmutación por error de prueba *no* afecta las cargas de trabajo de producción, la relación SnapMirror utilizada en el sitio de prueba y las cargas de trabajo protegidas que deben seguir funcionando normalmente.

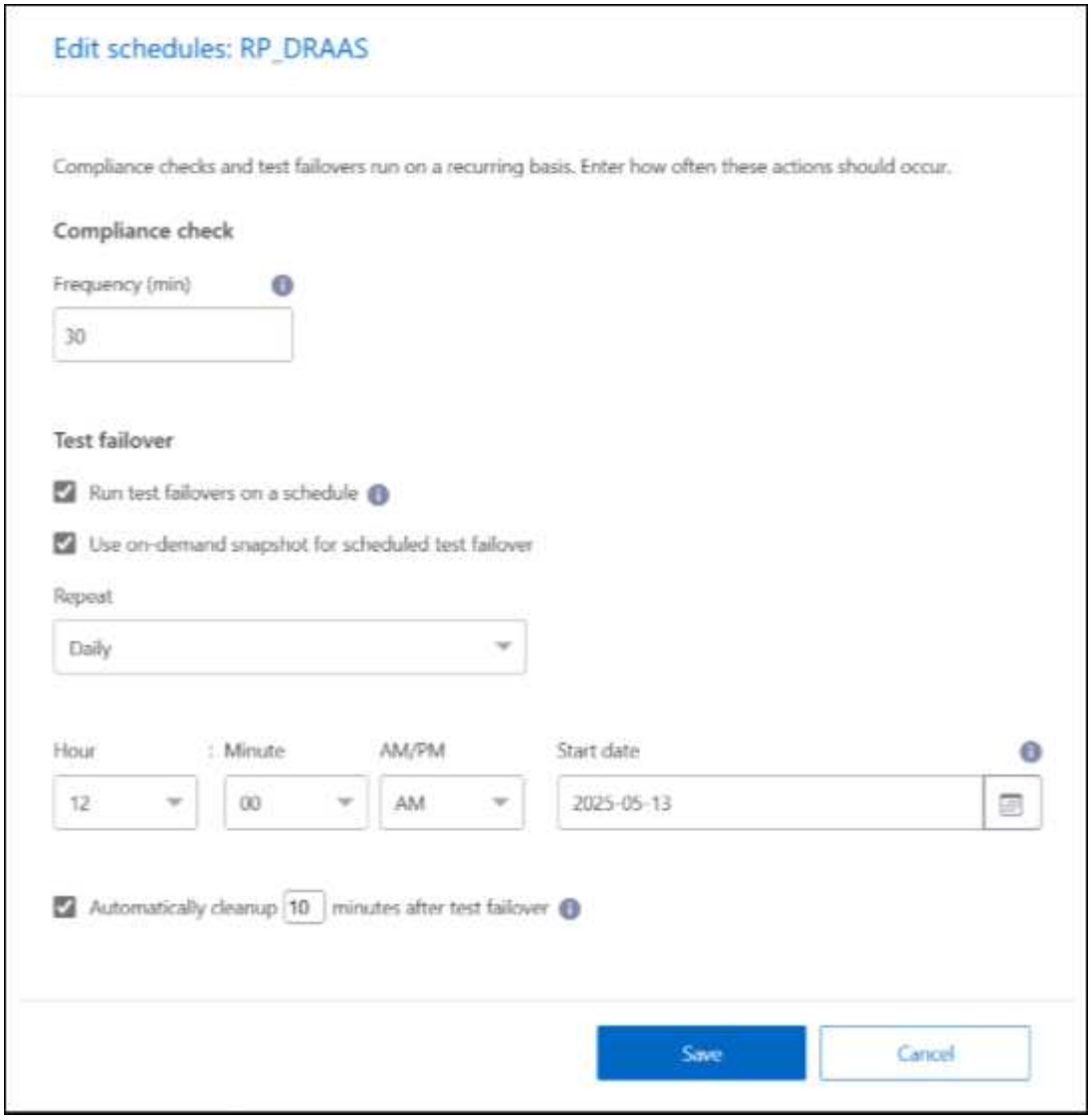
Según el cronograma, se ejecuta la prueba de conmutación por error y garantiza que las cargas de trabajo se muevan al destino especificado por el plan de replicación.

**Pasos**

1. En el menú NetApp Disaster Recovery, seleccione **Planes de replicación**.




2. Seleccione las **Acciones*** ••• **icono y seleccione *Editar horarios**.
3. Ingrese la frecuencia en minutos con la que desea que NetApp Disaster Recovery verifique el cumplimiento de las pruebas.
4. Para comprobar que sus pruebas de conmutación por error funcionan correctamente, marque **Ejecutar conmutaciones por error según una programación mensual**.
   a. Seleccione el día del mes y la hora en que desea que se ejecuten estas pruebas.
   b. Ingrese la fecha en formato aaaa-mm-dd en la que desea que comience la prueba.




5. **Usar instantánea a pedido para conmutación por error de prueba programada**: para tomar una nueva instantánea antes de iniciar la conmutación por error de prueba automatizada, marque esta casilla.
6. Para limpiar el entorno de prueba una vez finalizada la prueba de conmutación por error, marque **Limpiar automáticamente después de la conmutación por error de prueba** e ingrese la cantidad de minutos que desea esperar antes de que comience la limpieza.

> Este proceso anula el registro de las máquinas virtuales temporales de la ubicación de prueba, elimina el volumen FlexClone que se creó y desmonta los almacenes de datos temporales.

7. Seleccione **Guardar**.

# Replique aplicaciones a otro sitio con NetApp Disaster Recovery

Con NetApp Disaster Recovery, puede replicar aplicaciones de VMware en su sitio de origen a un sitio remoto de recuperación ante desastres en la nube mediante la replicación SnapMirror .

Después de crear el plan de recuperación ante desastres, identificar la recurrencia en el asistente e iniciar una replicación en un sitio de recuperación ante desastres, cada 30 minutos NetApp Disaster Recovery verifica que la replicación realmente se esté realizando de acuerdo con el plan. Puede supervisar el progreso en la página Monitor de trabajo.

**Rol de consola de NetApp requerido** Administrador de organización, Administrador de carpeta o proyecto, Administrador de recuperación ante desastres o Administrador de conmutación por error de recuperación ante desastres.

"Obtenga información sobre los roles y permisos de usuario en NetApp Disaster Recovery" . "Obtenga información sobre los roles de acceso a la consola de NetApp para todos los servicios" .

**Antes de empezar**

Antes de iniciar la replicación, debe haber creado un plan de replicación y haber seleccionado replicar las aplicaciones. Luego, aparece la opción **Replicar** en el menú Acciones.

**Pasos**

1. Iniciar sesión en el "Consola de NetApp" .
2. Desde el panel de navegación izquierdo de la consola NetApp , seleccione **Protección** > **Recuperación ante desastres**.
3. Desde el menú, seleccione **Planes de replicación**.
4. Seleccione el plan de replicación.
5. A la derecha, seleccione la opción **Acciones*** ••• **y seleccione *Replicar**.

# Migre aplicaciones a otro sitio con NetApp Disaster Recovery

Con NetApp Disaster Recovery, puede migrar aplicaciones de VMware en su sitio de origen a otro sitio.

Después de crear el plan de replicación, identificar la recurrencia en el asistente e iniciar la migración, cada 30 minutos NetApp Disaster Recovery verifica que la migración realmente se esté realizando según el plan. Puede supervisar el progreso en la página Monitor de trabajo.

**Antes de empezar**

Antes de iniciar la migración, debe haber creado un plan de replicación y haber seleccionado migrar las aplicaciones. Luego, aparece la opción **Migrar** en el menú Acciones.

**Pasos**

1. Iniciar sesión en el "Consola de NetApp" .
2. Desde el panel de navegación izquierdo de la consola NetApp , seleccione **Protección** > **Recuperación ante desastres**.
3. Desde el menú, seleccione **Planes de replicación**.
4. Seleccione el plan de replicación.
5. A la derecha, seleccione la opción **Acciones*** ••• **y seleccione *Migrar**.

# Conmute por error aplicaciones a un sitio remoto con NetApp Disaster Recovery

En caso de desastre, conmute su sitio local principal de VMware a otro sitio local de VMware o VMware Cloud en AWS. Puede probar el proceso de conmutación por error para garantizar el éxito cuando lo necesite.

**Rol de consola de NetApp requerido** Administrador de organización, Administrador de carpeta o proyecto, Administrador de recuperación ante desastres o Administrador de conmutación por error de recuperación ante desastres.

"Obtenga información sobre los roles y permisos de usuario en NetApp Disaster Recovery" . "Obtenga información sobre los roles de acceso a la consola de NetApp para todos los servicios" .

**Acerca de esta tarea**

Durante una conmutación por error, Disaster Recovery utiliza la copia de instantánea de SnapMirror más reciente. O bien, puede seleccionar una instantánea específica de una instantánea de un punto en el tiempo (según la política de retención de SnapMirror).

Utilice la opción de punto en el tiempo si las réplicas más recientes están comprometidas, como durante un ataque de ransomware. La BlueXP disaster recovery muestra todos los puntos disponibles en el tiempo.

Este proceso difiere dependiendo de si el sitio de producción está en buen estado y si está realizando una conmutación por error al sitio de recuperación ante desastres por motivos distintos a una falla crítica de la infraestructura:

- Falla crítica del sitio de producción donde el vCenter de origen o el clúster ONTAP no son accesibles: NetApp Disaster Recovery le permite seleccionar cualquier instantánea disponible desde la cual restaurar.
- El entorno de producción está en buen estado: puede "Tomar una instantánea ahora" o seleccionar una instantánea creada previamente.

Este procedimiento rompe la relación de replicación, coloca las máquinas virtuales de origen de vCenter fuera de línea, registra los volúmenes como almacenes de datos en el vCenter de recuperación ante desastres, reinicia las máquinas virtuales protegidas utilizando las reglas de conmutación por error del plan y habilita la lectura/escritura en el sitio de destino.

## Probar el proceso de conmutación por error

Antes de iniciar la conmutación por error, puede probar el proceso. La prueba no coloca las máquinas virtuales fuera de línea.

Durante una prueba de conmutación por error, la BlueXP disaster recovery crea temporalmente máquinas virtuales. La BlueXP disaster recovery asigna un almacén de datos temporal que respalda el volumen FlexClone a los hosts ESXi.

Este proceso no consume capacidad física adicional en el almacenamiento ONTAP local ni en FSx para el almacenamiento ONTAP de NetApp en AWS. El volumen de origen original no se modifica y los trabajos de réplica pueden continuar incluso durante la recuperación ante desastres.

Cuando finalice la prueba, deberá reiniciar las máquinas virtuales con la opción **Limpiar prueba**. Si bien esto se recomienda, no es obligatorio.

Una operación de conmutación por error de prueba *no* afecta las cargas de trabajo de producción, la relación SnapMirror utilizada en el sitio de prueba y las cargas de trabajo protegidas que deben seguir funcionando normalmente.

Para una conmutación por error de prueba, Disaster Recovery realiza las siguientes operaciones:

- Realice comprobaciones previas en el clúster de destino y la relación SnapMirror .
- Cree un nuevo volumen FlexClone a partir de la instantánea seleccionada para cada volumen ONTAP protegido en el clúster ONTAP del sitio de destino.
- Si alguno de los almacenes de datos es VMFS, cree y asigne un iGroup a cada LUN.
- Registre las máquinas virtuales de destino dentro de vCenter como nuevos almacenes de datos.
- Encienda las máquinas virtuales de destino según el orden de arranque capturado en la página Grupos de recursos.
- Desactive cualquier aplicación de base de datos compatible en las máquinas virtuales indicadas como "compatibles con la aplicación".
- Si los clústeres de origen vCenter y ONTAP aún están activos, cree una relación SnapMirror en dirección inversa para replicar cualquier cambio mientras esté en estado de conmutación por error en el sitio de origen original.

**Pasos**

1. Iniciar sesión en el "Consola de NetApp" .
2. Desde el panel de navegación izquierdo de la consola NetApp , seleccione **Protección** > **Recuperación ante desastres**.
3. En el menú NetApp Disaster Recovery, seleccione **Planes de replicación**.
4. Seleccione el plan de replicación.
5. A la derecha, seleccione la opción **Acciones*** ••• **y seleccione *Probar conmutación por error**.
6. En la página de Conmutación por error de prueba, ingrese “Conmutación por error de prueba” y seleccione **Conmutación por error de prueba**.
7. Una vez finalizada la prueba, limpie el entorno de prueba.

## Limpiar el entorno de prueba después de una prueba de conmutación por error

Una vez finalizada la prueba de conmutación por error, debe limpiar el entorno de prueba. Este proceso elimina las máquinas virtuales temporales de la ubicación de prueba, los FlexClones y los almacenes de datos temporales.

**Pasos**

1. En el menú NetApp Disaster Recovery, seleccione **Planes de replicación**.
2. Seleccione el plan de replicación.
3. A la derecha, seleccione la opción **Acciones*** ••• **y seleccione *Limpiar prueba de conmutación por error**.
4. En la página de prueba de conmutación por error, ingrese “Limpiar conmutación por error” y seleccione **Limpiar prueba de conmutación por error**.

## Conmutar por error el sitio de origen a un sitio de recuperación ante desastres

En caso de desastre, conmute su sitio local principal de VMware a pedido a otro sitio local de VMware o VMware Cloud en AWS con FSx para NetApp ONTAP.

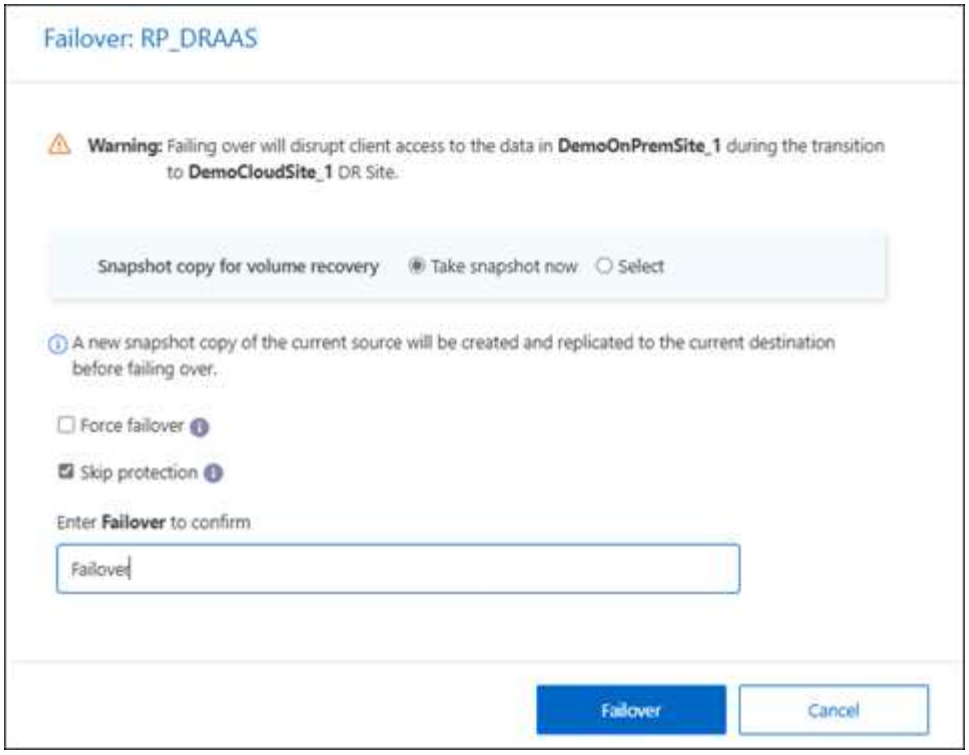
El proceso de conmutación por error implica las siguientes operaciones:

- Disaster Recovery realiza comprobaciones previas en el clúster de destino y en la relación SnapMirror .
- Si seleccionó la última instantánea, se realiza la actualización de SnapMirror para replicar los últimos cambios.
- Las máquinas virtuales de origen están apagadas.
- La relación SnapMirror se rompe y el volumen de destino pasa a ser de lectura y escritura.
- Según la selección de la instantánea, el sistema de archivos activo se restaura a la instantánea especificada (la más reciente o la seleccionada).
- Los almacenes de datos se crean y se montan en el clúster o host VMware o VMC según la información capturada en el plan de replicación. Si alguno de los almacenes de datos es VMFS, cree y asigne un iGroup a cada LUN.
- Las máquinas virtuales de destino se registran en vCenter como nuevos almacenes de datos.
- Las máquinas virtuales de destino se encienden según el orden de arranque capturado en la página Grupos de recursos.
- Si el vCenter de origen aún está activo, apague todas las máquinas virtuales del lado de origen que se están conmutando por error.
- Desactive cualquier aplicación de base de datos compatible en las máquinas virtuales indicadas como "compatibles con la aplicación".
- Si los clústeres de origen vCenter y ONTAP aún están activos, cree una relación SnapMirror en dirección inversa para replicar cualquier cambio mientras se encuentre en estado de conmutación por error en el sitio de origen original. La relación de SnapMirror se invierte de la máquina virtual de destino a la de origen.

Una vez iniciada la conmutación por error, podrá ver las máquinas virtuales recuperadas en el vCenter del sitio de recuperación ante desastres (máquinas virtuales, redes y almacenes de datos). De forma predeterminada, las máquinas virtuales se recuperan en la carpeta Carga de trabajo.

**Pasos**

1. En el menú NetApp Disaster Recovery, seleccione **Planes de replicación**.
2. Seleccione el plan de replicación.
3. A la derecha, seleccione la opción **Acciones*** ••• **y seleccione *Conmutación por error**.




4. En la página Conmutación por error, inicie una instantánea ahora o elija la instantánea para el almacén de datos desde el cual desea recuperar. El valor predeterminado es el más reciente.

   Se tomará una instantánea de la fuente actual y se replicará en el destino actual antes de que se produzca la conmutación por error.

5. De manera opcional, seleccione **Forzar conmutación por error** si desea que la conmutación por error se produzca incluso si se detecta un error que normalmente evitaría que se produzca la conmutación por error.
6. De manera opcional, seleccione **Omitir protección** si desea que el servicio no cree automáticamente una relación de protección SnapMirror inversa después de una conmutación por error del plan de replicación. Esto es útil si desea realizar operaciones adicionales en el sitio restaurado antes de volver a ponerlo en línea dentro de NetApp Disaster Recovery.

   Puede establecer protección inversa seleccionando **Proteger recursos** en el menú Acciones del plan de replicación. Esto intenta crear una relación de replicación inversa para cada volumen del plan. Puede ejecutar este trabajo repetidamente hasta que se restablezca la protección. Cuando se restablezca la protección, puede iniciar una conmutación por error de la forma habitual.

7. Escriba "conmutación por error" en el cuadro.
8. Seleccione **Conmutación por error**.
9. Para comprobar el progreso, en el menú, seleccione **Monitorización de trabajos**.

# Regrese las aplicaciones a la fuente original con NetApp Disaster Recovery

Una vez resuelto un desastre, se realiza un retorno desde el sitio de recuperación ante

desastres al sitio de origen para regresar a las operaciones normales. Puede seleccionar la instantánea desde la cual desea recuperar.

**Rol de consola de NetApp requerido** Administrador de organización, Administrador de carpeta o proyecto, Administrador de recuperación ante desastres o Administrador de conmutación por error de recuperación ante desastres.

"Obtenga información sobre los roles y permisos de usuario en NetApp Disaster Recovery" . "Obtenga información sobre los roles de acceso a la consola de NetApp para todos los servicios" .

**Acerca de esta tarea**

En este flujo de trabajo, NetApp Disaster Recovery replica (resincroniza) cualquier cambio en la máquina virtual de origen original antes de revertir la dirección de replicación. Este proceso comienza a partir de una relación que ha completado la conmutación por error a un destino e implica los siguientes pasos:

- Realice una verificación de cumplimiento en el sitio recuperado.
- Actualice la información de vCenter para cada clúster de vCenter identificado como ubicado en el sitio recuperado.
- En el sitio de destino, apague y anule el registro de las máquinas virtuales y desmonte los volúmenes.
- Romper la relación SnapMirror en la fuente original para que pueda leer y escribir.
- Vuelva a sincronizar la relación SnapMirror para revertir la replicación.
- Encienda y registre las máquinas virtuales de origen y monte los volúmenes en el origen.

**Pasos**

1. Iniciar sesión en el "Consola de NetApp" .
2. Desde el panel de navegación izquierdo de la consola NetApp , seleccione **Protección** > **Recuperación ante desastres**.
3. En el menú NetApp Disaster Recovery, seleccione **Planes de replicación**.
4. Seleccione el plan de replicación.
5. A la derecha, seleccione la opción **Acciones*** ••• **y seleccione *Revertir**.
6. Ingrese el nombre del plan de replicación para confirmar e iniciar la conmutación por error.
7. Seleccione la instantánea del almacén de datos desde el cual desea recuperar. El valor predeterminado es el más reciente.
8. Para comprobar el progreso, en el menú, seleccione **Monitorización de trabajos**.

# Administre sitios, grupos de recursos, planes de replicación, almacenes de datos e información de máquinas virtuales con NetApp Disaster Recovery

Puede obtener un vistazo rápido de todos sus recursos de recuperación ante desastres de NetApp o ver cada uno en detalle:

- Sitios
- Grupos de recursos

- Planes de replicación
- Almacenes de datos
- Máquinas virtuales

Las tareas requieren diferentes roles de la consola de NetApp . Para obtener más detalles, consulte la sección **Rol de consola de NetApp requerido** en cada tarea.

"Obtenga información sobre los roles y permisos de usuario en NetApp Disaster Recovery" . "Obtenga información sobre los roles de acceso a la consola de NetApp para todos los servicios" .

## Administrar sitios de vCenter

Puede editar el nombre del sitio de vCenter y el tipo de sitio (local o AWS).

**Rol de consola de NetApp requerido** Rol de administrador de organización, administrador de carpeta o proyecto, o administrador de recuperación ante desastres.

**Pasos**

1. Desde el menú, seleccione **Sitios**.
2. Seleccione la opción **Acciones***  **a la derecha del nombre de vCenter y seleccione *Editar**.
3. Edite el nombre y la ubicación del sitio vCenter.

## Administrar grupos de recursos

Si bien puede agregar un grupo de recursos como parte de la creación de un plan de replicación, es posible que le resulte más conveniente agregar los grupos por separado y luego usar esos grupos en el plan. Puede crear grupos de recursos por máquinas virtuales o por almacenes de datos.

**Rol de consola de NetApp requerido** Administrador de organización, Administrador de carpeta o proyecto, Administrador de recuperación ante desastres o Administrador de aplicación de recuperación ante desastres.

Puede crear un grupo de recursos por almacenes de datos de las siguientes maneras:

- Cuando agrega un grupo de recursos mediante almacenes de datos, puede ver una lista de almacenes de datos. Puede seleccionar uno o más almacenes de datos para crear un grupo de recursos.
- Cuando crea un plan de replicación y crea un grupo de recursos dentro del plan, puede ver las máquinas virtuales en los almacenes de datos.

Puede realizar las siguientes tareas con grupos de recursos:

- Cambiar el nombre del grupo de recursos.
- Agregue máquinas virtuales al grupo de recursos.
- Eliminar máquinas virtuales del grupo de recursos.
- Eliminar grupos de recursos.

Para obtener detalles sobre cómo crear un grupo de recursos, consulte"Crear un grupo de recursos para organizar las máquinas virtuales juntas" .

**Pasos**

1. Desde el menú, seleccione **Grupos de recursos**.
2. Para agregar un grupo de recursos, seleccione **Agregar grupo**.
3. Para realizar acciones con el grupo de recursos, seleccione la opción **Acciones*** ••• **a la derecha y seleccione cualquiera de las opciones, como *Editar grupo de recursos** o **Eliminar grupo de recursos**.

## Administrar planes de replicación

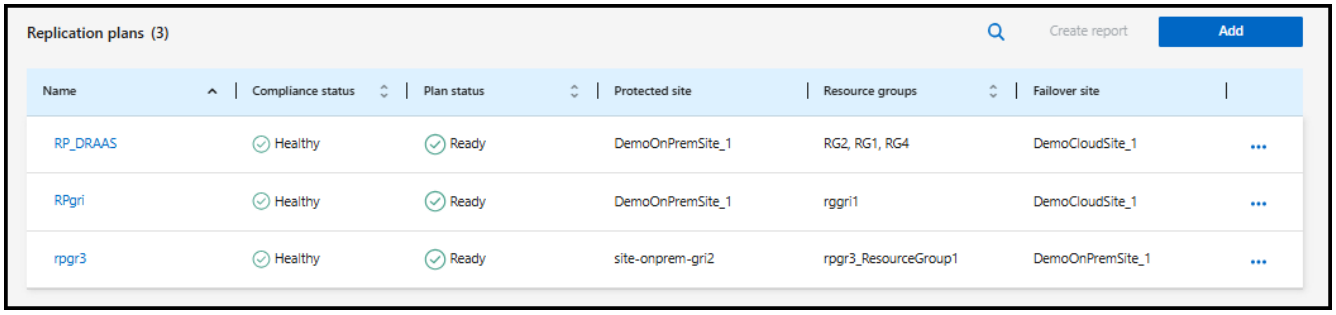
Puede deshabilitar, habilitar y eliminar planes de replicación. Puedes cambiar los horarios.

**Rol de consola de NetApp requerido** Administrador de organización, Administrador de carpeta o proyecto, Administrador de recuperación ante desastres, Administrador de conmutación por error de recuperación ante desastres o Administrador de aplicación de recuperación ante desastres.

- Si desea pausar un plan de replicación temporalmente, puede deshabilitarlo y habilitarlo más tarde.
- Si ya no necesitas el plan, puedes eliminarlo.

**Pasos**

1. Desde el menú, seleccione **Planes de replicación**.




2. Para ver los detalles del plan, seleccione la opción **Acciones*** ••• **y seleccione *Ver detalles del plan**.
3. Realice cualquiera de las siguientes acciones:
   - Para editar los detalles del plan (cambiar la recurrencia), seleccione la pestaña **Detalles del plan** y seleccione el ícono **Editar** a la derecha.
   - Para editar las asignaciones de recursos, seleccione la pestaña **Asignación de conmutación por error** y seleccione el ícono **Editar**.
   - Para agregar o editar las máquinas virtuales, seleccione la pestaña **Máquinas virtuales** y seleccione la opción **Agregar máquinas virtuales** o el ícono **Editar**.
4. Regrese a la lista de planes seleccionando “Planes de replicación” en las rutas de navegación de la izquierda.
5. Para realizar acciones con el plan, de la lista de planes de replicación, seleccione la opción **Acciones*** ••• **a la derecha del plan y seleccione cualquiera de las opciones, como *Editar programaciones**, **Probar conmutación por error**, **Conmutación por error**, **Conmutación por recuperación**, **Migrar**, **Tomar instantánea ahora**, **Limpiar instantáneas antiguas**, **Deshabilitar**, **Habilitar** o **Eliminar**.
6. Para establecer o cambiar un programa de conmutación por error de prueba o establecer la verificación de frecuencia de cumplimiento, seleccione la opción **Acciones*** ••• **a la derecha del plan y seleccione *Editar horarios**.
   a. En la página Editar programaciones, ingrese la frecuencia en minutos con la que desea que se realice

la verificación de cumplimiento de conmutación por error.

b. Marque **Ejecutar conmutaciones por error de prueba según un cronograma**.

c. En la opción Repetir, seleccione la programación diaria, semanal o mensual.

d. Seleccione **Guardar**.

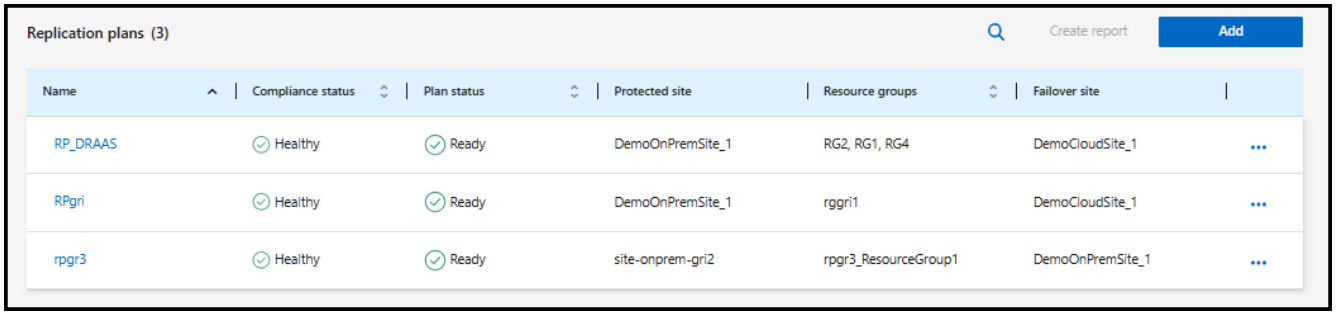
### Conciliar instantáneas a pedido

Puede conciliar instantáneas que no estén sincronizadas entre el origen y el destino. Esto podría ocurrir si se eliminan instantáneas en un destino fuera de NetApp Disaster Recovery. El servicio elimina automáticamente la instantánea de la fuente cada 24 horas. Sin embargo, puedes realizar esto bajo demanda. Esta función le permite garantizar que las instantáneas sean consistentes en todos los sitios.

**Rol de consola de NetApp requerido** Administrador de organización, Administrador de carpeta o proyecto, Administrador de recuperación ante desastres, Administrador de conmutación por error de recuperación ante desastres o Administrador de aplicación de recuperación ante desastres.

#### Pasos

1. Desde el menú, seleccione **Planes de replicación**.




2. De la lista de planes de replicación, seleccione la opción **Acciones*** ••• **a la derecha del plan y seleccione *Reconciliar instantáneas**.
3. Revise la información de conciliación.
4. Seleccione **Reconciliar**.

### Eliminar un plan de replicación

Puede eliminar un plan de replicación si ya no lo necesita. Si elimina un plan de replicación, también puede eliminar las instantáneas principales y secundarias creadas por el plan.

**Rol de consola de NetApp requerido** Administrador de organización, Administrador de carpeta o proyecto, Administrador de recuperación ante desastres, Administrador de conmutación por error de recuperación ante desastres o Administrador de aplicación de recuperación ante desastres.

#### Pasos

1. Desde el menú, seleccione **Planes de replicación**.
2. Seleccione la opción **Acciones*** ••• **a la derecha del plan y seleccione *Eliminar**.
3. Seleccione si desea eliminar las instantáneas principales, las instantáneas secundarias o solo los metadatos creados por el plan.
4. Escriba "eliminar" para confirmar la eliminación.
5. Seleccione **Eliminar**.

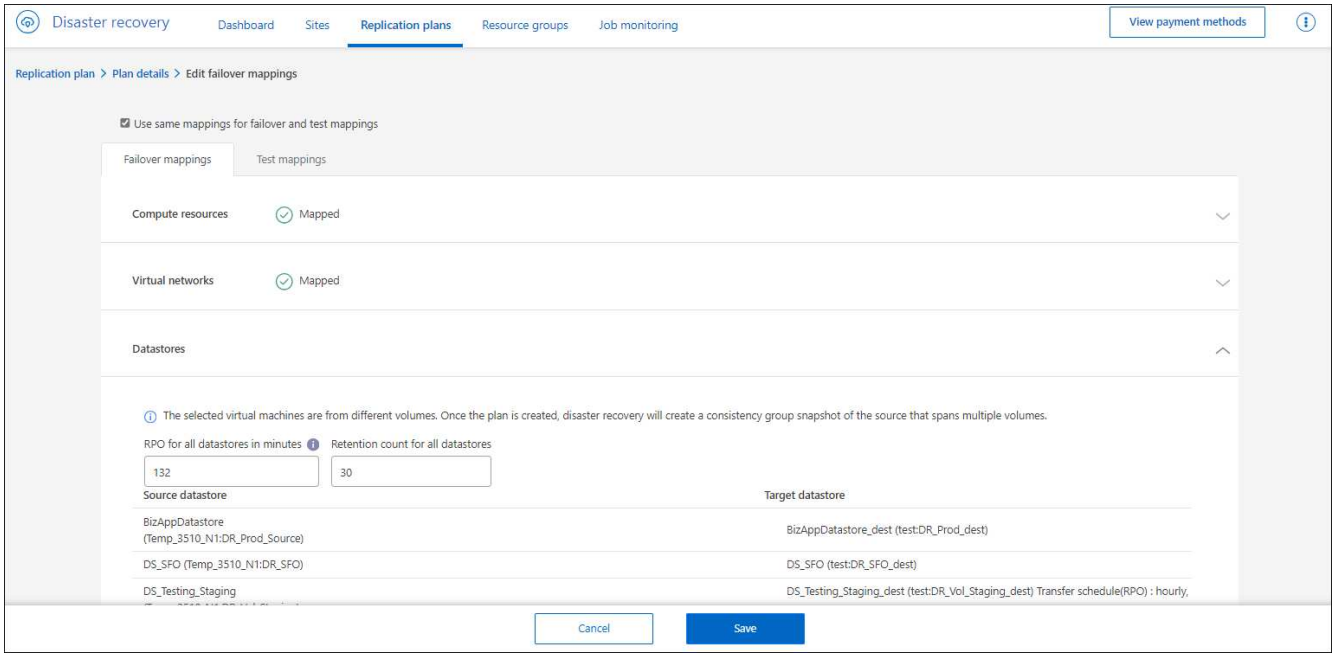
### Cambiar el recuento de retención para programaciones de conmutación por error

Puede cambiar la cantidad de almacenes de datos que se conservan.

**Rol de consola de NetApp requerido** Administrador de organización, Administrador de carpeta o proyecto, Administrador de recuperación ante desastres, Administrador de conmutación por error de recuperación ante desastres o Administrador de aplicación de recuperación ante desastres.

**Pasos**

1. Desde el menú, seleccione **Planes de replicación**.
2. Seleccione el plan de replicación, seleccione la pestaña **Asignación de conmutación por error** y seleccione el ícono de lápiz **Editar**.
3. Seleccione la flecha **Almacenes de datos** para expandirla.




4. Cambiar el valor del recuento de retención en el plan de replicación.
5. Con el plan de replicación seleccionado, seleccione el menú Acciones, luego seleccione **Limpiar instantáneas antiguas** para eliminar instantáneas antiguas en el destino para que coincidan con el nuevo recuento de retención.

## Ver información de almacenes de datos

Puede ver información sobre cuántos almacenes de datos existen en el origen y en el destino.

**Rol de consola de NetApp requerido** Administrador de organización, Administrador de carpeta o proyecto, Administrador de recuperación ante desastres, Administrador de conmutación por error de recuperación ante desastres, Administrador de aplicaciones de recuperación ante desastres o Rol de visualizador de recuperación ante desastres.

**Pasos**

1. Desde el menú, seleccione **Panel de control**.
2. Seleccione el vCenter en la fila del sitio.
3. Seleccione **Almacenes de datos**.

4. Ver la información de los almacenes de datos.

### Ver información de máquinas virtuales

Puede ver información sobre cuántas máquinas virtuales existen en el origen y en el destino junto con la CPU, la memoria y la capacidad disponible.

**Rol de consola de NetApp requerido** Administrador de organización, Administrador de carpeta o proyecto, Administrador de recuperación ante desastres, Administrador de conmutación por error de recuperación ante desastres, Administrador de aplicaciones de recuperación ante desastres o Rol de visualizador de recuperación ante desastres.

**Pasos**

1. Desde el menú, seleccione **Panel de control**.
2. Seleccione el vCenter en la fila del sitio.
3. Seleccione **Máquinas virtuales**.
4. Ver la información de las máquinas virtuales.

# Supervisar trabajos de recuperación ante desastres de NetApp

Puede supervisar todos los trabajos de recuperación ante desastres de NetApp y determinar su progreso.

### Ver trabajos

**Rol de consola de NetApp requerido** Administrador de organización, Administrador de carpeta o proyecto, Administrador de recuperación ante desastres, Administrador de aplicaciones de recuperación ante desastres o Rol de visualizador de recuperación ante desastres.

"Obtenga información sobre los roles y permisos de usuario en NetApp Disaster Recovery" . "Obtenga información sobre los roles de acceso a la consola de NetApp para todos los servicios" .

**Pasos**

1. Iniciar sesión en el "Consola de NetApp" .
2. Desde el panel de navegación izquierdo de la consola NetApp , seleccione **Protección** > **Recuperación ante desastres**.
3. Desde el menú, seleccione **Supervisión de trabajos**.
4. Explora todos los trabajos relacionados con operaciones y revisa sus marcas de tiempo y estado.
5. Para ver los detalles de un trabajo en particular, seleccione esa fila.
6. Para actualizar la información, seleccione **Actualizar**.

### Cancelar un trabajo

Si un trabajo está en progreso o en estado de cola y no desea que continúe, puede cancelarlo. Es posible que desee cancelar un trabajo si está atascado en el mismo estado y desea liberar la siguiente operación en la cola. Es posible que desees cancelar un trabajo antes de que caduque.

**Rol de consola de NetApp requerido** Administrador de organización, Administrador de carpeta o proyecto, Administrador de recuperación ante desastres, Administrador de conmutación por error de recuperación ante desastres o Administrador de aplicación de recuperación ante desastres.

"Obtenga información sobre los roles y permisos de usuario en NetApp Disaster Recovery" . "Obtenga información sobre los roles de acceso a la consola de NetApp para todos los servicios" .

**Pasos**

1. Desde la barra de navegación izquierda de la consola de NetApp , seleccione **Protección** > **Recuperación ante desastres**.
2. Desde el menú, seleccione **Supervisión de trabajos**.
3. En la página del Monitor de trabajos, anote el ID del trabajo que desea cancelar.

   El trabajo debe estar en estado "En progreso" o "En cola".

4. En la columna Acciones, seleccione **Cancelar trabajo**.

# Crear informes de recuperación ante desastres de NetApp

Revisar los informes de recuperación ante desastres de NetApp puede ayudarlo a analizar su preparación para la recuperación ante desastres. Los informes prediseñados incluyen un resumen de las conmutaciones por error de pruebas, detalles del plan de replicación y detalles del trabajo en todos los sitios dentro de una cuenta durante los últimos siete días.

Puede descargar informes en formato PDF, HTML o JSON.

El enlace de descarga es válido por seis horas.

**Pasos**

1. Iniciar sesión en el "Consola de NetApp" .
2. Desde el panel de navegación izquierdo de la consola NetApp , seleccione **Protección** > **Recuperación ante desastres**.
3. Desde la barra de navegación izquierda de la consola de NetApp , seleccione **Planes de replicación**.
4. Seleccione **Crear informe**.
5. Seleccione el tipo de formato de archivo y el período de tiempo dentro de los últimos 7 días.
6. Seleccione **Crear**.

   El informe podría tardar unos minutos en mostrarse.

7. Para descargar un informe, seleccione **Descargar informe** y selecciónelo en la carpeta de descargas del administrador.

# Referencia

## Privilegios de vCenter necesarios para NetApp Disaster Recovery

La cuenta de vCenter debe tener un conjunto mínimo de privilegios de vCenter para permitir que NetApp Disaster Recovery realice sus servicios, como registrar y anular el registro de almacenes de datos, iniciar y detener máquinas virtuales y reconfigurar máquinas virtuales (VM). En la siguiente tabla se enumeran todos los privilegios necesarios para que NetApp Disaster Recovery interactúe con un clúster de vCenter.

| Tipo | Nombre del privilegio | Descripción |
|---|---|---|
| **Almacén de datos** | Almacén de datos.Configurar almacén de datos | Úselo para configurar un almacén de datos. |
| | Almacén de datos.Eliminar almacén de datos | Úselo para eliminar un almacén de datos. |
| **Máquina virtual** | Máquina virtual.Configuración.Cambiar configuración | Úselo para cambiar la configuración general de la máquina virtual. |
| | Máquina virtual.Configuración.Modificar la configuración del dispositivo | Úselo para cambiar las propiedades de un dispositivo existente. |
| | Máquina virtual.Configuración.Recargar desde la ruta | Úselo para cambiar un parche de configuración de VM preservando la identidad de la VM. Soluciones como VMware vCenter Site Recovery Manager utilizan esta operación para mantener la identidad de la máquina virtual durante la conmutación por error y la recuperación. |
| | Máquina virtual.Configuración.Cambiar nombre | Úselo para cambiar el nombre de una VM o modificar los nodos asociados de una VM. |
| | Máquina virtual.Configuración.Restablecer información del invitado | Úselo para editar la información del sistema operativo invitado para una máquina virtual. |
| | Máquina virtual.Configuración.Cambiar memoria | Úselo para cambiar la cantidad de memoria asignada a la VM. |

| Tipo | Nombre del privilegio | Descripción |
| --- | --- | --- |
| | Máquina virtual.Configuración.Cambiar el número de CPU | Úselo para cambiar el número de CPU virtuales. |
| **Invitado de máquina virtual** | Máquina virtual.Operaciones de invitado.Modificaciones de operaciones de invitado | Permite operaciones de invitado de VM que implican cambios en un sistema operativo invitado en una VM, como transferir un archivo a la VM. |
| **Interacción con máquinas virtuales** | Máquina virtual.Interacción.Apagado | Úselo para apagar una máquina virtual encendida. Esta operación apaga el sistema operativo invitado. |
| | Máquina virtual.Interacción.Encendido | Úselo para encender una máquina virtual apagada y reanudar una máquina virtual suspendida. |
| | Máquina virtual.Interacción.Instalación de VMware Tools | Úselo para montar y desmontar el instalador del CD de VMware Tools como un CD-ROM para el sistema operativo invitado. |
| **Inventario de máquinas virtuales** | Máquina virtual.Inventario.Crear nuevo | Úselo para crear una máquina virtual y asignar recursos para su ejecución. |
| | Máquina virtual.Inventario.Registrar | Úselo para agregar una máquina virtual existente a un servidor vCenter o al inventario de host. |
| | Máquina virtual.Inventario.Cancelar registro | Úselo para anular el registro de una máquina virtual de un inventario de host o de un servidor vCenter. |
| **Estado de la máquina virtual** | Máquina virtual. Gestión de instantáneas. Crear instantánea | Úselo para crear una instantánea del estado actual de la máquina virtual. |
| | Máquina virtual.Administración de instantáneas.Eliminar instantánea | Úselo para eliminar una instantánea del historial de instantáneas. |
| | Máquina virtual.Administración de instantáneas.Volver a instantánea | Úselo para establecer la máquina virtual al estado en el que se encontraba en una instantánea determinada. |

# Acceso a funciones basado en roles de NetApp Disaster Recovery

NetApp Disaster Recovery emplea roles para gobernar el acceso que tiene cada usuario a funciones y acciones específicas.

El servicio utiliza los siguientes roles que son específicos de NetApp Disaster Recovery.

- **Administrador de recuperación ante desastres**: realiza cualquier acción en NetApp Disaster Recovery.
- **Administrador de conmutación por error de recuperación ante desastres**: realiza acciones de conmutación por error y migración en NetApp Disaster Recovery.
- **Administrador de aplicaciones de recuperación ante desastres**: crear y modificar planes de replicación e iniciar conmutaciones por error de prueba.
- **Visor de recuperación ante desastres**: ve información en NetApp Disaster Recovery, pero no puede realizar ninguna acción.

Estos roles son específicos de NetApp Disaster Recovery y no son los mismos que los roles de plataforma que se utilizan en la consola de NetApp . Para obtener detalles sobre todas las funciones de la plataforma NetApp Console, consulte "la documentación de configuración y administración de la consola de NetApp" .

La siguiente tabla indica las acciones que puede realizar cada rol de recuperación ante desastres de NetApp .

| Característica y acción | Administración de recuperación ante desastres | Administrador de conmutación por error de recuperación ante desastres | Administrador de aplicaciones de recuperación ante desastres | Visor de recuperación ante desastres |
|---|---|---|---|---|
| Ver el panel y todas las pestañas | Sí | Sí | Sí | Sí |
| Comience una prueba gratuita | Sí | No | No | No |
| Iniciar el descubrimiento de cargas de trabajo | Sí | No | No | No |
| Ver información de la licencia | Sí | Sí | Sí | Sí |
| Activar licencia | Sí | No | Sí | No |
| **En la opción Sitios**: | | | | |
| Ver sitios | Sí | Sí | Sí | Sí |
| Agregar, modificar o eliminar sitios | Sí | No | No | No |
| **En la opción Planes de replicación**: | | | | |
| Ver planes de replicación | Sí | Sí | Sí | Sí |

| Característica y acción | Administración de recuperación ante desastres | Administrador de conmutación por error de recuperación ante desastres | Administrador de aplicaciones de recuperación ante desastres | Visor de recuperación ante desastres |
|---|---|---|---|---|
| Ver detalles del plan de replicación | Sí | Sí | Sí | Sí |
| Crear o modificar planes de replicación | Sí | Sí | Sí | No |
| Crear informes | Sí | No | No | No |
| Ver instantáneas | Sí | Sí | Sí | Sí |
| Realizar pruebas de conmutación por error | Sí | Sí | Sí | No |
| Realizar conmutaciones por error | Sí | Sí | No | No |
| Realizar conmutaciones por recuperación | Sí | Sí | No | No |
| Realizar migraciones | Sí | Sí | No | No |
| **En la opción Grupos de recursos**: | | | | |
| Ver grupos de recursos | Sí | Sí | Sí | Sí |
| Crear, modificar o eliminar grupos de recursos | Sí | No | Sí | No |
| **Opción de Monitoreo en el Trabajo**: | | | | |
| Ver trabajos | Sí | No | Sí | Sí |
| Cancelar trabajos | Sí | Sí | Sí | No |

# Utilice NetApp Disaster Recovery con Amazon EVS

## Introducción de NetApp Disaster Recovery mediante Amazon Elastic VMware Service y Amazon FSx for NetApp ONTAP

Cada vez más, los clientes dependen más de las infraestructuras virtualizadas para cargas de trabajo informáticas de producción, como aquellas basadas en VMware vSphere. A medida que estas máquinas virtuales (VM) se han vuelto más críticas para sus negocios, los clientes necesitan proteger estas VM de los mismos tipos de desastres que sus recursos informáticos físicos. Las soluciones de recuperación ante desastres (DR) que se ofrecen actualmente son complejas, costosas y requieren un uso intensivo de recursos. NetApp, el mayor proveedor de almacenamiento utilizado para

infraestructuras virtualizadas, tiene un interés personal en garantizar que las máquinas virtuales de sus clientes estén protegidas de la misma manera que protegemos los datos alojados en el almacenamiento ONTAP de cualquier tipo. Para alcanzar este objetivo, NetApp creó el servicio NetApp Disaster Recovery.

Uno de los principales desafíos de cualquier solución de recuperación ante desastres es administrar el costo incremental de comprar, configurar y mantener recursos de computación, red y almacenamiento adicionales solo para brindar una infraestructura de replicación y recuperación de recuperación ante desastres. Una opción popular para proteger recursos virtuales críticos locales es utilizar recursos virtuales alojados en la nube como infraestructura de replicación y recuperación ante desastres. Amazon es un ejemplo de una solución que puede proporcionar recursos rentables que son compatibles con las infraestructuras de máquinas virtuales alojadas en NetApp ONTAP .

Amazon presentó su Amazon Elastic VMware Service (Amazon EVS) que habilita VMware Cloud Foundation dentro de su nube privada virtual (VPC). Amazon EVS ofrece la resiliencia y el rendimiento de AWS junto con el software y las herramientas familiares de VMware, lo que permite integrar Amazon EVS vCenters como una extensión de su infraestructura virtualizada local.

Si bien Amazon EVS viene con recursos de almacenamiento incluidos, el uso de almacenamiento nativo puede reducir su eficacia para las organizaciones con cargas de trabajo que requieren mucho almacenamiento. En estos casos, combinar Amazon EVS con Amazon FSx for NetApp ONTAP (Amazon FSxN) puede proporcionar una solución de almacenamiento más flexible. Además, cuando utiliza soluciones de almacenamiento NetApp ONTAP en sus instalaciones para alojar su infraestructura VMware, el uso de Amazon EVS con FSx para ONTAP significa que obtiene las mejores funciones de protección e interoperabilidad de datos de su clase entre sus infraestructuras locales y alojadas en la nube.

Para obtener información sobre Amazon FSx for NetApp ONTAP, consulte "Introducción a Amazon FSx for NetApp ONTAP" .

## Descripción general de la solución de recuperación ante desastres de NetApp con Amazon EVS y Amazon FSs para NetApp ONTAP

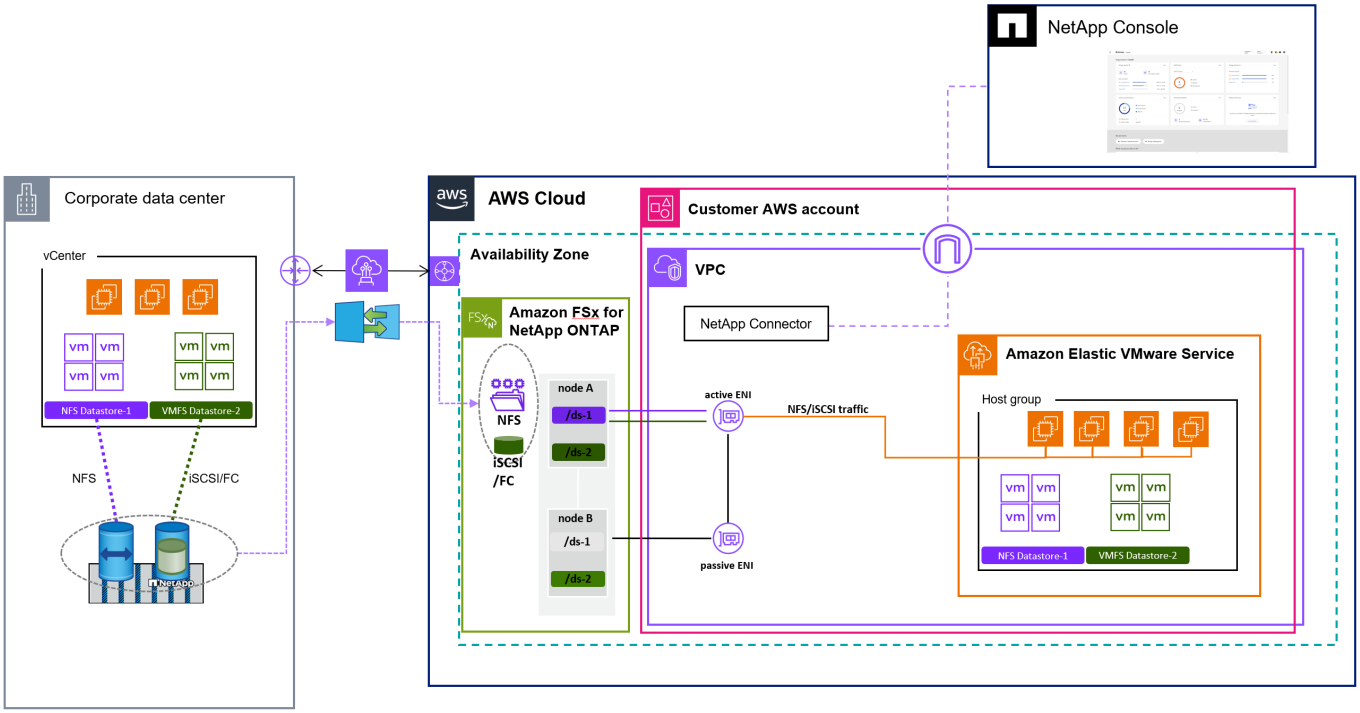
NetApp Disaster Recovery es un servicio de valor agregado alojado dentro del entorno de software como servicio de NetApp Console, que depende de la arquitectura central de NetApp Console. Varios componentes principales comprenden el servicio DR para la protección de VMware dentro de la consola.

Para obtener una descripción general completa de la solución NetApp Disaster Recovery, consulte"Obtenga más información sobre NetApp Disaster Recovery para VMware" .

Si desea proteger sus máquinas virtuales alojadas en VMware localmente en Amazon AWS, utilice el servicio para realizar copias de seguridad en Amazon EVS con Amazon FSx for NetApp ONTAP .

La siguiente figura muestra cómo funciona el servicio para proteger sus máquinas virtuales con Amazon EVS.

Descripción general de NetApp Disaster Recovery con Amazon EVS y FSx para ONTAP




1. Amazon EVS se implementa en su cuenta en una única configuración de zona de disponibilidad (AZ) y dentro de su nube privada virtual (VPC).
2. Un sistema de archivos FSx para ONTAP se implementa en la misma AZ que la implementación de Amazon EVS. El sistema de archivos se conecta a Amazon EVS directamente a través de una interfaz de red elástica (ENI), una conexión de pares de VPC o un AmazonTransit Gateway.
3. El agente de la consola de NetApp está instalado en su VPC. El agente de la consola de NetApp aloja varios servicios de administración de datos (llamados agentes), incluido el agente de recuperación ante desastres de NetApp que administra la recuperación ante desastres de la infraestructura de VMware tanto en sus centros de datos físicos locales como en sus recursos alojados en Amazon AWS.
4. El agente de recuperación ante desastres de NetApp se comunica de forma segura con el servicio alojado en la nube de la consola de NetApp para recibir tareas y distribuirlas a las instancias de almacenamiento locales adecuadas, alojadas en AWS y vCenter y ONTAP .
5. Puede crear un plan de replicación mediante la consola de interfaz de usuario alojada en la nube de NetApp Console, que indica las máquinas virtuales que se deben proteger, la frecuencia con la que se deben proteger y los procedimientos que se deben realizar para reiniciar esas máquinas virtuales en caso de una conmutación por error desde el sitio local.
6. El plan de replicación determina qué almacenes de datos de vCenter alojan las máquinas virtuales protegidas y los volúmenes de ONTAP que alojan esos almacenes de datos. Si aún no existen volúmenes en el clúster FSx para ONTAP , NetApp Disaster Recovery los crea automáticamente.
7. Se crea una relación SnapMirror para cada volumen ONTAP de origen identificado con cada FSx de destino para el volumen ONTAP alojado en ONTAP y se crea un programa de replicación basado en el RPO proporcionado por el usuario en el plan de replicación.
8. En caso de falla del sitio principal, un administrador inicia un proceso de conmutación por error manual dentro de la consola de NetApp y selecciona una copia de seguridad para usar como punto de restauración.
9. El agente de recuperación ante desastres de NetApp activa FSx para volúmenes de protección de datos alojados en ONTAP .
10. El agente registra cada volumen FSx para ONTAP activado con Amazon EVS vCenter, registra cada VM

protegida con Amazon EVS vCenter y las inicia según las reglas predefinidas contenidas en el plan de replicación.

## Instalar el agente de la consola de NetApp para NetApp Disaster Recovery

Un agente de consola de NetApp es un software de NetApp que se ejecuta en su nube o red local. Ejecuta las acciones que la consola de NetApp necesita realizar para administrar su infraestructura de datos. El agente de consola sondea constantemente el software NetApp Disaster Recovery como una capa de servicio para detectar cualquier acción que deba tomar.

Para NetApp Disaster Recovery, las acciones que se realizan orquestan los clústeres de VMware vCenter y las instancias de almacenamiento de ONTAP mediante API nativas para cada servicio respectivo a fin de brindar protección a las máquinas virtuales de producción que se ejecutan en una ubicación local. Si bien el agente de consola se puede instalar en cualquiera de las ubicaciones de su red, para NetApp Disaster Recovery recomendamos que instale el agente de consola en el sitio de DR. Esto garantiza que, en caso de una falla del sitio principal, la interfaz de usuario de la consola basada en la nube de NetApp continúa teniendo contacto con el agente de la consola y puede orquestar el proceso de recuperación dentro de ese sitio de recuperación ante desastres.

Para utilizar el servicio, instale el agente de consola en modo estándar. Para obtener más información sobre los tipos de instalaciones del agente de consola, visite "Obtenga más información sobre los modos de implementación de la consola de NetApp | Documentación de NetApp" .

Si bien el agente de consola es fundamental para utilizar el servicio, los pasos de instalación para instalar el agente de consola dependen de sus necesidades y de la configuración de la red. Está fuera del alcance de esta información proporcionar instrucciones específicas para la instalación.

El método más simple para instalar el agente de consola con Amazon AWS es utilizar AWS Marketplace. Para obtener detalles sobre la instalación del agente de consola mediante AWS Marketplace, consulte "Crear un agente de consola desde AWS Marketplace | Documentación de NetApp" .

## Configurar NetApp Disaster Recovery para Amazon EVS

### Descripción general de la configuración de NetApp Disaster Recovery para Amazon EVS

Después de instalar el agente de la consola de NetApp , debe integrar todos los recursos de almacenamiento de ONTAP y VMware vCenter que participarán en el proceso de recuperación ante desastres con NetApp Disaster Recovery.

- "Requisitos previos para Amazon EVS con NetApp Disaster Recovery"
- "Agregue matrices de almacenamiento ONTAP a NetApp Disaster Recovery"
- "Habilitar la recuperación ante desastres de NetApp para Amazon EVS"
- "Agregar sitios de vCenter a NetApp Disaster Recovery"
- "Agregar clústeres de vCenter a NetApp Disaster Recovery"

### Requisitos previos para Amazon EVS con NetApp Disaster Recovery

Debe asegurarse de que se cumplan varios requisitos previos antes de continuar configurando Amazon EVS con NetApp Disaster Recovery.

En concreto, haga lo siguiente:

- Cree una cuenta de usuario de vCenter con los privilegios específicos de VMware necesarios para que NetApp Disaster Recovery realice las operaciones necesarias.

> No recomendamos utilizar la cuenta de administrador predeterminada "administrator@vsphere.com". En su lugar, debe crear una cuenta de usuario específica de NetApp Disaster Recovery en todos los clústeres de vCenter que participarán en el proceso de recuperación ante desastres. Para obtener una lista de los privilegios específicos requeridos, consulte"Privilegios de vCenter necesarios para NetApp Disaster Recovery" .

- Asegúrese de que todos los almacenes de datos de vCenter que alojarán máquinas virtuales protegidas por NetApp Disaster Recovery estén ubicados en recursos de almacenamiento de NetApp ONTAP .

  El servicio admite NFS y VMFS en iSCSI (y no FC) cuando se utiliza Amazon FSx en NetApp ONTAP. Si bien el servicio admite FC, Amazon FSx for NetApp ONTAP no lo hace.

- Asegúrese de que su Amazon EVS vCenter esté conectado a un clúster de almacenamiento Amazon FSx for NetApp ONTAP .
- Asegúrese de que las herramientas de VMware estén instaladas en todas las máquinas virtuales protegidas.
- Asegúrese de que su red local esté conectada a su red AWS VPC mediante un método de conexión aprobado por Amazon. Le recomendamos que utilice AWS Direct Connect, AWS Private Link o una VPN de sitio a sitio de AWS.

### Agregue matrices locales al sistema de consola de NetApp para Amazon EVS con NetApp Disaster Recovery

Antes de utilizar NetApp Disaster Recovery, debe agregar instancias de almacenamiento alojadas en la nube y locales al sistema de consola de NetApp .

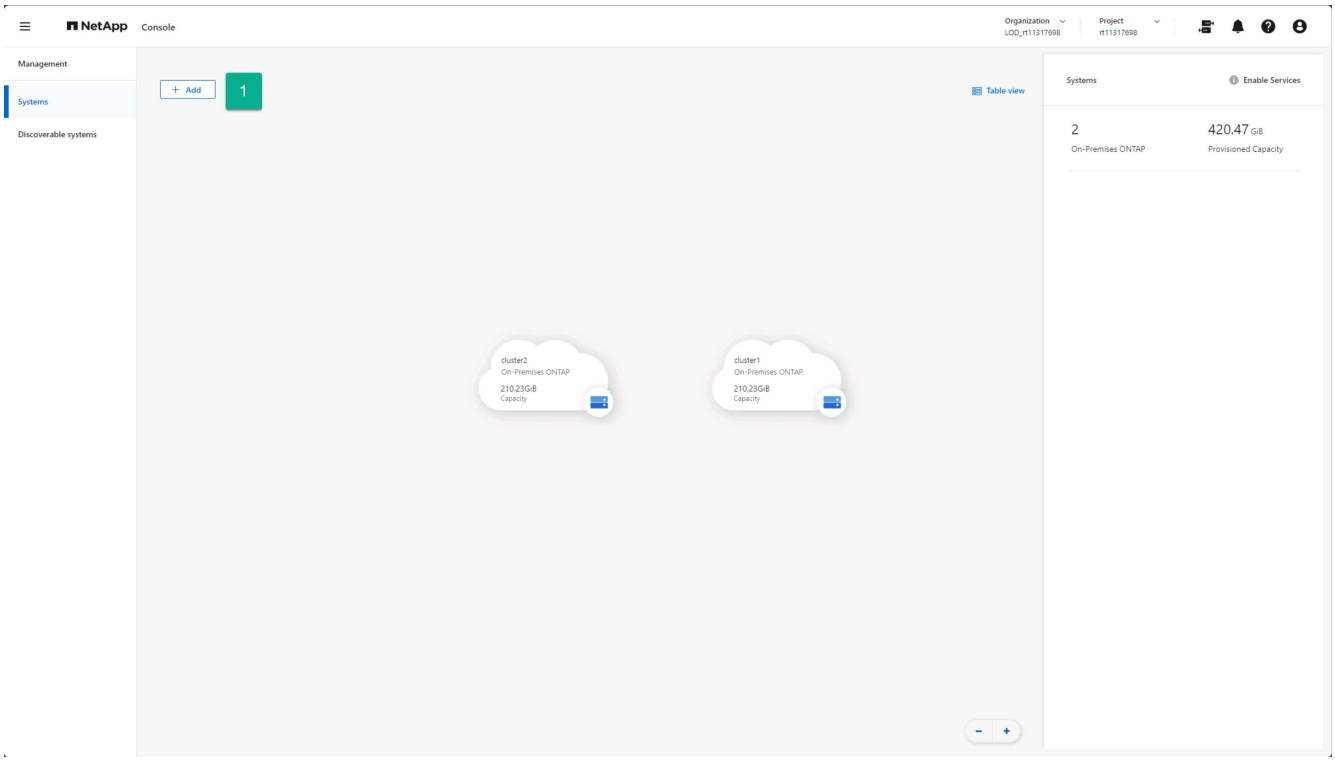
Necesitas hacer lo siguiente:

- Agregue matrices locales a su sistema de consola NetApp .
- Agregue instancias de Amazon FSx for NetApp ONTAP (FSx for ONTAP) a su sistema de consola NetApp .

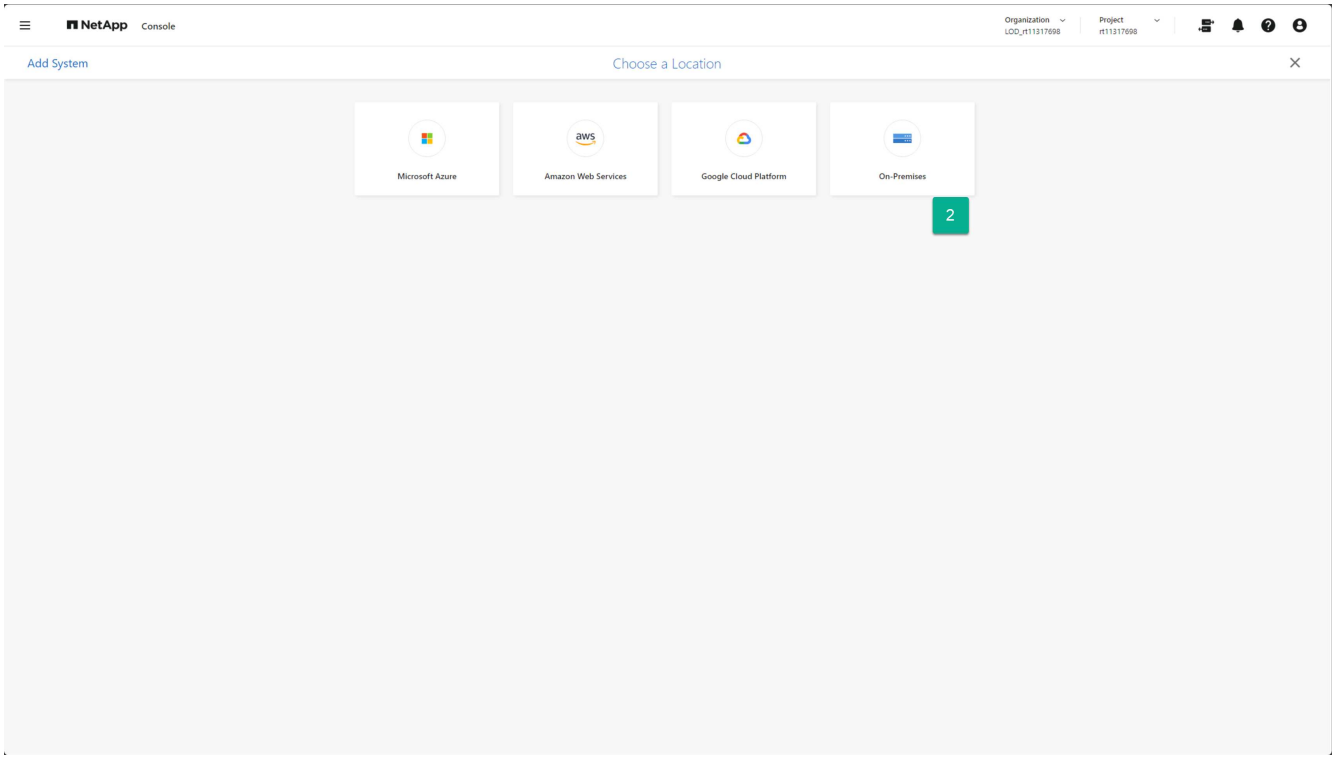
#### Agregue matrices de almacenamiento locales al sistema de consola de NetApp

Agregue recursos de almacenamiento ONTAP locales a su sistema de consola NetApp .

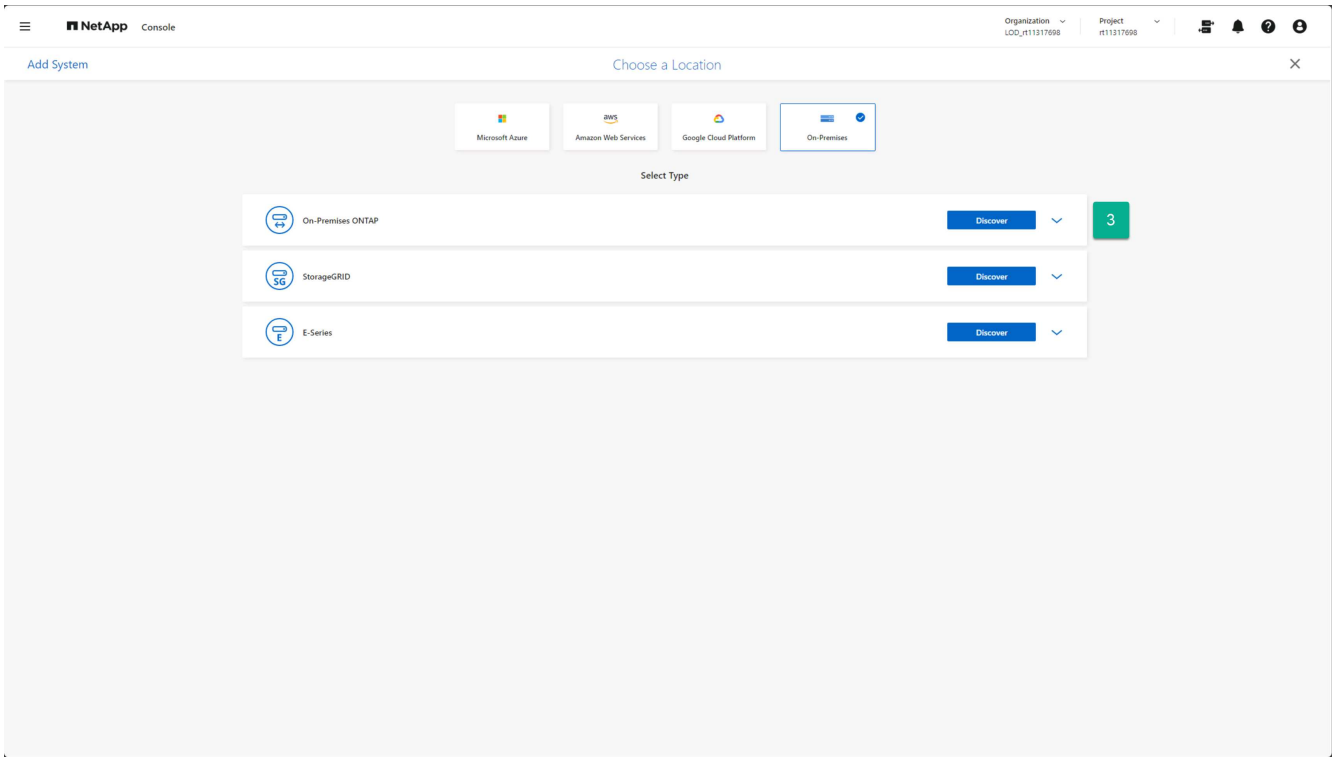
1. Desde la página Sistemas de consola de NetApp , seleccione **Agregar sistema**.



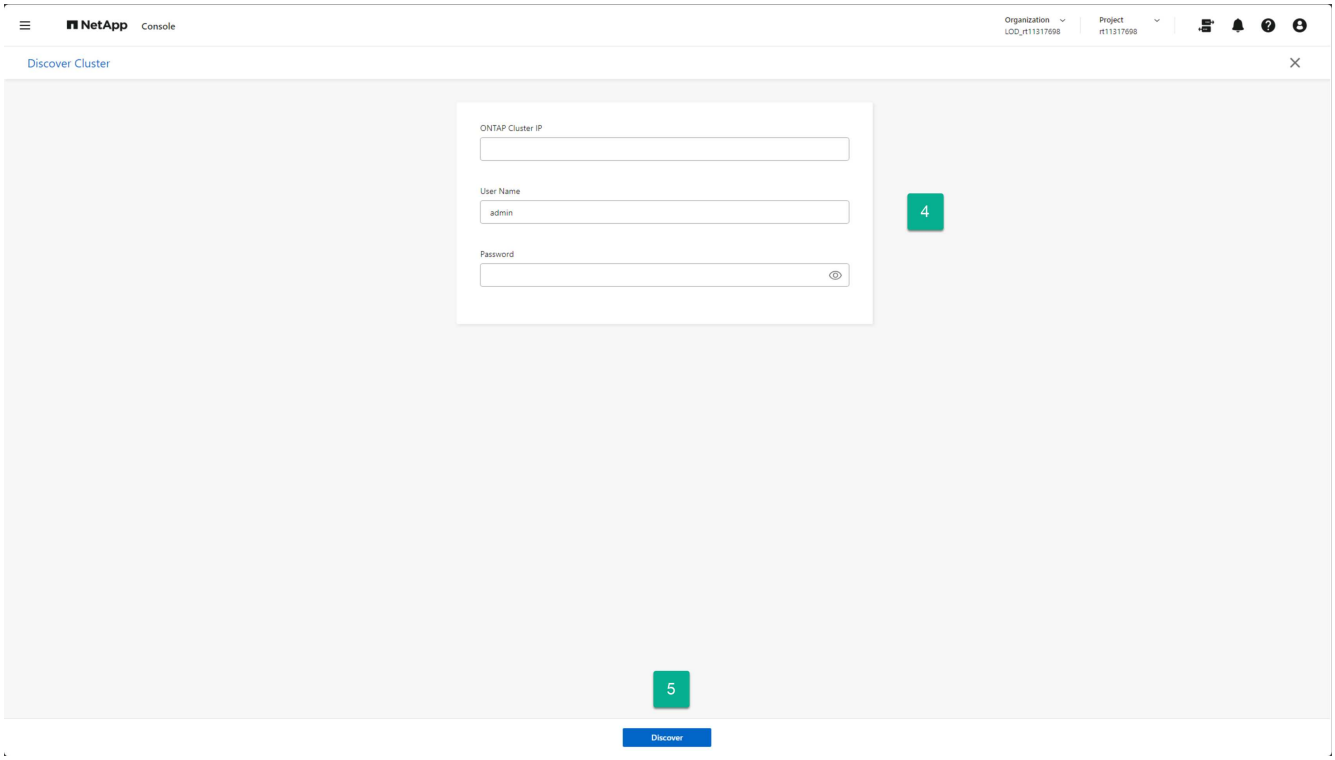

2. Desde la página Agregar sistema, seleccione la tarjeta **En las instalaciones**.




3. Seleccione **Descubrir** en la tarjeta On-Premises ONTAP .




4. En la página Descubrir clúster, ingrese la siguiente información:
   a. La dirección IP del puerto de administración del clúster de matriz ONTAP
   b. El nombre de usuario del administrador
   c. La contraseña del administrador
5. Seleccione **Descubrir** en la parte inferior de la página.

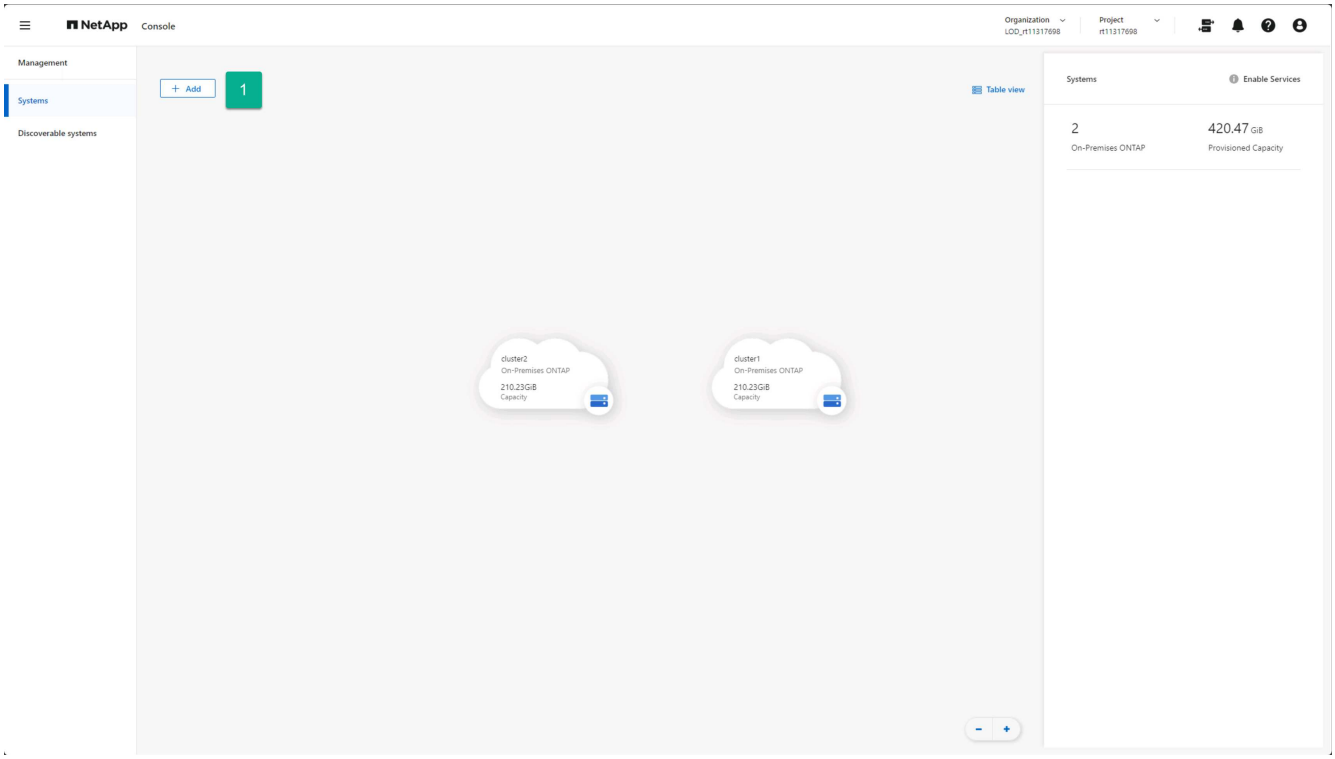



6. Repita los pasos 1 a 5 para cada matriz ONTAP que alojará almacenes de datos de vCenter.

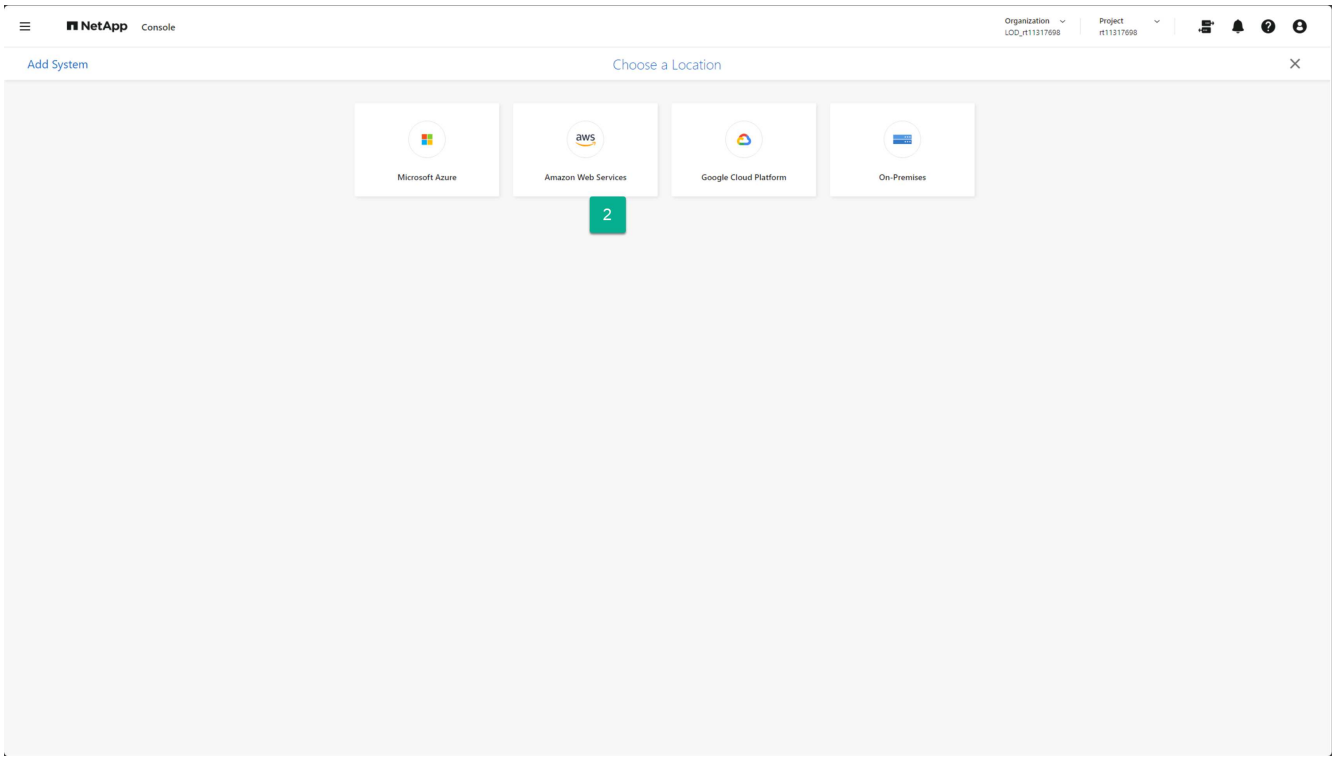
**Agregue instancias de almacenamiento de Amazon FSx for NetApp ONTAP al sistema de consola de NetApp**

A continuación, agregue un recurso de almacenamiento de Amazon FSx for NetApp ONTAP a su sistema de consola NetApp .

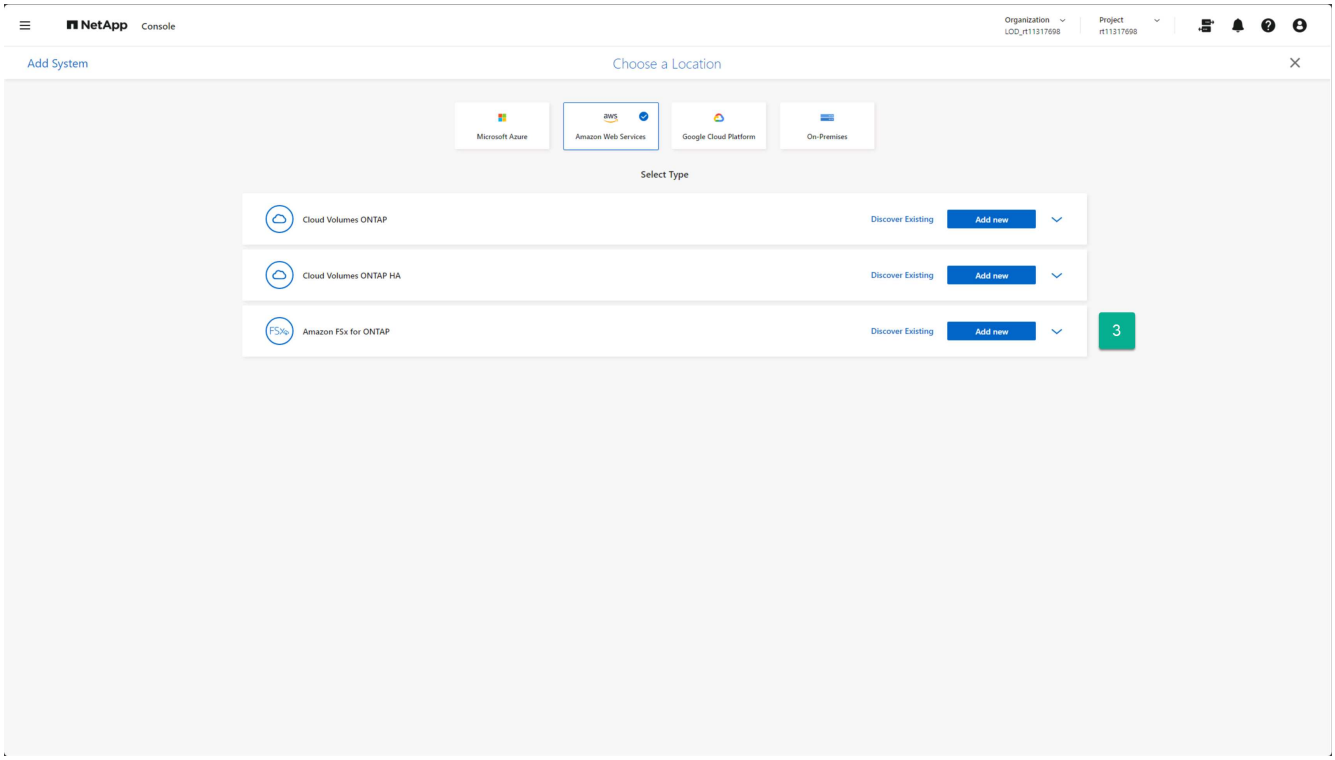
1. Desde la página Sistemas de consola de NetApp , seleccione **Agregar sistema**.



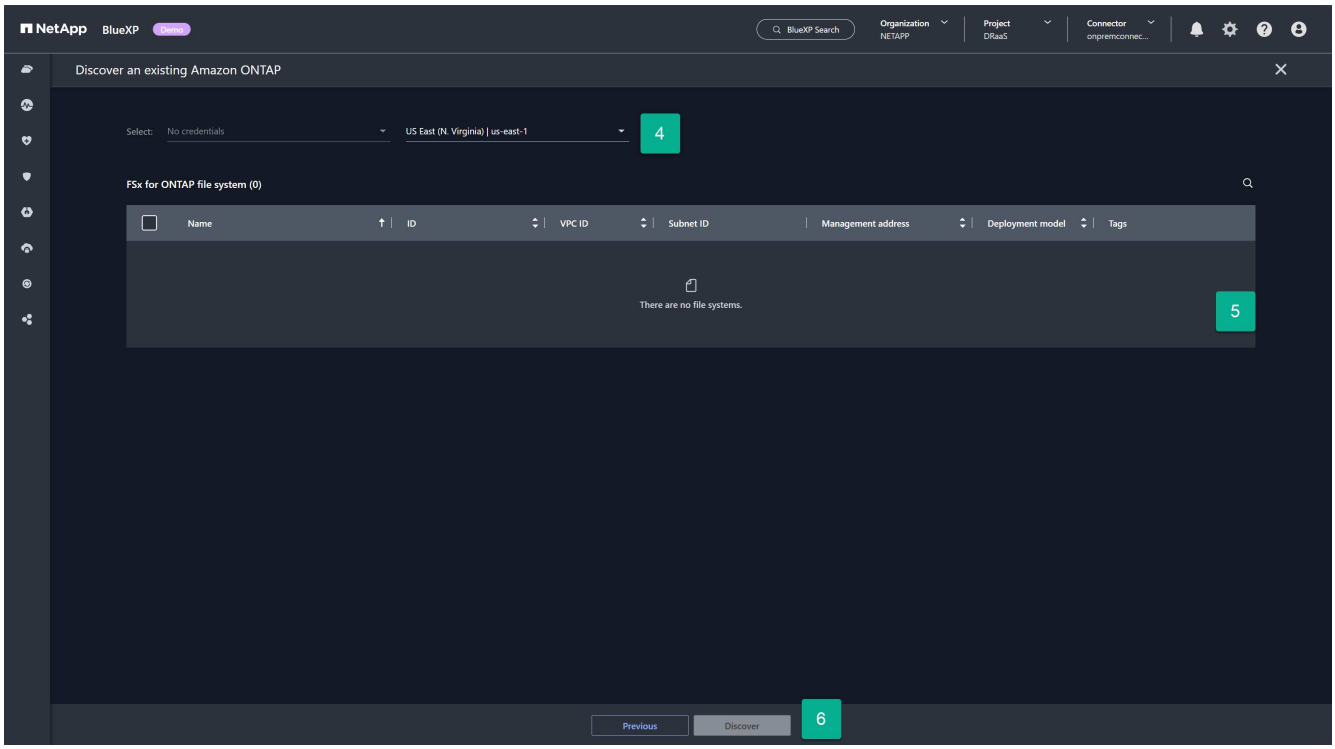

2. Desde la página Agregar sistema, seleccione la tarjeta **Amazon Web Services**.



3. Seleccione el enlace **Descubrir existente** en la tarjeta Amazon FSx para ONTAP .




4. Seleccione las credenciales y la región de AWS que aloja la instancia de FSx para ONTAP .
5. Seleccione uno o más sistemas de archivos FSx para ONTAP que se agregarán.
6. Seleccione **Descubrir** en la parte inferior de la página.




7. Repita los pasos 1 a 6 para cada instancia de FSx for ONTAP que alojará almacenes de datos de vCenter.

### Agregue el servicio NetApp Disaster Recovery a su cuenta de consola NetApp para Amazon EVS

NetApp Disaster Recovery es un producto con licencia que debe adquirirse antes de poder usarse. Existen varios tipos de licencias y varias formas de adquirirlas. Una licencia le da derecho a proteger una cantidad específica de datos durante un período de tiempo específico.

Para obtener más información sobre las licencias de NetApp Disaster Recovery, consulte"Configurar licencias para NetApp Disaster Recovery" .

#### Tipos de licencia

Hay dos tipos de licencias principales:

- NetApp ofrece una"Licencia de prueba de 30 días" que puede utilizar para evaluar NetApp Disaster Recovery utilizando sus recursos ONTAP y VMware. Esta licencia proporciona 30 días de uso para una cantidad ilimitada de capacidad protegida.
- Compre una licencia de producción si desea protección contra desastres más allá del período de prueba de 30 días. Esta licencia se puede comprar a través de los mercados de cualquiera de los socios de nube de NetApp, pero para esta guía, recomendamos que compre su licencia de mercado para NetApp Disaster Recovery utilizando Amazon AWS Marketplace. Para obtener más información sobre cómo comprar una licencia a través de Amazon Marketplace, consulte"Suscríbete a través de AWS Marketplace" .

#### Dimensione sus necesidades de capacidad de recuperación ante desastres

Antes de comprar su licencia, debe comprender cuánta capacidad de almacenamiento de ONTAP necesita proteger. Una de las ventajas de utilizar el almacenamiento NetApp ONTAP es la alta eficiencia con la que NetApp almacena sus datos. Todos los datos almacenados en un volumen ONTAP (como un almacén de datos VMware que aloja máquinas virtuales) se almacenan de manera altamente eficiente. ONTAP utiliza de forma predeterminada tres tipos de eficiencia de almacenamiento al escribir datos en el almacenamiento físico: compactación, deduplicación y compresión. El resultado neto es una eficiencia de almacenamiento de entre 1,5:1 y 4:1, dependiendo de los tipos de datos que se almacenen. De hecho, NetApp ofrece una "garantía de eficiencia de almacenamiento" para ciertas cargas de trabajo.

Esto puede beneficiarlo porque NetApp Disaster Recovery calcula la capacidad para fines de licencia después de que se aplican todas las eficiencias de almacenamiento de ONTAP . Por ejemplo, supongamos que ha aprovisionado un almacén de datos NFS de 100 terabytes (TiB) dentro de vCenter para alojar 100 máquinas virtuales que desea proteger mediante el servicio. Además, supongamos que cuando los datos se escriben en el volumen ONTAP , las técnicas de eficiencia de almacenamiento aplicadas automáticamente dan como resultado que esas máquinas virtuales consuman solo 33 TiB (eficiencia de almacenamiento de 3:1). NetApp Disaster Recovery solo necesita una licencia de 33 TiB, no de 100 TiB. Esto puede representar un beneficio muy grande para el costo total de propiedad de su solución de DR en comparación con otras soluciones de DR.

#### Pasos

1. Para determinar cuántos datos se consumen en cada volumen que aloja un almacén de datos VMware que se va a proteger, determine el consumo de capacidad en disco ejecutando el comando CLI de ONTAP para cada volumen: `volume show-space -volume < volume name > -vserver < SVM name >` .

   Por ejemplo:

```
cluster1::> volume show-space
Vserver : vm-nfs-ds1
Volume  : vol0
Feature                                  Used      Used%
--------------------------------      --------     ------
User Data                              163.4MB         3%
Filesystem Metadata                      172KB         0%
Inodes                                  2.93MB         0%
Snapshot Reserve                       292.9MB         5%
Total Metadata                           185KB         0%
Total Used                             459.4MB         8%
Total Physical Used                    166.4MB         3%
```

2. Tenga en cuenta el valor **Total físico utilizado** para cada volumen. Esta es la cantidad de datos que NetApp Disaster Recovery necesita proteger y es el valor que utilizará para determinar cuánta capacidad necesita licenciar.

#### Agregar sitios en NetApp Disaster Recovery para Amazon EVS

Antes de poder proteger su infraestructura de VM, identifique qué clústeres de VMware vCenter alojan las VM que se van a proteger y dónde se encuentran esos vCenters. El primer paso es crear un sitio para representar los centros de datos de origen y destino. Un sitio es un dominio de falla o un dominio de recuperación.

Necesitas crear lo siguiente:

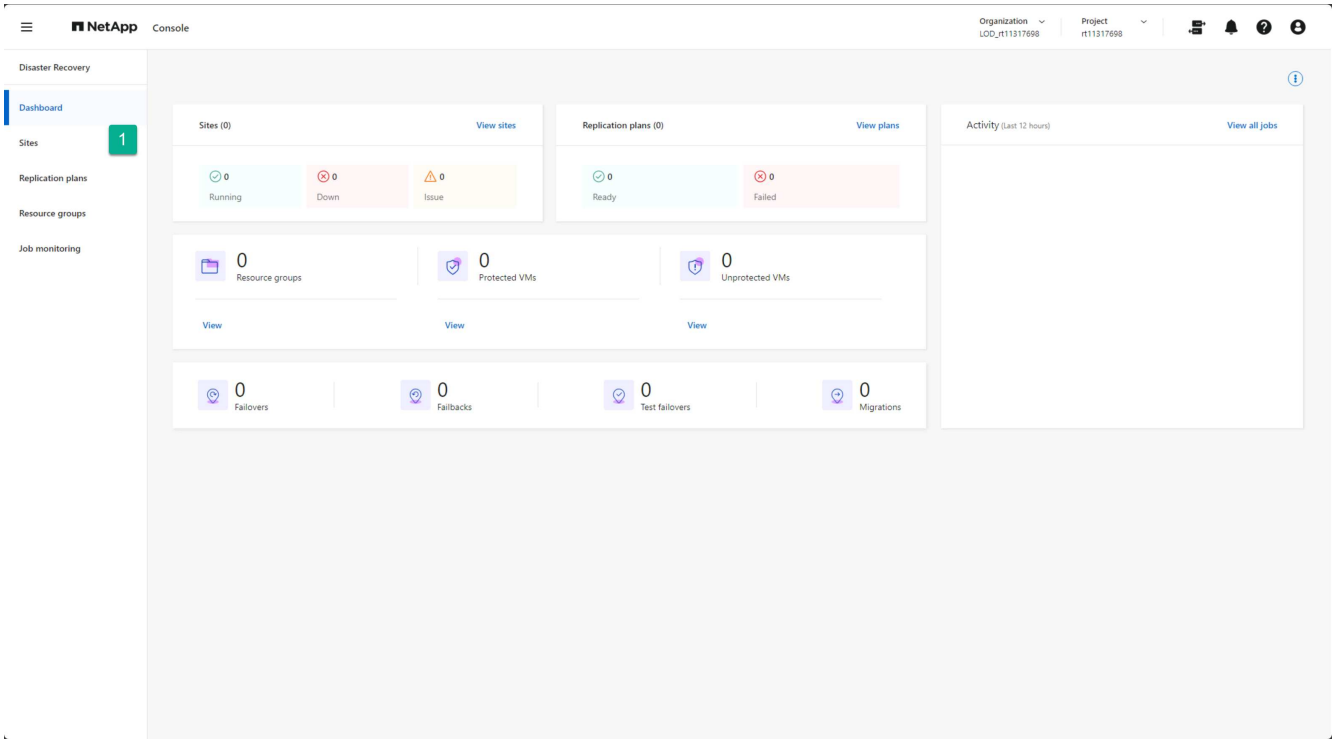
- Un sitio para representar cada centro de datos de producción donde residen sus clústeres de vCenter de producción
- Un sitio para su centro de datos en la nube Amazon EVS/ Amazon FSx for NetApp ONTAP

##### Crear sitios locales

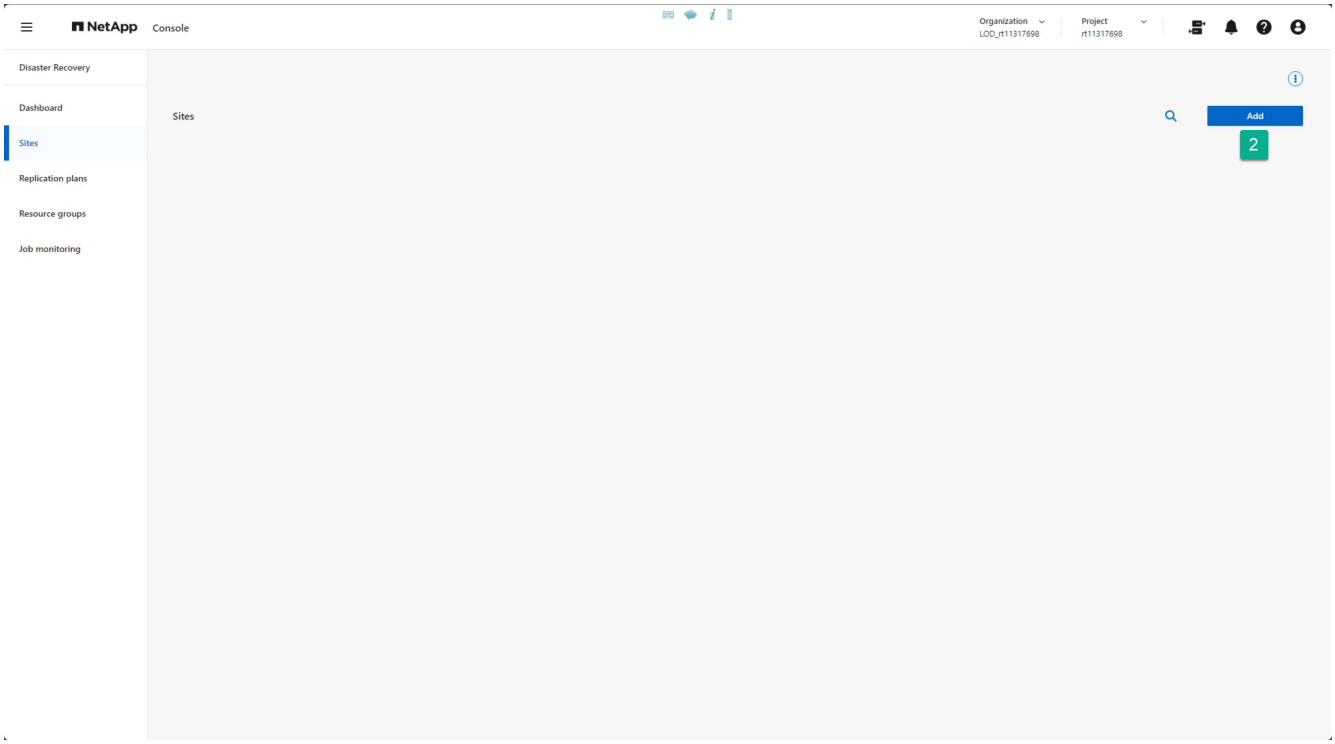
Cree un sitio vCenter de producción.

**Pasos**

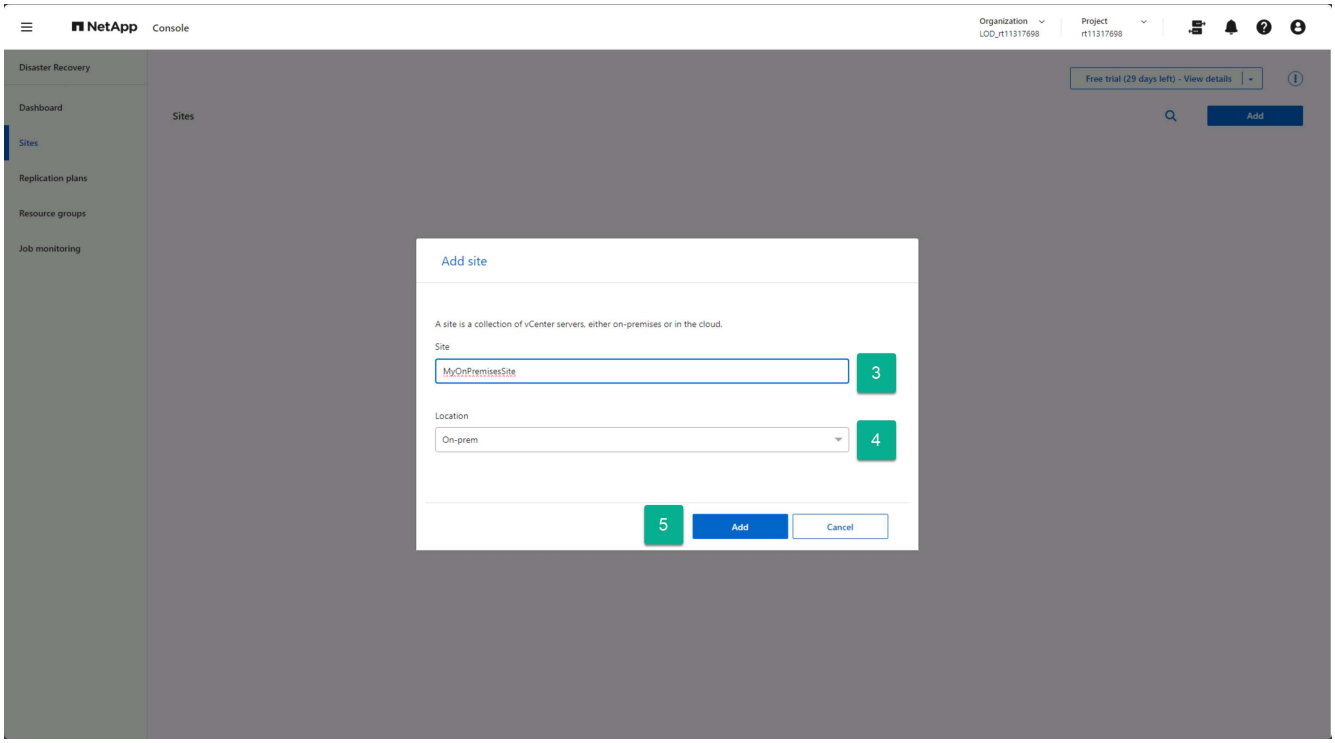
1. Desde la barra de navegación izquierda de la consola de NetApp , seleccione **Protección** > **Recuperación ante desastres**.
2. Desde cualquier página de NetApp Disaster Recovery, seleccione la opción **Sitios**.




3. Desde la opción Sitios, seleccione **Agregar**.




4. En el cuadro de diálogo Agregar sitio, proporcione un nombre para el sitio.
5. Seleccione “En las instalaciones” como ubicación.
6. Seleccione **Agregar**.

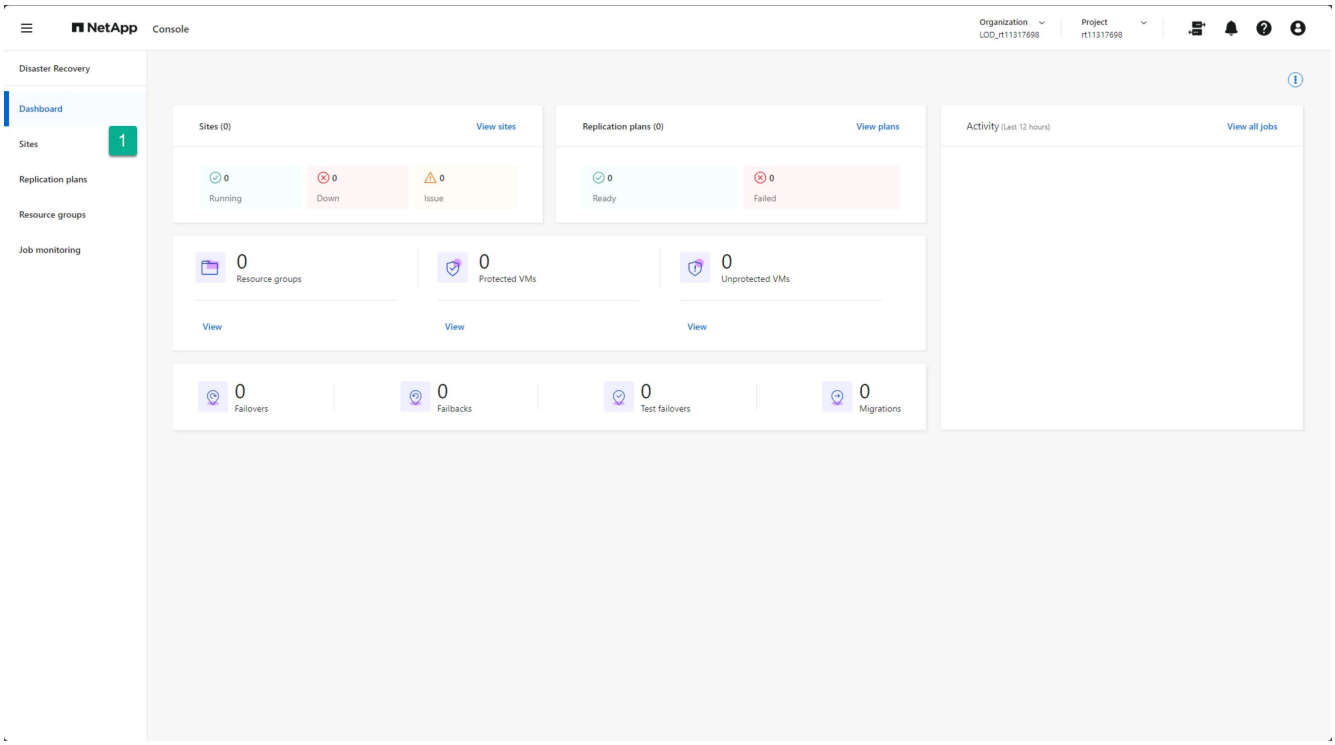



Si tiene otros sitios de vCenter de producción, puede agregarlos siguiendo los mismos pasos.

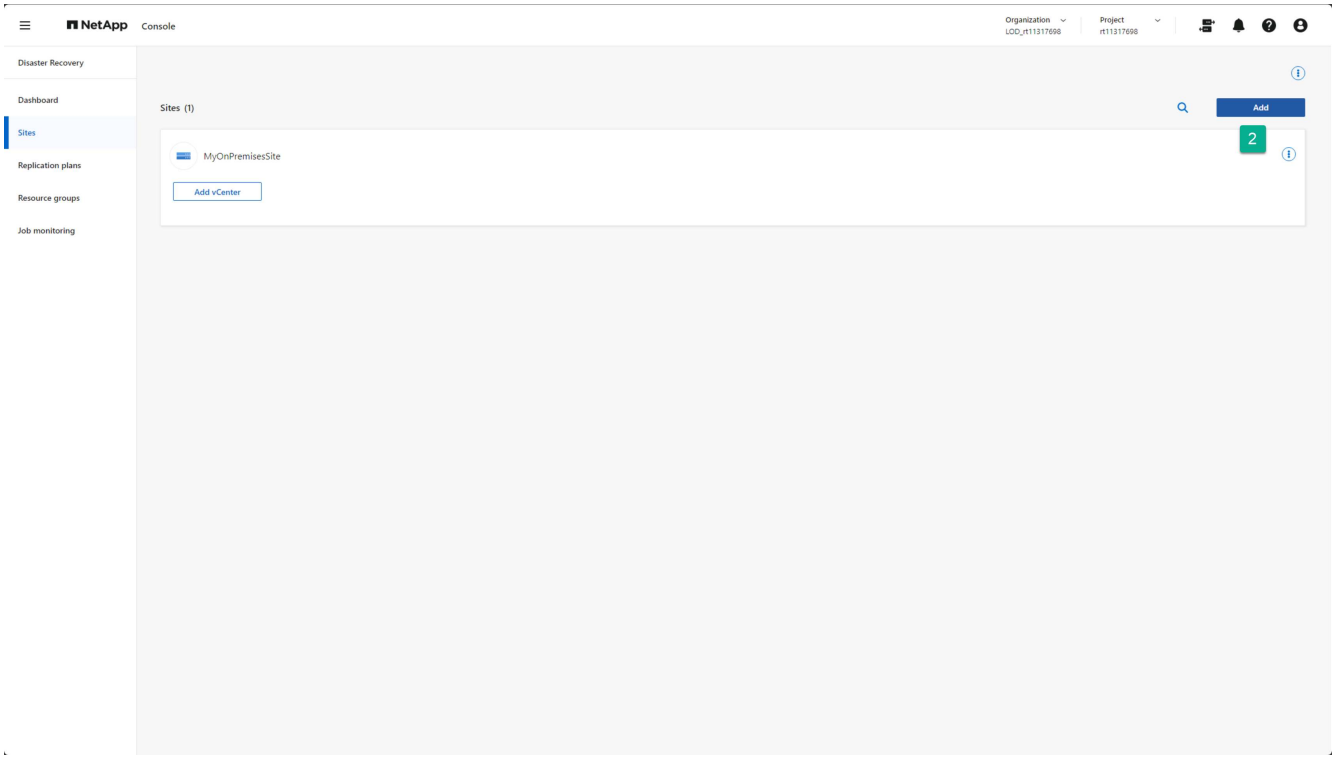
#### Crear sitios en la nube de Amazon

Cree un sitio de recuperación ante desastres para Amazon EVS utilizando Amazon FSx for NetApp ONTAP .

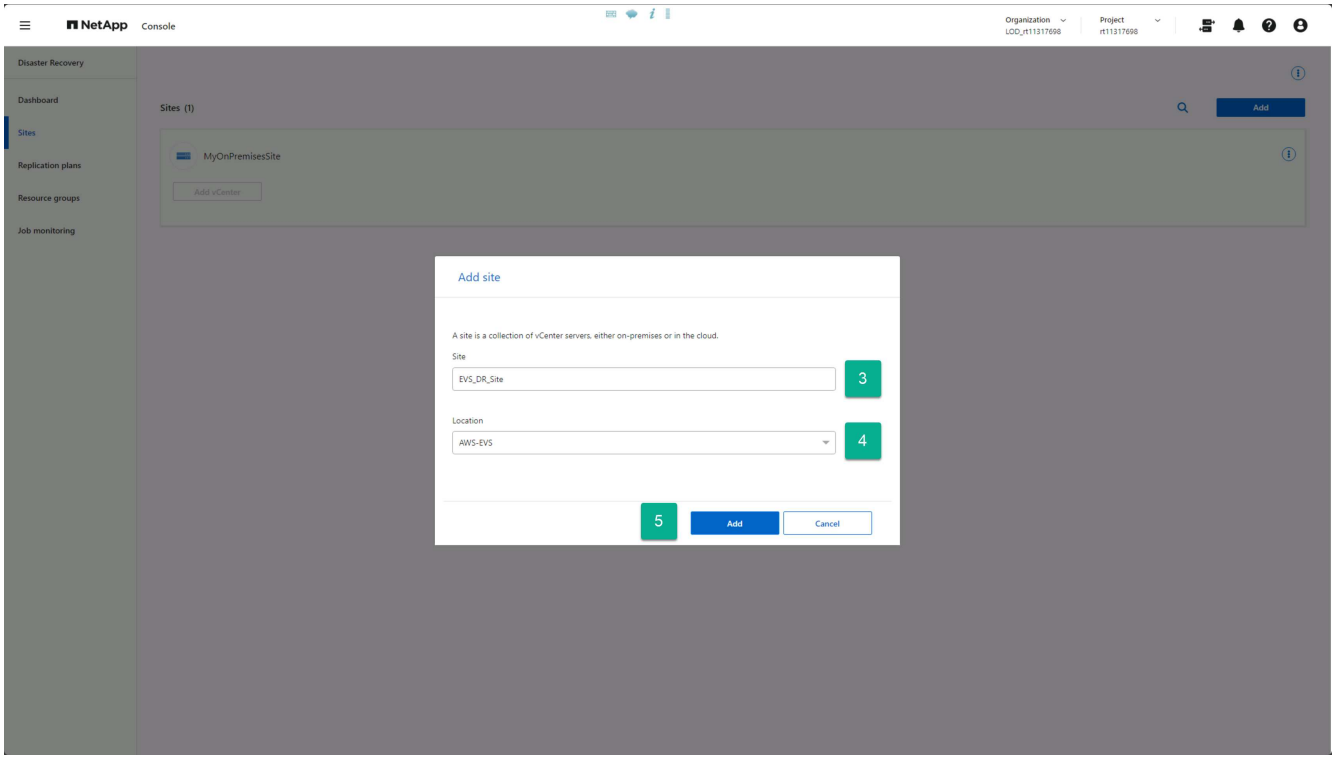
1. Desde cualquier página de NetApp Disaster Recovery, seleccione la opción **Sitios**.




2. Desde la opción Sitios, seleccione **Agregar**.




3. En el cuadro de diálogo Agregar sitio, proporcione un nombre para el sitio.
4. Seleccione “AWS-EVS” como ubicación.
5. Seleccione **Agregar**.




**Resultado**

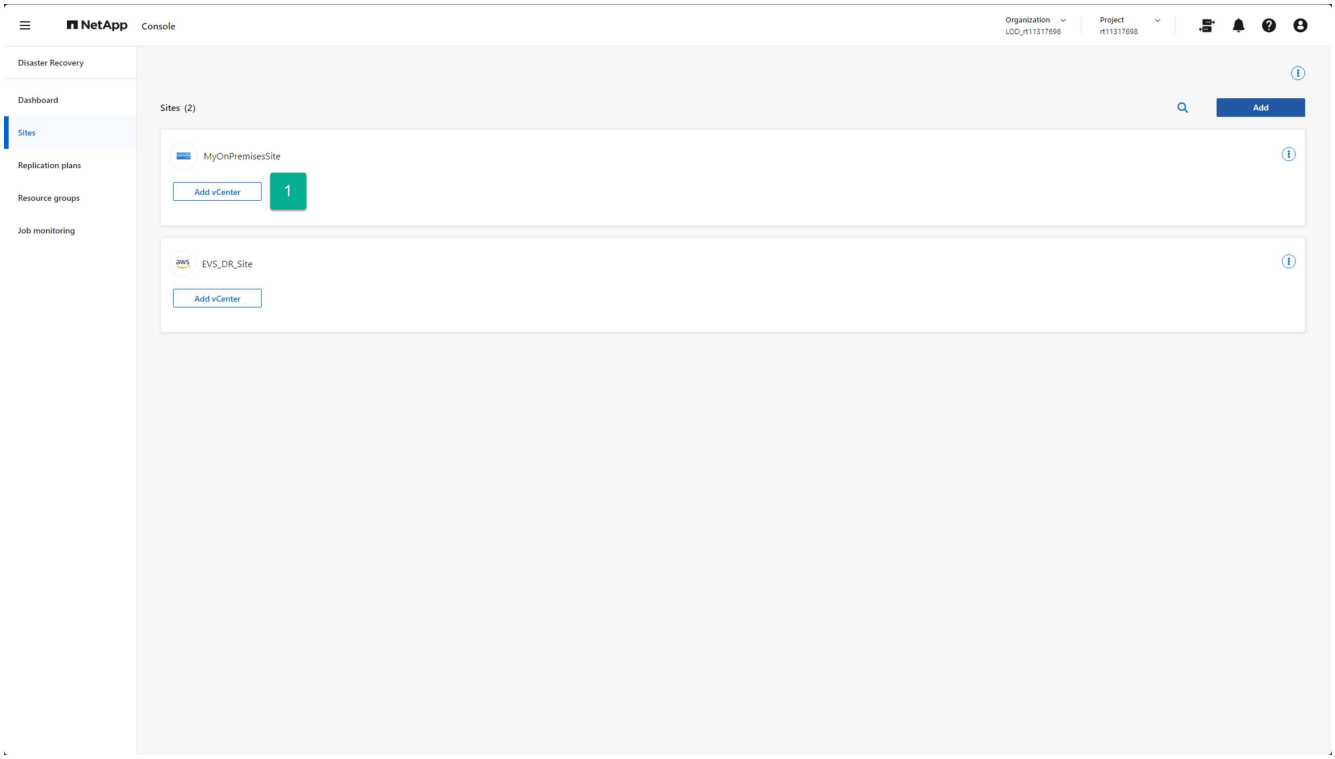
Ahora tiene un sitio de producción (origen) y un sitio de DR (destino) creados.

### Agregue clústeres locales y de Amazon EVS vCenter en NetApp Disaster Recovery

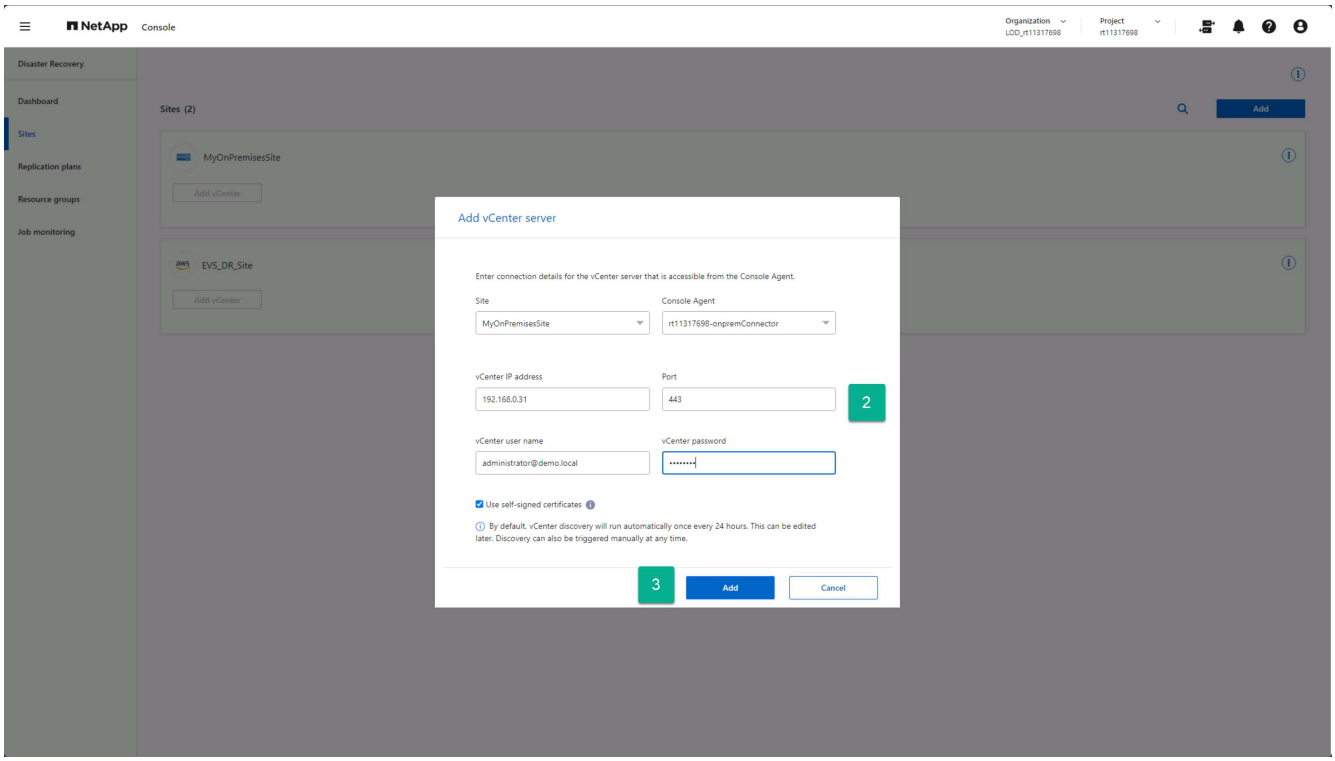
Una vez creados los sitios, ahora puede agregar sus clústeres de vCenter a cada sitio en NetApp Disaster Recovery. Cuando creamos cada sitio, indicamos cada tipo de sitio. Esto le indica a NetApp Disaster Recovery qué tipo de acceso se requiere para los vCenters alojados en cada tipo de sitio. Una de las ventajas de Amazon EVS es que no existe una diferenciación real entre un vCenter de Amazon EVS y un vCenter local. Ambos requieren la misma conexión e información de autenticación.

#### Pasos para agregar un vCenter a cada sitio

1. Desde la opción **Sitios**, seleccione **Agregar vCenter** para el sitio que desee.




2. En el cuadro de diálogo Agregar servidor vCenter, seleccione o proporcione la siguiente información:
   a. El agente de consola de NetApp alojado dentro de su VPC de AWS.
   b. La dirección IP o FQDN del vCenter que se agregará.
   c. Si es diferente, cambie el valor del puerto al puerto TCP utilizado por el administrador de clúster de vCenter.
   d. El nombre de usuario de vCenter para la cuenta creada anteriormente que NetApp Disaster Recovery utilizará para administrar vCenter.
   e. La contraseña de vCenter para el nombre de usuario proporcionado.
   f. Si su empresa utiliza una autoridad de certificación (CA) externa o el almacén de certificados de puntos finales de vCenter para obtener acceso a sus vCenters, desmarque la casilla de verificación **Usar certificados autofirmados**. De lo contrario, deje la casilla marcada.
3. Seleccione **Agregar**.



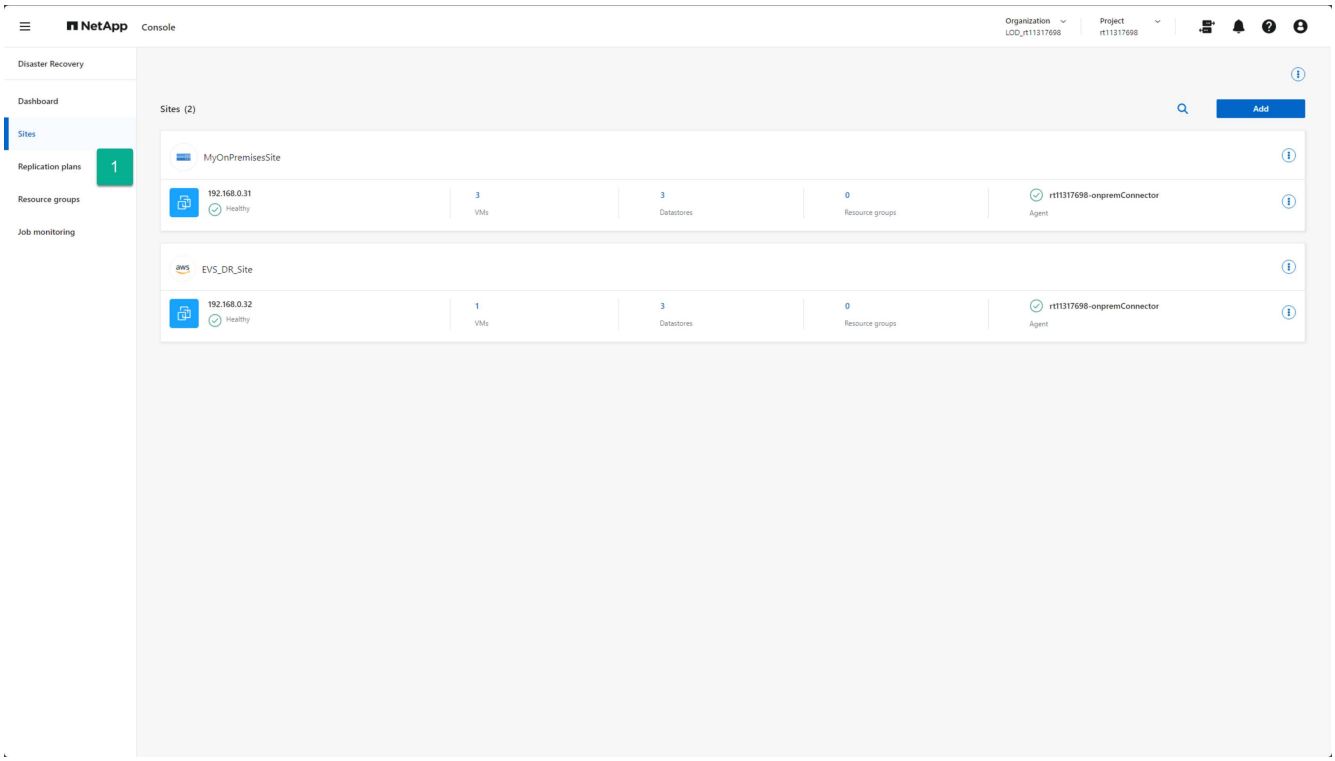

## Crear planes de replicación para Amazon EVS

### Descripción general de la creación de planes de replicación en NetApp Disaster Recovery

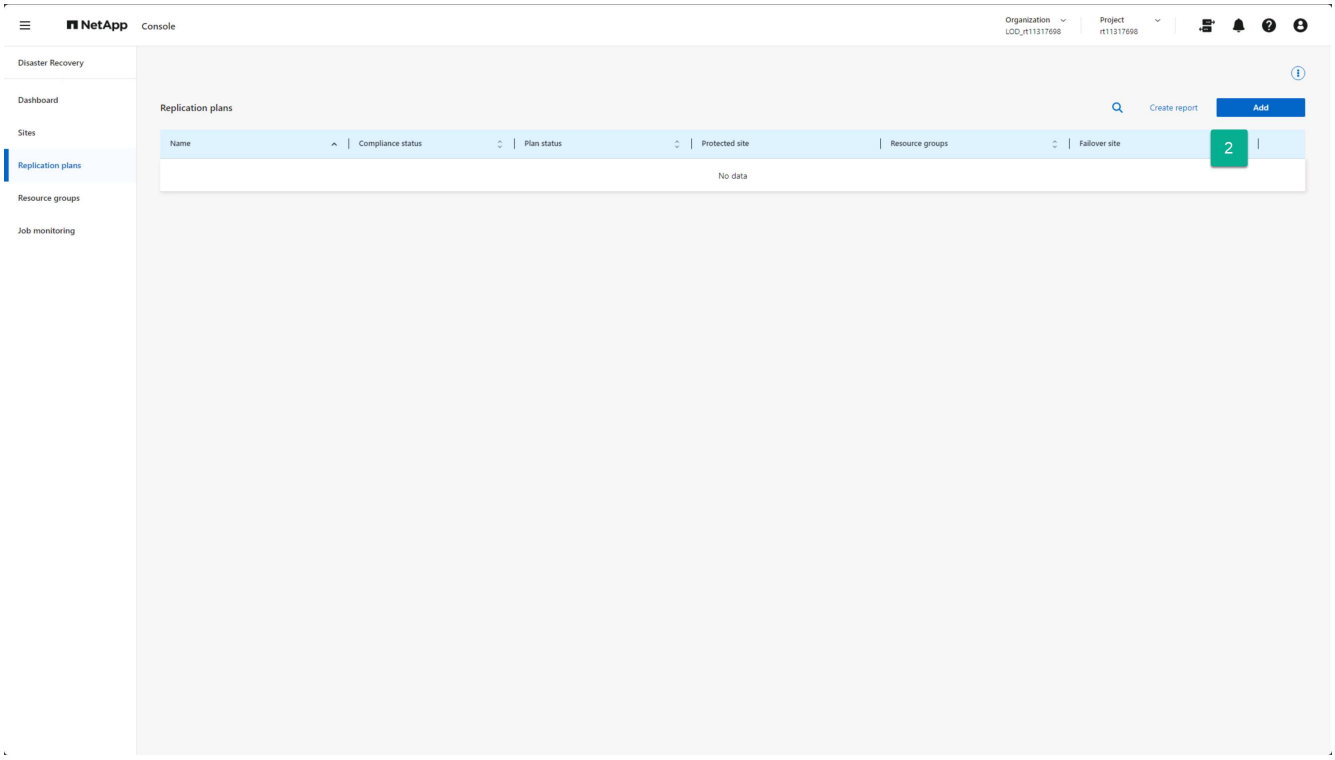
Una vez que tenga vCenters para proteger en el sitio local y tenga un sitio de Amazon EVS configurado para usar Amazon FSx for NetApp ONTAP que pueda usar como destino de recuperación ante desastres, puede crear un plan de replicación (RP) para proteger cualquier conjunto de máquinas virtuales alojadas en el clúster de vCenter dentro de su sitio local.

**Para iniciar el proceso de creación del plan de replicación:**

1. Desde cualquier pantalla de NetApp Disaster Recovery, seleccione la opción **Planes de replicación**.




2. Desde la página Planes de replicación, seleccione **Agregar**.




Esto abre el asistente Crear plan de replicación.

Continuar con"Asistente para crear un plan de replicación Paso 1" .

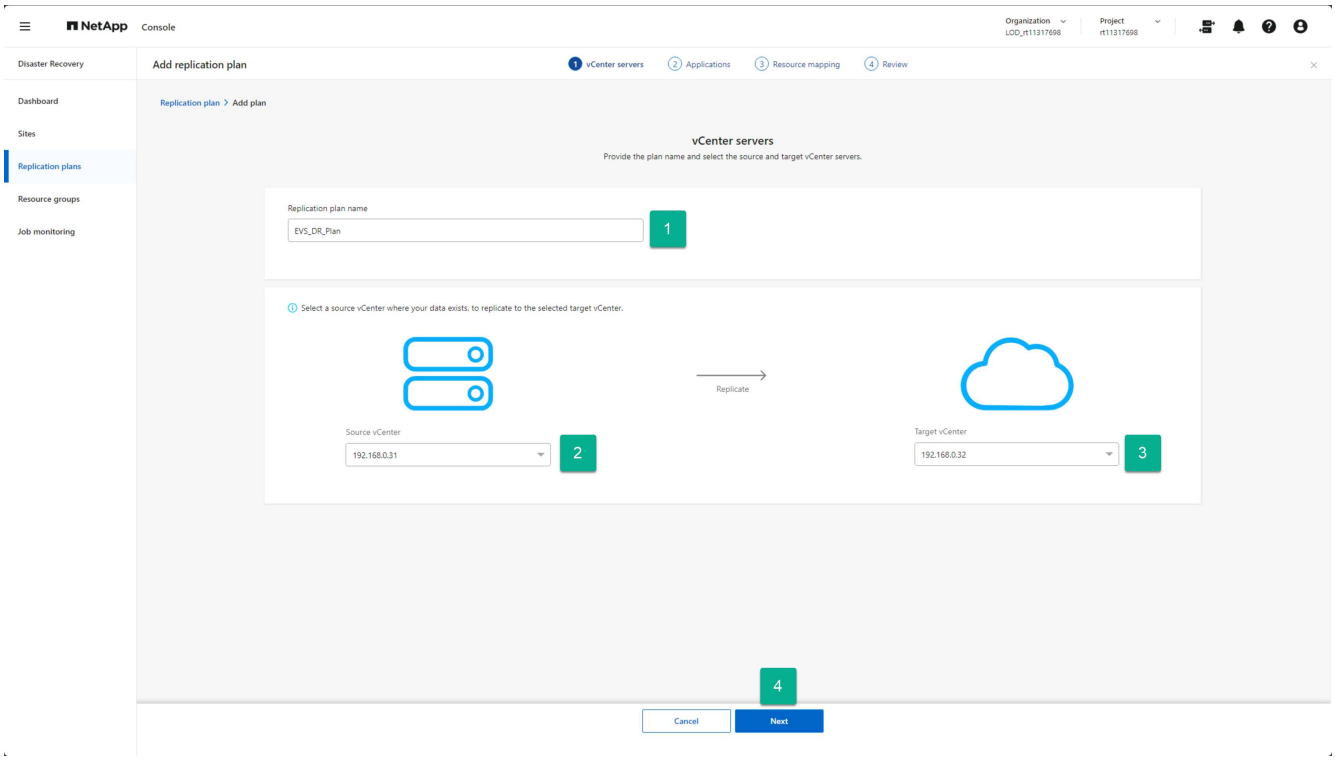
### Crear un plan de replicación: Paso 1: Seleccionar vCenters en NetApp Disaster Recovery

Primero, utilizando NetApp Disaster Recovery, proporcione un nombre de plan de replicación y seleccione los vCenters de origen y destino para la replicación.

1. Introduzca un nombre único para el plan de replicación.

   Solo se permiten caracteres alfanuméricos y guiones bajos (_) para los nombres de los planes de replicación.

2. Seleccione un clúster de vCenter de origen.
3. Seleccione un clúster de vCenter de destino.
4. Seleccione **Siguiente**.




Continuar con"Asistente para crear un plan de replicación Paso 2" .

### Crear un plan de replicación: Paso 2: Seleccionar recursos de VM en NetApp Disaster Recovery

Seleccione las máquinas virtuales que se protegerán mediante NetApp Disaster Recovery.

Hay varias formas de seleccionar máquinas virtuales para protección:

- **Seleccionar máquinas virtuales individuales**: al hacer clic en el botón **Máquinas virtuales** podrá seleccionar máquinas virtuales individuales para proteger. A medida que selecciona cada VM, el servicio la agrega a un grupo de recursos predeterminado ubicado en el lado derecho de la pantalla.
- **Seleccionar grupos de recursos creados previamente**: puede crear grupos de recursos personalizados de antemano utilizando la opción Grupo de recursos del menú NetApp Disaster Recovery. Esto no es un requisito ya que puede utilizar los otros dos métodos para crear un grupo de recursos como parte del

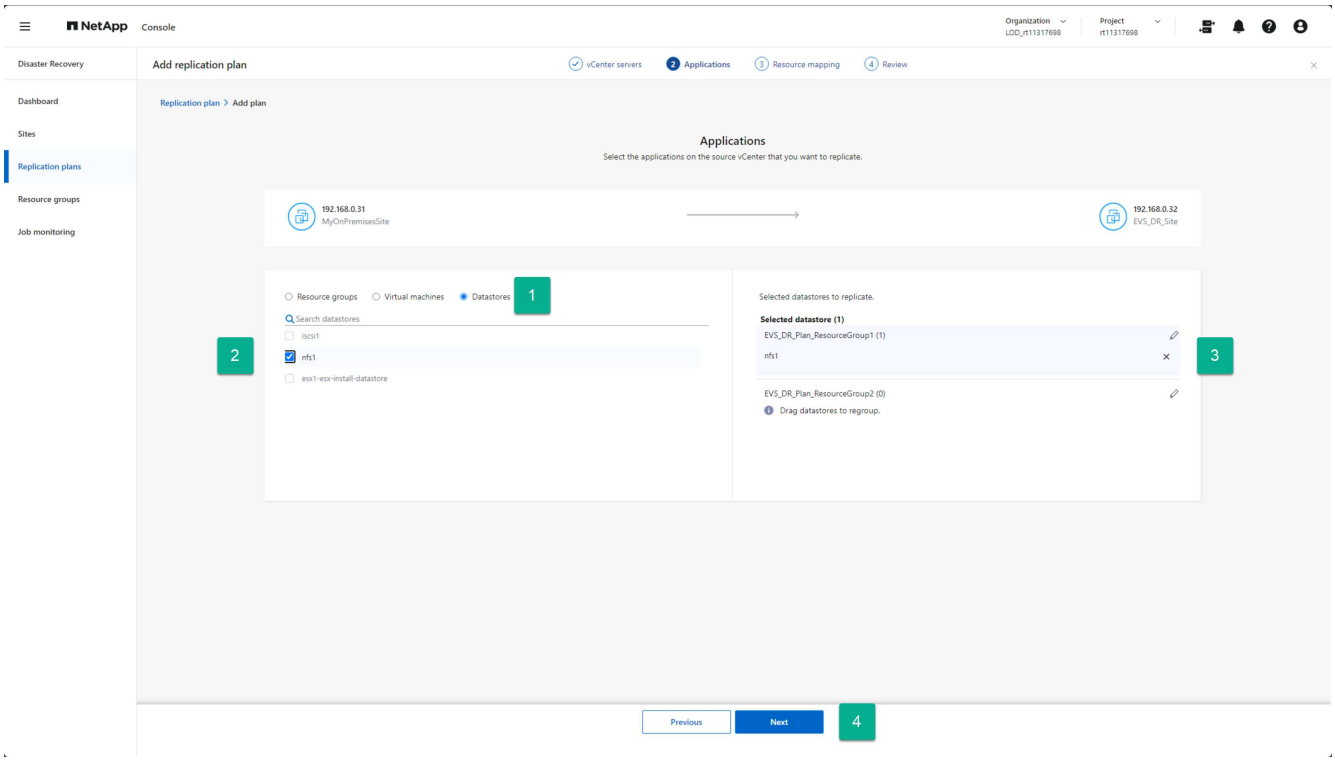
proceso del plan de replicación. Para obtener más información, consulte "Crear un plan de replicación" .

- **Seleccionar almacenes de datos de vCenter completos**: si tiene muchas máquinas virtuales para proteger con este plan de replicación, es posible que no sea tan eficiente seleccionar máquinas virtuales individuales. Debido a que NetApp Disaster Recovery utiliza la replicación SnapMirror basada en volumen para proteger las máquinas virtuales, todas las máquinas virtuales que residen en un almacén de datos se replicarán como parte del volumen. En la mayoría de los casos, debe hacer que NetApp Disaster Recovery proteja y reinicie cualquier máquina virtual ubicada en el almacén de datos. Utilice esta opción para indicarle al servicio que agregue cualquier máquina virtual alojada en un almacén de datos seleccionado a la lista de máquinas virtuales protegidas.

Para esta instrucción guiada, seleccionamos todo el almacén de datos de vCenter.

**Pasos para acceder a esta página**

1. Desde la página **Plan de replicación**, continúe a la sección **Aplicaciones**.
2. Revise la información en la página **Aplicaciones** que se abre.




**Pasos para seleccionar el almacén o almacenes de datos:**

1. Seleccione **Almacenes de datos**.
2. Marque las casillas de verificación junto a cada almacén de datos que desee proteger.
3. (Opcionalmente) Cambie el nombre del grupo de recursos a un nombre adecuado seleccionando el ícono de lápiz junto al nombre del grupo de recursos.
4. Seleccione **Siguiente**.

Continuar con"Asistente para crear un plan de replicación Paso 3" .

**Crear un plan de replicación: Paso 3: Asignar recursos en NetApp Disaster Recovery**

Una vez que tenga una lista de máquinas virtuales que desea proteger mediante NetApp

Disaster Recovery, proporcione información de configuración de máquina virtual y mapeo de conmutación por error para usar durante una conmutación por error.

Es necesario mapear cuatro tipos principales de información:

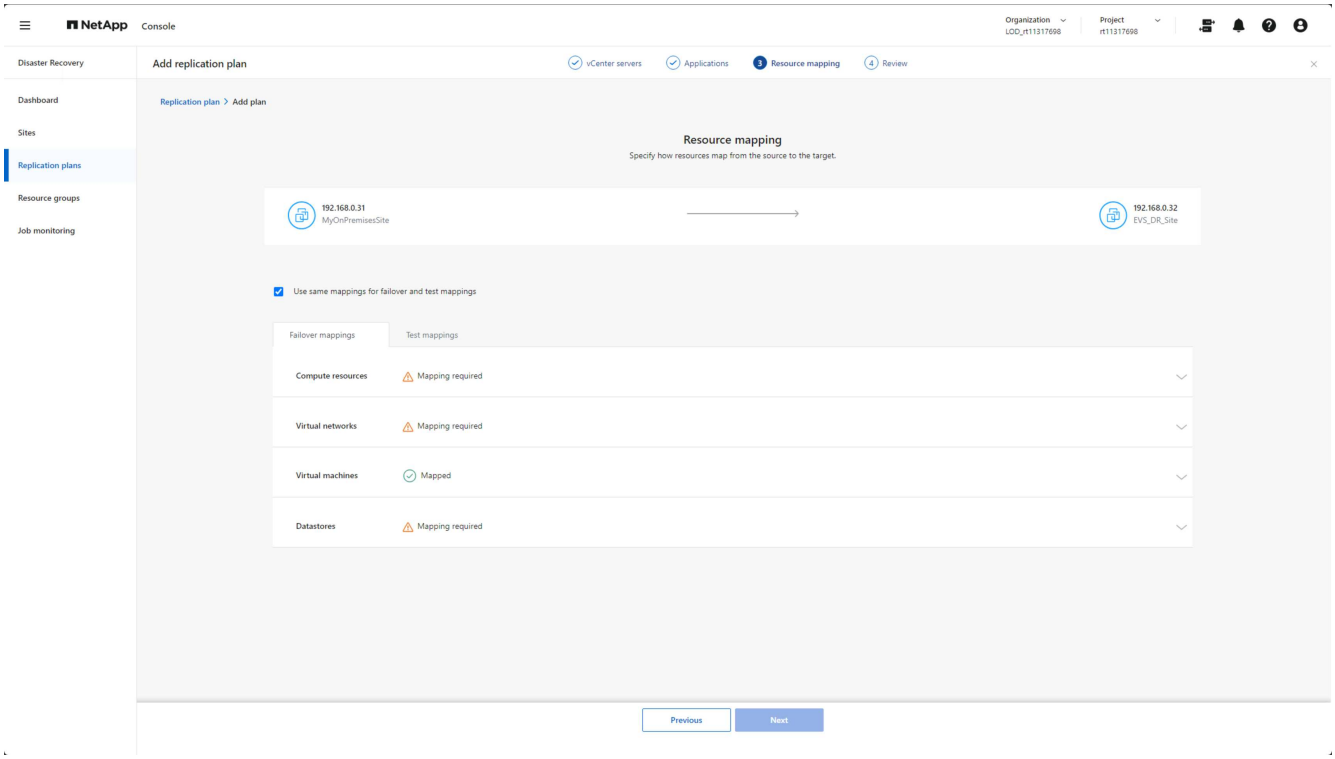
- Recursos computacionales
- Redes virtuales
- Reconfiguración de VM
- Mapeo de almacenes de datos

Cada VM requiere los primeros tres tipos de información. Se requiere el mapeo del almacén de datos para cada almacén de datos que aloja máquinas virtuales que se van a proteger.

- Las secciones con el icono de precaución ( ) requieren que usted proporcione información cartográfica.
- La sección marcada con el icono de verificación ( ) han sido mapeados o tienen asignaciones predeterminadas. Revísalos para asegurarte de que la configuración actual cumpla con tus requisitos.

**Pasos para acceder a esta página**

1. Desde la página **Plan de replicación**, continúe a la sección **Mapeo de recursos**.
2. Revise la información en la página **Mapeo de recursos** que se abre.




3. Para abrir cada categoría de asignaciones requeridas, seleccione la flecha hacia abajo (**v**) junto a la sección.

### Mapeo de recursos computacionales

Debido a que un sitio puede alojar varios centros de datos virtuales y varios clústeres de vCenter, debe identificar en qué clúster de vCenter recuperar las máquinas virtuales en caso de una conmutación por error.

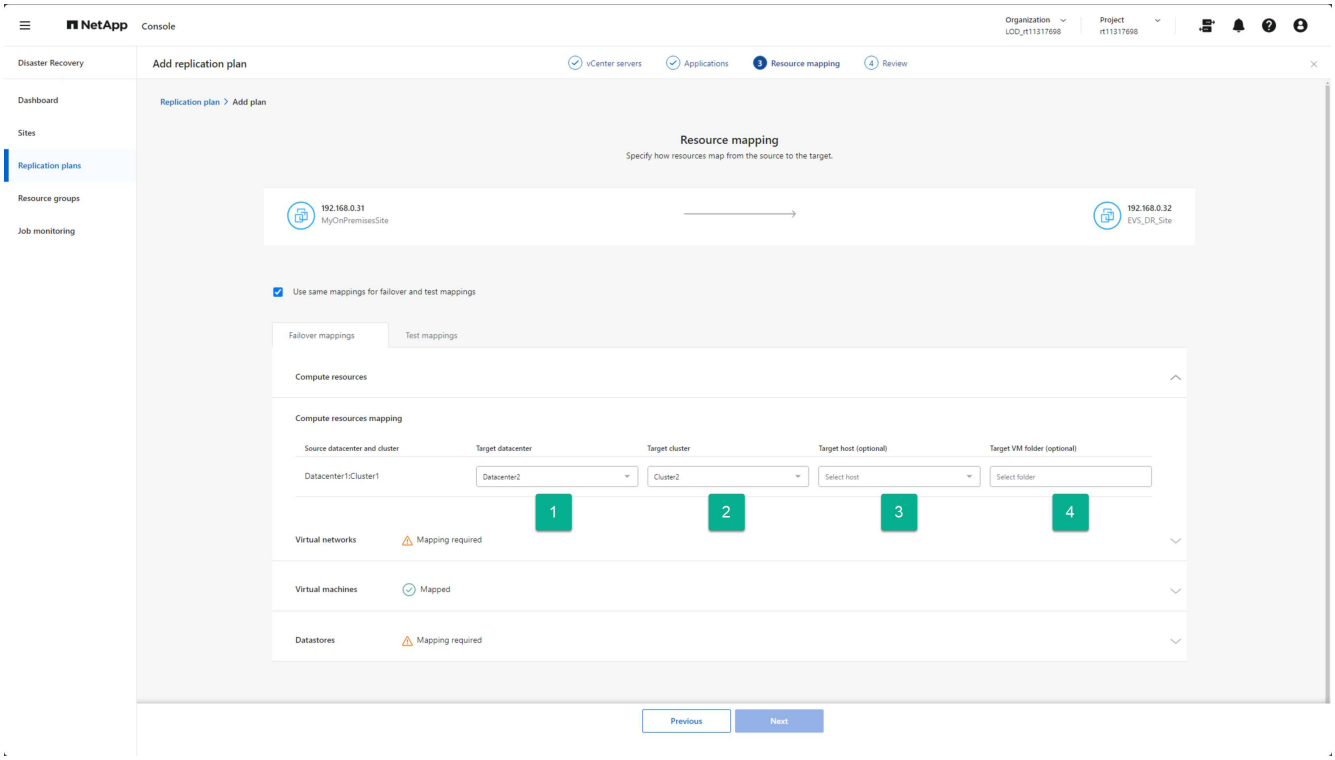
### Pasos para mapear recursos computacionales

1. Seleccione el centro de datos virtual de la lista de centros de datos ubicados en el sitio de recuperación ante desastres.
2. Seleccione el clúster para alojar los almacenes de datos y las máquinas virtuales de la lista de clústeres dentro del centro de datos virtual seleccionado.
3. (Opcional) Seleccione un host de destino en el clúster de destino.

   Este paso no es necesario porque NetApp Disaster Recovery selecciona el primer host agregado al clúster en vCenter. En ese momento, las máquinas virtuales continúan ejecutándose en ese host ESXi o VMware DRS mueve la máquina virtual a un host ESXi diferente según sea necesario en función de las reglas de DRS configuradas.

4. (Opcional) Proporcione el nombre de una carpeta vCenter de nivel superior donde colocar los registros de VM.

   Esto es para sus necesidades organizativas y no es obligatorio.

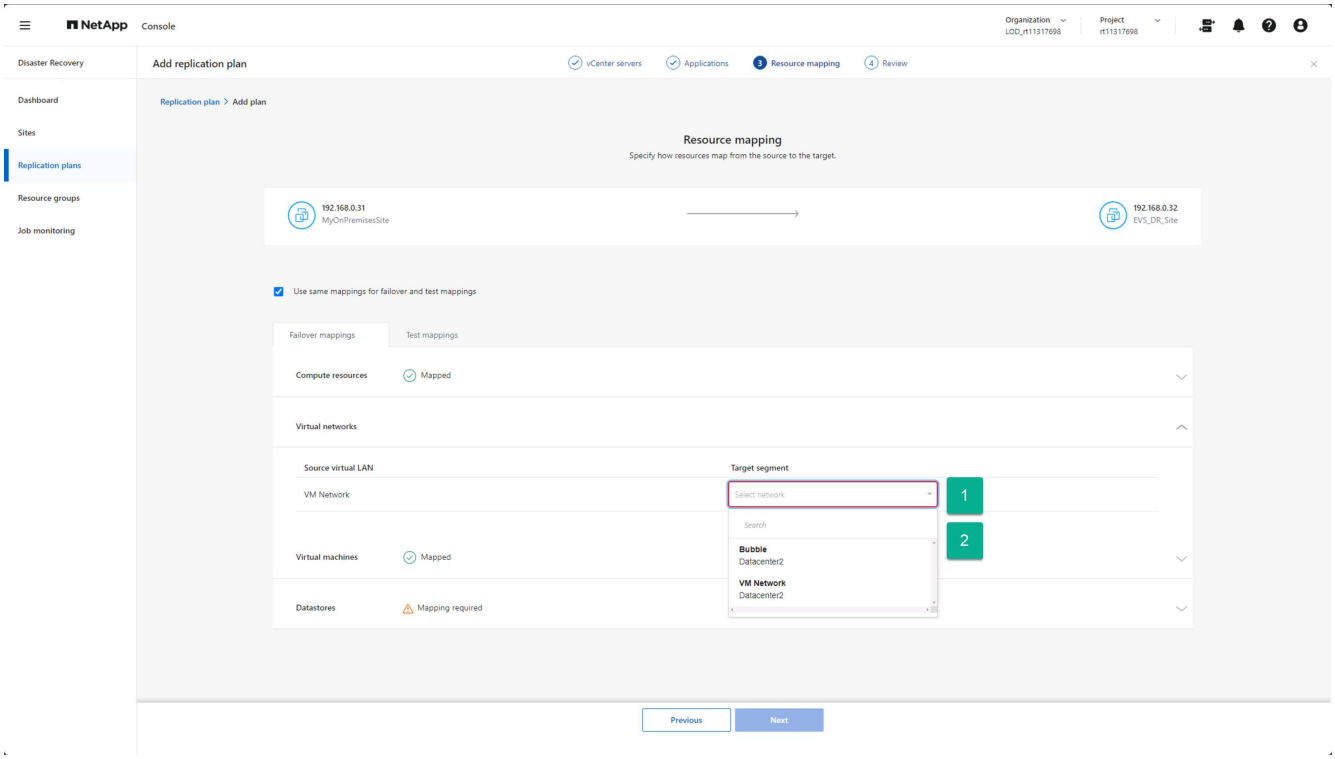



### Mapear recursos de red virtual

Cada máquina virtual puede tener una o más NIC virtuales conectadas a redes virtuales dentro de la infraestructura de red de vCenter. Para garantizar que cada máquina virtual esté conectada correctamente a las redes deseadas al reiniciar en el sitio de DR, identifique a qué redes virtuales del sitio de DR conectará estas máquinas virtuales. Para ello, asigne cada red virtual del sitio local a una red asociada en el sitio de recuperación ante desastres.

### Seleccione qué red virtual de destino asignar a cada red virtual de origen

1. Seleccione el segmento objetivo de la lista desplegable.
2. Repita el paso anterior para cada red virtual de origen indicada.




**Definir opciones para la reconfiguración de la máquina virtual durante la conmutación por error**

Es posible que cada máquina virtual requiera modificaciones para funcionar correctamente en el sitio DR vCenter. La sección Máquinas virtuales le permite proporcionar los cambios necesarios.

De forma predeterminada, NetApp Disaster Recovery utiliza la misma configuración para cada máquina virtual que la utilizada en el sitio local de origen. Esto supone que las máquinas virtuales utilizarán la misma dirección IP, CPU virtual y configuración de DRAM virtual.

### Reconfiguración de la red

Los tipos de direcciones IP admitidos son estáticos y DHCP. Para direcciones IP estáticas, tienes las siguientes configuraciones de IP de destino:

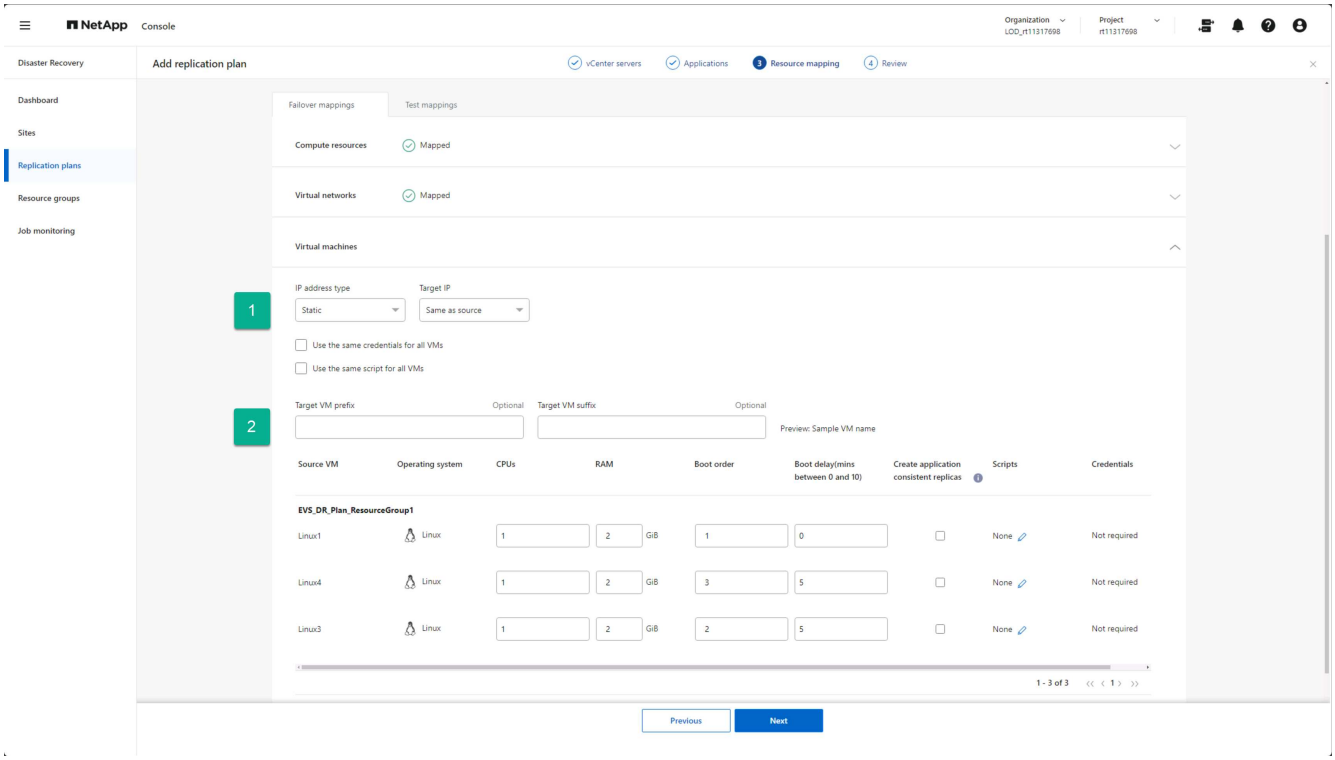
- **Igual que el origen**: como sugiere el nombre, el servicio utiliza la misma dirección IP en la máquina virtual de destino que se utilizó en la máquina virtual en el sitio de origen. Esto requiere que configure las redes virtuales que se asignaron en el paso anterior para las mismas configuraciones de subred.
- **Diferente de la fuente**: el servicio proporciona un conjunto de campos de dirección IP para cada VM que deben configurarse para la subred adecuada utilizada en la red virtual de destino, que asignó en la sección anterior. Para cada máquina virtual debe proporcionar una dirección IP, una máscara de subred, un DNS y valores de puerta de enlace predeterminados. De manera opcional, utilice la misma máscara de subred, DNS y configuración de puerta de enlace para todas las máquinas virtuales para simplificar el proceso cuando todas las máquinas virtuales se conectan a la misma subred.
- **Mapeo de subred**: esta opción reconfigura la dirección IP de cada máquina virtual en función de la configuración CIDR de la red virtual de destino. Para utilizar esta función, asegúrese de que las redes virtuales de cada vCenter tengan una configuración CIDR definida dentro del servicio, como se modificó en la información de vCenter en la página Sitios.

Después de configurar las subredes, la asignación de subredes utiliza el mismo componente de unidad de la dirección IP para la configuración de la máquina virtual de origen y de destino, pero reemplaza el componente de subred de la dirección IP en función de la información CIDR proporcionada. Esta función también requiere que tanto la red virtual de origen como la de destino tengan la misma clase de dirección IP (la `/xx` componente del CIDR). Esto garantiza que haya suficientes direcciones IP disponibles en el sitio de destino para alojar todas las máquinas virtuales protegidas.

Para esta configuración de EVS, asumimos que las configuraciones de IP de origen y destino son las mismas y no requieren ninguna reconfiguración adicional.

**Realizar cambios en la reconfiguración de la configuración de red**

1. Seleccione el tipo de dirección IP que se utilizará para las máquinas virtuales conmutadas por error.
2. (Opcional) Proporcione un esquema de cambio de nombre de VM para las VM reiniciadas proporcionando un valor de prefijo y sufijo opcionales.

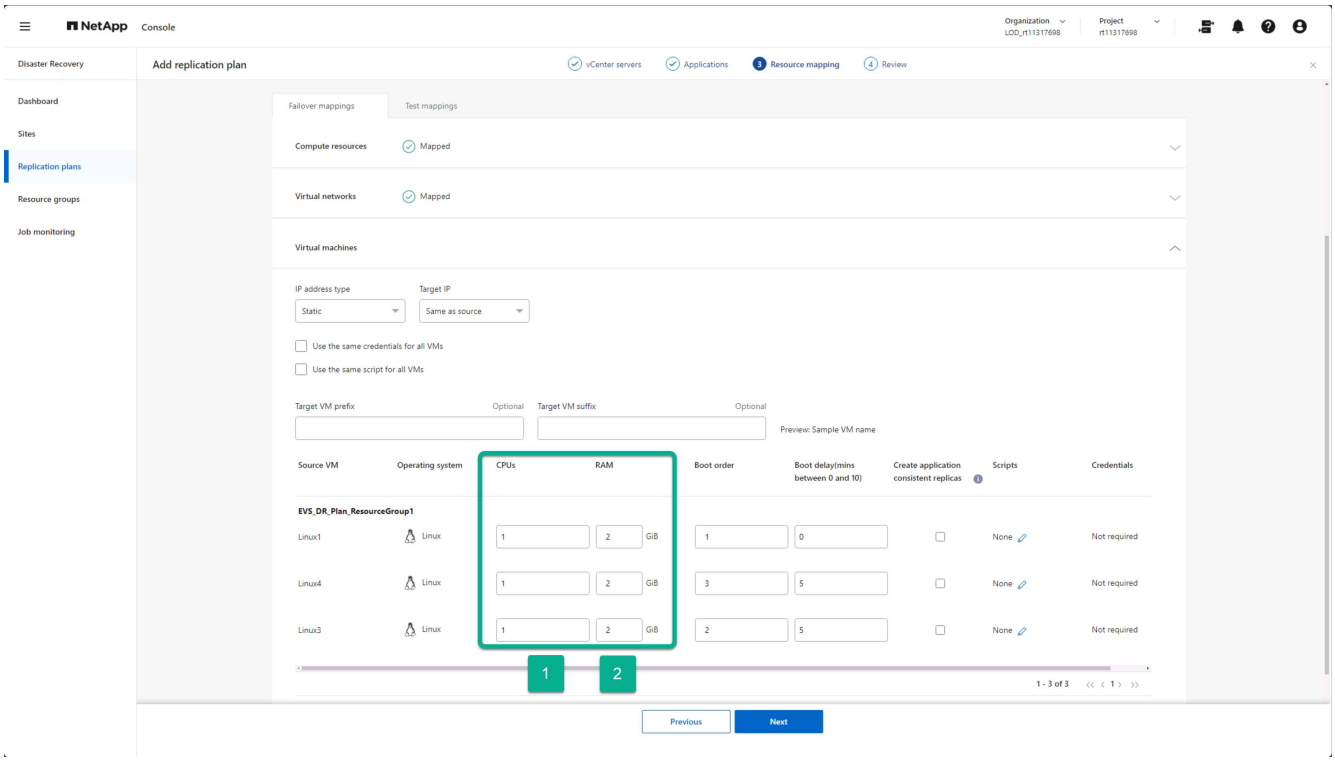



**Reconfiguración de recursos informáticos de la máquina virtual**

Hay varias opciones para reconfigurar los recursos informáticos de la máquina virtual. NetApp Disaster Recovery admite cambiar la cantidad de CPU virtuales, la cantidad de DRAM virtual y el nombre de la máquina virtual.

**Especifique cualquier cambio en la configuración de la máquina virtual**

1. (Opcional) Modifique la cantidad de CPU virtuales que debe utilizar cada máquina virtual. Esto puede ser necesario si los hosts del clúster vCenter de DR no tienen tantos núcleos de CPU como el clúster vCenter de origen.
2. (Opcional) Modifique la cantidad de DRAM virtual que debe utilizar cada máquina virtual. Esto puede ser necesario si los hosts del clúster vCenter de DR no tienen tanta DRAM física como los hosts del clúster vCenter de origen.

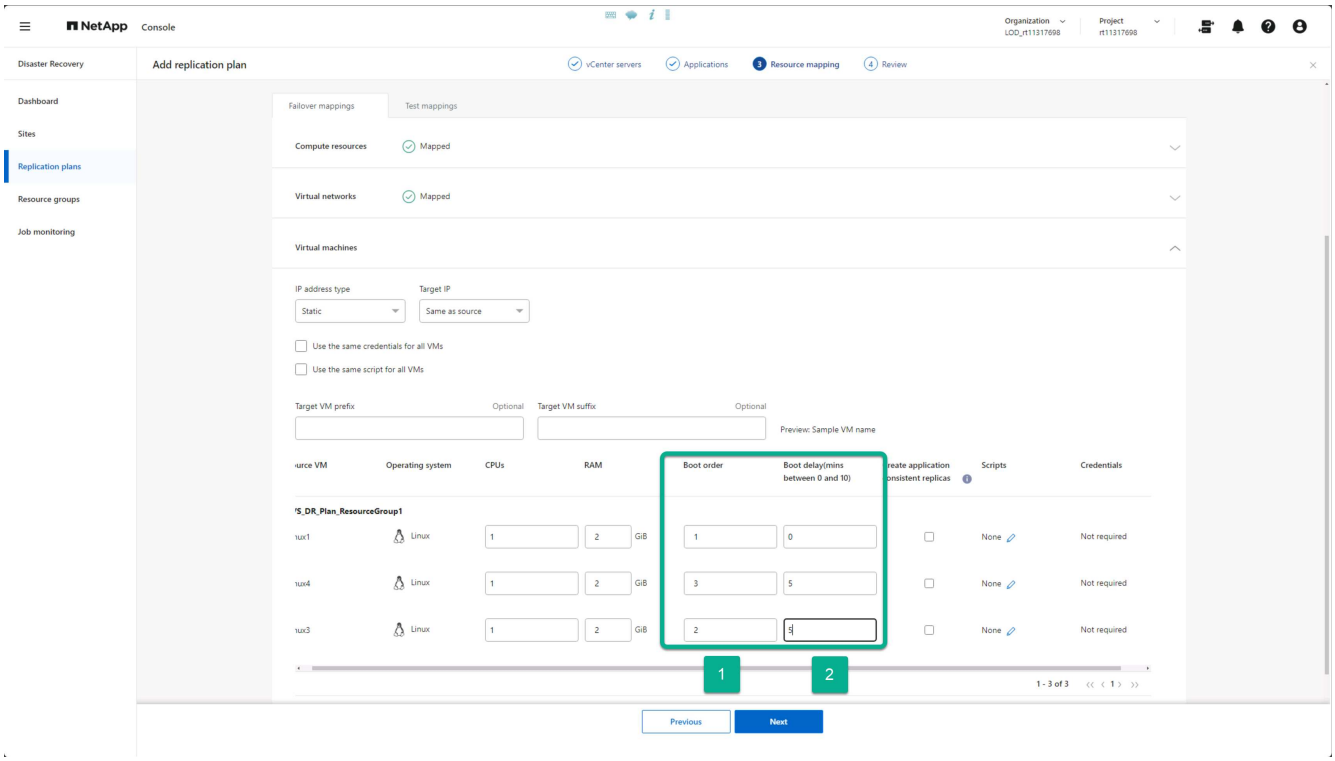



## Orden de arranque

NetApp Disaster Recovery admite un reinicio ordenado de las máquinas virtuales según un campo de orden de arranque. El campo Orden de arranque indica cómo se inician las máquinas virtuales en cada grupo de recursos. Aquellas máquinas virtuales con el mismo valor en el campo Orden de arranque arrancan en paralelo.

### Modificar la configuración del orden de arranque

1. (Opcionalmente) Modifique el orden en que desea que se reinicien sus máquinas virtuales. Este campo acepta cualquier valor numérico. NetApp Disaster Recovery intenta reiniciar las máquinas virtuales que tienen el mismo valor numérico en paralelo.
2. (Opcionalmente) Proporcione un retraso que se utilizará entre cada reinicio de la máquina virtual. El tiempo se inyecta después de que se completa el reinicio de esta VM y antes de las VM con el siguiente número de orden de arranque más alto. Este número está en minutos.



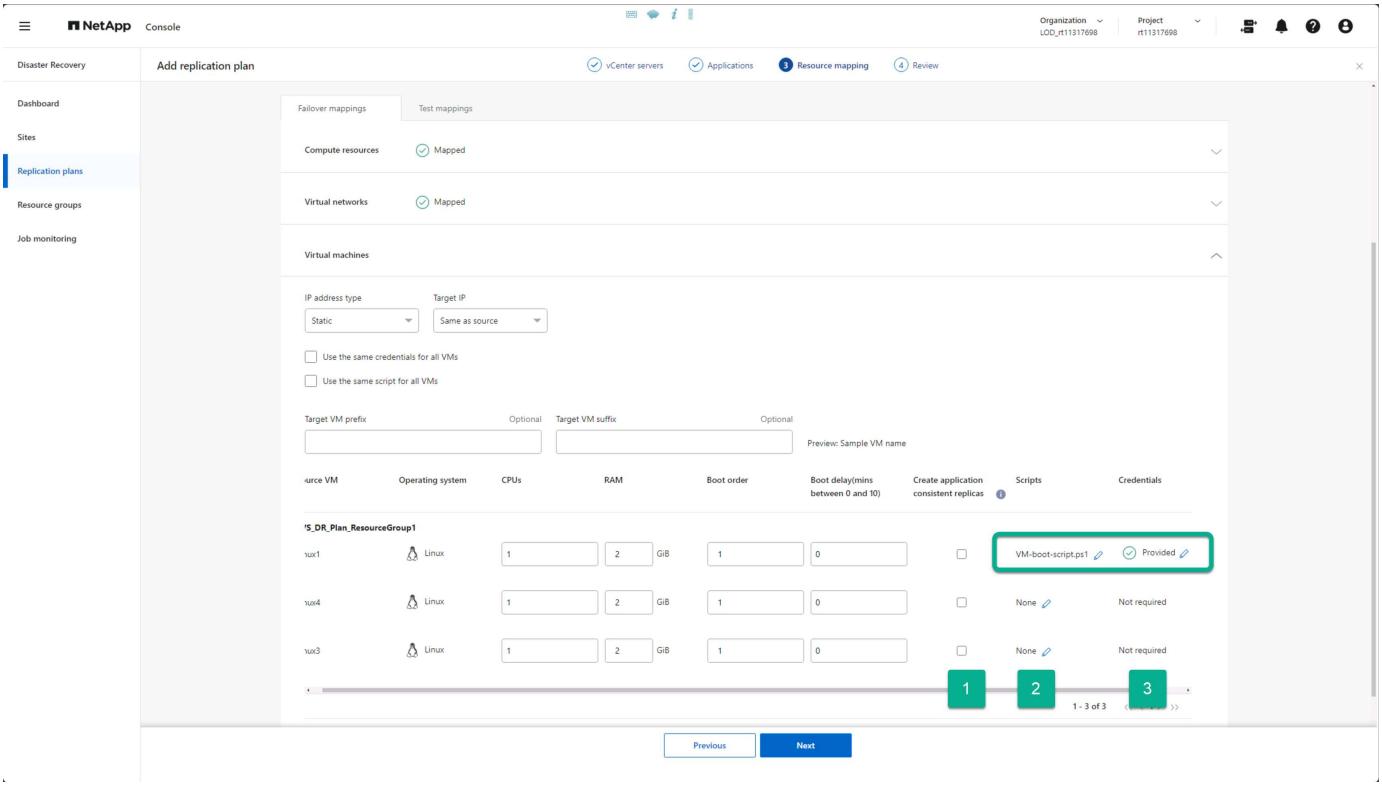

### Operaciones personalizadas del sistema operativo invitado

NetApp Disaster Recovery permite realizar algunas operaciones del sistema operativo invitado para cada máquina virtual:

- NetApp Disaster Recovery puede realizar copias de seguridad consistentes con las aplicaciones de las máquinas virtuales que ejecutan bases de datos Oracle y Microsoft SQL Server.
- NetApp Disaster Recovery puede ejecutar scripts personalizados definidos adecuados para el sistema operativo invitado para cada máquina virtual. La ejecución de dichos scripts requiere credenciales de usuario aceptables para el sistema operativo invitado con amplios privilegios para ejecutar las operaciones enumeradas en el script.

#### Modificar las operaciones del sistema operativo invitado personalizado de cada máquina virtual

1. (Opcional) Marque la casilla de verificación **Crear réplicas consistentes de la aplicación** si la máquina virtual aloja una base de datos Oracle o SQL Server.
2. (Opcional) Para realizar acciones personalizadas dentro del sistema operativo invitado como parte del proceso de inicio, cargue un script para cualquier máquina virtual. Para ejecutar un solo script en todas las máquinas virtuales, utilice la casilla de verificación resaltada y complete los campos.
3. Ciertos cambios de configuración requieren credenciales de usuario con permisos adecuados para realizar las operaciones. Proporcionar credenciales en los siguientes casos:
    - El sistema operativo invitado ejecutará un script dentro de la máquina virtual.
    - Es necesario realizar una instantánea consistente con la aplicación.




**Almacenes de datos de mapas**

El paso final en la creación de un plan de replicación es identificar cómo ONTAP debe proteger los almacenes de datos. Estas configuraciones definen el objetivo de punto de recuperación (RPO) de los planes de replicación, cuántas copias de seguridad se deben mantener y dónde replicar los volúmenes ONTAP de alojamiento de cada almacén de datos de vCenter.

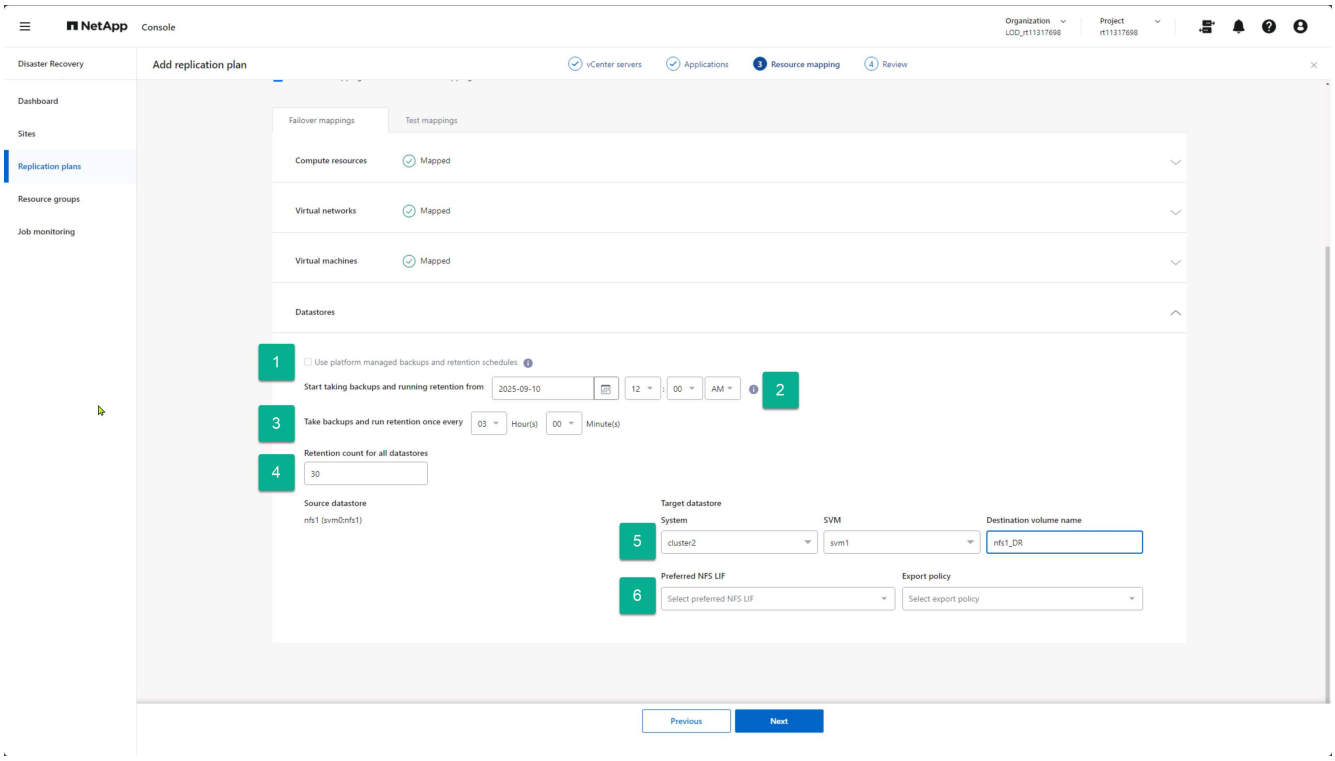
De manera predeterminada, NetApp Disaster Recovery administra su propio programa de replicación de instantáneas; sin embargo, de manera opcional, puede especificar que desea utilizar el programa de política de replicación de SnapMirror existente para la protección del almacén de datos.

Además, puede personalizar opcionalmente qué LIF de datos (interfaces lógicas) y política de exportación utilizar. Si no proporciona estas configuraciones, NetApp Disaster Recovery utiliza todos los LIF de datos asociados con el protocolo apropiado (NFS, iSCSI o FC) y utiliza la política de exportación predeterminada para volúmenes NFS.

**Para configurar la asignación de almacén de datos (volumen)**

1. (Opcional) Decida si desea utilizar un programa de replicación de ONTAP SnapMirror existente o que NetApp Disaster Recovery administre la protección de sus máquinas virtuales (predeterminado).
2. Proporcionar un punto de partida para indicar cuándo el servicio debe comenzar a realizar copias de seguridad.
3. Especifique con qué frecuencia el servicio debe realizar una copia de seguridad y replicarla en el clúster de destino de recuperación ante desastres de Amazon FSx for NetApp ONTAP .
4. Especifique cuántas copias de seguridad históricas se deben conservar. El servicio mantiene la misma cantidad de copias de seguridad en el clúster de almacenamiento de origen y destino.
5. (Opcional) Seleccione una interfaz lógica predeterminada (LIF de datos) para cada volumen. Si no se selecciona ninguno, se configuran todos los LIF de datos en el SVM de destino que admiten el protocolo de acceso al volumen.

6. (Opcional) Seleccione una política de exportación para cualquier volumen NFS. Si no se selecciona, se utiliza la política de exportación predeterminada




Continuar con"Asistente para crear un plan de replicación Paso 4" .

**Crear un plan de replicación: Paso 4: Verificar la configuración en NetApp Disaster Recovery**

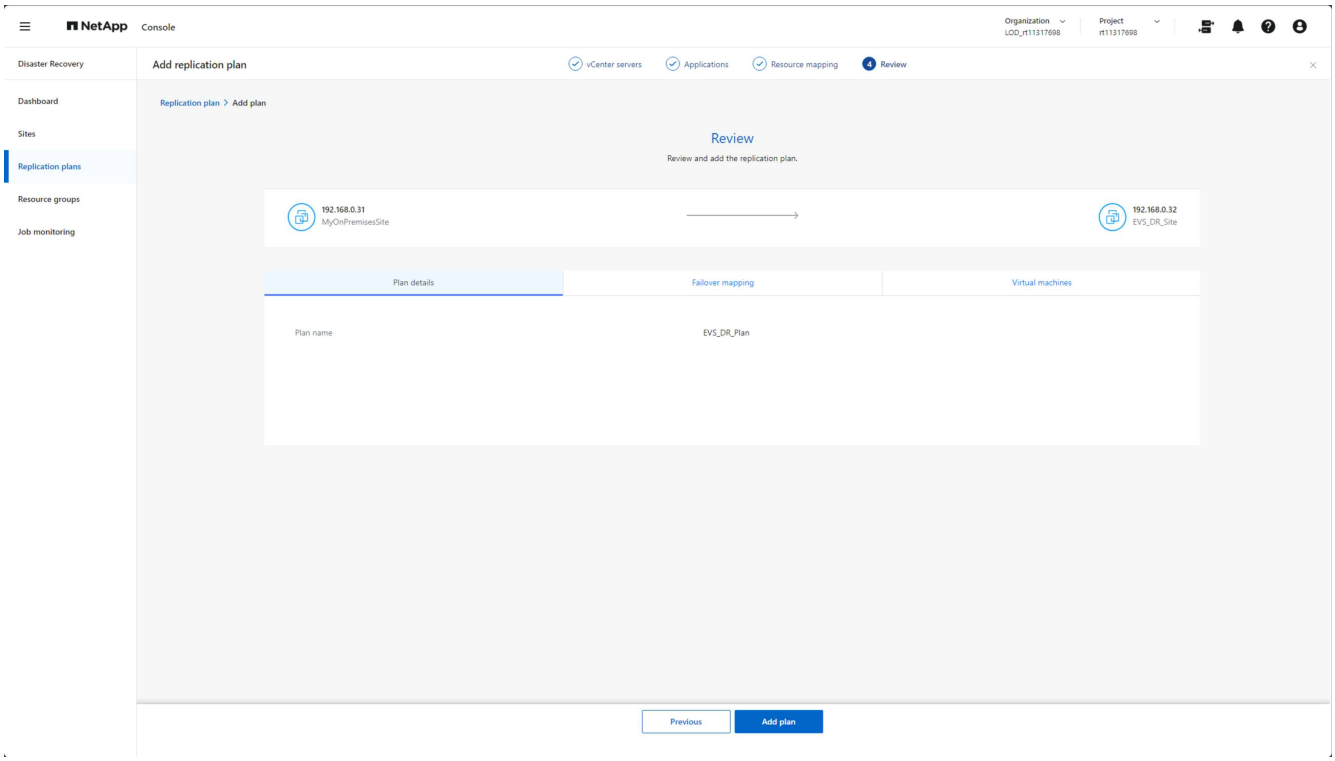
Después de agregar la información del plan de replicación en NetApp Disaster Recovery, verifique que la información ingresada sea correcta.

**Pasos**

1. Seleccione **Guardar** para revisar su configuración antes de activar el plan de replicación.

   Puede seleccionar cada pestaña para revisar la configuración y realizar cambios en cualquier pestaña seleccionando el ícono de lápiz.

   Revisión de la configuración del plan de replicación



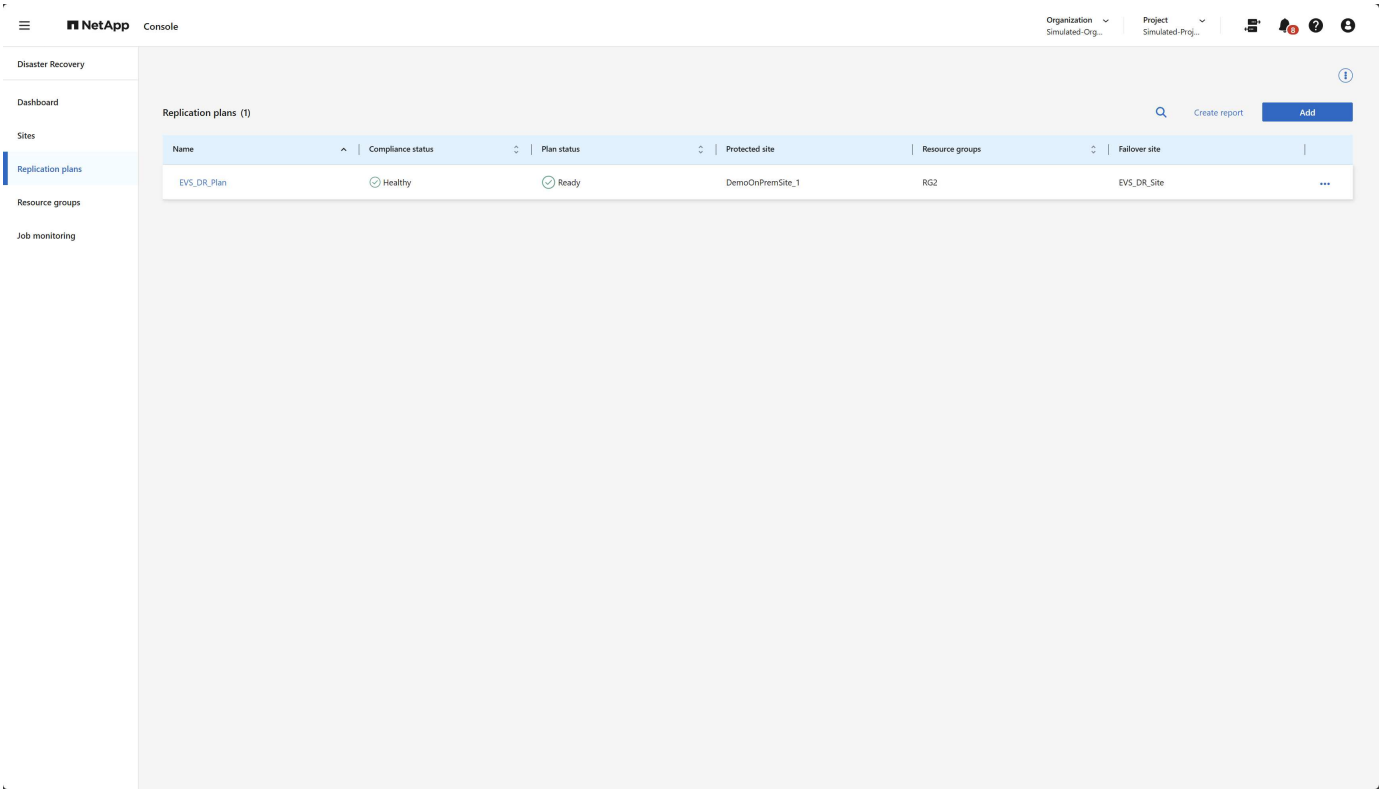

2. Cuando esté satisfecho de que todas las configuraciones sean correctas, seleccione **Agregar plan** en la parte inferior de la pantalla.

Continuar con"Verificar el plan de replicación" .

### Verifique que todo funcione en NetApp Disaster Recovery

Después de agregar el plan de replicación en NetApp Disaster Recovery, regresará a la página Planes de replicación, donde podrá ver sus planes de replicación y su estado. Debe verificar que el plan de replicación se encuentre en estado **Saludable**. Si no es así, debe verificar el estado del plan de replicación y corregir cualquier problema antes de continuar.

Figura: Página de planes de replicación




NetApp Disaster Recovery realiza una serie de pruebas para verificar que todos los componentes (clúster ONTAP , clústeres vCenter y máquinas virtuales) sean accesibles y estén en el estado adecuado para que el servicio proteja las máquinas virtuales. Esto se llama verificación de cumplimiento y se ejecuta periódicamente.

Desde la página de Planes de replicación, puede ver la siguiente información:

- Estado de la última verificación de cumplimiento
- El estado de replicación del plan de replicación
- El nombre del sitio protegido (fuente)
- La lista de grupos de recursos protegidos por el plan de replicación
- El nombre del sitio de conmutación por error (destino)

## Realice operaciones de plan de replicación con NetApp Disaster Recovery

Utilice NetApp Disaster Recovery con Amazon EVS y Amazon FSx for NetApp ONTAP para realizar las siguientes operaciones: conmutación por error, probar la conmutación por error, actualizar recursos, migrar, tomar una instantánea ahora, deshabilitar/habilitar el plan de replicación, limpiar instantáneas antiguas, conciliar instantáneas, eliminar el plan de replicación y editar programaciones.

### Conmutación por error

La operación principal que posiblemente necesite realizar es la que espera que nunca suceda: conmutar por error al centro de datos de DR (destino) en caso de una falla catastrófica en el sitio de producción local.

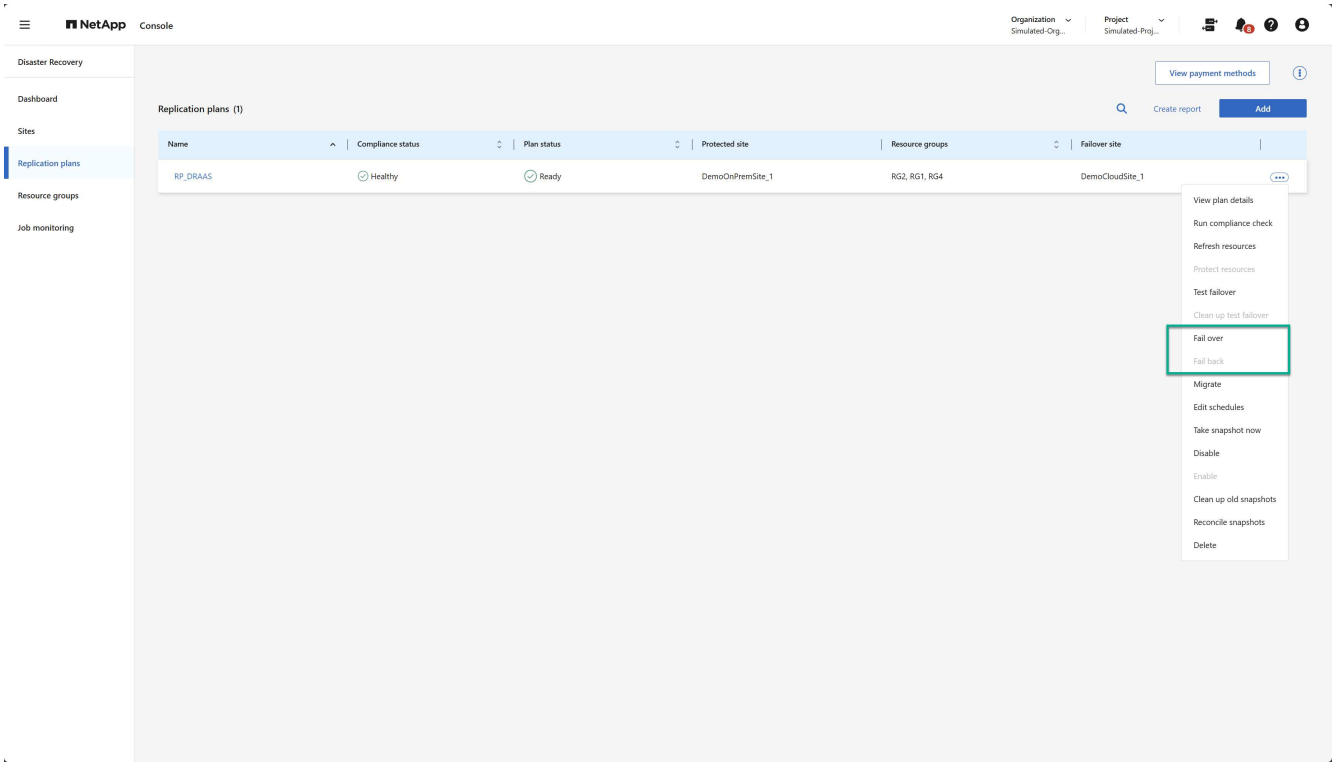
La conmutación por error es un proceso iniciado manualmente.

**Pasos para acceder a la operación de conmutación por error**

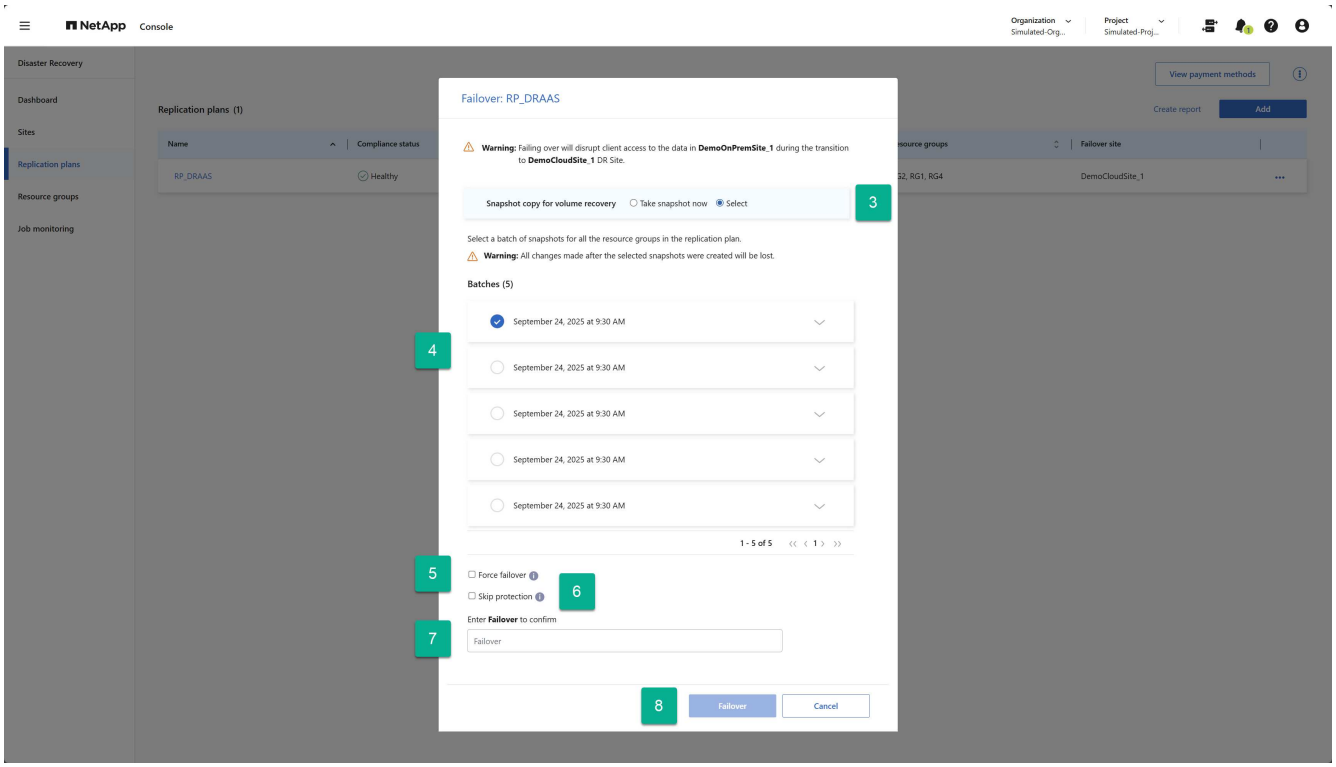
1. Desde la barra de navegación izquierda de la consola de NetApp , seleccione **Protección** > **Recuperación ante desastres**.
2. En el menú NetApp Disaster Recovery, seleccione **Planes de replicación**.

**Pasos para realizar una conmutación por error**

1. Desde la página Planes de replicación, seleccione la opción Acciones del plan de replicación ••• .
2. Seleccione **Conmutación por error**.




3. Si el sitio de producción (protegido) no es accesible, seleccione una instantánea creada previamente como su imagen de recuperación. Para ello, seleccione **Seleccionar**.
4. Seleccione la copia de seguridad que se utilizará para la recuperación.
5. (Opcional) Seleccione si desea que NetApp Disaster Recovery fuerce el proceso de conmutación por error independientemente del estado del plan de replicación. Esto sólo debe hacerse como último recurso.
6. (Opcional) Seleccione si desea que NetApp Disaster Recovery cree automáticamente una relación de protección inversa después de que se haya recuperado el sitio de producción.
7. Escriba la palabra “Failover” para verificar que desea continuar.
8. Seleccione **Conmutación por error**.




### Prueba de conmutación por error

Una conmutación por error de prueba es similar a una conmutación por error, excepto por dos diferencias.

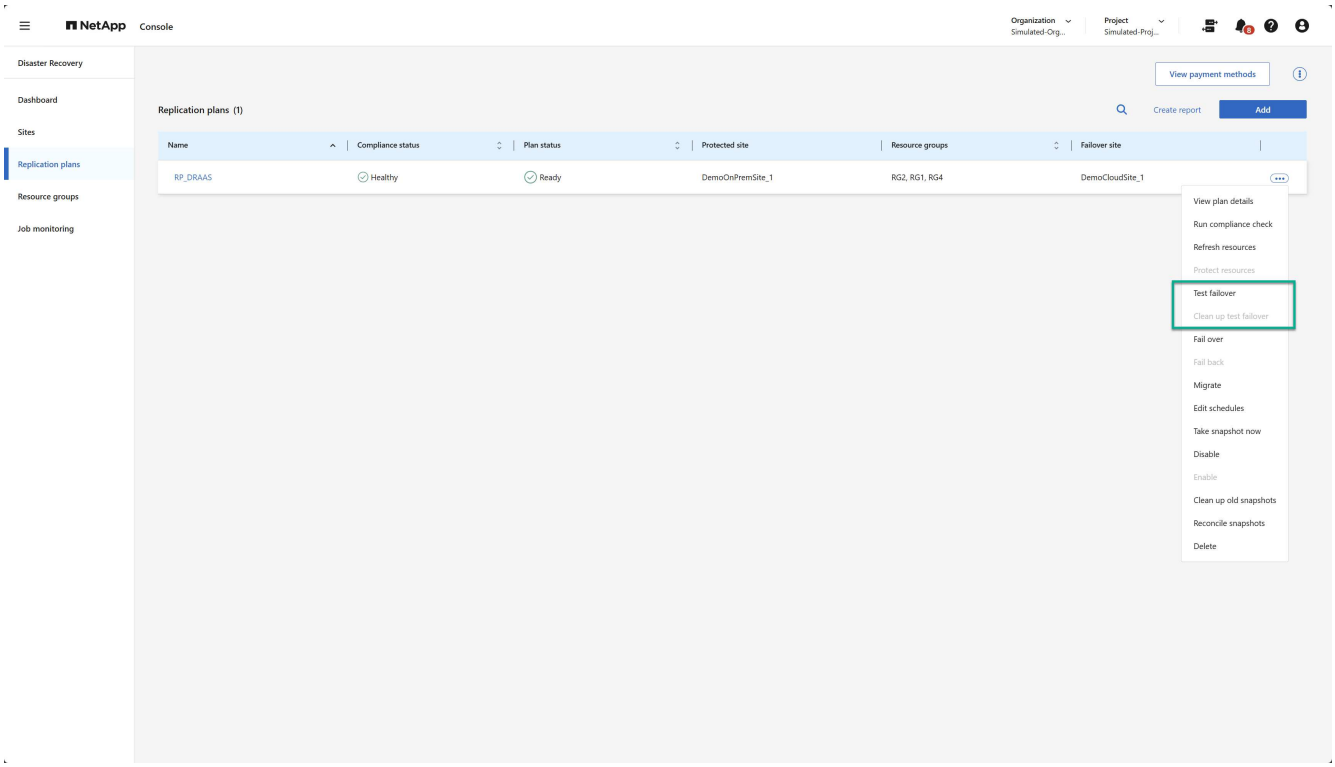
- El sitio de producción todavía está activo y todas las máquinas virtuales siguen funcionando como se esperaba.
- La protección de recuperación ante desastres de NetApp de las máquinas virtuales de producción continúa.

Esto se logra mediante el uso de volúmenes ONTAP FlexClone nativos en el sitio de destino. Para obtener más información sobre la conmutación por error de pruebas, consulte"Conmutación por error de aplicaciones a un sitio remoto | Documentación de NetApp" .

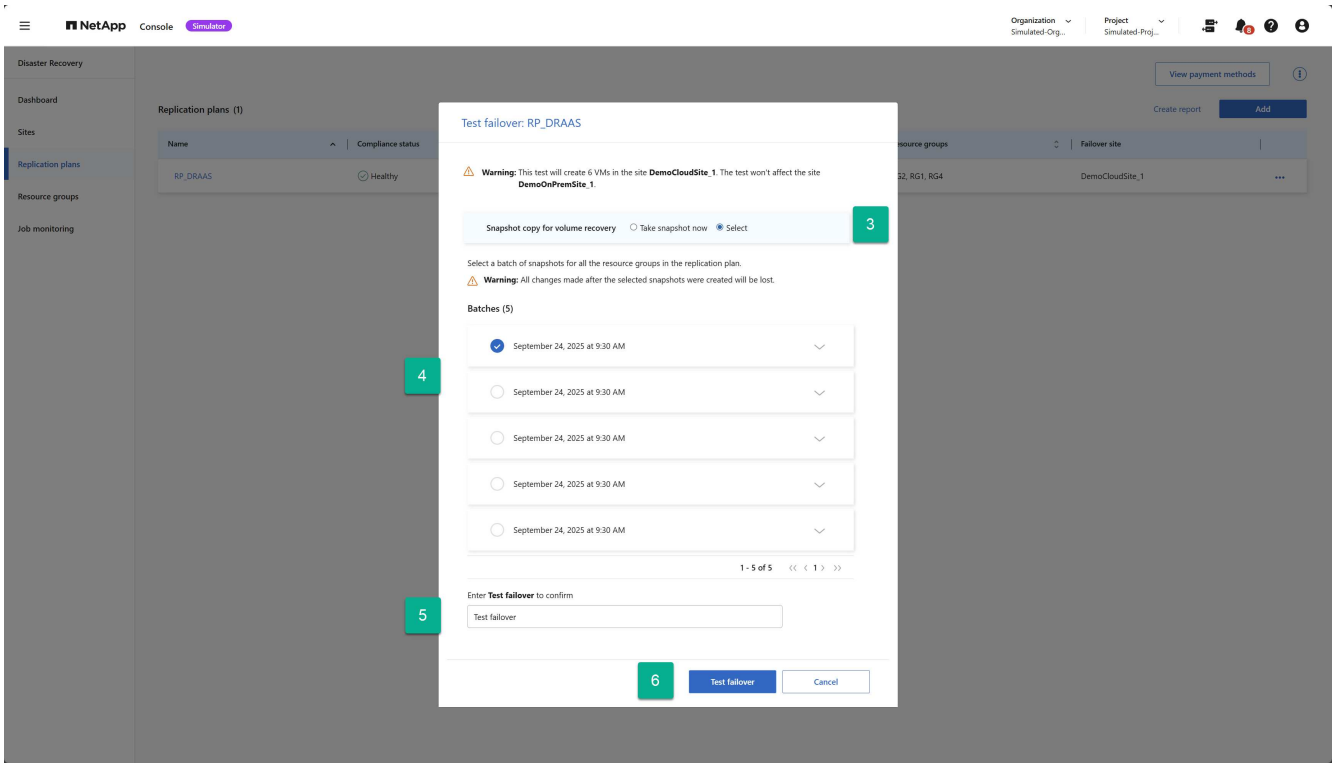
Los pasos para ejecutar una conmutación por error de prueba son idénticos a los utilizados para ejecutar una conmutación por error real, excepto que se utiliza la operación Conmutación por error de prueba en el menú contextual del plan de replicación.

#### Pasos

1. Seleccione la opción Acciones del plan de replicación ••• .
2. Seleccione **Prueba de conmutación por error** en el menú.




3. Decide si quieres obtener el último estado del entorno de producción (Tomar instantánea ahora) o utilizar una copia de seguridad del plan de replicación creada previamente (Seleccionar)
4. Si eligió una copia de seguridad creada previamente, seleccione la copia de seguridad que se utilizará para la recuperación.
5. Escriba la palabra “Prueba de conmutación por error” para verificar que desea continuar.
6. Seleccione **Prueba de conmutación por error**.

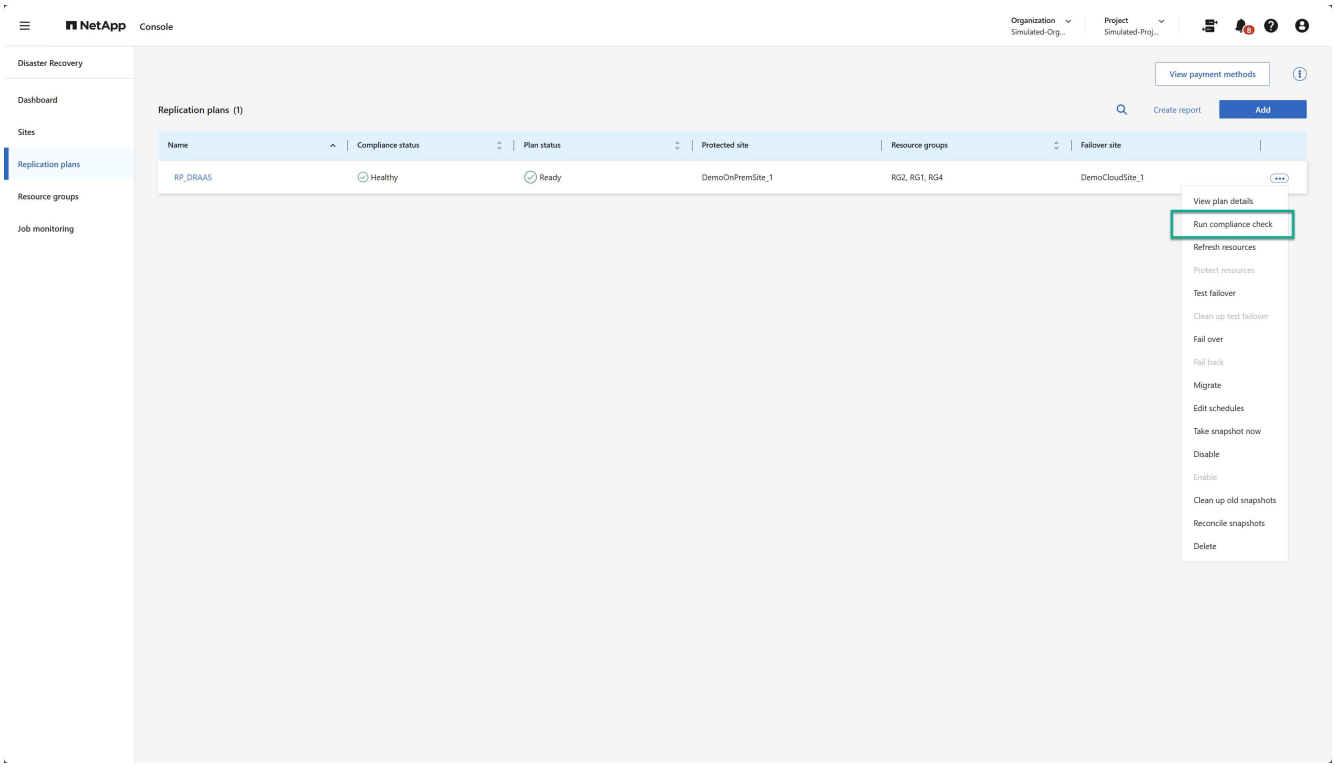


### Ejecutar una verificación de cumplimiento

Las comprobaciones de cumplimiento se ejecutan cada tres horas, de forma predeterminada. En cualquier momento, es posible que desees ejecutar manualmente una verificación de cumplimiento.

#### Pasos

1. Seleccione la opción *Acciones* ••• junto al plan de replicación.
2. Seleccione la opción **Ejecutar verificación de cumplimiento** en el menú Acciones del plan de replicación:



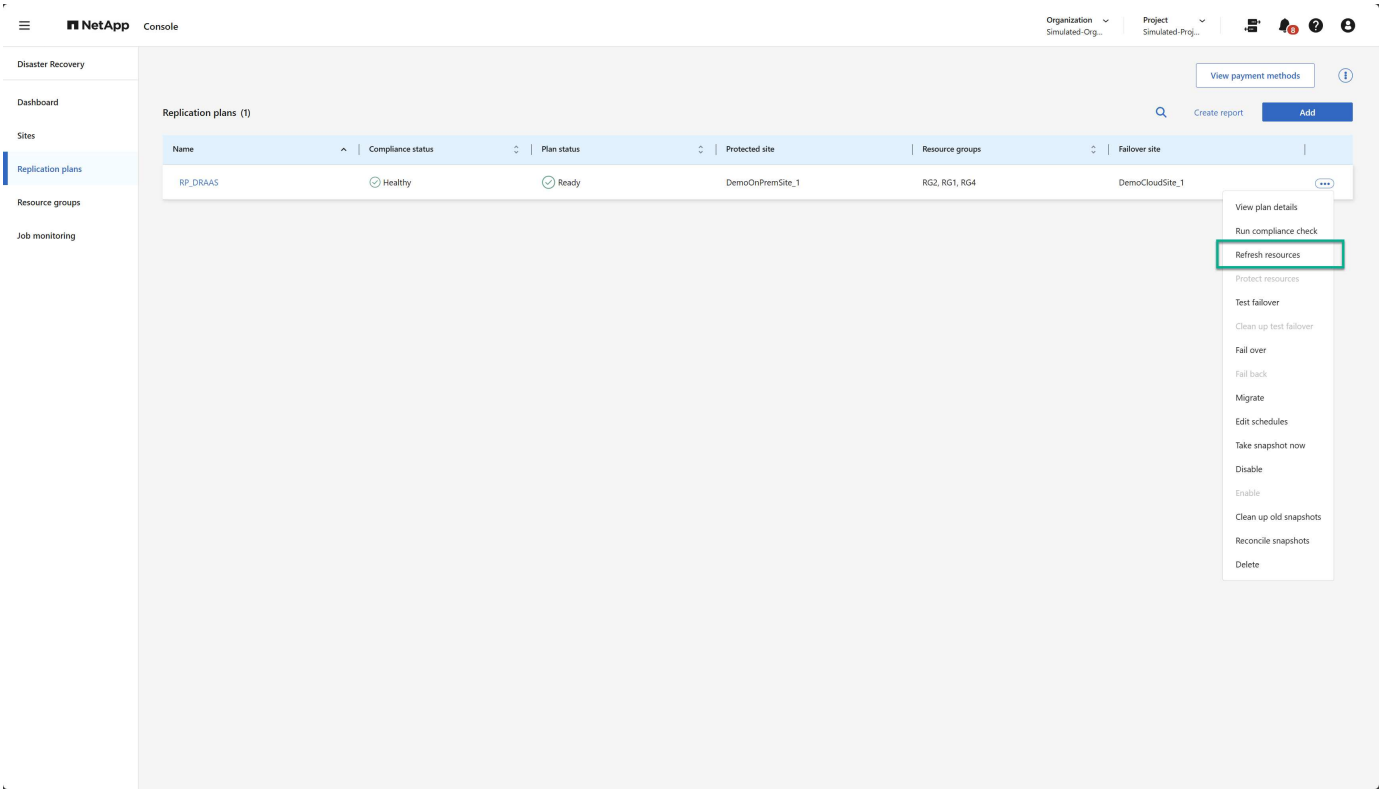

3. Para cambiar la frecuencia con la que NetApp Disaster Recovery ejecuta automáticamente comprobaciones de cumplimiento, seleccione la opción **Editar programaciones** en el menú Acciones del plan de replicación.

### Actualizar recursos

Cada vez que realice cambios en su infraestructura virtual (como agregar o eliminar máquinas virtuales, agregar o eliminar almacenes de datos o mover máquinas virtuales entre almacenes de datos), deberá realizar una actualización de los clústeres de vCenter afectados en el servicio NetApp Disaster Recovery. El servicio hace esto automáticamente una vez cada 24 horas de manera predeterminada, pero una actualización manual garantiza que la información más reciente sobre la infraestructura virtual esté disponible y se tenga en cuenta para la protección contra desastres.

Hay dos casos en los que es necesaria una actualización:

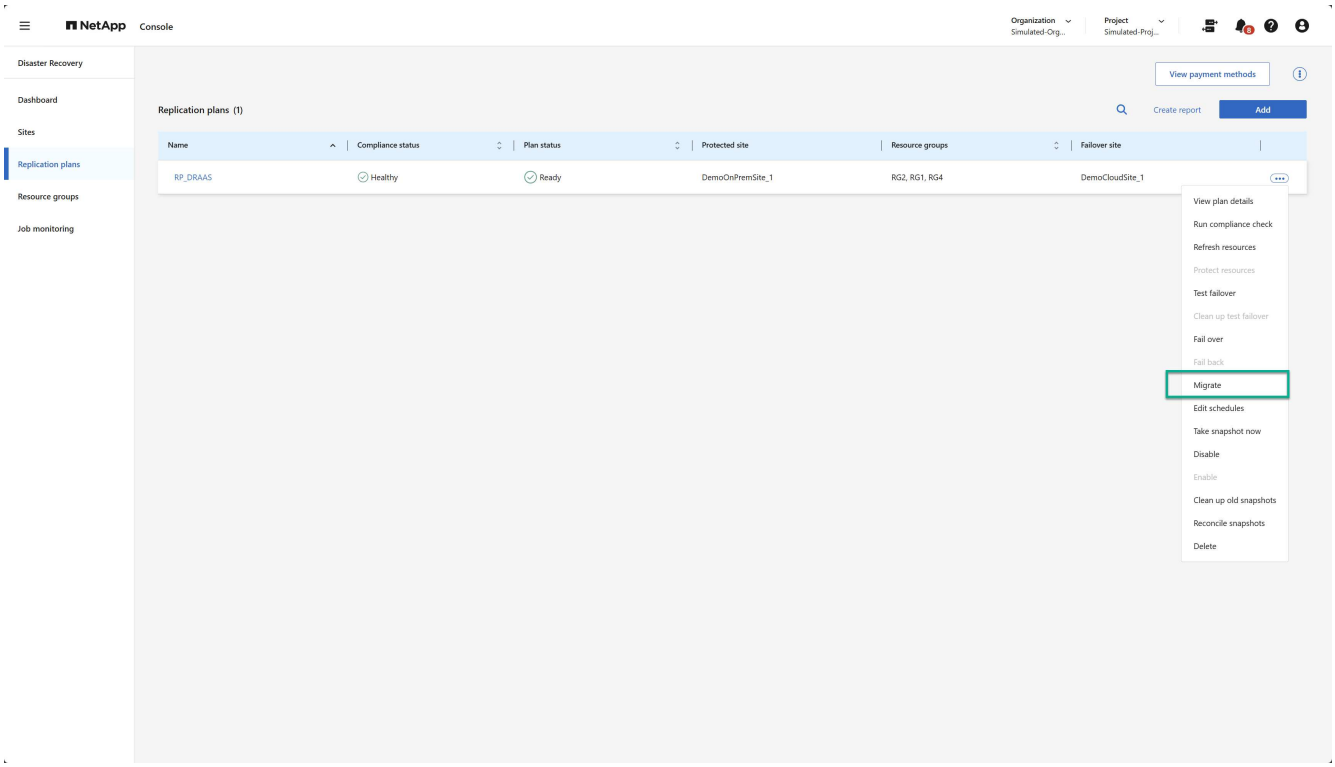
- Actualización de vCenter: realice una actualización de vCenter cada vez que se agreguen, eliminen o muevan máquinas virtuales de un clúster de vCenter:
- Actualización del plan de replicación: realice una actualización del plan de replicación cada vez que una máquina virtual se mueva entre almacenes de datos en el mismo clúster de vCenter de origen.




## Emigrar

Si bien NetApp Disaster Recovery se utiliza principalmente para casos de uso de recuperación ante desastres, también puede permitir movimientos únicos de un conjunto de máquinas virtuales desde el sitio de origen al sitio de destino. Esto podría ser para un proyecto de migración concertada a la nube o podría usarse para evitar desastres, como mal tiempo, conflictos políticos u otros posibles eventos catastróficos temporales.

1. Seleccione la opción *Acciones* ••• junto al plan de replicación.
2. Para mover las máquinas virtuales en un plan de replicación al clúster de Amazon EVS de destino, seleccione **Migrar** en el menú Acciones del plan de replicación:

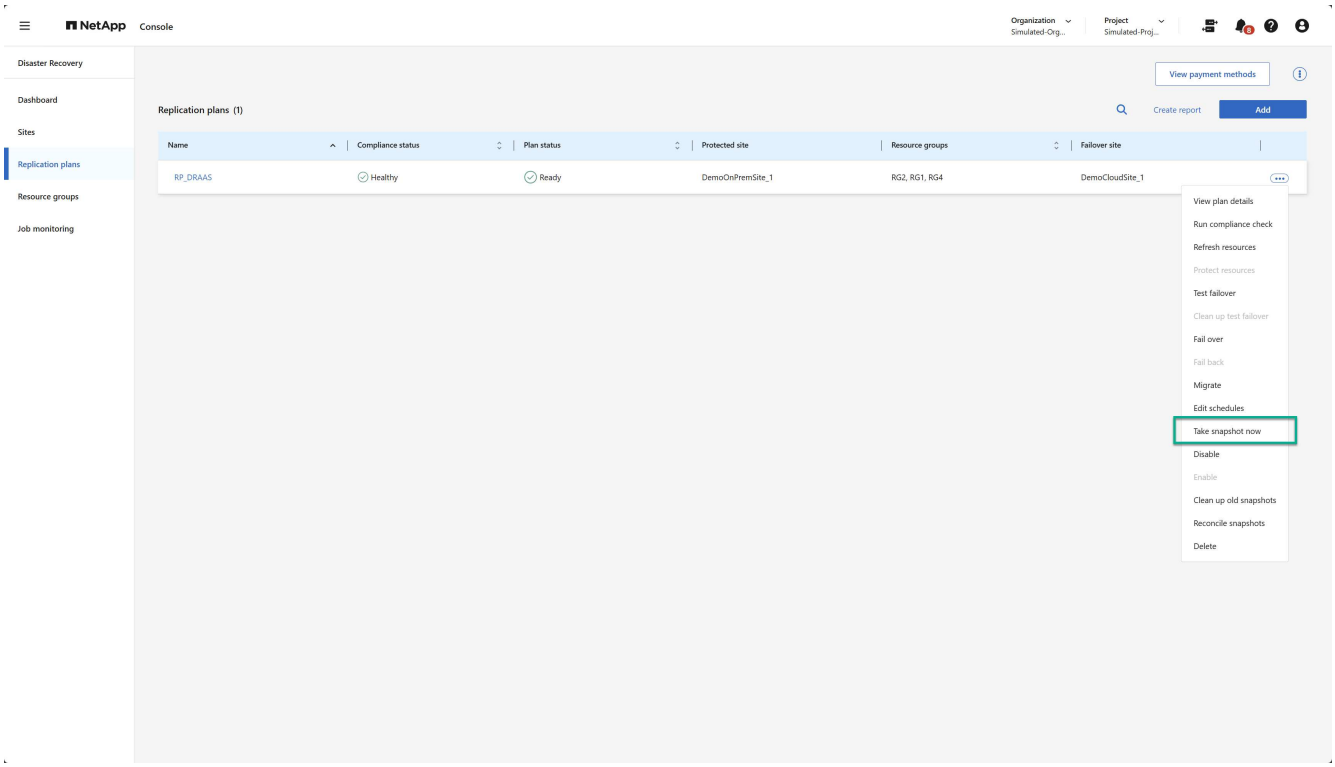



3. Introduzca información en el cuadro de diálogo Migrar.

### Toma una instantánea ahora

En cualquier momento, puede tomar una instantánea inmediata del plan de replicación. Esta instantánea está incluida en las consideraciones de recuperación ante desastres de NetApp establecidas por el recuento de retención de instantáneas del plan de replicación.

1. Seleccione la opción *Acciones* ••• junto al plan de replicación.
2. Para tomar una instantánea inmediata de los recursos del plan de replicación, seleccione **Tomar instantánea ahora** en el menú Acciones del plan de replicación:

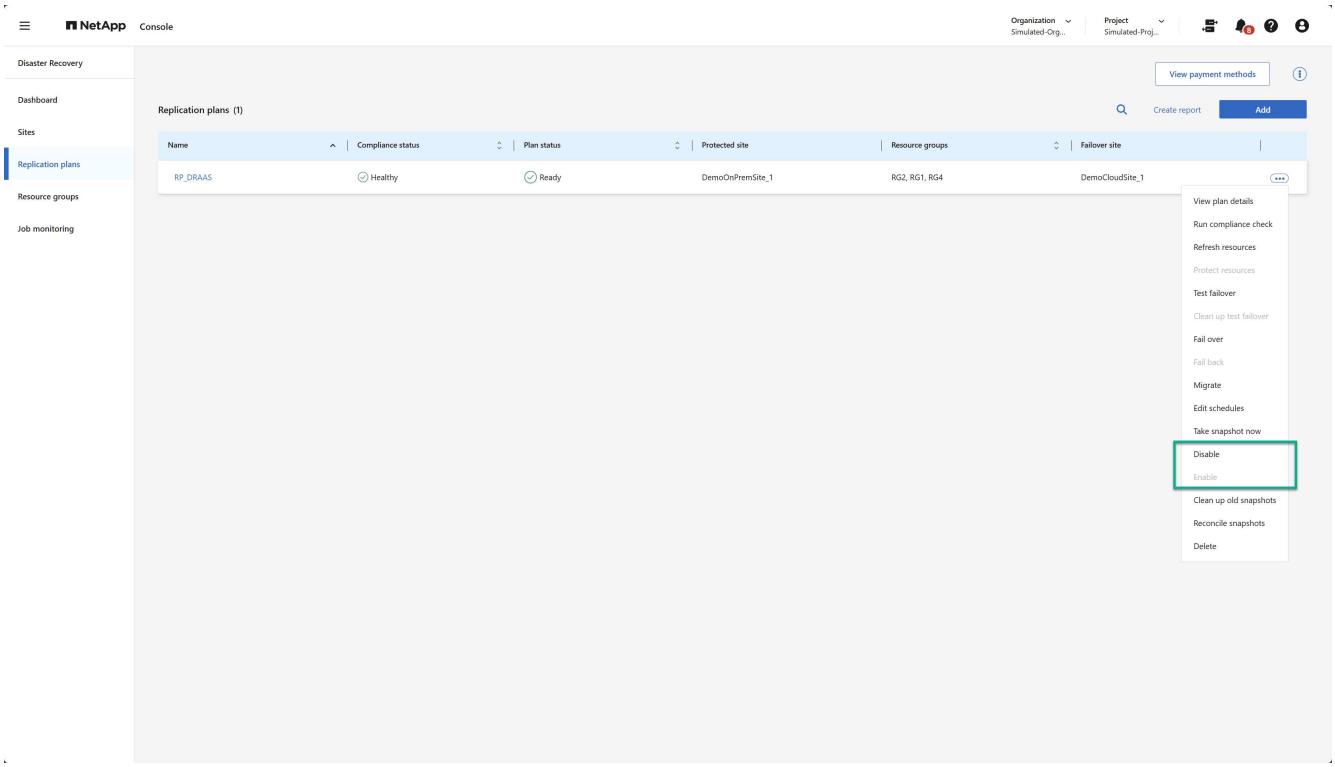



## Deshabilitar o habilitar el plan de replicación

Es posible que sea necesario detener temporalmente el plan de replicación para realizar alguna operación o mantenimiento que pueda afectar el proceso de replicación. El servicio proporciona un método para detener e iniciar la replicación.

1. Para detener temporalmente la replicación, seleccione **Deshabilitar** en el menú Acciones del plan de replicación.
2. Para reiniciar la replicación, seleccione **Habilitar** en el menú Acciones del plan de replicación.

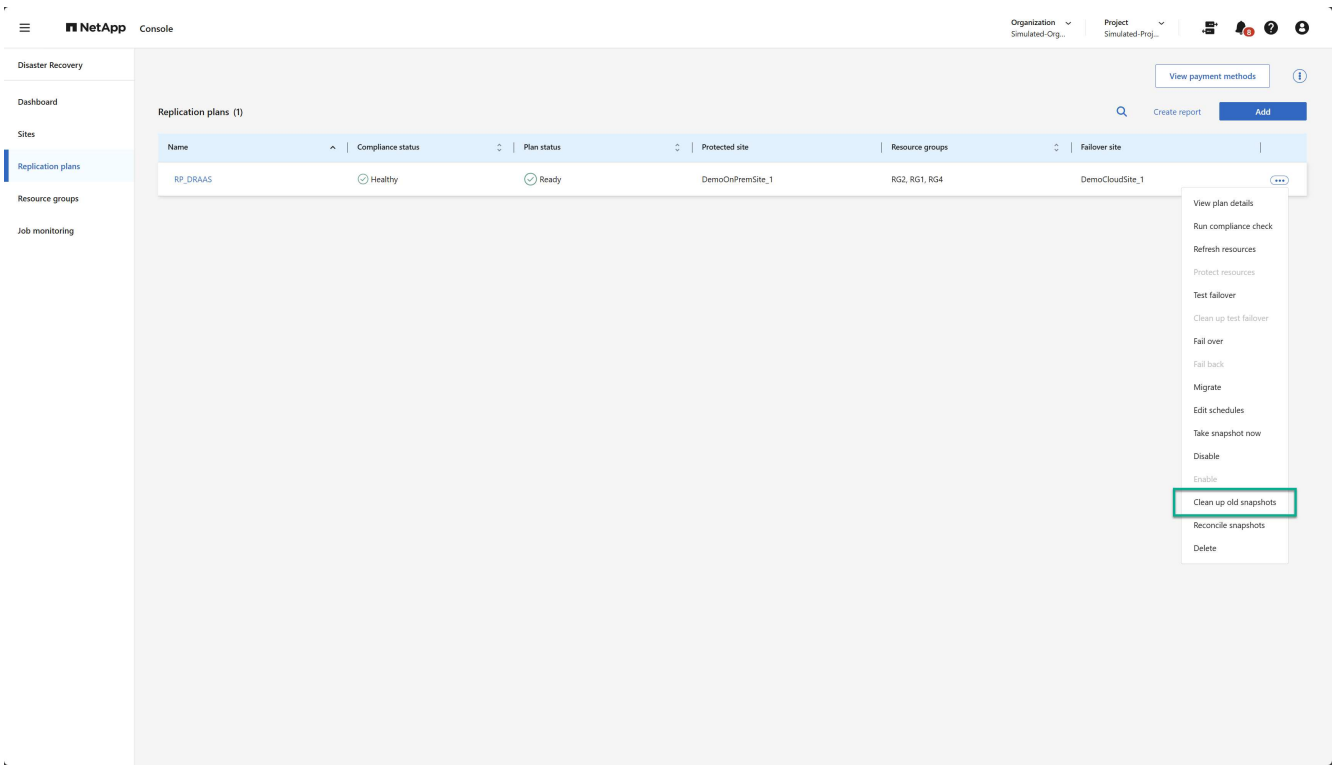
   Cuando el plan de replicación está activo, el comando **Habilitar** aparece desactivado. Cuando el plan de replicación está deshabilitado, el comando **Deshabilitar** aparece desactivado.




## Limpiar instantáneas antiguas

Es posible que desees limpiar instantáneas antiguas que se hayan conservado en los sitios de origen y destino. Esto puede suceder si se modifica el recuento de retención de instantáneas del plan de replicación.

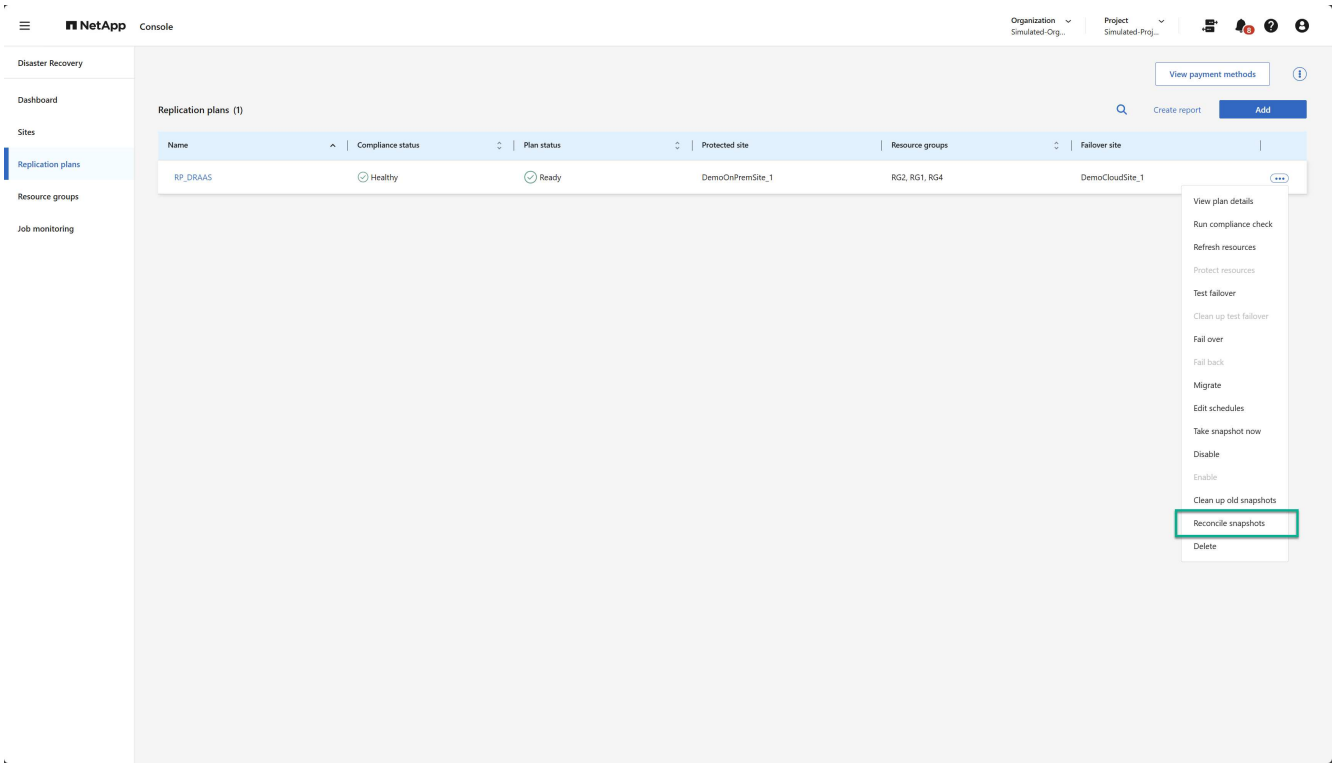
1. Seleccione la opción *Acciones* ••• junto al plan de replicación.
2. Para eliminar estas instantáneas antiguas manualmente, seleccione **Limpiar instantáneas antiguas** en el menú Acciones del plan de replicación.



### Conciliar instantáneas

Debido a que el servicio orquesta instantáneas de volumen de ONTAP , es posible que un administrador de almacenamiento de ONTAP elimine directamente instantáneas mediante el Administrador del sistema de ONTAP , la CLI de ONTAP o las API REST de ONTAP sin el conocimiento del servicio. El servicio elimina automáticamente cualquier instantánea del origen que no esté en el clúster de destino cada 24 horas. Sin embargo, puedes realizar esto bajo demanda. Esta función le permite garantizar que las instantáneas sean consistentes en todos los sitios.

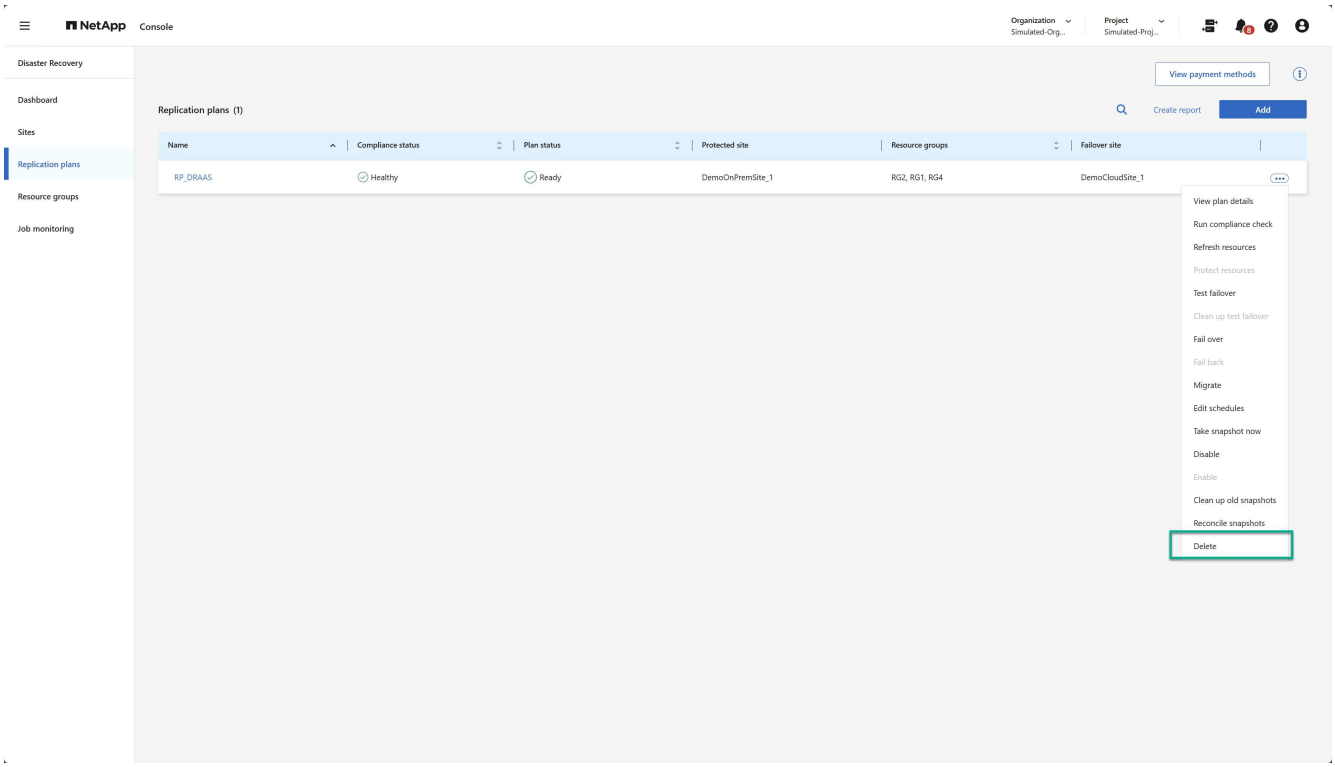
1. Seleccione la opción *Acciones* ••• junto al plan de replicación.
2. Para eliminar instantáneas del clúster de origen que no existen en el clúster de destino, seleccione **Reconciliar instantáneas** en el menú Acciones del plan de replicación.




### Eliminar plan de replicación

Si el plan de replicación ya no es necesario, puede eliminarlo.

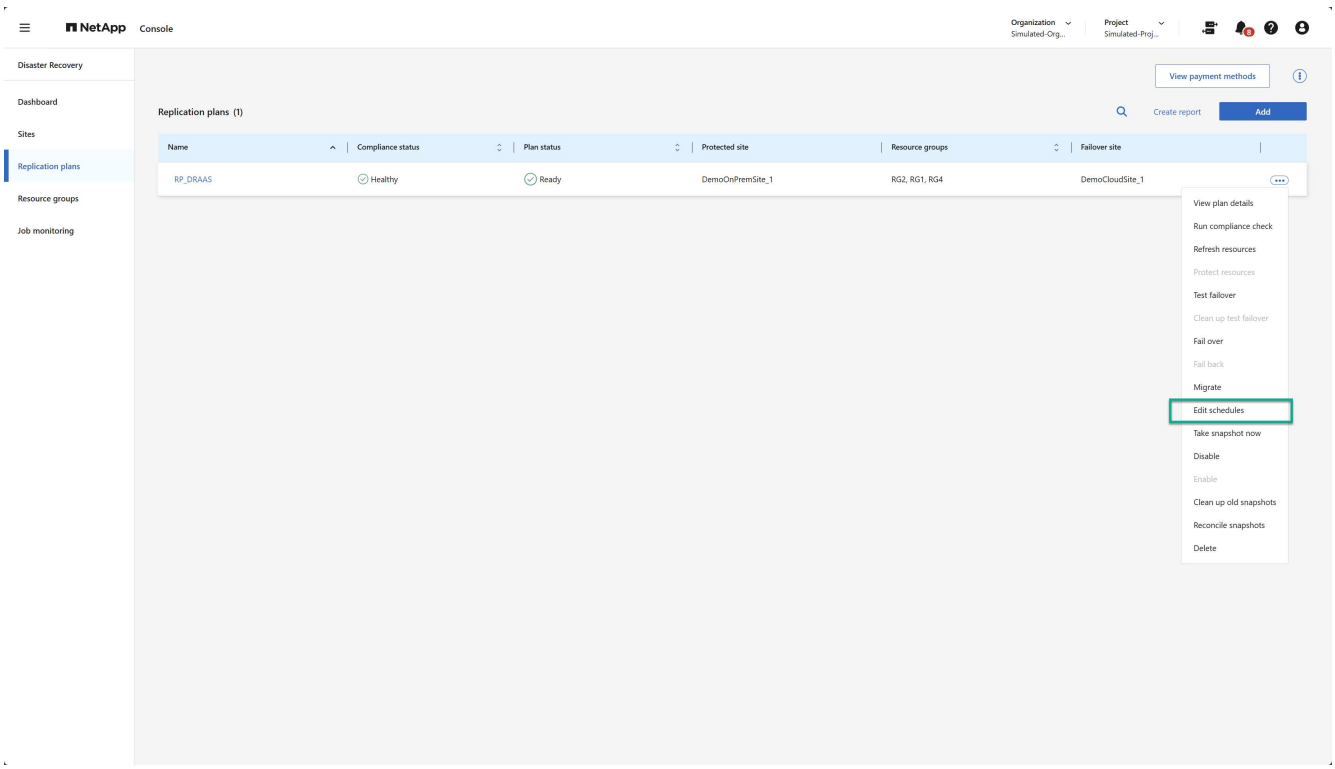
1. Seleccione la opción *Acciones* ••• junto al plan de replicación.
2. Para eliminar el plan de replicación, seleccione **Eliminar** en el menú contextual del plan de replicación.




## Editar horarios

Se realizan dos operaciones de forma automática según una programación regular: conmutaciones por error de prueba y comprobaciones de cumplimiento.

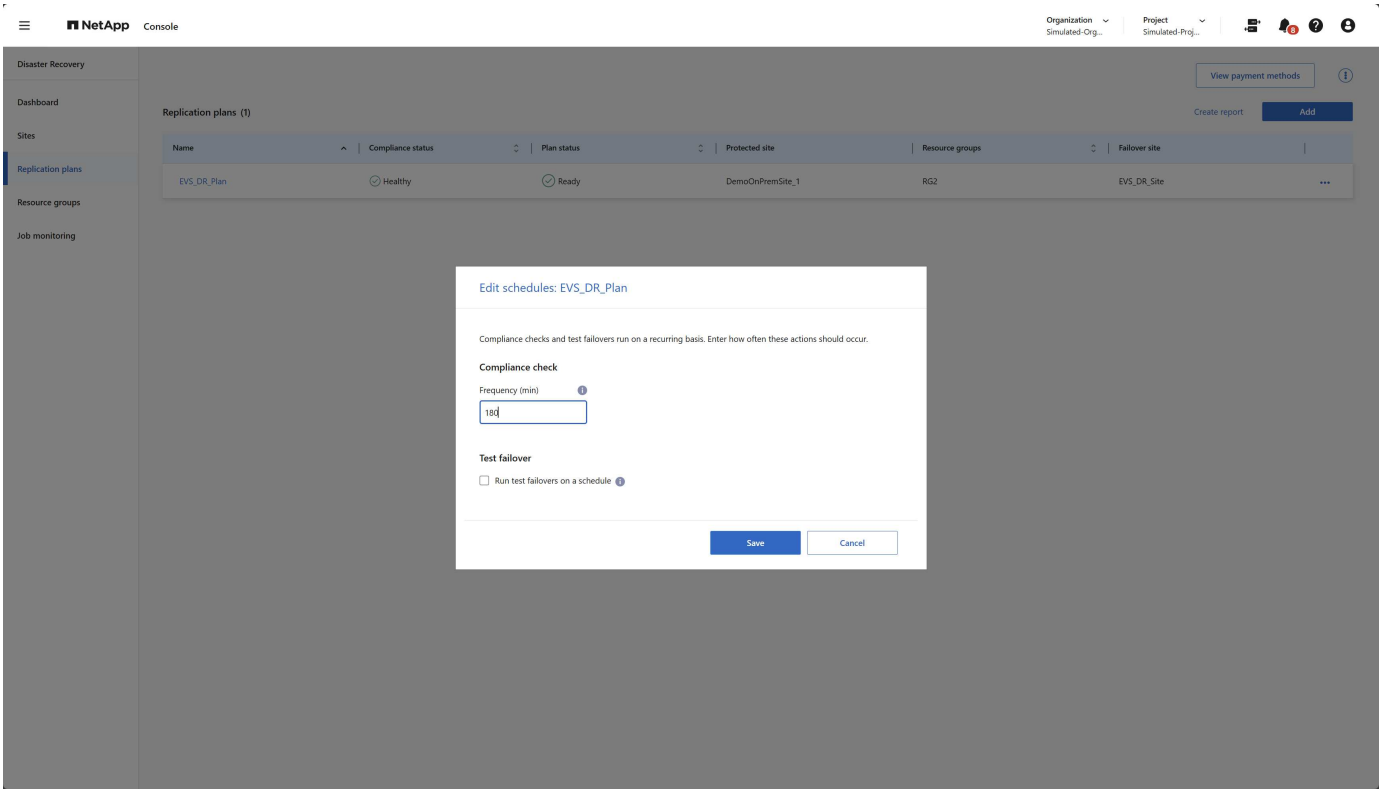
1. Seleccione la opción *Acciones* ••• junto al plan de replicación.
2. Para cambiar estos programas para cualquiera de estas dos operaciones, seleccione **Editar programas** para el plan de replicación.



### Cambiar el intervalo de verificación de cumplimiento

De forma predeterminada, las comprobaciones de cumplimiento se realizan cada tres horas. Puede cambiar esto a cualquier intervalo entre 30 minutos y 24 horas.

Para cambiar este intervalo, cambie el campo Frecuencia en el cuadro de diálogo Editar horarios:



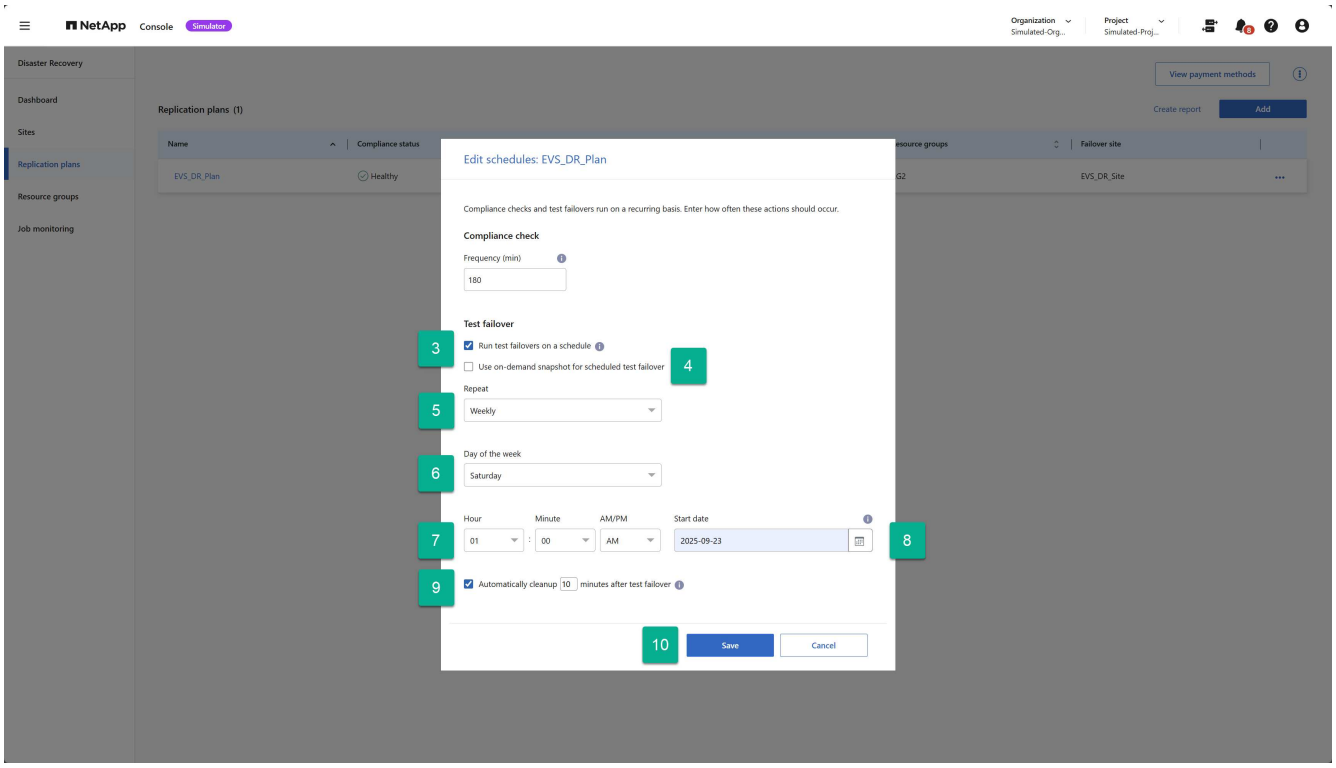

### Programar conmutaciones por error de pruebas automatizadas

Las conmutaciones por error de prueba se ejecutan manualmente de forma predeterminada. Puede programar conmutaciones por error de pruebas automáticas, lo que ayuda a garantizar que sus planes de replicación funcionen como se espera. Para obtener más información sobre el proceso de conmutación por error de prueba, consulte"Probar el proceso de conmutación por error" .

#### Pasos para programar conmutaciones por error de pruebas

1. Seleccione la opción *Acciones* ••• junto al plan de replicación.
2. Seleccione **Ejecutar conmutación por error**.
3. Marque la casilla de verificación **Ejecutar conmutaciones por error de prueba según un cronograma**.
4. (Opcional) Marque la opción **Usar instantánea a pedido para conmutación por error de prueba programada**.
5. Seleccione un tipo de intervalo en el menú desplegable Repetir.
6. Seleccione cuándo realizar la prueba de conmutación por error
   a. Semanal: seleccione el día de la semana
   b. Mensual: seleccione el día del mes
7. Elija la hora del día para ejecutar la prueba de conmutación por error
8. Elija la fecha de inicio.

9. Decida si desea que el servicio limpie automáticamente el entorno de prueba y durante cuánto tiempo desea que el entorno de prueba se ejecute antes de que comience el proceso de limpieza.
10. Seleccione **Guardar**.



# Preguntas frecuentes sobre NetApp Disaster Recovery

Estas preguntas frecuentes pueden ayudarte si simplemente buscas una respuesta rápida a una pregunta.

¿Cuál es la URL de recuperación ante desastres de NetApp ? Para la URL, en un navegador, ingrese: "https://console.netapp.com/" para acceder a la consola de NetApp .

¿Necesita una licencia para utilizar NetApp Disaster Recovery? Se requiere una licencia de NetApp Disaster Recovery para obtener acceso completo. Sin embargo, puedes probarlo con la versión de prueba gratuita.

Para obtener detalles sobre la configuración de licencias para NetApp Disaster Recovery, consulte"Configurar la licencia de NetApp Disaster Recovery" .

¿Cómo acceder a NetApp Disaster Recovery? NetApp Disaster Recovery no requiere ninguna habilitación. La opción de recuperación ante desastres aparece automáticamente en la navegación izquierda de la consola NetApp .

# Conocimiento y apoyo

## Regístrese para recibir asistencia

Es necesario registrarse para recibir soporte técnico específico para BlueXP y sus soluciones y servicios de almacenamiento. También es necesario registrarse para obtener soporte técnico para habilitar flujos de trabajo clave para los sistemas Cloud Volumes ONTAP .

Registrarse para recibir soporte no habilita el soporte de NetApp para un servicio de archivos de un proveedor de nube. Para obtener asistencia técnica relacionada con un servicio de archivos de un proveedor de nube, su infraestructura o cualquier solución que utilice el servicio, consulte "Obtener ayuda" en la documentación de BlueXP para ese producto.

- "Amazon FSx para ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

### Descripción general del registro de soporte

Existen dos formas de registro para activar el derecho a recibir ayuda:

- Registrar el número de serie de su cuenta BlueXP (su número de serie 960xxxxxxxx de 20 dígitos ubicado en la página de Recursos de soporte en BlueXP).

  Esto sirve como su ID de suscripción de soporte único para cualquier servicio dentro de BlueXP. Cada suscripción de soporte a nivel de cuenta de BlueXP debe estar registrada.

- Registrar los números de serie de Cloud Volumes ONTAP asociados con una suscripción en el mercado de su proveedor de nube (son números de serie 909201xxxxxxxx de 20 dígitos).

  Estos números de serie se conocen comúnmente como *números de serie PAYGO* y son generados por BlueXP en el momento de la implementación de Cloud Volumes ONTAP .

El registro de ambos tipos de números de serie permite funciones como la apertura de tickets de soporte y la generación automática de casos. El registro se completa agregando cuentas del sitio de soporte de NetApp (NSS) a BlueXP como se describe a continuación.

### Registre BlueXP para obtener soporte de NetApp

Para registrarse para recibir soporte y activar el derecho a soporte, un usuario de su organización (o cuenta) de BlueXP debe asociar una cuenta del sitio de soporte de NetApp con su inicio de sesión de BlueXP . La forma de registrarse para el soporte de NetApp depende de si ya tiene una cuenta del sitio de soporte de NetApp (NSS).

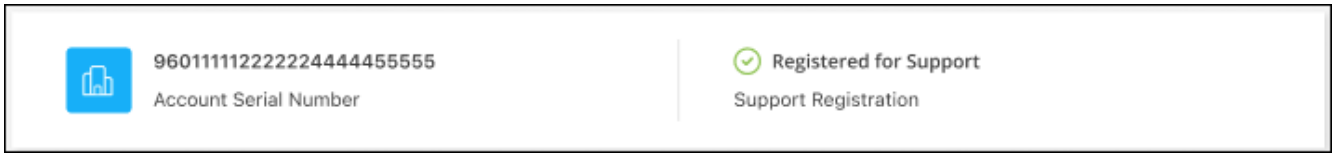
#### Cliente existente con una cuenta NSS

Si es cliente de NetApp con una cuenta NSS, simplemente necesita registrarse para recibir soporte a través de BlueXP.

#### Pasos

1. En la parte superior derecha de la consola BlueXP , seleccione el ícono Configuración y seleccione **Credenciales**.
2. Seleccione **Credenciales de usuario**.
3. Seleccione **Agregar credenciales NSS** y siga las instrucciones de autenticación del sitio de soporte de NetApp (NSS).
4. Para confirmar que el proceso de registro fue exitoso, seleccione el ícono de Ayuda y seleccione **Soporte**.

   La página **Recursos** debería mostrar que su organización BlueXP está registrada para recibir soporte.




   Tenga en cuenta que otros usuarios de BlueXP no verán este mismo estado de registro de soporte si no han asociado una cuenta del sitio de soporte de NetApp con su inicio de sesión de BlueXP . Sin embargo, eso no significa que su organización BlueXP no esté registrada para recibir soporte. Siempre que un usuario de la organización haya seguido estos pasos, su organización quedará registrada.

### Soy cliente actual pero no tengo cuenta NSS

Si es un cliente existente de NetApp con licencias y números de serie existentes pero *no* una cuenta NSS, debe crear una cuenta NSS y asociarla con su inicio de sesión de BlueXP .

**Pasos**

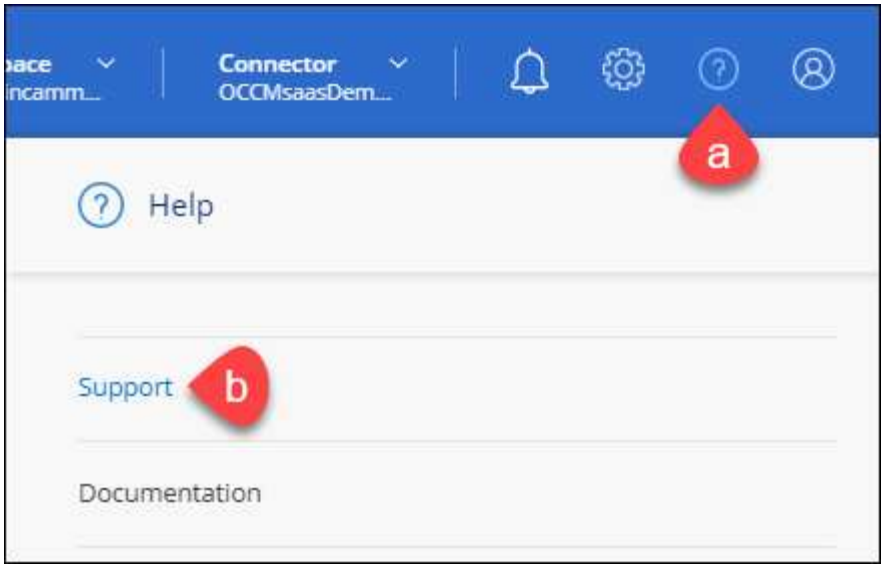
1. Cree una cuenta en el sitio de soporte de NetApp completando el "Formulario de registro de usuario del sitio de soporte de NetApp"
   a. Asegúrese de seleccionar el nivel de usuario apropiado, que normalmente es **Cliente de NetApp /Usuario final**.
   b. Asegúrese de copiar el número de serie de la cuenta BlueXP (960xxxx) utilizado anteriormente para el campo de número de serie. Esto acelerará el procesamiento de la cuenta.
2. Asocie su nueva cuenta NSS con su inicio de sesión de BlueXP completando los pasos a continuaciónCliente existente con una cuenta NSS .

### Completamente nuevo en NetApp

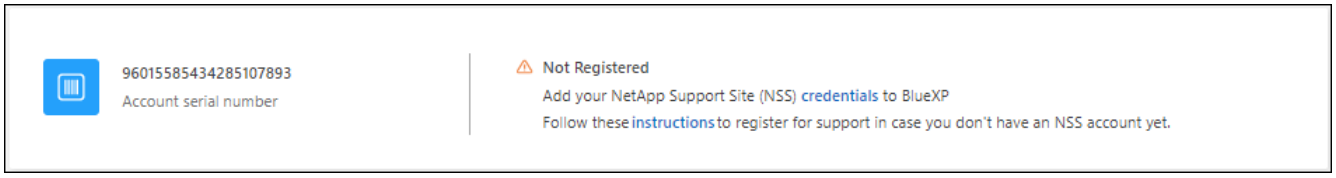
Si es nuevo en NetApp y no tiene una cuenta NSS, siga cada paso a continuación.

**Pasos**

1. En la parte superior derecha de la consola BlueXP , seleccione el ícono Ayuda y seleccione **Soporte**.




2. Localice el número de serie de su ID de cuenta en la página de Registro de soporte.




3. Navegar a "Sitio de registro de soporte de NetApp" y seleccione *No soy un cliente registrado de NetApp *.
4. Llene los campos obligatorios (aquellos con asteriscos rojos).
5. En el campo **Línea de productos**, seleccione **Administrador de nube** y luego seleccione su proveedor de facturación correspondiente.
6. Copie el número de serie de su cuenta del paso 2 anterior, complete la verificación de seguridad y luego confirme que leyó la Política de privacidad de datos global de NetApp.

   Se envía inmediatamente un correo electrónico al buzón proporcionado para finalizar esta transacción segura. Asegúrese de revisar sus carpetas de correo no deseado si el correo electrónico de validación no llega en unos minutos.

7. Confirme la acción desde el correo electrónico.

   Al confirmar, se envía su solicitud a NetApp y se recomienda que cree una cuenta en el sitio de soporte de NetApp .

8. Cree una cuenta en el sitio de soporte de NetApp completando el "Formulario de registro de usuario del sitio de soporte de NetApp"
   a. Asegúrese de seleccionar el nivel de usuario apropiado, que normalmente es **Cliente de NetApp /Usuario final**.
   b. Asegúrese de copiar el número de serie de la cuenta (960xxxx) utilizado anteriormente para el campo de número de serie. Esto acelerará el procesamiento.

**Después de terminar**

NetApp debería comunicarse con usted durante este proceso. Este es un ejercicio de incorporación único para nuevos usuarios.

Una vez que tenga su cuenta del sitio de soporte de NetApp , asocie la cuenta con su inicio de sesión de BlueXP completando los pasos a continuación.Cliente existente con una cuenta NSS .

## Asociar credenciales NSS para la compatibilidad con Cloud Volumes ONTAP

Es necesario asociar las credenciales del sitio de soporte de NetApp con su organización BlueXP para habilitar los siguientes flujos de trabajo clave para Cloud Volumes ONTAP:

- Registro de sistemas Cloud Volumes ONTAP de pago por uso para obtener soporte

  Es necesario proporcionar su cuenta NSS para activar el soporte para su sistema y obtener acceso a los recursos de soporte técnico de NetApp .

- Implementación de Cloud Volumes ONTAP cuando trae su propia licencia (BYOL)

  Es necesario proporcionar su cuenta NSS para que BlueXP pueda cargar su clave de licencia y habilitar la suscripción por el período que compró. Esto incluye actualizaciones automáticas para renovaciones de plazos.

- Actualización del software Cloud Volumes ONTAP a la última versión

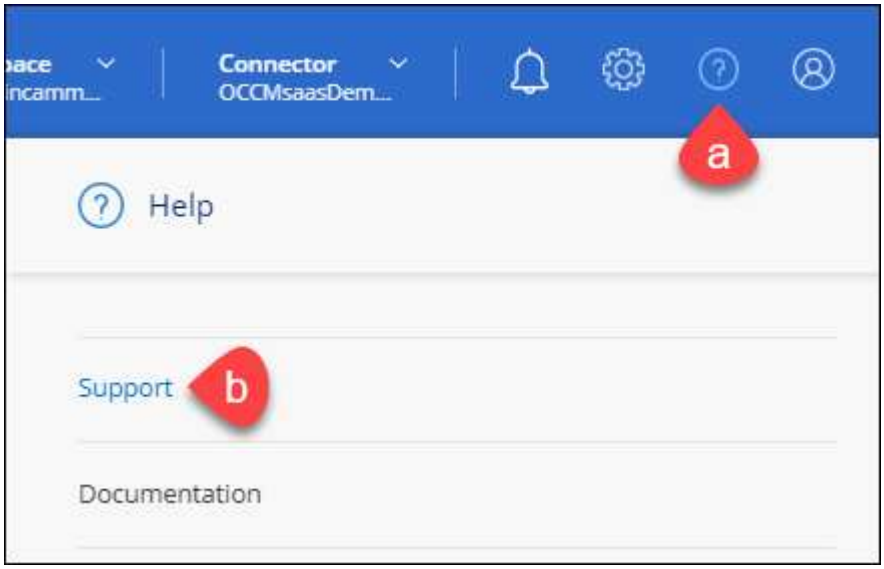
La asociación de credenciales NSS con su organización BlueXP es diferente a la asociación de una cuenta NSS con un inicio de sesión de usuario de BlueXP .

Estas credenciales NSS están asociadas con su ID de organización BlueXP específica. Los usuarios que pertenecen a la organización BlueXP pueden acceder a estas credenciales desde **Soporte > Administración de NSS**.

- Si tiene una cuenta de nivel de cliente, puede agregar una o más cuentas NSS.
- Si tiene una cuenta de socio o revendedor, puede agregar una o más cuentas NSS, pero no se pueden agregar junto con cuentas de nivel de cliente.

**Pasos**

1. En la parte superior derecha de la consola BlueXP , seleccione el ícono Ayuda y seleccione **Soporte**.




2. Seleccione **Administración de NSS > Agregar cuenta NSS**.

3. Cuando se le solicite, seleccione **Continuar** para ser redirigido a una página de inicio de sesión de Microsoft.

   NetApp utiliza Microsoft Entra ID como proveedor de identidad para servicios de autenticación específicos de soporte y licencias.

4. En la página de inicio de sesión, proporcione su dirección de correo electrónico y contraseña registradas en el sitio de soporte de NetApp para realizar el proceso de autenticación.

   Estas acciones permiten que BlueXP utilice su cuenta NSS para cosas como descargas de licencias, verificación de actualizaciones de software y futuros registros de soporte.

   Tenga en cuenta lo siguiente:

   - La cuenta NSS debe ser una cuenta de nivel de cliente (no una cuenta de invitado o temporal). Puede tener varias cuentas NSS a nivel de cliente.
   - Solo puede haber una cuenta NSS si esa cuenta es una cuenta de nivel de socio. Si intenta agregar cuentas NSS de nivel de cliente y existe una cuenta de nivel de socio, recibirá el siguiente mensaje de error:

     "El tipo de cliente NSS no está permitido para esta cuenta porque ya hay usuarios NSS de otro tipo".

   Lo mismo ocurre si tiene cuentas NSS de nivel de cliente preexistentes e intenta agregar una cuenta de nivel de socio.

   - Tras iniciar sesión correctamente, NetApp almacenará el nombre de usuario NSS.

     Esta es una identificación generada por el sistema que se asigna a su correo electrónico. En la página **Administración de NSS**, puede mostrar su correo electrónico desde el ••• menú.

   - Si alguna vez necesita actualizar sus tokens de credenciales de inicio de sesión, también hay una opción **Actualizar credenciales** en el ••• menú.

     Al utilizar esta opción se le solicitará que inicie sesión nuevamente. Tenga en cuenta que el token de estas cuentas caduca después de 90 días. Se publicará una notificación para avisarle de esto.

# Obtener ayuda

NetApp ofrece soporte para BlueXP y sus servicios en la nube de diversas maneras. Disponemos de amplias opciones de autoasistencia gratuitas las 24 horas, los 7 días de la semana, como artículos de la base de conocimientos (KB) y un foro comunitario. Su registro de soporte incluye soporte técnico remoto mediante tickets web.

## Obtenga soporte para un servicio de archivos de un proveedor de nube

Para obtener asistencia técnica relacionada con un servicio de archivos de un proveedor de nube, su infraestructura o cualquier solución que utilice el servicio, consulte "Obtener ayuda" en la documentación de BlueXP para ese producto.

- "Amazon FSx para ONTAP"
- "Azure NetApp Files"

- "Google Cloud NetApp Volumes"

Para recibir soporte técnico específico para BlueXP y sus soluciones y servicios de almacenamiento, utilice las opciones de soporte que se describen a continuación.

## Utilice opciones de autosuficiencia

Estas opciones están disponibles de forma gratuita, las 24 horas del día, los 7 días de la semana:

- Documentación

  La documentación de BlueXP que estás viendo actualmente.

- "Base de conocimientos"

  Busque en la base de conocimientos de BlueXP para encontrar artículos útiles para solucionar problemas.

- "Comunidades"

  Únase a la comunidad BlueXP para seguir las discusiones en curso o crear otras nuevas.

## Cree un caso con el soporte de NetApp

Además de las opciones de autosoporte anteriores, puede trabajar con un especialista de soporte de NetApp para resolver cualquier problema después de activar el soporte.

**Antes de empezar**

- Para utilizar la función **Crear un caso**, primero debe asociar sus credenciales del sitio de soporte de NetApp con su inicio de sesión de BlueXP . "Aprenda a administrar las credenciales asociadas con su inicio de sesión de BlueXP" .
- Si está abriendo un caso para un sistema ONTAP que tiene un número de serie, entonces su cuenta NSS debe estar asociada con el número de serie de ese sistema.

**Pasos**

1. En BlueXP, seleccione **Ayuda > Soporte**.
2. En la página **Recursos**, elija una de las opciones disponibles en Soporte técnico:

   a. Seleccione **Llámenos** si desea hablar con alguien por teléfono. Serás dirigido a una página en netapp.com que enumera los números de teléfono a los que puedes llamar.

   b. Seleccione **Crear un caso** para abrir un ticket con un especialista de soporte de NetApp :

      - **Servicio**: Seleccione el servicio con el que está asociado el problema. Por ejemplo, BlueXP cuando es específico para un problema de soporte técnico con flujos de trabajo o funcionalidad dentro del servicio.
      - **Entorno de trabajo**: si corresponde al almacenamiento, seleccione * Cloud Volumes ONTAP* o **On-Prem** y luego el entorno de trabajo asociado.

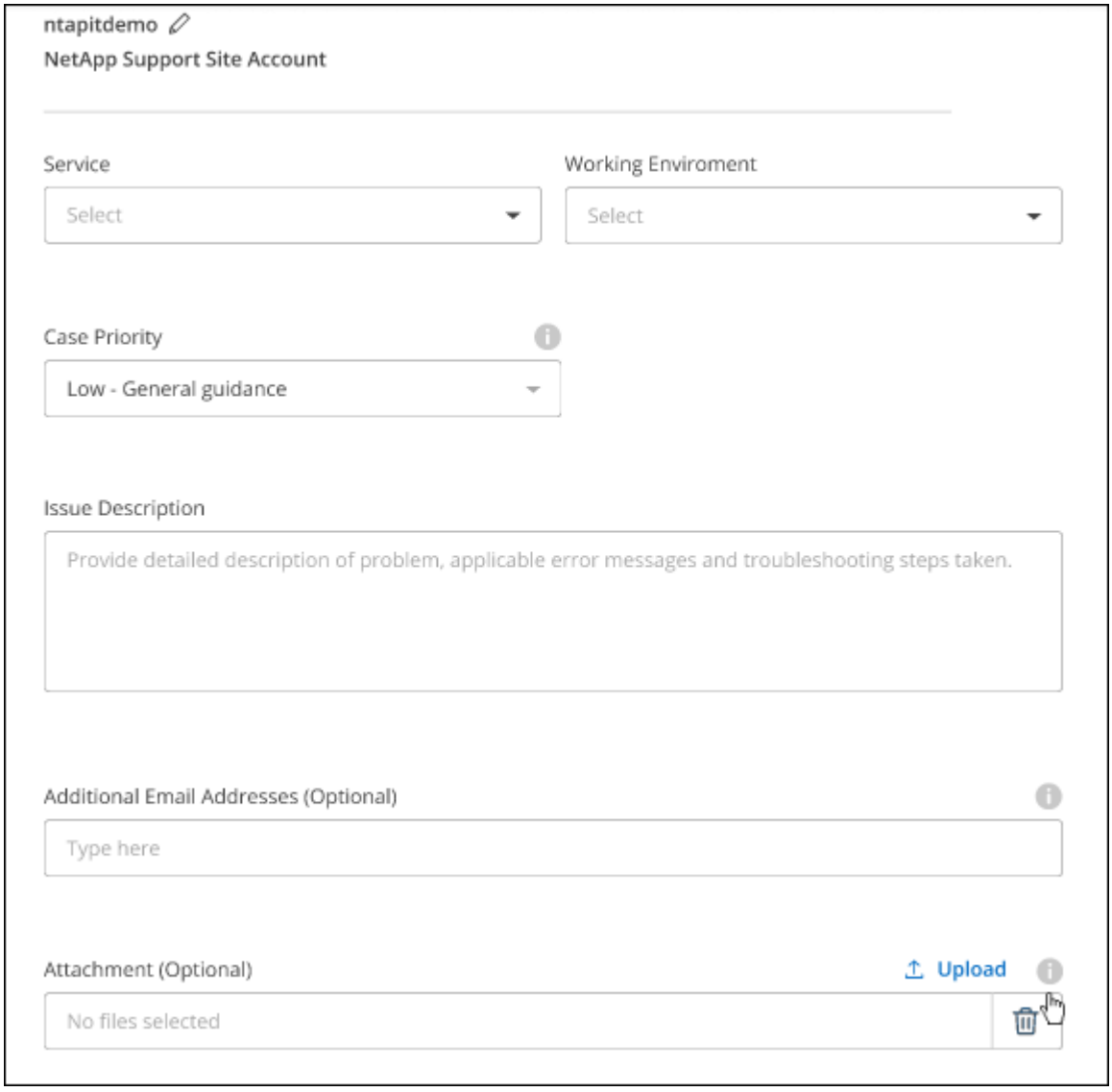
        La lista de entornos de trabajo está dentro del alcance de la organización (o cuenta), el proyecto (o espacio de trabajo) y el conector de BlueXP que haya seleccionado en el banner superior del servicio.

      - **Prioridad del caso**: elija la prioridad del caso, que puede ser Baja, Media, Alta o Crítica.

Para obtener más detalles sobre estas prioridades, pase el mouse sobre el ícono de información junto al nombre del campo.

- **Descripción del problema**: proporcione una descripción detallada de su problema, incluidos los mensajes de error aplicables o los pasos de solución de problemas que realizó.
- **Direcciones de correo electrónico adicionales**: Ingrese direcciones de correo electrónico adicionales si desea informar a otra persona sobre este problema.
- **Adjunto (opcional)**: cargue hasta cinco archivos adjuntos, uno a la vez.

  Los archivos adjuntos están limitados a 25 MB por archivo. Se admiten las siguientes extensiones de archivo: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx y csv.




**Después de terminar**

Aparecerá una ventana emergente con su número de caso de soporte. Un especialista de soporte de NetApp revisará su caso y se comunicará con usted pronto.

Para obtener un historial de sus casos de soporte, puede seleccionar **Configuración > Cronología** y buscar acciones llamadas "crear caso de soporte". Un botón en el extremo derecho le permite expandir la acción para ver detalles.

Es posible que encuentres el siguiente mensaje de error al intentar crear un caso:

"No está autorizado a crear un caso contra el servicio seleccionado"

Este error podría significar que la cuenta NSS y la empresa registrada con la que está asociada no son la misma empresa registrada para el número de serie de la cuenta BlueXP (es decir, 960xxxx) o el número de serie del entorno de trabajo. Puede buscar ayuda utilizando una de las siguientes opciones:

- Utilice el chat dentro del producto
- Envíe un caso no técnico a https://mysupport.netapp.com/site/help

## Gestione sus casos de soporte (Vista previa)

Puede ver y administrar casos de soporte activos y resueltos directamente desde BlueXP. Podrás gestionar los casos asociados a tu cuenta NSS y a tu empresa.

La gestión de casos está disponible como vista previa. Planeamos perfeccionar esta experiencia y agregar mejoras en próximas versiones. Envíenos sus comentarios mediante el chat del producto.

Tenga en cuenta lo siguiente:

- El panel de gestión de casos en la parte superior de la página ofrece dos vistas:
  - La vista de la izquierda muestra el total de casos abiertos en los últimos 3 meses por la cuenta de usuario NSS que usted proporcionó.
  - La vista de la derecha muestra el total de casos abiertos en los últimos 3 meses a nivel de su empresa en función de su cuenta de usuario NSS.

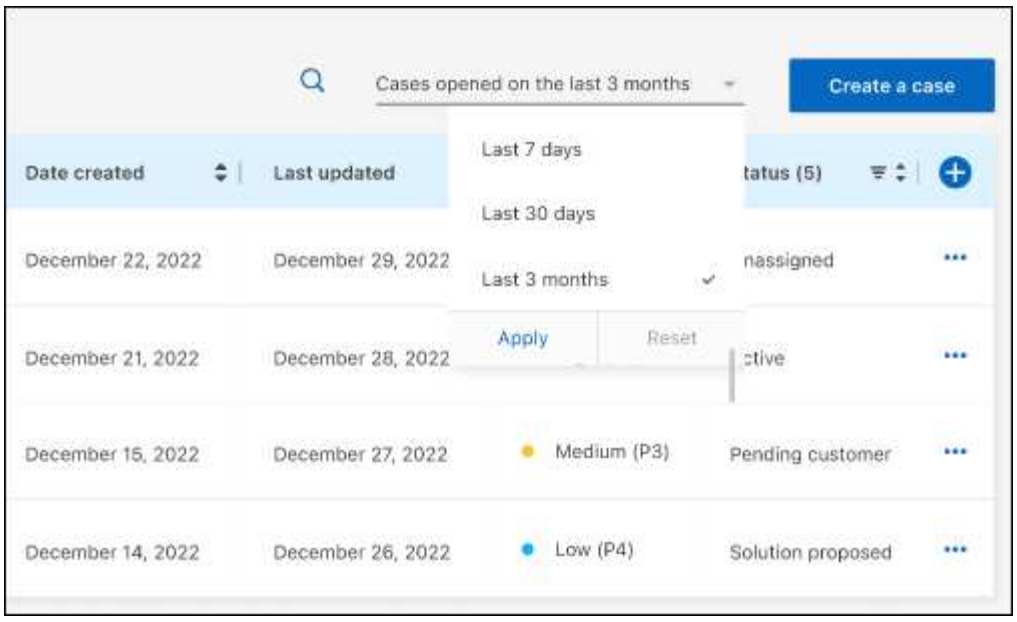
  Los resultados en la tabla reflejan los casos relacionados con la vista que usted seleccionó.
- Puede agregar o eliminar columnas de interés y puede filtrar el contenido de columnas como Prioridad y Estado. Otras columnas sólo proporcionan capacidades de clasificación.

  Vea los pasos a continuación para obtener más detalles.
- A nivel de caso, ofrecemos la posibilidad de actualizar notas de caso o cerrar un caso que aún no esté en estado Cerrado o Pendiente de cierre.

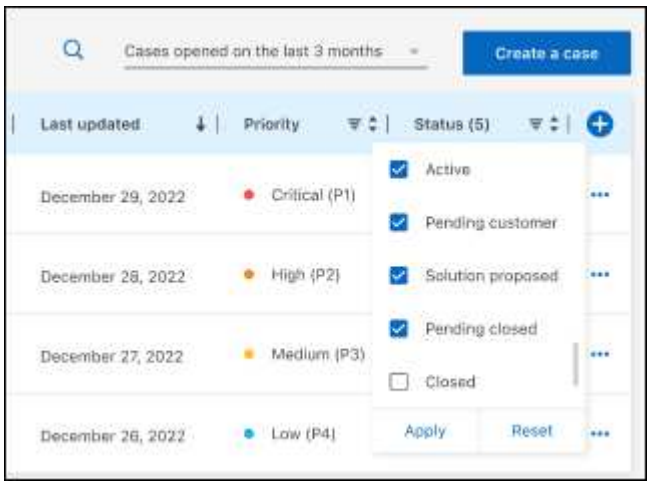
**Pasos**

1. En BlueXP, seleccione **Ayuda > Soporte**.
2. Seleccione **Administración de casos** y, si se le solicita, agregue su cuenta NSS a BlueXP.

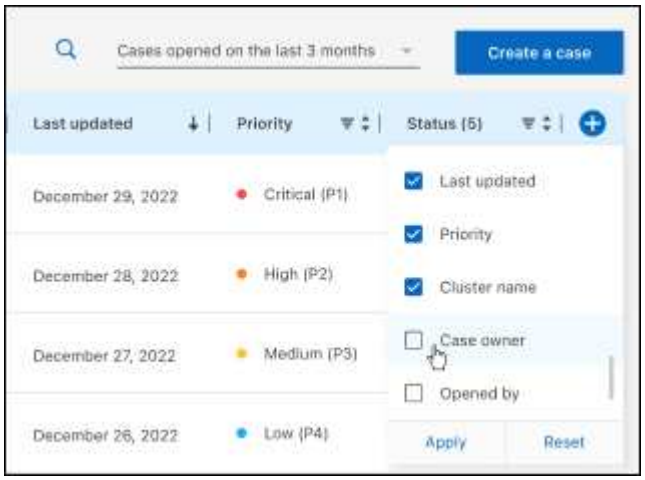
   La página **Administración de casos** muestra casos abiertos relacionados con la cuenta NSS que está asociada con su cuenta de usuario de BlueXP . Esta es la misma cuenta NSS que aparece en la parte superior de la página de **administración de NSS**.
3. Modifique opcionalmente la información que se muestra en la tabla:
   - En **Casos de la organización**, seleccione **Ver** para ver todos los casos asociados a su empresa.
   - Modifique el rango de fechas eligiendo un rango de fechas exacto o eligiendo un período de tiempo diferente.




- Filtrar el contenido de las columnas.




- Cambie las columnas que aparecen en la tabla seleccionando y luego elegir las columnas que desea mostrar.

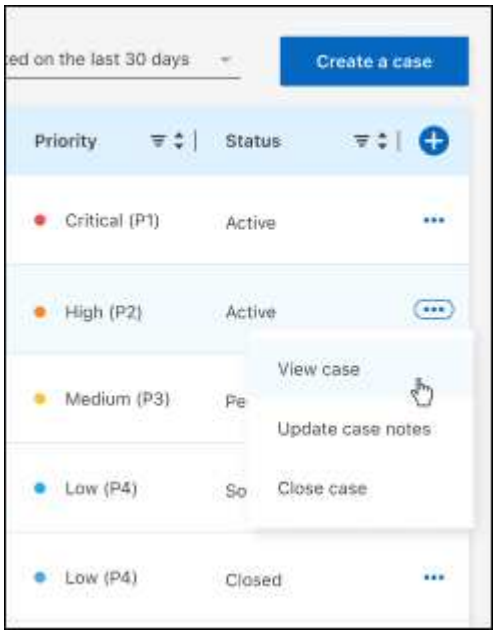


4. Gestionar un caso existente seleccionando ••• y seleccionando una de las opciones disponibles:

   - **Ver caso**: Ver detalles completos sobre un caso específico.
   - **Actualizar notas del caso**: proporcione detalles adicionales sobre su problema o seleccione **Cargar archivos** para adjuntar hasta un máximo de cinco archivos.

     Los archivos adjuntos están limitados a 25 MB por archivo. Se admiten las siguientes extensiones de archivo: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx y csv.

   - **Cerrar caso**: proporcione detalles sobre el motivo por el cual está cerrando el caso y seleccione **Cerrar caso**.



# Avisos legales

Los avisos legales proporcionan acceso a declaraciones de derechos de autor, marcas comerciales, patentes y más.

## Copyright

"https://www.netapp.com/company/legal/copyright/"

## Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de Marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Otros nombres de empresas y productos pueden ser marcas comerciales de sus respectivos propietarios.

"https://www.netapp.com/company/legal/trademarks/"

## Patentes

Puede encontrar una lista actualizada de las patentes propiedad de NetApp en:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

## Política de privacidad

"https://www.netapp.com/company/legal/privacy-policy/"

## Código abierto

Los archivos de aviso proporcionan información sobre derechos de autor y licencias de terceros utilizados en el software de NetApp .

"Aviso para NetApp Disaster Recovery"