

Configure Data Protection in Hyperflex

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Additional Background Information](#)

[Procedure](#)

[Protection Group Considerations](#)

[Troubleshoot](#)

[Verify VM Protection Configuration](#)

[Monitor Replication Activities](#)

[Common Issues](#)

[Pair Issues](#)

[Connectivity Issues](#)

[Protection Issues](#)

[Related Information](#)

Introduction

This document describes how to configure replication in Hyperflex.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

The information in this document is based on these software and hardware versions:

- HyperFlex Connect 5.0.2d
- Hyperflex Stretch Cluster
- Hyperflex Standard Cluster
- UCSM 4.2(11)
- vCenter 7.0 U3



Note: For the Data protection is required to have the same Hyperflex Data Platform version in both clusters, cluster can be different in size and type.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Hyperflex Data Protection provides you with a disaster recovery plan. It allows you to have automatic snapshots that are replicated to remote cluster. Snapshots for the protected virtual machines are sent to the remote cluster depending on the frequency configured in the cluster. Nevertheless, only most recently taken snapshot remains on the destination cluster.

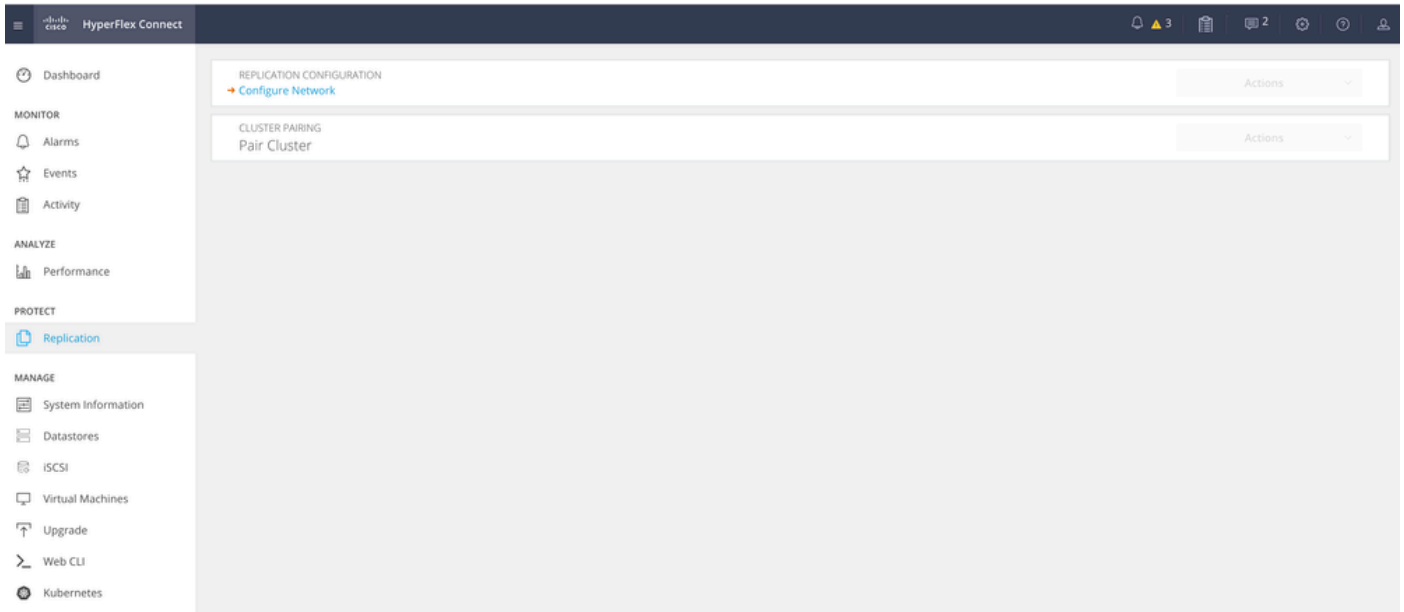
Additional Background Information

- It is a best practice when configuring IP range, to allocate more IPs than nodes present in the cluster in case that an expansion is planned for the future.
- MTU must be the same in both ends.

- Replication network must use the same IP subnet in both clusters along the same VLAN.

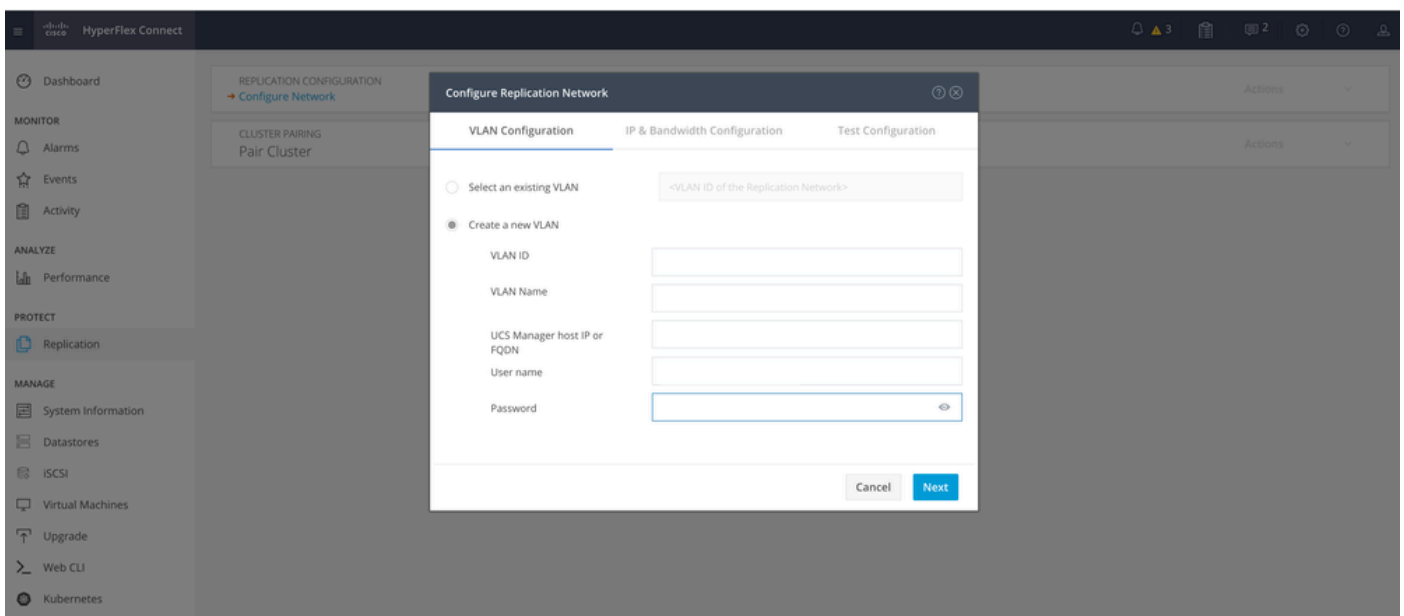
Procedure

Step 1. Log into the Hyperflex system and go to the **Replication** option in the left action pane:



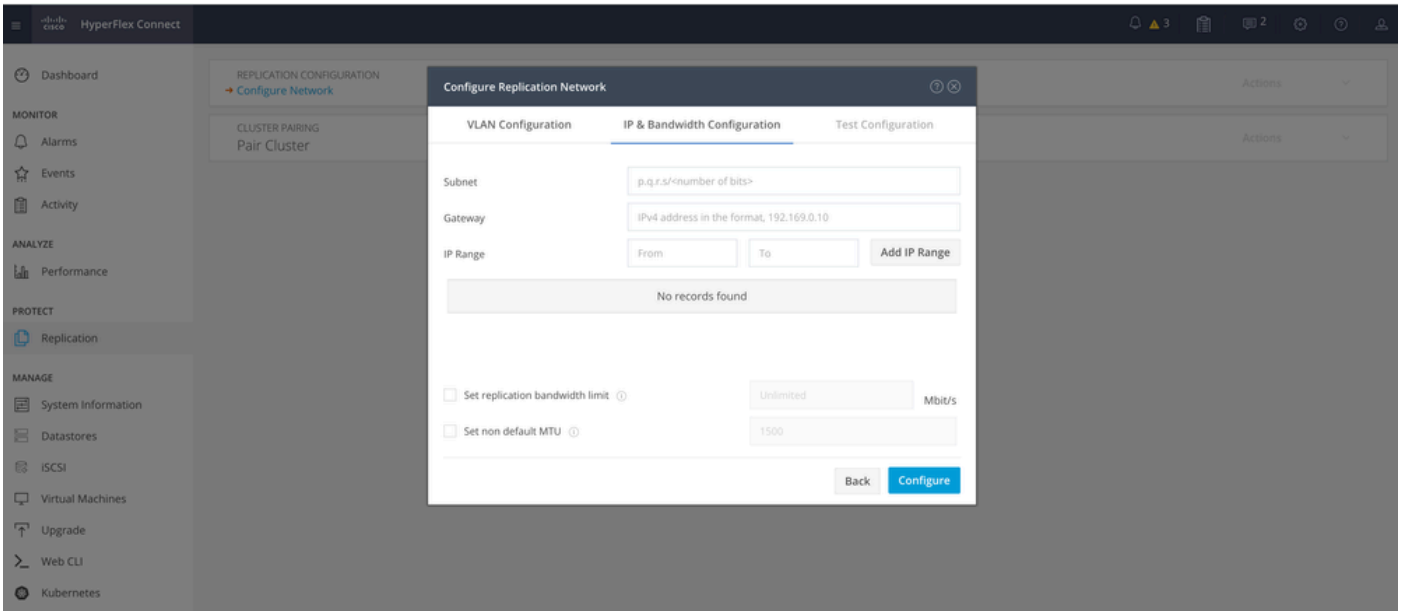
Replication Option

Step 2. Click on the **Configure Network** option, and fill the information for each of the fields and click **Next**:



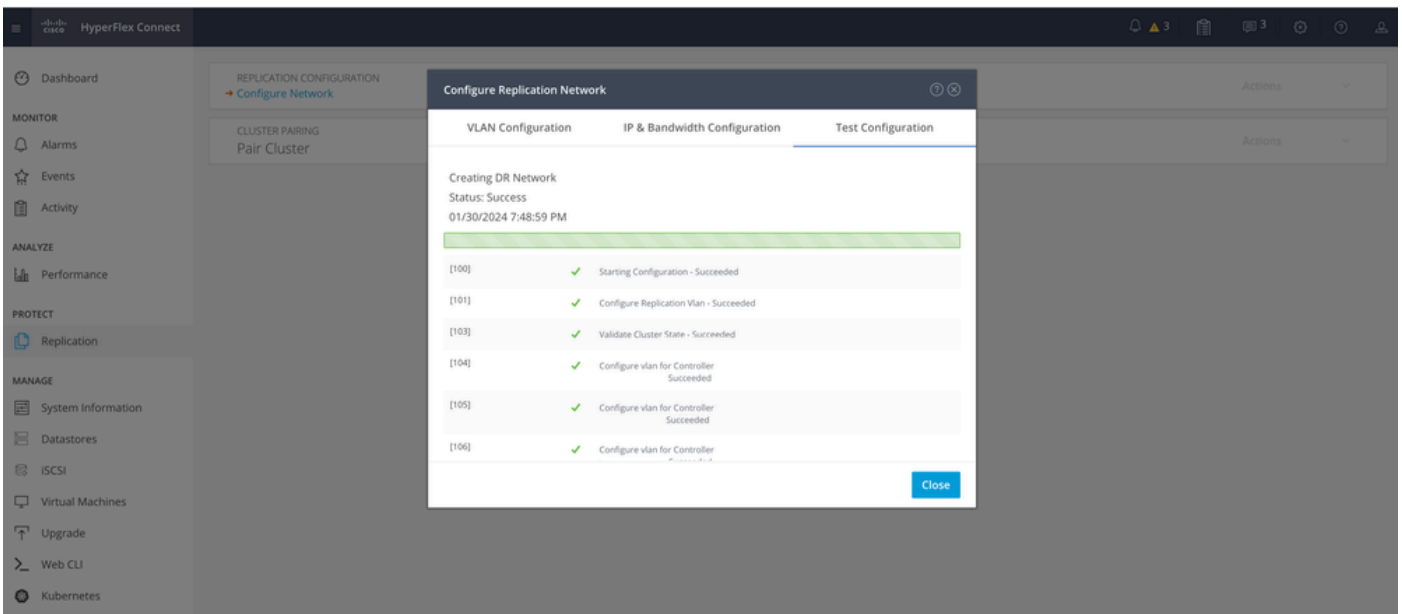
Configure Replication Network

Step 3. Set the IP information for the replication network, adding the subnet, gateway and IP range. Once the IP range is assigned, click on **Add IP Range**, then click **Configure**.



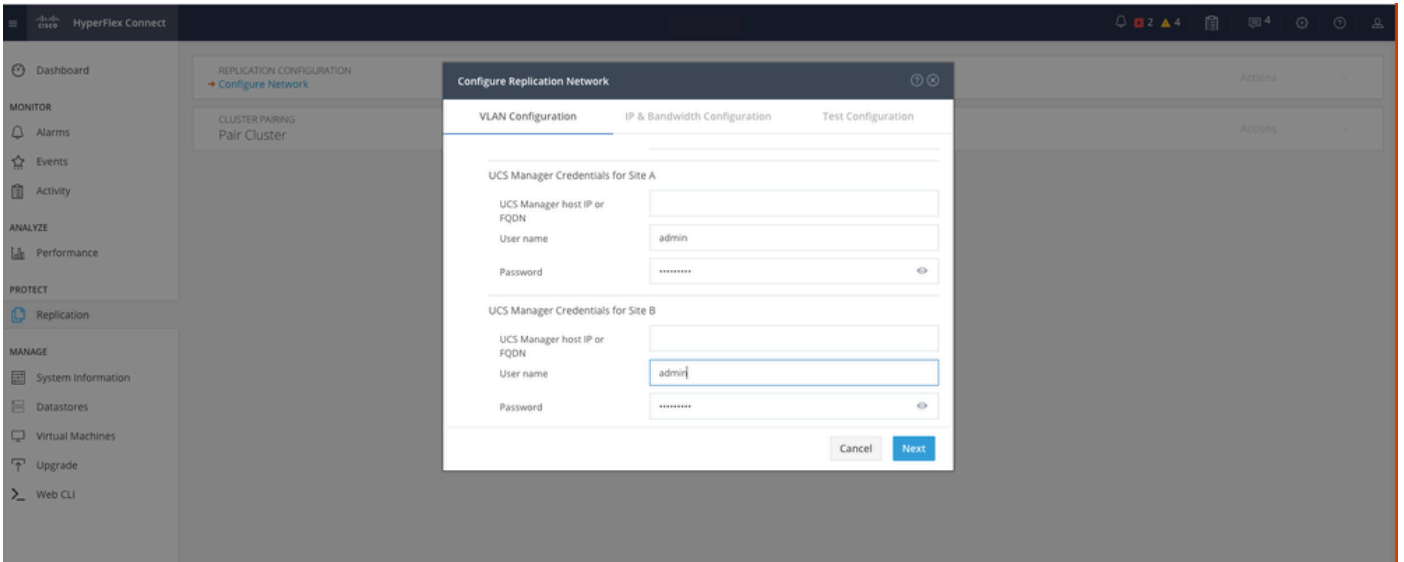
Configure Replication Network

Step 4. The configuration is validated and applied, once completed, click **Close**:



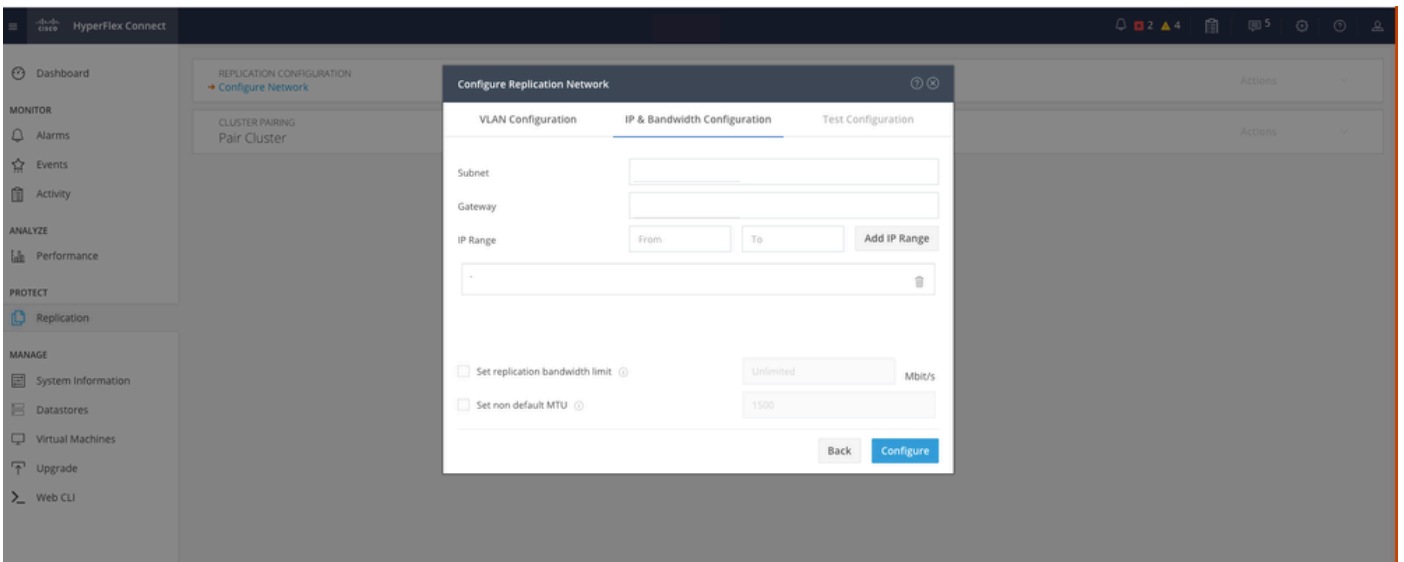
DR Network Configuration

Step 5. Configure the network in the other cluster. For this example the second cluster is stretch, hence both UCSM credentials are required. Fill the information as applicable and click **Next**:



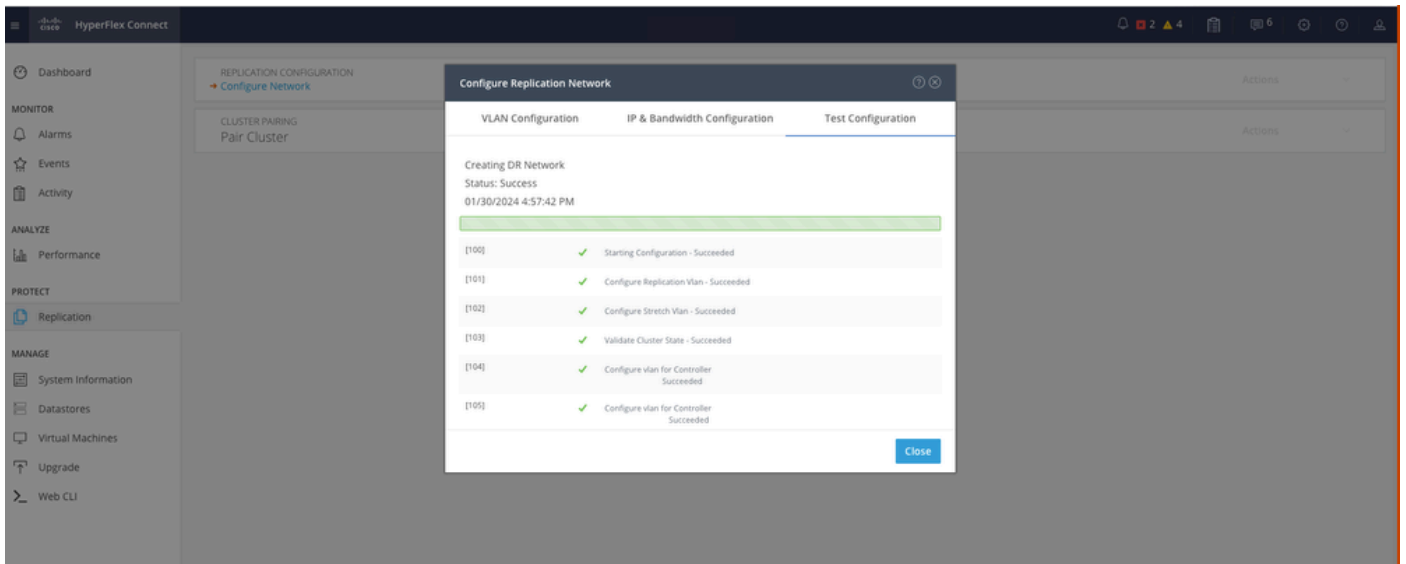
Second Cluster Network Configuration

Step 6. Set the IP information for the replication network on the second cluster, adding the same subnet, gateway and IP range. Once the IP range is assign, click on **Add IP Range**, then click **Configure**:

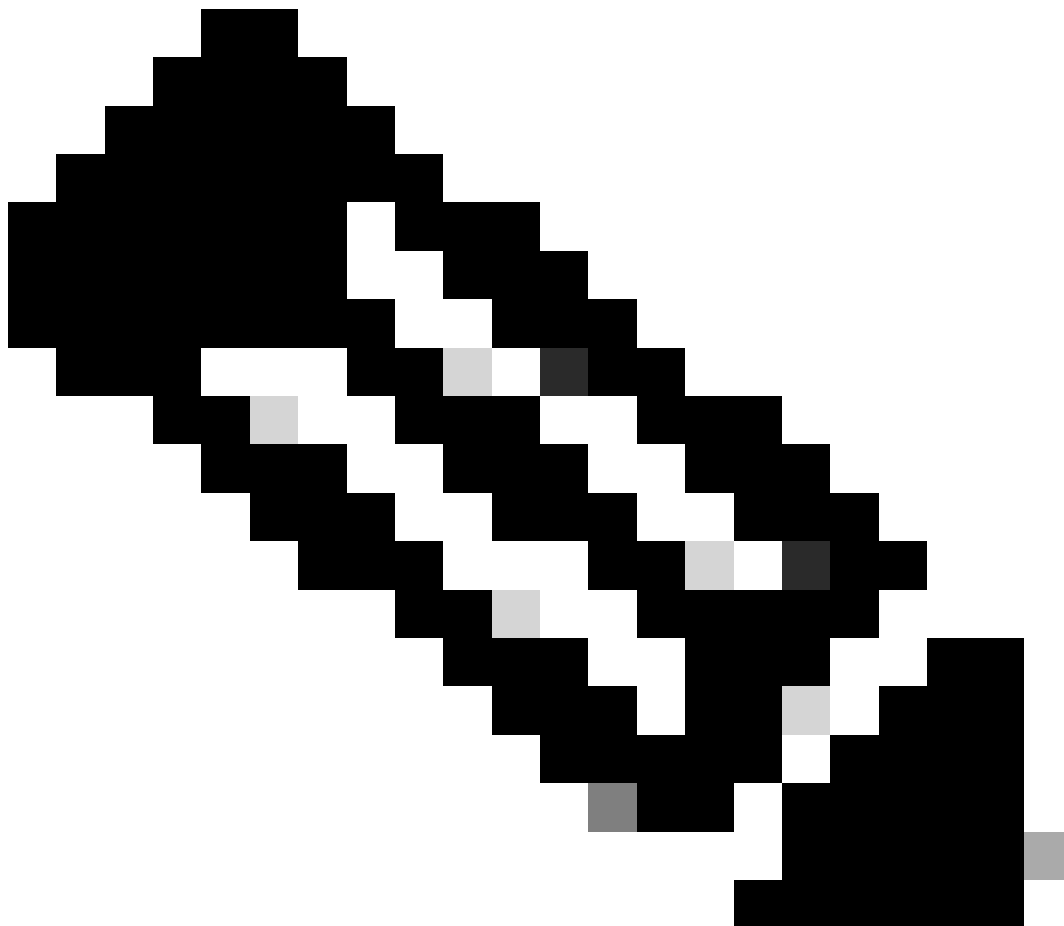


Configuring Network Second Cluster

Step 7. Once the configuration is completed a success status appears, then click **Close**:



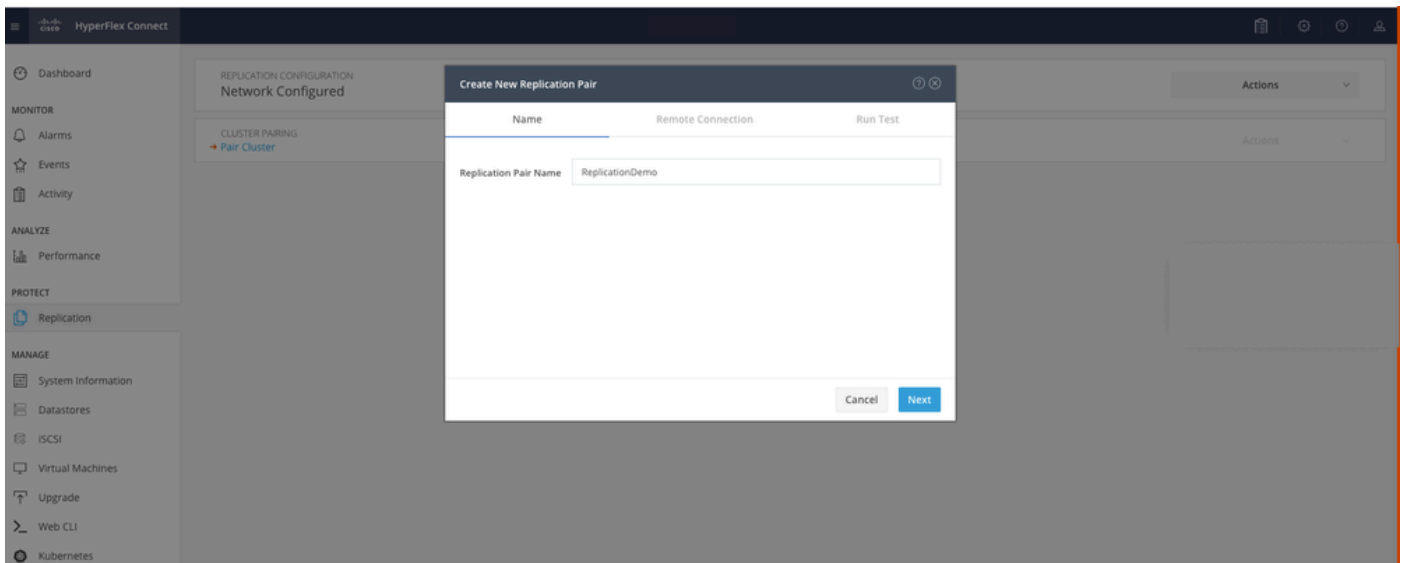
DR Network Configuration Second Cluster



Note: Once the network is configured, it is a best practice to do a network test between the two clusters to confirm they are able to reach each other. Use ping to test the IPs reachability between

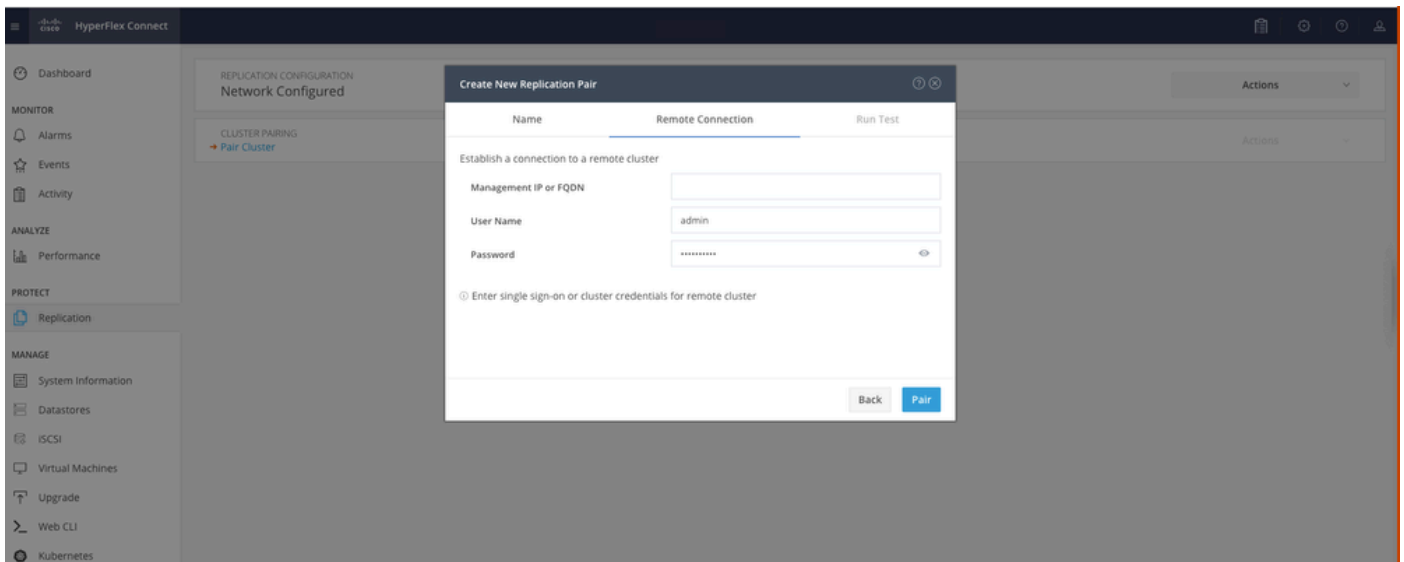
the eth2 interfaces.

Step 7. Creating the replication pair, click **Replication** and then click on **Pair Cluster** in the **Cluster Pairing** option. Assign a name for the **Replication Pair Name** and click Next:



Replication Pair

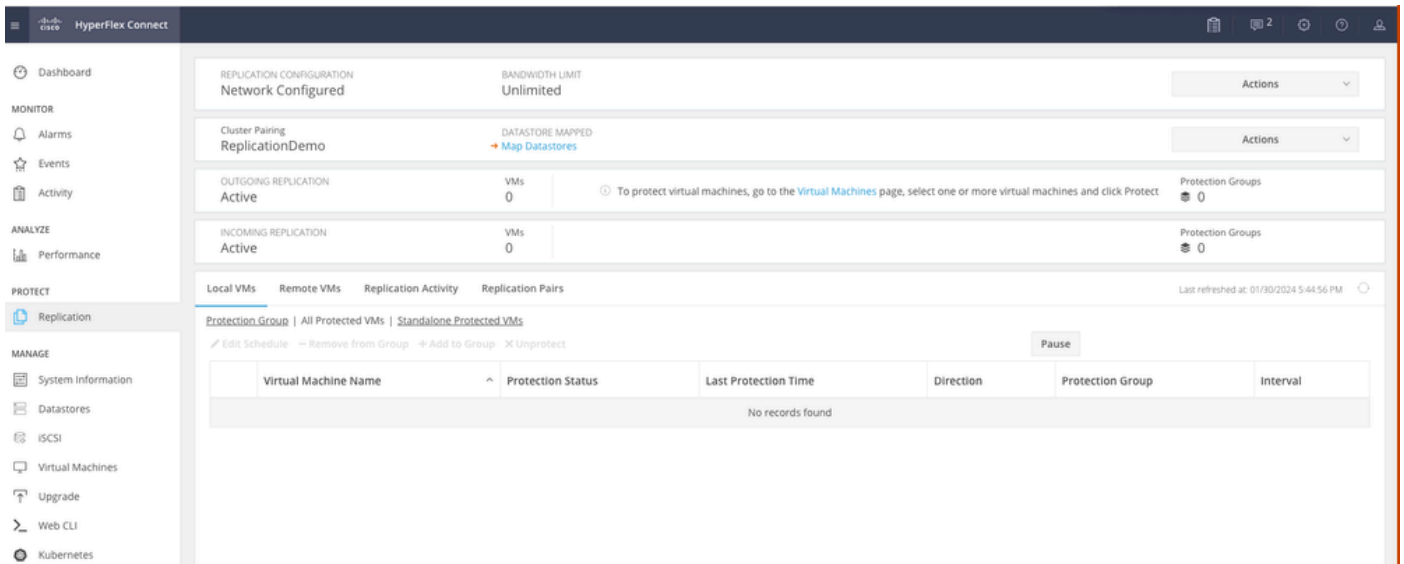
Step 8. Provide the cluster **Management IP** or **FQDN** for the cluster to be the replication pair and then click **Pair**:



Pairing Cluster

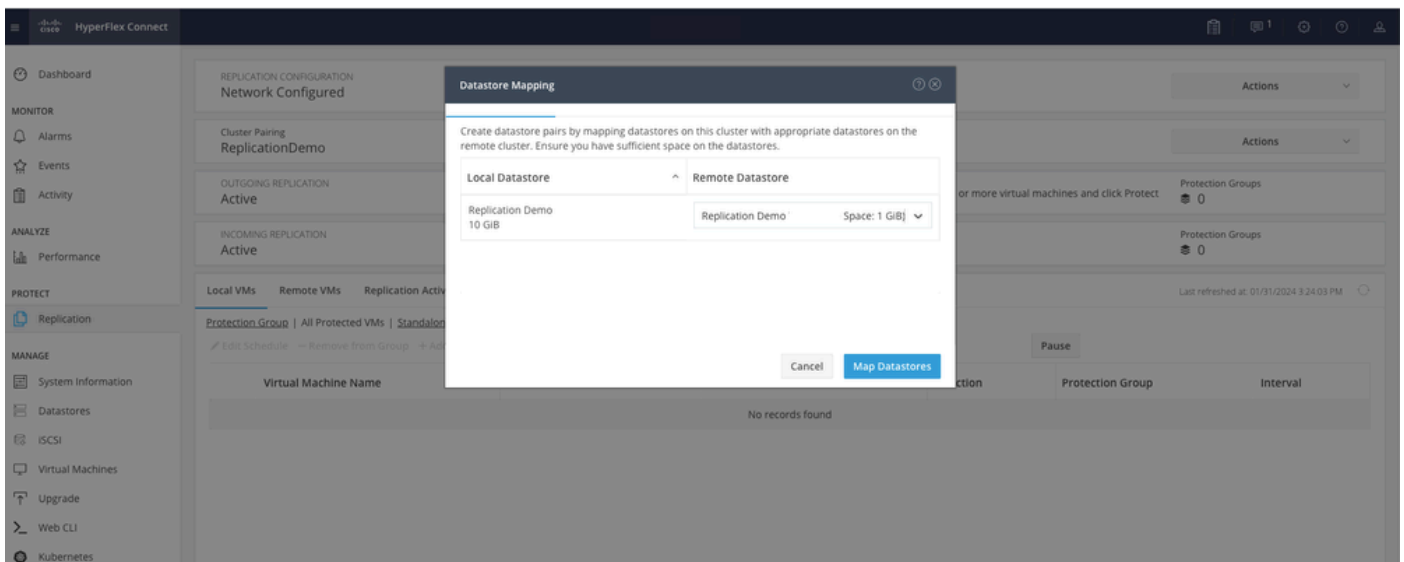
m

Step 8. Once the clusters are paired, everything is set to start the datastore mapping between the two clusters, within the same replication page. The **Map Datastore** option appears, click on it:

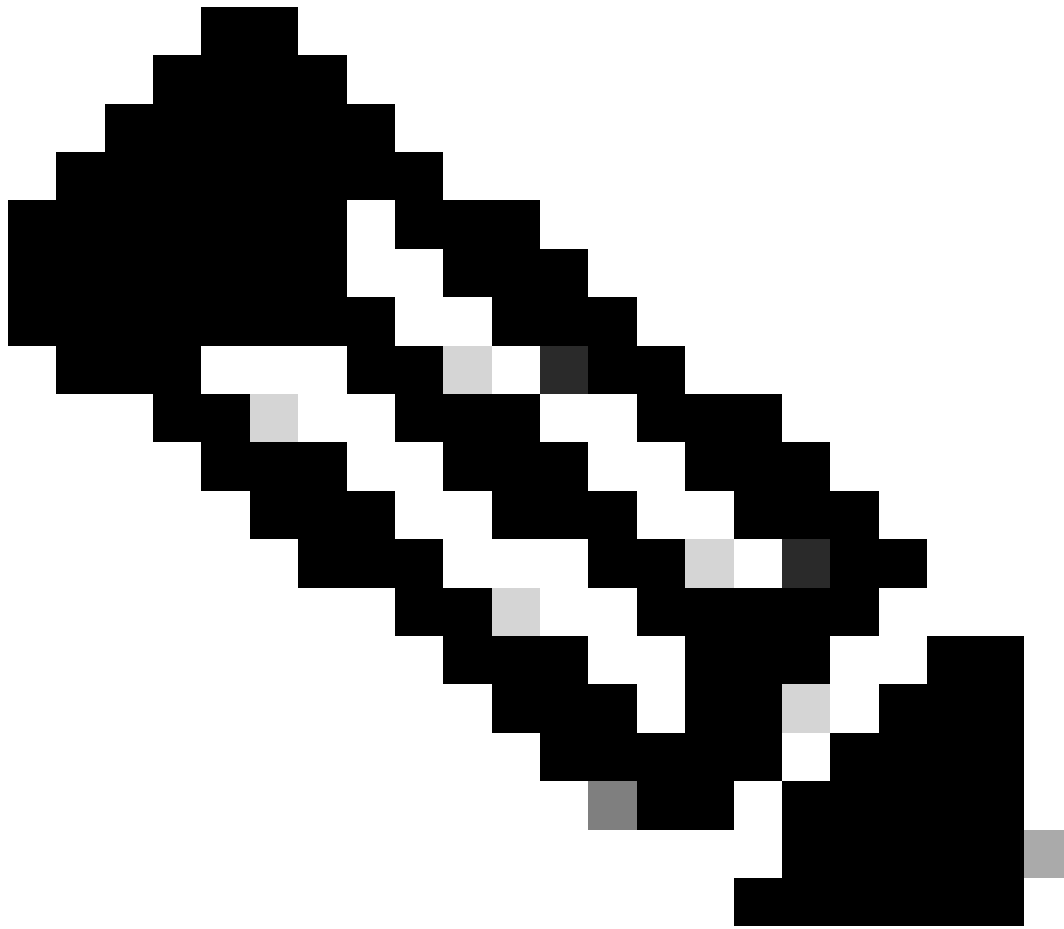


Mapping Datastore

Step 9. In the pop up window the **Datastore Mapping** appears, showing the available datastores in the cluster in the left, and a drop down menu with the available datastores in the paired cluster where the VMs are attempted to be protected:

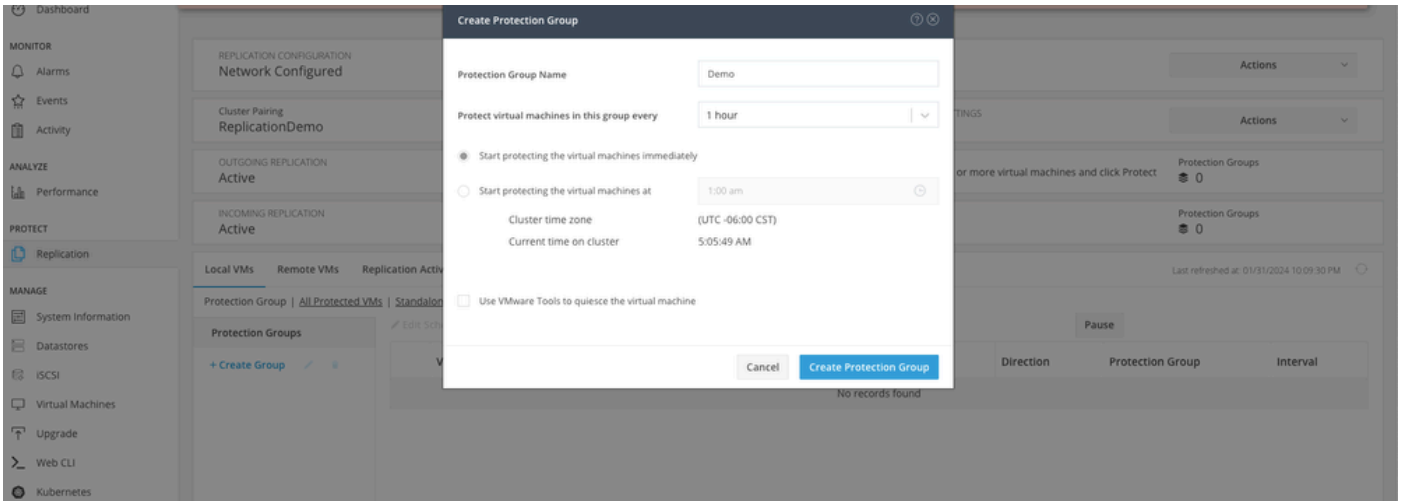


Mapping Datastores



Note: Mapping datastores can be done from both sites to each other, for example, Cluster1 can Map datastores to cluster2 and Cluster2 can map datastores to cluster1 without any additional configuration.

Step 10. Once the datastores are mapped, define the protection group, specify a name and select a time period to protect the virtual machines to be associated to it. Finally, specify the time when the protection group starts, then click **Create Protection Group**.

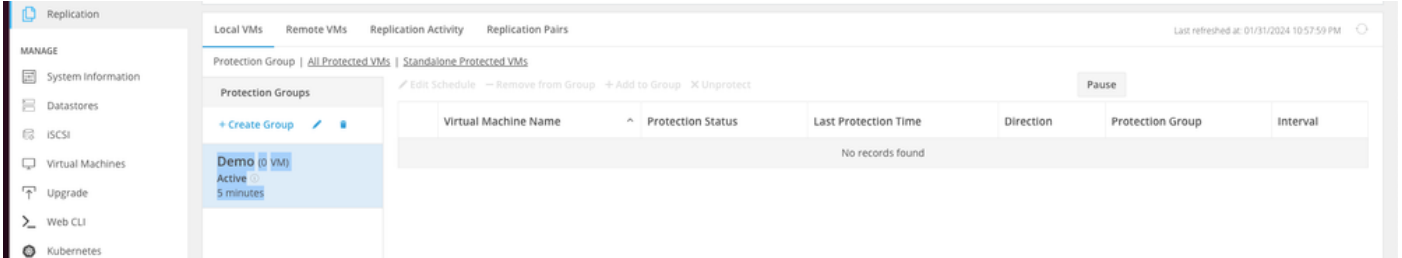


Protection Group Creation

Protection Group Considerations

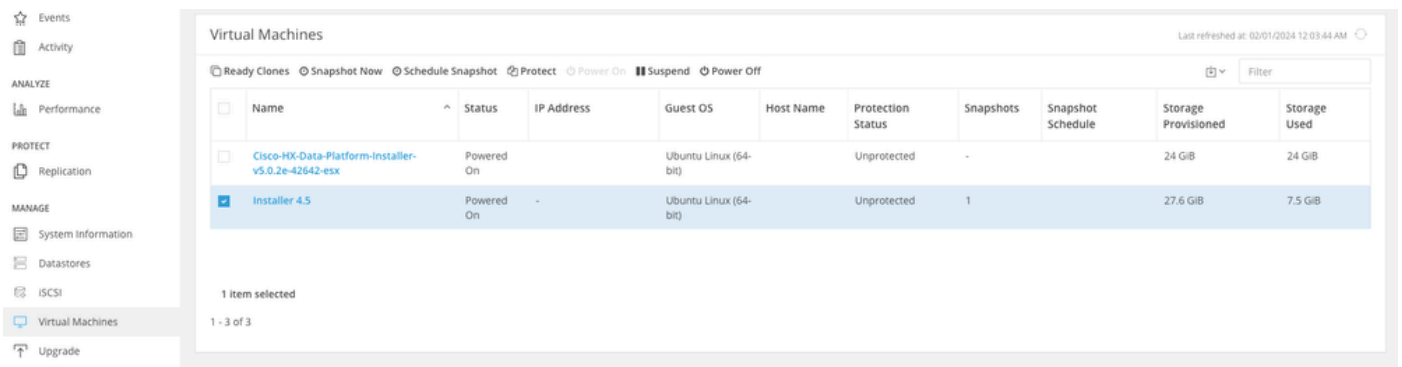
- The protection group defines how the data protection behaves.
- It allows you to specify the frequency to protect the virtual machine.
- It can go from 5 minutes to 24 hours, also the time when the protection starts.
- It can have an immediate or specific time.
- VMware tools can be enabled to quiet the virtual machine.

A success message appears indicating that the **Protection Group** was created and it appears listed in the protection group area:



Protection Group Created

Step 11. With the protection group created, the final step is to assign it to the virtual machines that are to be protected. Navigate to the **Virtual Machines** tab, select the virtual machine to be protected and then click on **Protect**:



Virtual Machine Protection

A pop up window appears to attach the Protection Group created, select it, and click on **Protect Virtual Machine**:

Protect Virtual Machine

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 6:35:47 AM

Use VMware Tools to quiesce the virtual machine

Cancel Protect Virtual Machine

Selecting the Protection Group

Once protected, the VM displays as protected for the Protection Group.

Virtual Machines Last refreshed at: 02/01/2024 12:11:22 AM

Ready Clones Snapshot Now Schedule Snapshot Protect Power On Suspend Power Off Filter

<input type="checkbox"/>	Name	Status	IP Address	Guest OS	Host Name	Protection Status	Snapshots	Snapshot Schedule	Storage Provisioned	Storage Used
<input type="checkbox"/>	Cisco-HX-Data-Platform-Installer-v5.0.2e-42642-esx	Powered On		Ubuntu Linux (64-bit)		Unprotected	-		24 GiB	24 GiB
<input checked="" type="checkbox"/>	Installer 4.5	Powered On		Ubuntu Linux (64-bit)		Protected (Demo)	-		27.6 GiB	7.5 GiB

1 item selected
1 - 3 of 3

VM protected



Note: Ensure that the protected VM belongs to a datastore being mapped, otherwise the protection fails.

Troubleshoot

Verify VM Protection Configuration

It is a best practice to monitor the VM protection under the **Replication** tab:

The screenshot shows the 'Replication Configuration' page. At the top, it indicates 'Network Configured' and 'Bandwidth Limit: Unlimited'. Below this, there are sections for 'Cluster Pairing' (ReplicationDemo), 'OUTGOING REPLICATION' (Active, 1 VM, Protected: 1, Exceeds Interval: 0, Current Replication Failures: 0), and 'INCOMING REPLICATION' (Active, 0 VMs). The main table is titled 'Local VMs' and shows one protected VM:

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

Monitoring Protected VMs

Monitor Replication Activities

Replication activities can be monitored by clicking in the **Replication Activity** tab:

The screenshot shows the 'Replication Activity' tab. It displays a table of replication activities for the 'Installer 4.5' VM:

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

Replication Activities

Common Issues

Pair Issues

Pairing issues can appear:

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; margin-bottom: 10px;"> <div style="width: 30%;">Management IP or FQDN</div> <input style="width: 60%; border: 1px solid #ccc;" type="text"/> </div> <div style="display: flex; justify-content: space-between; margin-bottom: 10px;"> <div style="width: 30%;">User Name</div> <input style="width: 60%; border: 1px solid #ccc; border-bottom: none;" type="text" value="admin"/> </div> <div style="display: flex; justify-content: space-between;"> <div style="width: 30%;">Password</div> <input style="width: 60%; border: 1px solid #ccc; border-bottom: none;" type="password"/> 👁 </div> <p style="font-size: 0.8em; margin-top: 10px;"> i Enter single sign-on or cluster credentials for remote cluster </p>		
		Back Pair

Pairing issues

- Ensure the replication network is configured in both clusters.
- Ensure clusters are reachable from each other.

Connectivity Issues

- Verify the eth2 is present. Use the ifconfig command on each of the storage Controller Virtual Machines to confirm the eth2 is properly configured on them.
- Use ping to test connectivity between the eth2 interfaces.
- Ensure the Replication VLAN in both clusters match.
- Ensure the replication VLAN is properly configured in all the paths between the clusters.

```

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:~$ █

```

Ping Test

Protection Issues

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

Protection Issues

- Ensure that the VM to be protected belongs to a mapped datastore.
- Ensure datastores are properly mapped.



Note: Some fixes require Technical Assistance Center (TAC) intervention. Open a case with TAC, if necessary.

Related Information

- [Cisco HyperFlex Data Platform Administration Guide, Release 5.0](#)
- [Cisco Technical Support & Downloads](#)