

Configurare la protezione dei dati in Hyperflex

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Ulteriori informazioni generali](#)

[Procedura](#)

[Considerazioni sul gruppo protezione dati](#)

[Risoluzione dei problemi](#)

[Verifica configurazione protezione macchina virtuale](#)

[Monitoraggio delle attività di replica](#)

[Problemi comuni](#)

[Associa problemi](#)

[Problemi di connettività](#)

[Problemi relativi alla protezione](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come configurare la replica in Hyperflex.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

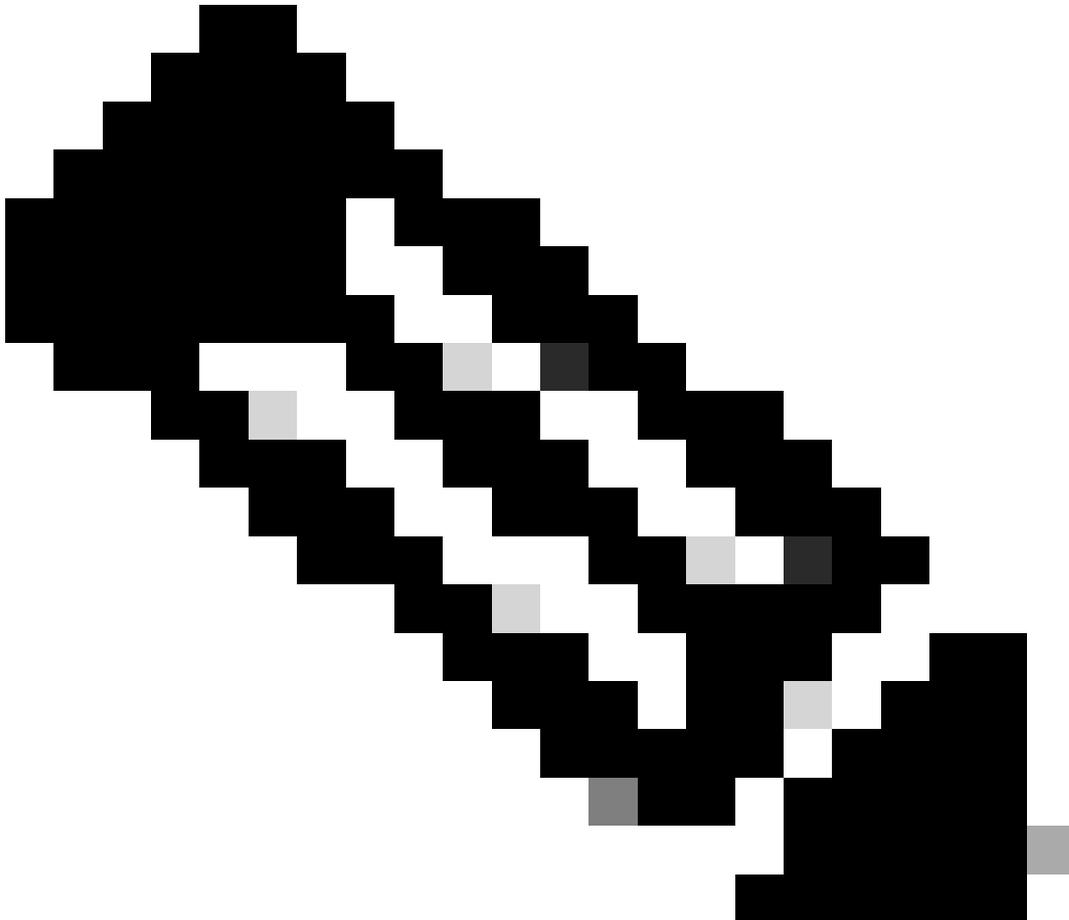
- Unified Computing System Manager (UCSM)
- HyperFlex
- vCenter
- Networking
- DNS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- HyperFlex Connect 5.0.2d

- Hyperflex Stretch Cluster
 - Cluster Hyperflex Standard
 - UCSM 4.2(1I)
 - vCenter 7.0 U3
-



Nota: poiché la protezione dei dati deve avere la stessa versione di Hyperflex Data Platform in entrambi i cluster, le dimensioni e il tipo del cluster possono essere diversi.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Hyperflex Data Protection offre un piano di disaster recovery. Consente di disporre di snapshot automatiche replicate nel cluster remoto. Gli snapshot per le macchine virtuali protette vengono

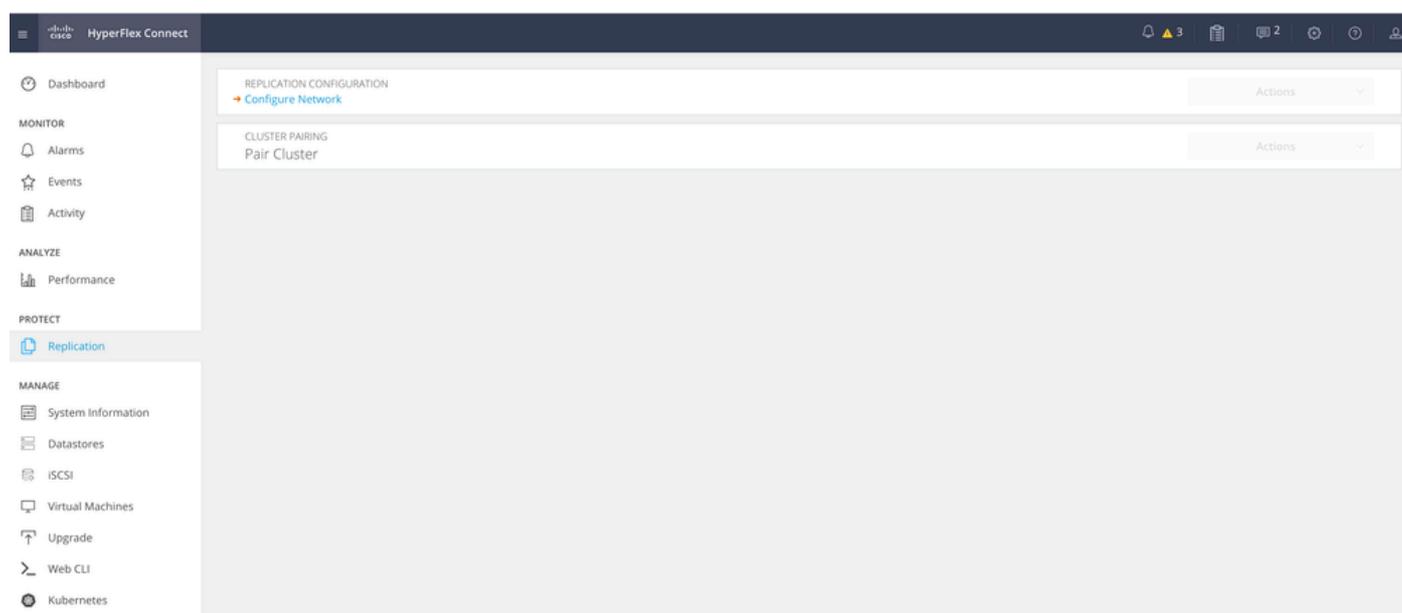
inviati al cluster remoto a seconda della frequenza configurata nel cluster. Tuttavia, nel cluster di destinazione rimane solo l'ultima istantanea acquisita.

Ulteriori informazioni generali

- È buona norma, quando si configura un intervallo IP, allocare più IP rispetto ai nodi presenti nel cluster nel caso in cui si preveda un'espansione per il futuro.
- L'MTU deve essere la stessa su entrambe le estremità.
- La rete di replica deve utilizzare la stessa subnet IP in entrambi i cluster della stessa VLAN.

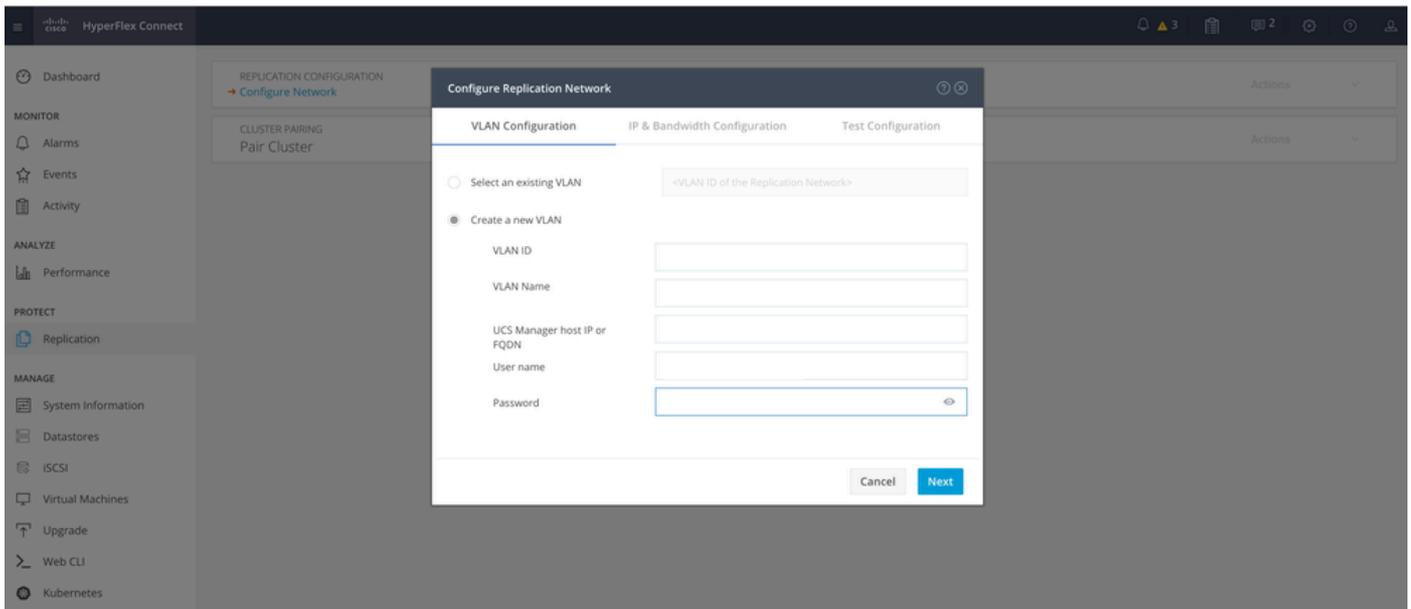
Procedura

Passaggio 1. Accedere al sistema Hyperflex e selezionare l'opzione Replication nel riquadro azioni a sinistra:



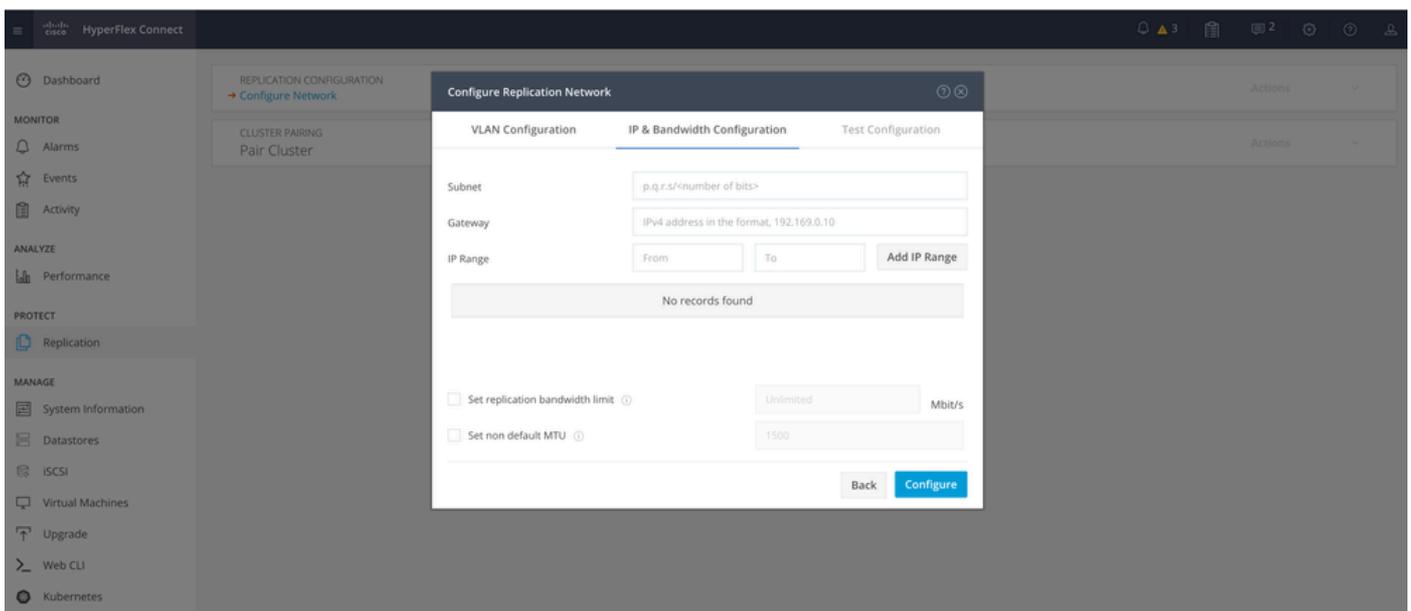
Opzione di replica

Passaggio 2. Fare clic sull'opzione Configura rete, compilare le informazioni per ogni campo e fare clic su Avanti:



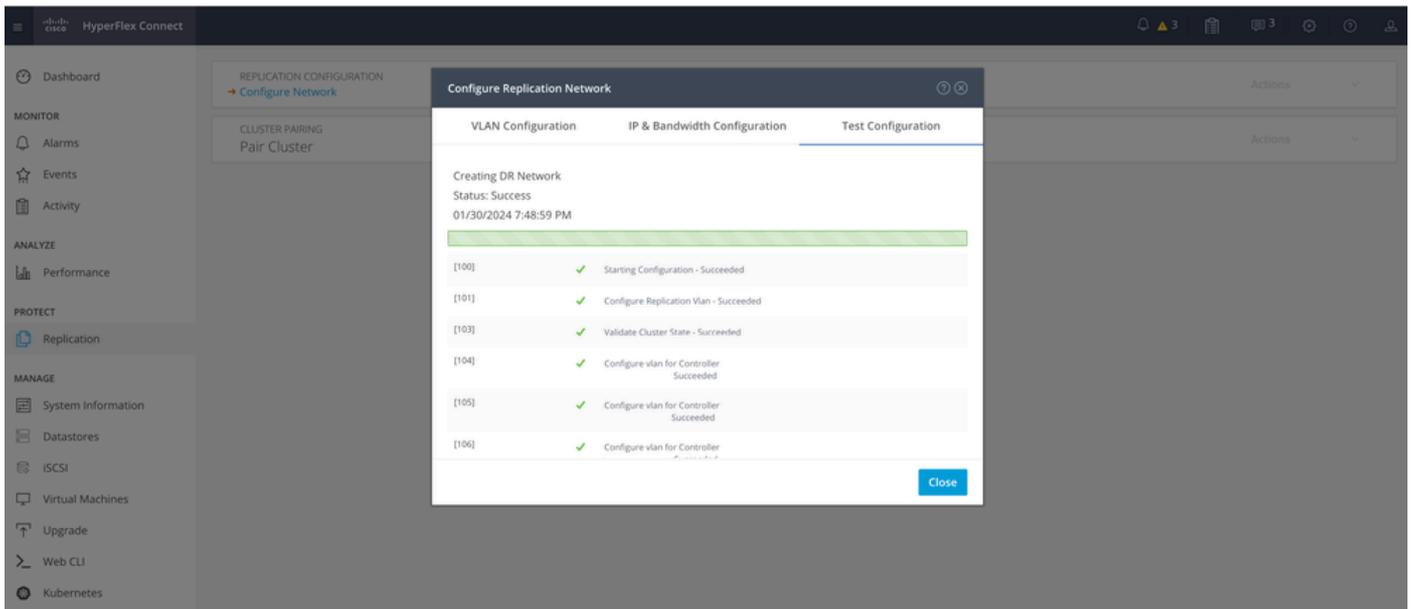
Configura rete di replica

Passaggio 3. Impostare le informazioni IP per la rete di replica, aggiungendo la subnet, il gateway e l'intervallo IP. Una volta assegnato l'intervallo IP, fare clic su Add IP Range (Aggiungi intervallo IP), quindi su Configure (Configura).



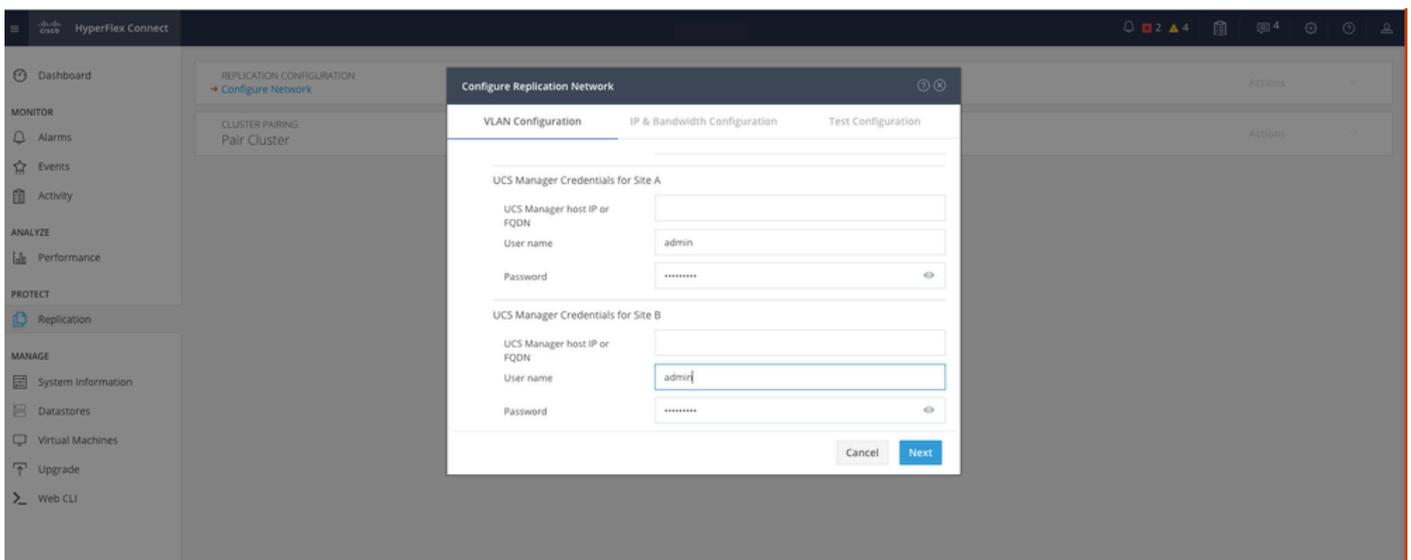
Configura rete di replica

Passaggio 4. La configurazione viene convalidata e applicata. Al termine, fare clic su Chiudi:



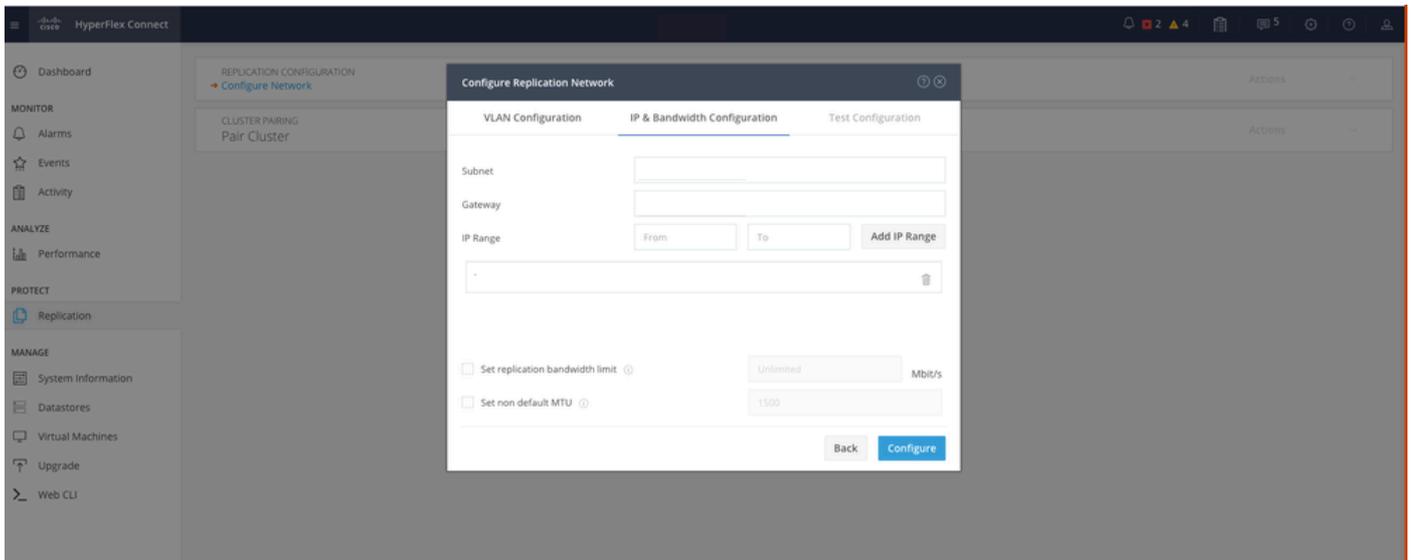
Configurazione rete DR

Passaggio 5. Configurare la rete nell'altro cluster. Per questo esempio il secondo cluster è stretch, pertanto sono necessarie entrambe le credenziali UCSM. Immettere le informazioni appropriate e fare clic su Avanti:



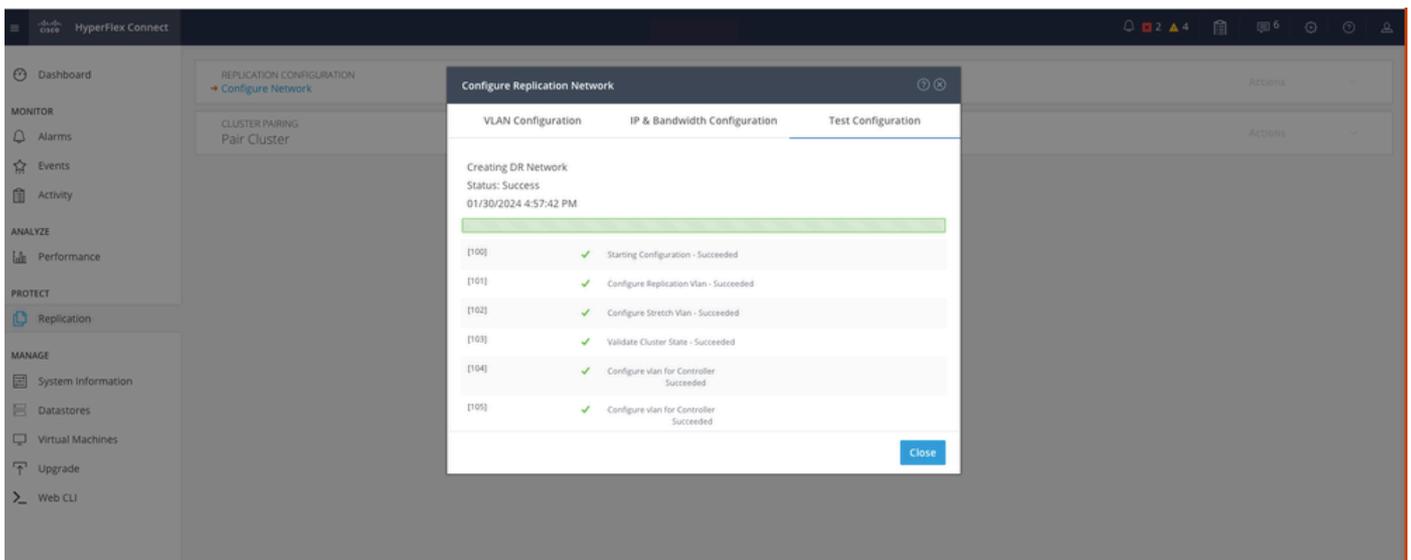
Configurazione rete secondo cluster

Passaggio 6. Impostare le informazioni IP per la rete di replica nel secondo cluster, aggiungendo la stessa subnet, lo stesso gateway e lo stesso intervallo IP. Una volta assegnato l'intervallo IP, fare clic su Add IP Range (Aggiungi intervallo IP), quindi su Configure (Configura):



Configurazione del secondo cluster di rete

Passaggio 7. Una volta completata la configurazione, viene visualizzato lo stato di operazione riuscita, quindi fare clic su Close (Chiudi):

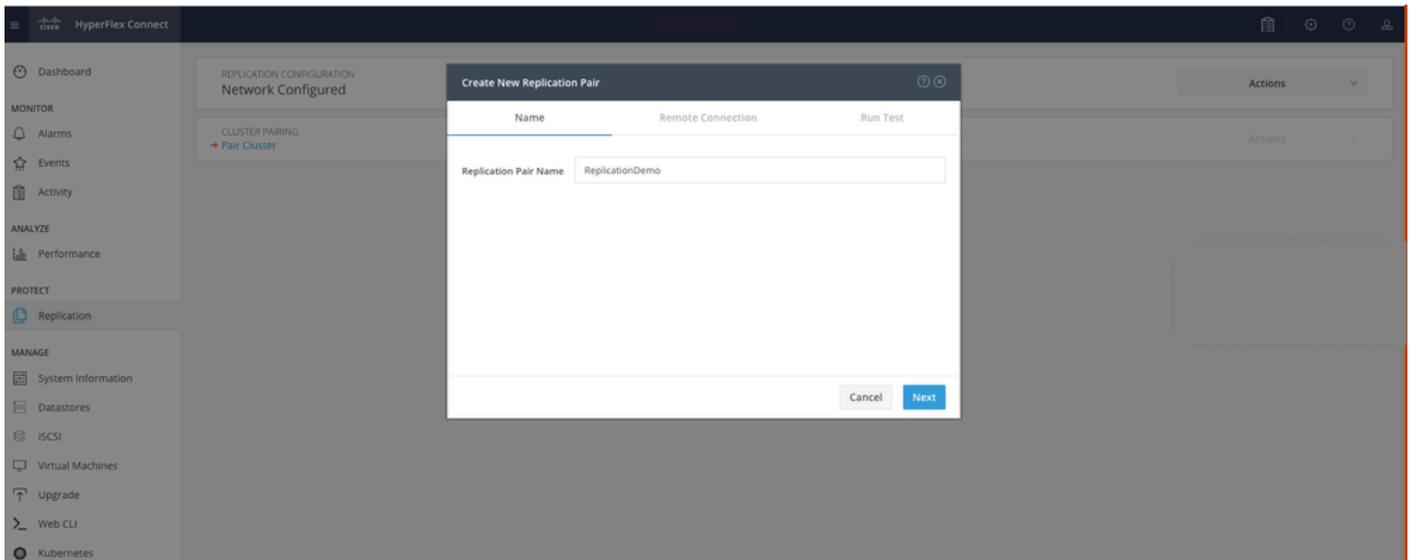


Secondo cluster configurazione rete DR



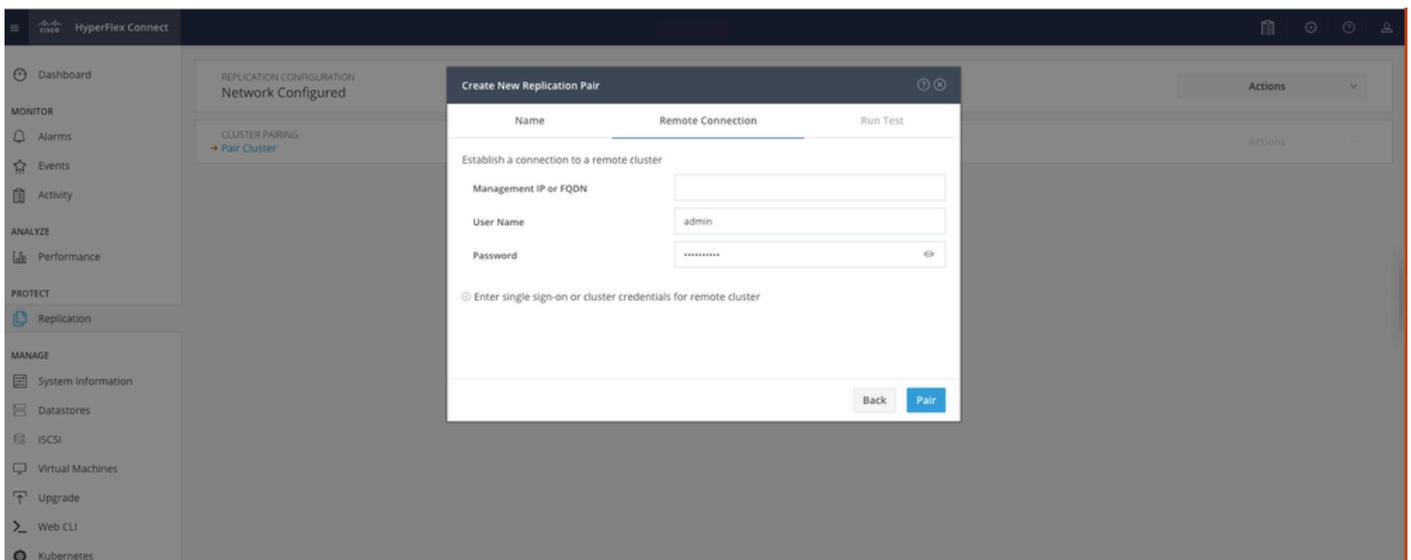
Nota: una volta configurata la rete, è consigliabile eseguire un test di rete tra i due cluster per verificare che siano in grado di comunicare tra loro. Utilizzare il comando ping per verificare la raggiungibilità degli IP tra le interfacce eth2.

Passaggio 7. Per creare la coppia di replica, fare clic su Replica e quindi su Associa cluster nell'opzione Associazione cluster. Assegnare un nome alla coppia di repliche e fare clic su Avanti:



Coppia di repliche

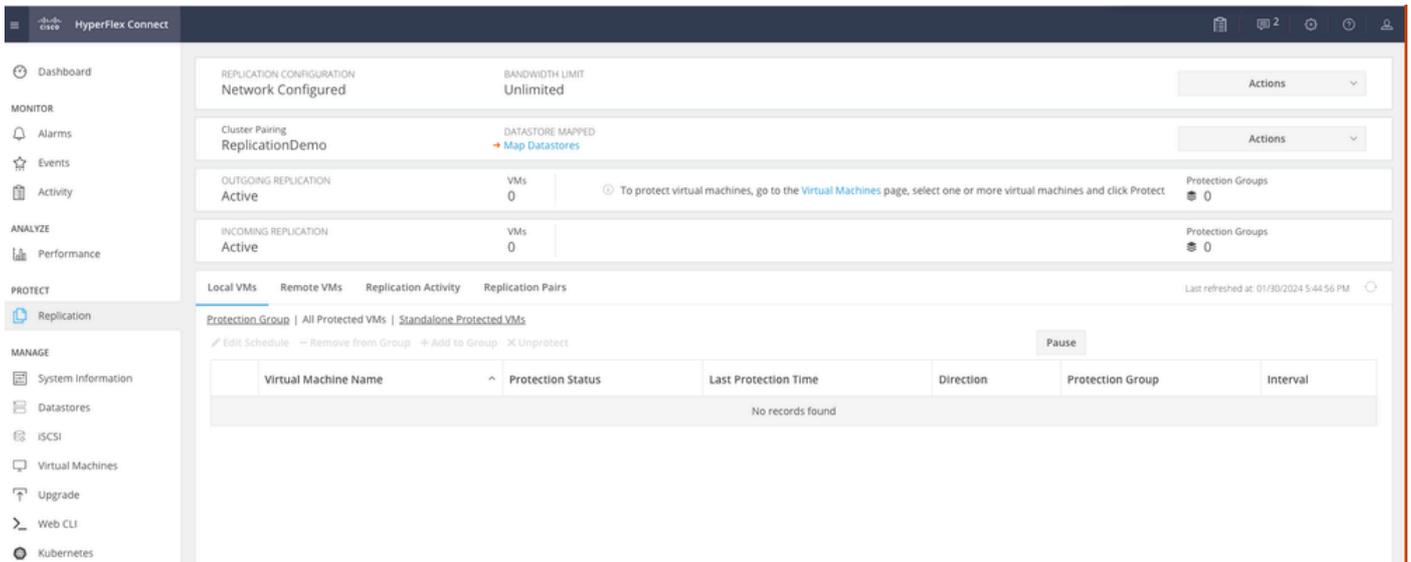
Passaggio 8. Specificare l'IP o l'FQDN di gestione del cluster per il cluster come coppia di replica, quindi fare clic su Associa:



Cluster di associazione

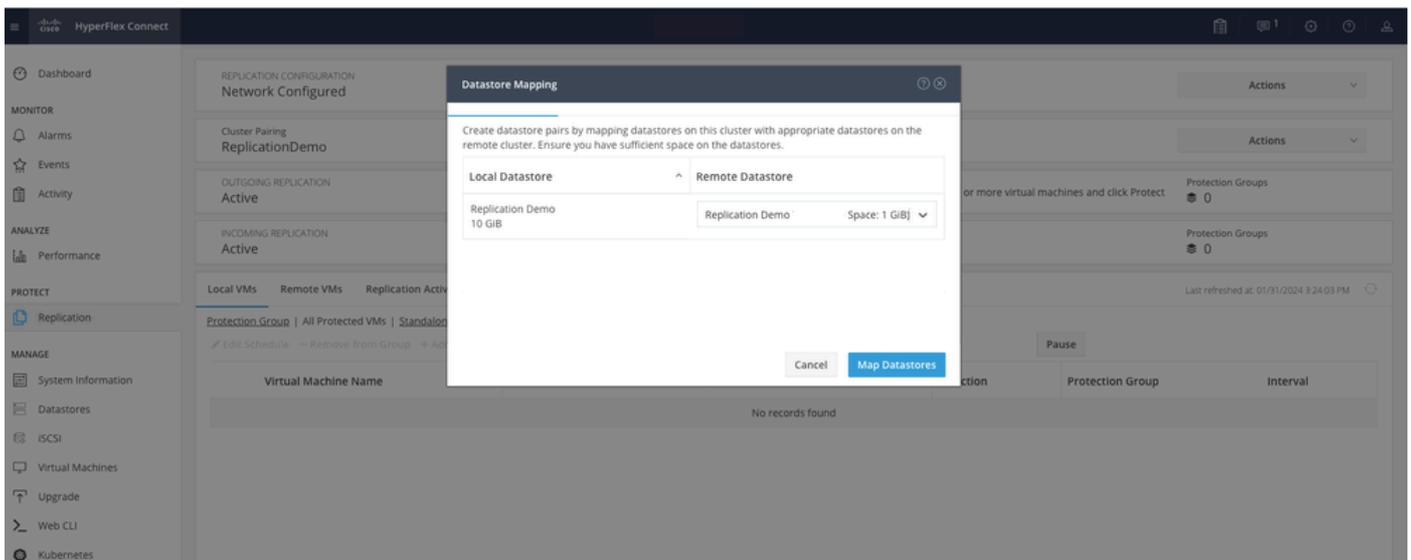
m

Passaggio 8. Una volta accoppiati i cluster, tutto viene impostato per avviare il mapping dell'archivio dati tra i due cluster, all'interno della stessa pagina di replica. Viene visualizzata l'opzione Map Datastore (Mappa archivio dati). Fare clic su di essa:

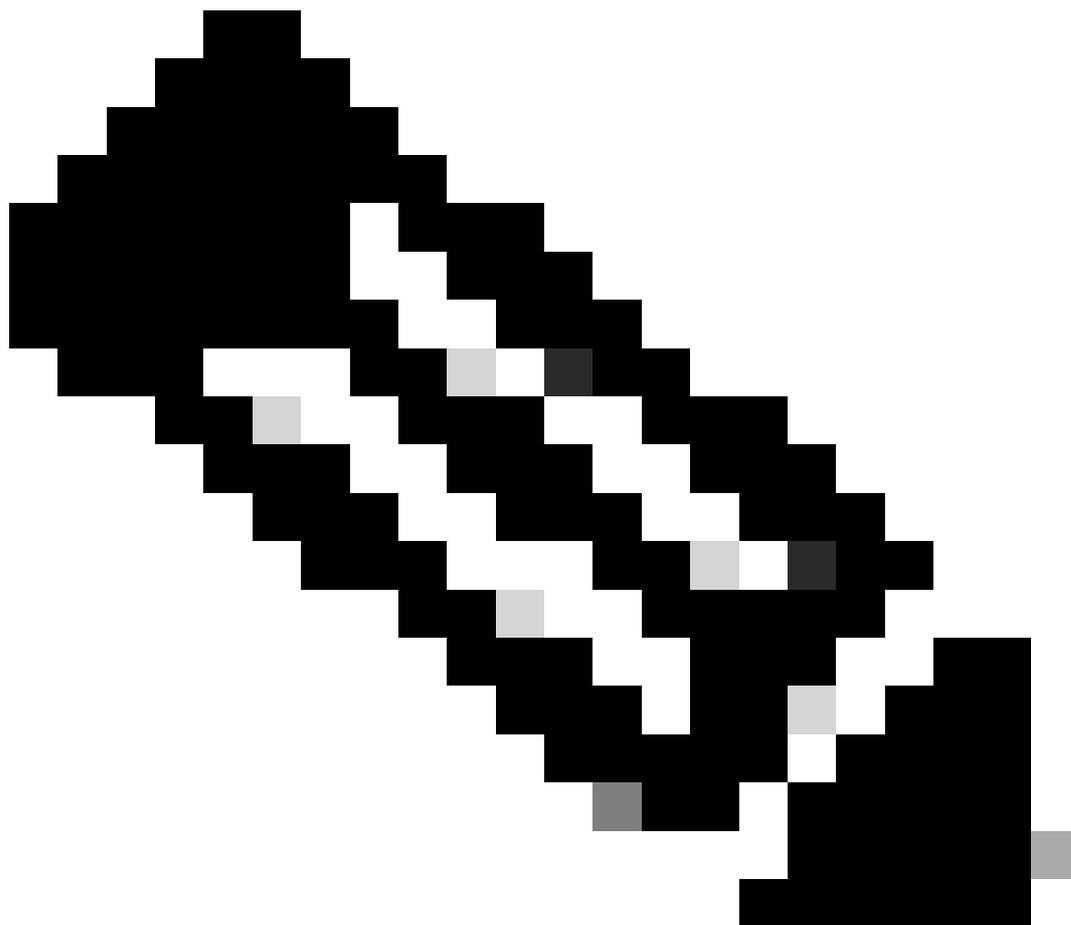


Mappatura dell'archivio dati

Passaggio 9. Nella finestra popup viene visualizzata la mappatura dell'archivio dati che mostra gli archivi dati disponibili nel cluster a sinistra e un menu a discesa con gli archivi dati disponibili nel cluster accoppiato in cui le VM vengono tentate di essere protette:

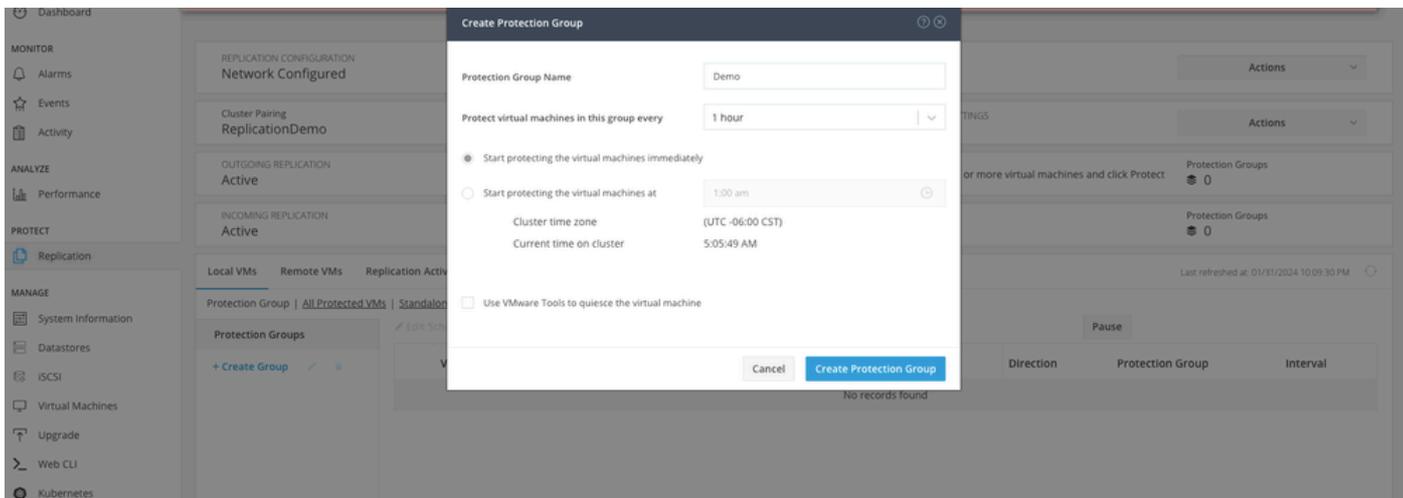


Mappatura degli archivi dati



Nota: il mapping degli archivi dati può essere eseguito da entrambi i siti l'uno all'altro. Ad esempio, Cluster1 può eseguire il mapping degli archivi dati al cluster2 e Cluster2 può eseguire il mapping degli archivi dati al cluster1 senza ulteriori configurazioni.

Passaggio 10. Una volta mappati gli archivi dati, definire il gruppo protezione dati, specificare un nome e selezionare un periodo di tempo per proteggere le macchine virtuali da associare. Specificare infine l'ora di avvio del gruppo protezione dati, quindi fare clic su Crea gruppo protezione dati.

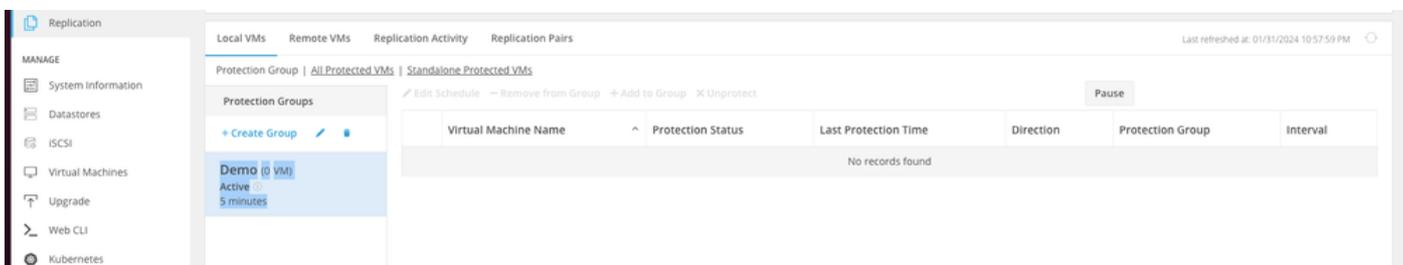


Creazione gruppo protezione dati

Considerazioni sul gruppo protezione dati

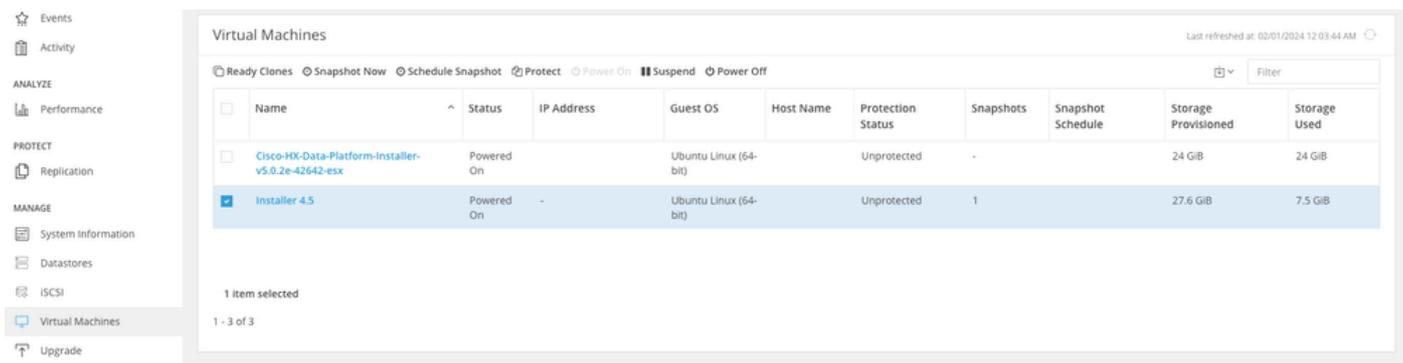
- Il gruppo protezione dati definisce il comportamento della protezione dati.
- Consente di specificare la frequenza di protezione della macchina virtuale.
- Può andare da 5 minuti a 24 ore, anche l'ora in cui inizia la protezione.
- Può avere un'ora immediata o specifica.
- Gli strumenti VMware possono essere attivati per rendere silenziosa la macchina virtuale.

Verrà visualizzato un messaggio che indica che il gruppo protezione dati è stato creato e che è elencato nell'area del gruppo protezione dati:

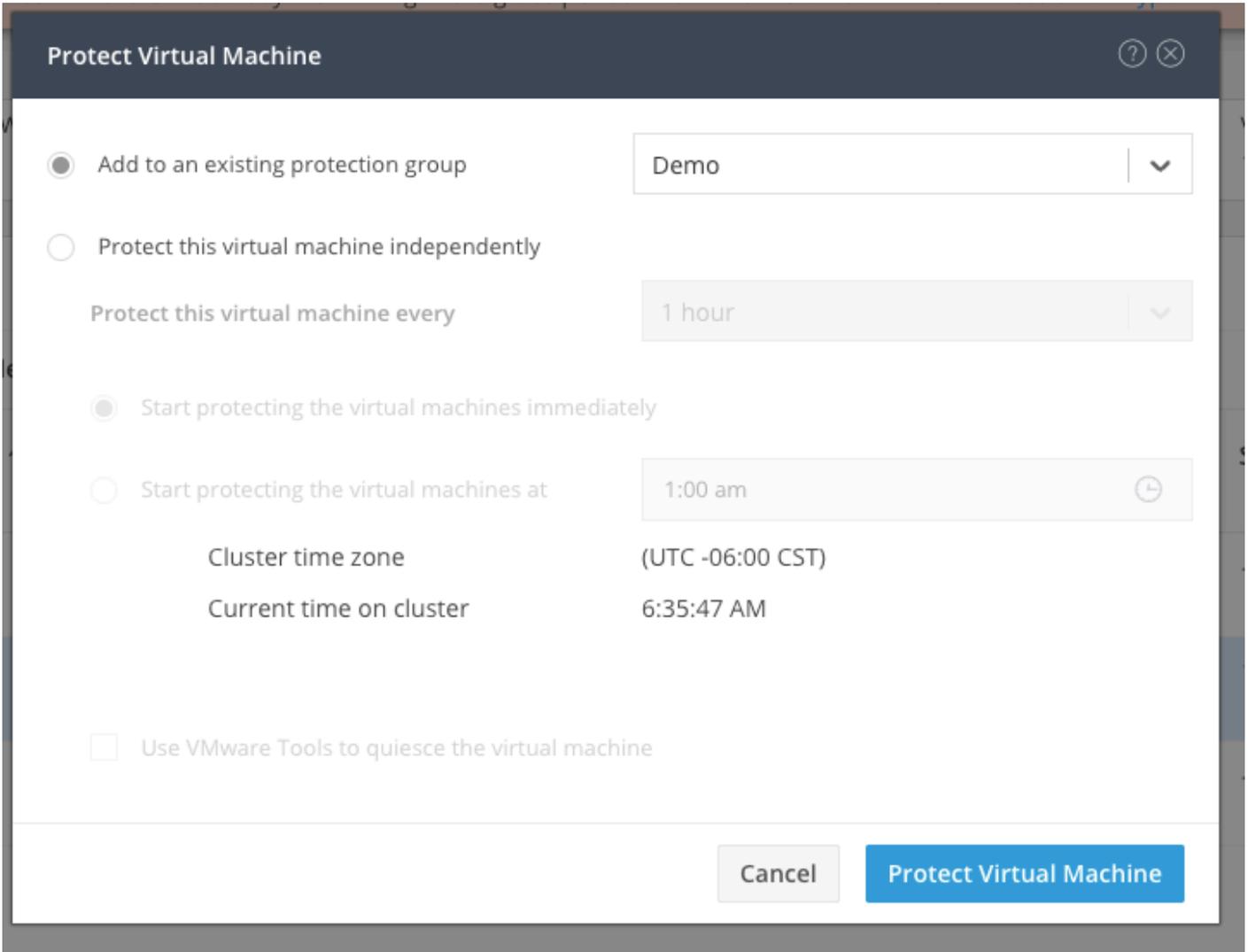


Gruppo protezione dati creato

Passaggio 11. Una volta creato il gruppo protezione dati, il passaggio finale consiste nell'assegnarlo alle macchine virtuali da proteggere. Passare alla scheda Macchine virtuali, selezionare la macchina virtuale da proteggere e fare clic su Proteggi:

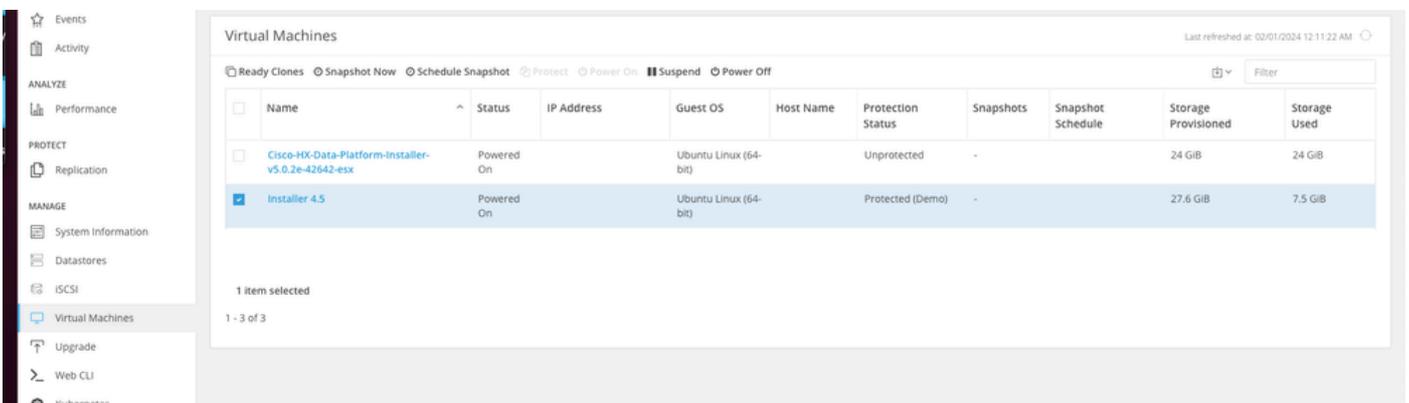


Viene visualizzata una finestra popup che consente di collegare il gruppo protezione dati creato, selezionarlo e fare clic su Proteggi macchina virtuale:

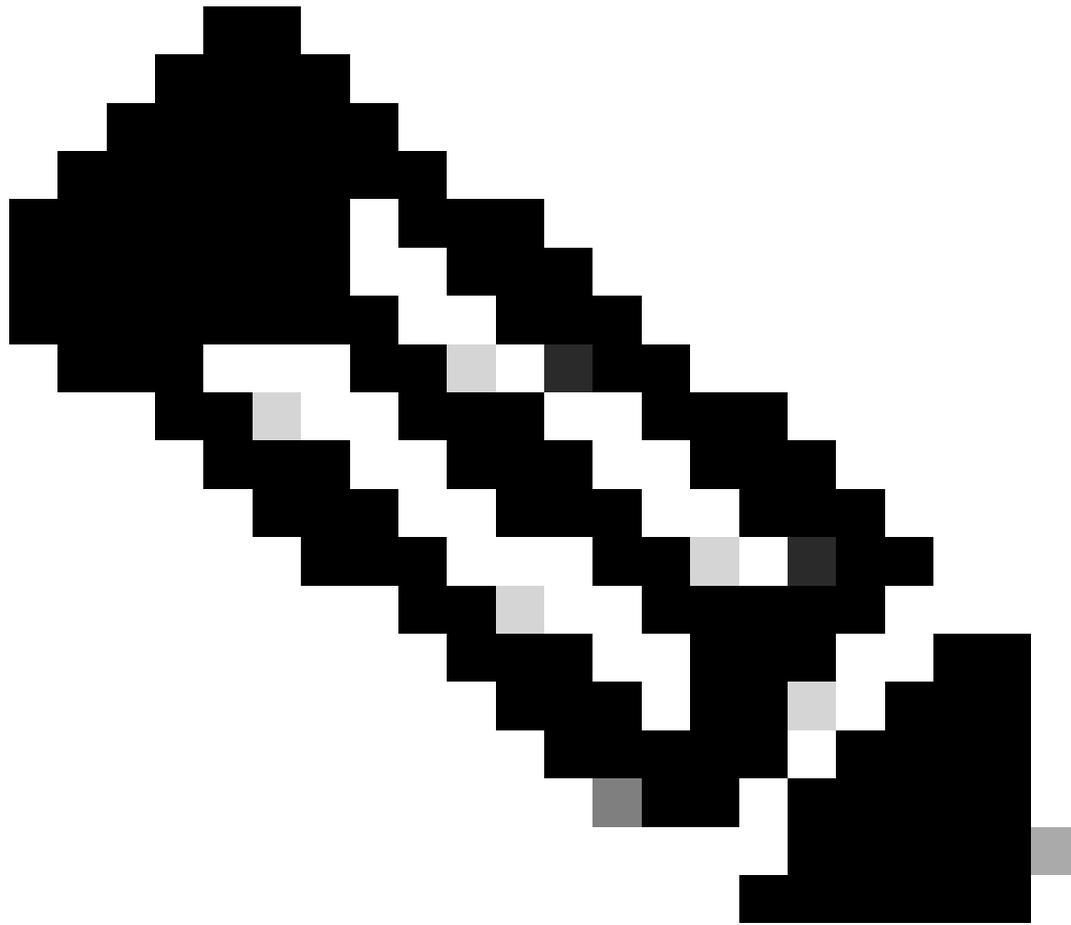


Selezione del gruppo protezione dati

Una volta protetta, la VM viene visualizzata come protetta per il gruppo protezione dati.



VM protetta



Nota: assicurarsi che la macchina virtuale protetta appartenga a un datastore di cui si sta eseguendo il mapping, altrimenti la protezione non riuscirà.

Risoluzione dei problemi

Verifica configurazione protezione macchina virtuale

È buona norma monitorare la protezione della VM nella scheda Replica:

The screenshot displays the VMware vSphere Replication configuration page. The left sidebar shows navigation options: MONITOR (Alarms, Events, Activity), ANALYZE (Performance), PROTECT (Replication), and MANAGE (System Information, Datastores, iSCSI, Virtual Machines, Upgrade, Web CLI, Kubernetes). The main content area shows 'REPLICATION CONFIGURATION' with 'Network Configured' and 'BANDWIDTH LIMIT Unlimited'. Below this, 'Cluster Pairing' is set to 'ReplicationDemo' with '2' datastores mapped. The 'OUTGOING REPLICATION' status is 'Active' with 1 VM protected, 0 exceeding intervals, and 0 current failures. The 'INCOMING REPLICATION' status is also 'Active' with 0 VMs. The 'Replication Activity' tab is selected, showing a table of protected VMs:

Virtual Machine Name	Protection Status	Last Protection Time	Direction	Protection Group	Interval
Installer 4.5	Protected	02/01/2024 6:50:46 AM	Outgoing	Demo	Every 5 minutes

Monitoraggio delle VM protette

Monitoraggio delle attività di replica

Le attività di replica possono essere monitorate facendo clic su nella scheda Attività di replica:

This screenshot shows the 'Replication Activity' tab in the VMware vSphere Replication interface. It displays a table of completed replication activities for the 'Installer 4.5' VM across five instances:

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

Attività di replica

Problemi comuni

Associa problemi

I problemi di accoppiamento possono apparire:

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. ✘		
<p>Establish a connection to a remote cluster</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <p>Management IP or FQDN</p> <p>User Name</p> <p>Password</p> </div> <div style="width: 65%;"> <input style="width: 100%; height: 25px; margin-bottom: 5px;" type="text"/> <input style="width: 100%; height: 25px; margin-bottom: 5px;" type="text" value="admin"/> <input style="width: 100%; height: 25px; margin-bottom: 5px;" type="password"/> </div> </div> <p style="font-size: 0.8em; margin-top: 10px;"> i Enter single sign-on or cluster credentials for remote cluster </p>		
		Back Pair

Problemi di accoppiamento

- Verificare che la rete di replica sia configurata in entrambi i cluster.
- Assicurarsi che i cluster siano raggiungibili l'uno dall'altro.

Problemi di connettività

- Verificare che eth2 sia presente. Utilizzare il comando ifconfig su ciascuna delle macchine virtuali del controller di storage per verificare che eth2 sia configurato correttamente su di esse.
- Usare il comando ping per verificare la connettività tra le interfacce eth2.
- Verificare che la VLAN di replica in entrambi i cluster corrisponda.
- Verificare che la VLAN di replica sia configurata correttamente in tutti i percorsi tra i cluster.

```

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:~$ █

```

Test Ping

Problemi relativi alla protezione

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

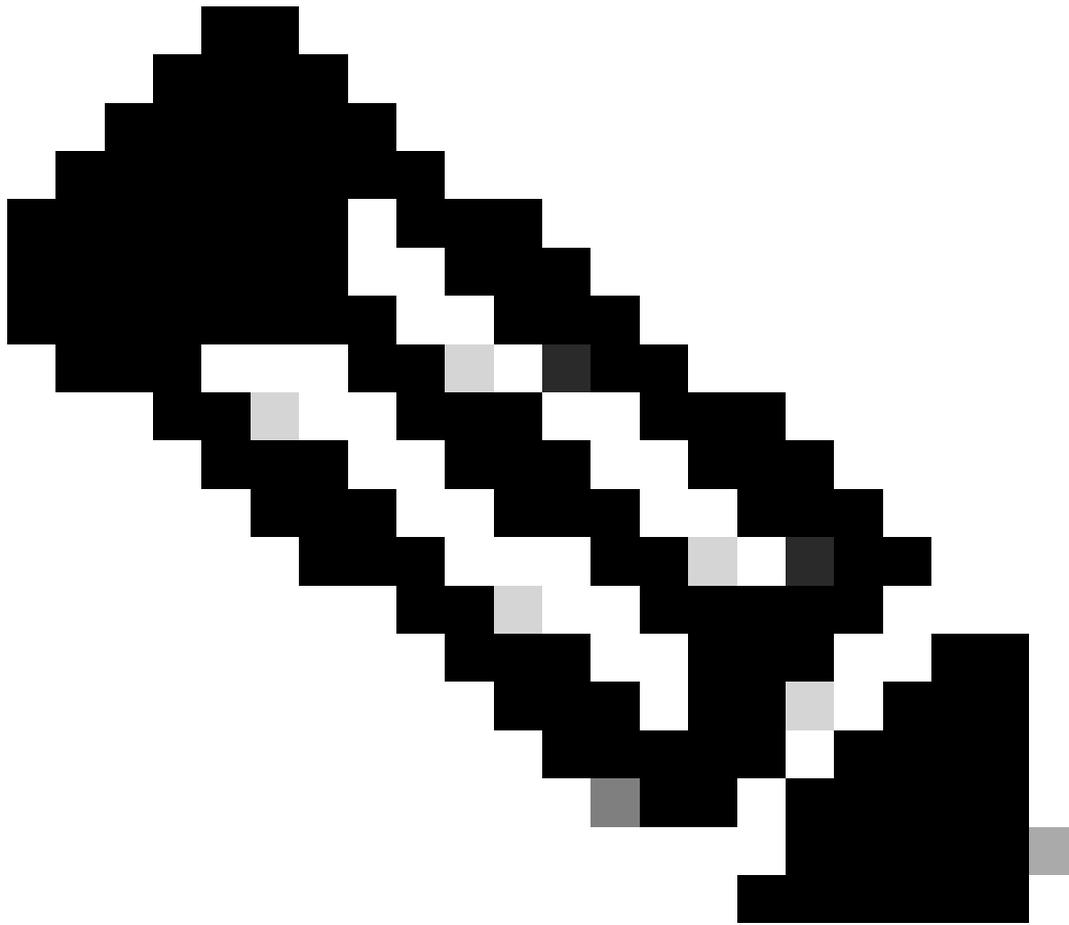
Use VMware Tools to quiesce the virtual machine

Cancel

Protect Virtual Machine

Problemi relativi alla protezione

- Verificare che la macchina virtuale da proteggere appartenga a un archivio dati mappato.
- Assicurarsi che gli archivi dati siano mappati correttamente.



Nota: per alcune correzioni è necessario l'intervento del Technical Assistance Center (TAC). Apri una richiesta con TAC, se necessario.

Informazioni correlate

- [Guida all'amministrazione di Cisco HyperFlex Data Platform, versione 5.0](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).