

Configurar la protección de datos en Hyperflex

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Información general adicional](#)

[Procedimiento](#)

[Consideraciones sobre grupos de protección](#)

[Troubleshoot](#)

[Verificar configuración de protección de VM](#)

[Supervisar actividades de replicación](#)

[Problemas comunes](#)

[Problemas de pares](#)

[Inconvenientes de conectividad](#)

[Problemas de protección](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar la replicación en Hyperflex.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

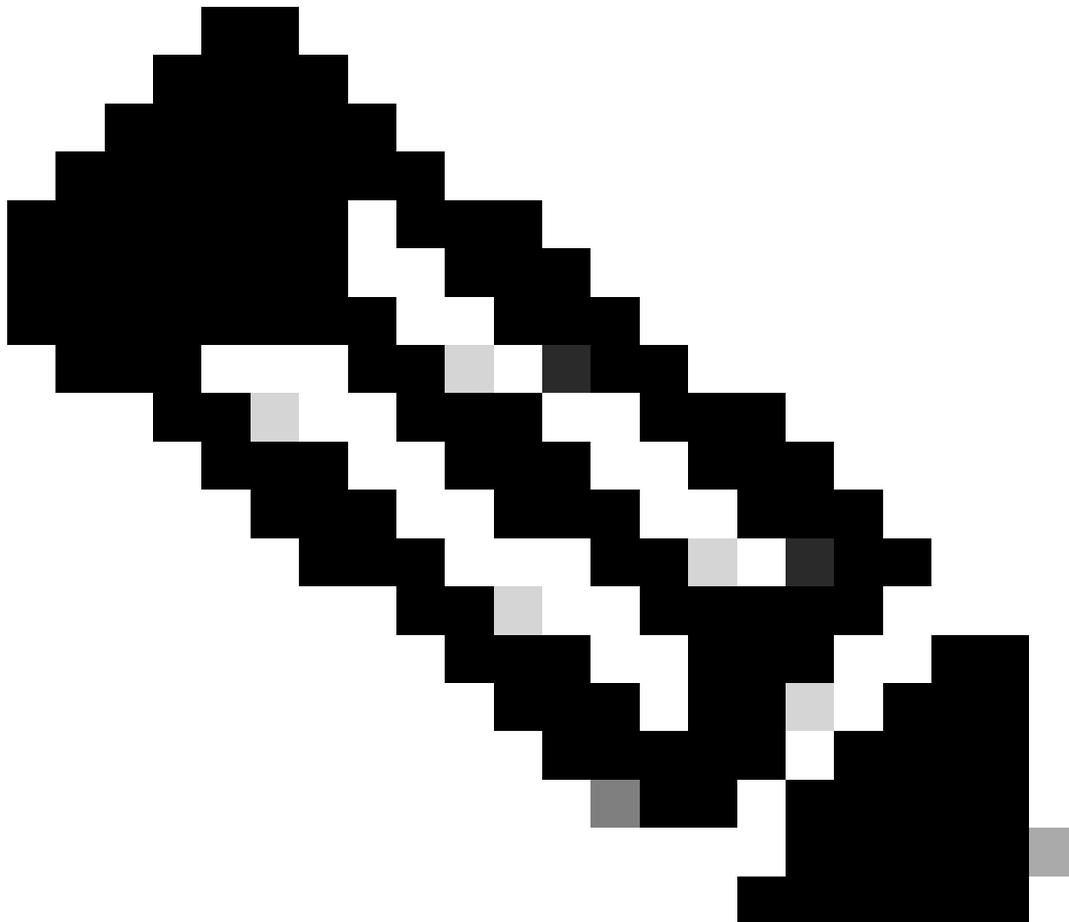
- Unified Computing System Manager (UCSM)
- HyperFlex
- vCenter
- Redes
- DNS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- HyperFlex Connect 5.0.2d

- Clúster de expansión de hiperflex
 - Clúster estándar Hyperflex
 - UCSM 4.2(1I)
 - vCenter 7.0 U3
-



Nota: para que la protección de datos tenga la misma versión de la plataforma de datos Hyperflex en ambos clústeres, el clúster puede ser de un tamaño y tipo diferentes.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Hyperflex Data Protection le proporciona un plan de recuperación ante desastres. Le permite tener instantáneas automáticas que se replican en el clúster remoto. Las instantáneas de las

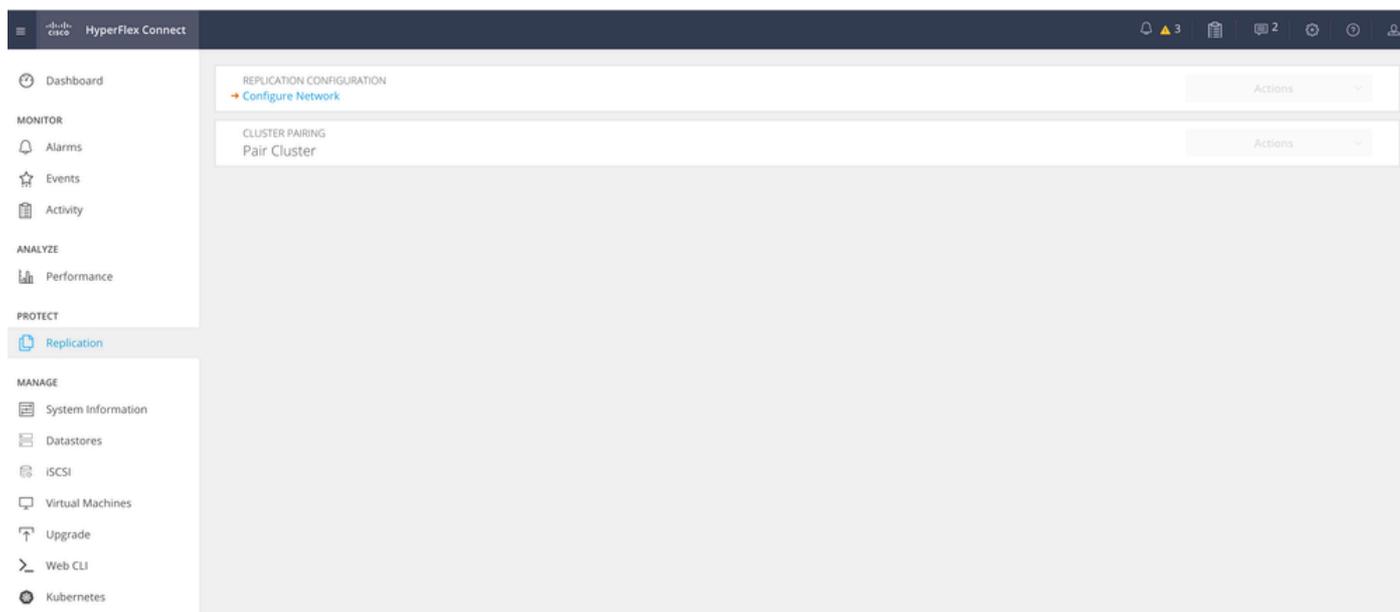
máquinas virtuales protegidas se envían al clúster remoto en función de la frecuencia configurada en el clúster. Sin embargo, sólo la instantánea tomada más recientemente permanece en el clúster de destino.

Información general adicional

- Se recomienda, al configurar el rango de IP, asignar más IP que nodos presentes en el clúster en caso de que se planee una expansión en el futuro.
- MTU debe ser el mismo en ambos extremos.
- La red de replicación debe utilizar la misma subred IP en ambos clústeres a lo largo de la misma VLAN.

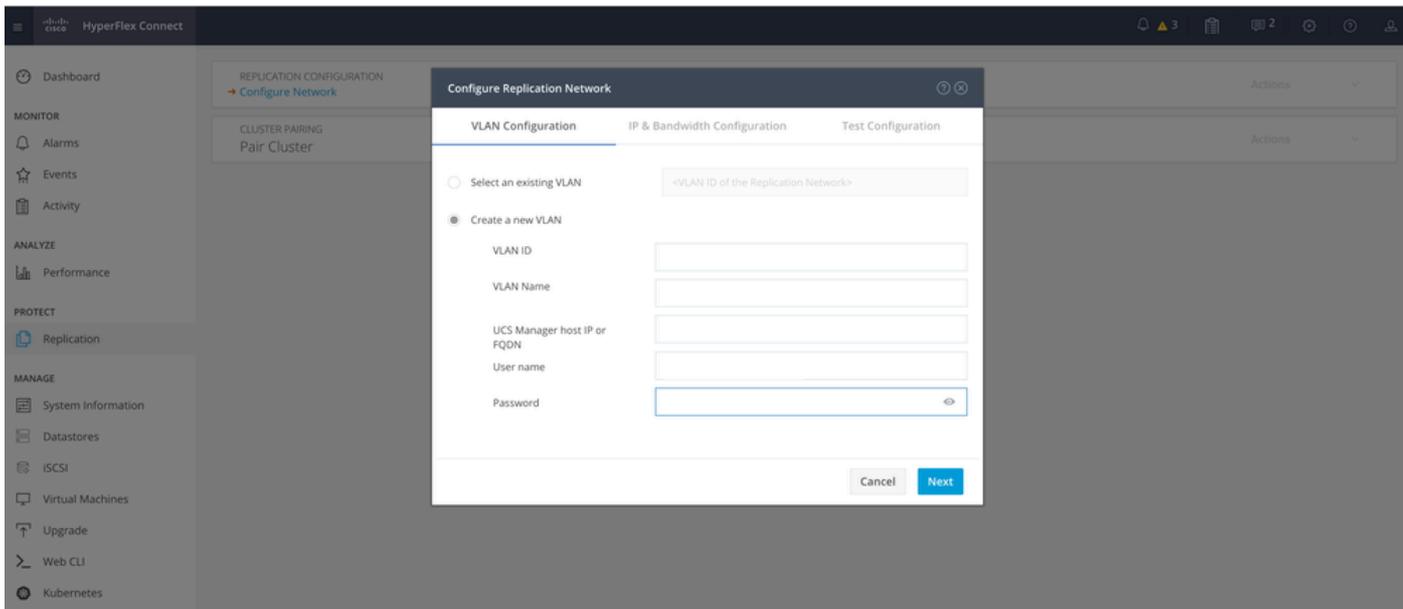
Procedimiento

Paso 1. Inicie sesión en el sistema Hyperflex y vaya a la opción Replicación en el panel de acción izquierdo:



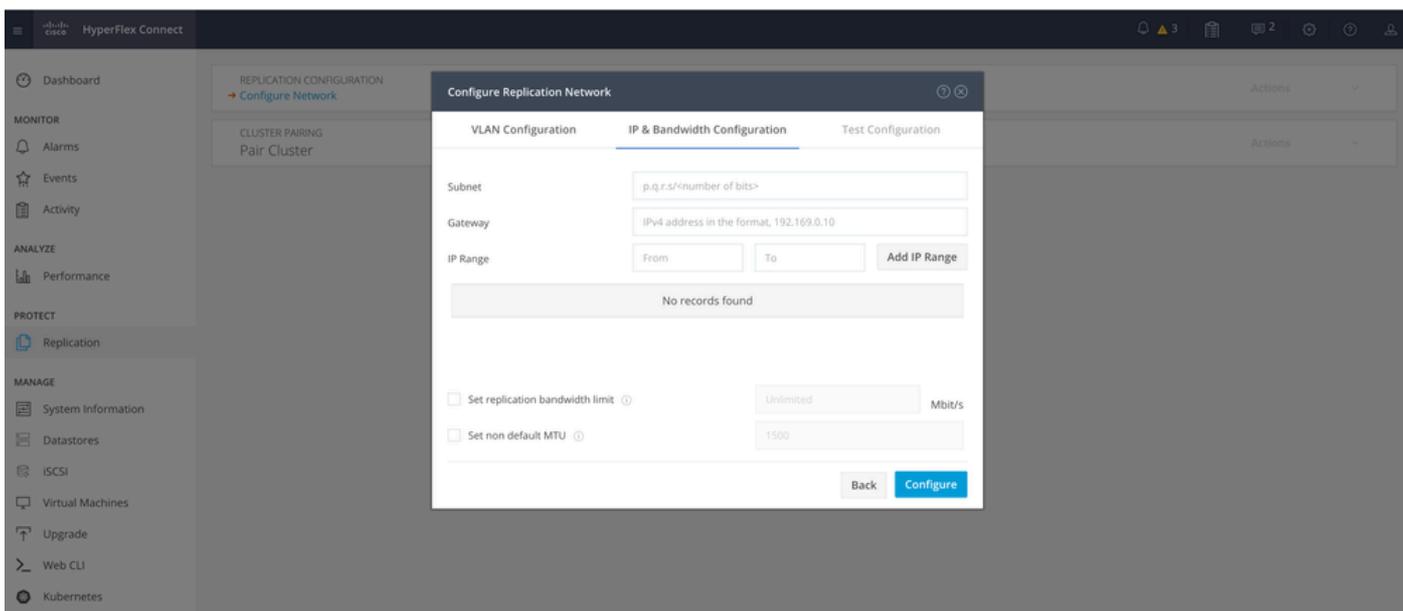
Opción de replicación

Paso 2. Haga clic en la opción Configure Network, rellene la información de cada uno de los campos y haga clic en Next:



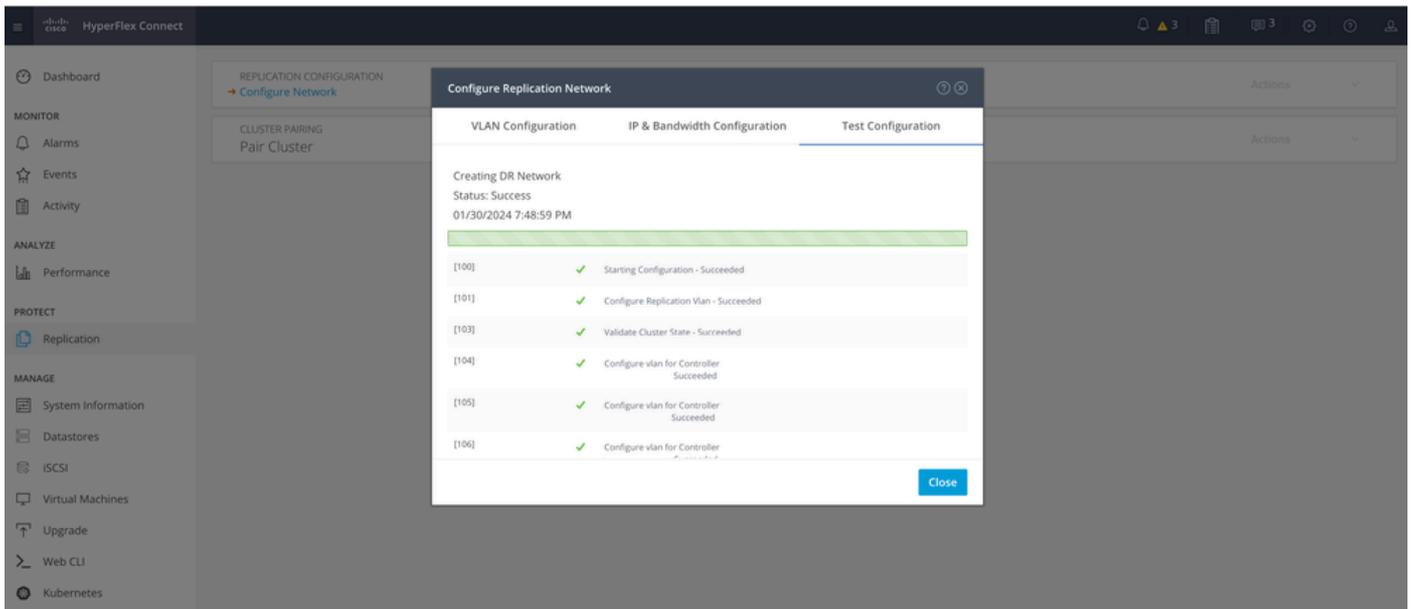
Configurar red de replicación

Paso 3. Establezca la información IP para la red de replicación, agregando la subred, la gateway y el rango de IP. Una vez asignado el intervalo IP, haga clic en Add IP Range y, a continuación, haga clic en Configure.



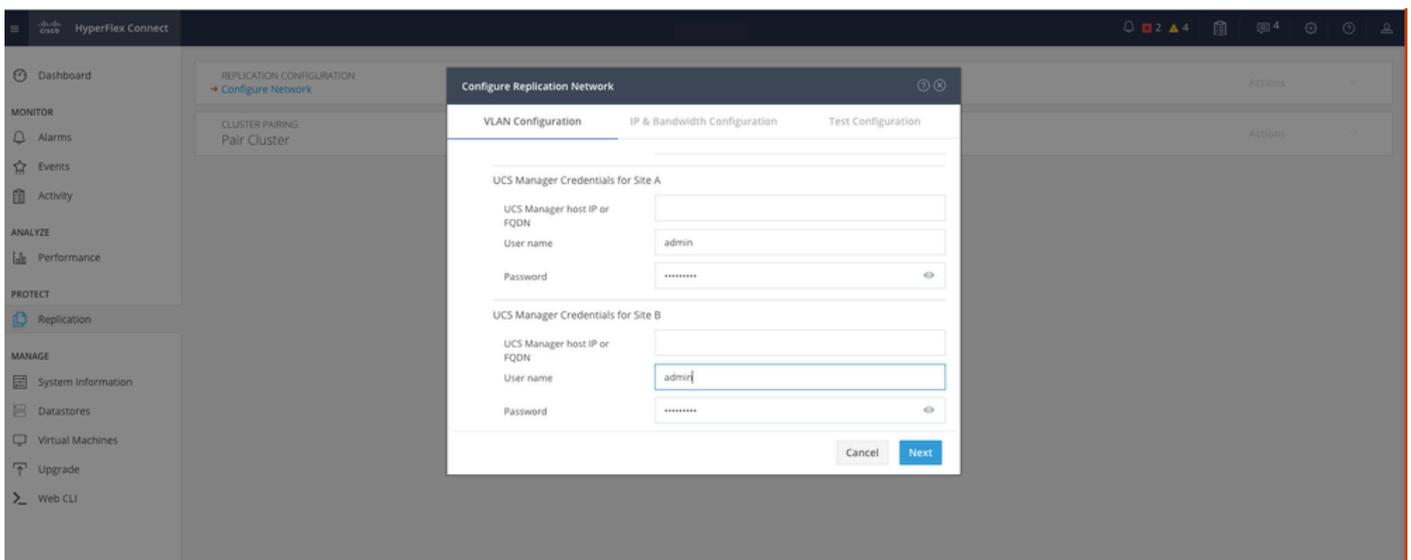
Configurar red de replicación

Paso 4. La configuración se valida y se aplica. Una vez completada, haga clic en Cerrar:



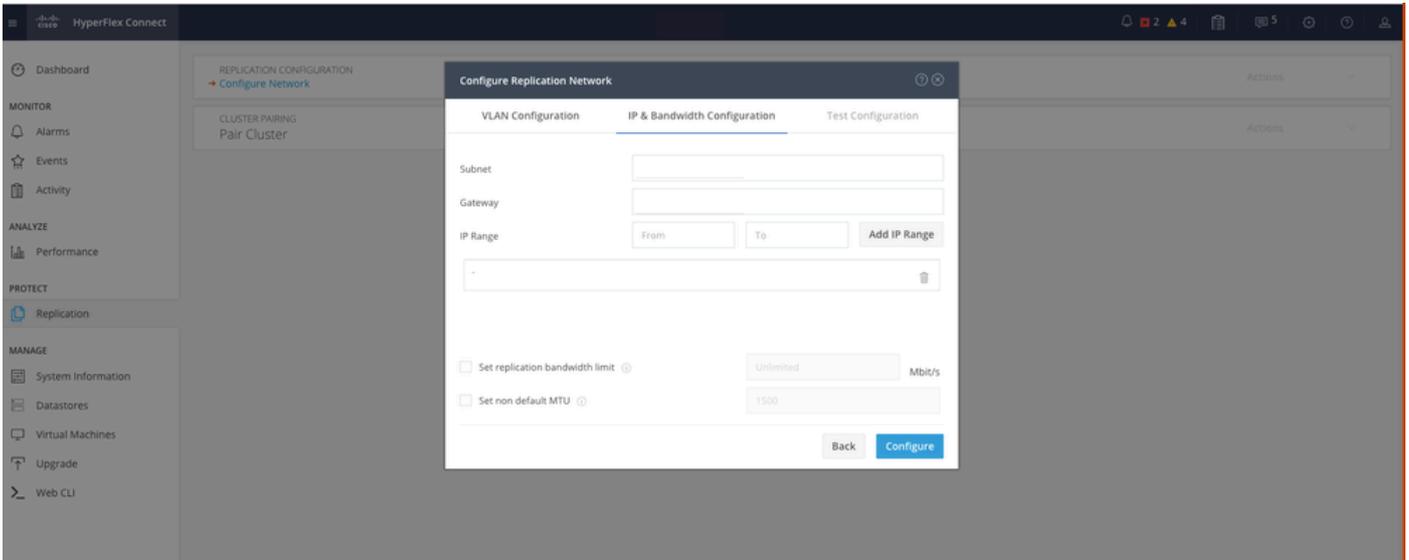
Configuración de red DR

Paso 5. Configure la red en el otro clúster. Para este ejemplo, el segundo clúster es elástico, por lo que se requieren ambas credenciales de UCSM. Rellene la información según corresponda y haga clic en Next:



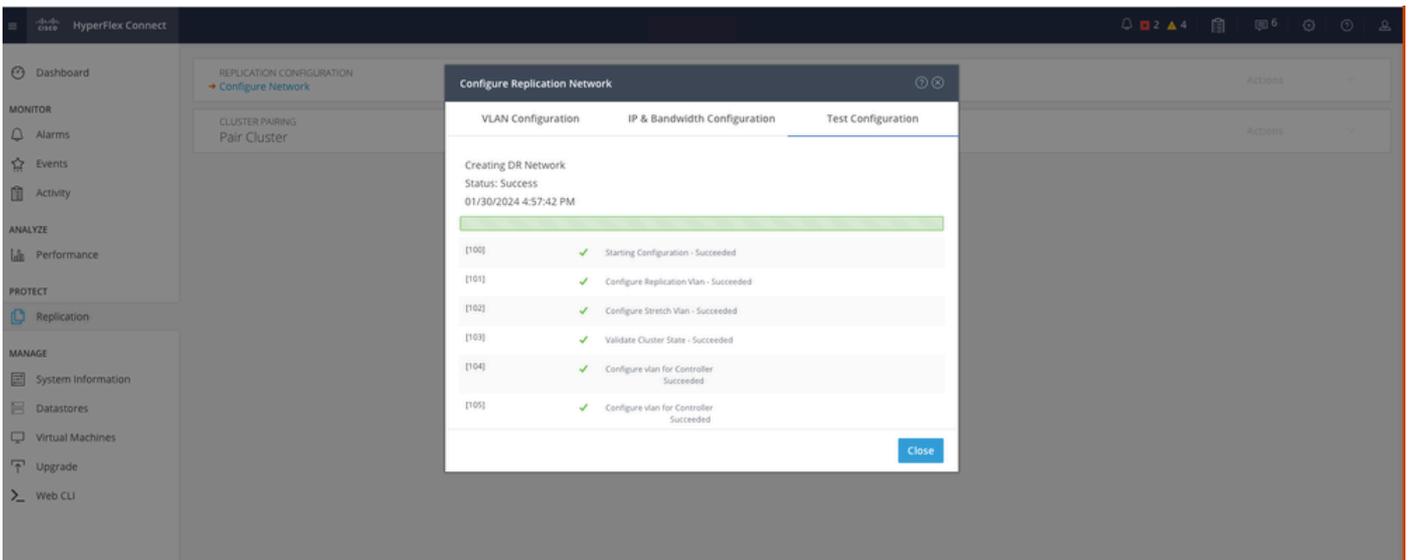
Segunda configuración de red de clúster

Paso 6. Establezca la información IP para la red de replicación en el segundo clúster, agregando la misma subred, gateway e intervalo IP. Una vez asignado el intervalo IP, haga clic en Add IP Range y, a continuación, haga clic en Configure:



Configuración del Segundo Clúster de Red

Paso 7. Cuando la configuración se haya completado, aparecerá un estado correcto y, a continuación, haga clic en Cerrar:

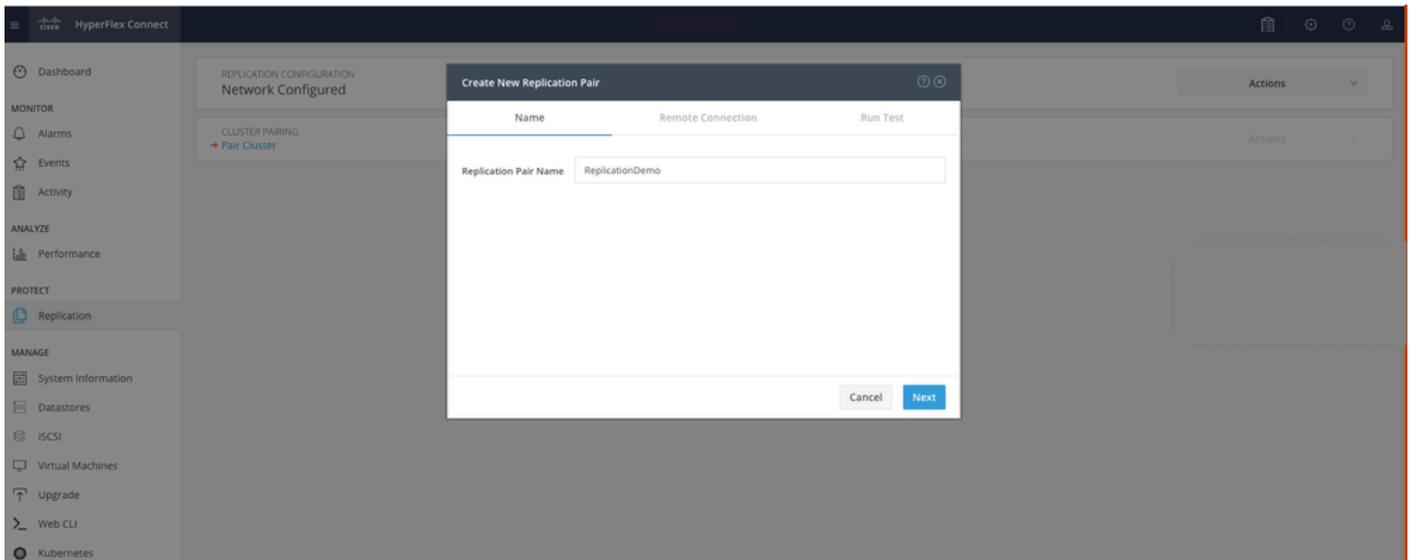


Segundo clúster de configuración de red DR



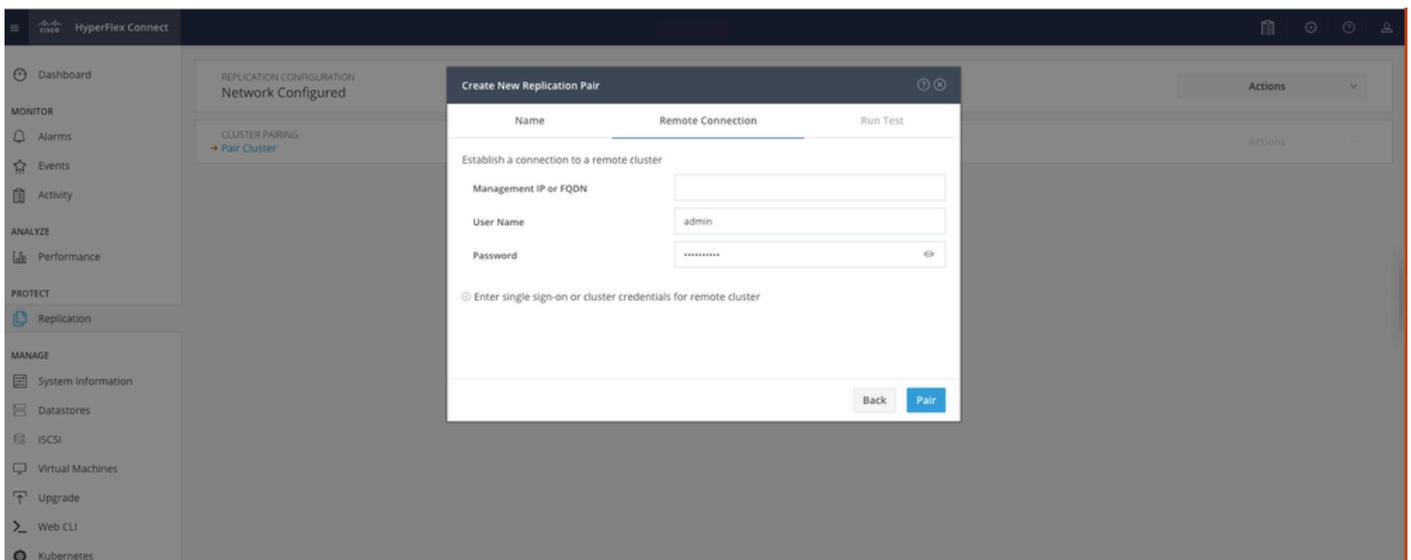
Nota: Una vez configurada la red, se recomienda realizar una prueba de red entre los dos clústeres para confirmar que pueden comunicarse entre sí. Utilice ping para probar la disponibilidad de las IP entre las interfaces eth2.

Paso 7. Para crear el par de replicación, haga clic en Replicación y luego haga clic en Vincular clúster en la opción Vinculación de clústeres. Asigne un nombre para el Nombre del Par de Replicación y haga clic en Siguiente:



Par de replicación

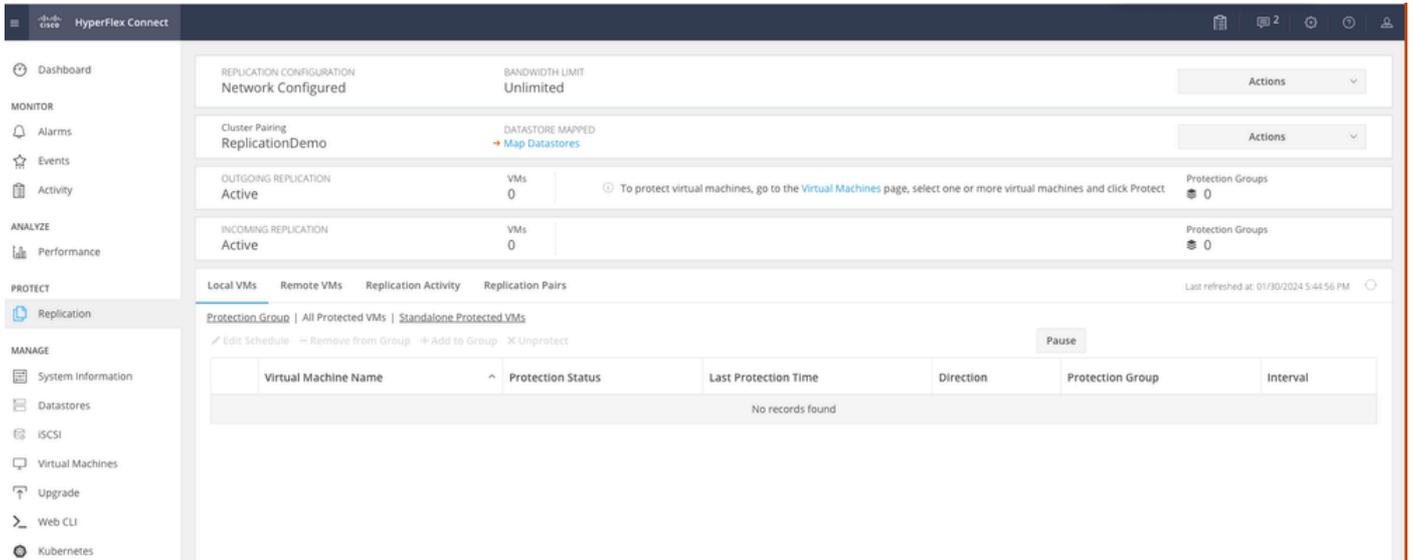
Paso 8. Proporcione la IP de administración del clúster o FQDN para que el clúster sea el par de replicación y, a continuación, haga clic en Vincular:



Clúster de emparejamiento

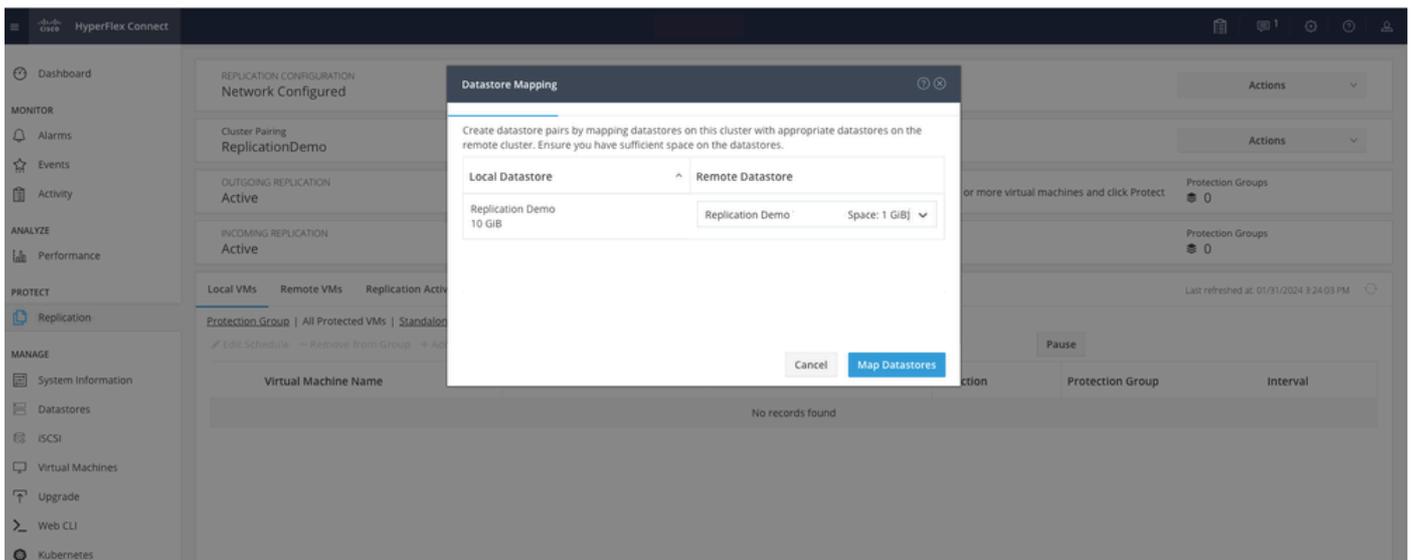
m

Paso 8. Una vez que se han emparejado los clústeres, todo está configurado para iniciar la asignación del almacén de datos entre los dos clústeres, dentro de la misma página de replicación. Aparece la opción Map Datastore, haga clic en ella:



Almacén de datos de asignación

Paso 9. En la ventana emergente, aparece Datastore Mapping, que muestra los datastores disponibles en el clúster a la izquierda, y un menú desplegable con los datastores disponibles en el clúster emparejado donde se intenta proteger las VM:

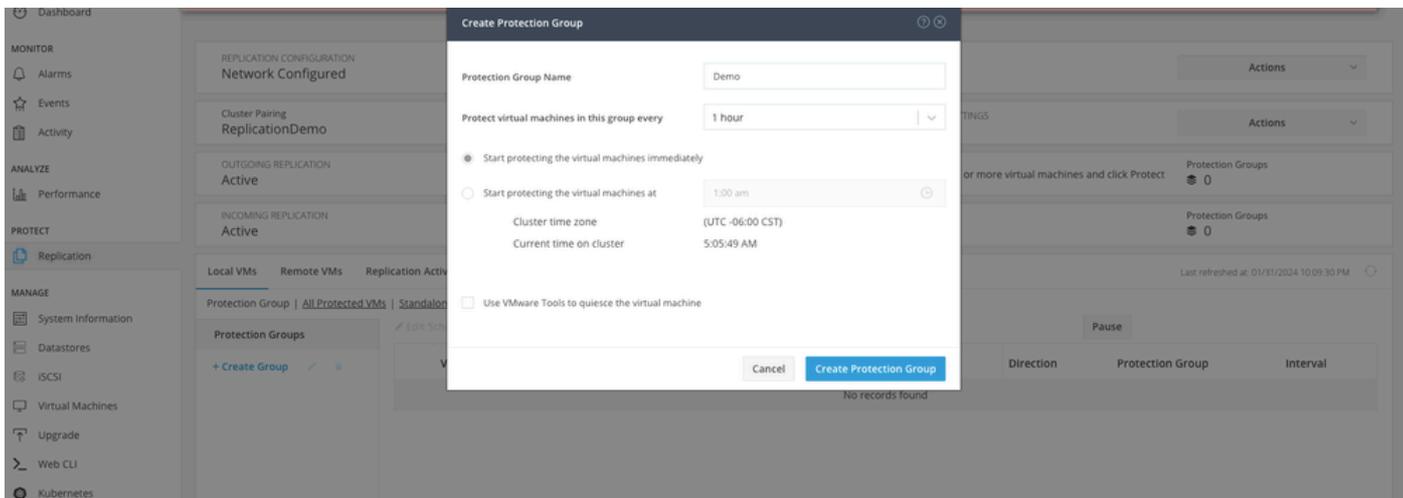


Asignación de almacenes de datos



Nota: La asignación de almacenes de datos se puede realizar de ambos sitios entre sí; por ejemplo, el Clúster 1 puede asignar almacenes de datos al clúster 2 y el Clúster 2 puede asignar almacenes de datos al clúster 1 sin ninguna configuración adicional.

Paso 10. Una vez asignados los almacenes de datos, defina el grupo de protección, especifique un nombre y seleccione un período de tiempo para proteger las máquinas virtuales que se van a asociar a él. Por último, especifique la hora a la que se inicia el grupo de protección y, a continuación, haga clic en Crear grupo de protección.

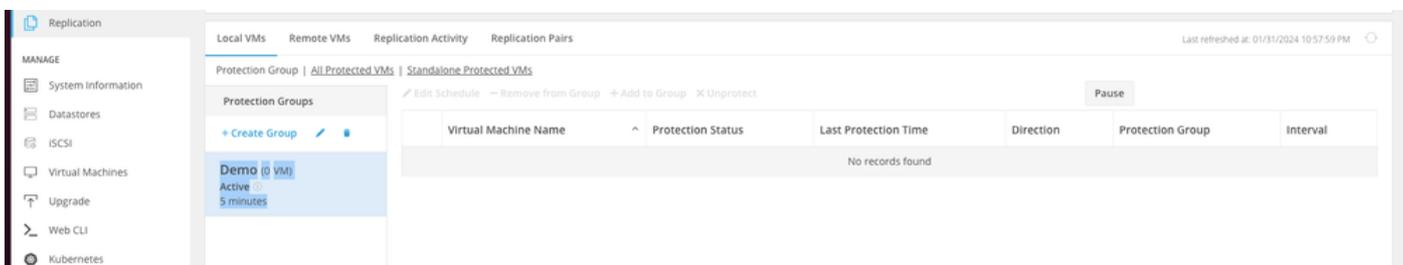


Creación de grupos de protección

Consideraciones sobre grupos de protección

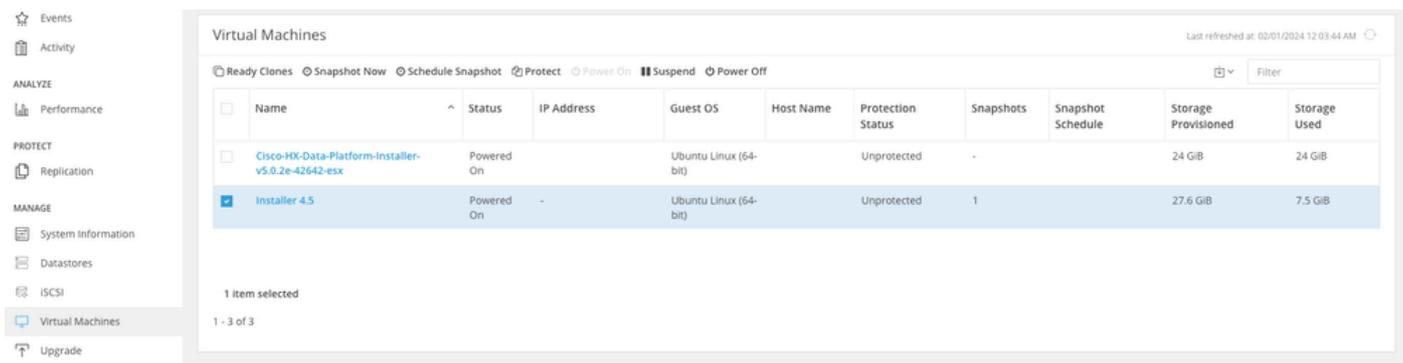
- El grupo de protección define cómo se comporta la protección de datos.
- Permite especificar la frecuencia para proteger la máquina virtual.
- Puede durar de 5 minutos a 24 horas, también el tiempo en que comienza la protección.
- Puede tener una hora inmediata o específica.
- Las herramientas de VMware se pueden habilitar para silenciar la máquina virtual.

Aparece un mensaje de confirmación que indica que se ha creado el grupo de protección y aparece enumerado en el área del grupo de protección:

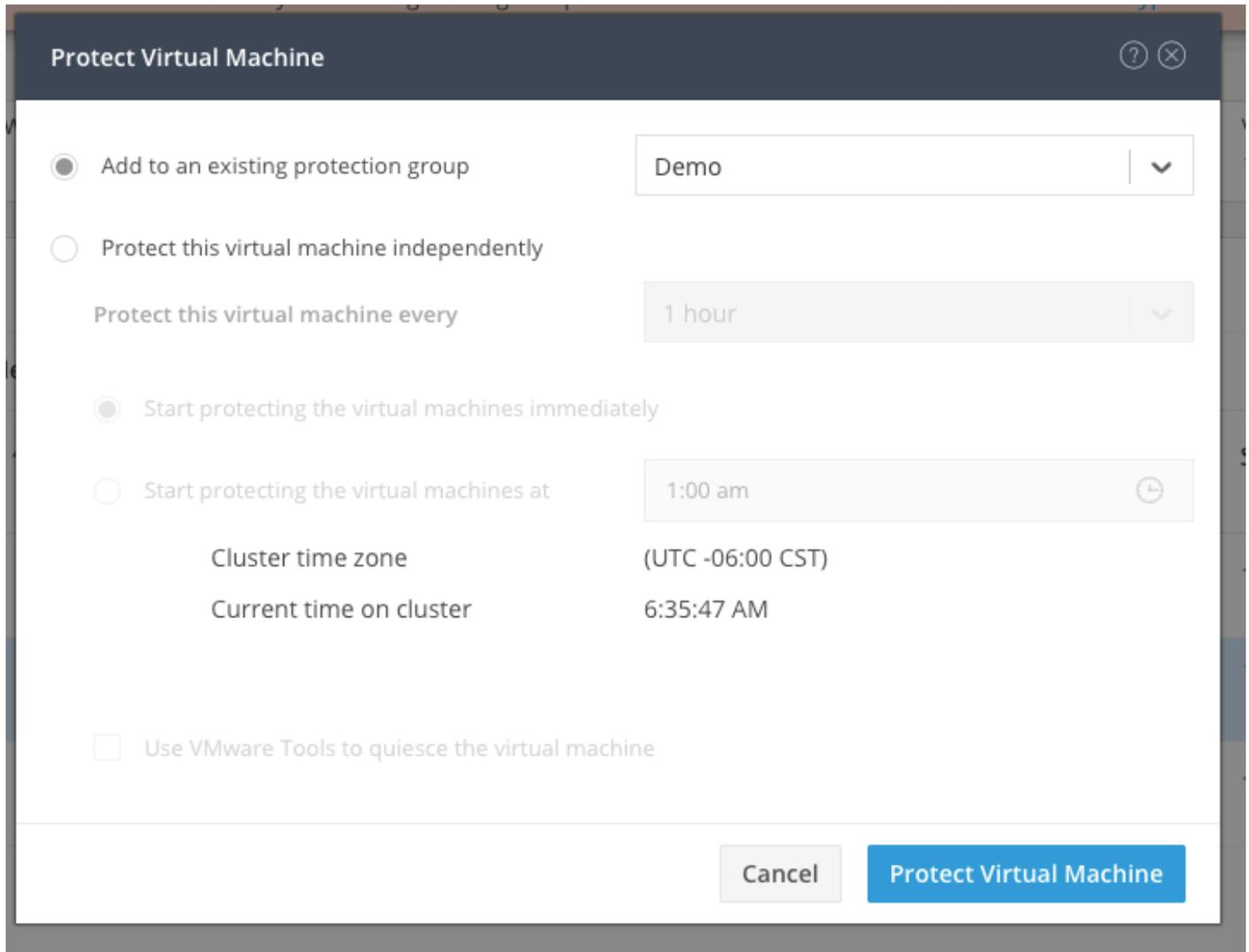


Grupo de protección creado

Paso 11. Con el grupo de protección creado, el paso final es asignarlo a las máquinas virtuales que se van a proteger. Vaya a la pestaña Máquinas virtuales, seleccione la máquina virtual que desea proteger y, a continuación, haga clic en Proteger:

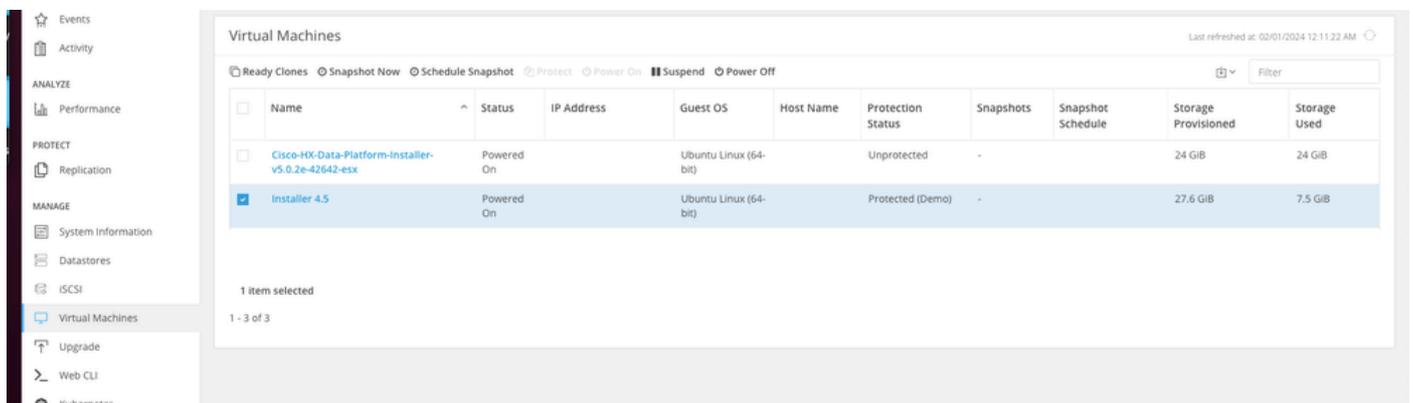


Aparece una ventana emergente para adjuntar el grupo de protección creado, seleccionarlo y hacer clic en Proteger máquina virtual:

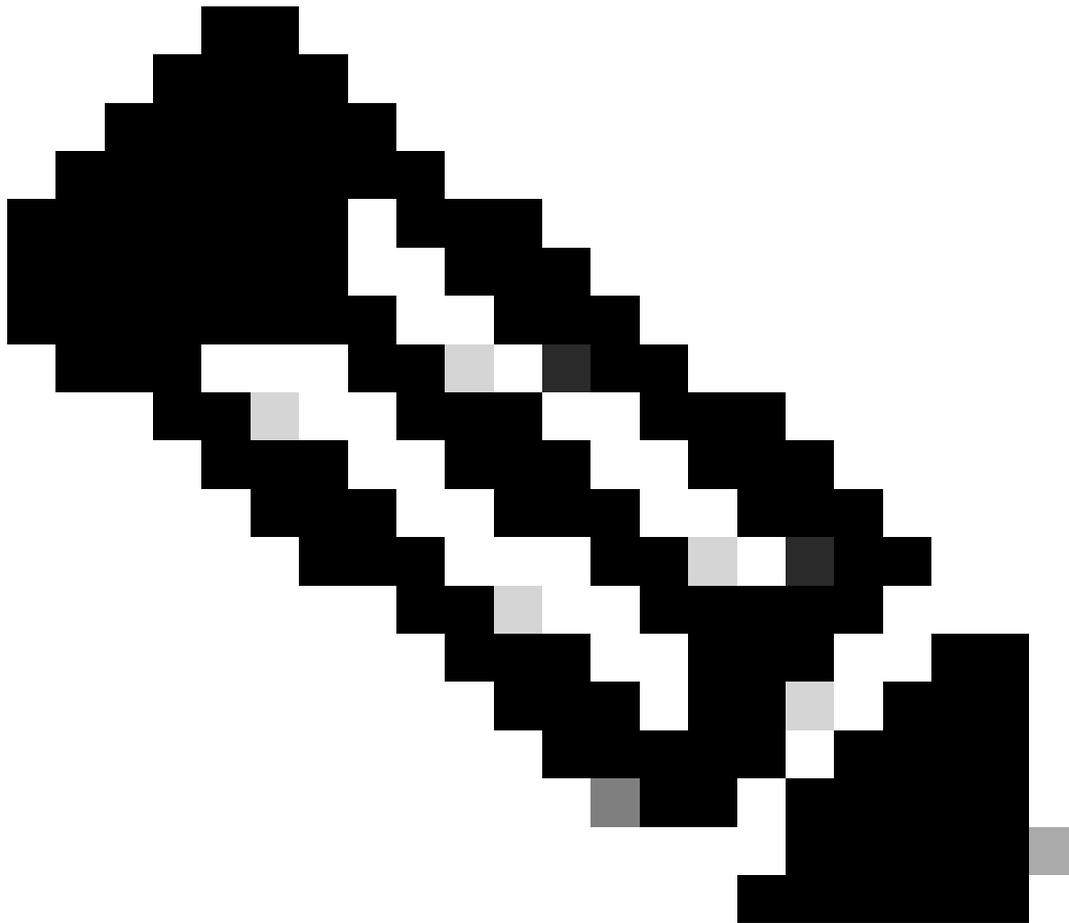


Selección del grupo de protección

Una vez protegida, la VM se muestra como protegida para el grupo de protección.



VM protegida



Nota: Asegúrese de que la máquina virtual protegida pertenece a un almacén de datos que se está asignando; de lo contrario, la protección fallará.

Troubleshoot

Verificar configuración de protección de VM

Una práctica recomendada es supervisar la protección de VM en la pestaña Replicación:

The screenshot shows the VMware vSphere Replication interface. The left sidebar includes sections for MONITOR (Alarms, Events, Activity), ANALYZE (Performance), PROTECT (Replication), and MANAGE (System Information, Datastores, iSCSI, Virtual Machines, Upgrade, Web CLI, Kubernetes). The main content area displays replication configuration and activity. Key metrics include: Network Configured, Bandwidth Limit Unlimited, Cluster Pairing ReplicationDemo, Datastore Mapped 2, Recovery Settings, and Outgoing Replication Active with 1 VMs protected and 0 exceeds intervals. Below this, a table lists VMs under the 'Protection Group' 'Demo'. The table shows one VM, 'Installer 4.5', with a 'Protected' status and a 'Last Protection Time' of 02/01/2024 6:50:46 AM. The direction is 'Outgoing' and the interval is 'Every 5 minutes'.

Supervisión de VM protegidas

Supervisar actividades de replicación

Las actividades de replicación se pueden supervisar haciendo clic en la pestaña Actividad de Replicación:

This screenshot shows the 'Replication Activity' tab in the VMware vSphere Replication interface. It displays a detailed table of replication activities. The table has columns for Virtual Machine, Remote Cluster, Status, Start Time, End Time, Protection Group, Direction, and Data Transferred. Five entries are shown, all for 'Installer 4.5' on the 'Tokio' remote cluster, with a 'Completed' status. The data transferred ranges from 464 KiB to 5.8 GiB. The interface also shows navigation options like 'Edit Schedule', 'Remove from Group', 'Add to Group', and 'Unprotect', along with a 'Pause' button and a filter input.

Virtual Machine	Remote Cluster	Status	Start Time	End Time	Protection Group	Direction	Data Transferred
Installer 4.5	Tokio	Completed	02/01/2024 6:54:49 AM	02/01/2024 6:54:49 AM	Demo	Outgoing	464 KiB
Installer 4.5	Tokio	Completed	02/01/2024 6:50:46 AM	02/01/2024 6:50:47 AM	Demo	Outgoing	692 KiB
Installer 4.5	Tokio	Completed	02/01/2024 6:46:43 AM	02/01/2024 6:46:44 AM	Demo	Outgoing	520 KiB
Installer 4.5	Tokio	Completed	02/01/2024 6:42:40 AM	02/01/2024 6:42:40 AM	Demo	Outgoing	724 KiB
Installer 4.5	Tokio	Completed	02/01/2024 6:38:35 AM	02/01/2024 6:38:49 AM	Demo	Outgoing	5.8 GiB

Actividades de replicación

Problemas comunes

Problemas de pares

Pueden aparecer problemas de emparejamiento:

Create New Replication Pair

Name	Remote Connection	Run Test
------	-------------------	----------

✘ Unable to fetch the DR network configuration from remote Cluster. Please retry the operation after validating DR network configuration in remote Cluster.

Establish a connection to a remote cluster

Management IP or FQDN

User Name

Password 

i Enter single sign-on or cluster credentials for remote cluster

Problemas de emparejamiento

- Asegúrese de que la red de replicación esté configurada en ambos clústeres.
- Asegúrese de que los clústeres sean accesibles entre sí.

Inconvenientes de conectividad

- Verifique que eth2 esté presente. Utilice el comando ifconfig en cada una de las máquinas virtuales del controlador de almacenamiento para confirmar que eth2 esté configurado correctamente en ellas.
- Utilice ping para probar la conectividad entre las interfaces eth2.
- Asegúrese de que la VLAN de replicación en ambos clústeres coincida.
- Asegúrese de que la VLAN de replicación esté configurada correctamente en todas las rutas entre los clústeres.

```

eth2      Link encap:Ethernet  HWaddr
          inet addr:172      .3 Bcast:172      .255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:797975 errors:0 dropped:87 overruns:0 frame:0
          TX packets:799505 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:74023721 (74.0 MB)  TX bytes:74168965 (74.1 MB)

eth2:0    Link encap:Ethernet  HWaddr
          inet addr:172      .2 Bcast:172      .255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

eth0:mgmtip Link encap:Ethernet  HWaddr
          inet addr:      Bcast:10.31.123.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:15509057612 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15509057612 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3349146489309 (3.3 TB)  TX bytes:3349146489309 (3.3 TB)

hxshell:~$ ping 172      .9
PING 172      .9 (172      .9) 56(84) bytes of data.
64 bytes from 172      .9: icmp_seq=1 ttl=64 time=0.332 ms
64 bytes from 172      .9: icmp_seq=2 ttl=64 time=0.119 ms
64 bytes from 172      .9: icmp_seq=3 ttl=64 time=0.127 ms
64 bytes from 172      .9: icmp_seq=4 ttl=64 time=0.107 ms
64 bytes from 172      .9: icmp_seq=5 ttl=64 time=0.106 ms
64 bytes from 172      .9: icmp_seq=6 ttl=64 time=0.132 ms
64 bytes from 172      .9: icmp_seq=7 ttl=64 time=0.123 ms
64 bytes from 172      .9: icmp_seq=8 ttl=64 time=0.114 ms
64 bytes from 172      .9: icmp_seq=9 ttl=64 time=0.144 ms
^C
--- 172      .9 ping statistics ---
9 packets transmitted, 9 received. 0% packet loss, time 8194ms
rtt min/avg/max/mdev =
069 ms
hxshell:~$ █

eth2      Link encap:Ethernet  HWaddr
          inet addr:172      .9 Bcast:172      .255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:30774 errors:0 dropped:29 overruns:0 frame:0
          TX packets:32960 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2893235 (2.8 MB)  TX bytes:3141789 (3.1 MB)

eth2:0    Link encap:Ethernet  HWaddr
          inet addr:172      .7 Bcast:172      .255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

eth0:mgmtip Link encap:Ethernet  HWaddr
          inet addr:      Bcast
          Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:12876504225 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12876504225 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2722351786798 (2.7 TB)  TX bytes:2722351786798 (2.7 TB)

hxshell:~$ ping 172      .3
PING 172      .3 (172      .3) 56(84) bytes of data.
64 bytes from 172      .3: icmp_seq=1 ttl=64 time=0.158 ms
64 bytes from 172      .3: icmp_seq=2 ttl=64 time=0.137 ms
64 bytes from 172      .3: icmp_seq=3 ttl=64 time=0.115 ms
64 bytes from 172      .3: icmp_seq=4 ttl=64 time=0.107 ms
64 bytes from 172      .3: icmp_seq=5 ttl=64 time=0.143 ms
64 bytes from 172      .3: icmp_seq=6 ttl=64 time=0.105 ms
64 bytes from 172      .3: icmp_seq=7 ttl=64 time=0.149 ms
64 bytes from 172      .3: icmp_seq=8 ttl=64 time=0.140 ms
64 bytes from 172      .3: icmp_seq=9 ttl=64 time=0.145 ms
^C
--- 172      .3 ping statistics ---
9 packets transmitted, 9 received. 0% packet loss, time 8199ms
rtt min/avg/max/mdev =
019 ms
hxshell:~$ █

```

Prueba de ping

Problemas de protección

Protect Virtual Machine



✘ Cisco-HX-Data-Platform-Installer-v5.0.2e-42642-esx : Unable to protect the VM, some datastores are not paired. ✘

Add to an existing protection group

Demo



Protect this virtual machine independently

Protect this virtual machine every

1 hour



Start protecting the virtual machines immediately

Start protecting the virtual machines at

1:00 am



Cluster time zone

(UTC -06:00 CST)

Current time on cluster

3:45:32 AM

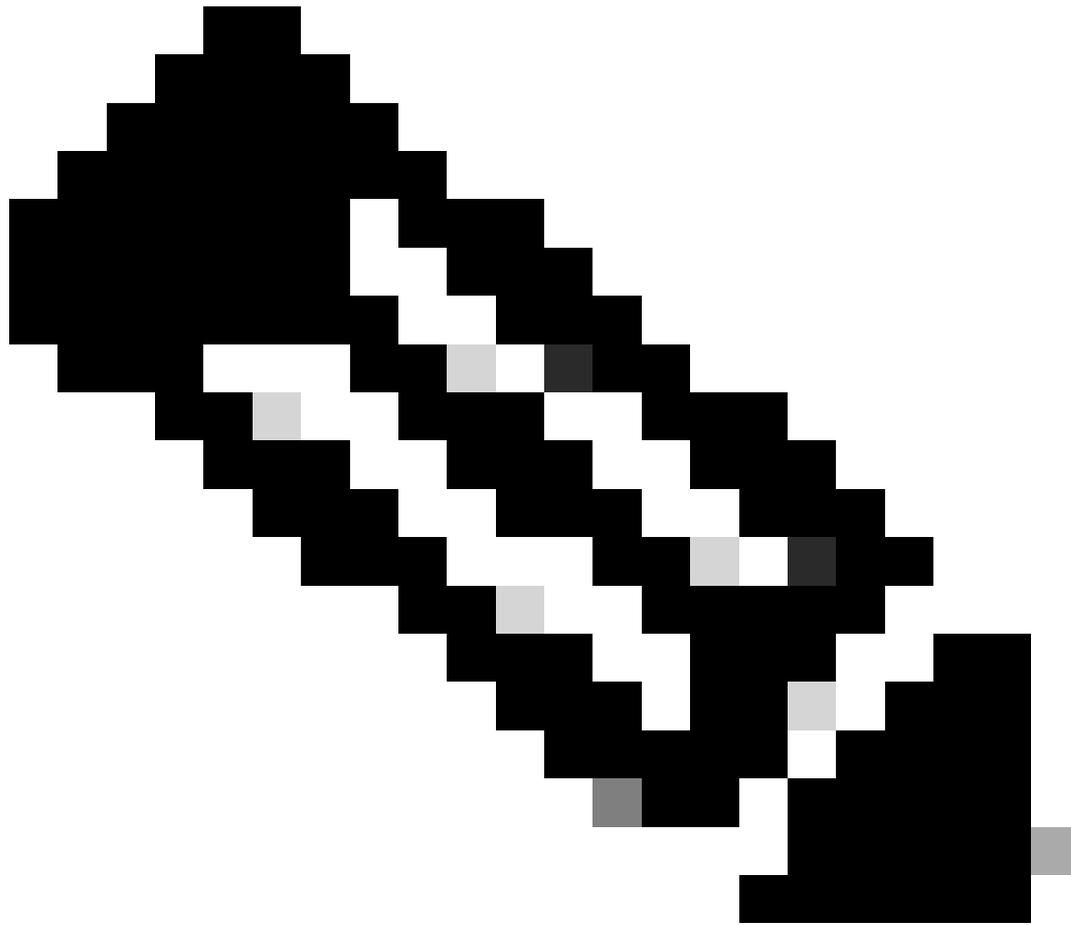
Use VMware Tools to quiesce the virtual machine

Cancel

Protect Virtual Machine

Problemas de protección

- Asegúrese de que la máquina virtual que se va a proteger pertenece a un almacén de datos asignado.
- Asegúrese de que los almacenes de datos están asignados correctamente.



Nota: algunas correcciones requieren la intervención del Technical Assistance Center (TAC). Abra un caso con el TAC, si es necesario.

Información Relacionada

- [Guía de administración de la plataforma de datos Cisco HyperFlex, versión 5.0](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).