Recuperación ante desastres de BlueXP

NetApp Solutions

NetApp
December 19, 2024

Tabla de contenidos

Recuperación ante desastres de BlueXP

3-2-1 Protección de datos para VMware con complemento SnapCenter y backup y recuperación de datos de BlueXP para máquinas virtuales

La estrategia de respaldo 3-2-1 es un método de protección de datos aceptado en el sector, que proporciona un enfoque integral para proteger datos valiosos. Esta estrategia es fiable y garantiza que, incluso si se produce algún desastre inesperado, todavía habrá una copia de los datos disponibles.

Autor: Josh Powell: Ingeniería de soluciones de NetApp

Descripción general

La estrategia se compone de tres reglas fundamentales:

1. Conserve al menos tres copias de sus datos. Esto garantiza que, incluso si una copia se pierde o está dañada, todavía tiene al menos dos copias restantes para volver a caer.
2. Almacene dos copias de seguridad en dispositivos o medios de almacenamiento diferentes. La diversificación de los medios de almacenamiento ayuda a protegerse contra fallos específicos de dispositivos o de medios. Si un dispositivo se daña o un tipo de soporte falla, la otra copia de seguridad no se ve afectada.
3. Por último, asegúrese de que al menos una copia de backup esté fuera de las instalaciones. El almacenamiento externo actúa como protección ante desastres localizados, como incendios o inundaciones, que podrían inutilizar las copias in situ.

Este documento de solución abarca una solución de backups 3-2-1 mediante el complemento SnapCenter para VMware vSphere (SCV) para crear backups primarios y secundarios de nuestras máquinas virtuales en las instalaciones y backup y recuperación de BlueXP para máquinas virtuales y realizar un backup de una copia de nuestros datos en el almacenamiento en cloud o StorageGRID.

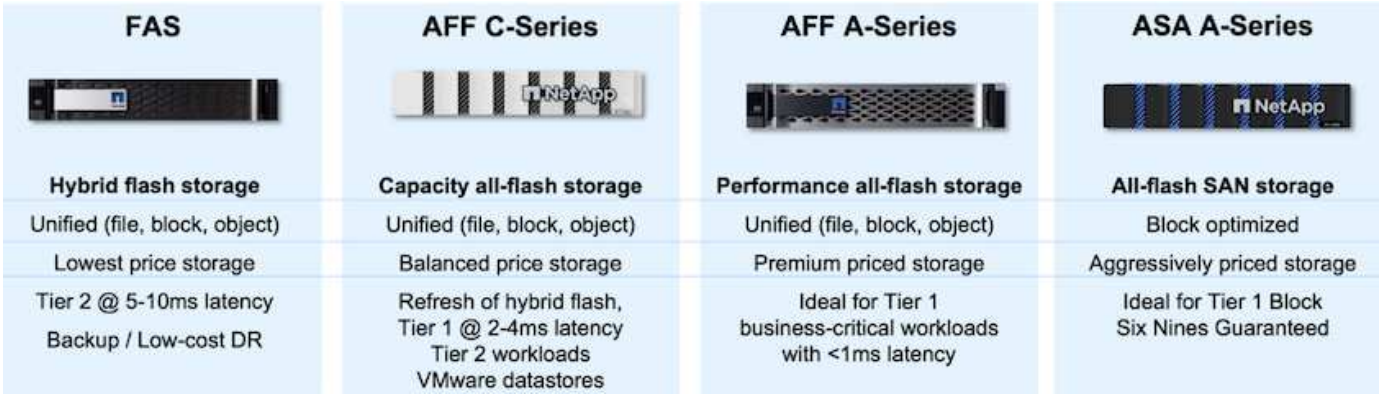
Casos de uso

Esta solución aborda los siguientes casos prácticos:

- Backup y restauración de máquinas virtuales y almacenes de datos en las instalaciones mediante el plugin de SnapCenter para VMware vSphere.
- Backup y restauración de máquinas virtuales y almacenes de datos on-premises, alojadas en clústeres de ONTAP y realizando backups en el almacenamiento de objetos mediante backup y recuperación de BlueXP para máquinas virtuales.

Almacenamiento de datos de NetApp ONTAP

ONTAP es la solución de almacenamiento líder del sector de NetApp que ofrece almacenamiento unificado, tanto si se accede a través de protocolos SAN o NAS. La estrategia de backup 3-2-1 garantiza que los datos en las instalaciones estén protegidos en más de un tipo de medio, y NetApp ofrece plataformas que van desde flash de alta velocidad a medios de bajo coste.



Para obtener más información acerca de toda la plataforma de hardware de NetApp, consulte "Almacenamiento de datos de NetApp".

Plugin de SnapCenter para VMware vSphere

El complemento de SnapCenter para VMware vSphere es una oferta de protección de datos que está perfectamente integrada con VMware vSphere y permite una gestión sencilla de backup y restauraciones de máquinas virtuales. Como parte de esa solución, SnapMirror proporciona un método rápido y fiable para crear una segunda copia de backup inmutable de datos de un equipo virtual en un clúster de almacenamiento de ONTAP secundario. Con esta arquitectura en vigor, las operaciones de restauración de máquinas virtuales pueden iniciarse fácilmente desde ubicaciones de backup principales o secundarias.

SCV se pone en marcha como dispositivo virtual linux mediante un archivo OVA. El plugin ahora utiliza un plugin remoto
arquitectura. El plugin remoto se ejecuta fuera del servidor vCenter y se aloja en el dispositivo virtual SCV.

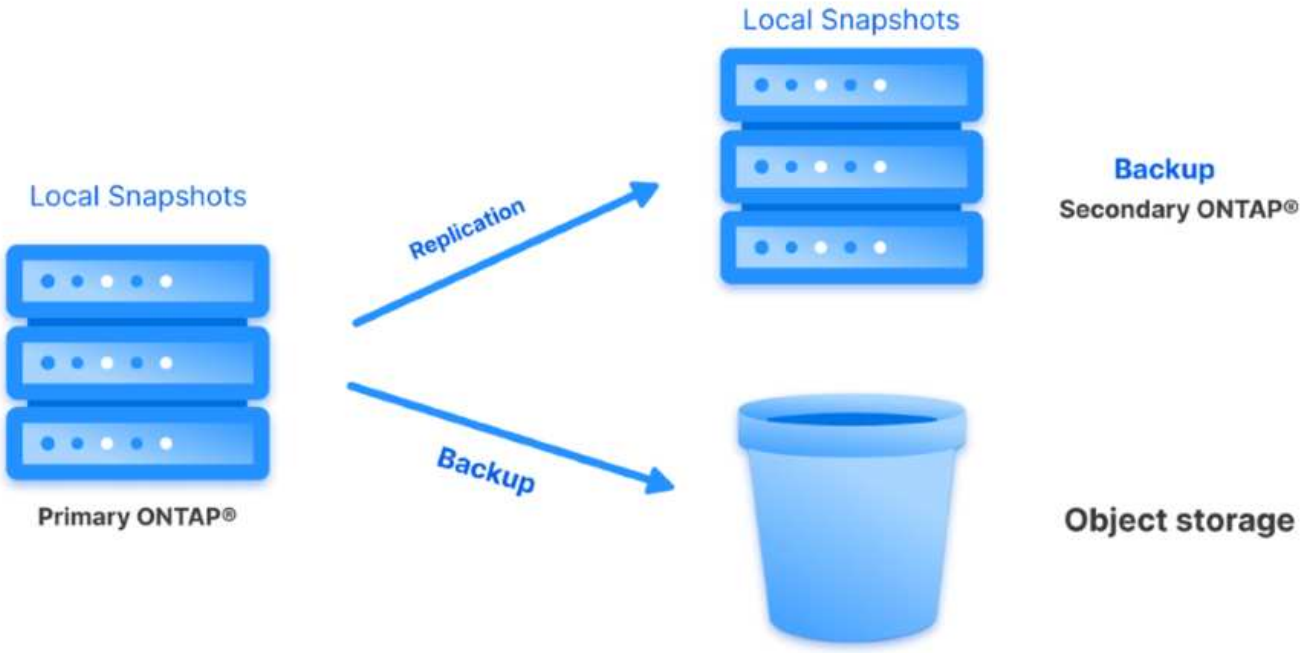
Para obtener información detallada sobre SCV, consulte "Documentación del plugin de SnapCenter para VMware vSphere".

Backup y recuperación de BlueXP para máquinas virtuales

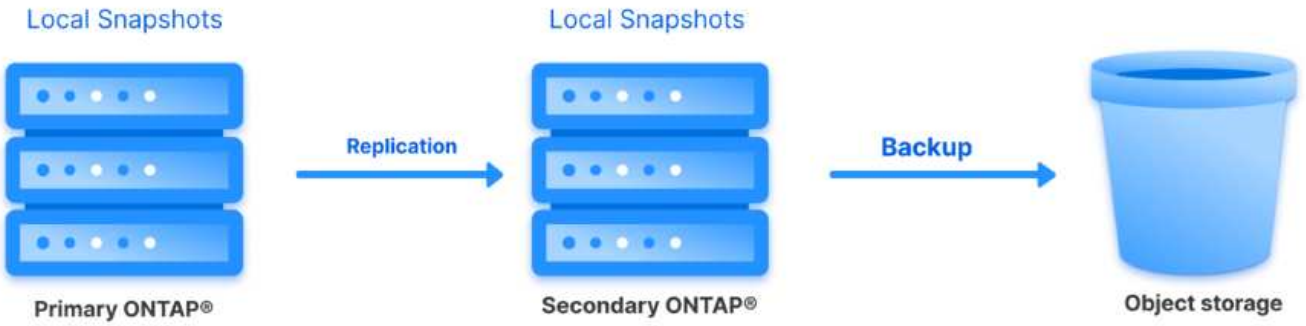
El backup y recuperación de datos de BlueXP es una herramienta basada en la nube para la gestión de datos que proporciona un único plano de control para una amplia gama de operaciones de backup y recuperación tanto en entornos on-premises como en la nube. Parte de la suite de backup y recuperación de datos de NetApp BlueXP es una función que se integra con el complemento SnapCenter para VMware vSphere (en las instalaciones) para ampliar una copia de los datos al almacenamiento de objetos en el cloud. De este modo se establece una tercera copia de los datos fuera de las instalaciones que se obtiene a partir de los backups del almacenamiento principal o secundario. El backup y la recuperación de datos de BlueXP facilita la configuración de políticas de almacenamiento que transfieren copias de tus datos desde cualquiera de estas dos ubicaciones on-premises.

Si se elige entre los backups primarios y secundarios como origen en el backup y recuperación de BlueXP, se implementará una de las dos topologías:

Topología de Fan-Out – Cuando el plugin de SnapCenter inicia una copia de seguridad para VMware vSphere, se toma inmediatamente una instantánea local. A continuación, SCV inicia una operación de SnapMirror que replica la snapshot más reciente en el clúster de ONTAP secundario. En el backup y recuperación de BlueXP, una política especifica el clúster de ONTAP principal como el origen de una copia Snapshot de los datos que se transferirán al almacenamiento de objetos en el proveedor de cloud de su elección.



Topología en cascada – Crear las copias de datos primarias y secundarias usando SCV es idéntica a la topología de fan-out mencionada anteriormente. Sin embargo, esta vez se crea una política en BlueXP Backup and Recovery que especifica que el backup en el almacenamiento de objetos se originará en el clúster de ONTAP secundario.



El backup y la recuperación de datos de BlueXP puede crear copias de backup de copias de Snapshot de ONTAP en las instalaciones en el almacenamiento de AWS Glacier, Azure Blob y GCP Archive.

AWS Glacier and Deep Glacier

Azure Blob Archive

GCP Archive Storage

Además, es posible usar NetApp StorageGRID como destino de backup de almacenamiento de objetos. Para obtener más información acerca de StorageGRID, consulte la "Página de destino de StorageGRID".

Descripción general de la puesta en marcha de soluciones

Esta lista proporciona los pasos altos necesarios para configurar esta solución y ejecutar las operaciones de backup y restauración a partir de backup y recuperación de SCV y BlueXP:

1. Configure la relación de SnapMirror entre los clústeres de ONTAP que se van a utilizar para copias de datos primarias y secundarias.
2. Configure el plugin de SnapCenter para VMware vSphere.
   a. Añadir sistemas de almacenamiento
   b. Cree políticas de backup
   c. Crear grupos de recursos
   d. Ejecute las primeras tareas de backup
3. Configurar el backup y la recuperación de datos de BlueXP para máquinas virtuales
   a. Agregar entorno de trabajo
   b. Detectar dispositivos SCV y vCenter
   c. Cree políticas de backup
   d. Activar backups
4. Restaure máquinas virtuales del almacenamiento principal y secundario con SCV.
5. Restaura las máquinas virtuales desde el almacenamiento de objetos mediante el backup y la restauración de BlueXP.

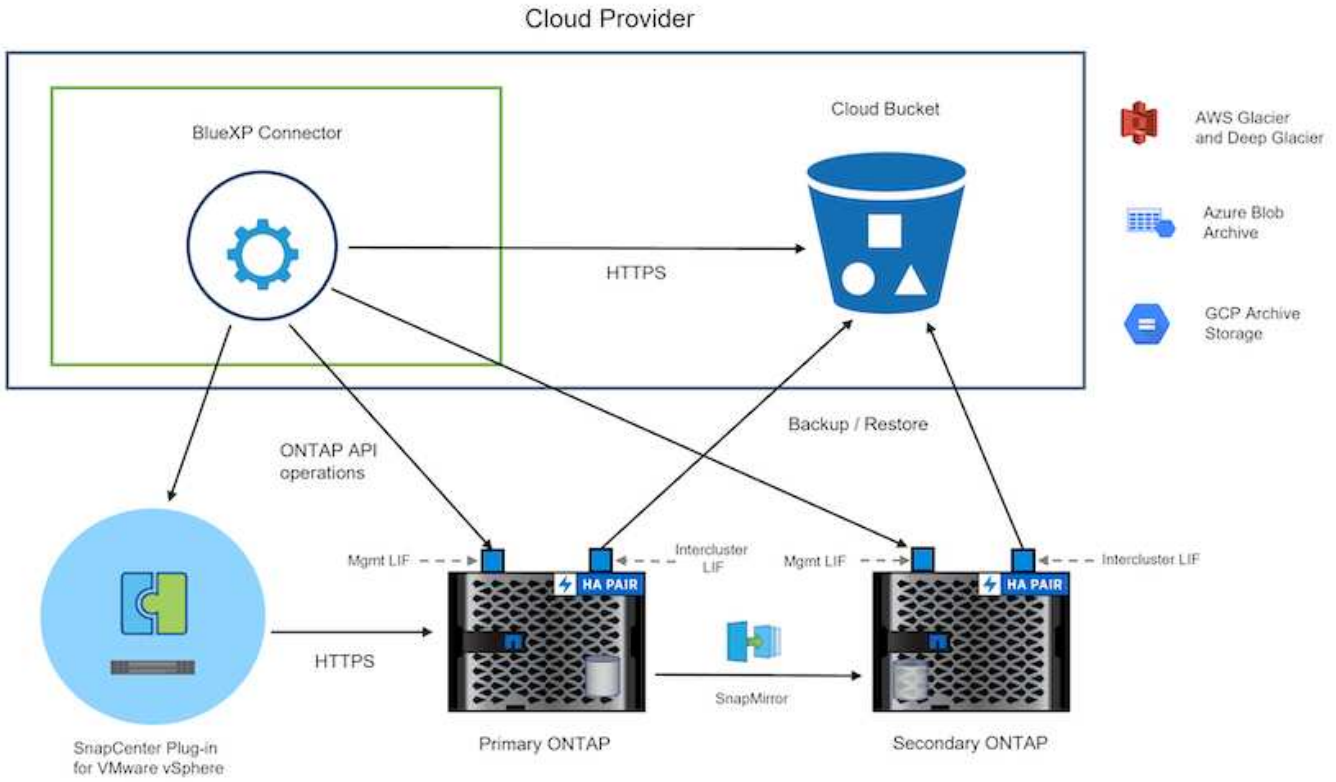
Requisitos previos

El objetivo de esta solución es demostrar la protección de datos de equipos virtuales que se ejecutan en VMware vSphere y que se encuentran en almacenes de datos NFS alojados por NetApp ONTAP. Esta solución asume que los siguientes componentes están configurados y listos para su uso:

1. Clúster de almacenamiento de ONTAP con almacenes de datos NFS o VMFS conectados a VMware vSphere. Se admiten almacenes de datos NFS y VMFS. Para esta solución, se utilizaron almacenes de datos NFS.
2. Clúster de almacenamiento secundario de ONTAP con relaciones de SnapMirror establecidas para volúmenes utilizados para almacenes de datos NFS.
3. El conector BlueXP instalado para el proveedor cloud se utiliza para los backups de almacenamiento de objetos.
4. Las máquinas virtuales a las que se va a realizar un backup se encuentran en almacenes de datos NFS que residen en el clúster de almacenamiento de ONTAP principal.
5. Conectividad de red entre el conector de BlueXP y las interfaces de gestión del clúster de almacenamiento de ONTAP en las instalaciones.
6. Conectividad de red entre el conector BlueXP y la máquina virtual del dispositivo SCV en las instalaciones, y entre el conector de BlueXP y vCenter.
7. La conectividad de red entre las LIF de interconexión de clústeres de ONTAP en las instalaciones y el servicio de almacenamiento de objetos.
8. DNS configurado para la SVM de gestión en clústeres de almacenamiento de ONTAP principales y secundarios. Para obtener más información, consulte "Configure DNS para la resolución de nombres de host".

Arquitectura de alto nivel

Las pruebas y la validación de esta solución se llevaron a cabo en un laboratorio que puede o no coincidir con el entorno de puesta en marcha final.



Puesta en marcha de la solución

Con esta solución, ofrecemos instrucciones detalladas para poner en marcha y validar una solución que utilice el plugin de SnapCenter para VMware vSphere, junto con backup y recuperación de datos de BlueXP, para realizar backups y recuperaciones de máquinas virtuales de Windows y Linux en un clúster de VMware vSphere ubicado en un centro de datos en las instalaciones. Las máquinas virtuales incluidas en esta configuración se almacenan en almacenes de datos NFS alojados en un clúster de almacenamiento de ONTAP A300. Además, un clúster de almacenamiento independiente A300 de ONTAP sirve como destino secundario para los volúmenes replicados con SnapMirror. Además, el almacenamiento de objetos alojado en Amazon Web Services y Azure Blob se emplearon como objetivos para una tercera copia de los datos.

Continuaremos creando relaciones de SnapMirror para copias secundarias de nuestros backups gestionados por SCV y la configuración de trabajos de backup tanto en el backup y recuperación de SCV como en BlueXP.

Para obtener información detallada sobre el plugin de SnapCenter para VMware vSphere, consulte la "Documentación del plugin de SnapCenter para VMware vSphere".

Para obtener información detallada sobre el backup y la recuperación de BlueXP, consulte la "Documentación de backup y recuperación de BlueXP".

Establecer relaciones de SnapMirror entre clústeres de ONTAP

El plugin de SnapCenter para VMware vSphere utiliza la tecnología SnapMirror de ONTAP para gestionar el transporte de copias de SnapMirror o SnapVault secundarias a un clúster de ONTAP secundario.

Las políticas de backup de SCV tienen la opción de usar relaciones de SnapMirror o SnapVault. La diferencia principal radica en que, al utilizar la opción de SnapMirror, el programa de retención configurado para backups en la política será el mismo en las ubicaciones primaria y secundaria. El SnapVault se ha diseñado para archivado y cuando se utiliza esta opción, se puede establecer un programa de retención independiente con la relación de SnapMirror para las copias snapshot en el clúster de almacenamiento de ONTAP secundario.

La configuración de las relaciones de SnapMirror puede realizarse en BlueXP, donde muchos de los pasos se automatizan, o bien puede realizarse mediante System Manager y la interfaz de línea de comandos de ONTAP. Todos estos métodos se discuten a continuación.

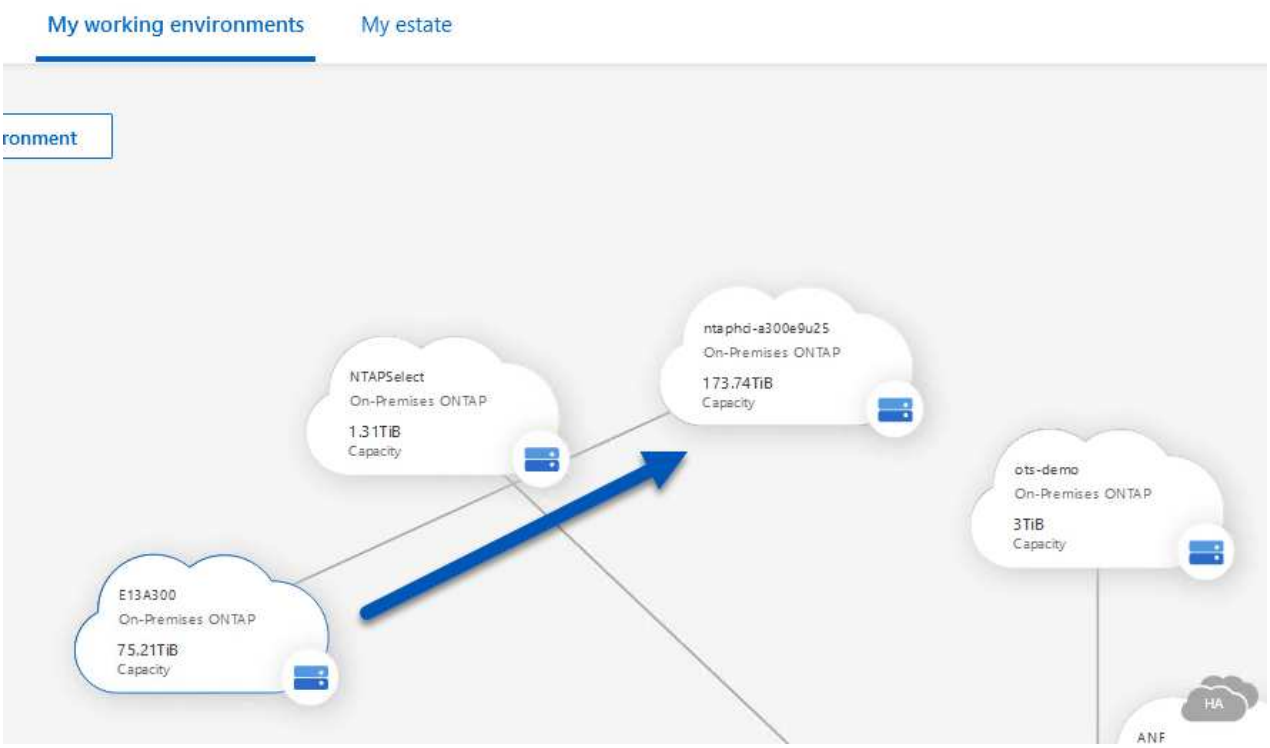
Establece relaciones de SnapMirror con BlueXP

Se deben completar los siguientes pasos desde la consola web de BlueXP:

Configuración de replicación para sistemas de almacenamiento de ONTAP principales y secundarios

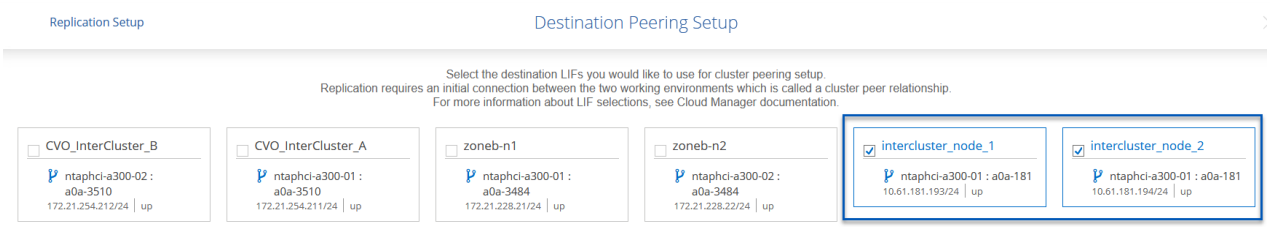
Para empezar, inicie sesión en la consola web de BlueXP y vaya a Canvas.

1. Arrastre y suelte el sistema de almacenamiento ONTAP de origen (principal) en el sistema de almacenamiento ONTAP (secundario) de destino.

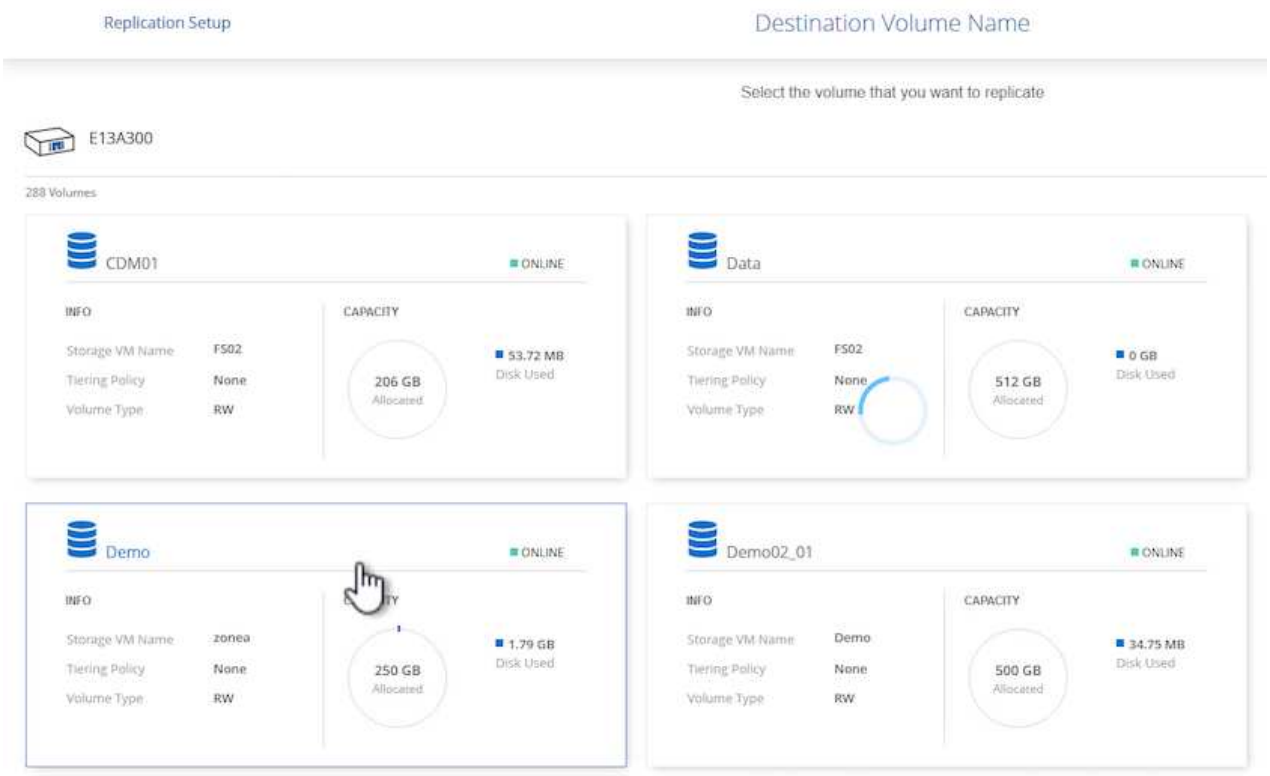


2. En el menú que aparece seleccione **Replicación**.

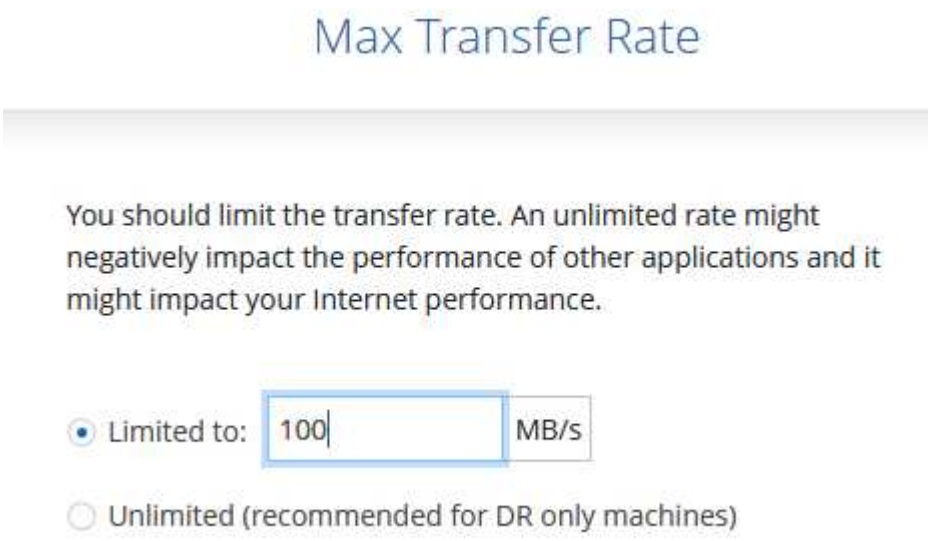
3. En la página **Configuración de pares de destino**, seleccione las LIF de interconexión de clústeres de destino que se utilizarán para la conexión entre sistemas de almacenamiento.



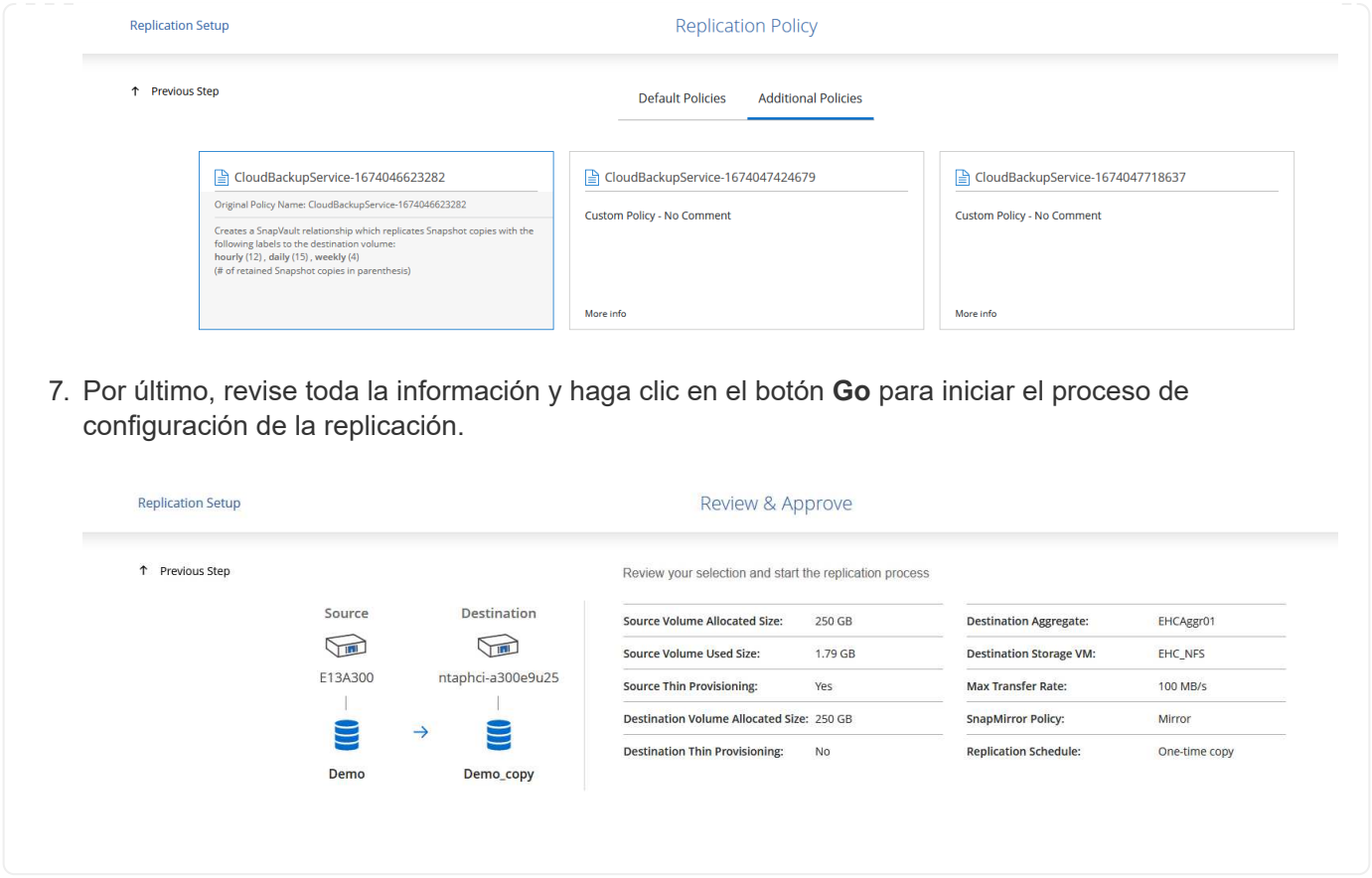
4. En la página **Nombre del volumen de destino**, seleccione primero el volumen de origen y, a continuación, rellene el nombre del volumen de destino y seleccione la SVM de destino y el agregado. Haga clic en **Siguiente** para continuar.



5. Elija la velocidad de transferencia máxima para que se produzca la replicación.



6. Seleccione la política que determinará la programación de retención para backups secundarios. Esta política se puede crear de antemano (consulte el proceso manual a continuación en el paso **Crear una política de retención de instantáneas**) o se puede cambiar después del hecho si lo desea.



7. Por último, revise toda la información y haga clic en el botón **Go** para iniciar el proceso de configuración de la replicación.

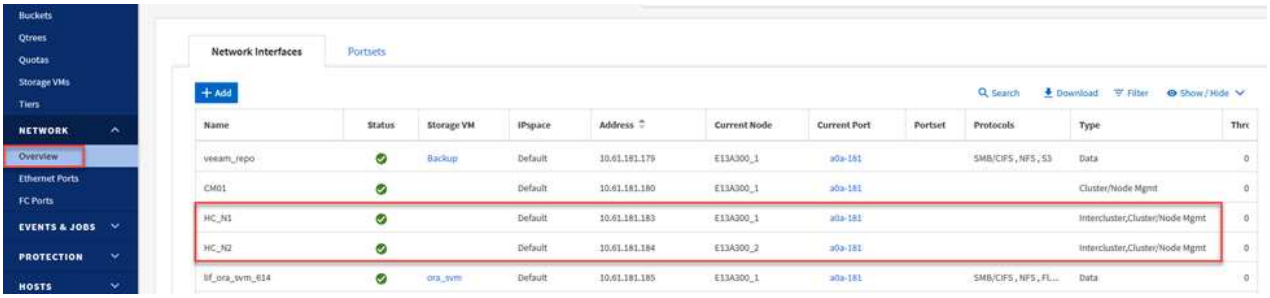
Establezca relaciones de SnapMirror con System Manager y la interfaz de línea de comandos de ONTAP

Todos los pasos necesarios para establecer relaciones de SnapMirror pueden realizarse con System Manager o la interfaz de línea de comandos de ONTAP. En la siguiente sección se proporciona información detallada para ambos métodos:

Registre las interfaces lógicas de interconexión de clústeres de origen y destino

Para los clústeres de ONTAP de origen y de destino, puede recuperar la información de LIF entre clústeres desde System Manager o desde la CLI.

1. En ONTAP System Manager, desplácese a la página Network Overview y recupere las direcciones IP de Type: Interclúster configurado para comunicarse con el VPC donde se instaló FSX.



2. Para recuperar las direcciones IP de interconexión de clústeres mediante la CLI, ejecute el siguiente comando:

```
ONTAP-Dest::> network interface show -role intercluster
```

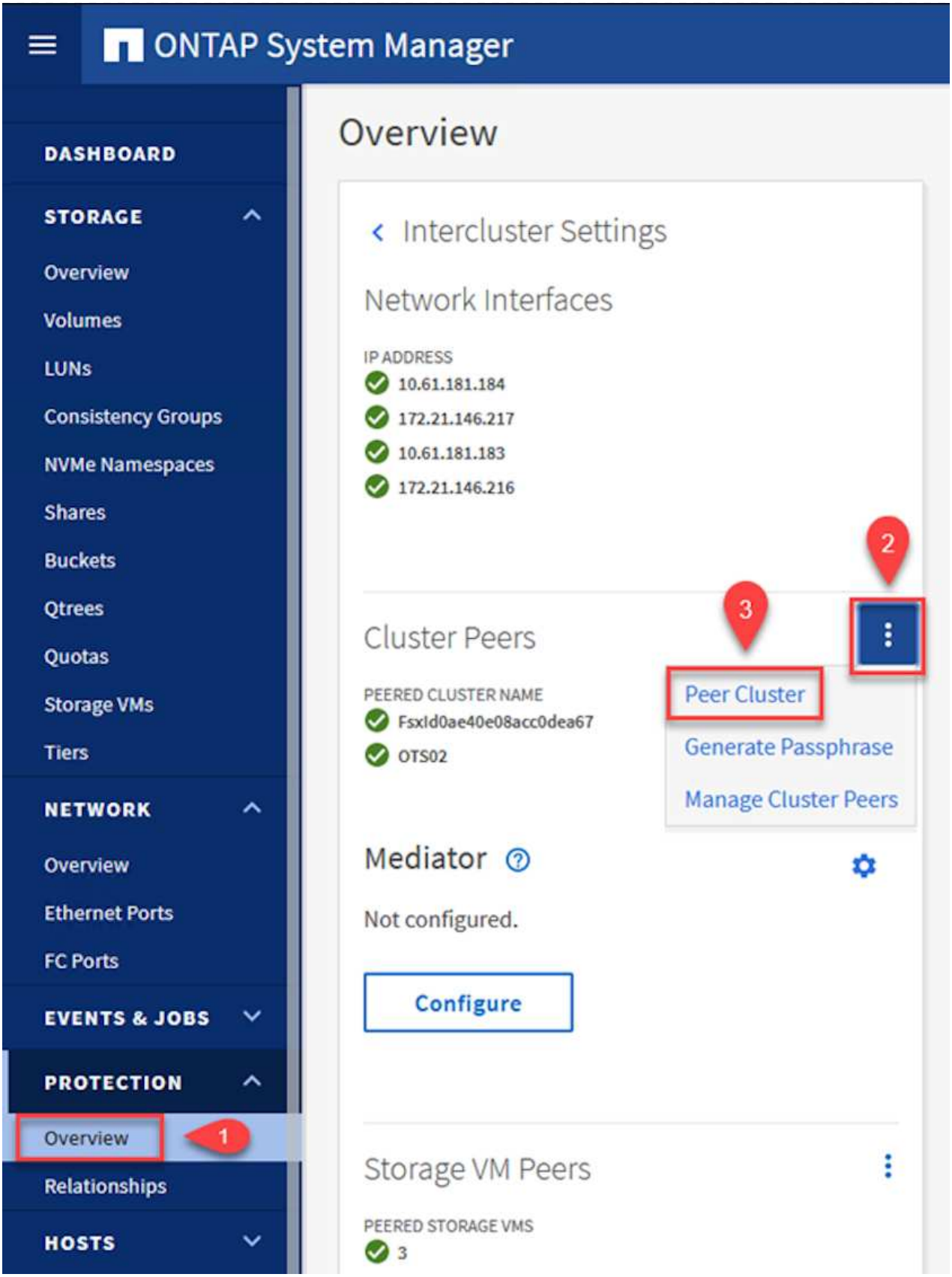
Establezca las relaciones de clústeres entre iguales entre clústeres de ONTAP

Para establecer una relación entre iguales de clústeres entre clústeres ONTAP, se debe confirmar una clave de acceso única introducida en el clúster de ONTAP de inicio en el otro clúster de paridad.

1. Configure los iguales en el clúster ONTAP de destino mediante el `cluster peer create` comando. Cuando se le solicite, introduzca una clave de acceso única que se usará más adelante en el clúster de origen para finalizar el proceso de creación.

```
ONTAP-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

2. En el clúster de origen, puede establecer la relación de paridad de clústeres mediante ONTAP System Manager o CLI. En ONTAP System Manager, desplácese hasta Protection > Overview y seleccione Peer Cluster.

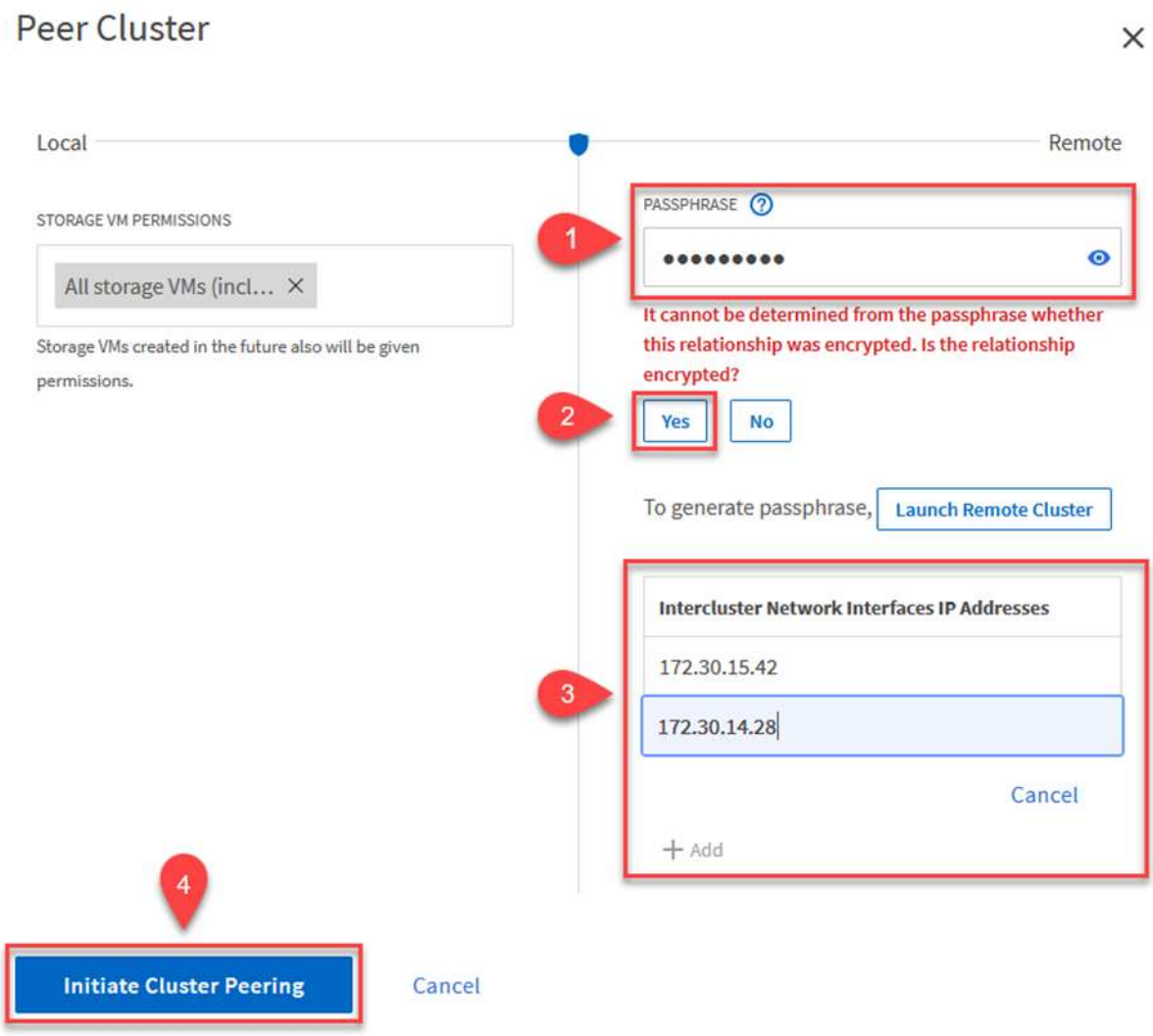


3. En el cuadro de diálogo Peer Cluster, rellene la información que corresponda:
   a. Introduzca la clave de acceso que se utilizó para establecer la relación entre iguales del clúster en el clúster de ONTAP de destino.

b. Seleccione `Yes` para establecer una relación cifrada.

c. Introduzca las direcciones IP de LIF entre clústeres del clúster de ONTAP de destino.

d. Haga clic en Iniciar Cluster peering para finalizar el proceso.



4. Compruebe el estado de la relación entre iguales de clústeres en el clúster de ONTAP de destino con el siguiente comando:

```
ONTAP-Dest::> cluster peer show
```

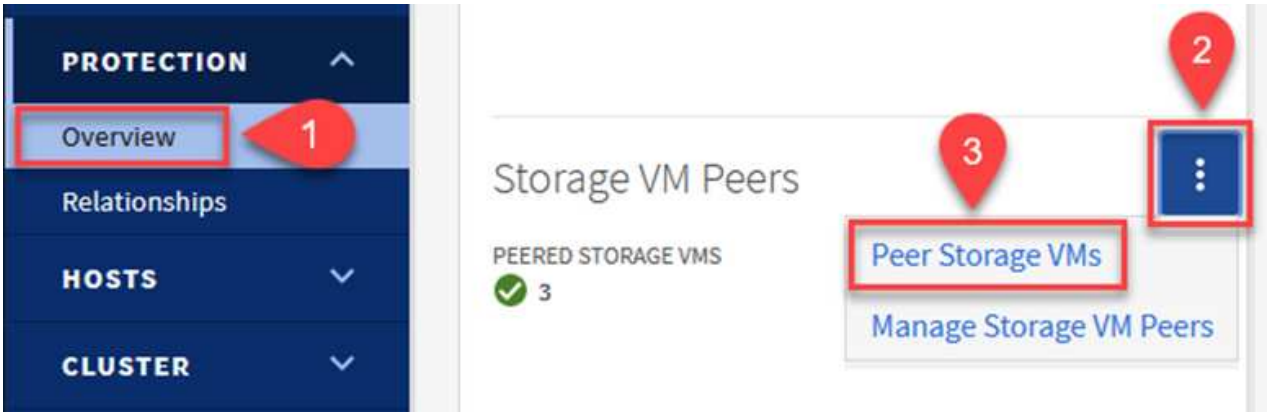
Establecer la relación de paridad de SVM

El siguiente paso consiste en configurar una relación de SVM entre las máquinas virtuales de almacenamiento de destino y origen que contengan los volúmenes que se incluirán en las relaciones de SnapMirror.

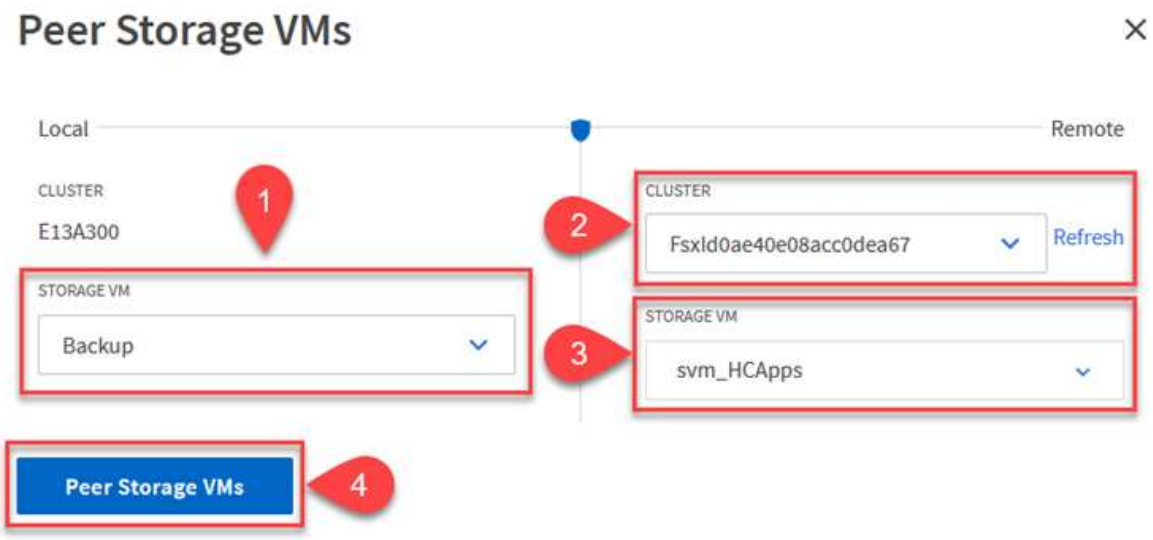
1. Desde el clúster de ONTAP de destino, utilice el siguiente comando desde la interfaz de línea de comandos para crear la relación entre iguales de SVM:

```
ONTAP-Dest::> vserver peer create -vserver DestSVM -peer-vserver
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. En el clúster de ONTAP de origen, acepte la relación de paridad con ONTAP System Manager o CLI.
3. En ONTAP System Manager, vaya a Protection > Overview y seleccione Peer Storage VMs, en Storage VM peers.



4. En el cuadro de diálogo de la VM de almacenamiento del mismo nivel, rellene los campos necesarios:
   - La máquina virtual de almacenamiento de origen
   - El clúster de destino
   - La máquina virtual de almacenamiento de destino



5. Haga clic en Peer Storage VMs para completar el proceso de paridad de SVM.

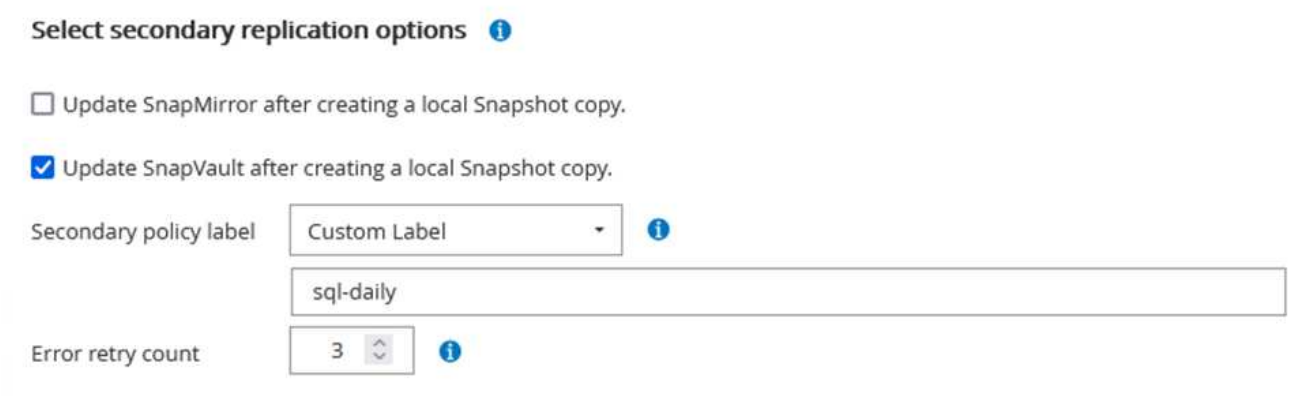
Crear una política de retención de snapshots

SnapCenter gestiona los programas de retención para los backups que existen como copias Snapshot en el sistema de almacenamiento principal. Esto se establece al crear una política en SnapCenter. SnapCenter no gestiona las políticas de retención para backups que se conservan en sistemas de almacenamiento secundario. Estas políticas se gestionan por separado mediante una política de SnapMirror creada en el clúster FSX secundario y asociada con los volúmenes de destino que se encuentran en una relación de SnapMirror con el volumen de origen.

Al crear una política de SnapCenter, tiene la opción de especificar una etiqueta de política secundaria que se añada a la etiqueta de SnapMirror de cada snapshot generada al realizar un backup de SnapCenter.

> En el almacenamiento secundario, estas etiquetas se adaptan a las reglas de normativas asociadas con el volumen de destino con el fin de aplicar la retención de copias Snapshot.

El siguiente ejemplo muestra una etiqueta de SnapMirror presente en todas las copias de Snapshot generadas como parte de una política utilizada para los backups diarios de nuestros volúmenes de registros y base de datos de SQL Server.



Para obtener más información sobre la creación de políticas de SnapCenter para una base de datos de SQL Server, consulte "Documentación de SnapCenter".

Primero debe crear una política de SnapMirror con reglas que exijan el número de copias de snapshot que se retendrán.

1. Cree la política SnapMirror en el clúster FSX.

```
ONTAP-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. Añada reglas a la política con etiquetas de SnapMirror que coincidan con las etiquetas de política secundaria especificadas en las políticas de SnapCenter.

```
ONTAP-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

El siguiente script ofrece un ejemplo de una regla que se puede agregar a una directiva:

```
ONTAP-Dest::> snapmirror policy add-rule -vserver sql_svm_dest
-policy Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

Crear reglas adicionales para cada etiqueta de SnapMirror y el número de copias de Snapshot que se retendrán (período de retención).

Crear volúmenes de destino

Para crear un volumen de destino en ONTAP que será el destinatario de las copias Snapshot de nuestros volúmenes de origen, ejecute el siguiente comando en el clúster de ONTAP de destino:

```
ONTAP-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

Crear las relaciones de SnapMirror entre los volúmenes de origen y de destino

Para crear una relación de SnapMirror entre un volumen de origen y uno de destino, ejecute el siguiente comando en el clúster de ONTAP de destino:

```
ONTAP-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

Inicializar las relaciones de SnapMirror

Inicialice la relación de SnapMirror. Este proceso inicia una snapshot nueva generada del volumen de origen y la copia al volumen de destino.

Para crear un volumen, ejecute el siguiente comando en el clúster de ONTAP de destino:

```
ONTAP-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

Configure el plugin de SnapCenter para VMware vSphere

Una vez instalado, puede accederse al plugin de SnapCenter para VMware vSphere desde la interfaz de gestión de vCenter Server Appliance. SCV gestionará backups para los almacenes de datos NFS montados en los hosts ESXi y que contienen máquinas virtuales Windows y Linux.

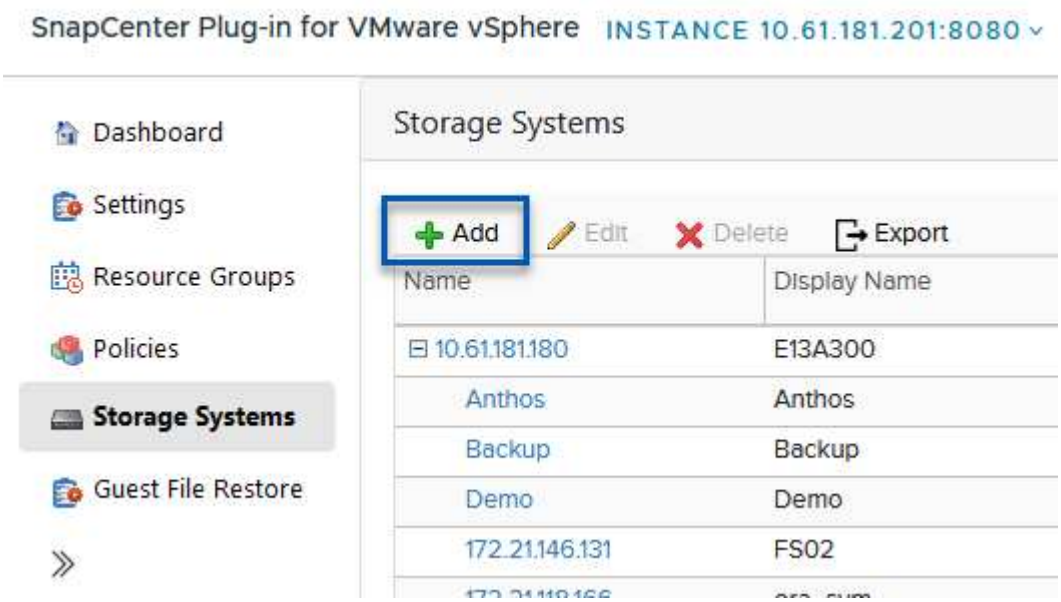
Revise la "Flujo de trabajo de protección de datos" Sección de la documentación de SCV, para obtener más información sobre los pasos involucrados en la configuración de backups.

Para configurar backups de las máquinas virtuales y los almacenes de datos, será necesario completar los siguientes pasos desde la interfaz del plugin.

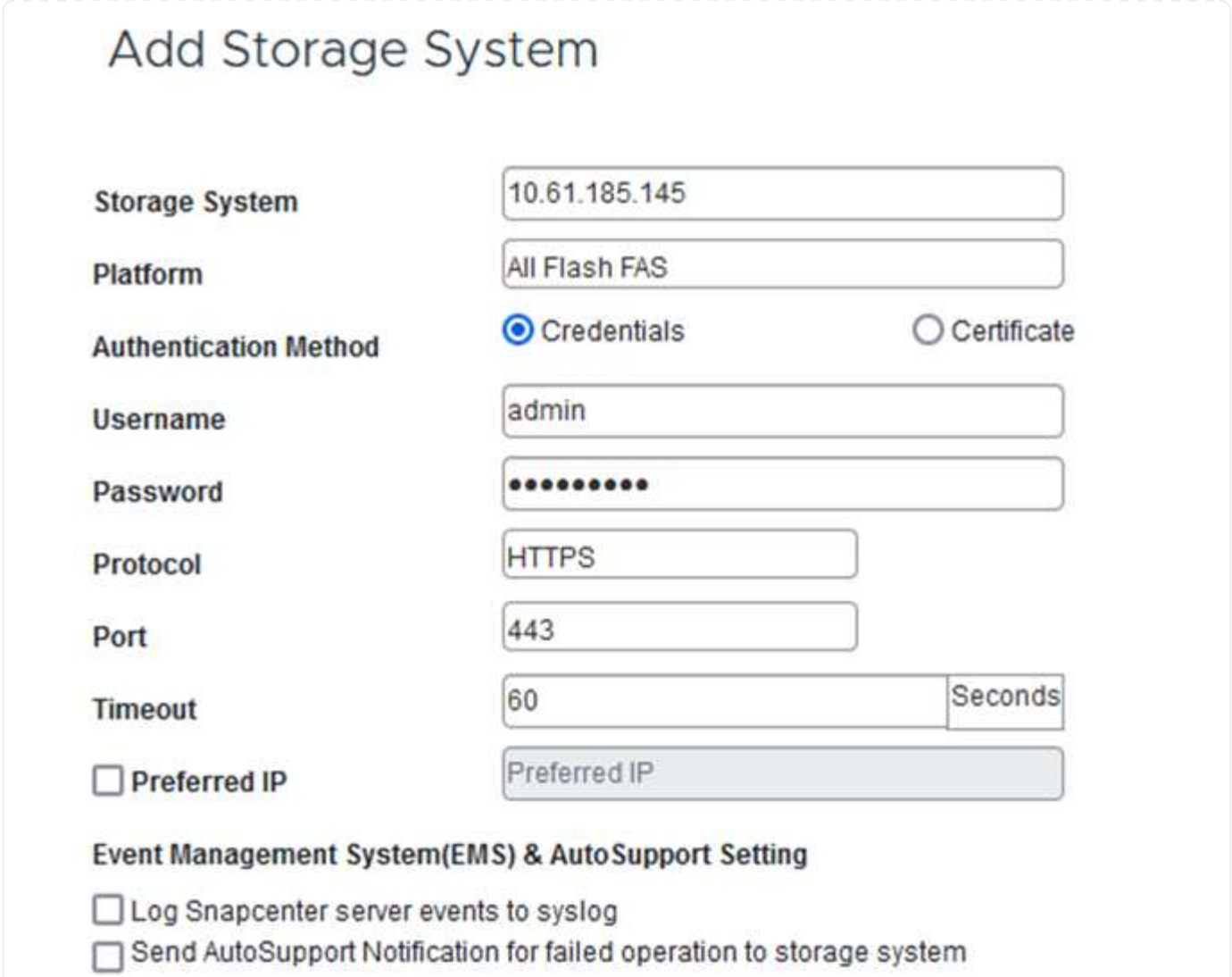
Detección de sistemas de almacenamiento ONTAP

Detectar los clústeres de almacenamiento de ONTAP que se usarán para backups primarios y secundarios.

1. En el plug-in de SnapCenter para VMware vSphere navegue hasta **Sistemas de almacenamiento** en el menú de la izquierda y haga clic en el botón **Agregar**.



2. Complete las credenciales y el tipo de plataforma para el sistema de almacenamiento ONTAP principal y haga clic en **Agregar**.



3. Repita este procedimiento para el sistema de almacenamiento ONTAP secundario.

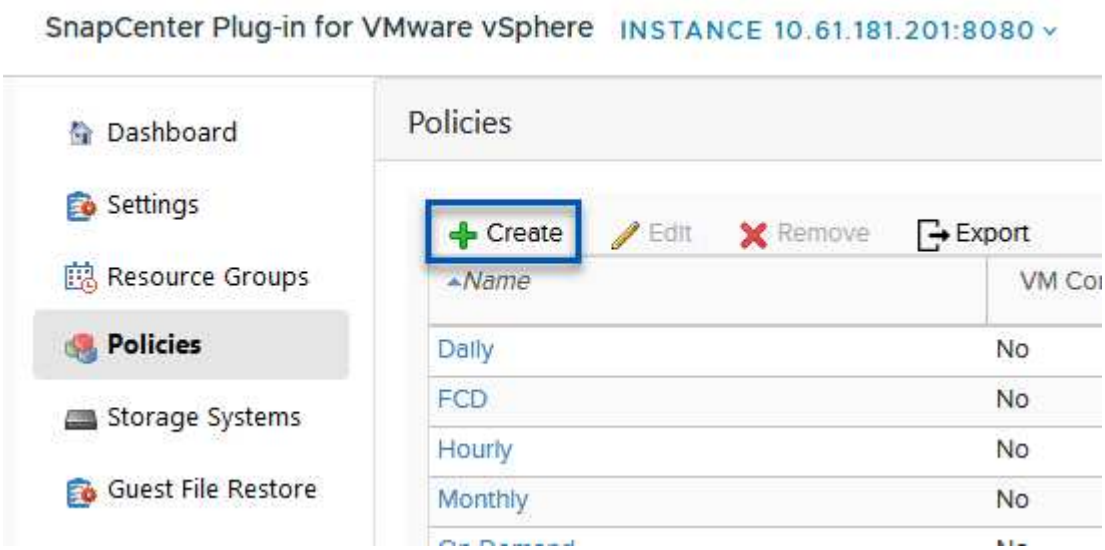
Crear políticas de backup de SCV

Las políticas especifican el período de retención, la frecuencia y las opciones de replicación para los backups gestionados por SCV.

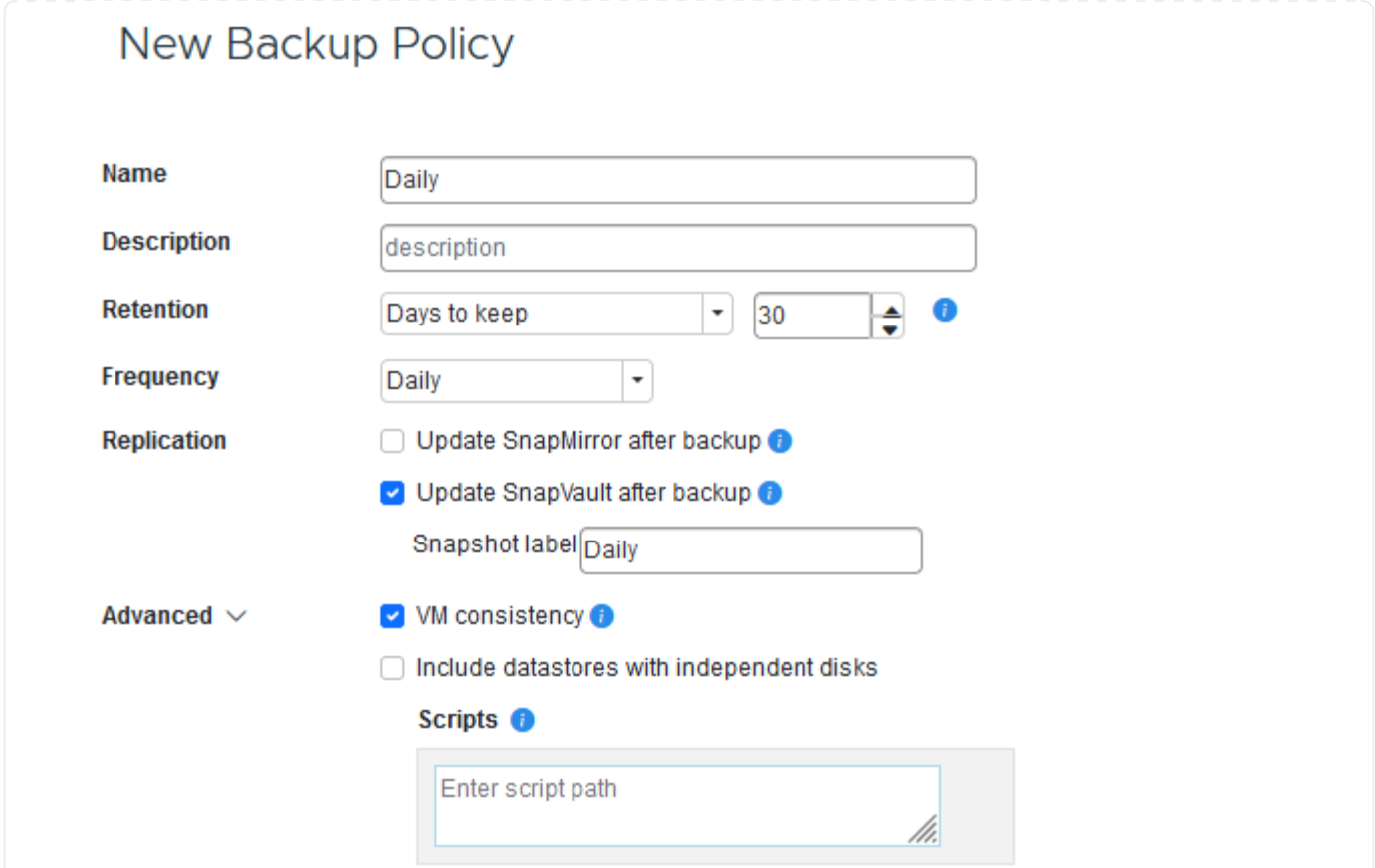
Revise la "Crear políticas de backup para máquinas virtuales y almacenes de datos" sección de la documentación para más información.

Para crear políticas de backup complete los siguientes pasos:

1. En el complemento de SnapCenter para VMware vSphere, navegue hasta **Políticas** en el menú de la izquierda y haga clic en el botón **Crear**.



2. Escriba un nombre para la política, el período de retención, las opciones de frecuencia y replicación y la etiqueta de la snapshot.



Al crear una política en el plugin de SnapCenter, verá opciones para SnapMirror y SnapVault. Si elige SnapMirror, la programación de retención especificada en la política será la misma para las copias de Snapshot primarias y secundarias. Si elige SnapVault, la programación de retención de la snapshot secundaria se basará en una programación independiente implementada con la relación de SnapMirror. Esto es útil cuando se desean períodos de retención más largos para backups secundarios.

Las etiquetas de Snapshot son útiles porque se pueden usar para aplicar políticas con un período de retención específico para las copias de SnapVault replicadas en el clúster de ONTAP secundario. Cuando SCV se utiliza con BlueXP Backup and Restore, el campo de etiqueta de Snapshot debe estar en blanco o Match la etiqueta especificada en la política de backup de BlueXP.

3. Repita el procedimiento para cada política necesaria. Por ejemplo, políticas independientes para backups diarios, semanales y mensuales.

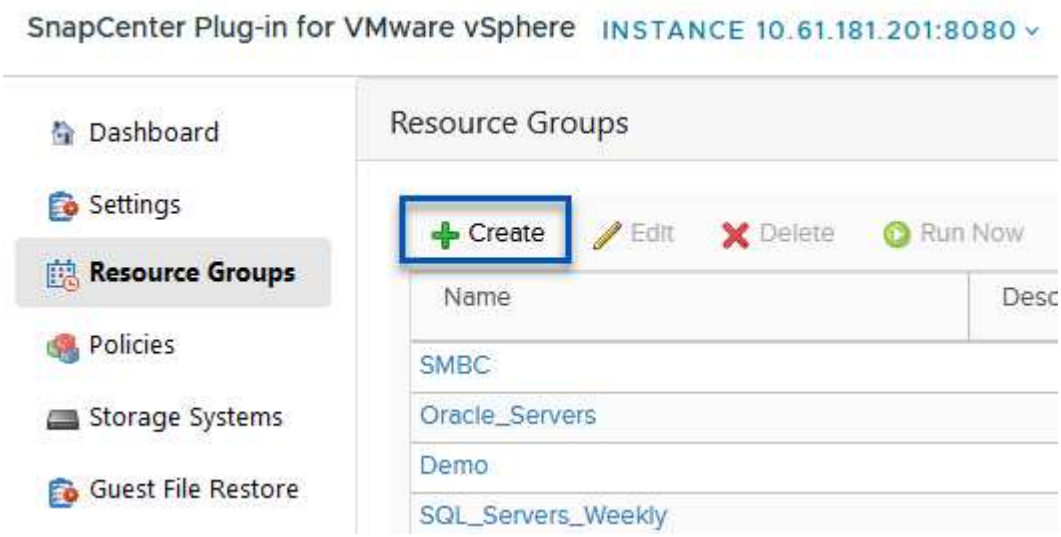
Crear grupos de recursos

Los grupos de recursos contienen los almacenes de datos y las máquinas virtuales que se incluirán en un trabajo de backup, junto con la política y la programación de backup asociadas.

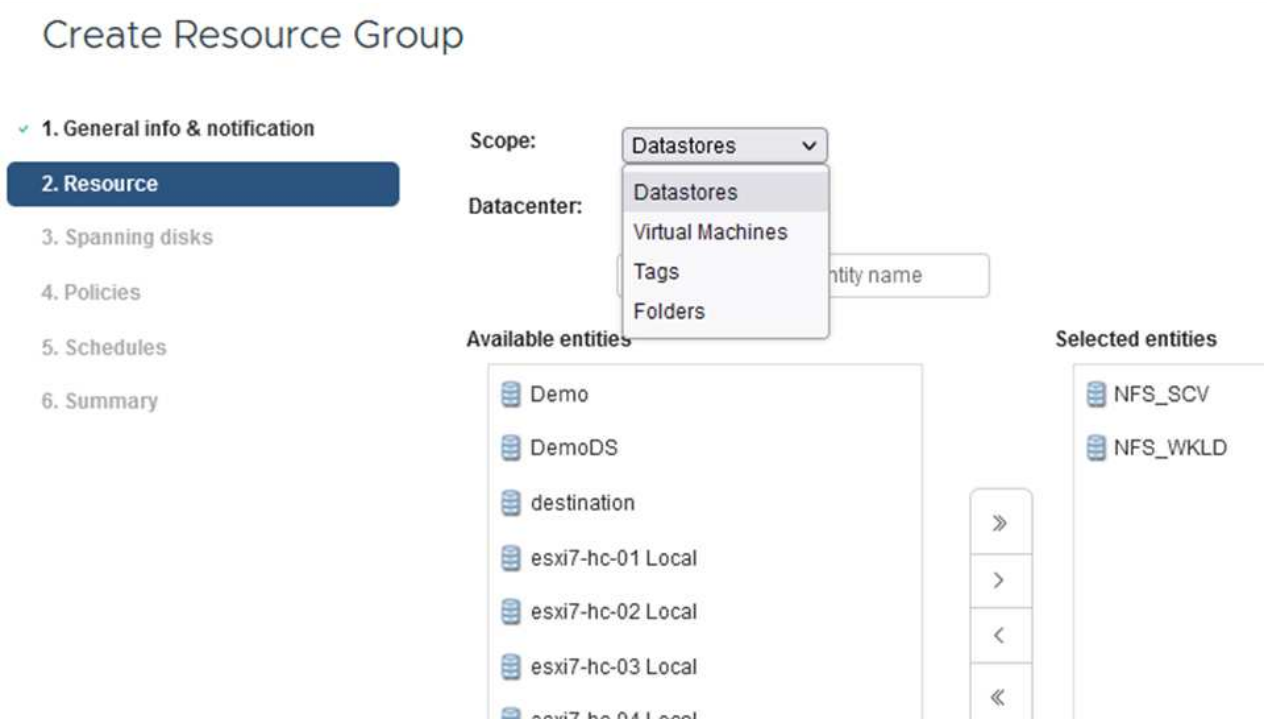
Revise la "Crear grupos de recursos" sección de la documentación para más información.

Para crear grupos de recursos, complete los siguientes pasos.

1. En el plugin de SnapCenter para VMware vSphere, navegue hasta **Grupos de recursos** en el menú de la izquierda y haga clic en el botón **Crear**.

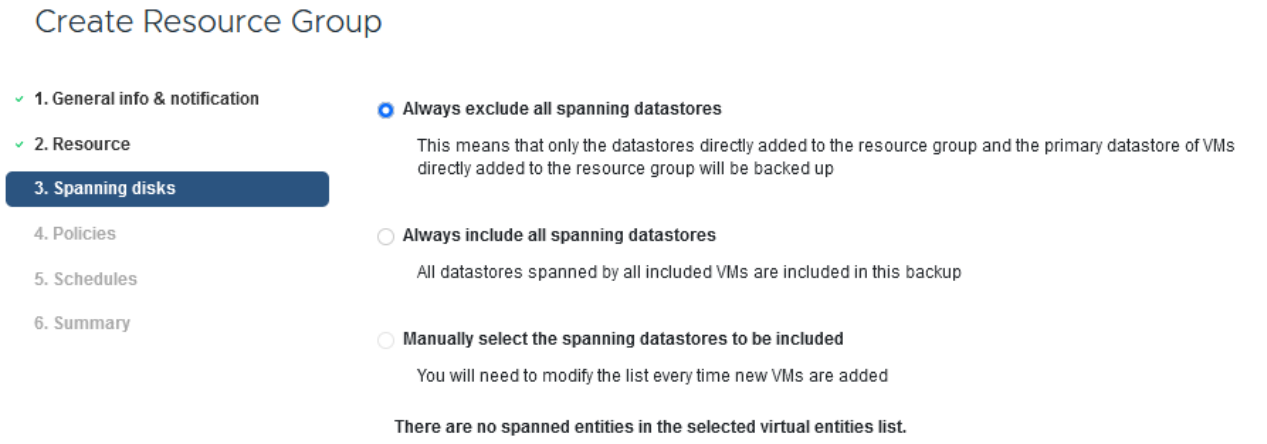


2. En el asistente Create Resource Group, escriba un nombre y una descripción para el grupo, así como la información necesaria para recibir notificaciones. Haga clic en **Siguiente**
3. En la página siguiente, seleccione los almacenes de datos y las máquinas virtuales que desean incluirse en el trabajo de copia de seguridad y luego haga clic en **Siguiente**.



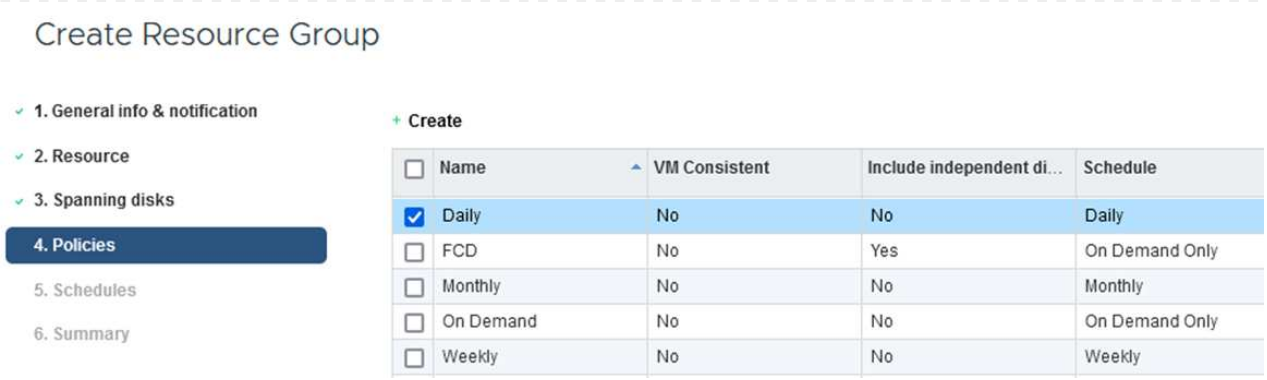
Puede seleccionar máquinas virtuales específicas o almacenes de datos completos. Independientemente del lugar que elija, se realiza el backup de todo el volumen (y el almacén de datos), ya que el backup es el resultado de tomar una snapshot del volumen subyacente. En la mayoría de los casos, es más fácil elegir todo el almacén de datos. Sin embargo, si desea limitar la lista de máquinas virtuales disponibles al restaurar, puede seleccionar solo un subconjunto de máquinas virtuales para realizar backups.

4. Elija opciones para ampliar almacenes de datos para máquinas virtuales con VMDK que residen en varios almacenes de datos y luego haga clic en **Siguiente**.



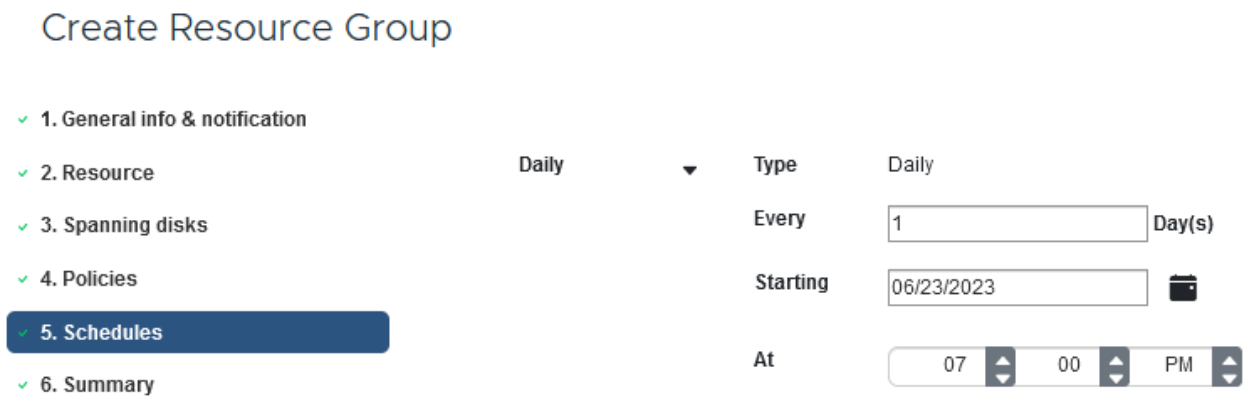
El backup y la recuperación de datos de BlueXP no admite actualmente el backup de máquinas virtuales con VMDK que abarquen varios almacenes de datos.

5. En la página siguiente, seleccione las políticas que se asociarán con el grupo de recursos y haga clic en **Siguiente**.



Al realizar un backup de las snapshots gestionadas de SCV en el almacenamiento de objetos mediante el backup y recuperación de BlueXP, cada grupo de recursos solo puede estar asociado con una sola política.

6. Seleccione un programa que determinará en qué momento se ejecutarán las copias de seguridad. Haga clic en **Siguiente**.

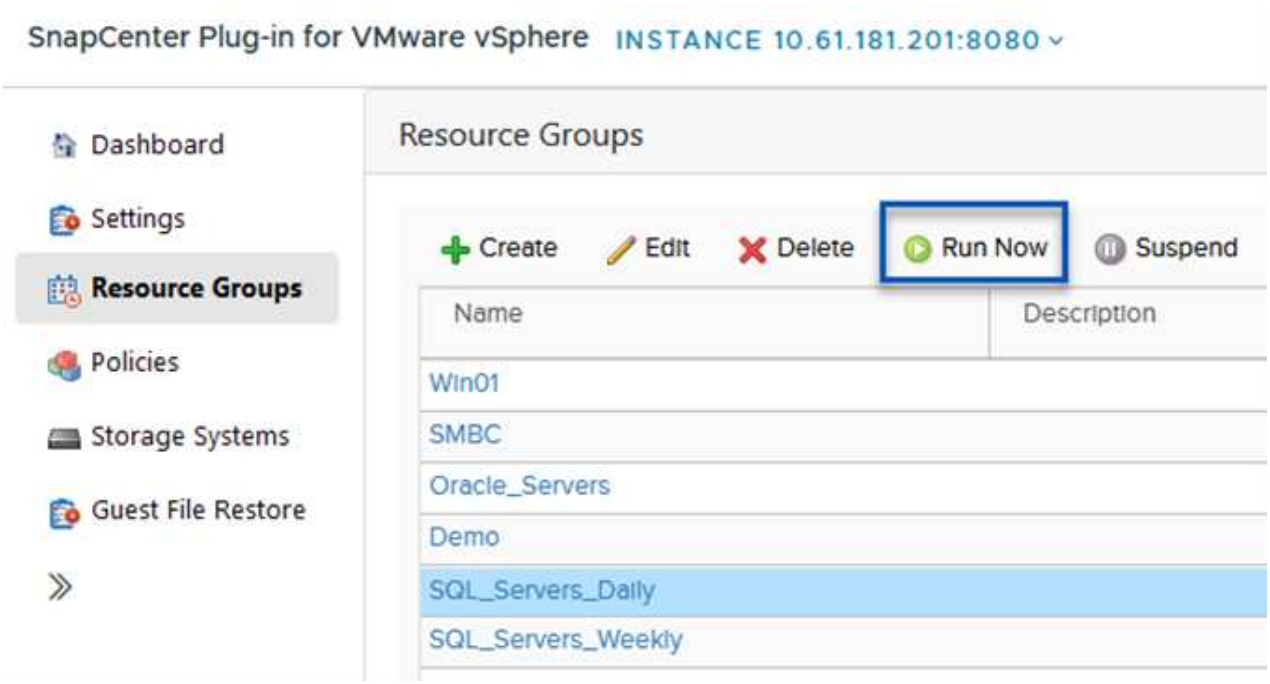


7. Finalmente, revise la página de resumen y luego en **Finish** para completar la creación del grupo de recursos.

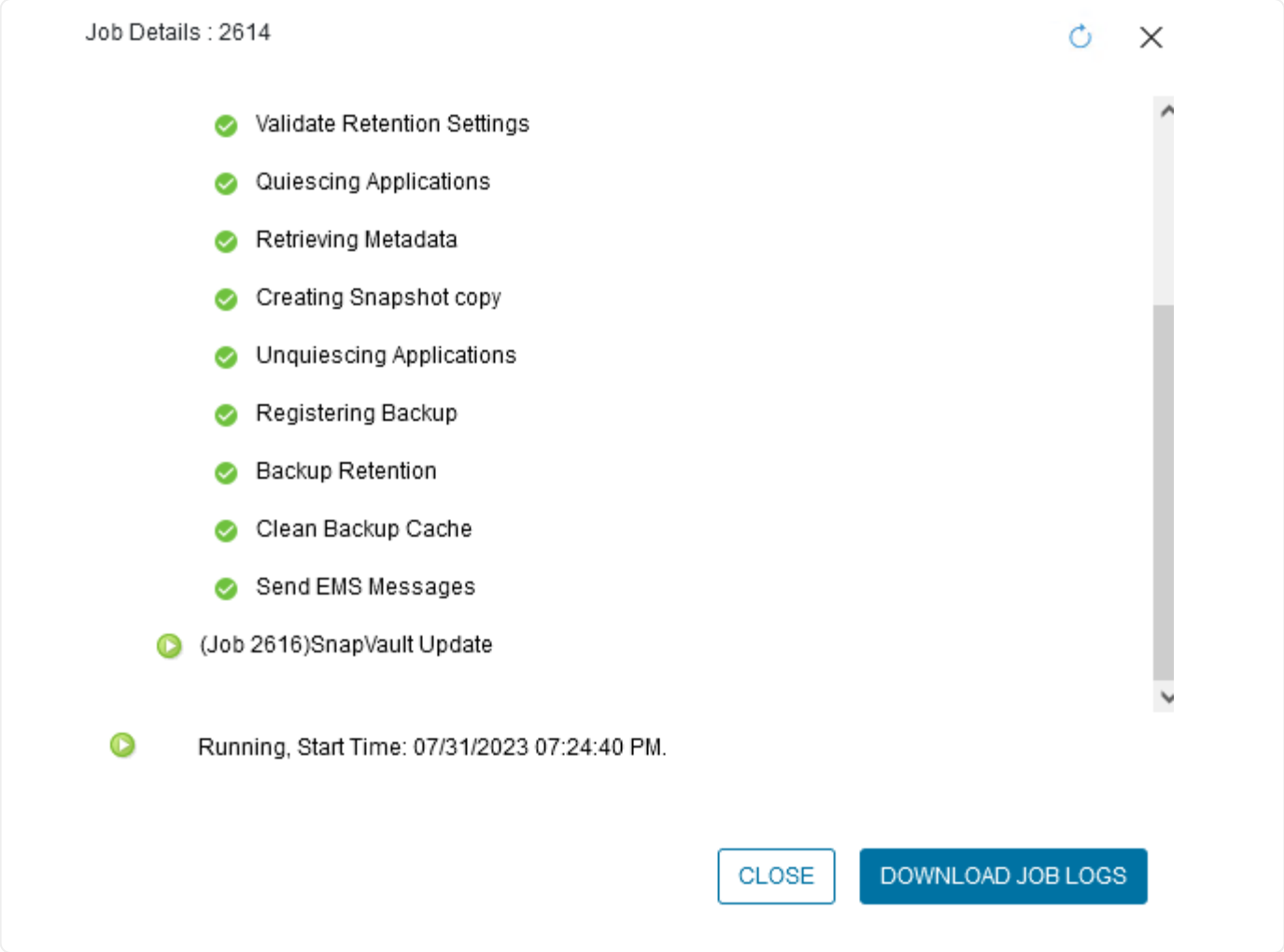
Ejecute una tarea de backup

En este paso final, ejecute un trabajo de copia de seguridad y supervise su progreso. Se debe completar correctamente al menos una tarea de backup en SCV antes de que se puedan detectar los recursos desde el backup y la recuperación de BlueXP.

1. En el plugin de SnapCenter para VMware vSphere, desplácese hasta **Resource Groups** en el menú de la izquierda.
2. Para iniciar una tarea de copia de seguridad, seleccione el grupo de recursos deseado y haga clic en el botón **Ejecutar ahora**.



3. Para supervisar el trabajo de copia de seguridad, navegue hasta **Dashboard** en el menú de la izquierda. En **Actividades recientes del trabajo**, haga clic en el número de ID del trabajo para supervisar el progreso del trabajo.



Configura backups en el almacenamiento de objetos en el backup y la recuperación de BlueXP

Para que BlueXP gestione la infraestructura de datos de forma eficaz, hace falta instalar antes un Connector. El conector ejecuta las acciones involucradas en la detección de recursos y la gestión de operaciones de datos.

Para obtener más información sobre el conector BlueXP, consulte "Más información sobre conectores" En la documentación de BlueXP.

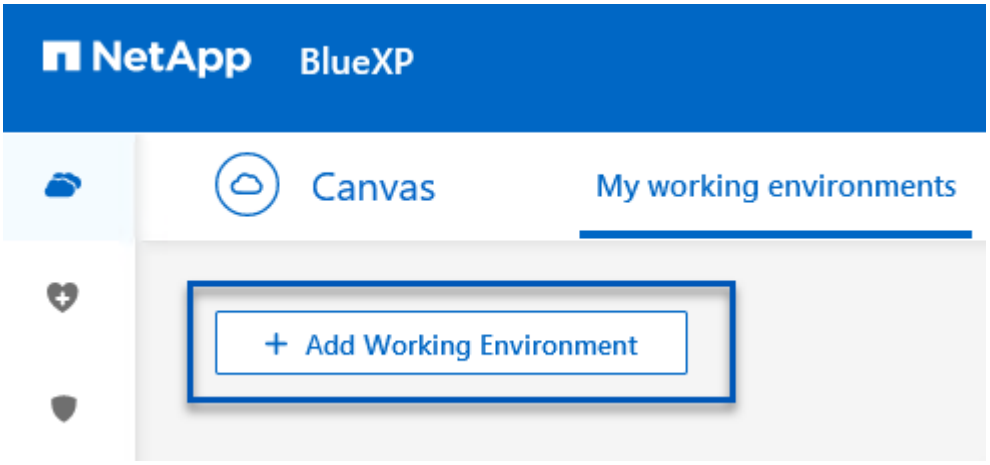
Una vez instalado el conector para el proveedor de nube que se está utilizando, se podrá ver una representación gráfica del almacenamiento de objetos desde Canvas.

Para configurar el backup y la recuperación de BlueXP en los datos de backup gestionados por SCV on-premises, complete los siguientes pasos:

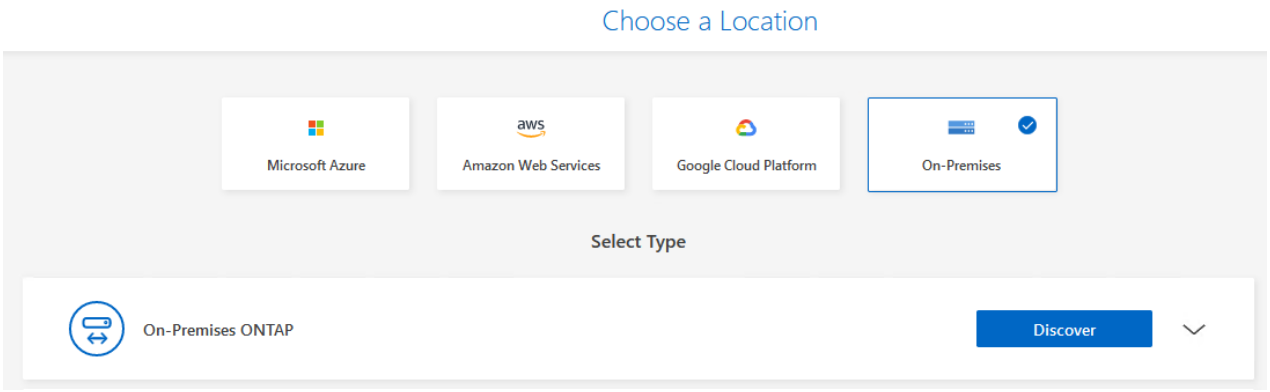
Agregue entornos de trabajo al lienzo

El primer paso es añadir los sistemas de almacenamiento de ONTAP on-premises a BlueXP

1. En el lienzo seleccione **Agregar entorno de trabajo** para comenzar.



2. Seleccione **on-premises** de la selección de ubicaciones y luego haga clic en el botón **Discover**.



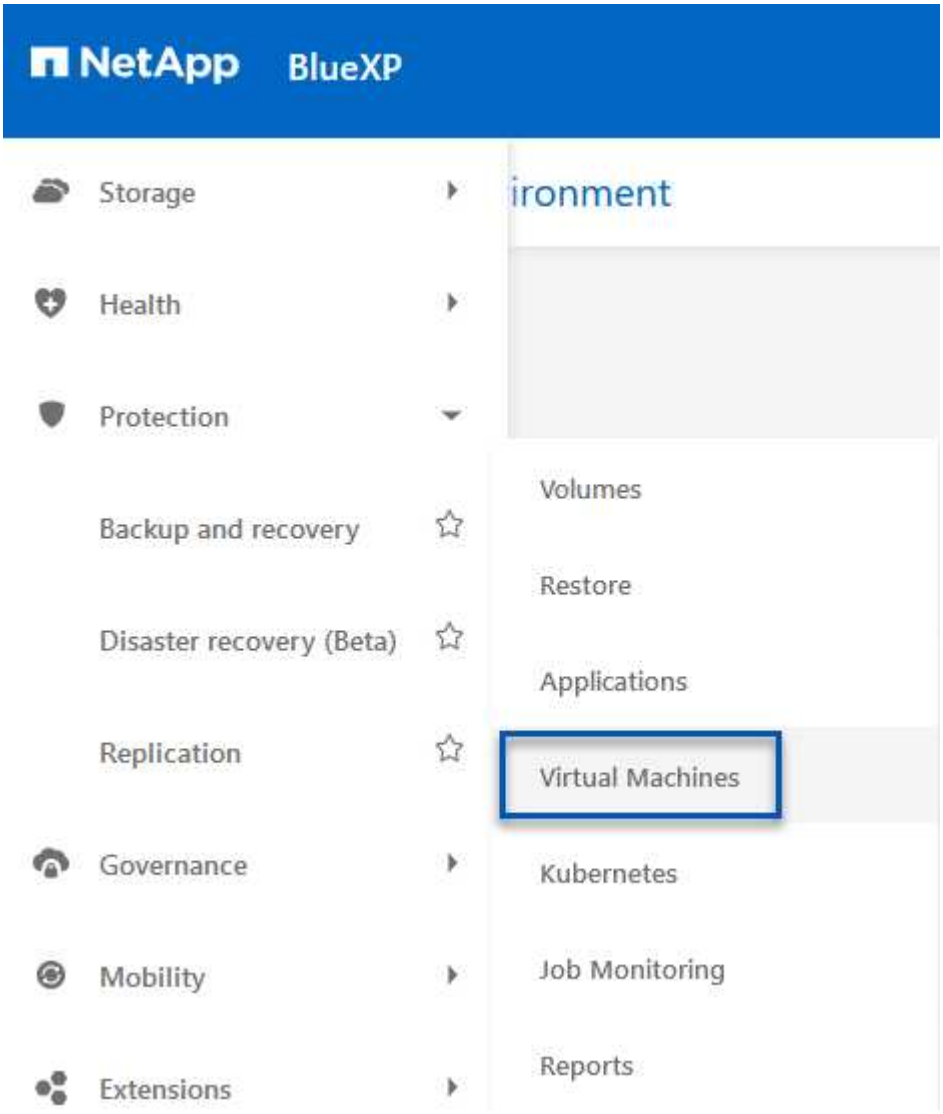
3. Rellene las credenciales del sistema de almacenamiento ONTAP y haga clic en el botón **Descubrir** para agregar el entorno de trabajo.


ONTAP Cluster IP
10.61.181.180
User Name
admin
Password

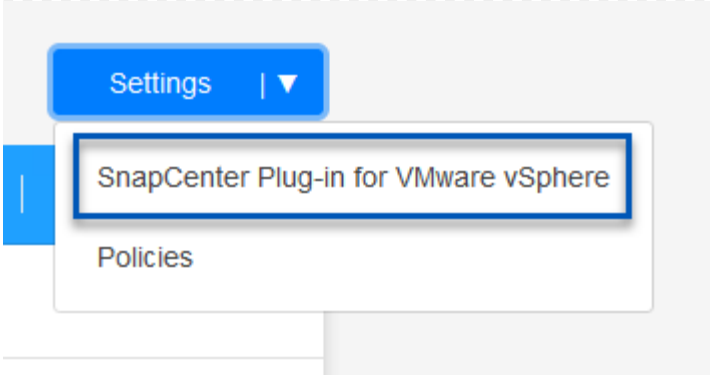
Detecte el dispositivo SCV local y vCenter

Para detectar el almacén de datos en las instalaciones y los recursos de máquinas virtuales, añada información del agente de datos SCV y las credenciales para el dispositivo de gestión de vCenter.

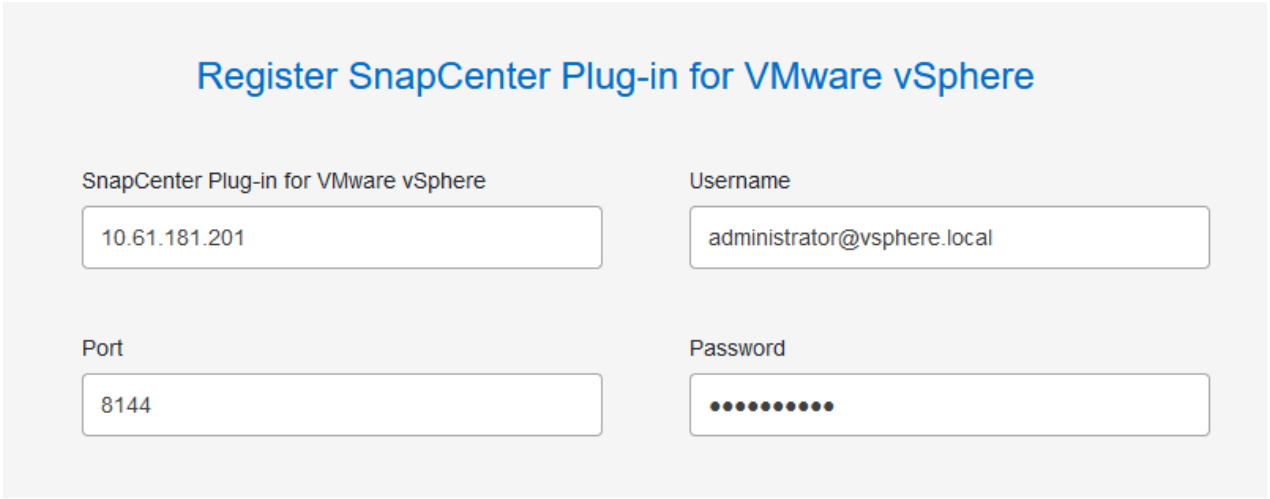
1. En el menú de la izquierda de BlueXP, seleccione **Protección > Copia de seguridad y recuperación > Máquinas virtuales**



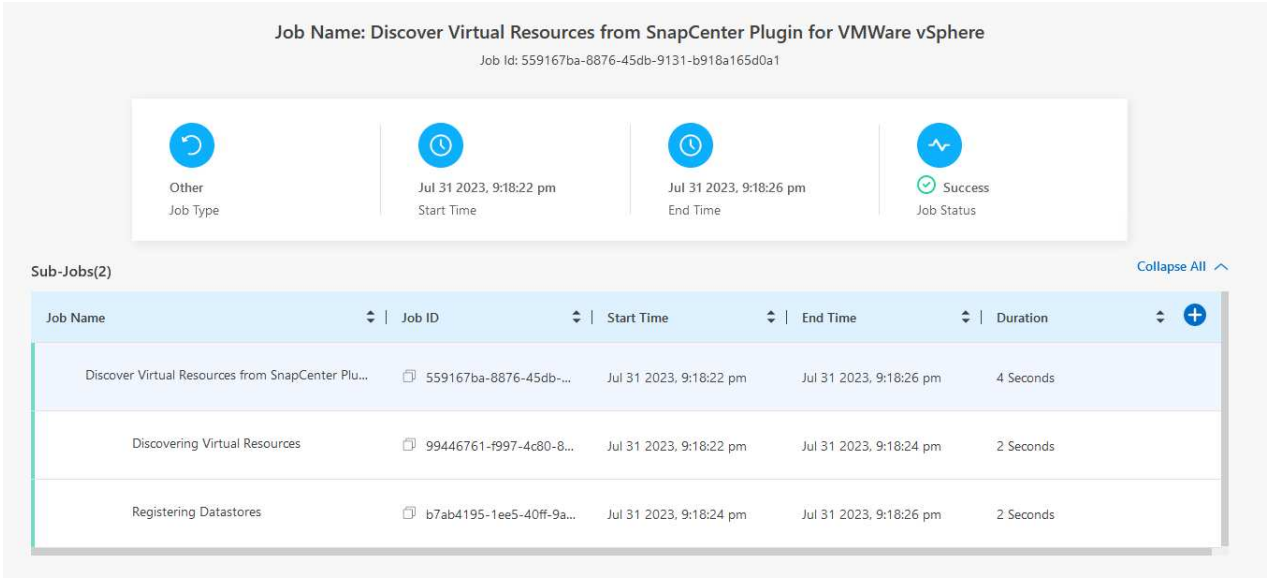
2. Desde la pantalla principal de Máquinas virtuales, acceda al menú desplegable **Configuración** y seleccione **SnapCenter Plug-in for VMware vSphere**.



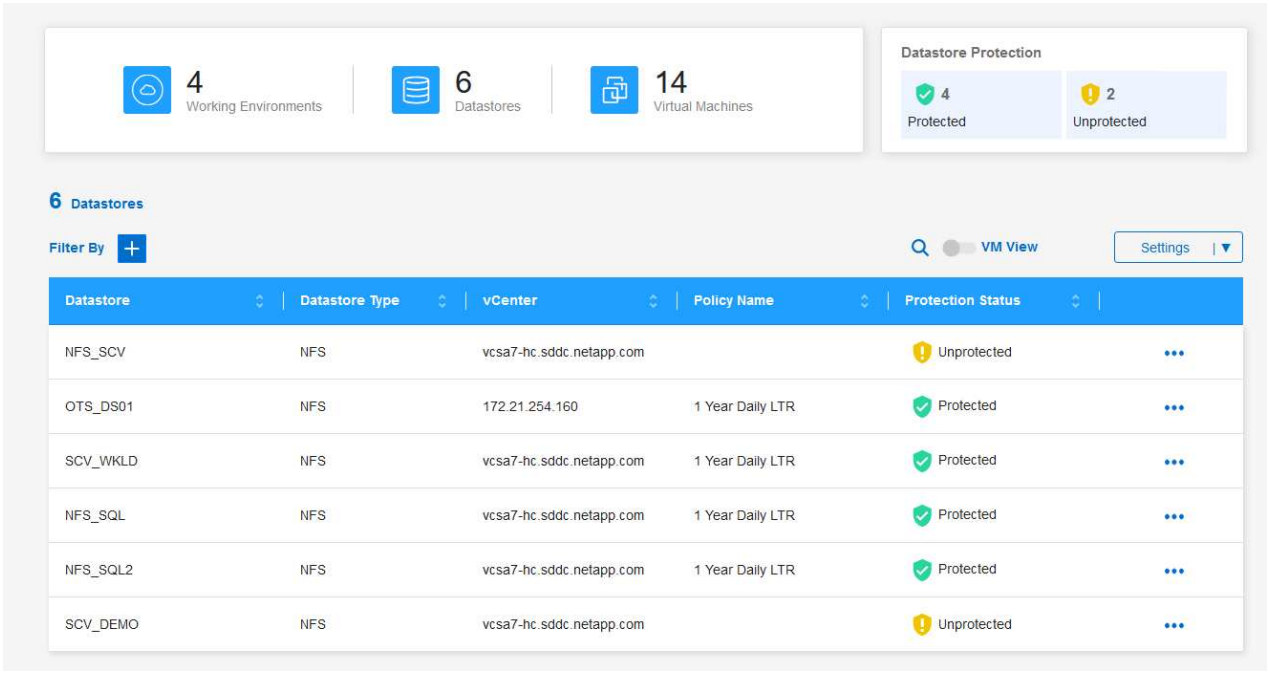
3. Haga clic en el botón **Registrar** y, a continuación, introduzca la dirección IP y el número de puerto para el dispositivo de complemento de SnapCenter y el nombre de usuario y la contraseña para el dispositivo de administración de vCenter. Haga clic en el botón **Registrar** para comenzar el proceso de descubrimiento.



4. El progreso de los trabajos se puede supervisar desde la pestaña Supervisión de trabajos.



5. Una vez completada la detección, podrá ver los almacenes de datos y las máquinas virtuales en todos los dispositivos SCV detectados.

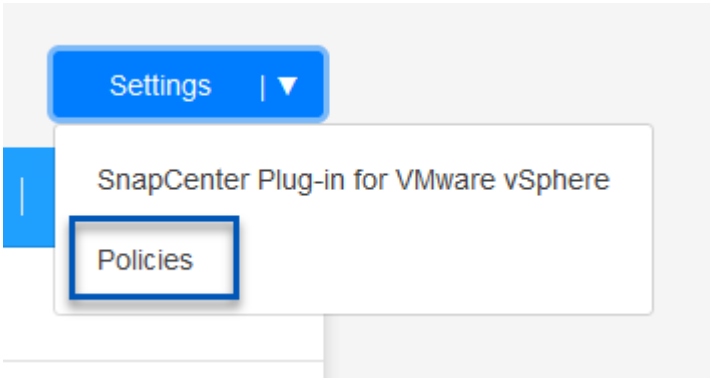

4
Working Environments
6
Datastores
14
Virtual Machines
Datastore Protection
4
Protected
2
Unprotected
6 Datastores
Filter By
VM View
Settings
Datastore
Datastore Type
vCenter
Policy Name
Protection Status
NFS_SCV
NFS
vcsa7-hc.sddc.netapp.com
Unprotected
OTS_DS01
NFS
172.21.254.160
1 Year Daily LTR
Protected
SCV_WKLD
NFS
vcsa7-hc.sddc.netapp.com
1 Year Daily LTR
Protected
NFS_SQL
NFS
vcsa7-hc.sddc.netapp.com
1 Year Daily LTR
Protected
NFS_SQL2
NFS
vcsa7-hc.sddc.netapp.com
1 Year Daily LTR
Protected
SCV_DEMO
NFS
vcsa7-hc.sddc.netapp.com
Unprotected

Cree políticas de backup de BlueXP

En el backup y recuperación de datos de BlueXP para máquinas virtuales, cree políticas que especifiquen el período de retención, el origen de backup y la política de archivado.

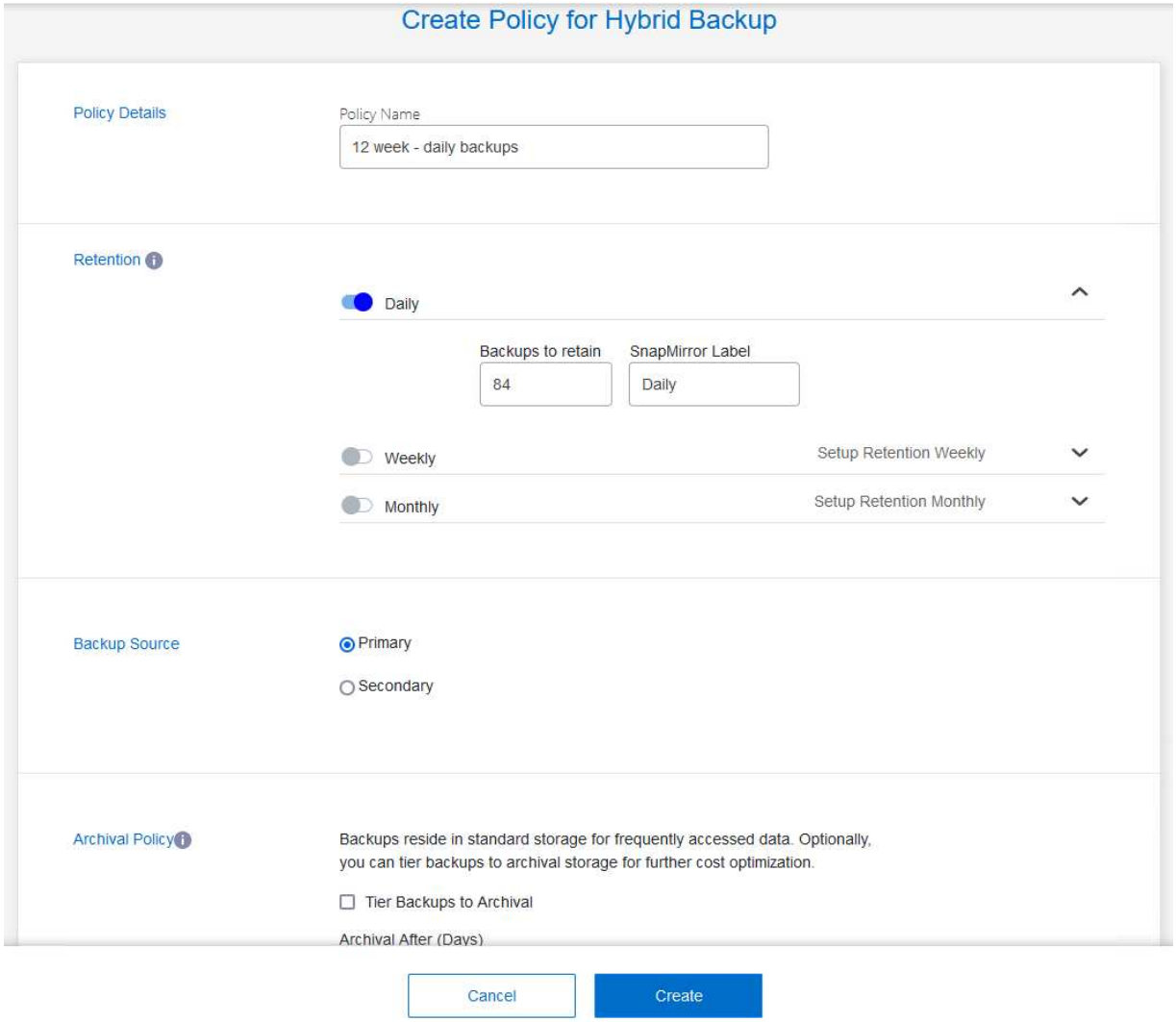
Para obtener más información sobre la creación de políticas, consulte "Crear una política para realizar backups de almacenes de datos".

1. Desde la página principal de copia de seguridad y recuperación de BlueXP para máquinas virtuales, accede al menú desplegable **Configuración** y selecciona **Políticas**.



2. Haga clic en **Crear política** para acceder a la ventana **Crear política para copia de seguridad híbrida**.

   a. Agregue un nombre para la política
   b. Seleccione el período de retención deseado
   c. Seleccione si se asignarán los backups del sistema de almacenamiento de ONTAP principal o secundario en las instalaciones
   d. Opcionalmente, especifique tras qué período de tiempo se organizarán los backups en niveles en el almacenamiento archivado para reducir aún más los costes.



La etiqueta de SnapMirror introducida aquí se utiliza también para identificar qué backups aplicarán la política. El nombre de etiqueta debe coincidir con el nombre de etiqueta en la política de SCV en las instalaciones correspondiente.

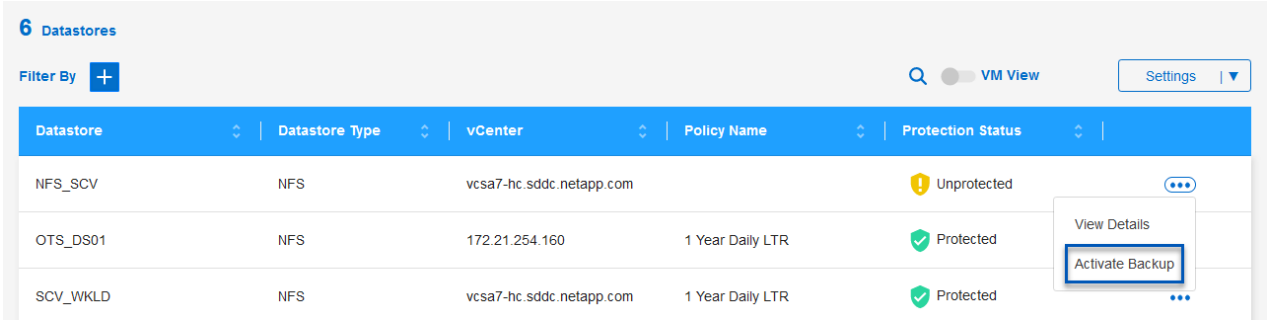
3. Haga clic en **Crear** para completar la creación de la política.

Backup de almacenes de datos en Amazon Web Services

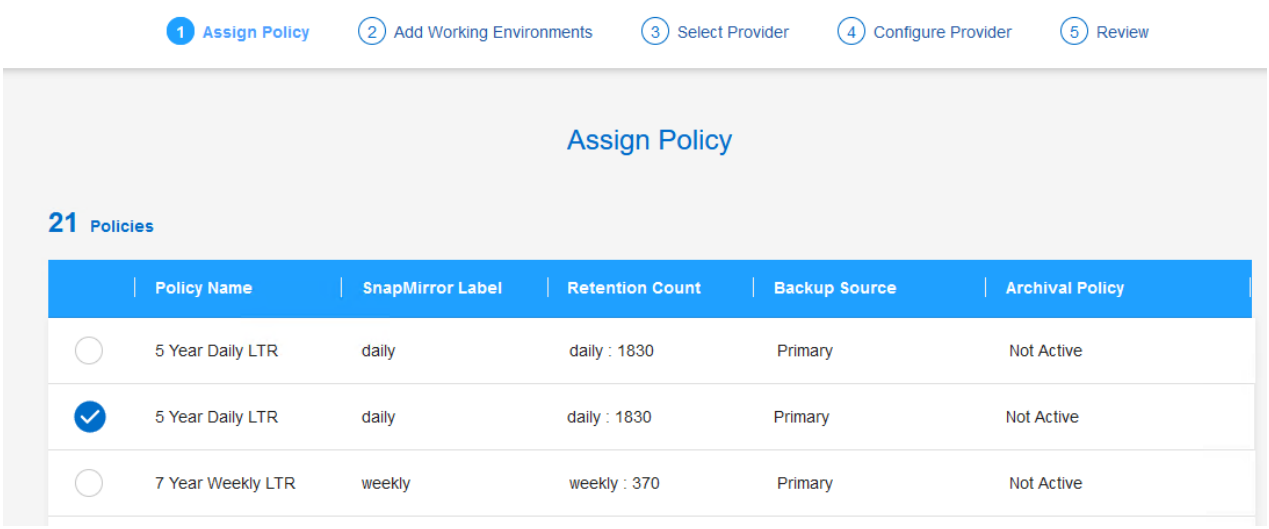
El paso final es activar la protección de datos para los almacenes de datos individuales y los equipos virtuales. Los siguientes pasos describen cómo activar copias de seguridad en AWS.

Para obtener más información, consulte "Backup de almacenes de datos en Amazon Web Services".

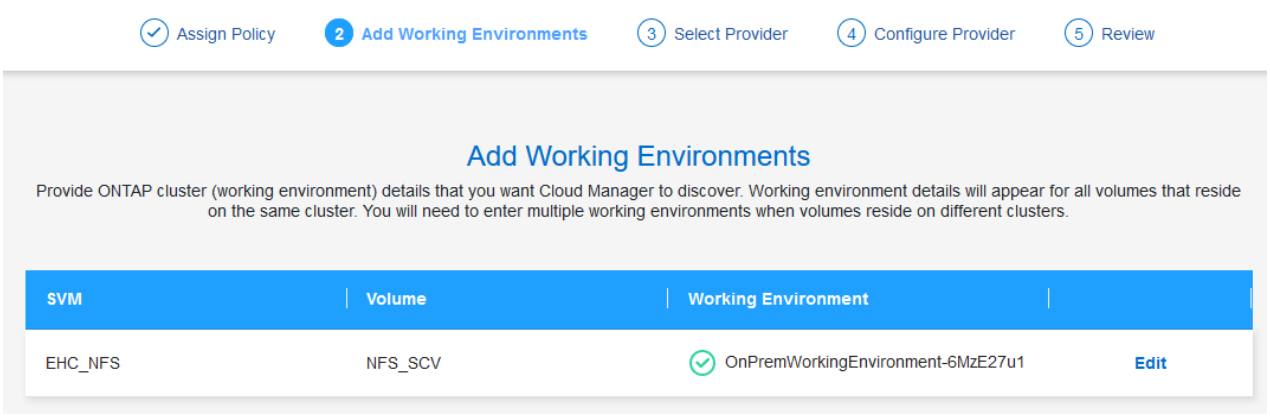
1. Desde la página principal de copia de seguridad y recuperación de BlueXP para máquinas virtuales, accede a la lista desplegable de configuración para que se realice una copia de seguridad del almacén de datos y selecciona **Activar copia de seguridad**.



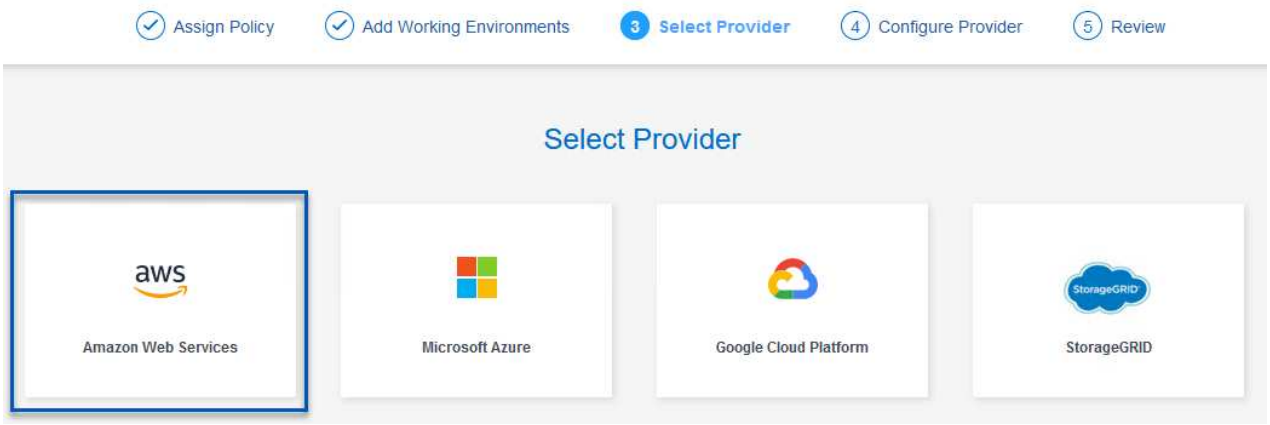
2. Asigne la política que se utilizará para la operación de protección de datos y haga clic en **Siguiente**.



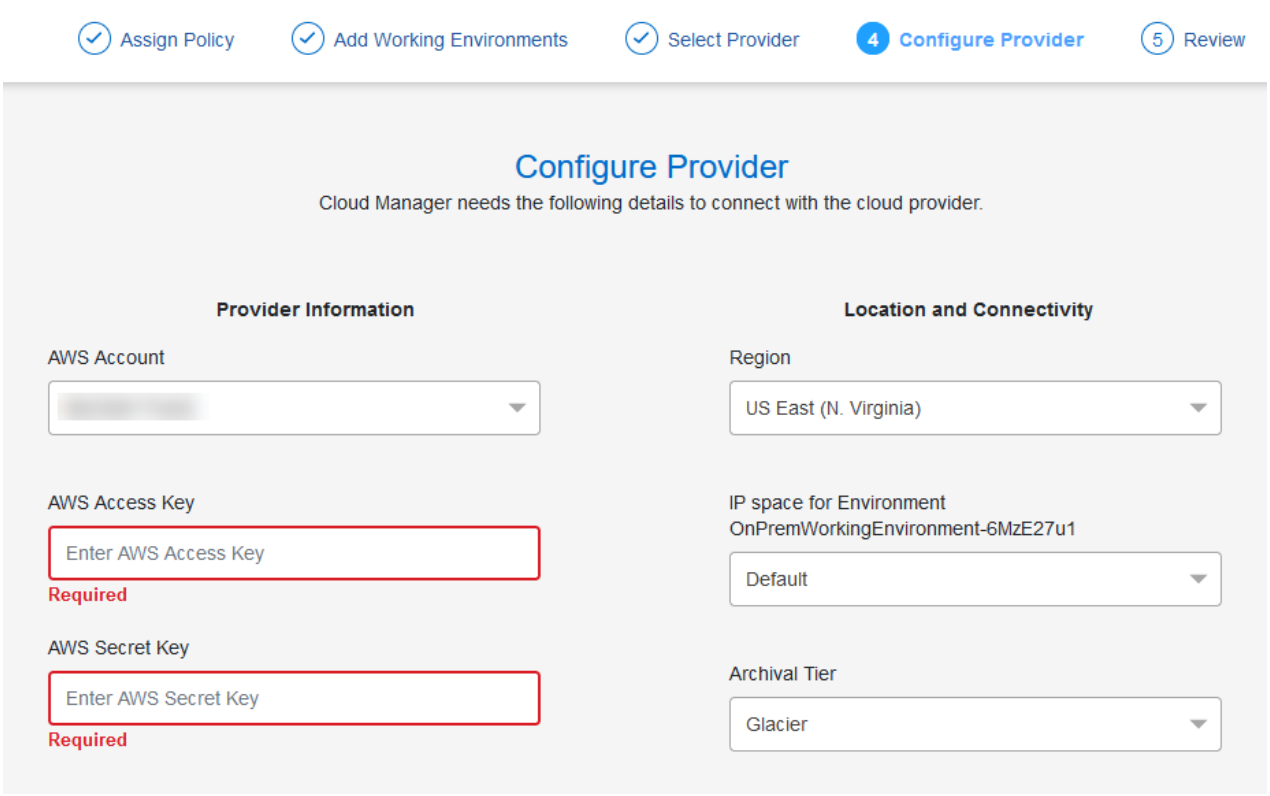
3. En la página **Agregar entornos de trabajo**, el almacén de datos y el entorno de trabajo con una marca de verificación deben aparecer si el entorno de trabajo se ha detectado previamente. Si el entorno de trabajo no se ha detectado anteriormente, puede agregarlo aquí. Haga clic en **Siguiente** para continuar.



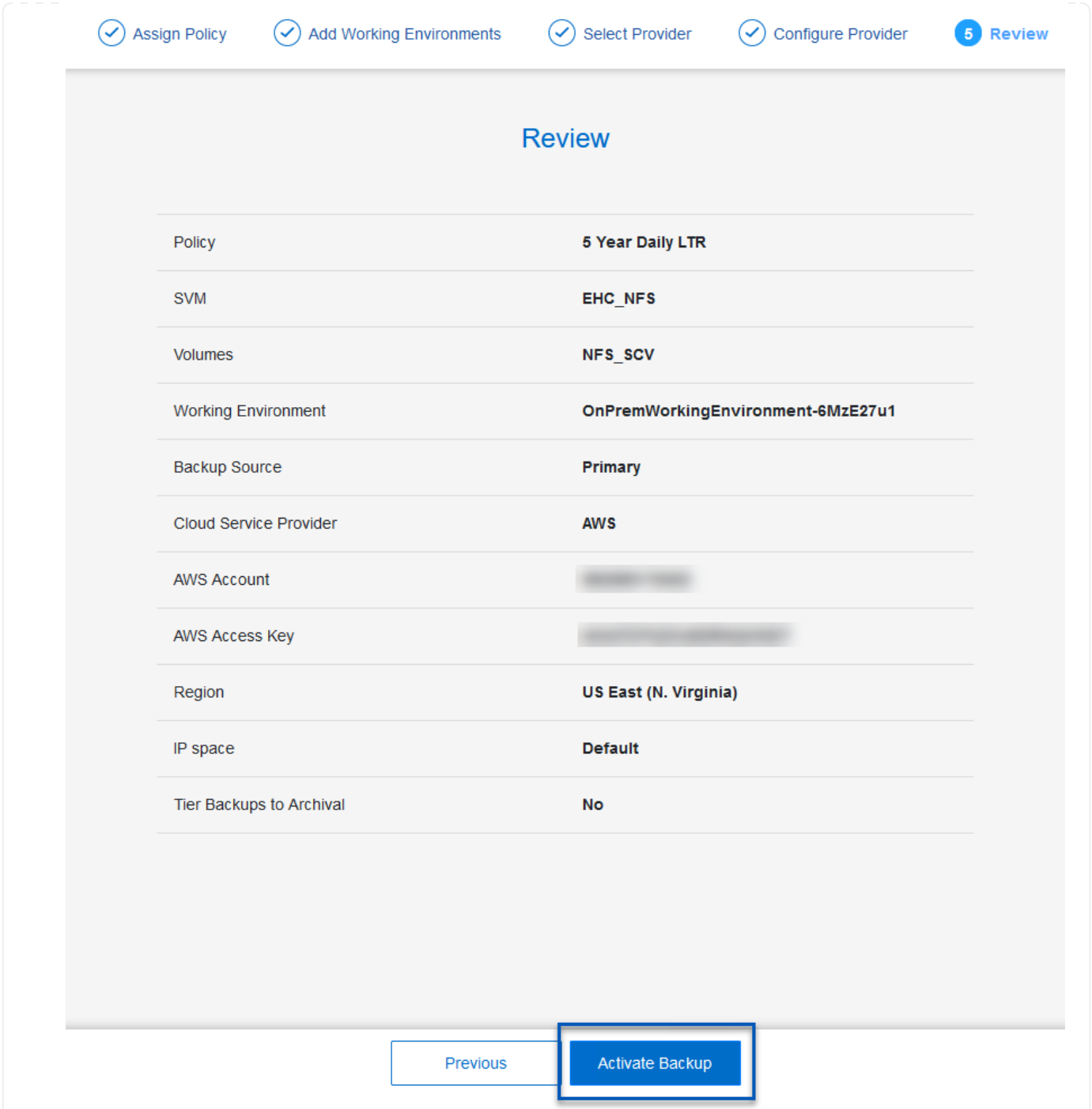
4. En la página **Seleccionar proveedor**, haga clic en AWS y luego haga clic en el botón **Siguiente** para continuar.



5. Rellene la información de credenciales específica del proveedor para AWS, incluida la clave de acceso de AWS y la clave secreta, la región y el nivel de archivado que se va a utilizar. Además, seleccione el espacio IP de ONTAP para el sistema de almacenamiento de ONTAP en las instalaciones. Haga clic en **Siguiente**.



6. Por último, revise los detalles del trabajo de copia de seguridad y haga clic en el botón **Activar copia de seguridad** para iniciar la protección de datos del almacén de datos.



En este punto, la transferencia de datos puede no comenzar inmediatamente. El backup y la recuperación de BlueXP analiza todas las copias Snapshot pendientes cada hora y luego las transfiere al almacenamiento de objetos.

Restauración de máquinas virtuales en caso de pérdida de datos

Garantizar la protección de los datos es tan solo un aspecto de la protección de datos completa. Igualmente importante es la capacidad de restaurar datos rápidamente desde cualquier ubicación en caso de pérdida de datos o ataque de ransomware. Esta funcionalidad es esencial para mantener operaciones empresariales transparentes y cumplir con los objetivos de punto de recuperación.

NetApp ofrece una estrategia 3-2-1 altamente adaptable que proporciona un control personalizado de los programas de retención en las ubicaciones de almacenamiento principal, secundario y de objetos. Esta estrategia proporciona la flexibilidad necesaria para adaptar los enfoques de protección de datos a necesidades específicas.

En esta sección se ofrece una descripción general del proceso de restauración de datos desde el plugin de SnapCenter para VMware vSphere y backup y recuperación de BlueXP para máquinas virtuales.

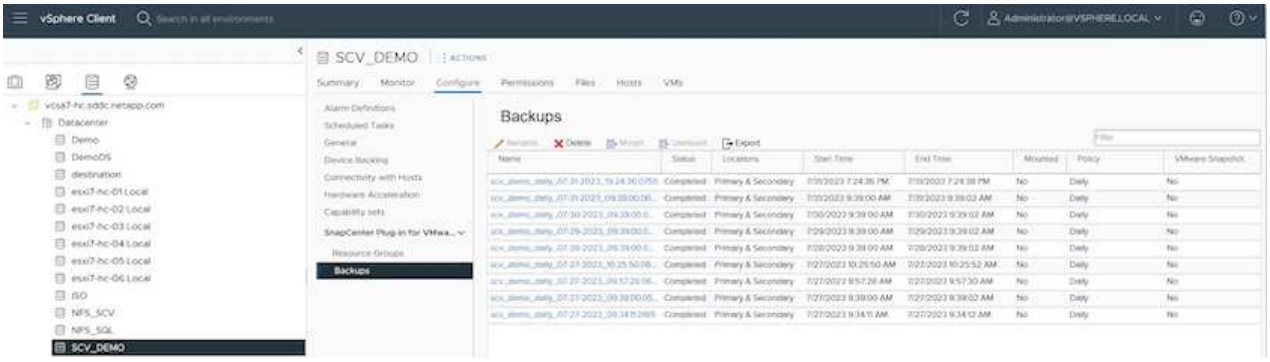
Restaurar máquinas virtuales desde el plugin de SnapCenter para VMware vSphere

Para esta solución, se restauraron las máquinas virtuales en ubicaciones originales y alternativas. No todos los aspectos de las funcionalidades de restauración de datos de SCV se tratarán en esta solución. Para obtener información detallada sobre todo lo que SCV tiene para ofrecer, consulte la "Restaurar máquinas virtuales desde backups" en la documentación del producto.

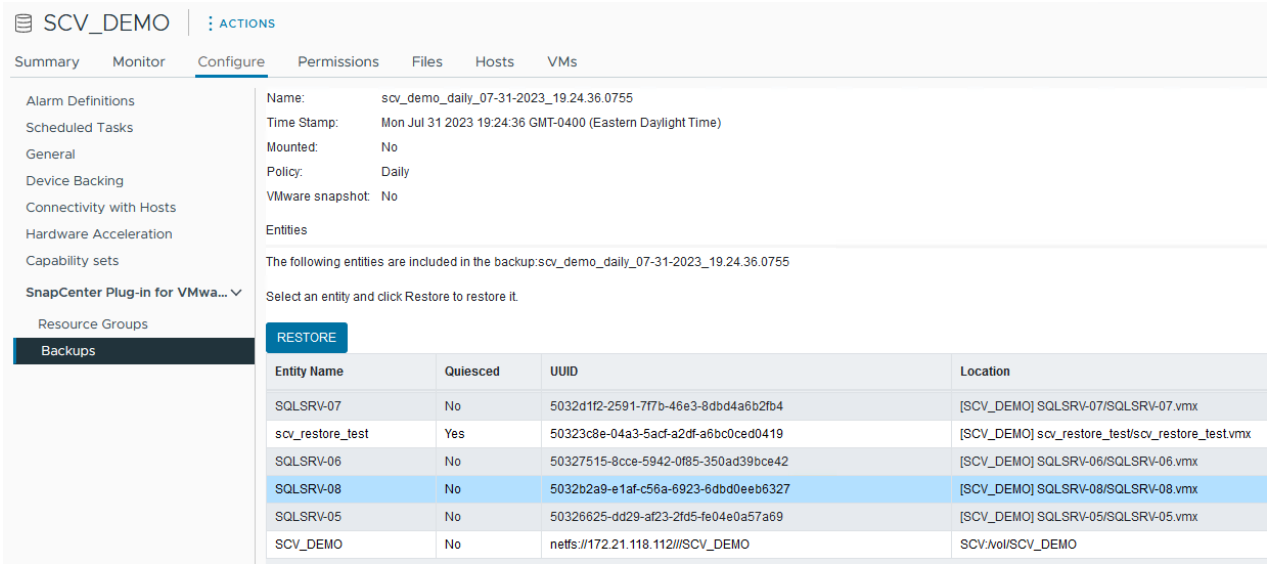
Restaurar máquinas virtuales desde SCV

Complete los siguientes pasos para restaurar una restauración de máquina virtual a partir de un almacenamiento principal o secundario.

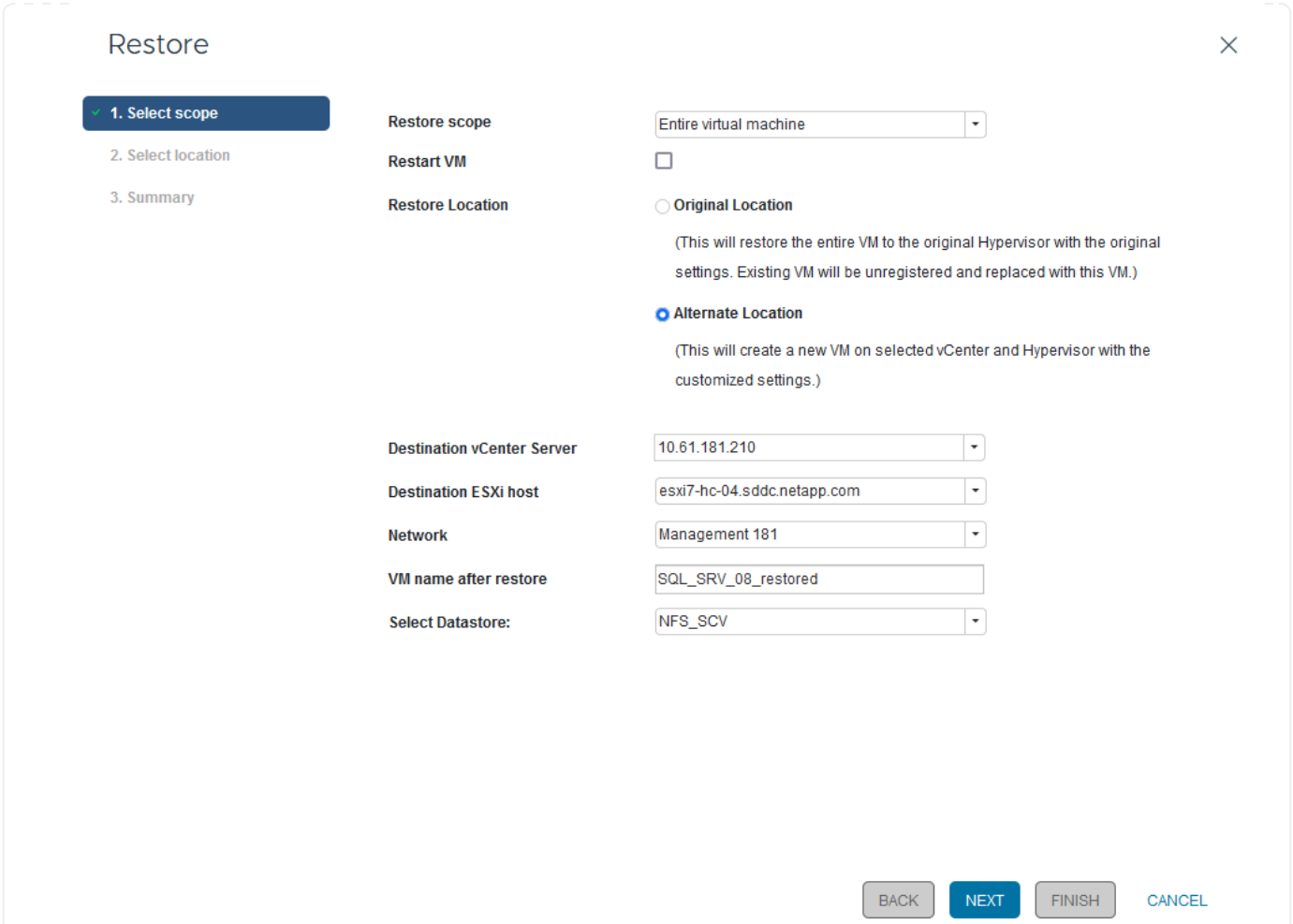
1. Desde el cliente de vCenter, navegue hasta **Inventory > Storage** y haga clic en el almacén de datos que contiene las máquinas virtuales que desea restaurar.
2. Desde la pestaña **Configure**, haga clic en **backups** para acceder a la lista de copias de seguridad disponibles.



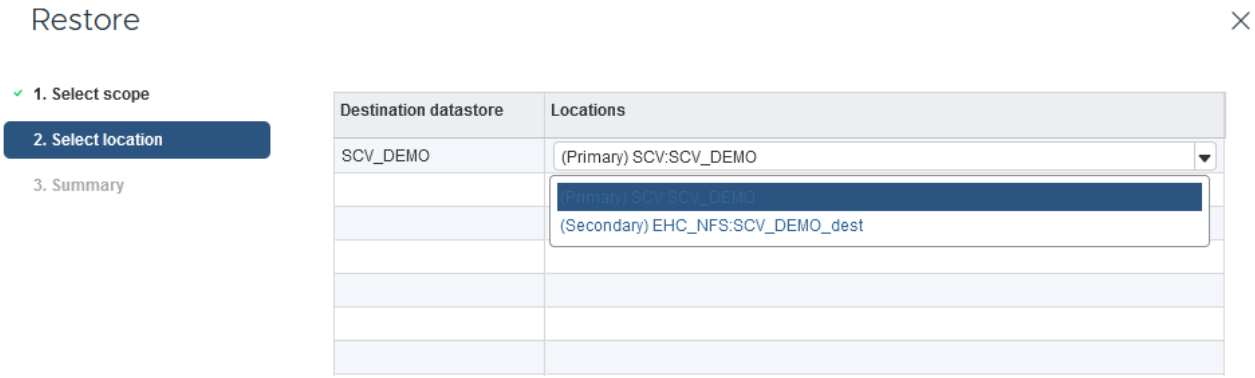
3. Haga clic en un backup para acceder a la lista de máquinas virtuales y, a continuación, seleccione una máquina virtual para restaurar. Haga clic en **Restaurar**.



4. En el asistente Restore, seleccione para restaurar toda la máquina virtual o un VMDK específico. Seleccione para instalar en la ubicación original o la ubicación alternativa, proporcione el nombre de máquina virtual después de la restauración y el almacén de datos de destino. Haga clic en **Siguiente**.



5. Seleccione realizar un backup desde la ubicación del almacenamiento principal o secundario.



6. Por último, revise un resumen del trabajo de copia de seguridad y haga clic en Finalizar para comenzar el proceso de restauración.

Restaurar máquinas virtuales a partir de backup y recuperación de datos de BlueXP para máquinas virtuales

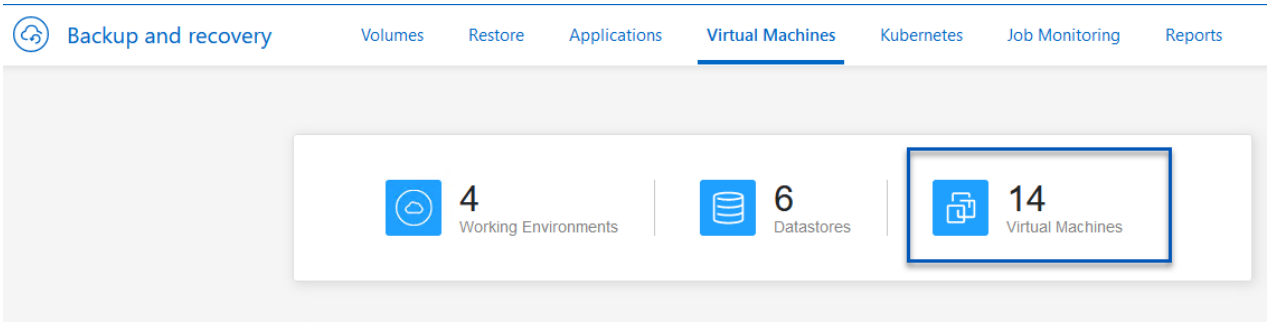
El backup y recuperación de datos de BlueXP para máquinas virtuales permite restaurar las máquinas virtuales a su ubicación original. Para acceder a las funciones de restauración a través de la consola web de BlueXP.

Para obtener más información, consulte "Restaure datos de máquinas virtuales desde el cloud".

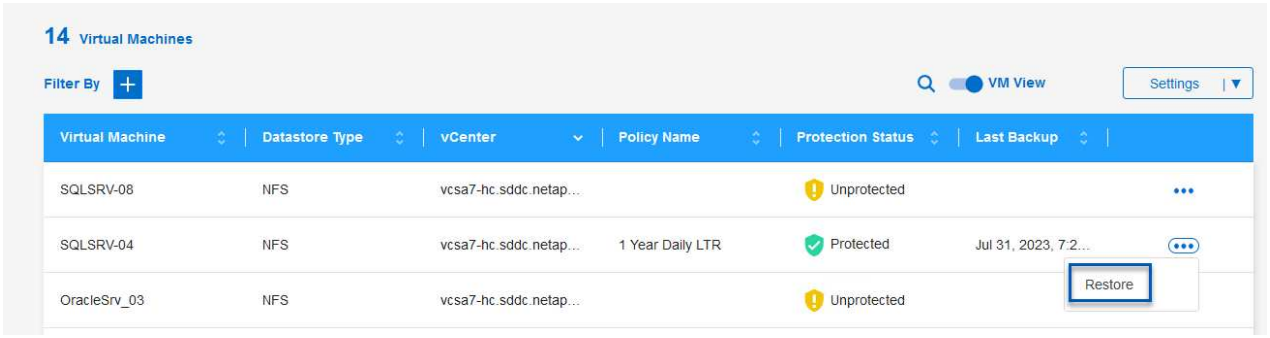
Restaura las máquinas virtuales desde el backup y la recuperación de BlueXP

Para restaurar una máquina virtual a partir de backup y recuperación de BlueXP, lleve a cabo los siguientes pasos.

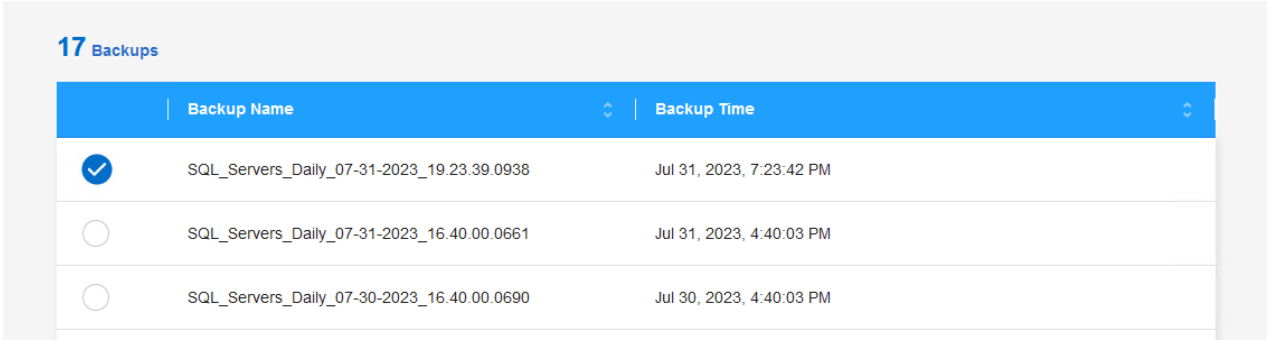
1. Vaya a **Protección > Copia de seguridad y recuperación > Máquinas virtuales** y haga clic en Máquinas virtuales para ver la lista de máquinas virtuales disponibles para restaurar.



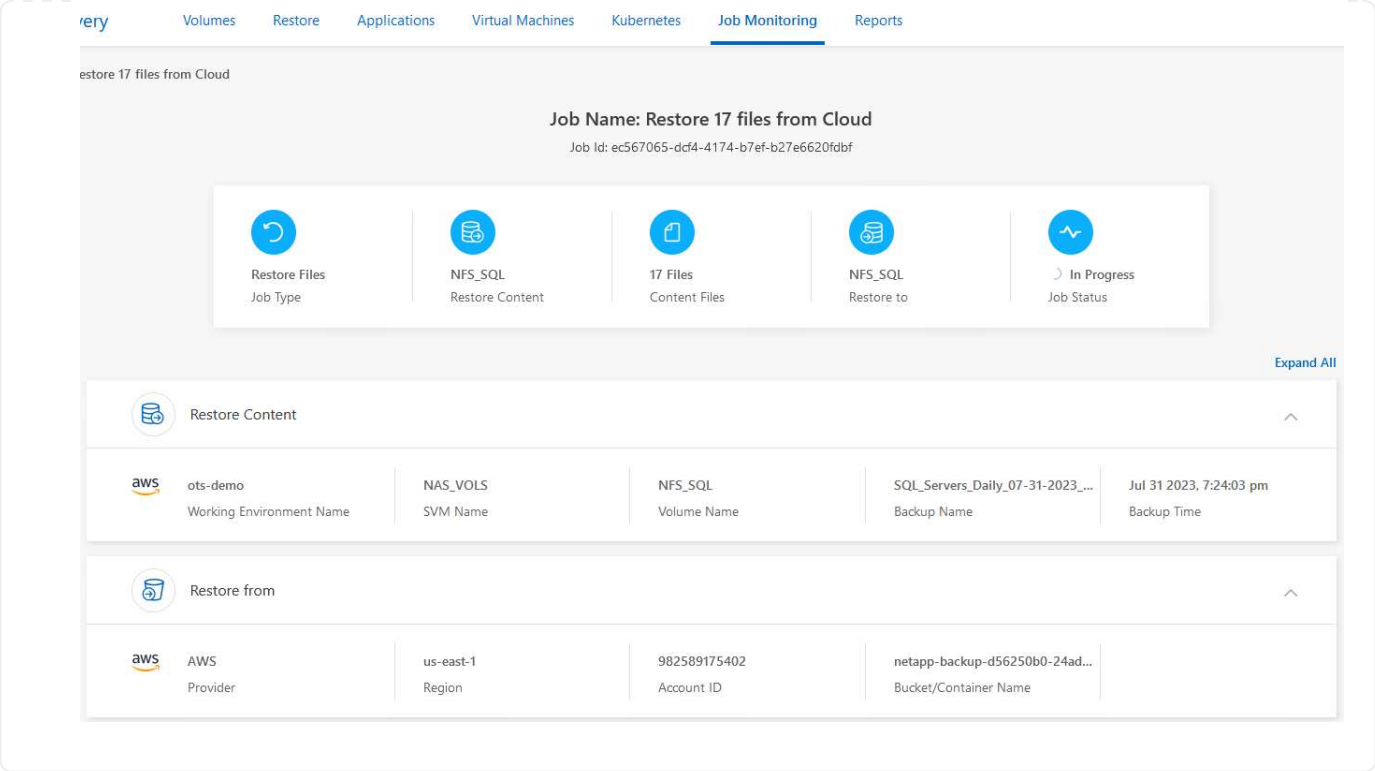
2. Acceda al menú desplegable de configuración de la máquina virtual que se va a restaurar y seleccione



3. Seleccione la copia de seguridad para restaurar y haga clic en **Siguiente**.



4. Revise un resumen del trabajo de copia de seguridad y haga clic en **Restaurar** para iniciar el proceso de restauración.
5. Supervise el progreso del trabajo de restauración desde la pestaña **Job Monitoring**.



Conclusión

La estrategia de backup 3-2-1, cuando se implementa con el complemento SnapCenter para VMware vSphere y backup y recuperación de datos BlueXP para máquinas virtuales, ofrece una solución sólida, fiable y rentable para la protección de datos. Esta estrategia no solo garantiza la redundancia de datos y la accesibilidad, sino que también proporciona la flexibilidad de restaurar datos desde cualquier ubicación y tanto desde sistemas de almacenamiento de ONTAP on-premises como desde el almacenamiento de objetos basado en la nube.

El caso de uso que se presenta en esta documentación se centra en las tecnologías de protección de datos demostradas que destacan la integración entre NetApp, VMware y los principales proveedores de cloud. El complemento de SnapCenter para VMware vSphere se integra sin problemas con VMware vSphere, lo que permite una gestión eficiente y centralizada de las operaciones de protección de datos. Esta integración optimiza los procesos de respaldo y recuperación para máquinas virtuales, lo que permite operaciones sencillas de programación, supervisión y restauración flexibles dentro del ecosistema VMware. El backup y recuperación de datos de BlueXP para máquinas virtuales ofrece un (1) en 3-2-1 al proporcionar backups seguros y aislados de datos de máquinas virtuales al almacenamiento de objetos basado en la nube. La interfaz intuitiva y el flujo de trabajo lógico proporcionan una plataforma segura para el archivado a largo plazo de datos críticos.

Información adicional

Para obtener más información sobre las tecnologías presentadas en esta solución, consulte la siguiente información adicional.

- "Documentación del plugin de SnapCenter para VMware vSphere"
- "Documentación de BlueXP"

Recuperación ante desastres con DRaaS de BlueXP

Descripción general

La recuperación ante desastres es lo más importante en la mente de cualquier administrador de VMware. Dado que VMware encapsula servidores completos en una serie de archivos que componen la máquina virtual, los administradores aprovechan las técnicas basadas en almacenamiento de bloques, como clones, copias Snapshot y réplicas para proteger estos equipos virtuales. Las cabinas de ONTAP ofrecen replicación integrada para transferir datos de volúmenes y, por lo tanto, los equipos virtuales que residen en los LUN de almacén de datos designados, desde un sitio a otro. DRaaS de BlueXP se integra con vSphere y automatiza todo el flujo de trabajo para obtener una conmutación al respaldo y una conmutación de retorno tras recuperación fluidas en caso de desastre. Combinando la replicación del almacenamiento con la automatización inteligente, los administradores cuentan ahora con una forma gestionable, no solo para configurar, automatizar y probar planes de recuperación ante desastres, sino que también ofrece la forma de ejecutarlos fácilmente en caso de desastre.

La mayoría de las partes que consumen mucho tiempo de una conmutación por error en recuperación ante desastres en un entorno VMware vSphere es la ejecución de los pasos necesarios para inventariar, registrar, reconfigurar y encender las máquinas virtuales en el centro de recuperación ante desastres. Una solución ideal tiene un objetivo de punto de recuperación bajo (medido en minutos) y un objetivo de tiempo de recuperación bajo (medido en minutos y horas). Un factor que a menudo se pasa por alto en una solución de recuperación ante desastres es la posibilidad de probar la solución de recuperación ante desastres con eficiencia a intervalos periódicos.

Para diseñar una solución de recuperación ante desastres, tenga en cuenta los siguientes factores:

- El objetivo de tiempo de recuperación. El objetivo de tiempo de recuperación es la rapidez con la que una empresa puede recuperarse de un desastre o, más concretamente, el tiempo que se tarda en ejecutar el proceso de recuperación para volver a garantizar la disponibilidad de los servicios empresariales.
- El objetivo de punto de recuperación (RPO). El objetivo de punto de recuperación es la antigüedad de los datos recuperados una vez que se han puesto a disposición, en relación con el momento en que ocurrió el desastre.
- Escalabilidad y adaptabilidad. Este factor incluye la posibilidad de aumentar los recursos de almacenamiento incrementalmente a medida que aumenta la demanda.

Para obtener más información técnica sobre las soluciones disponibles, consulte:

- "Recuperación ante desastres mediante DRaaS de BlueXP para almacenes de datos NFS"
- "Recuperación ante desastres mediante DRaaS de BlueXP para almacenes de datos de VMFS"

Recuperación ante desastres mediante DRaaS de BlueXP para almacenes de datos NFS

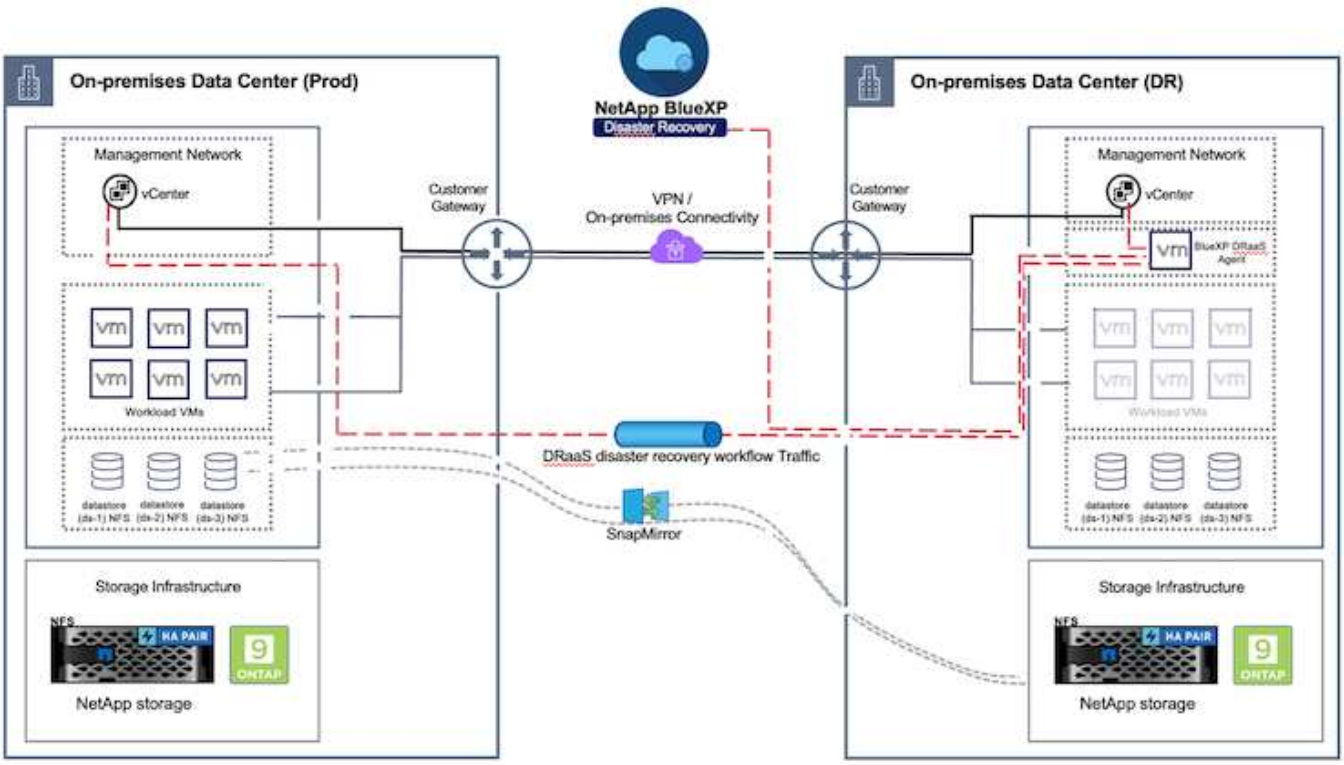
Implementar la recuperación ante desastres a través de la replicación a nivel de bloque desde el sitio de producción hasta el sitio de recuperación ante desastres es un método

flexible y rentable para proteger las cargas de trabajo contra interrupciones del sitio y eventos de corrupción de datos, como los ataques de ransomware. Mediante la replicación de NetApp SnapMirror, las cargas de trabajo de VMware que se ejecutan en sistemas de ONTAP en las instalaciones con almacén de datos NFS se pueden replicar en otro sistema de almacenamiento de ONTAP ubicado en un centro de datos de recuperación designado donde también se pone en marcha VMware.

Esta sección del documento describe la configuración de DRaaS de BlueXP para configurar la recuperación ante desastres para máquinas virtuales VMware on-premises en otro sitio designado. Como parte de esta configuración, la cuenta de BlueXP , el conector BlueXP , las cabinas ONTAP se agregaron dentro del espacio de trabajo de BlueXP para permitir la comunicación desde VMware vCenter con el sistema de almacenamiento de ONTAP. Además, este documento detalla cómo configurar la replicación entre sitios y cómo configurar y probar un plan de recuperación. La última sección contiene instrucciones para realizar una conmutación por error completa del sitio y cómo realizar una conmutación por error cuando el sitio principal se recupera y compra en línea.

Mediante el servicio de recuperación ante desastres de BlueXP , integrado en la consola de NetApp BlueXP , las empresas pueden descubrir con facilidad sus centros de VMware y almacenamiento ONTAP on-premises. Luego, las organizaciones pueden crear agrupaciones de recursos, crear un plan de recuperación de desastres, asociarlo con grupos de recursos y probar o ejecutar la conmutación por error y la conmutación de retorno tras recuperación. SnapMirror proporciona replicación de bloques a nivel de almacenamiento para mantener los dos sitios actualizados con cambios incrementales, lo que da como resultado un objetivo de punto de recuperación (RPO) de hasta 5 minutos. Además, es posible simular procedimientos de recuperación ante desastres sin afectar a la producción ni incurrir en costes adicionales de almacenamiento.

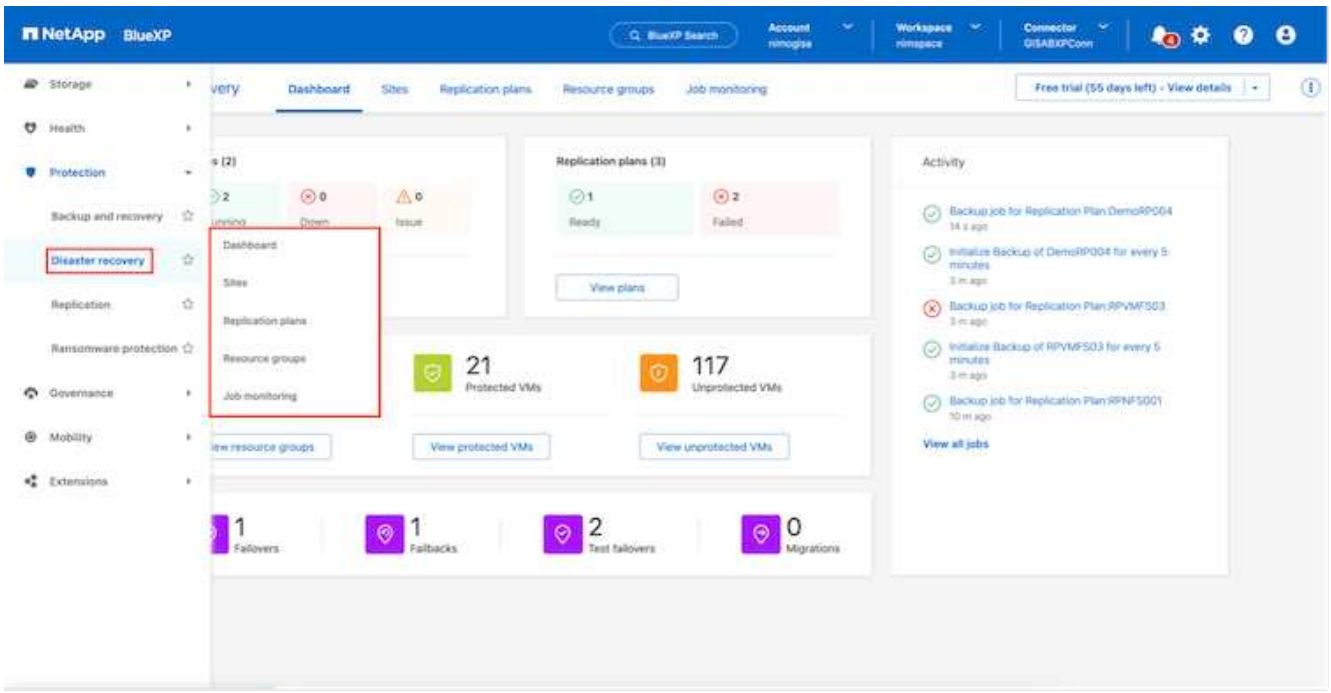
La recuperación ante desastres de BlueXP aprovecha la tecnología FlexClone de ONTAP para crear una copia del almacén de datos NFS con gestión eficiente del espacio del último Snapshot replicado del sitio de recuperación ante desastres. Una vez finalizada la prueba de recuperación ante desastres, los clientes pueden eliminar fácilmente el entorno de prueba sin que ello afecte a los recursos de producción replicados. En caso de una conmutación al respaldo real, el servicio de recuperación ante desastres de BlueXP orquesta todos los pasos necesarios para poner automáticamente las máquinas virtuales protegidas en el sitio de recuperación ante desastres designado con tan solo unos clics. El servicio también revertirá la relación de SnapMirror con el sitio principal y replicará cualquier cambio del secundario al primario para realizar una operación de conmutación tras recuperación, cuando sea necesario. Todas estas funciones suponen una fracción del coste en comparación con otras alternativas conocidas.



Primeros pasos

Para comenzar a usar la recuperación ante desastres de BlueXP , use la consola de BlueXP y, después, acceda al servicio.

1. Inicie sesión en BlueXP.
2. En el menú de navegación izquierdo de BlueXP , seleccione Protection > Disaster recovery.
3. Aparece la Consola de recuperación de desastres de BlueXP .

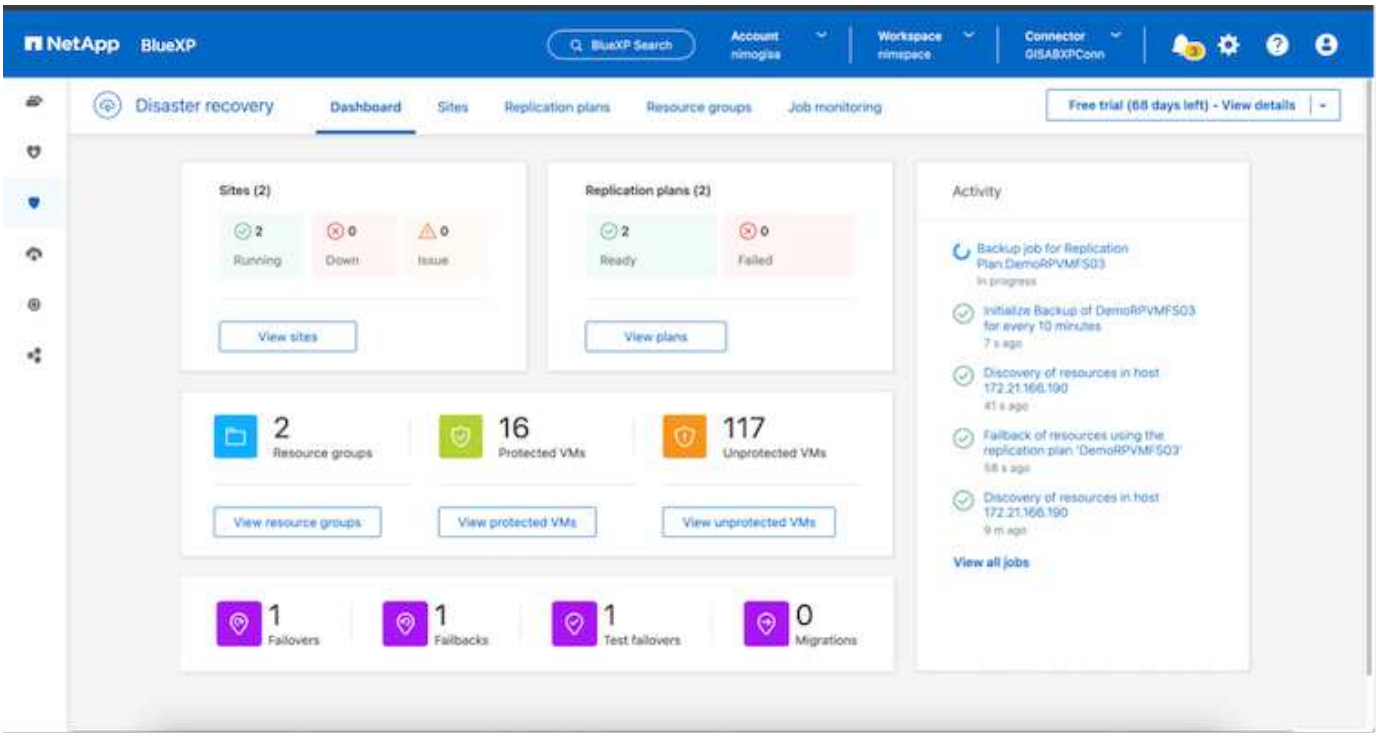


Antes de configurar el plan de recuperación ante desastres, asegúrese de que se cumplan los siguientes requisitos previos:

- El conector BlueXP se configura en NetApp BlueXP .
- La instancia del conector BlueXP tiene conectividad con los sistemas de almacenamiento y vCenter de origen y destino.
- Clúster de NetApp Data ONTAP para proporcionar almacenes de datos NFS de almacenamiento.
- Los sistemas de almacenamiento de NetApp on-premises que alojan almacenes de datos NFS para VMware se añaden en BlueXP .
- La resolución DNS debe estar en su lugar cuando se utilizan nombres DNS. De lo contrario, use direcciones IP para vCenter.
- La replicación de SnapMirror se configura para los volúmenes de almacén de datos basado en NFS designados.
- Compruebe que el entorno tenga versiones compatibles de vCenter Server y servidores ESXi.

Una vez establecida la conectividad entre los sitios de origen y destino, continúe con los pasos de configuración, que deben tomar un par de clics y alrededor de 3 a 5 minutos.

NetApp recomienda la puesta en marcha del conector BlueXP en el sitio de destino o en un tercer sitio para que el conector BlueXP pueda comunicarse a través de la red con recursos de origen y de destino.

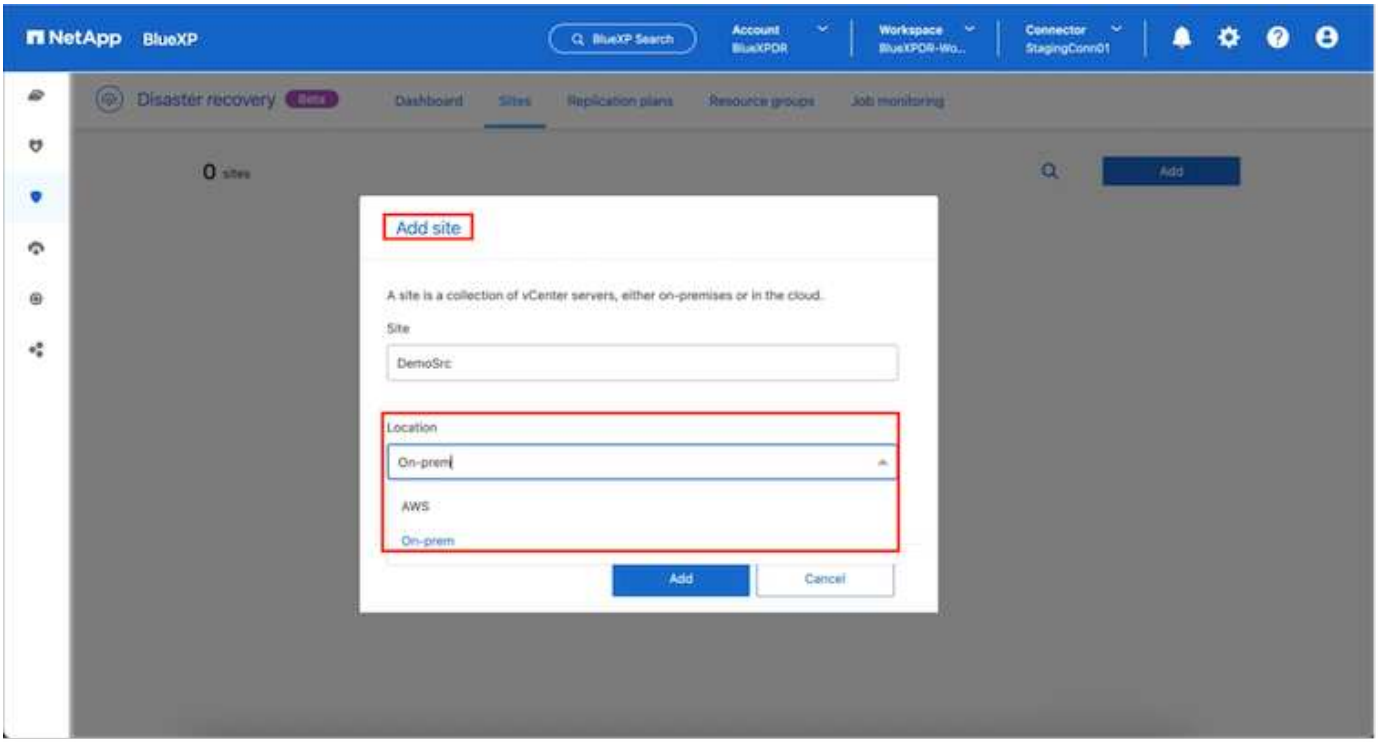


Configuración de la recuperación de desastres de BlueXP

El primer paso para prepararse para la recuperación de desastres es detectar y añadir los recursos de almacenamiento y vCenter en las instalaciones a la recuperación ante desastres de BlueXP .

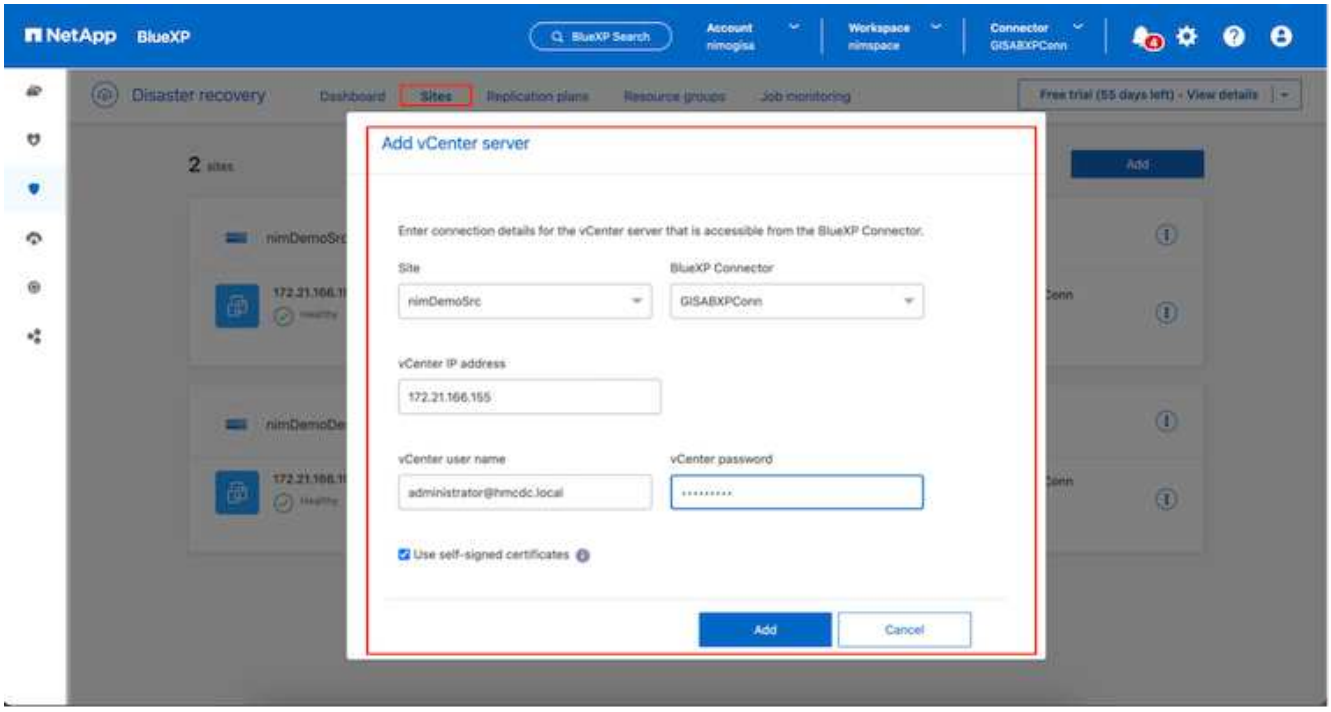
Abra la consola de BlueXP y seleccione **Protección > Recuperación ante desastres** en la navegación izquierda. Seleccione **Descubrir servidores de vCenter** o utilice el menú superior, seleccione **Sitios >**

Agregar > Agregar vCenter.

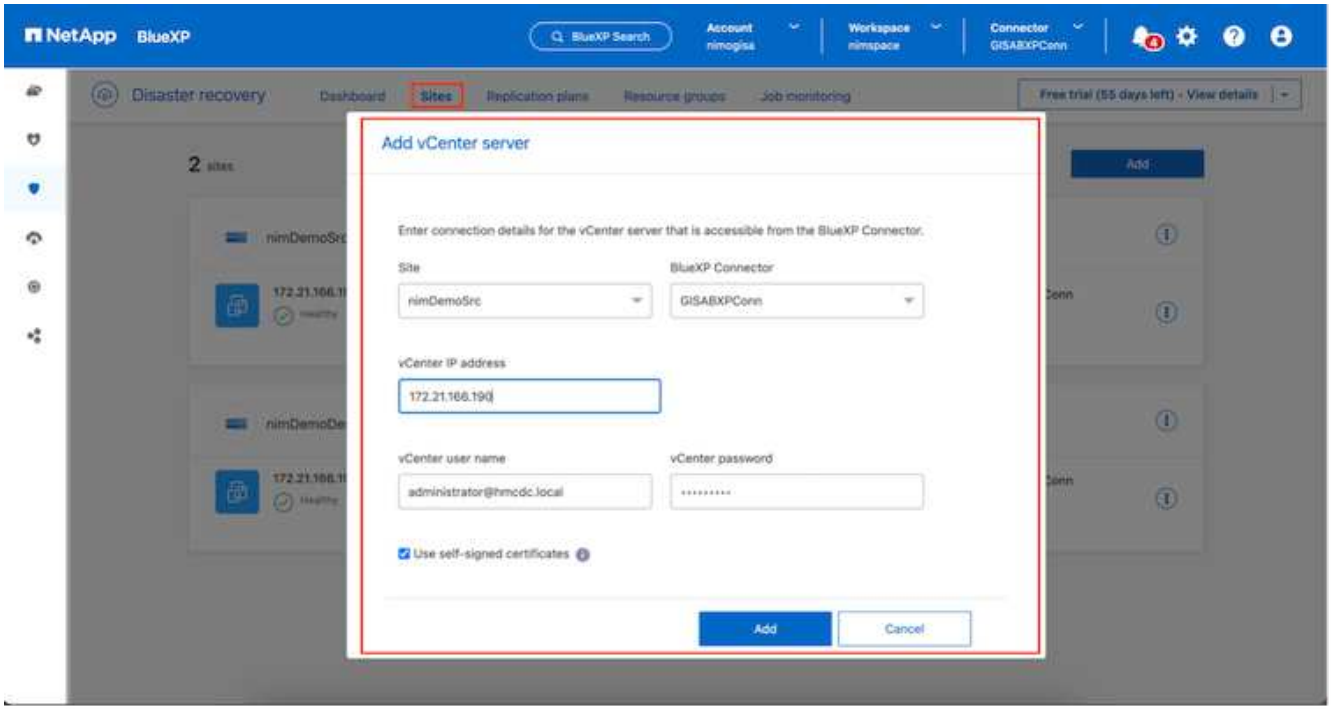


Añada las siguientes plataformas:

- **Fuente**. VCenter en las instalaciones.



- **Destino**. SDDC VMC vCenter.



Una vez que se añaden los vCenter, se activa la detección automatizada.

Configurar la replicación de almacenamiento entre la cabina del sitio de origen y la cabina del sitio de destino

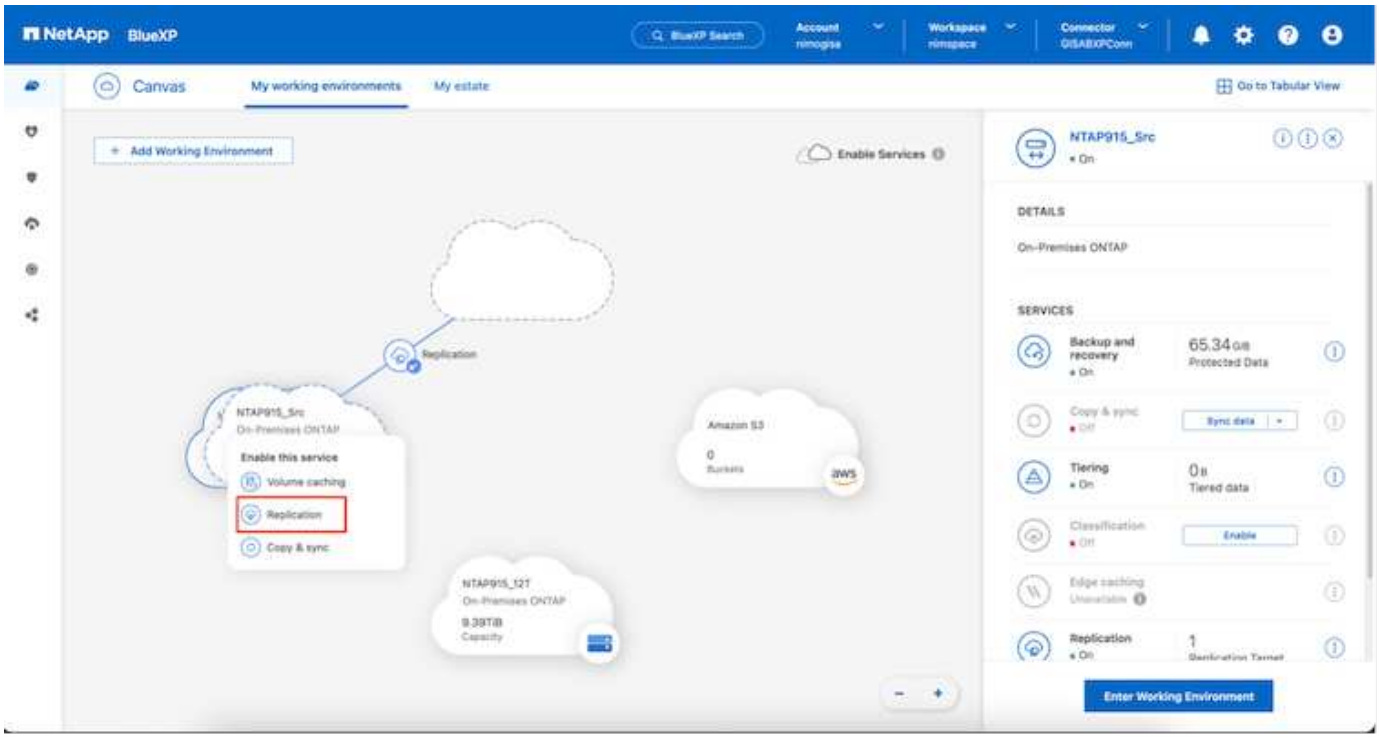
SnapMirror proporciona replicación de datos en un entorno NetApp. Basada en la tecnología Snapshot® de NetApp, la replicación de SnapMirror es extremadamente eficiente porque replica solo los bloques que se han cambiado o agregado desde la actualización anterior. SnapMirror se configura fácilmente mediante el uso de NetApp OnCommand® System Manager o la CLI de ONTAP. BlueXP DRaaS también crea la relación de SnapMirror proporcionada entre clústeres y SVM que se configura de antemano.

En los casos en los que no se pierda el almacenamiento primario por completo, SnapMirror proporciona un medio eficaz para volver a sincronizar los sitios primarios y de recuperación de desastres. SnapMirror puede volver a sincronizar los dos sitios, transfiriendo solo los datos nuevos o modificados de vuelta al sitio principal desde el sitio de recuperación ante desastres, simplemente revisando las relaciones de SnapMirror. Esto significa que los planes de replicación de DRaaS de BlueXP se pueden volver a sincronizar en cualquier dirección después de una conmutación por error sin recuperar el volumen completo. Si se vuelve a sincronizar una relación en dirección inversa, solo se envían al destino los datos nuevos que se hayan escrito desde la última sincronización correcta de la copia Snapshot.

> Si la relación de SnapMirror ya está configurada para el volumen a través de la interfaz de línea de comandos o de System Manager, BlueXP DRaaS recoge la relación y prosigue con el resto de las operaciones de flujo de trabajo.

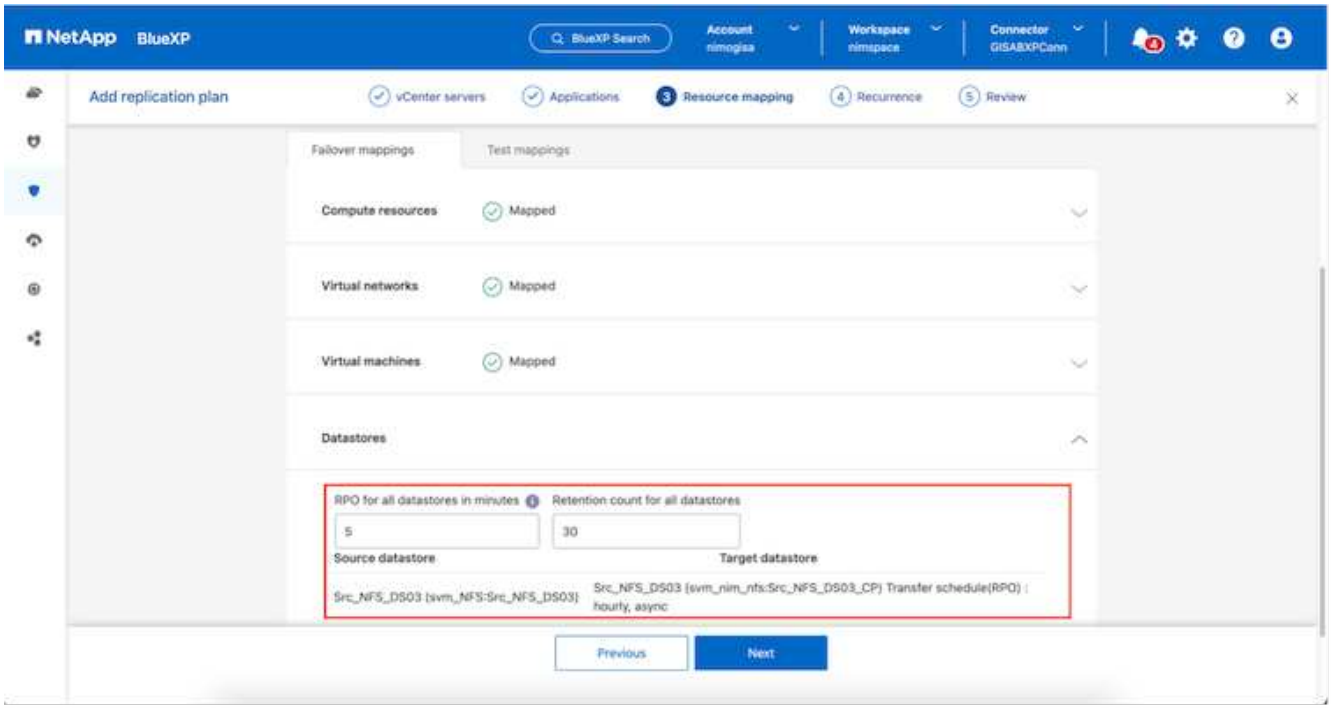
Cómo configurarlo para la recuperación ante desastres de VMware

El proceso para crear una replicación de SnapMirror sigue siendo el mismo para cualquier aplicación dada. El proceso puede ser manual o automatizado. La forma más sencilla es aprovechar BlueXP para configurar la replicación de SnapMirror mediante una simple acción de arrastrar y soltar el sistema ONTAP de origen del entorno en el destino para activar el asistente que guiará durante el resto del proceso.



BlueXP DRaaS también puede automatizar lo mismo siempre que se cumplan los siguientes dos criterios:

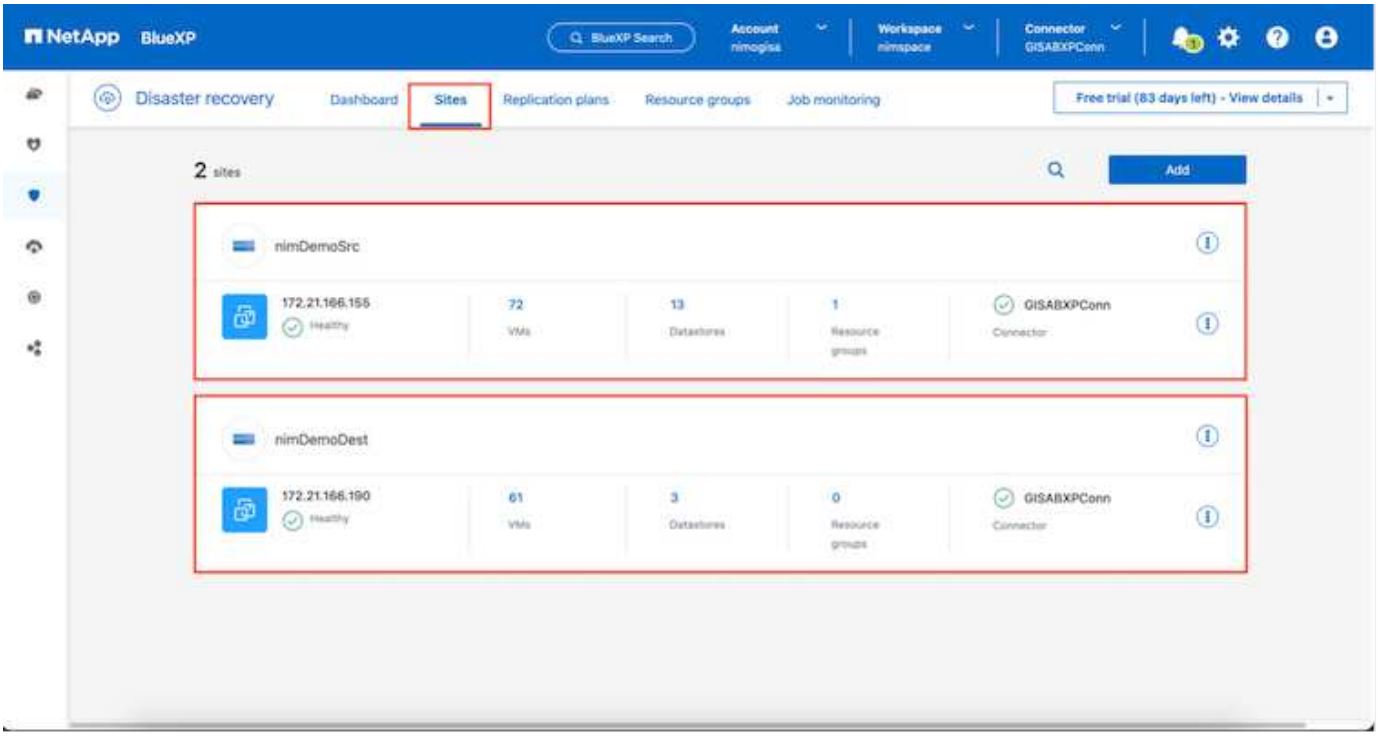
- Los clústeres de origen y destino tienen una relación entre iguales.
- La SVM de origen y la SVM de destino tienen una relación entre iguales.



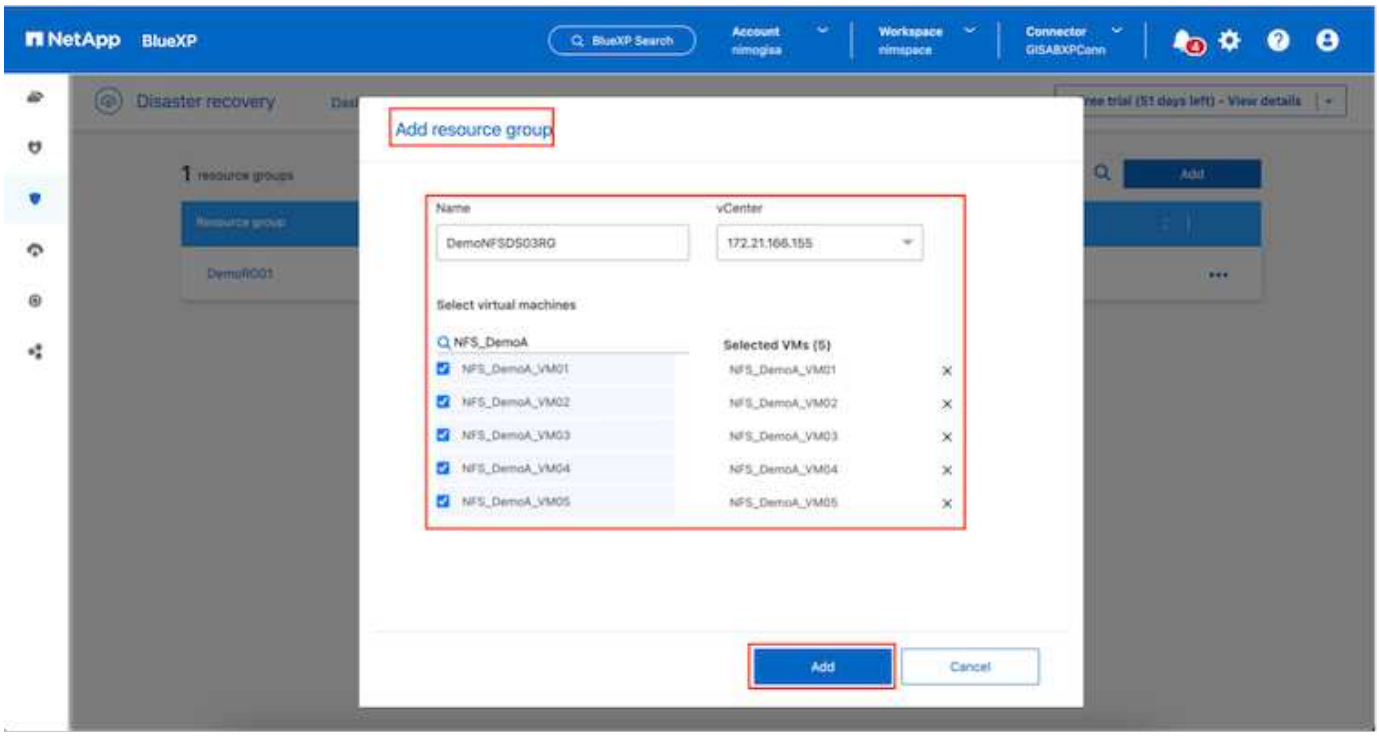
Si la relación de SnapMirror ya se ha configurado para el volumen a través de la interfaz de línea de comandos, BlueXP DRaaS recoge la relación y prosigue con el resto de las operaciones del flujo de trabajo.

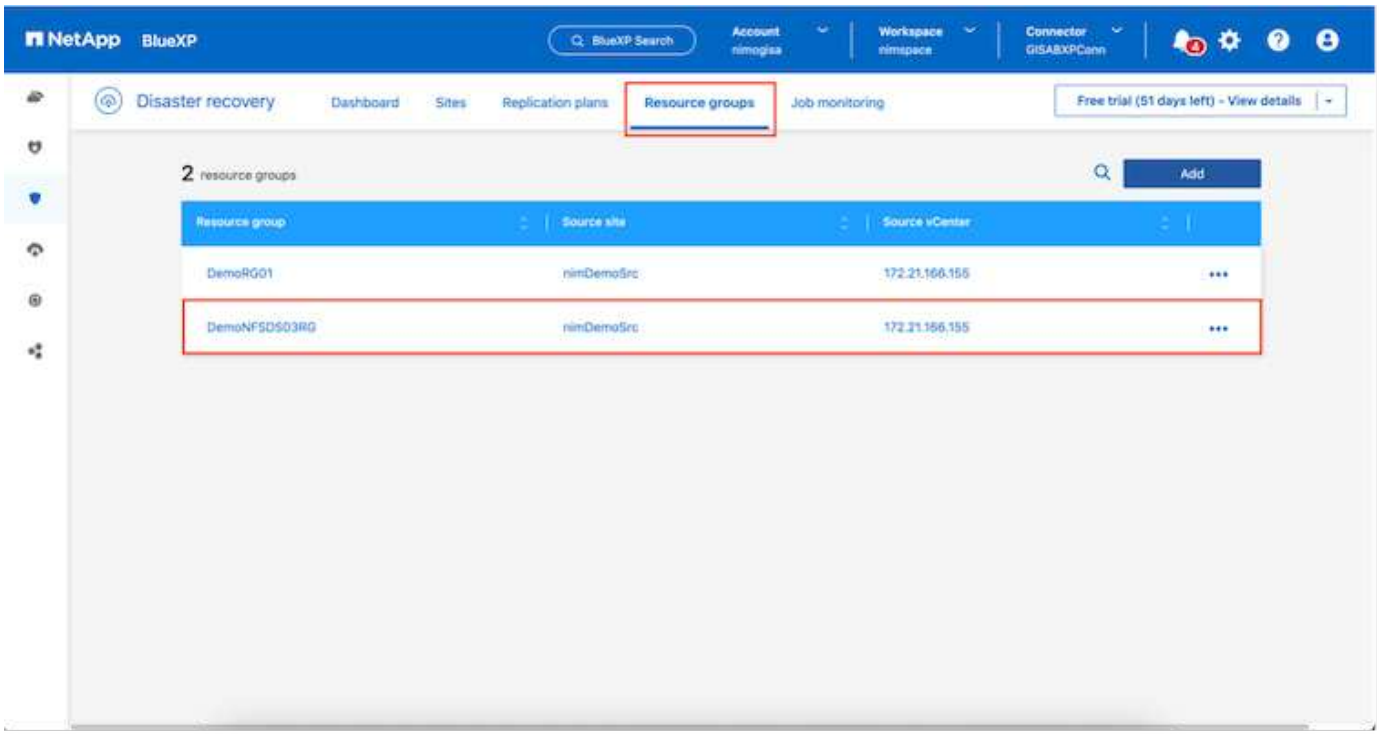
¿Cómo puede hacer la recuperación ante desastres de BlueXP por usted?

Después de añadir los sitios de origen y de destino, la recuperación de desastres de BlueXP lleva a cabo una detección profunda automática y muestra las máquinas virtuales junto con los metadatos asociados. La recuperación ante desastres de BlueXP también detecta automáticamente las redes y los grupos de puertos que utilizan las máquinas virtuales y los rellena.



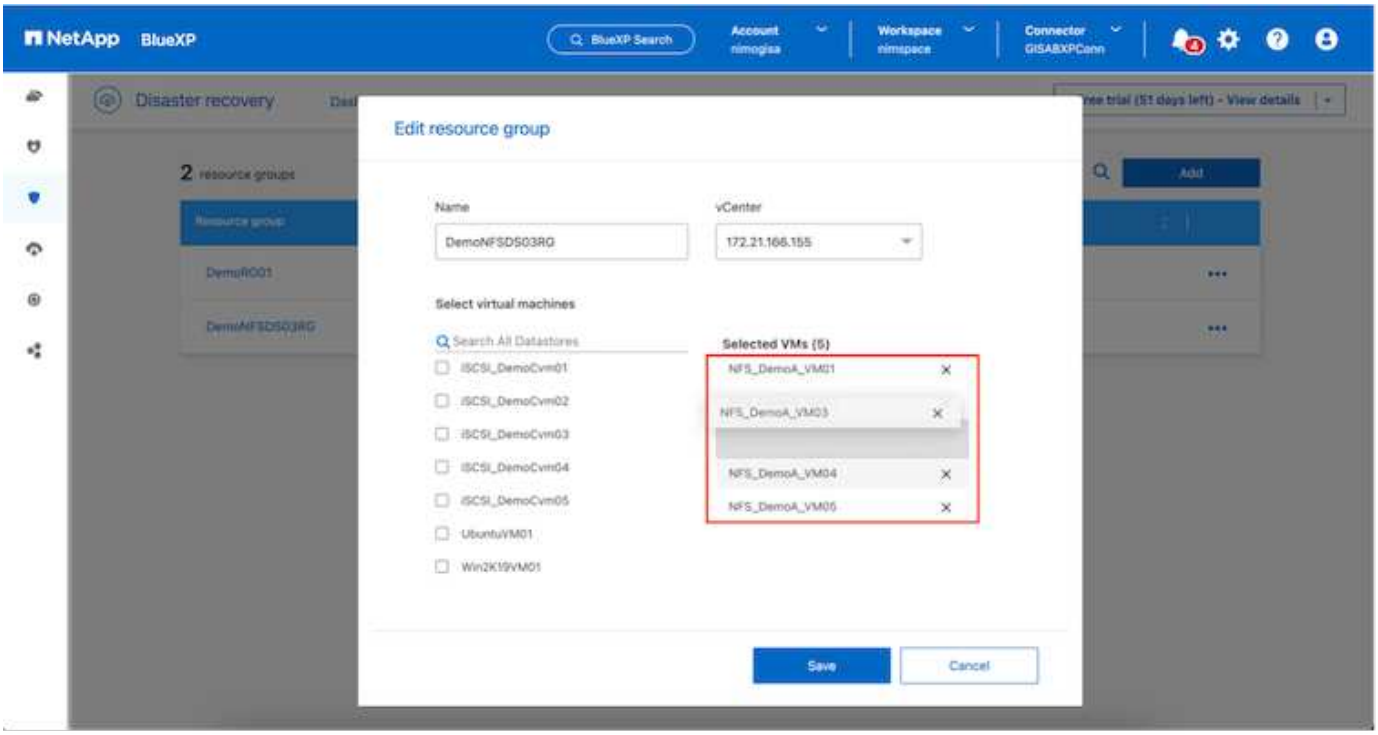
Una vez agregados los sitios, los equipos virtuales se pueden agrupar en grupos de recursos. Los grupos de recursos de recuperación ante desastres de BlueXP le permiten agrupar un conjunto de equipos virtuales dependientes en grupos lógicos que contengan sus órdenes de arranque y retrasos en el arranque que se pueden ejecutar en el momento de su recuperación. Para comenzar a crear grupos de recursos, navegue a **Grupos de recursos** y haga clic en **Crear nuevo grupo de recursos**.



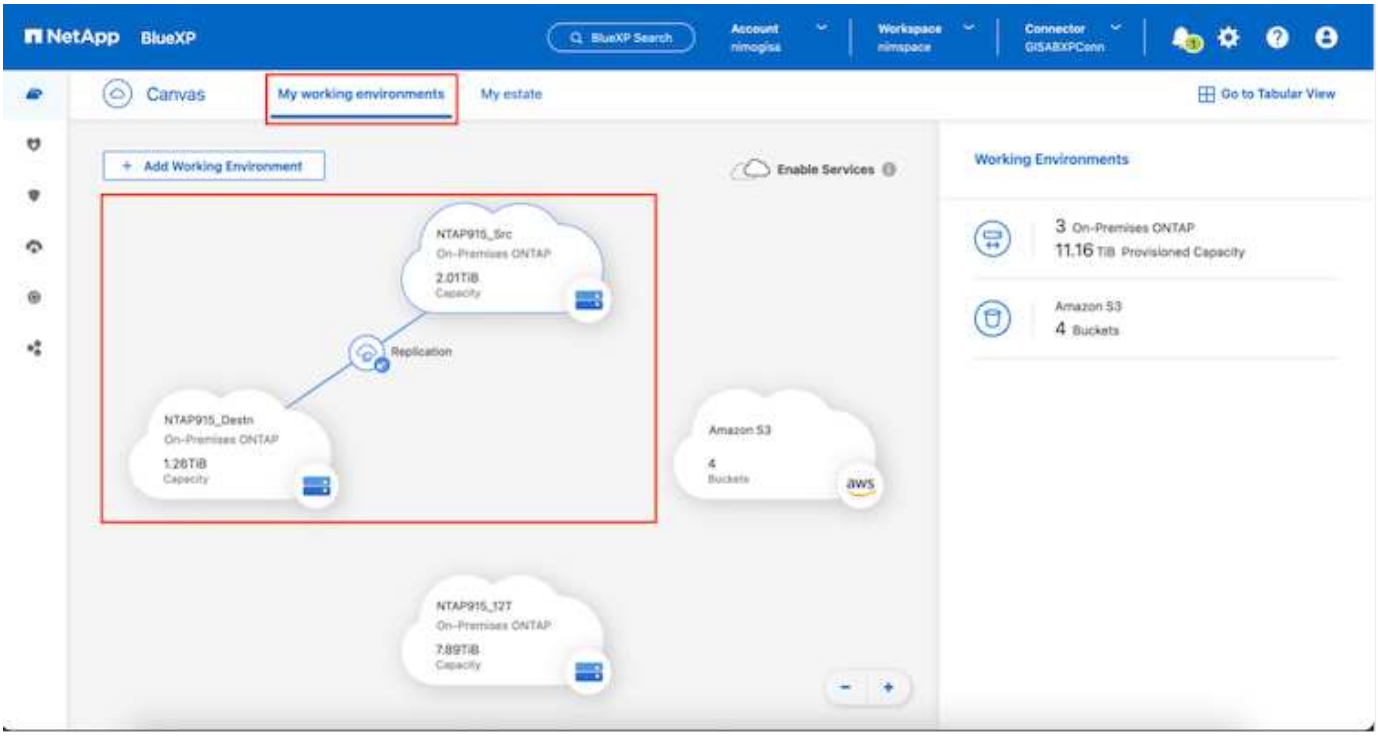


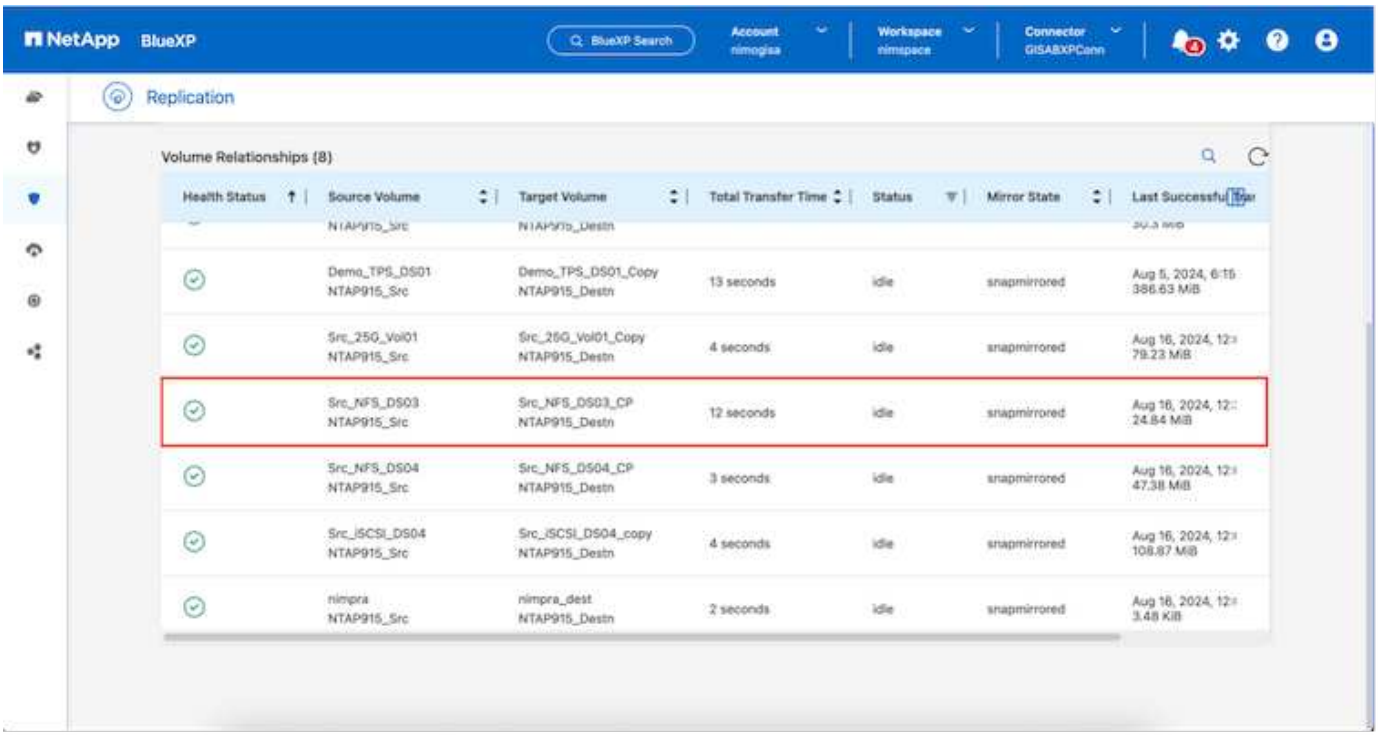
El grupo de recursos también se puede crear al crear un plan de replicación.

El orden de arranque de los equipos virtuales se puede definir o modificar durante la creación de grupos de recursos mediante un sencillo mecanismo de arrastrar y soltar.



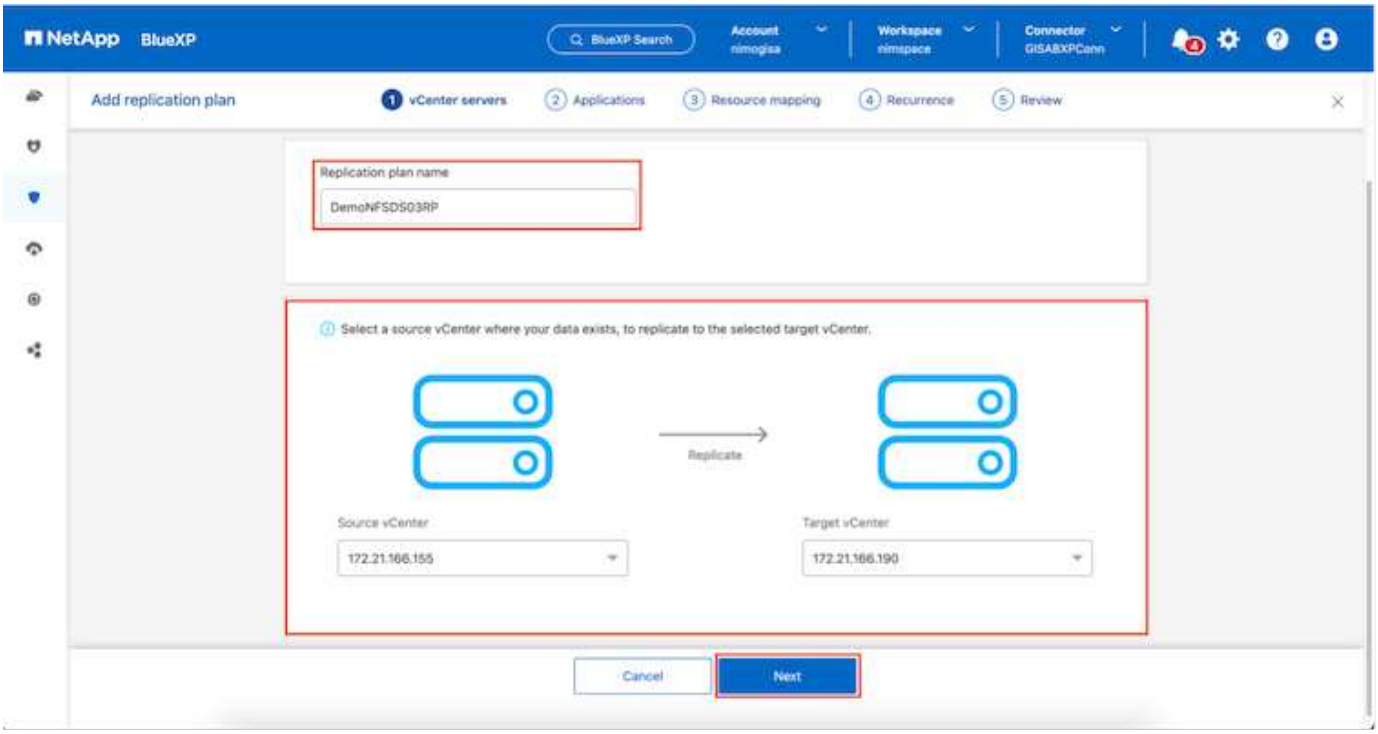
Una vez creados los grupos de recursos, el siguiente paso es crear el plan de ejecución o un plan para recuperar máquinas virtuales y aplicaciones en caso de desastre. Como se ha mencionado en los requisitos previos, la replicación de SnapMirror se puede configurar de antemano o DRaaS puede configurarla usando el RPO y el recuento de retención especificado durante la creación del plan de replicación.





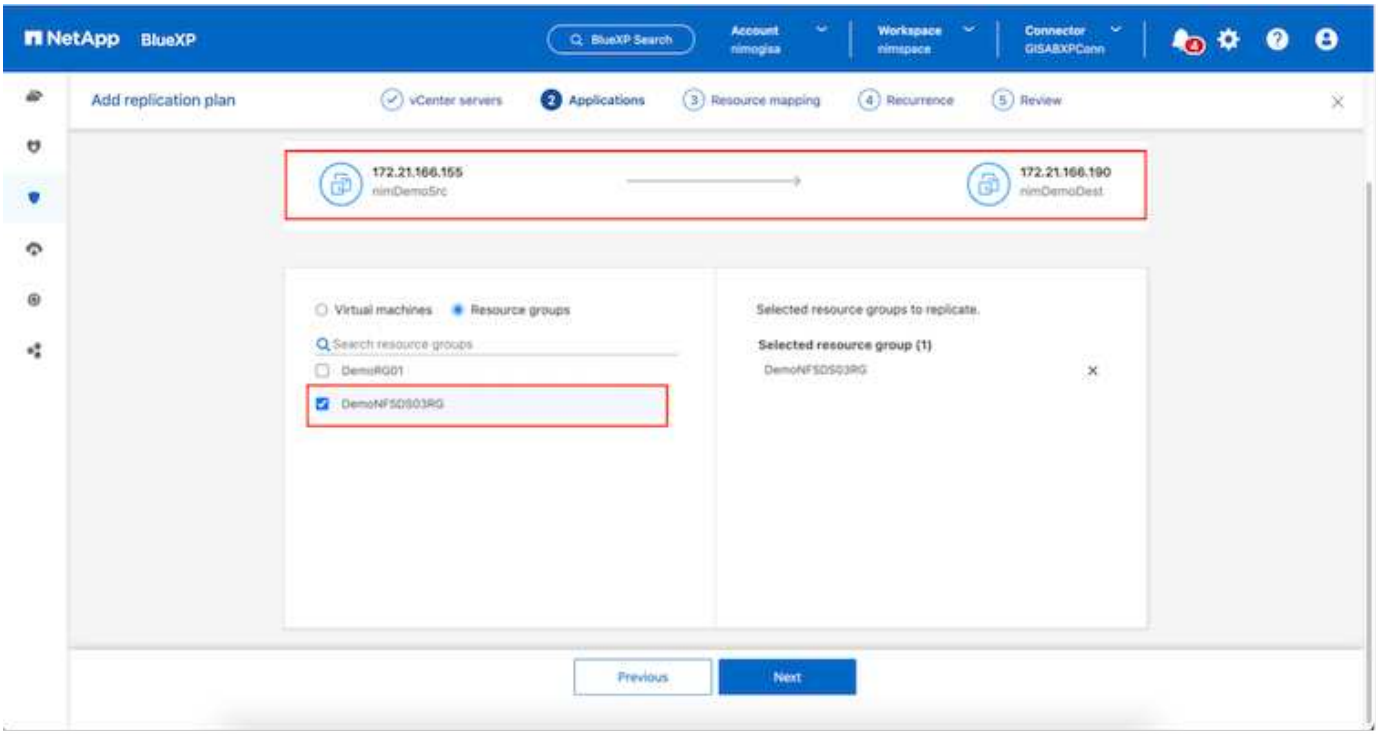
Configure el plan de replicación seleccionando desde el menú desplegable las plataformas vCenter de origen y de destino, y elija los grupos de recursos que se incluirán en el plan, junto con la agrupación de cómo se deben restaurar y encender las aplicaciones y la asignación de clústeres y redes. Para definir el plan de recuperación, vaya a la pestaña **Plan de replicación** y haga clic en **Agregar plan**.

Primero, seleccione la instancia de vCenter de origen y, a continuación, seleccione la instancia de vCenter de destino.



El siguiente paso es seleccionar grupos de recursos existentes. Si no se crearon grupos de recursos, el asistente ayuda a agrupar las máquinas virtuales necesarias (básicamente crear grupos de recursos

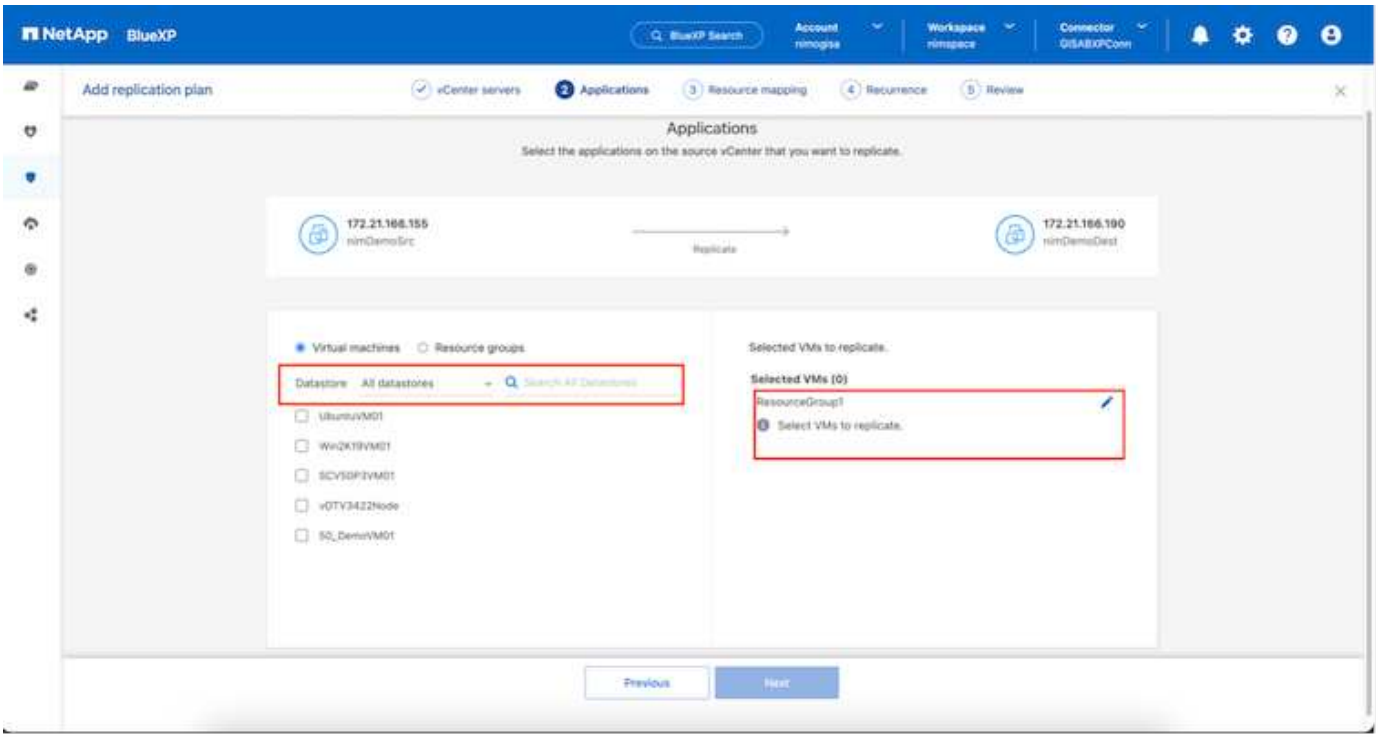
funcionales) en función de los objetivos de recuperación. Esto también ayuda a definir la secuencia de operaciones de cómo se deben restaurar las máquinas virtuales de aplicaciones.



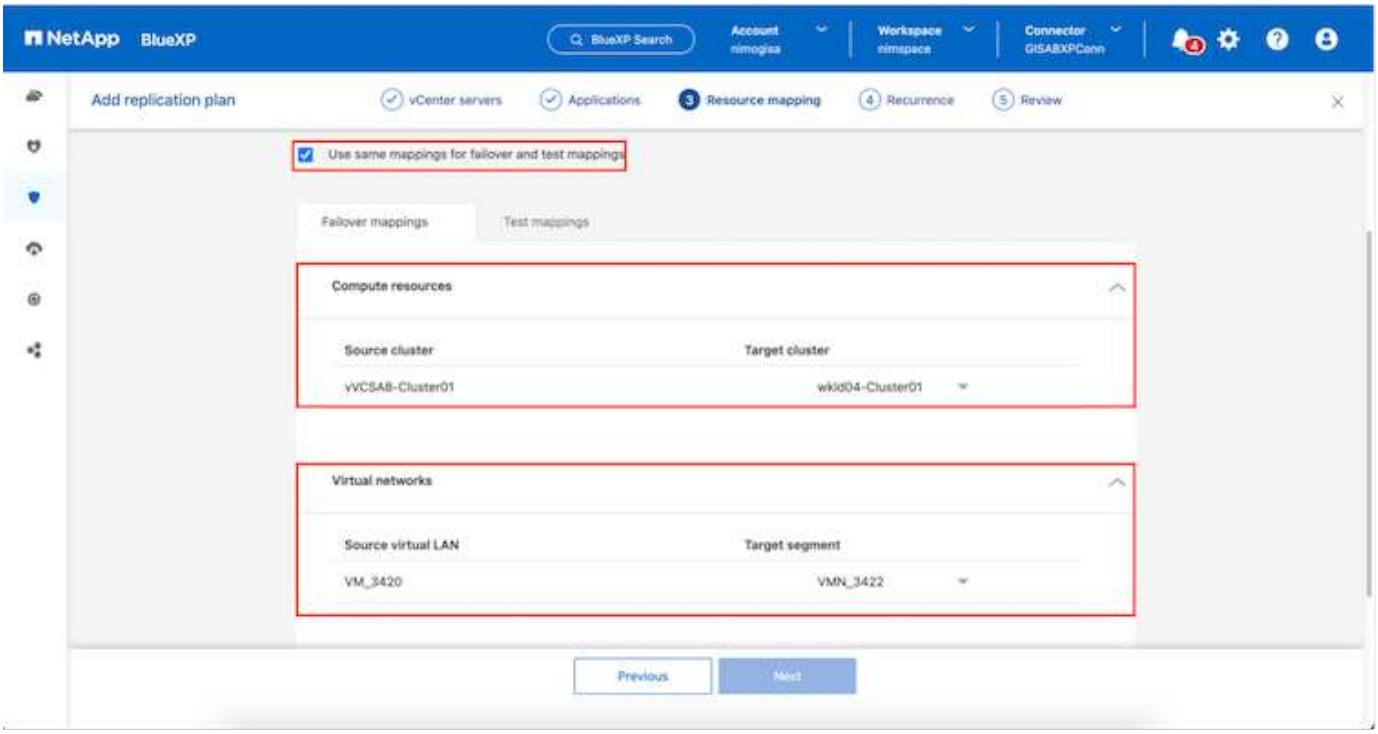
El grupo de recursos permite establecer el orden de inicio mediante la función de arrastrar y soltar. Se puede utilizar para modificar fácilmente el orden en el que se encenderían las VM durante el proceso de recuperación.

Cada máquina virtual de un grupo de recursos se inicia en secuencia según el orden. Dos grupos de recursos se inician en paralelo.

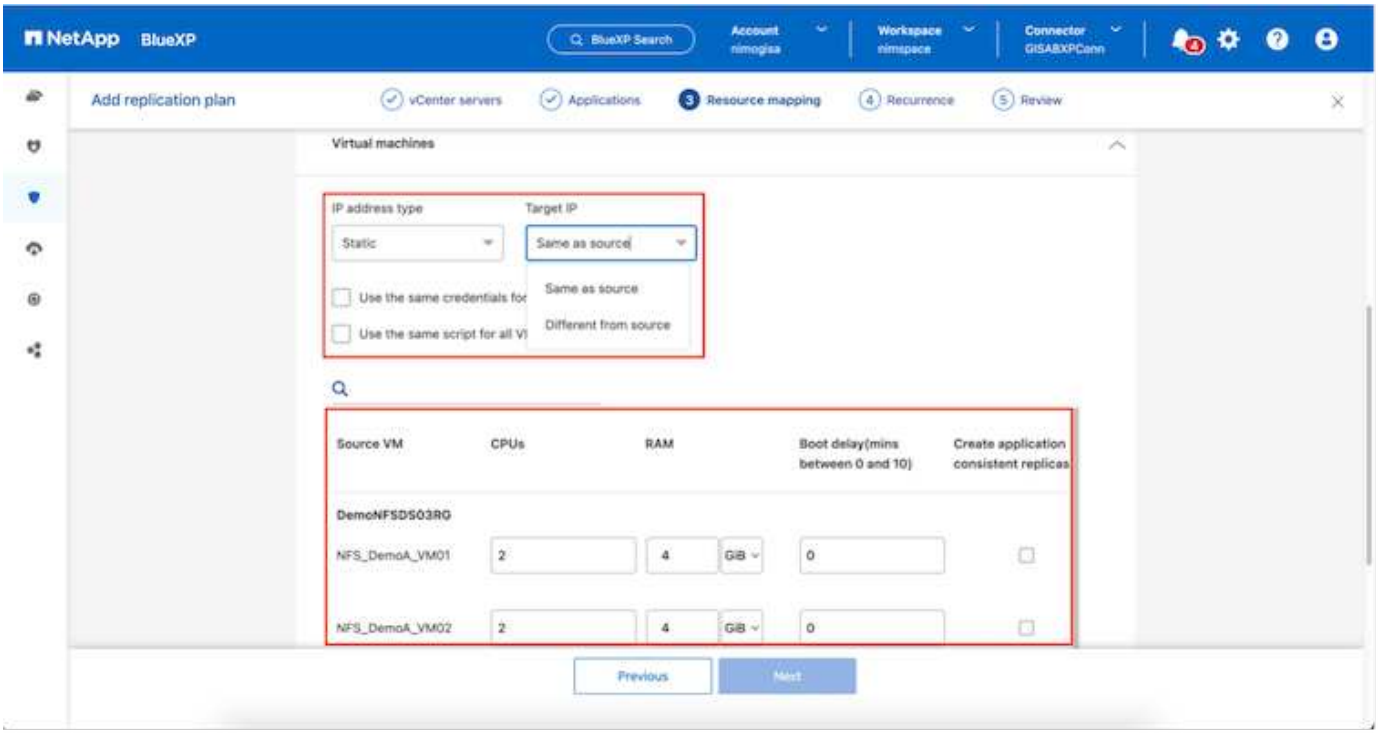
La siguiente captura de pantalla muestra la opción de filtrar máquinas virtuales o almacenes de datos específicos según los requisitos de la organización si no se crean grupos de recursos con antelación.



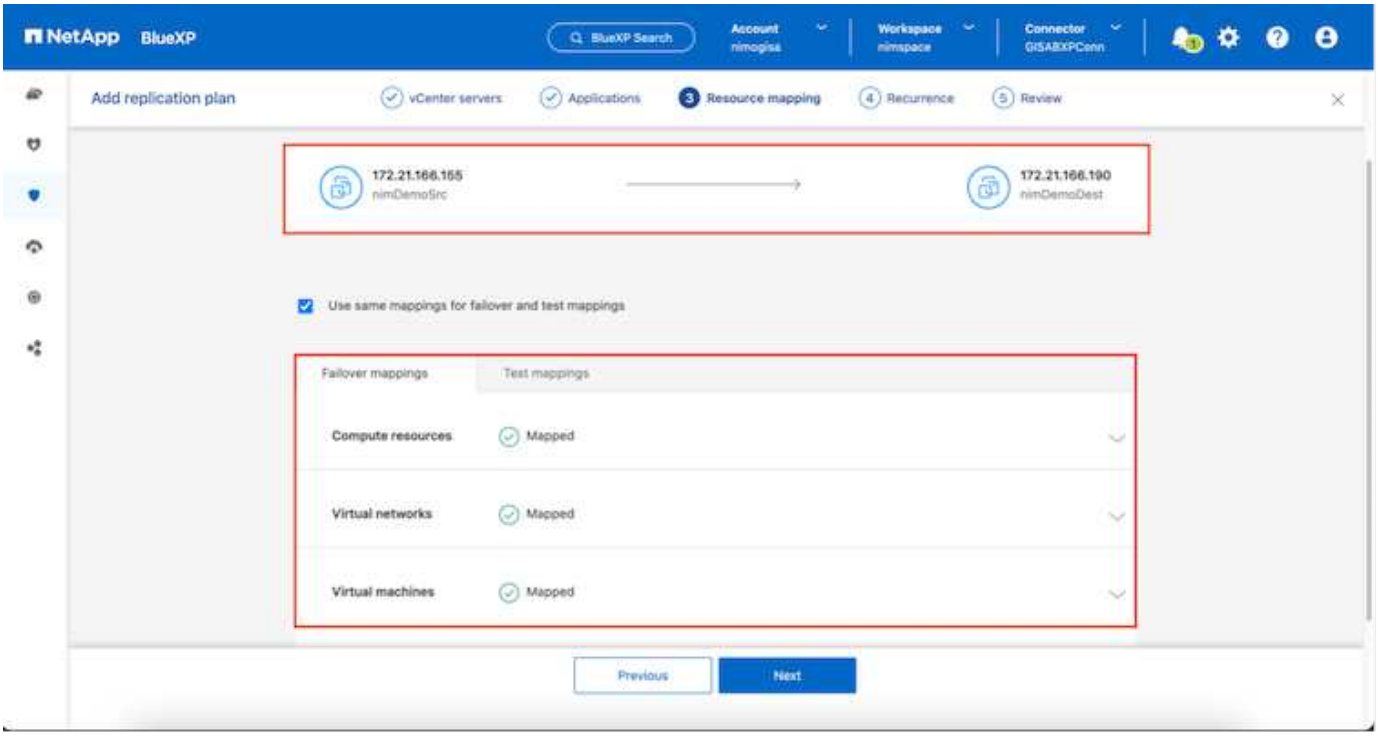
Una vez seleccionados los grupos de recursos, cree las asignaciones de conmutación por error. En este paso, especifique cómo se asignan los recursos del entorno de origen al destino. Esto incluye recursos de computación y redes virtuales. Personalización de IP, scripts previos y posteriores, retrasos en el inicio, coherencia de aplicaciones, etc. Para obtener información detallada, consulte "Cree un plan de replicación".



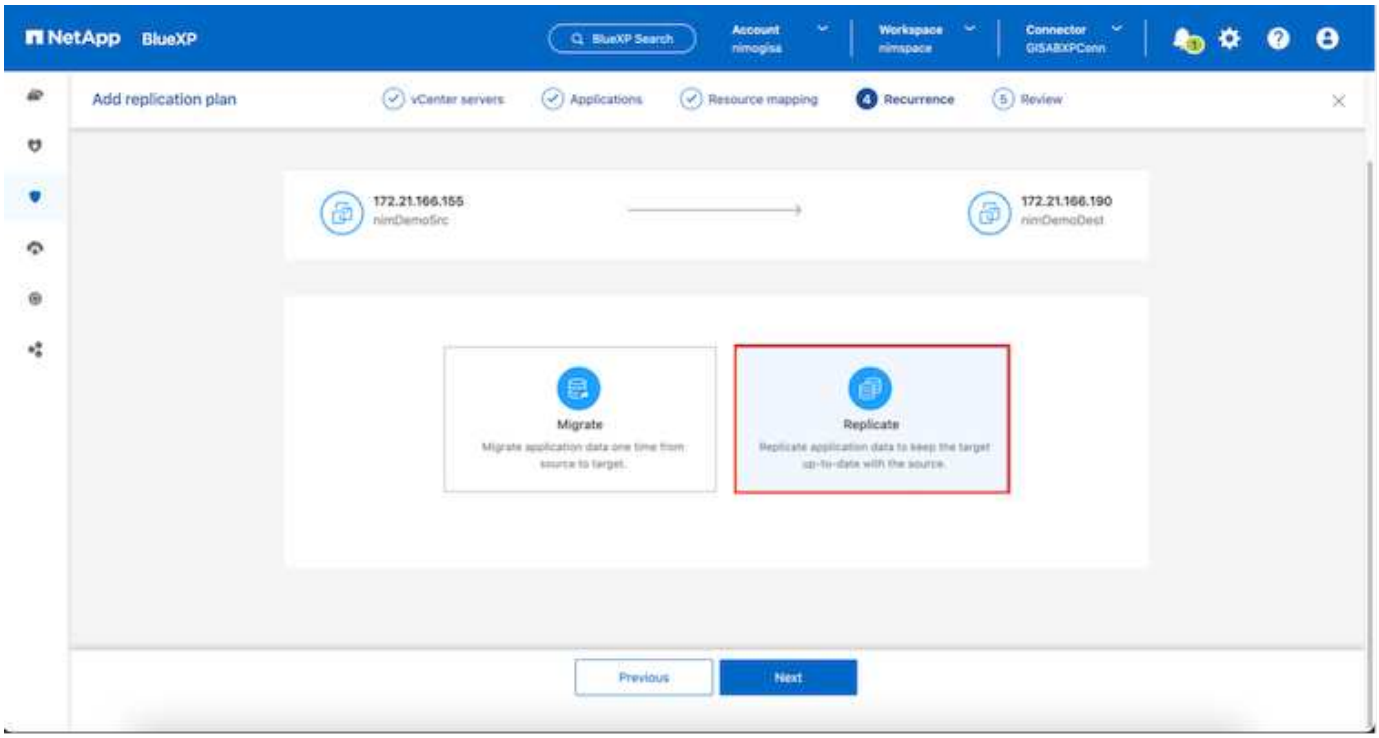
De forma predeterminada, se utilizan los mismos parámetros de asignación para las operaciones de prueba y conmutación por error. Para definir diferentes asignaciones para el entorno de prueba, seleccione la opción de asignación de prueba después de desactivar la casilla de verificación como se muestra a continuación:



Una vez finalizada la asignación de recursos, haga clic en Siguiente.

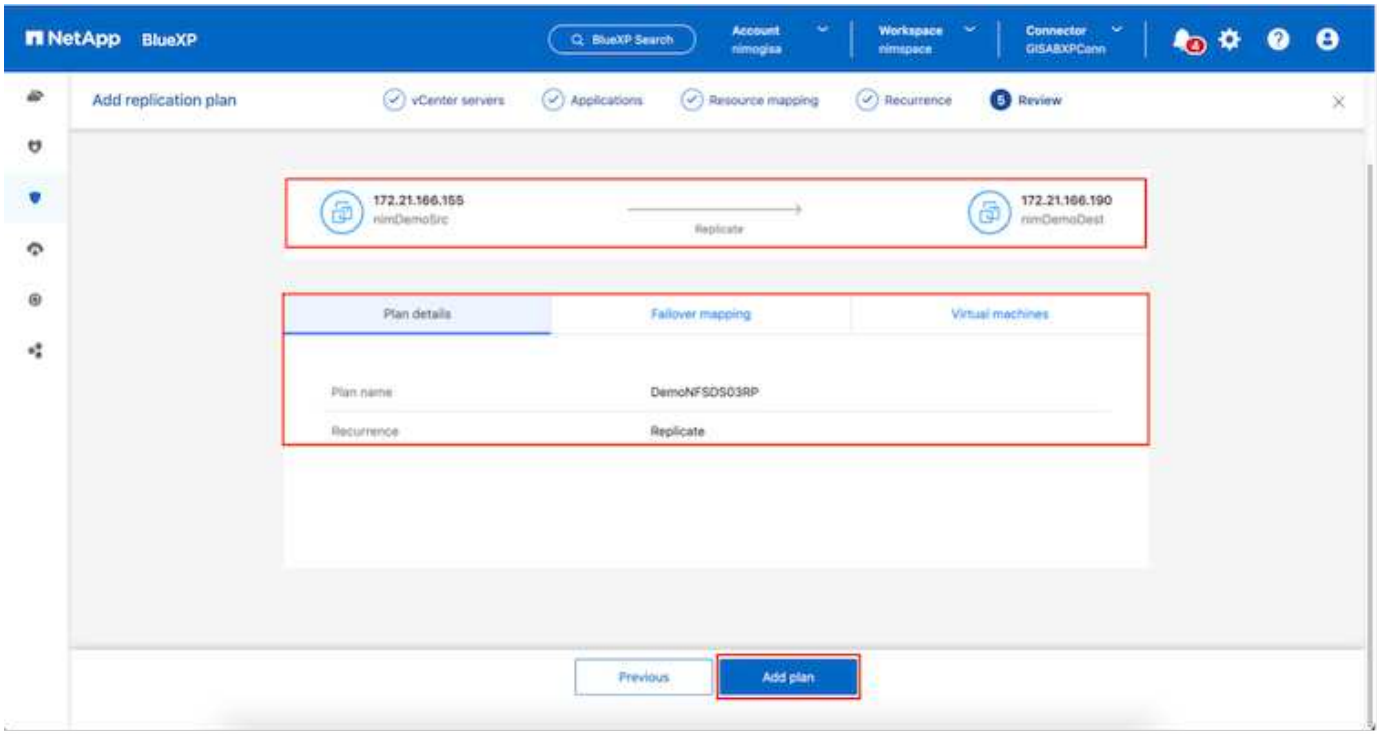


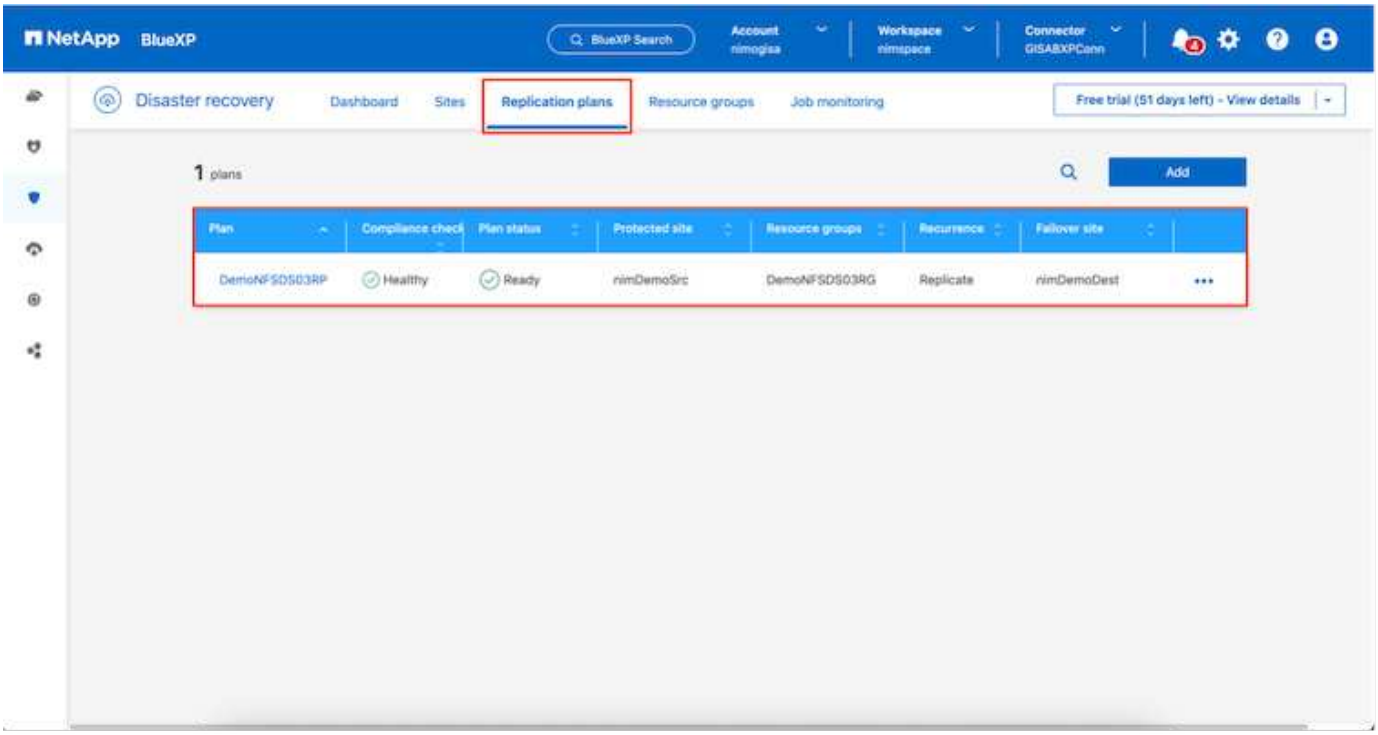
Seleccione el tipo de recurrencia. En pocas palabras, seleccione Migrate (one time migration using failover) o Recurring continuous replication option. En este tutorial, se selecciona la opción Replicar.



Una vez hecho esto, revisa las asignaciones creadas y luego haz clic en **Añadir plan**.

Las máquinas virtuales de diferentes volúmenes y SVM se pueden incluir en un plan de replicación. Según la ubicación de la máquina virtual (ya sea en el mismo volumen o en un volumen independiente dentro de la misma SVM, volúmenes independientes en distintas SVM), la recuperación ante desastres de BlueXP crea una Snapshot de grupo de consistencia.



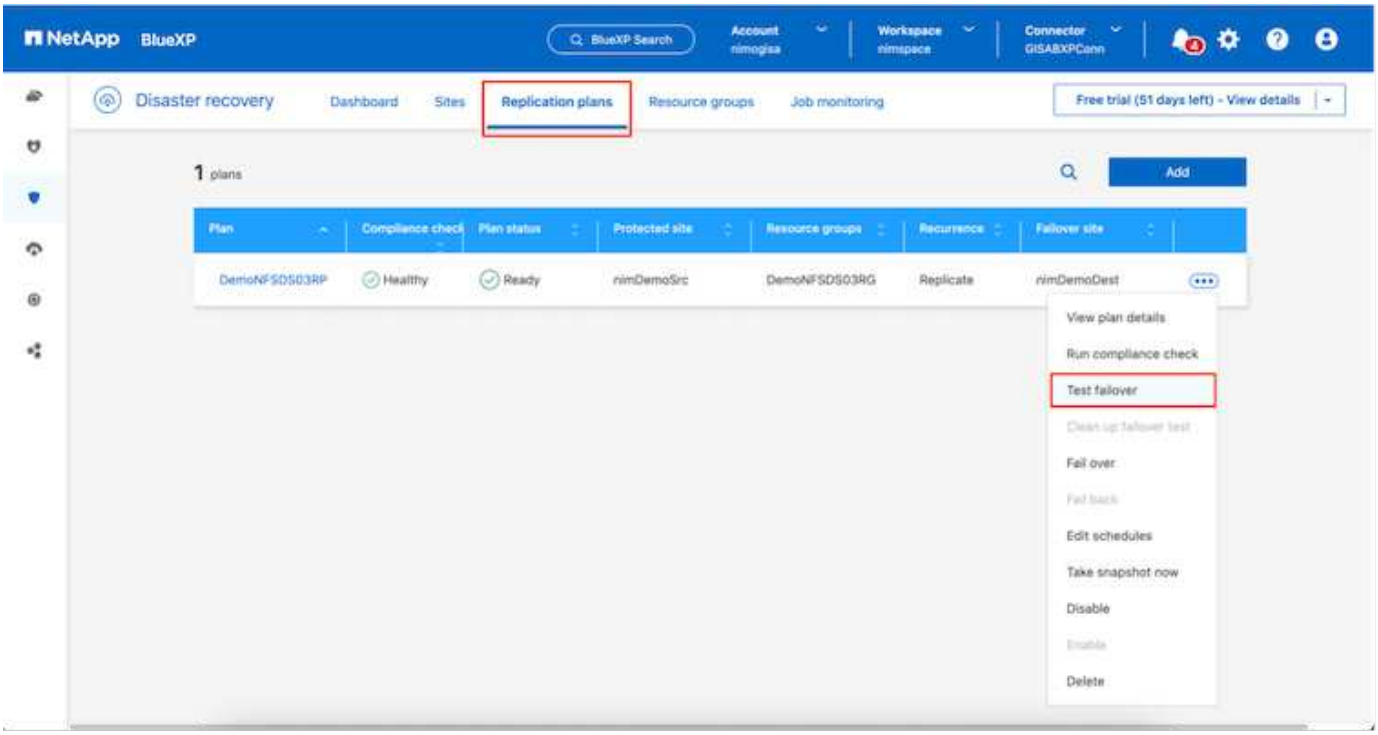


La recuperación ante desastres como servicio de BlueXP consta de los siguientes flujos de trabajo:

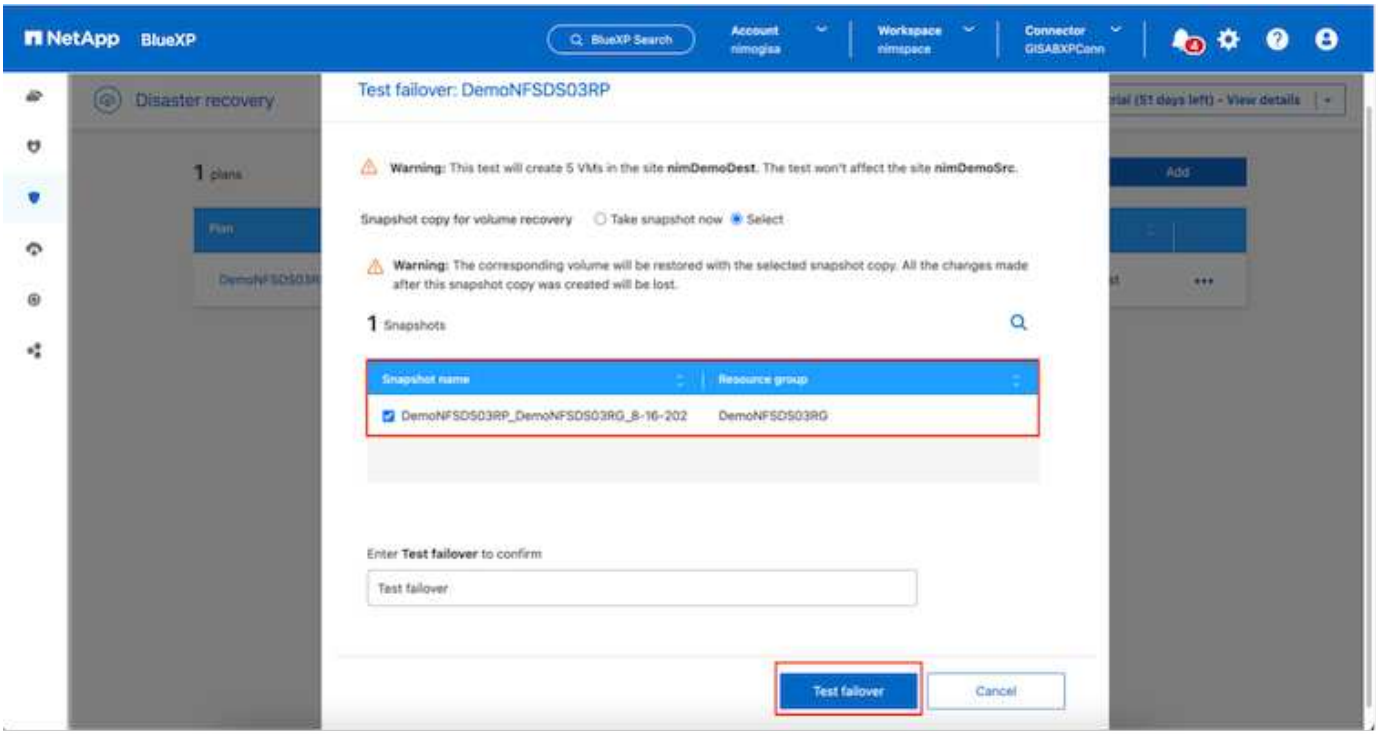
- Prueba de recuperación tras fallos (incluidas simulaciones automatizadas periódicas)
- Limpiar la prueba de conmutación por error
- Conmutación al respaldo
- Conmutación tras recuperación

Probar la recuperación tras fallos

La prueba de recuperación tras fallos en DRaaS de BlueXP es un procedimiento operativo que permite a los administradores de VMware validar por completo sus planes de recuperación sin que ello afecte a sus entornos de producción.



DRaaS de BlueXP incorpora la capacidad de seleccionar la instantánea como una funcionalidad opcional en la operación de prueba de conmutación por error. Esta funcionalidad permite al administrador de VMware verificar que los cambios realizados recientemente en el entorno se replican en el sitio de destino y que, por lo tanto, están presentes durante la prueba. Entre estos cambios se incluyen parches en el sistema operativo invitado de las máquinas virtuales

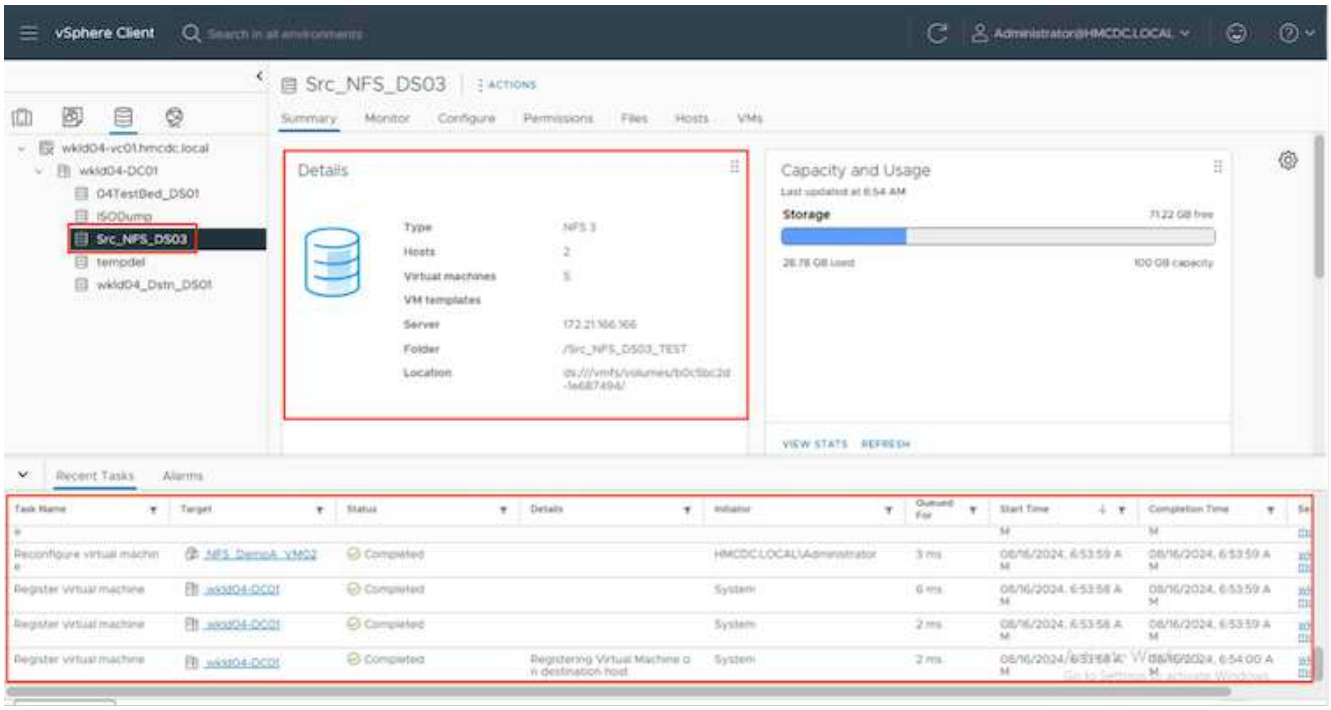


Cuando el administrador de VMware ejecuta una operación de recuperación tras fallos de prueba, DRaaS de BlueXP automatiza las siguientes tareas:

- Activación de relaciones de SnapMirror para actualizar el almacenamiento en el sitio de destino con los

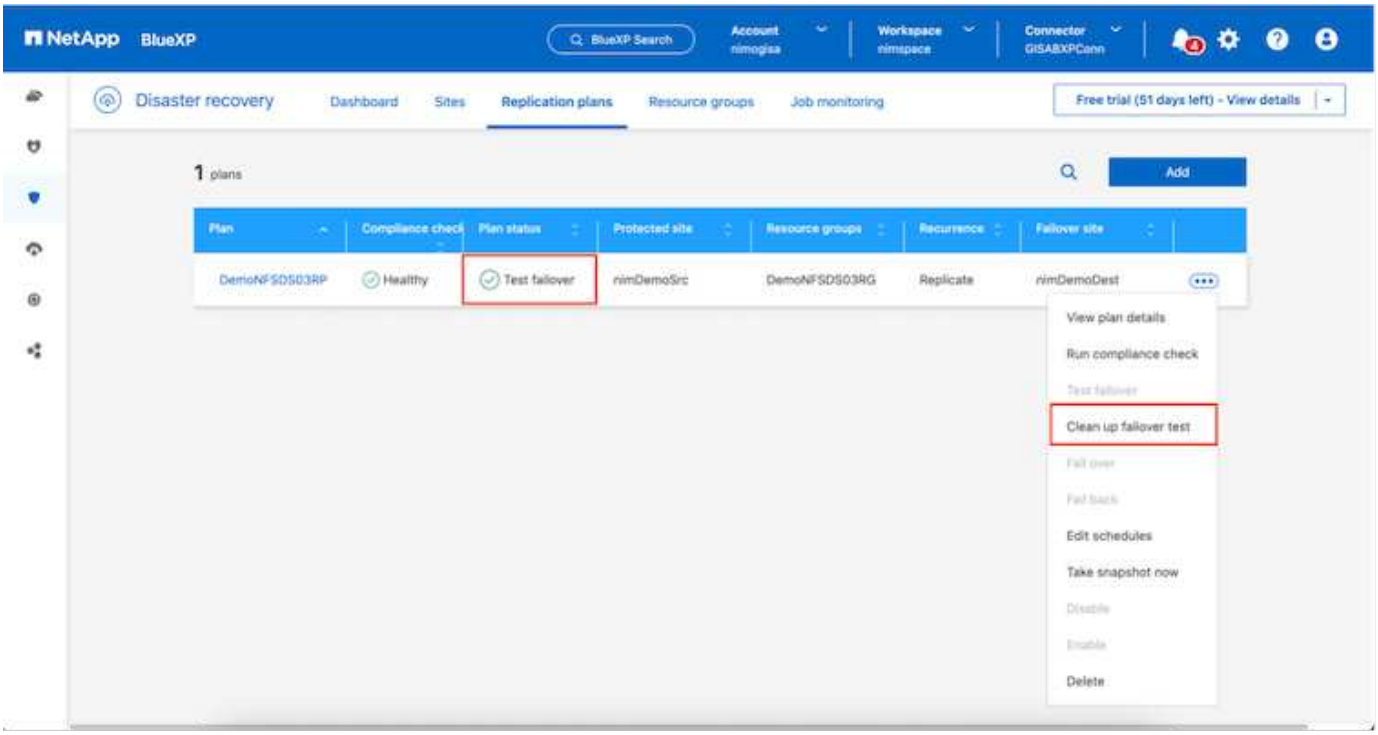
cambios recientes que se hayan realizado en el sitio de producción.

- Crear volúmenes NetApp FlexClone de los volúmenes de FlexVol en la cabina de almacenamiento de recuperación ante desastres.
- Conectar los almacenes de datos NFS de los volúmenes FlexClone a los hosts ESXi del sitio de recuperación de desastres.
- Conectando los adaptadores de red de la máquina virtual a la red de prueba especificada durante la asignación.
- Reconfigurar los ajustes de red del sistema operativo invitado de la máquina virtual según la definición de la red en el sitio de recuperación ante desastres.
- Ejecutando cualquier comando personalizado que se haya almacenado en el plan de replicación.
- Encendido de las máquinas virtuales en el orden definido en el plan de replicación.



Operación de prueba de failover de limpieza

La operación de prueba de limpieza de conmutación al nodo de respaldo se produce una vez que se completa la prueba del plan de replicación y el administrador de VMware responde al aviso de limpieza.



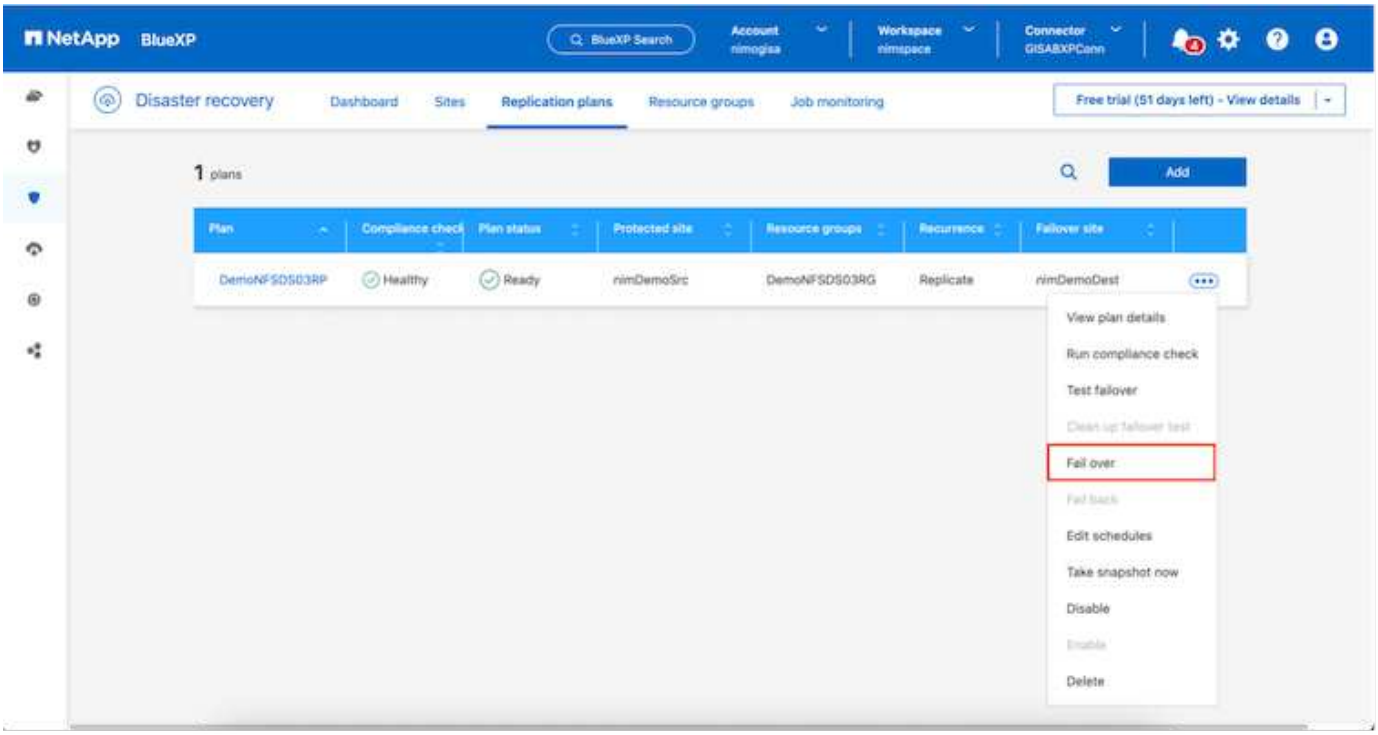
Esta acción restablecerá las máquinas virtuales (VM) y el estado del plan de replicación al estado Listo.

Cuando el administrador de VMware lleva a cabo una operación de recuperación, DRaaS de BlueXP completa el siguiente proceso:

1. Apaga todos los equipos virtuales recuperados en la copia FlexClone utilizada para la prueba.
2. Elimina el volumen FlexClone que se utilizó para presentar las máquinas virtuales recuperadas durante la prueba.

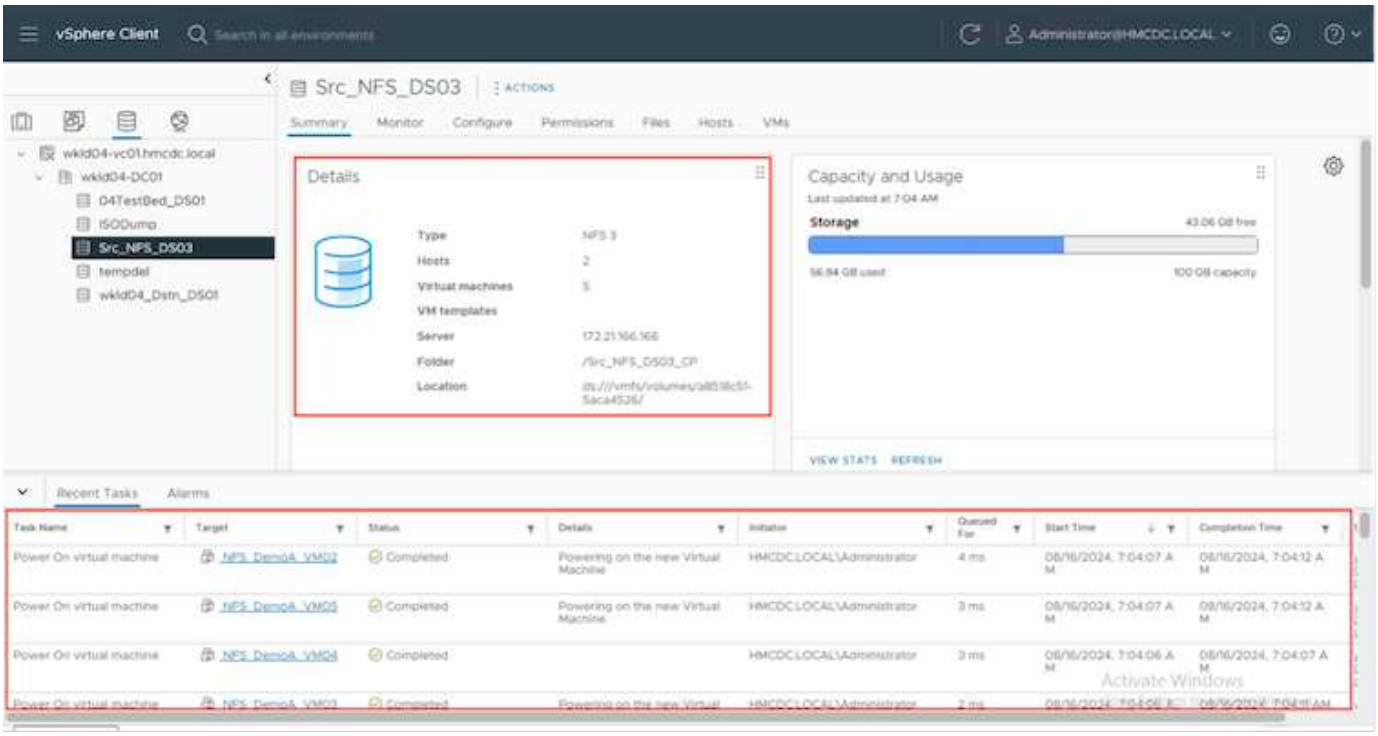
Migración planificada y conmutación por error

BlueXP DRaaS cuenta con dos métodos para realizar una recuperación tras fallos real: La migración planificada y la conmutación por error. El primer método, la migración planificada, incorpora la sincronización de apagado y replicación de almacenamiento de la máquina virtual al proceso para recuperar o mover eficazmente los equipos virtuales al site de destino. La migración planificada requiere acceso al sitio de origen. El segundo método, la conmutación al respaldo, es una conmutación al respaldo planificada/sin planificar en la que las máquinas virtuales se recuperan en el sitio de destino desde el último intervalo de replicación de almacenamiento que pudo finalizar. Dependiendo del objetivo de punto de recuperación que haya sido diseñado en la solución, cabe esperar cierta pérdida de datos en el escenario de recuperación de desastres.



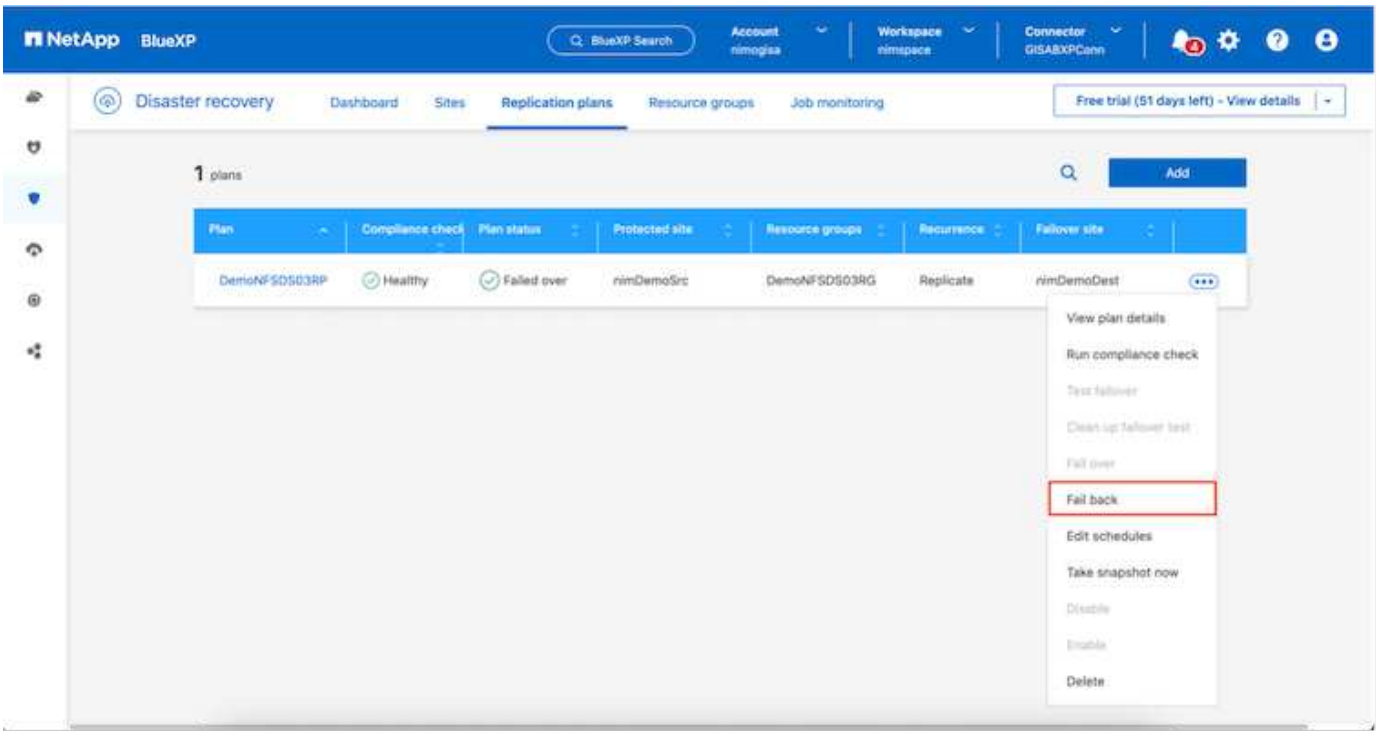
Cuando el administrador de VMware realiza una operación de recuperación tras fallos, DRaaS de BlueXP automatiza las siguientes tareas:

- Romper y conmutar por error las relaciones de NetApp SnapMirror.
- Conectar los almacenes de datos NFS replicados a los hosts ESXi del sitio de recuperación ante desastres.
- Conecte los adaptadores de red de las máquinas virtuales a la red de sitio de destino adecuada.
- Vuelva a configurar los ajustes de red del sistema operativo invitado de la máquina virtual según se hayan definido para la red en el sitio de destino.
- Ejecute los comandos personalizados (si los hay) que se hayan almacenado en el plan de replicación.
- Encienda las máquinas virtuales en el orden definido en el plan de replicación.



Conmutación tras recuperación

Una conmutación de retorno tras recuperación es un procedimiento opcional que restaura la configuración original de los sitios de origen y de destino después de una recuperación.



Los administradores de VMware pueden configurar y ejecutar un procedimiento de conmutación tras recuperación cuando estén preparados para restaurar servicios en el sitio de origen original.

NOTA: BlueXP DRaaS replica (resincroniza) cualquier cambio de vuelta a la máquina virtual de origen original antes de revertir la dirección de replicación. Este proceso comienza a partir de una relación que ha

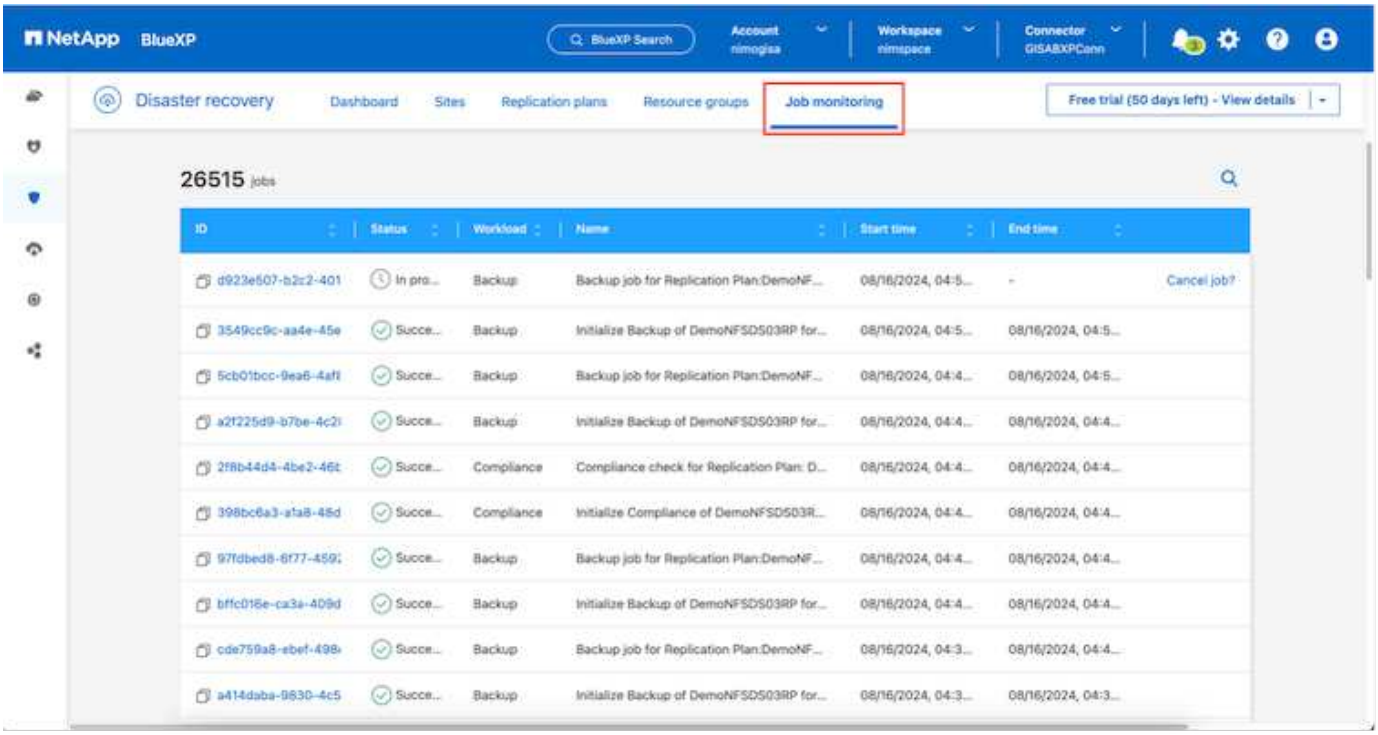
completado la conmutación por error a un destino e implica los siguientes pasos:

- Apagar y cancelar el registro de las máquinas virtuales y los volúmenes del sitio de destino están desmontados.
- Romper la relación de SnapMirror en el origen se rompe para que sea leída/escrita.
- Resincronice la relación de SnapMirror para revertir la replicación.
- Monte el volumen en la fuente, encienda y registre las máquinas virtuales de origen.

Para obtener más información sobre el acceso y la configuración de DRaaS de BlueXP , consulte la "Obtenga más información sobre la recuperación ante desastres de BlueXP para VMware".

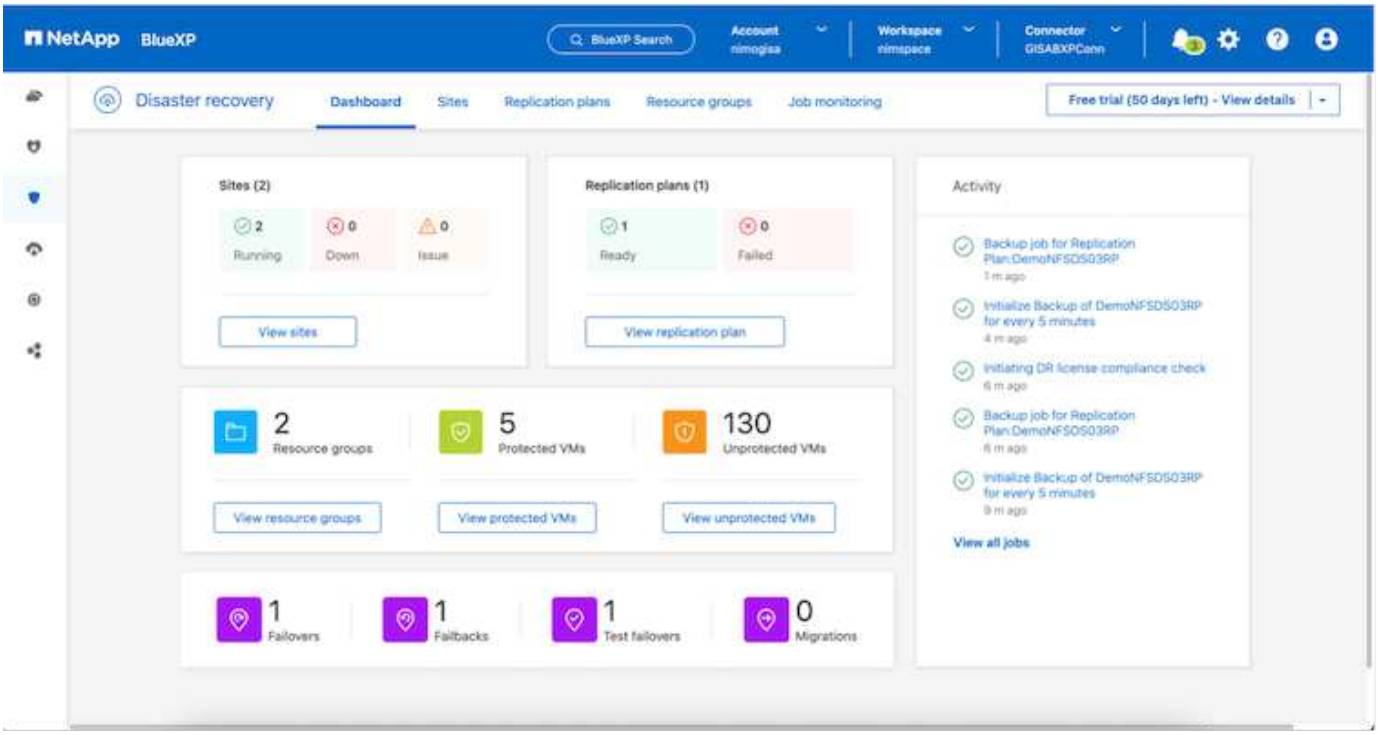
Supervisión y consola

Desde BlueXP o la CLI de ONTAP, se puede supervisar el estado de la replicación de los volúmenes de almacén de datos correspondientes, y se puede rastrear el estado de una conmutación por error o conmutación por error de prueba mediante la supervisión de trabajos.



Si un trabajo se encuentra en curso o en cola y desea detenerlo, existe una opción para cancelarlo.

Con el panel de recuperación ante desastres de BlueXP , evalúe con seguridad el estado de los sitios de recuperación ante desastres y los planes de replicación. Esto permite a los administradores identificar rápidamente sitios y planes en buen estado, desconectados o degradados.



Esto constituye una potente solución que le permite gestionar un plan de recuperación tras siniestros personalizado y personalizado. La conmutación por error se puede realizar como conmutación al respaldo planificada o conmutación al respaldo con un clic de un botón cuando se produce un desastre y se toma la decisión de activar el sitio de recuperación de desastres.

Para obtener más información sobre este proceso, siéntase libre de seguir el video detallado del tutorial o utilice el "simulador de soluciones".

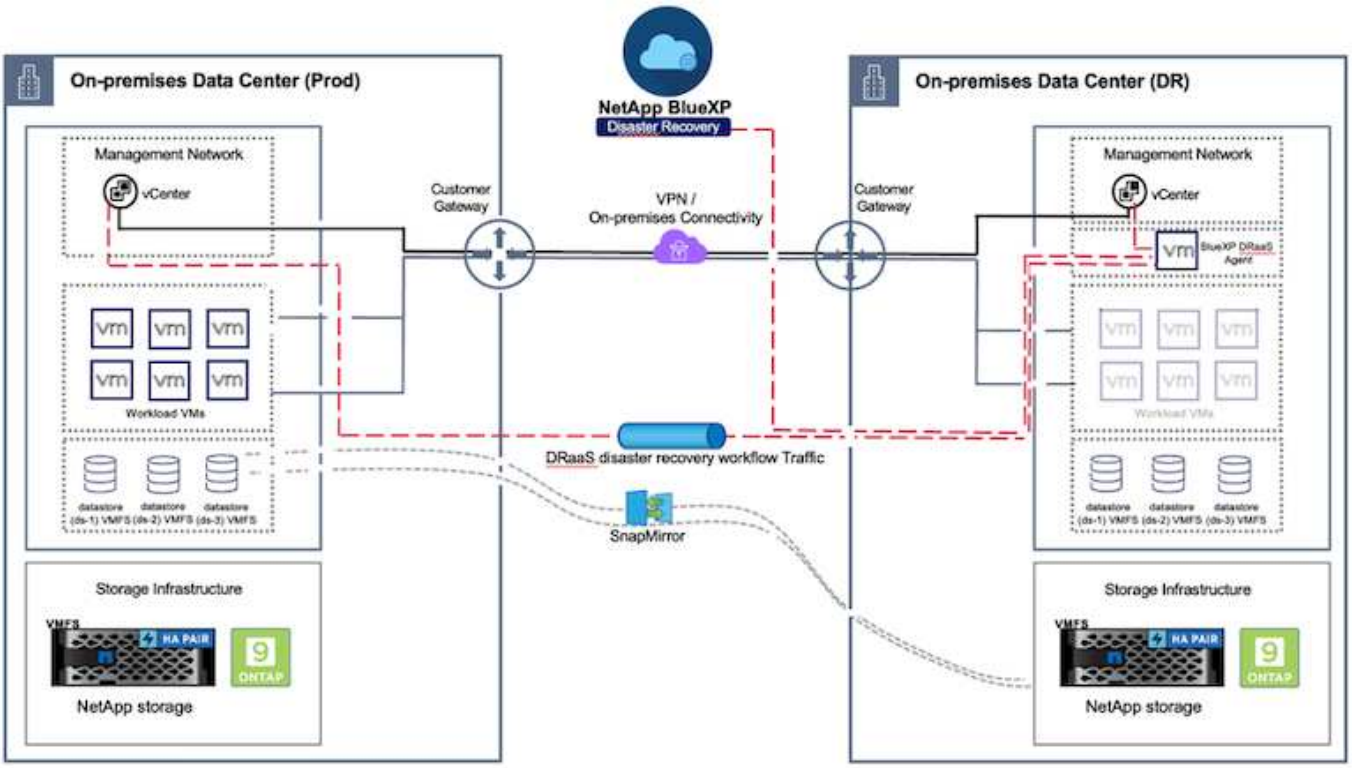
Recuperación ante desastres mediante DRaaS de BlueXP para almacenes de datos de VMFS

La recuperación ante desastres mediante replicación a nivel de bloque desde el sitio de producción hasta el sitio de recuperación de desastres es una forma resiliente y rentable de proteger las cargas de trabajo frente a interrupciones del servicio del sitio y eventos de corrupción de datos, como ataques de ransomware. Con la replicación de NetApp SnapMirror, las cargas de trabajo de VMware que se ejecutan sistemas ONTAP en las instalaciones mediante un almacén de datos VMFS se pueden replicar en otro sistema de almacenamiento de ONTAP en un centro de datos de recuperación designado donde reside VMware

Esta sección del documento describe la configuración de DRaaS de BlueXP para configurar la recuperación ante desastres para máquinas virtuales VMware on-premises en otro sitio designado. Como parte de esta configuración, la cuenta de BlueXP , el conector BlueXP , las cabinas ONTAP se agregaron dentro del espacio de trabajo de BlueXP para permitir la comunicación desde VMware vCenter con el sistema de almacenamiento de ONTAP. Además, este documento detalla cómo configurar la replicación entre sitios y cómo configurar y probar un plan de recuperación. La última sección contiene instrucciones para realizar una conmutación por error completa del sitio y cómo realizar una conmutación por error cuando el sitio principal se recupera y compra en línea.

Mediante el servicio de recuperación ante desastres de BlueXP , integrado en la consola de NetApp BlueXP ,

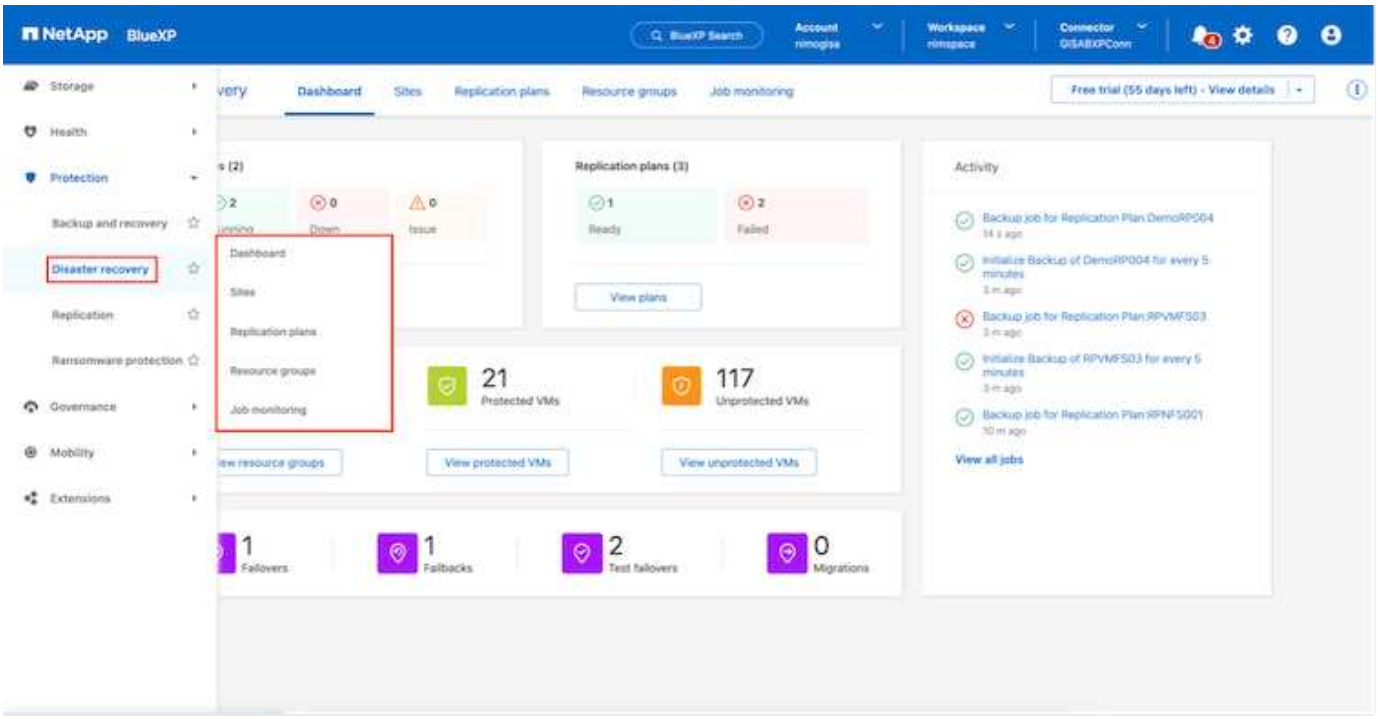
los clientes pueden detectar centros virtuales VMware en sus instalaciones junto con almacenamiento ONTAP, crear grupos de recursos, crear un plan de recuperación ante desastres, asociarlo con grupos de recursos y probar o ejecutar fallos y conmutación tras recuperación. SnapMirror proporciona replicación de bloques a nivel de almacenamiento para mantener los dos sitios actualizados con cambios incrementales, lo que da como resultado un objetivo de punto de recuperación de hasta 5 minutos. También es posible simular los procedimientos de DR como un simulacro regular sin afectar a la producción y los almacenes de datos replicados ni incurrir en costes de almacenamiento adicionales. La recuperación ante desastres de BlueXP aprovecha la tecnología FlexClone de ONTAP para crear una copia del almacén de datos de VMFS con gestión eficiente del espacio de la última copia Snapshot replicada del sitio de recuperación ante desastres. Una vez finalizada la prueba de recuperación ante desastres, los clientes pueden eliminar el entorno de prueba de nuevo sin que ello afecte a los recursos de producción replicados. Cuando exista la necesidad (planificada o no planificada) de recuperación tras fallos real, con unos pocos clics, el servicio de recuperación ante desastres de BlueXP orquestará todos los pasos necesarios para iniciar automáticamente las máquinas virtuales protegidas en el sitio de recuperación ante desastres designado. El servicio también revertirá la relación de SnapMirror con el sitio principal y replicará cualquier cambio del secundario al primario para una operación de conmutación tras recuperación, cuando sea necesario. Todo esto se puede lograr con una fracción de costo en comparación con otras alternativas bien conocidas.



Primeros pasos

Para comenzar a usar la recuperación ante desastres de BlueXP , use la consola de BlueXP y, después, acceda al servicio.

1. Inicie sesión en BlueXP.
2. En el menú de navegación izquierdo de BlueXP , seleccione Protection > Disaster recovery.
3. Aparece la Consola de recuperación de desastres de BlueXP .

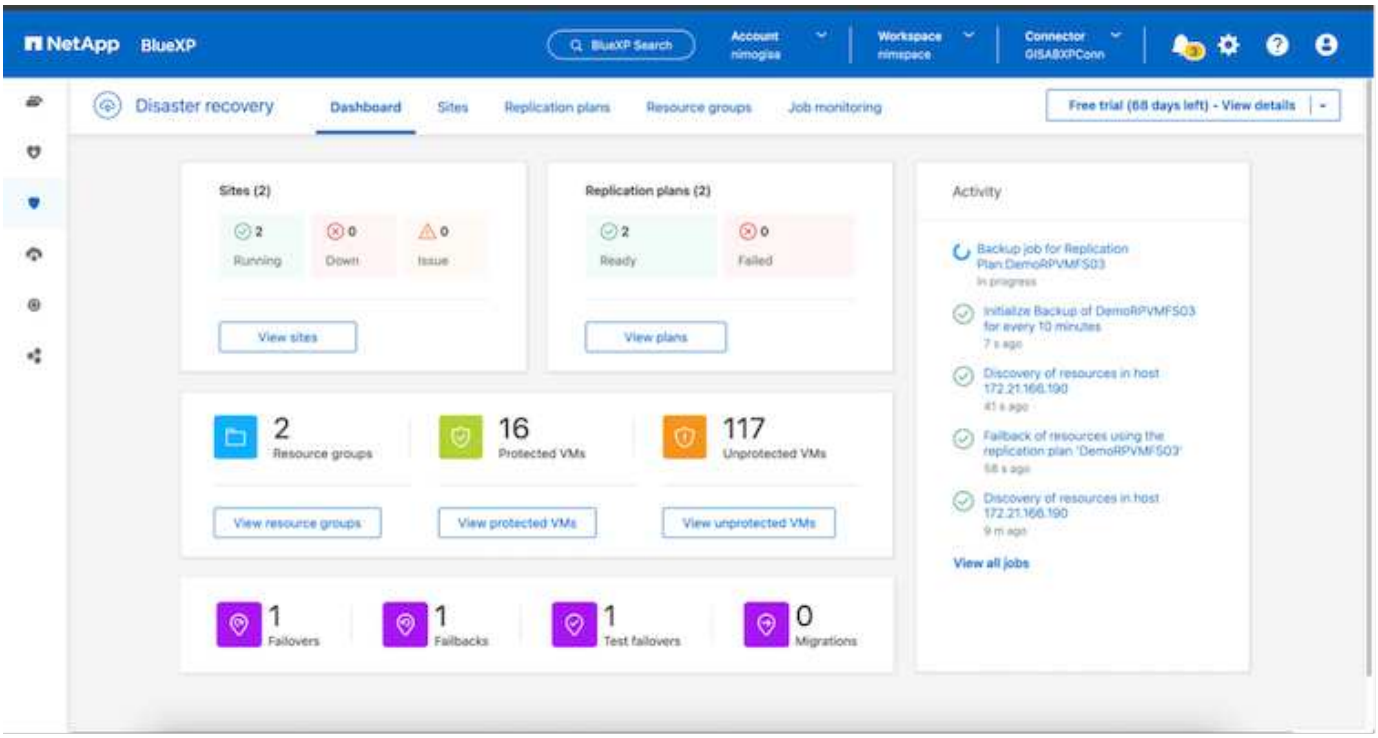


Antes de configurar el plan de recuperación ante desastres, asegúrese de que se cumplan los siguientes requisitos previos:

- El conector BlueXP se configura en NetApp BlueXP . El conector debe ponerse en marcha en AWS VPC.
- La instancia del conector BlueXP tiene conectividad con los sistemas de almacenamiento y vCenter de origen y destino.
- Los sistemas de almacenamiento de NetApp on-premises que alojan almacenes de datos VMFS para VMware se añaden en BlueXP .
- La resolución DNS debe estar en su lugar cuando se utilizan nombres DNS. De lo contrario, use direcciones IP para vCenter.
- La replicación de SnapMirror se configura para los volúmenes de almacén de datos basado en VMFS designados.

Una vez establecida la conectividad entre los sitios de origen y de destino, continúe con los pasos de configuración, que deberían tardar entre 3 y 5 minutos.

NetApp recomienda la instalación del conector BlueXP en el sitio de recuperación de desastres o en un tercer sitio para que el conector BlueXP pueda comunicarse a través de la red con los recursos de origen y de destino en caso de interrupciones del servicio reales o desastres naturales.

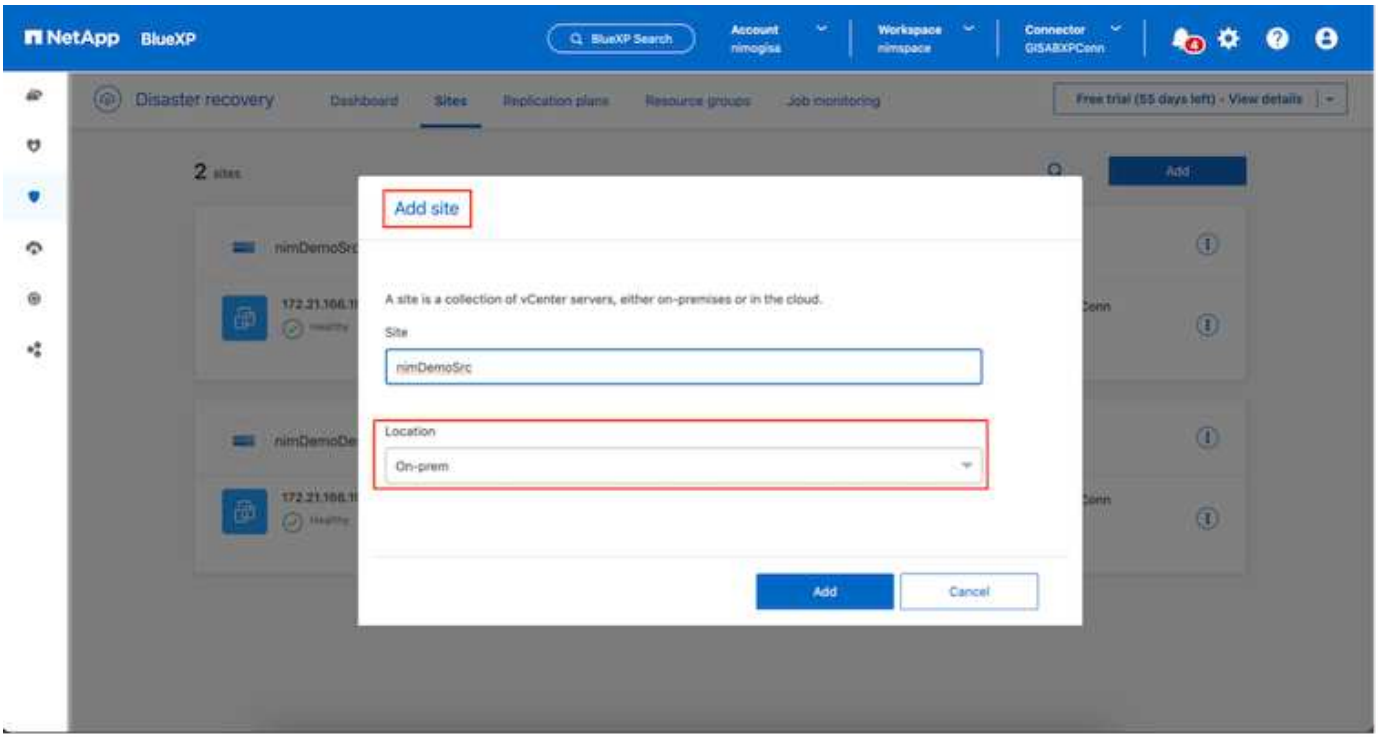


La compatibilidad con almacenes de datos VMFS locales y locales está en una vista previa tecnológica mientras se escribe este documento. La capacidad es compatible con almacenes de datos VMFS basados en protocolos FC e ISCSI.

Configuración de la recuperación de desastres de BlueXP

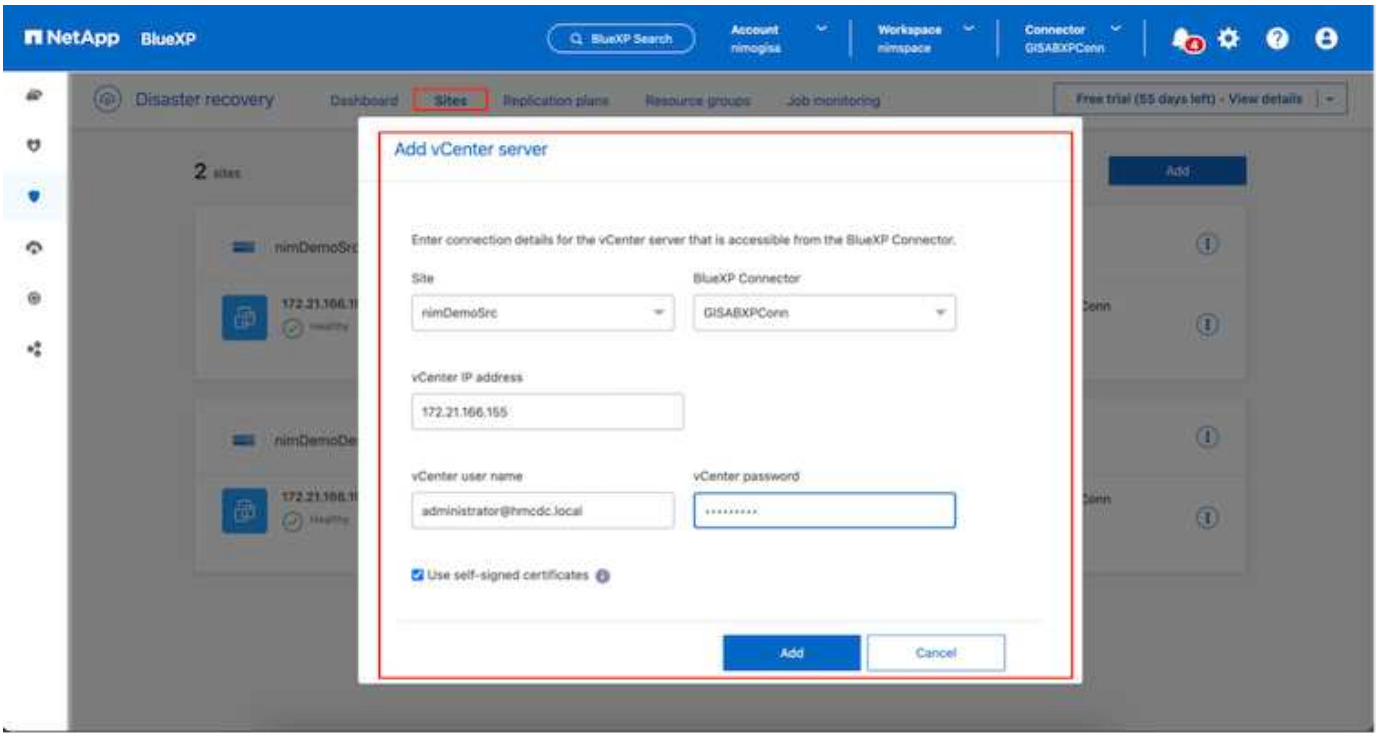
El primer paso para prepararse para la recuperación de desastres es detectar y añadir los recursos de almacenamiento y vCenter en las instalaciones a la recuperación ante desastres de BlueXP .

Asegúrese de agregar los sistemas de almacenamiento de ONTAP al entorno de trabajo dentro del lienzo. Abra la consola de BlueXP y seleccione **Protección > Recuperación ante desastres** en la navegación izquierda. Seleccione **Descubrir servidores de vCenter** o utilice el menú superior, seleccione **Sitios > Agregar > Agregar vCenter**.

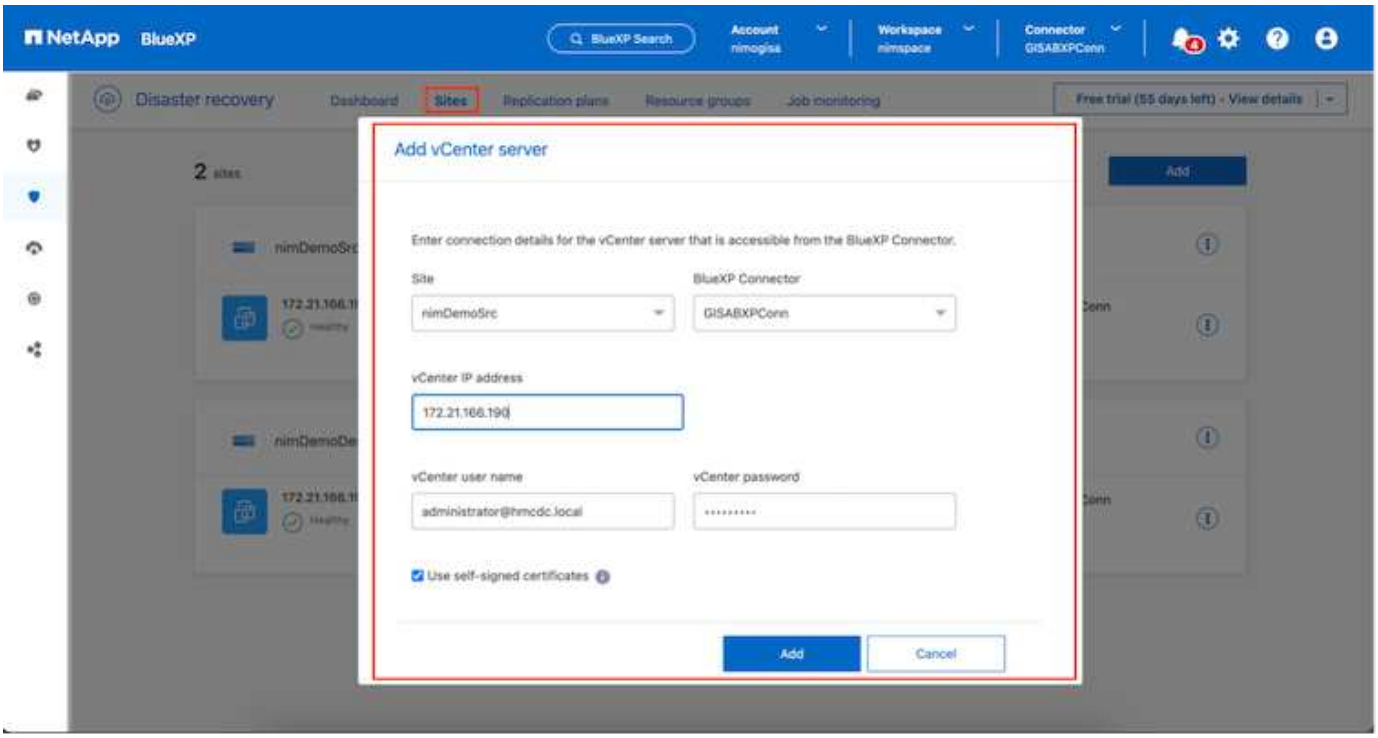


Añada las siguientes plataformas:

- **Fuente**. VCenter en las instalaciones.



- **Destino**. SDDC VMC vCenter.



Una vez que se añaden los vCenter, se activa la detección automatizada.

Configurar la replicación de almacenamiento entre las instalaciones de origen y de destino

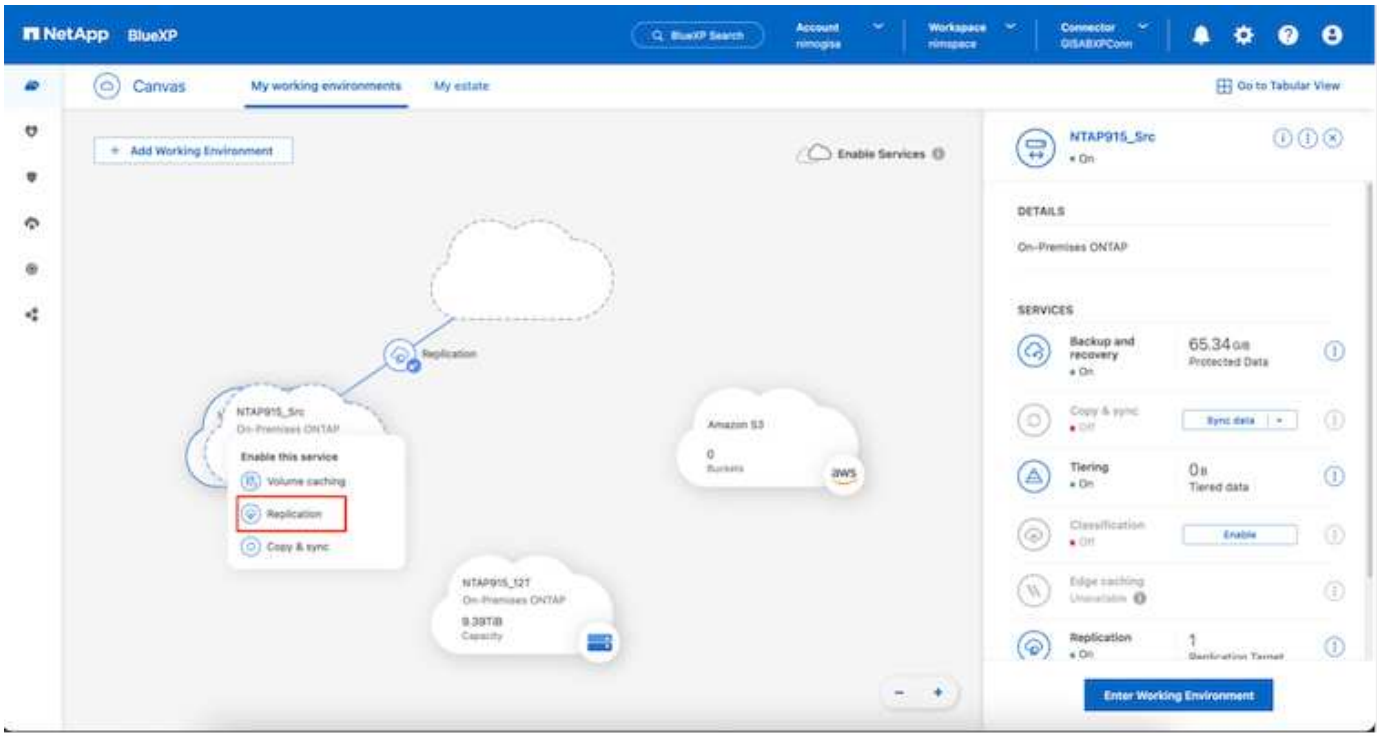
SnapMirror utiliza snapshots de ONTAP para gestionar la transferencia de datos de una ubicación a otra. Inicialmente, una copia completa basada en una copia Snapshot del volumen de origen se copia en el destino para realizar una sincronización básica. A medida que se producen cambios en los datos en el origen, se crea una nueva snapshot y se compara con la snapshot de base. Los bloques que se encontraron que han cambiado se replican en el destino, y la instantánea más reciente se convertirá en la línea base actual o en la instantánea común más reciente. Esto permite que el proceso se repita y que se envíen actualizaciones incrementales al destino.

Cuando se establece una relación de SnapMirror, el volumen de destino se encuentra en estado en línea de solo lectura, y así aún se puede acceder a él. SnapMirror funciona con bloques físicos de almacenamiento, en lugar de hacerlo a un archivo u otro nivel lógico. Esto significa que el volumen de destino es una réplica idéntica del origen, incluidas las snapshots, la configuración de volumen, etc. Si el volumen de origen utiliza funciones de eficiencia del espacio de ONTAP, como la compresión y deduplicación de datos, el volumen replicado conservará estas optimizaciones.

Si se rompe la relación de SnapMirror, el volumen de destino se puede escribir en el volumen de destino y, normalmente, se utilizará para realizar una conmutación al nodo de respaldo cuando se utiliza SnapMirror para sincronizar los datos en un entorno de recuperación de desastres. SnapMirror es lo suficientemente sofisticado para permitir que los datos modificados en el sitio de conmutación por error se resincronicen de manera eficiente de nuevo al sistema primario, en caso de que más adelante vuelva a estar online y, a continuación, se vuelva a establecer la relación con SnapMirror original.

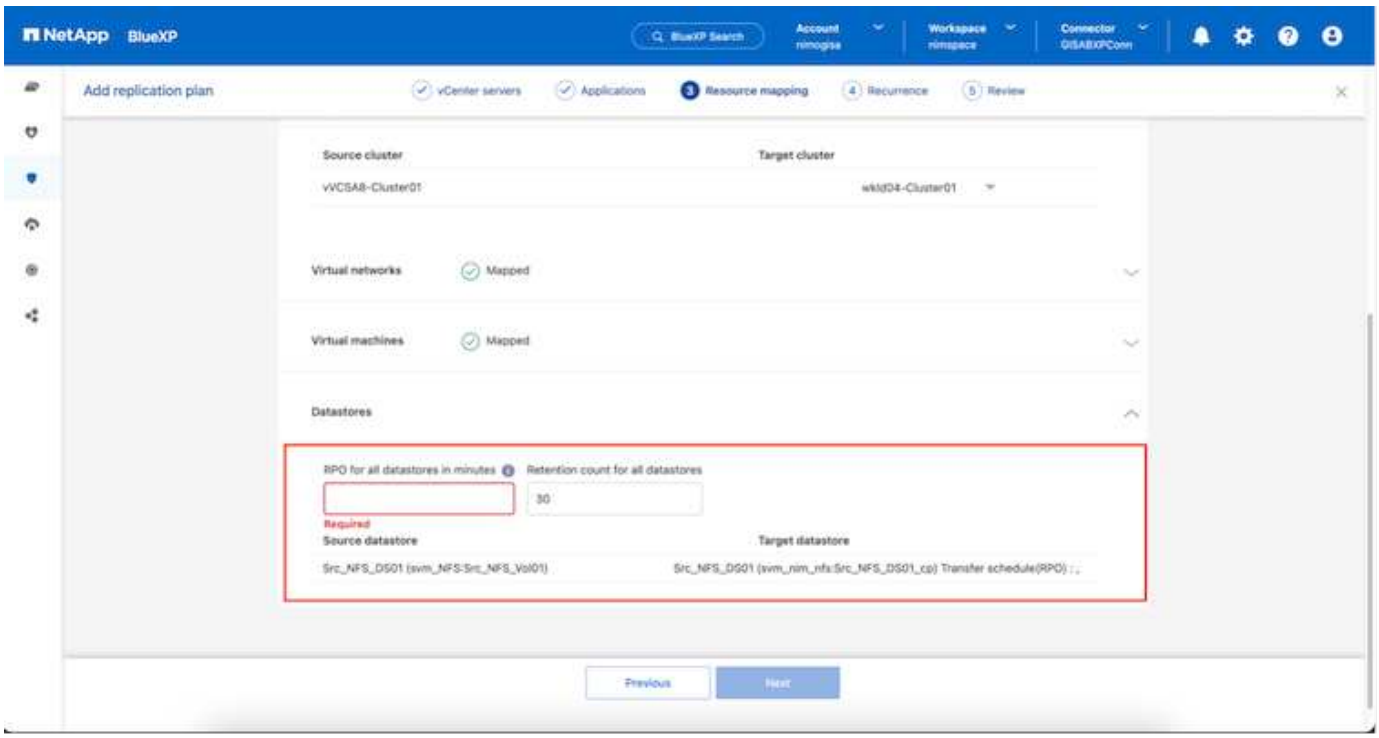
Cómo configurarlo para la recuperación ante desastres de VMware

El proceso para crear una replicación de SnapMirror sigue siendo el mismo para cualquier aplicación dada. El proceso puede ser manual o automatizado. La forma más sencilla es aprovechar BlueXP para configurar la replicación de SnapMirror mediante una simple acción de arrastrar y soltar el sistema ONTAP de origen del entorno en el destino para activar el asistente que guiará durante el resto del proceso.



BlueXP DRaaS también puede automatizar lo mismo siempre que se cumplan los siguientes dos criterios:

- Los clústeres de origen y destino tienen una relación entre iguales.
- La SVM de origen y la SVM de destino tienen una relación entre iguales.

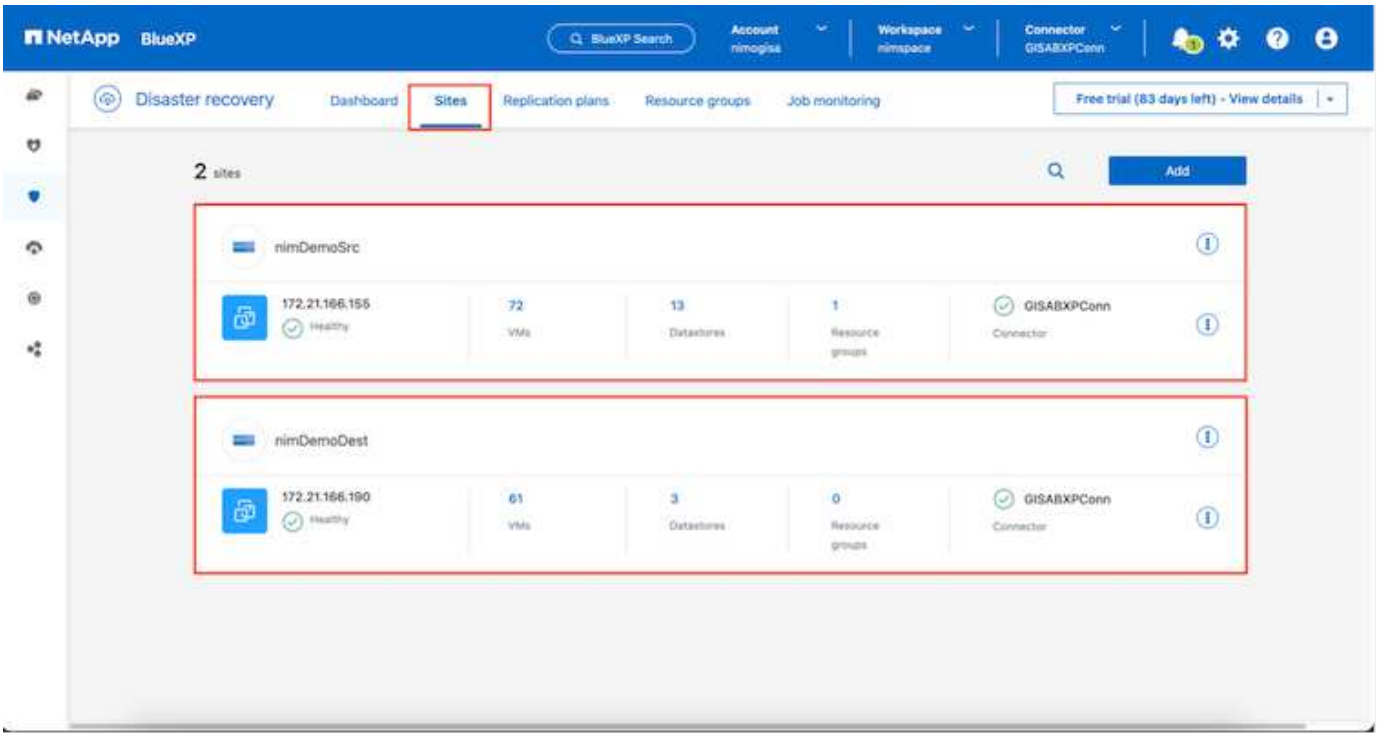


Si la relación de SnapMirror ya se ha configurado para el volumen a través de la interfaz de línea de comandos, BlueXP DRaaS recoge la relación y prosigue con el resto de las operaciones del flujo de trabajo.

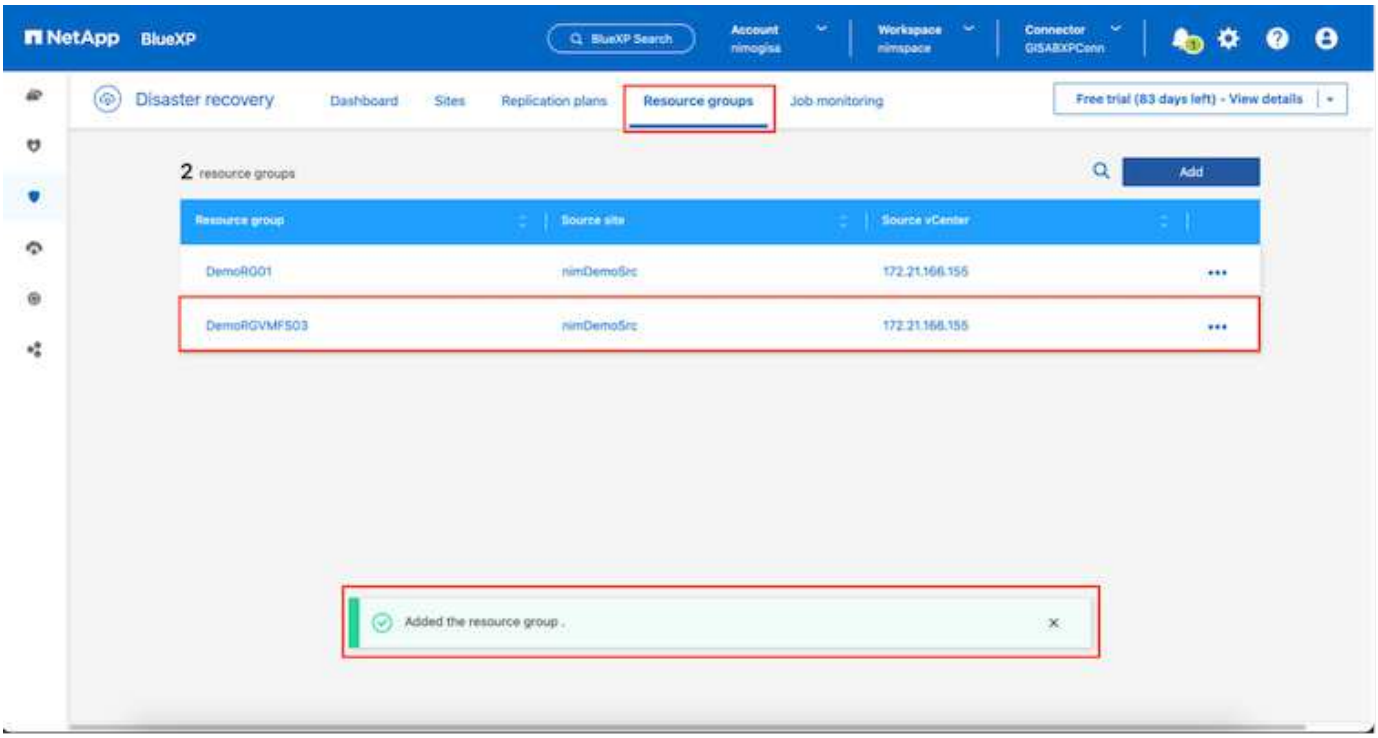
Además de los métodos anteriores, la replicación de SnapMirror también se puede crear mediante CLI de ONTAP o con System Manager. Independientemente del enfoque utilizado para sincronizar los datos mediante SnapMirror, DRaaS de BlueXP coordina el flujo de trabajo para lograr operaciones de recuperación ante desastres eficientes y fluidas.

¿Cómo puede hacer la recuperación ante desastres de BlueXP por usted?

Después de añadir los sitios de origen y de destino, la recuperación de desastres de BlueXP lleva a cabo una detección profunda automática y muestra las máquinas virtuales junto con los metadatos asociados. La recuperación ante desastres de BlueXP también detecta automáticamente las redes y los grupos de puertos que utilizan las máquinas virtuales y los rellena.

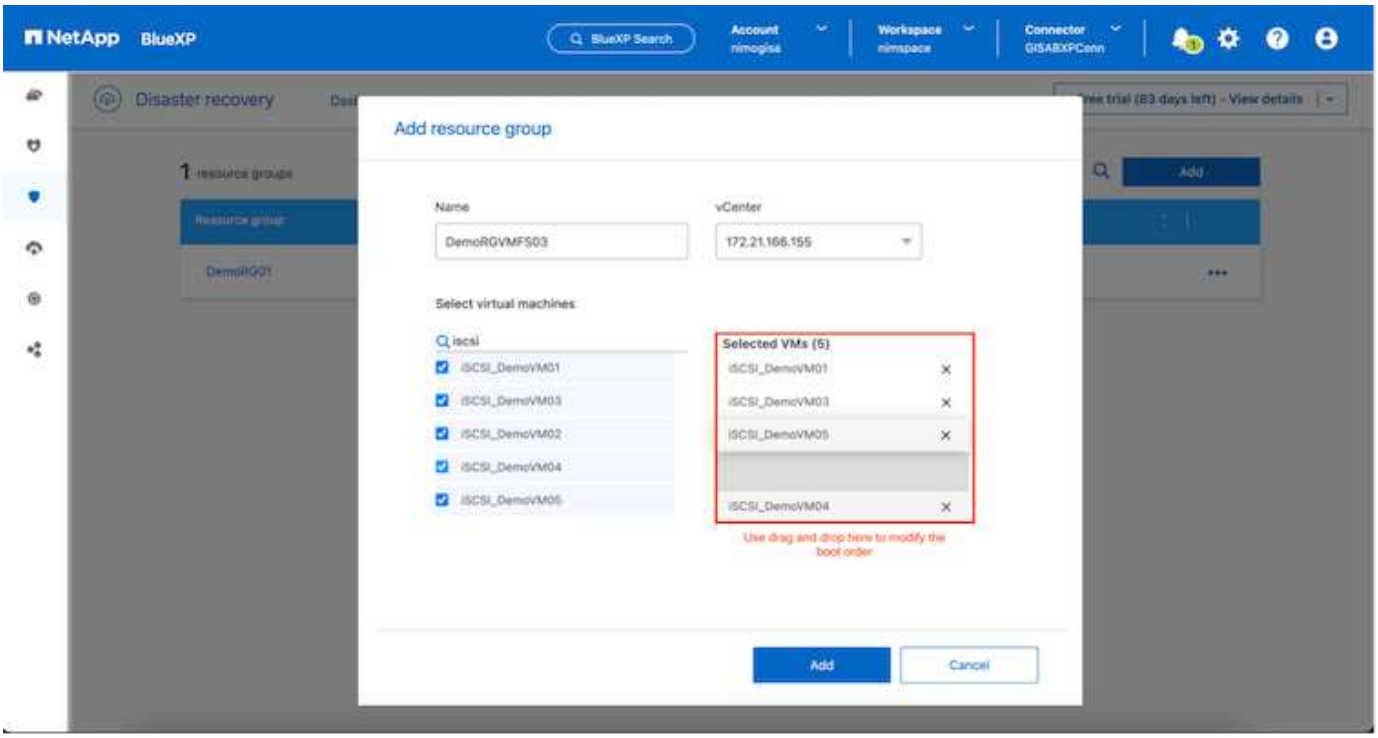


Una vez agregados los sitios, los equipos virtuales se pueden agrupar en grupos de recursos. Los grupos de recursos de recuperación ante desastres de BlueXP le permiten agrupar un conjunto de equipos virtuales dependientes en grupos lógicos que contengan sus órdenes de arranque y retrasos en el arranque que se pueden ejecutar en el momento de su recuperación. Para comenzar a crear grupos de recursos, navegue a **Grupos de recursos** y haga clic en **Crear nuevo grupo de recursos**.

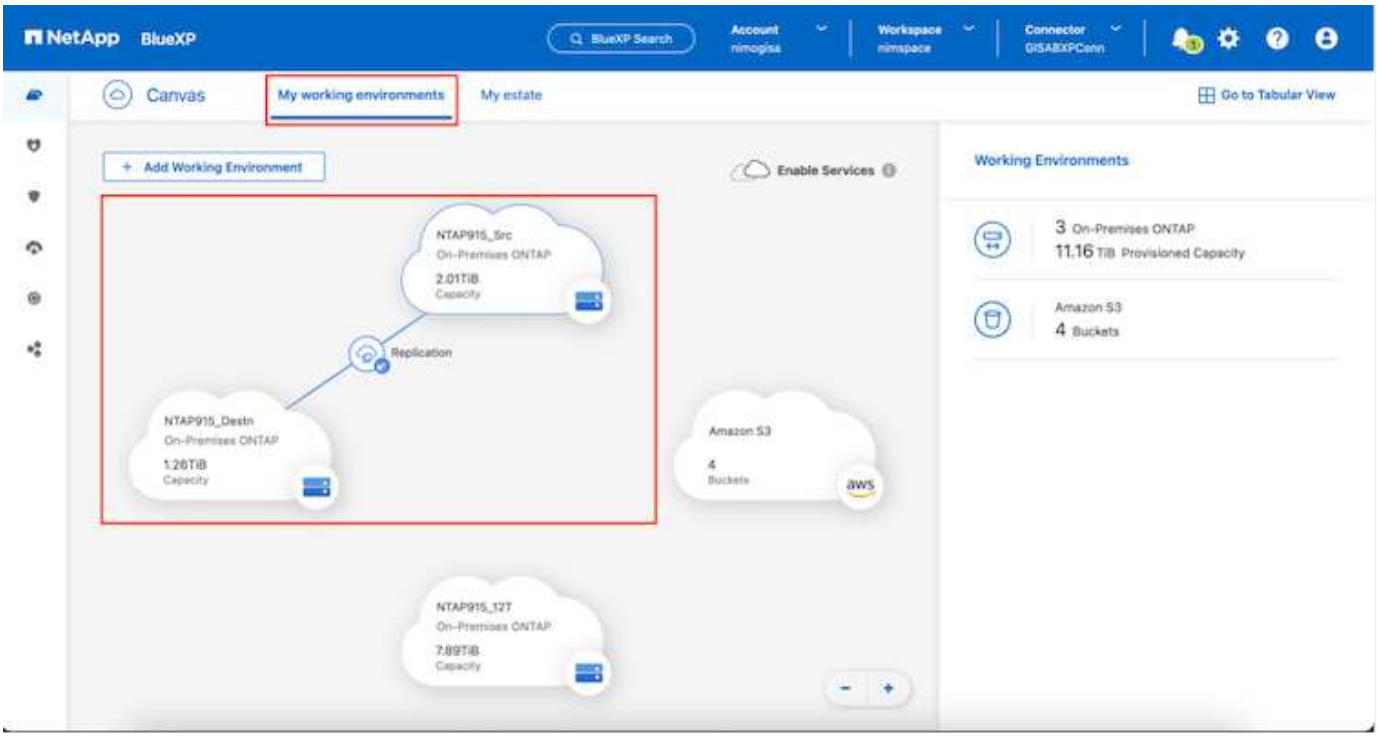


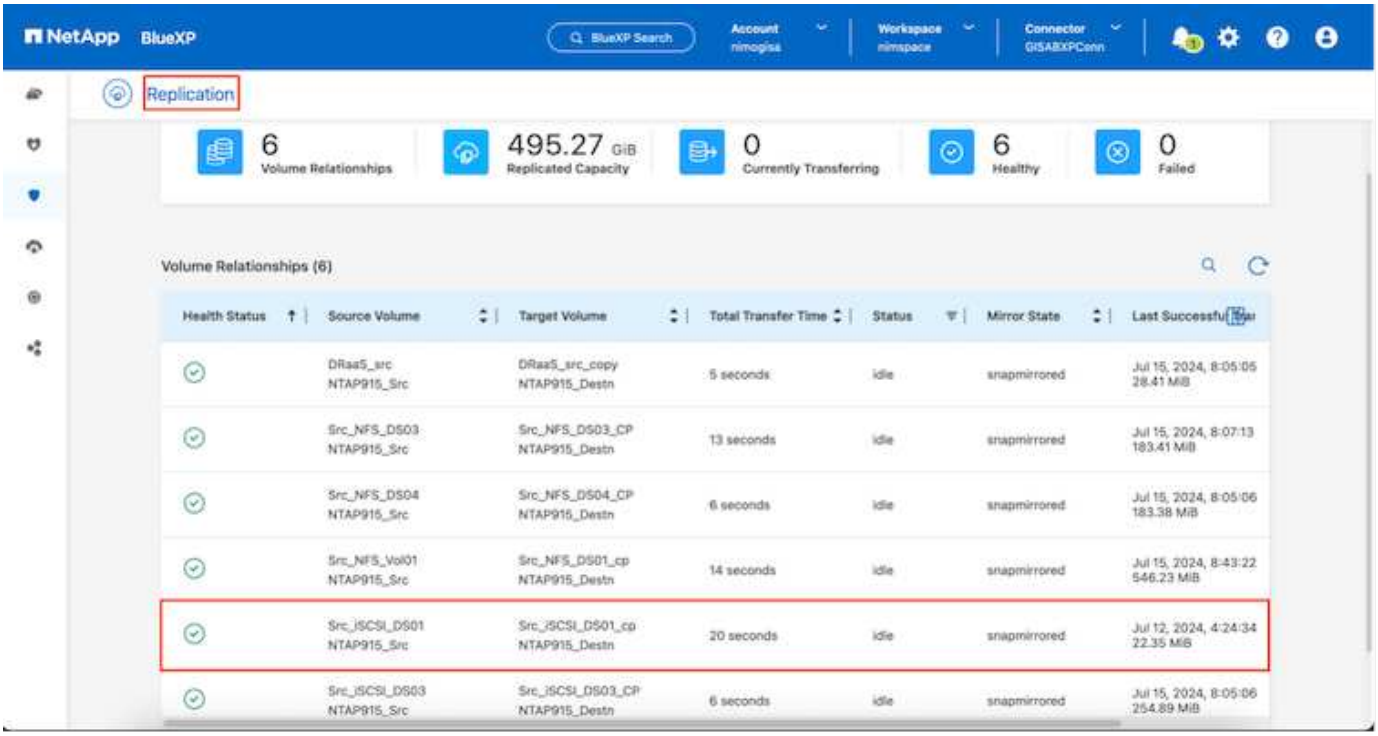
El grupo de recursos también se puede crear al crear un plan de replicación.

El orden de arranque de los equipos virtuales se puede definir o modificar durante la creación de grupos de recursos mediante un sencillo mecanismo de arrastrar y soltar.



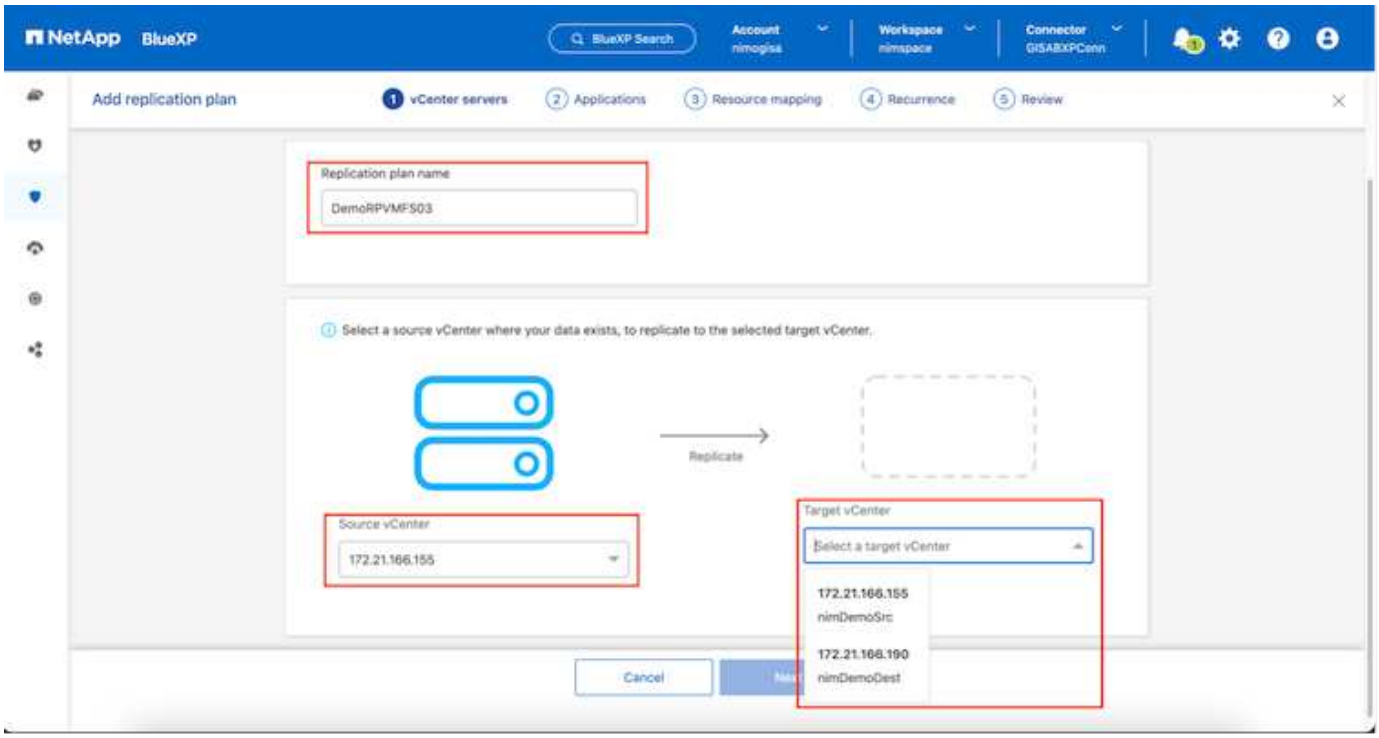
Una vez creados los grupos de recursos, el siguiente paso es crear el plan de ejecución o un plan para recuperar máquinas virtuales y aplicaciones en caso de desastre. Como se ha mencionado en los requisitos previos, la replicación de SnapMirror se puede configurar de antemano o DRaaS puede configurarla usando el RPO y el recuento de retención especificado durante la creación del plan de replicación.



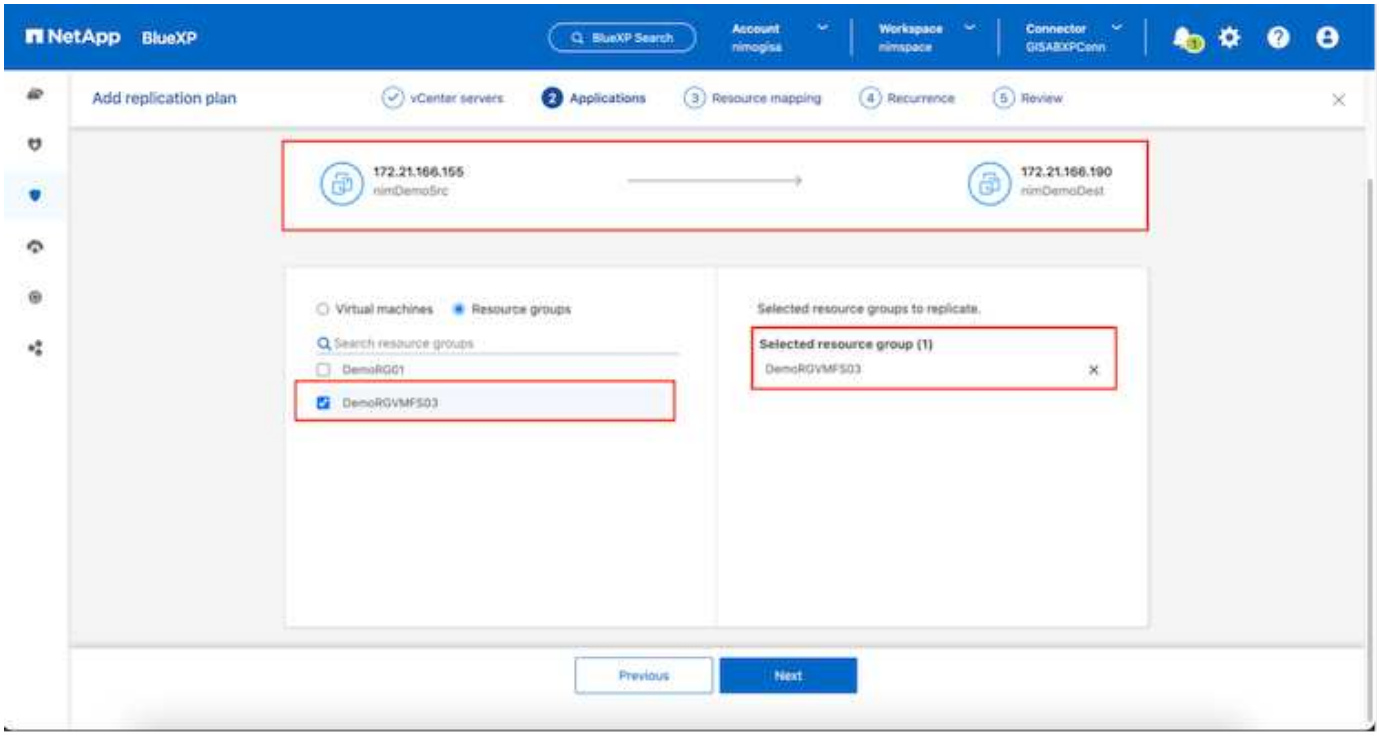


Configure el plan de replicación seleccionando desde el menú desplegable las plataformas vCenter de origen y de destino, y elija los grupos de recursos que se incluirán en el plan, junto con la agrupación de cómo se deben restaurar y encender las aplicaciones y la asignación de clústeres y redes. Para definir el plan de recuperación, vaya a la pestaña **Plan de replicación** y haga clic en **Agregar plan**.

Primero, seleccione la instancia de vCenter de origen y, a continuación, seleccione la instancia de vCenter de destino.



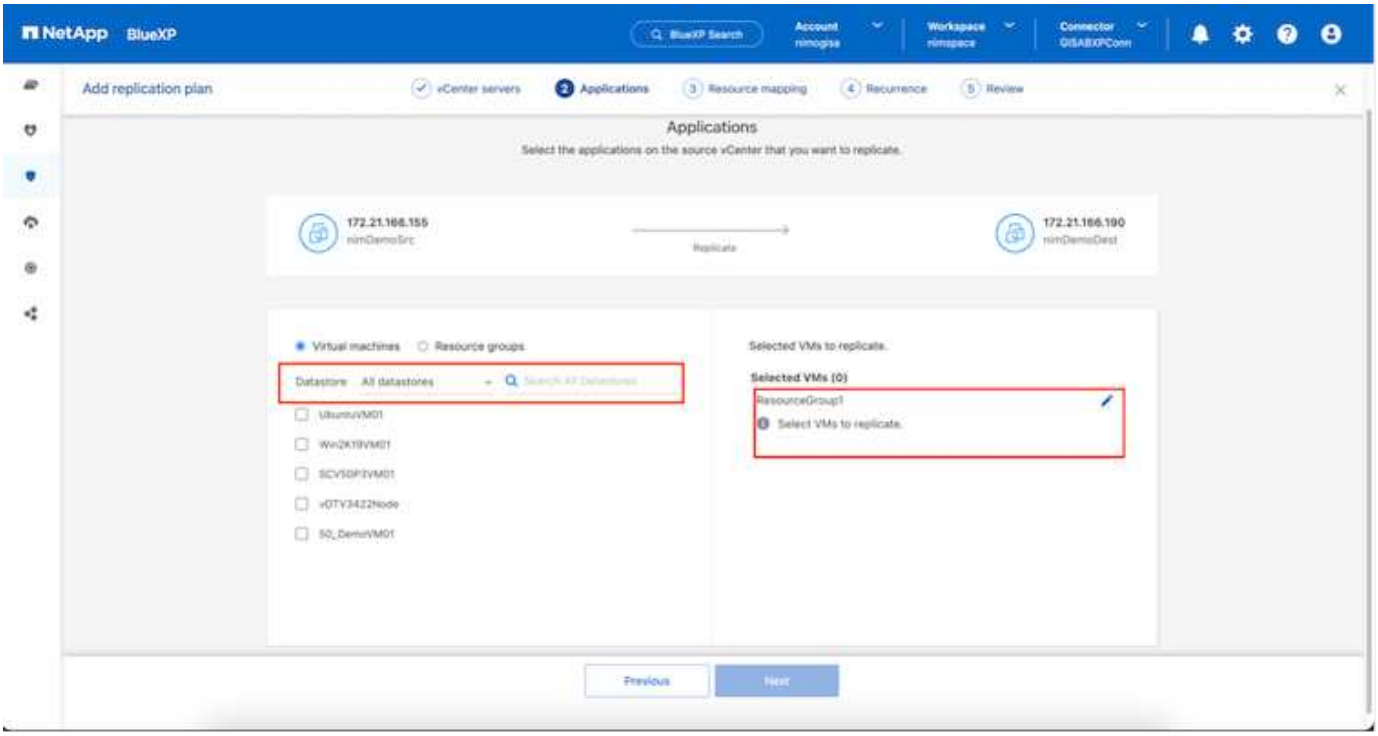
El siguiente paso es seleccionar grupos de recursos existentes. Si no se crearon grupos de recursos, el asistente ayuda a agrupar las máquinas virtuales necesarias (básicamente crear grupos de recursos funcionales) en función de los objetivos de recuperación. Esto también ayuda a definir la secuencia de operaciones de cómo se deben restaurar las máquinas virtuales de aplicaciones.



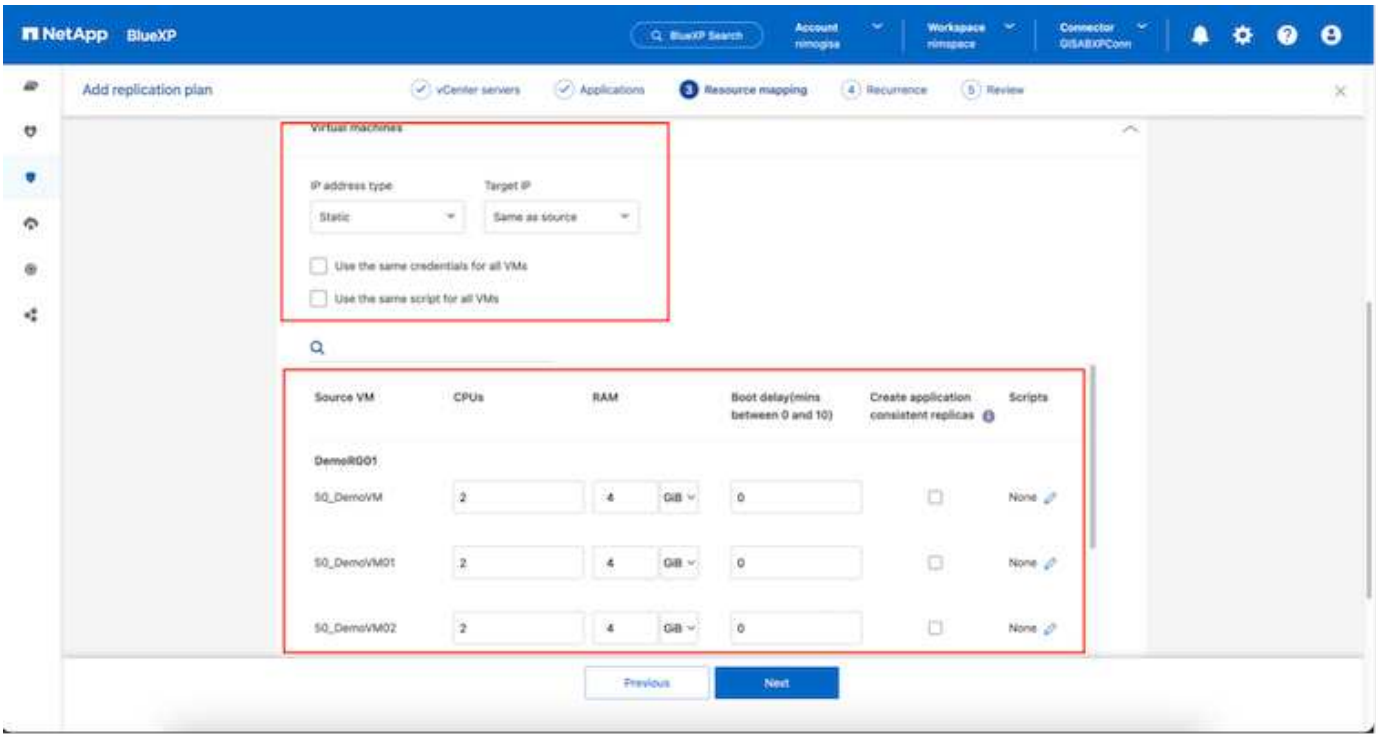
El grupo de recursos permite establecer el orden de inicio mediante la función de arrastrar y soltar. Se puede utilizar para modificar fácilmente el orden en el que se encenderían las VM durante el proceso de recuperación.

Cada máquina virtual de un grupo de recursos se inicia en secuencia según el orden. Dos grupos de recursos se inician en paralelo.

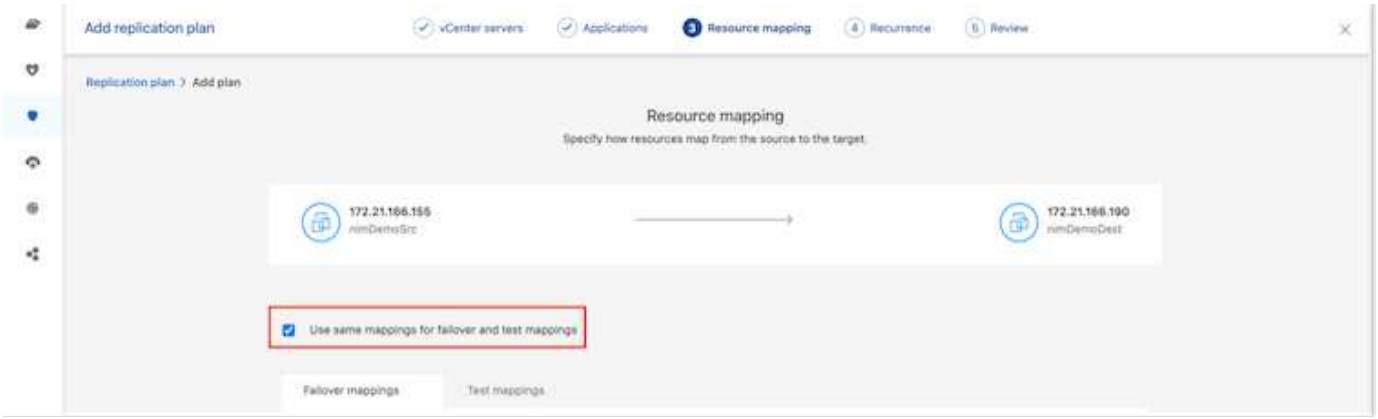
La siguiente captura de pantalla muestra la opción de filtrar máquinas virtuales o almacenes de datos específicos según los requisitos de la organización si no se crean grupos de recursos con antelación.



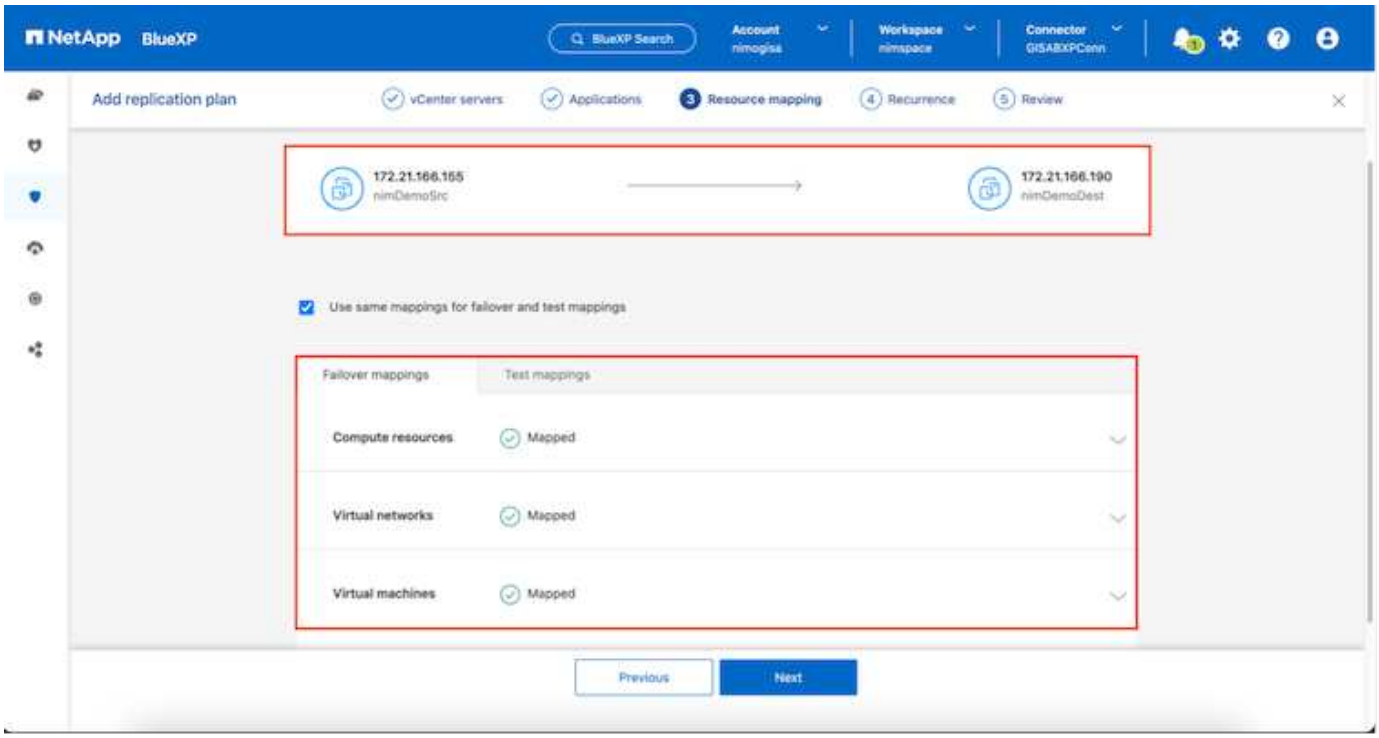
Una vez seleccionados los grupos de recursos, cree las asignaciones de conmutación por error. En este paso, especifique cómo se asignan los recursos del entorno de origen al destino. Esto incluye recursos de computación y redes virtuales. Personalización de IP, scripts previos y posteriores, retrasos en el inicio, coherencia de aplicaciones, etc. Para obtener información detallada, consulte "Cree un plan de replicación".



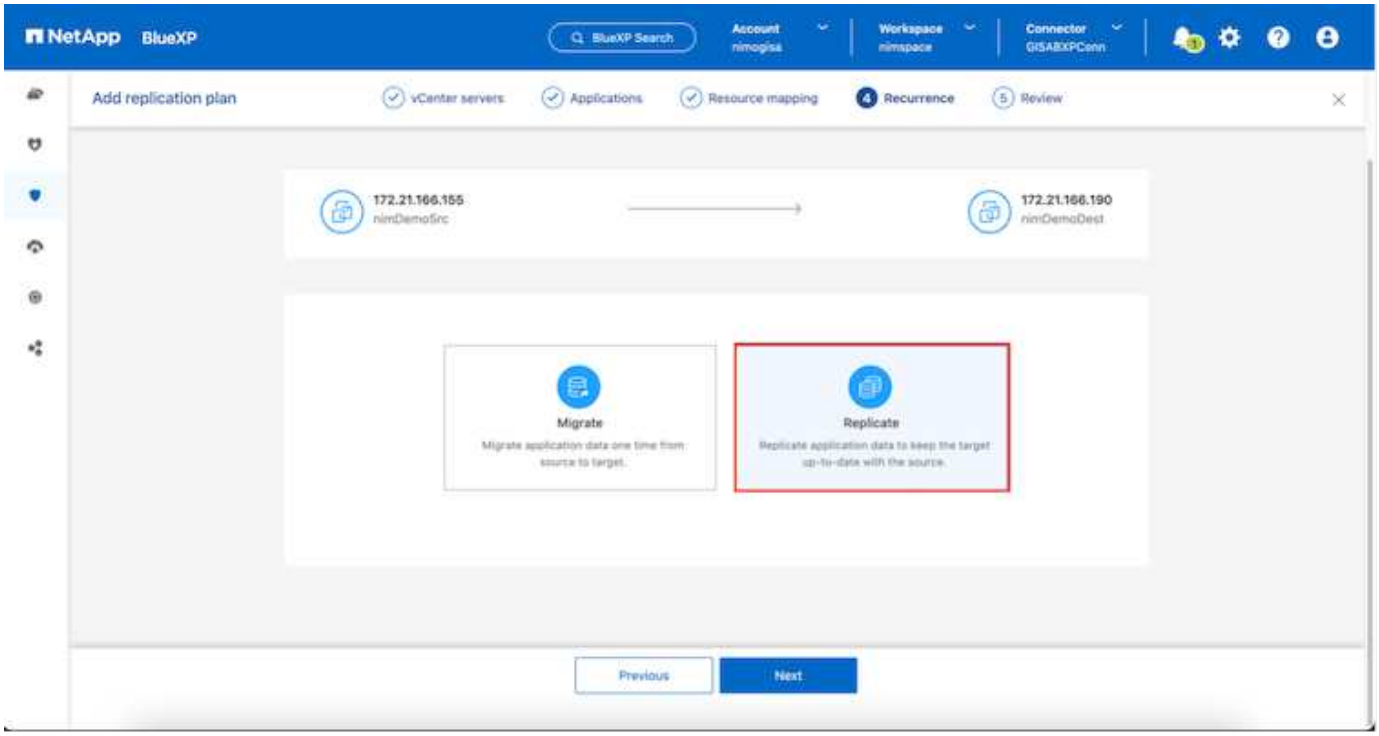
De forma predeterminada, se utilizan los mismos parámetros de asignación para las operaciones de prueba y conmutación por error. Para aplicar diferentes asignaciones al entorno de prueba, seleccione la opción de asignación de prueba después de desactivar la casilla de verificación como se muestra a continuación:



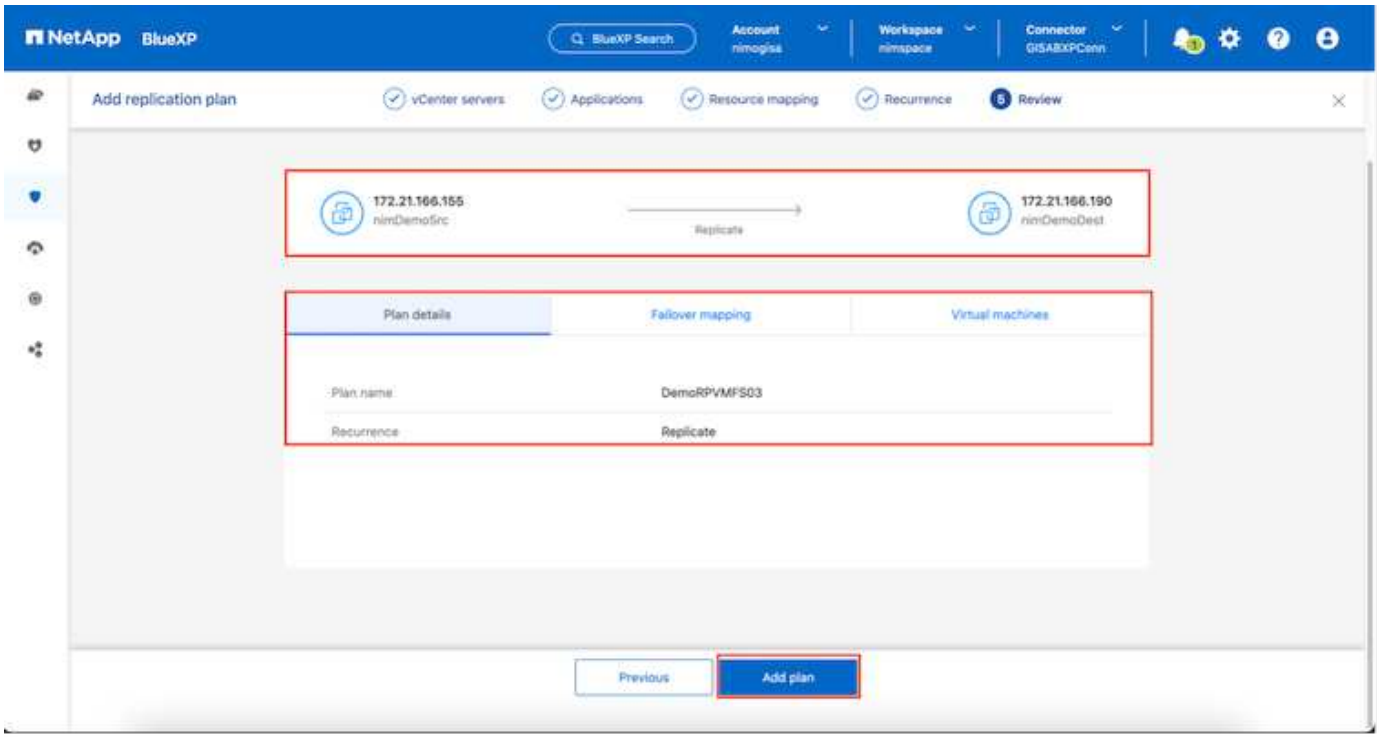
Una vez finalizada la asignación de recursos, haga clic en Siguiente.

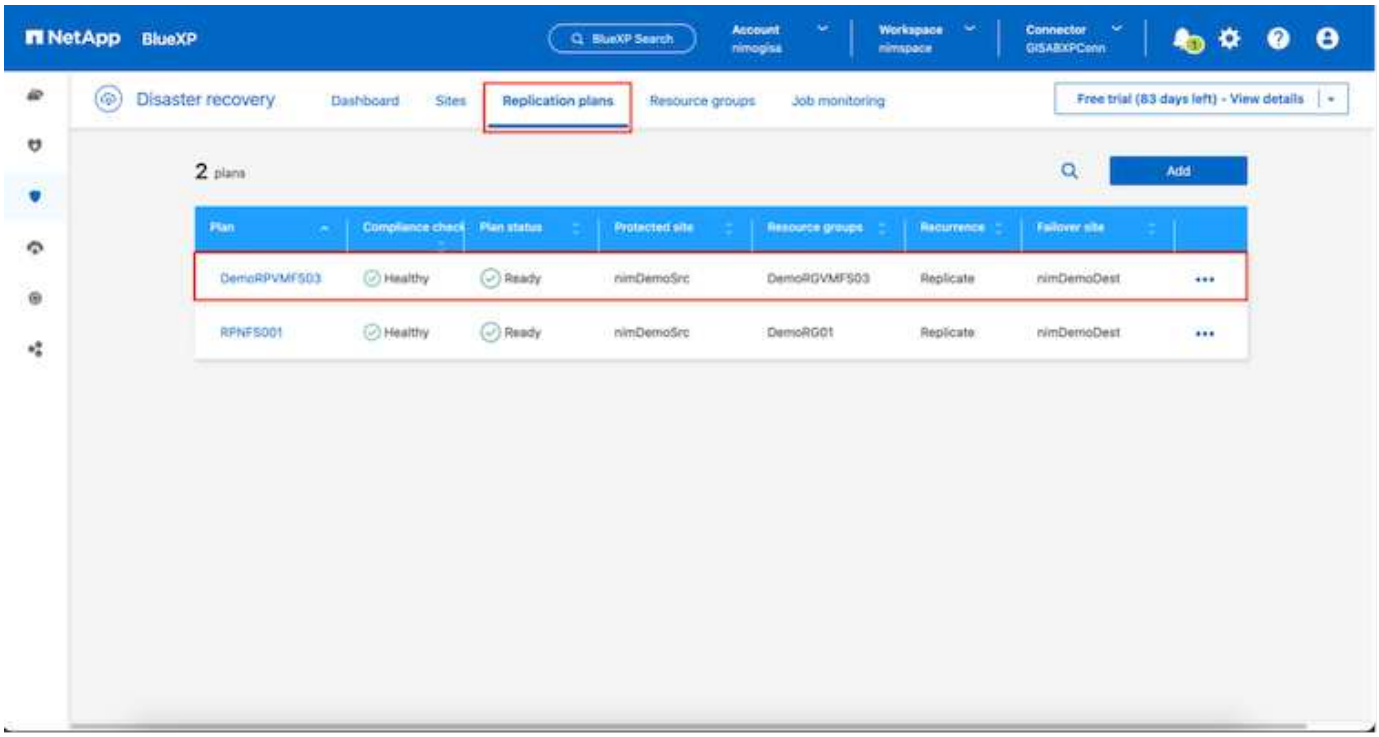


Seleccione el tipo de recurrencia. En pocas palabras, seleccione Migrate (one time migration using failover) o Recurring continuous replication option. En este tutorial, se selecciona la opción Replicar.

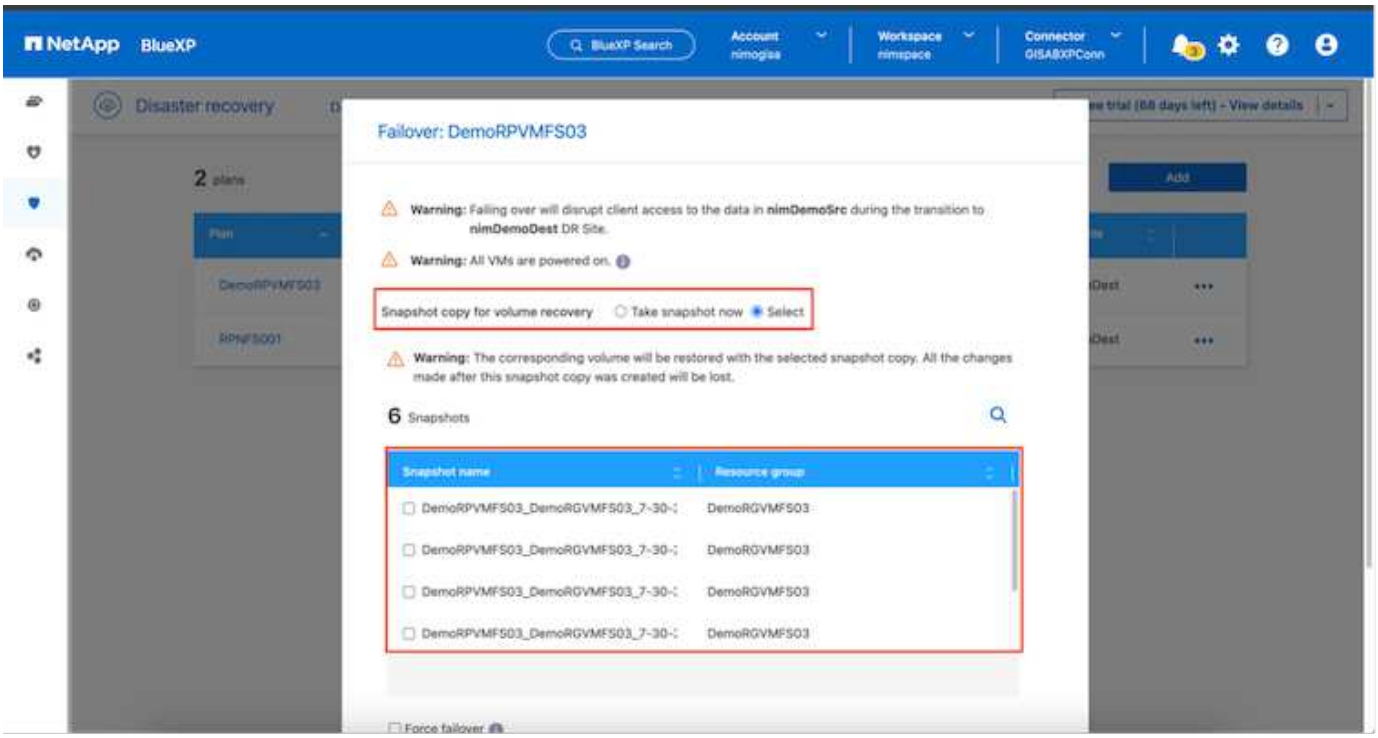


Una vez hecho esto, revise las asignaciones creadas y luego haga clic en Agregar plan.

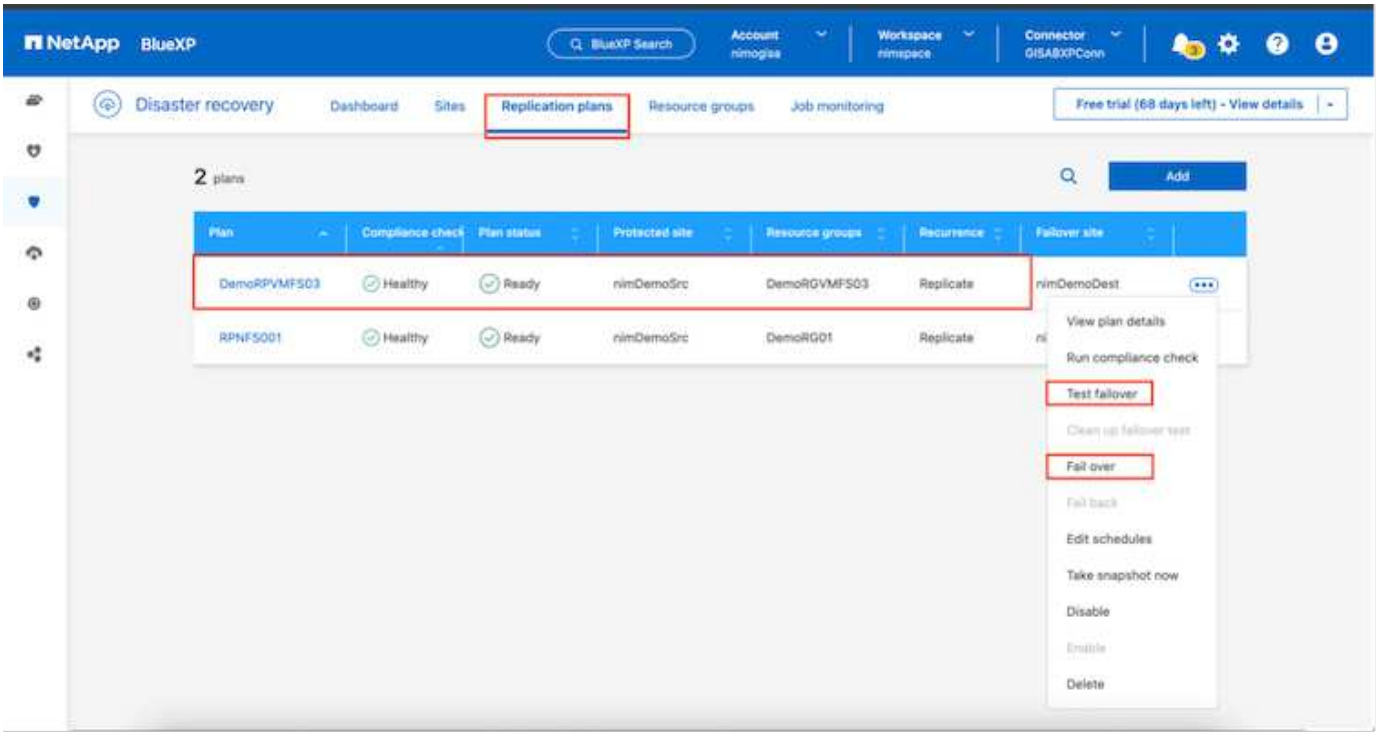




Una vez creado el plan de replicación, se puede realizar una conmutación por error en función de los requisitos seleccionando la opción de conmutación por error, la opción de prueba de conmutación por error o la opción de migración. La recuperación ante desastres de BlueXP garantiza que el proceso de replicación se ejecute según el plan cada 30 minutos. Durante las opciones de conmutación por error y prueba por error, puede utilizar la copia Snapshot de SnapMirror más reciente, o puede seleccionar una copia Snapshot específica de una copia Snapshot de un momento específico (según la política de retención de SnapMirror). La opción point-in-time puede ser muy útil si hay un evento de corrupción como ransomware, donde las réplicas más recientes ya están comprometidas o cifradas. La recuperación ante desastres de BlueXP muestra todos los puntos de recuperación disponibles.



Para activar la conmutación por error o la conmutación por error de prueba con la configuración especificada en el plan de replicación, haga clic en **Failover** o **Test Failover**.

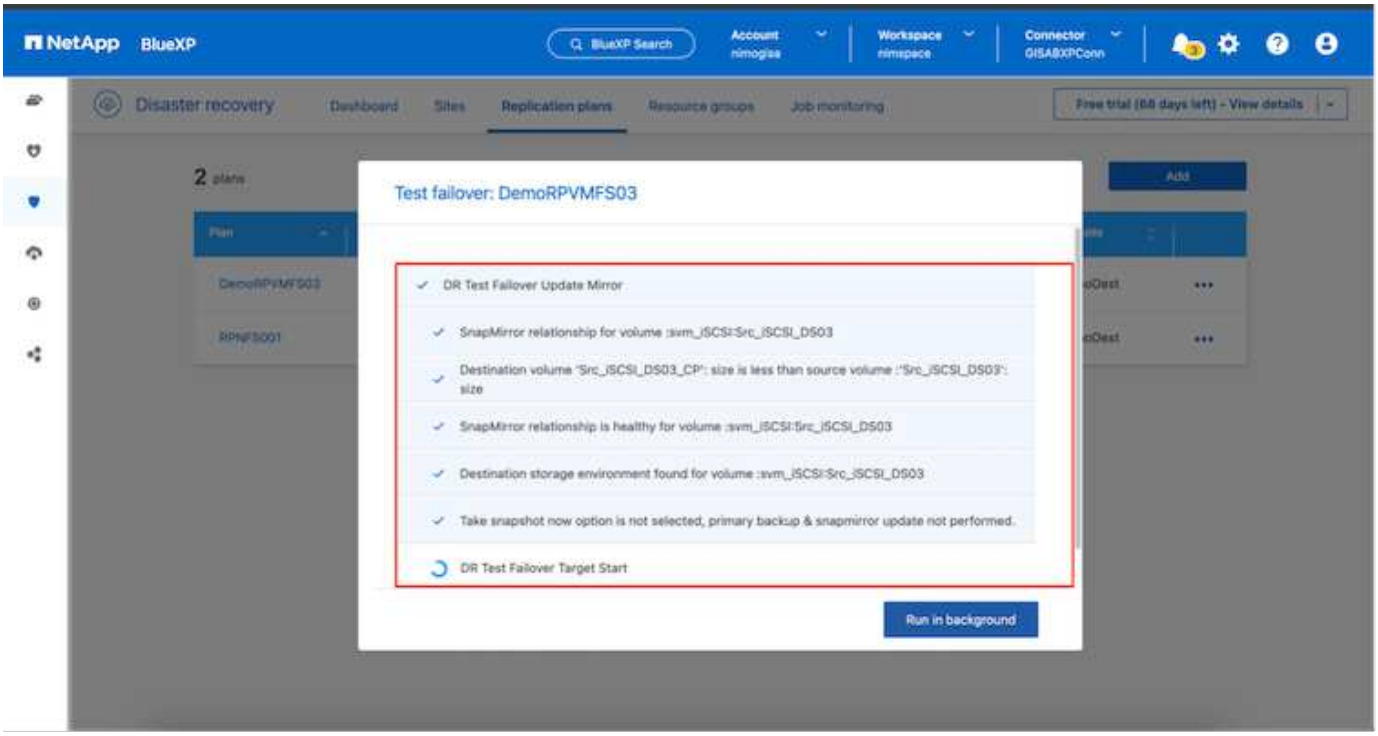


¿Qué sucede durante una operación de failover o failover de prueba?

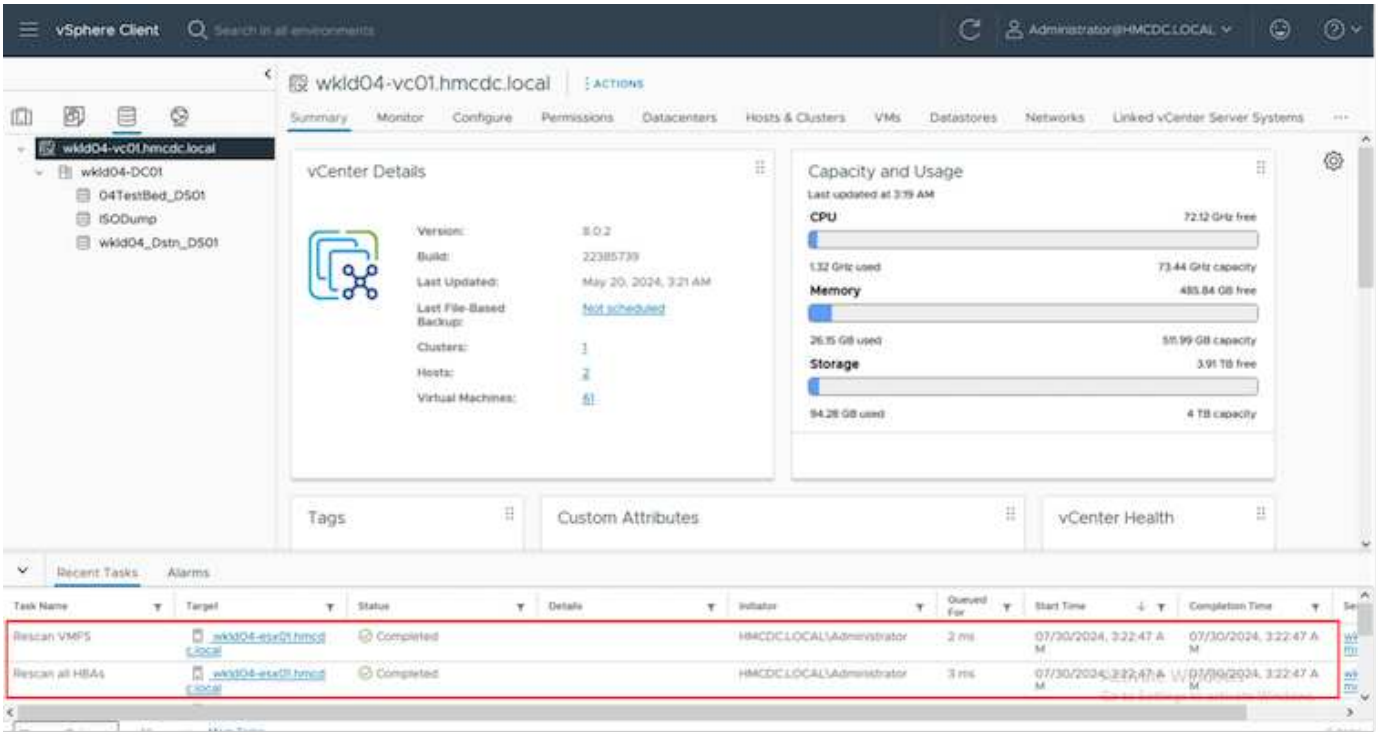
Durante una operación de conmutación al nodo de respaldo de prueba, la recuperación ante desastres de BlueXP crea un volumen FlexClone en el sistema de almacenamiento de ONTAP de destino usando la última copia Snapshot o una copia Snapshot seleccionada del volumen de destino.

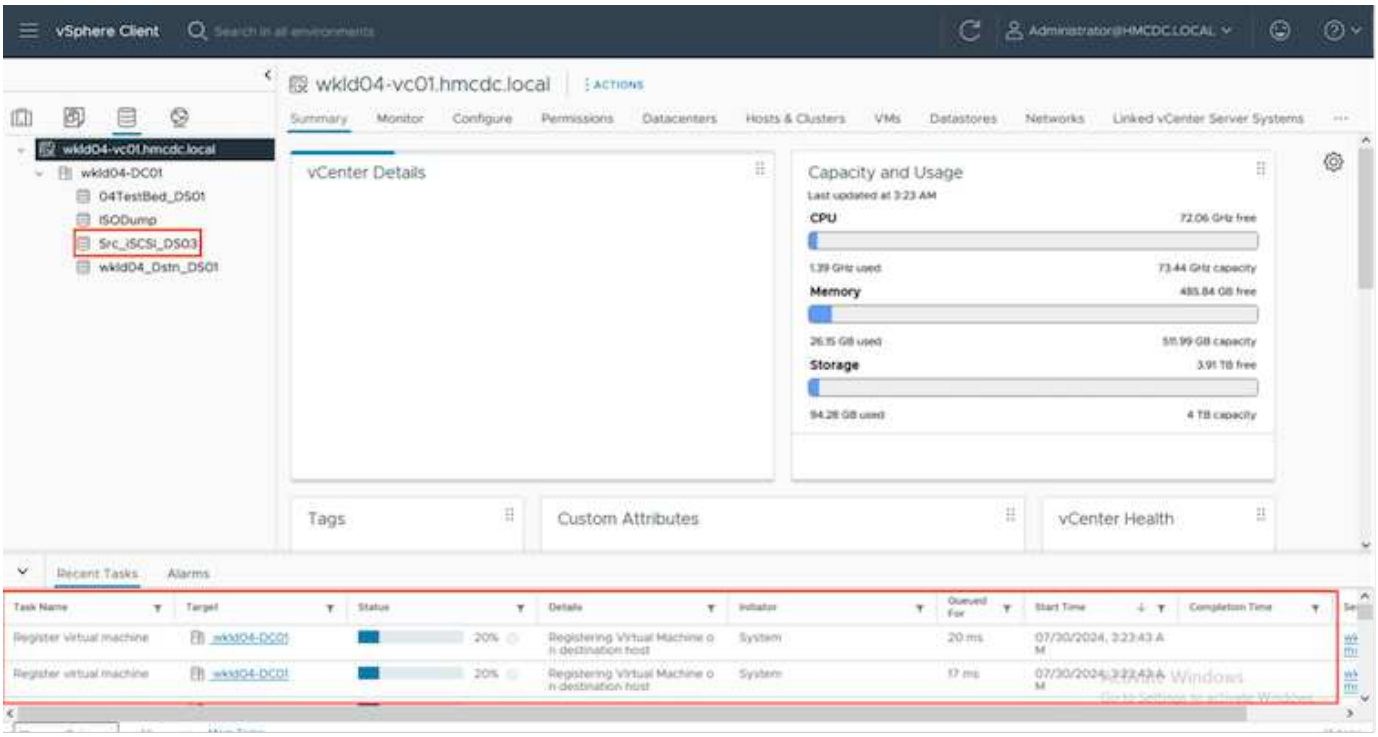
Una operación de prueba al nodo de respaldo crea un volumen clonado en el sistema de almacenamiento ONTAP de destino.

La ejecución de una operación de recuperación de prueba no afecta la replicación de SnapMirror.



Durante el proceso, la recuperación ante desastres de BlueXP no asigna el volumen de destino original. En cambio, posibilita que se asigne un nuevo volumen FlexClone de la Snapshot seleccionada y un almacén de datos temporal que respalda el volumen de FlexClone a los hosts ESXi.

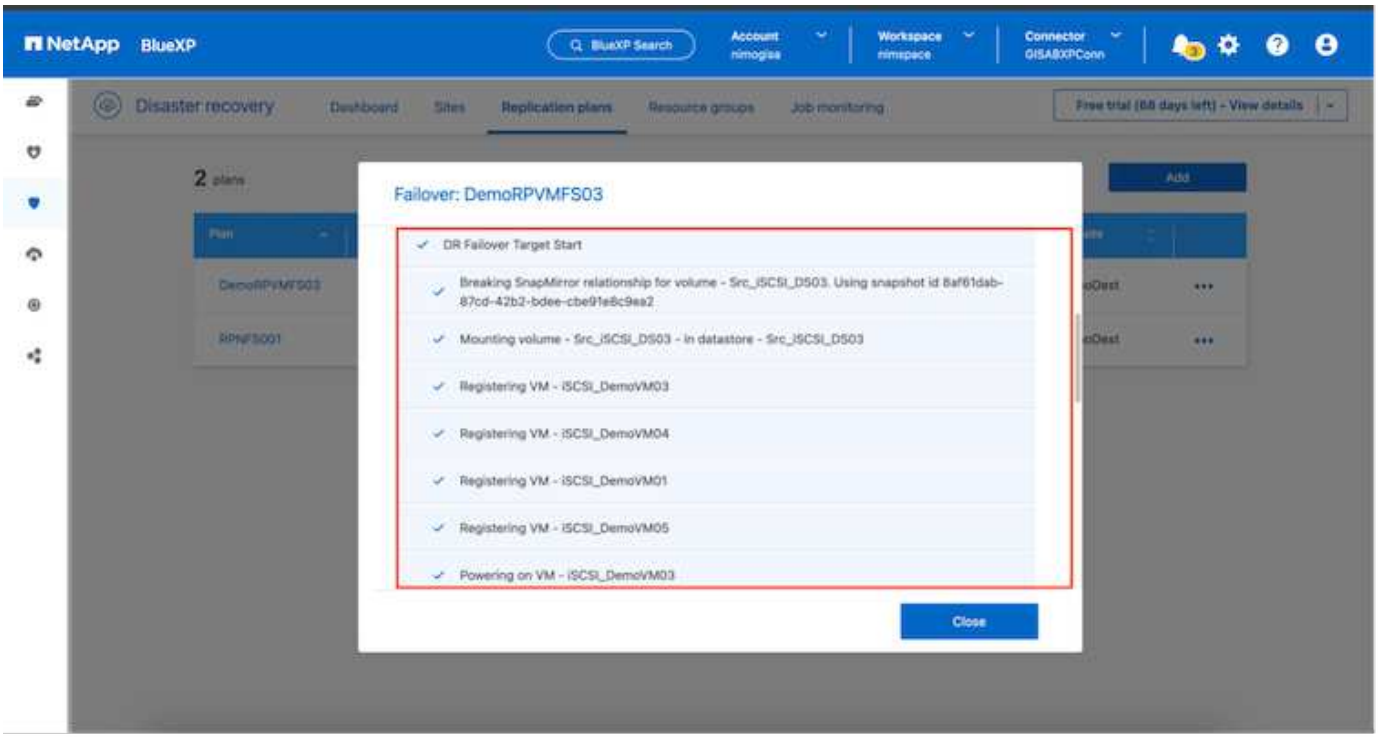




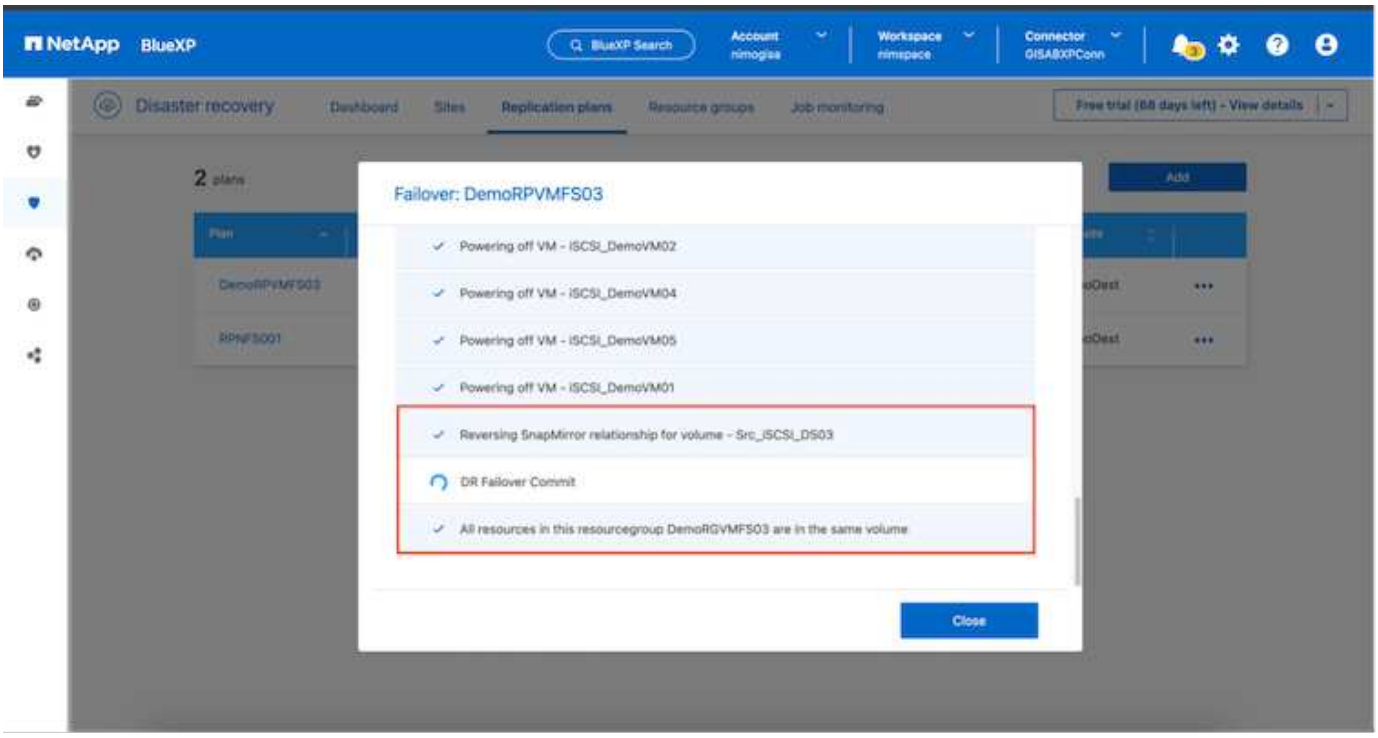
Cuando se complete la operación de failover de prueba, la operación de limpieza se puede activar utilizando **"Prueba de failover de limpieza"**. Durante esta operación, la recuperación ante desastres de BlueXP destruye el volumen de FlexClone que se utilizó en la operación.

En caso de que se produzca un desastre real, la recuperación de desastres de BlueXP realiza los siguientes pasos:

1. Interrumpe la relación SnapMirror entre los sitios.
2. Monta el volumen de almacenes de datos de VMFS después de la firma para su uso inmediato.
3. Registre las máquinas virtuales
4. Encienda las máquinas virtuales



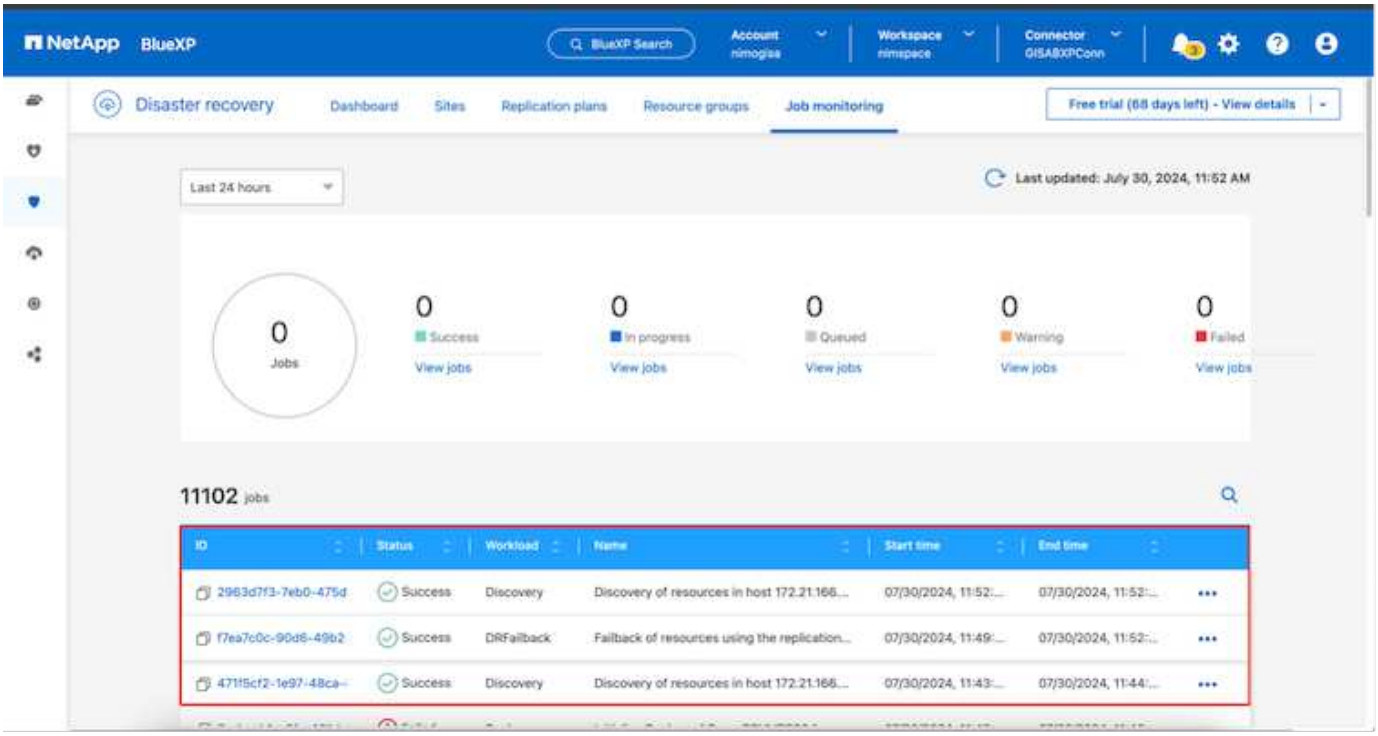
Una vez que el sitio principal está en funcionamiento, la recuperación ante desastres de BlueXP permite realizar una resincronización inversa para SnapMirror y posibilita la conmutación de retorno tras recuperación, que puede hacerse de nuevo con un solo clic.



Y, si se elige la opción de migración, se considera un evento de conmutación al respaldo planificado. En este caso, se activa un paso adicional que consiste en apagar las máquinas virtuales en el sitio de origen. El resto de los pasos sigue siendo el mismo que el evento de conmutación por error.

Desde BlueXP o la CLI de ONTAP, se puede supervisar el estado de la replicación de los volúmenes de almacén de datos correspondientes, y se puede rastrear el estado de una conmutación por error o

conmutación por error de prueba mediante la supervisión de trabajos.



Esto constituye una potente solución que le permite gestionar un plan de recuperación tras siniestros personalizado y personalizado. La conmutación por error se puede realizar como conmutación al respaldo planificada o conmutación al respaldo con un clic de un botón cuando se produce un desastre y se toma la decisión de activar el sitio de recuperación de desastres.

Para obtener más información sobre este proceso, siéntase libre de seguir el video detallado del tutorial o utilice el "simulador de soluciones".