# Table of Contents

ABOUT THE HCX ENTERPRISE USER MANUAL .......................................................... 5

INTENDED AUDIENCE .......................................................................................... 5

VMware Technical Publications Glossary ............................................................. 5

CHAPTER 1. INTRODUCTION TO VMWARE HCX .................................................... 6

1.1 VMware HCX Overview .................................................................................. 6

1.2 VMware HCX Components .......................................................................... 7

CHAPTER 2. PREPARING FOR VMWARE HCX DEPLOYMENTS ......................... 8

2.1 General Requirements .................................................................................. 8

2.1.1 HCX Virtual Hardware Requirements .................................................. 8

2.1.2 HCX Feature Interoperability Requirements ........................................ 9

2.1.3 Requirements for HCX Activation ......................................................... 9

2.2 HCX Network Requirements ...................................................................... 11

2.2.1 HCX Network Address Assignments .................................................... 11

2.2.2 Network Ports for HCX WAN Connections .......................................... 12

2.2.3 HCX Local Connections ....................................................................... 12

2.2.4 HCX Standard Management Connections .......................................... 12

2.2.5 HCX over MPLS/VPLS/Direct Connect ............................................... 12

CHAPTER 3. INSTALLING AND CONFIGURING VMWARE HCX ...................... 13

3.1 VMware HCX Manager Installation ............................................................. 13

3.1.1 Deployment Considerations .................................................................... 13

3.1.2 Obtaining the HCX OVA ...................................................................... 14

3.1.3 Installing the HCX Enterprise Manager OVA ........................................ 14

3.1.4 HCX Activation and Initial Configuration ............................................ 15

3.2 Building the HCX Interconnect .................................................................. 17

3.2.1 Configuring a Remote HCX Site ............................................................ 17

3.2.2 Selecting HCX Services to Enable ....................................................... 18

3.2.3 Configuring the HCX WAN Interconnect Component .......................... 19

3.2.4 Configuring the HCX WAN Optimization Component ....................... 21
CHAPTER 5. UPDATING HCX...........................................................................................................48

5.1 PLANNING FOR HCX UPDATES.................................................................................................48
5.1.1 HCX UPDATE CONSIDERATIONS & REQUIREMENTS..................................................48
5.1.2 RELEASE NOTES................................................................................................................49
5.1.3 DOWNLOADING THE HCX UPDATE SOFTWARE............................................................50
5.2 PERFORMING THE HCX UPDATE ..............................................................................................52
5.2.1 HCX MANAGER UPDATE (ENTERPRISE/SOURCE).......................................................52
5.2.2 HCX MANAGER UPDATE (CLOUD/TARGET).................................................................53
5.2.3 HCX SERVICES UPDATE....................................................................................................54

CHAPTER 6. TROUBLESHOOTING HCX........................................................................................56

6.1 HCX TROUBLESHOOTING BASICS..........................................................................................56
6.1.1 ENABLING SSH ON THE HCX MANAGER.................................................................56
6.1.2 LOGGING IN TO THE HCX MANAGER CLI ...............................................................56
6.1.3 LOCATING THE HCX SYSTEM IDS..................................................................................57
6.1.4 ENABLING CENTRAL CLI...............................................................................................58
6.1.5 USING CENTRAL CLI TO CONNECT TO HCX SERVICES........................................59
6.1.6 GATHERING HCX TECHNICAL SUPPORT LOGS.......................................................59
6.1.7 HCX MANAGER LOGS IN THE CONSOLE.................................................................61
6.2 HCX APPLIANCE HEALTH ......................................................................................................62
6.2.1 HCX MANAGER SERVICES ............................................................................................62
6.2.2 HCX SYSTEM RESOURCES ..........................................................................................63
6.2.3 HCX OPERATIONS IN THE vSPHERE TASK CONSOLE............................................64

6.3 HCX SERVICE HEALTH ........................................................................................................... Error! Bookmark not defined.

APPENDICES ....................................................................................................................................65

APPENDIX I - HCX NETWORK Ports...............................................................................................65
HCX WAN CONNECTIONS (HCX COMPONENTS TO REMOTE TARGETS).............................65
HCX LAN CONNECTIONS (WITHIN THE vSPHERE DATACENTER) ..........................................65
ENTERPRISE MANAGEMENT CONNECTIONS...........................................................................66
About the HCX Enterprise User Manual

The HCX Enterprise User Manual describes how to prepare the Enterprise environment for HCX services, and how to operate HCX services via the vSphere Web Client HCX plugin. The information includes step-by-step configuration instructions and suggested best practices.

Intended Audience

This manual is intended for anyone who will deploy and operate HCX Hybridity & Migration services to meet their multi-site business objectives. The information is written for Architects and Technical Staff who will design, install and operate VMware HCX services. This manual assumes familiarity with VMware vSphere, including VMware ESXi, vCenter Server the vSphere Web Client, and HCX enabled Cloud environment (the target site).

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.
Chapter 1. Introduction to VMware HCX

This chapter introduces VMware HCX, the HCX technologies, and the HCX components.

1.1 VMware HCX Overview

VMware HCX abstracts on-premises vs cloud notions and presents capabilities to Virtual Machines as a continuous hybrid cloud.

VMware HCX enables:

- The modernization of Mission-Critical Application Infrastructure with minimal operational overhead without requiring a retrofit of legacy infrastructure.

- New hybrid datacenter architectures, where premises/private cloud network topologies are efficiently replicated, accelerating app migration, mobility and business continuity, and at scale.

- Seamless migration of hundreds of VMs, bi-directionally, in parallel, on a secure high-performance overlay, over the existing WAN, VPN or Private lines.
1.2 VMware HCX Components

HCX Enterprise Manager (HCX-MGR)

The HCX Enterprise Manager provides a framework for deploying the service appliances. The integration with vCenter allows HCX Operators to be authenticated, and tasks authorized using the existing SSO identity sources. Hybridity actions can be initiated from the HCX manager via the HCX User Interface (in the vCenter Navigator), and via virtual machine and distributed port group context menus.

HCX WAN Interconnect Virtual Appliance (HCX-WAN-IX, CGW)

The HCX Interconnect service appliance provides migration and cross-cloud vMotion capabilities over the internet and private lines to the target site while providing strong encryption, traffic engineering and virtual machine mobility.

HCX WAN Optimization Virtual Appliance (HCX-WAN-OPT)

The HCX WAN Optimization service improves performance characteristics of the private lines or internet paths by leveraging WAN optimization techniques like data de-duplication and line conditioning. This makes performance closer to a LAN environment. It accelerates on-boarding to the cloud using Internet/VPN- without waiting for Direct Connect/MPLS circuits.

HCX Network Extension Virtual Appliance (HCX-NET-EXT, L2C, L2E)

The HCX Network Extension service provides a High Performance (4-6 Gbps) Layer 2 Extension capability. The extension service allows keeping the same IP and MAC addresses during a Virtual Machine migration. Network Extension with Proximity Routing enabled ensures that forwarding between virtual machines connected to extended and routed networks, both on-premises and in the cloud, is symmetrical.
Chapter 2. Preparing for VMware HCX Deployments

This section provides the various requirements, some deployment options, best practices and various design considerations implementation of VMware HCX.

2.1 General Requirements

2.1.1 HCX Virtual Hardware Requirements

<table>
<thead>
<tr>
<th>HCX Component</th>
<th>vCPU</th>
<th>Memory</th>
<th>Disk 1</th>
<th>Disk 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>HCX Enterprise Manager</td>
<td>4</td>
<td>12 GB</td>
<td>60 GB</td>
<td>N/A</td>
</tr>
<tr>
<td>HCX WAN Interconnect (HCX-WAN-IX)*</td>
<td>8</td>
<td>3 GB</td>
<td>2 GB</td>
<td>N/A</td>
</tr>
<tr>
<td>HCX Network Extension (HCX-NET-EXT)*</td>
<td>8</td>
<td>3 GB</td>
<td>2 GB</td>
<td>N/A MB</td>
</tr>
<tr>
<td>HCX WAN Optimization (HCX WAN-OPT)*</td>
<td>8</td>
<td>14 GB</td>
<td>30 GB</td>
<td>70 GB</td>
</tr>
</tbody>
</table>

- The HCX Enterprise Manager appliance will be typically deployed in the management cluster, in the vSphere management network on the management datastores.
- In Datacenters with multiple tiers of performance, plan the HCX Interconnect and WAN Optimization placement in the high performance CPU/Memory & Storage tiers to ensure the fastest migration speeds.
- With the exception of HCX WAN Optimization, the storage datastore can be selected per appliance. It will always be deployed on the datastore selected for the WAN Interconnect component.
2.1.2 HCX Feature Interoperability Requirements

The listed software versions must also meet the [VMware Product Interoperability Matrix](#) compatibility requirements. For example: vCenter 6.5 cannot be used with ESXi 5.1, even though both fall within the listed ranges.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>HCX (API Only)</td>
<td>• vCenter 5.1 - 5.5u1 with ESXi 5.0 - 5.5u3.</td>
</tr>
<tr>
<td>HCX Bulk Migration (UI based)</td>
<td>• vCenter 5.5u2 - with ESXi 5.0 and above.</td>
</tr>
<tr>
<td>HCX Cross-Cloud vMotion and Cold Migration</td>
<td>• vCenter 5.5 and above with ESXi 5.0 and above.</td>
</tr>
<tr>
<td>HCX Network Extension (VLAN)</td>
<td>• vCenter 5.1 and above with ESXi 5.0 and above.</td>
</tr>
<tr>
<td></td>
<td>• vSphere Distributed Switch must be installed.</td>
</tr>
<tr>
<td>HCX Network Extension (VXLAN)</td>
<td>• vCenter 5.5 and above with ESXi 5.1 and above (ESXi 5.0 by applying a workaround).</td>
</tr>
<tr>
<td></td>
<td>• vSphere Distributed Switch must be installed.</td>
</tr>
<tr>
<td></td>
<td>• NSX 6.2+ and above at the local/source site.</td>
</tr>
<tr>
<td>HCX Network Extension with Proximity Routing</td>
<td>• vCenter 5.1 and above with ESXi 5.0 and above.</td>
</tr>
<tr>
<td></td>
<td>• vSphere Distributed Switch must be installed.</td>
</tr>
<tr>
<td>HCX Network Extension of Cisco Nexus 1000v Networks</td>
<td>• vCenter 5.1 and above.</td>
</tr>
<tr>
<td></td>
<td>• vSphere Licensed at Enterprise Plus.</td>
</tr>
<tr>
<td>HCX Disaster Recovery</td>
<td>• vCenter 5.1 with ESXi 5.0 and above.</td>
</tr>
</tbody>
</table>

2.1.3 Requirements for HCX Activation

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>HCX Cloud URL</td>
<td>This is needed for registering a remote HCX site at the local HCX site.</td>
</tr>
<tr>
<td></td>
<td><a href="https://hcx-ip-or-fqdn">https://hcx-ip-or-fqdn</a></td>
</tr>
</tbody>
</table>
This URL is the public address of the Manager component of the HCX Target Site. The way this URL is obtained varies by target site provider.

**HCX in VMware Cloud on AWS**
- Login to console.cloud.vmware.com.
- Open **VMware Hybrid Cloud Extension** > SDDCs > Open HCX > HCX Cloud interface opens in a new tab
- Note the HCX URL.

**HCX in IBM Cloud**
- Login at [IBM Cloud for VMware Solutions Portal](https://cloud.ibm.com)
- Select the instance > Services > Installed Services > HCX > HCX Cloud interface opens in a new tab
- Note the External IP

### Activation Keys

Obtaining the activation keys:

**HCX in VMware Cloud on AWS**
- Login to console.cloud.vmware.com.
- Open VMware Hybrid Cloud Extension > Activation Keys > CREATE ACTIVATION KEYS
- Create an HCX Cloud key for VMware Cloud on AWS
- Create an HCX Enterprise key for HCX On-premises

**HCX in IBM Cloud**
- Login at [IBM Cloud for VMware Solutions Portal](https://cloud.ibm.com)
- Click HCX on IBM > Learn More > Scroll to bottom > Select On-premises HCX > Provide Instance Name > Click Next to place the order > Copy the activation key.
- Use this activation key on-premises. The IBM Cloud is activated automatically during provisioning.

---

1 The remote HCX can be added with IP instead of FQDN, as long as the certificates are imported in the source site HCX appliance management interface.
# 2.2 HCX Network Requirements

## 2.2.1 HCX Network Address Assignments

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HCX Enterprise Manager (HCX-ENT-MGR)</strong></td>
<td>• One management internal IP (typically from the ESXi management network).</td>
</tr>
<tr>
<td><strong>HCX WAN Interconnect (HCX-WAN-IX)</strong></td>
<td>• One management IP per remote site (Preferably allocated from the ESXi management network).</td>
</tr>
<tr>
<td></td>
<td>• One vMotion IP address per remote site (In most environments the vMotion network is not routed, this assignment keeps the network isolated and allows HCX to become a secure proxy to the configured remote site(s)).</td>
</tr>
<tr>
<td><strong>HCX Network Extension (HCX-NET-EXT)</strong></td>
<td>• One management internal IP per Distributed Switch. (Preferably allocated from the ESXi management network).</td>
</tr>
<tr>
<td><strong>On-premises/Local Internet Public IP / NAT</strong></td>
<td>• The local HCX components can share a single public NAT IP address, or they can be configured for 1 to 1 NAT. Both approaches are supported.</td>
</tr>
<tr>
<td><strong>On-premises/Local HTTPS Proxy Servers</strong></td>
<td>• HCX should be configured in the proxy bypass settings.</td>
</tr>
<tr>
<td></td>
<td>• The proxy server can be specified in HCX appliance management.</td>
</tr>
<tr>
<td><strong>Remote HCX components</strong></td>
<td>• For each HCX appliance deployed on-premises, a peer appliance is automatically deployed by the remote HCX Cloud (the target site).</td>
</tr>
<tr>
<td></td>
<td>• One Public IP is required per peer appliance. At minimum, two public IP addresses are needed.</td>
</tr>
<tr>
<td></td>
<td>• The current HCX Enabled Cloud services providers will include the minimum IP addresses out of the box but require additional HCX public IPs to be purchased.</td>
</tr>
</tbody>
</table>
2.2.2 Network Ports for HCX WAN Connections

HCX functionality always spans a source and remote site. The local HCX components make network connections to remote components. The connections are detailed in the table below. The perimeter firewalls should be updated to allow these connections.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol/Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Site HCX Enterprise Manager</td>
<td>connect.hcx.vmware.com</td>
<td>TCP-443</td>
<td>Activation Updates</td>
</tr>
<tr>
<td></td>
<td>hybridity-depot.vmware.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Site HCX Enterprise Manager</td>
<td>Remote Site HCX Cloud Manager</td>
<td>TCP-443</td>
<td>HCX Multisite Management</td>
</tr>
<tr>
<td>Local Site HCX-WAN-IX (CGW)</td>
<td>Remote Site HCX-WAN-IX (CGW)</td>
<td>UDP-500, UDP-4500</td>
<td>HCX WAN Transport Suite B Crypto; IKEv2</td>
</tr>
<tr>
<td>Local Site HCX-NET-EXT (L2C)</td>
<td>Remote Site HCX-NET-EXT (L2C)</td>
<td>UDP-500, UDP-4500</td>
<td>HCX WAN Transport Suite B Crypto; IKEv2</td>
</tr>
</tbody>
</table>

2.2.3 HCX Local Connections

VMware HCX is closely integrated with vSphere Products (vCenter, ESXi, Optionally NSX) - these local connections typically do not traverse a firewall. A complete table for the local connections is available in the appendices, at the end of this manual.

2.2.4 HCX Standard Management Connections

The HCX Manager should be integrated with the local DNS, NTP & Syslog servers. Use your existing processes to ensure these shared services are reachable. Standard protocol ports are used (a complete list is available in the appendices).

2.2.5 HCX over MPLS/VPLS/Direct Connect

By default, HCX will use a minimum of 2 Public IP addresses to connect the HCX-WAN-IX and HCX-NET-EXT components (Public IP addresses are assigned to their uplink interface). In most HCX-enabled Cloud providers, HCX can be configured to use Direct Connect IP/private lines addresses as the uplink IP addresses of the appliances.
Chapter 3. Installing and Configuring VMware HCX

This chapter describes the procedures for installing and configuring VMware HCX. The procedure assumes there is an activated HCX system at the target site.

A deployment of VMware HCX can be summarized in the following steps:

1. Use the previous chapter to plan the deployment. Ensure all requirements are satisfied.
2. Download the OVA from the HCX-enabled target site.
3. Deploy, Activate and Configure the HCX Manager on-premises.
4. Build the HCX Interconnect (establish the source HCX and destination HCX relationship, then deploy the HCX WAN-IX, WAN-OPT, NET-EXT components).

3.1 VMware HCX Manager Installation

3.1.1 Deployment Considerations

- HCX Enterprise Manager is typically placed in the same compute/network/storage resource objects as the vCenter server, and other management Virtual Machines.

- The HCX Enterprise Manager VM should be placed in a network that can make internet-bound HTTPS connections and route internal connections to the ESX Management network (if not placed directly on that network). Typically HCX Manager in the same network as the vCenter server and other management components.

- The HCX Enterprise Manager is deployed as a one-to-one pair with each vCenter Server. The HCX Cloud Manager (the target site HCX Manager) can attach to multiple vCenter Servers that are within a single physical datacenter.

- To integrate vCenter Linked-Mode, deploy HCX Manager as one-to-one pair with each vCenter where HCX is desired; in the HCX Manager’s SSO configuration, the shared Platform Services Controller (PSC) should be specified. HCX-Enabled Linked-mode vCenters will display objects from all linked vCenters during HCX Operations.
3.1.2 Obtaining the HCX OVA

The HCX installation begins with a standard OVF deployment in the vCenter environment. The HCX Manager OVA is deployed using standard OVF deployment procedures in the next section.

The HCX Cloud system contains a link to the correct HCX Enterprise Client (OVA).

Procedure

1. Connect to the HCX Cloud system (browse to the HCX cloud URL identified in the requirements section of this manual > Administration > System Updates tab
2. The OVA can be directly downloaded by clicking the ‘HCX Enterprise Client’ button
   Or, optionally copy the download link, by using the ‘Copy Link’ button, to download via a different system / client.

![HCX Download Link in the HCX Cloud UI](image)

3.1.3 Installing the HCX Enterprise Manager OVA

HCX is deployed from on-premises vCenter using the HCX-Enterprise OVA file.

Procedure

1. Right click the management cluster > click Deploy OVF Template
2. Review the details > Click Next > Accept the EULA > Click Next
3. Name the HCX Manager appliance > Select a Folder > Click Next
4. Select the management datastore (Typically where vCenter is deployed)
5. Select the management network (Typically where vCenter is connected)
6. Provide passwords for the admin and root default users.
7. Expand and fill the Network properties, DNS & Services sections (NTP is required)
   a. In the Network Properties section, provide the VM hostname, and IP address configurations.
b. In the DNS section, provide the local DNS server and Domain Name Search List.
c. In the Services Configuration section, provide the local NTP server (required). Optionally enable SSH.

8. Click Next. Finish.

The OVA deployment binds HCX to vCenter as an Extension. It may take up to 5 minutes for the HCX Manager appliance to fully initialize after deploying the OVA.

3.1.4 HCX Activation and Initial Configuration

A new HCX Manager system will need to be activated immediately upon launching the HCX Appliance Management interface, after the newly deployed system is initialized. In the appliance management procedure, vCenter, SSO & optionally NSX systems will be integrated.

![Activation/Initial Configuration Interface](image)

Procedure

1. Browse to the HCX appliance management and authenticate using the admin user. [https://hcx-manager-ip-or-fqdn:9443/](https://hcx-manager-ip-or-fqdn:9443/)

2. Enter the Activation Key (refer to the HCX Deployment Checklist) > click Continue

3. Select the major city to where the HCX Manager system geographically located). HCX sites will be represented visually in the HCX interface > click Continue

4. Click Yes, Continue to acknowledge successful activation.

5. Enter the vCenter Server FQDN, Username & Password

6. If NSX integration is required (e.g. Extending VXLAN networks):
   a. Check Connect your NSX
   b. Enter the NSX server, username and password.

7. Click Continue

8. Enter the PSC URL > click Continue

9. Verify the information. Click RESTART to reinitialize the HCX services. Allow up to 5 minutes for HCX to fully re-initialize (the Appliance Management interface will become
unavailable briefly). Once the HCX Manager system is initialized the HCX Manager Dashboard is displayed.

10. Browse to the Configuration tab, to the vSphere Role Mapping section.

11. Assign the HCX Roles to the vCenter User Groups that will be allowed to perform HCX operations. The groups assigned will need to have sufficient privileges to perform the HCX related operations in vCenter.

12. Click Save

13. Log into the vSphere Web Client > Look for the HCX plugin in the Navigator.

*Log out first if an active session existed during the HCX configuration*

The HCX Manager Initial Configuration is now complete!
3.2 Building the HCX Interconnect

The **HCX interconnect** term used here refers to the combination of HCX components and services abstracting complex operations across HCX connected sites as single end-to-end operations.

**Fig 3.2-1** The HCX Interconnect

3.2.1 Configuring a Remote HCX Site

HCX Enterprise Operations (Network Extension, Bulk migration, Cross-cloud vMotion Migrations, DR) are triggered from the HCX interface at the on-premises/source site. The operations is orchestrated and executed on both the HCX source the HCX-enabled target sites.

- A single HCX source site can be connected with one ore more HCX Cloud target sites.
- HCX service configurations are specific to the source/target site pair.

**Fig 3.2-2** An HCX Enterprise deployment with two remote sites registered
Procedure

1. In the vSphere Web Client, navigate to HCX > Interconnect > HCX Components > Install HCX Components
2. Existing Site connections are displayed.
3. In the top-right area of the Choose Hybrid Services UI, click Register new connection
4. The Remote Site Connection form is displayed.
5. Enter the HCX Cloud site URL, User Name and Passwords.

**Note:** https is required. When the FQDN is used, ensure HCX Enterprise Manager has a DNS server configured. If the remote HCX is entered with IP, the certificates must be imported manually. This is covered in a later step.
6. Click Register

### 3.2.2 Selecting HCX Services to Enable

After a site is registered successfully, the Choose Hybrid Services interface will launch and you will be able to select the HCX Services that will be used between the local and the newly registered Remote Site.

The Choose Hybrid Services interface can also be launched at a later time by in the HCX plugin.

Of the available services, the **HCX Interconnect Service** is always required, the WAN Optimization and Network Extension services are optional but highly recommended for the best end to end experience.

Procedure

1. In the vSphere Web Client, navigate to HCX > Interconnect > HCX Components > Install HCX Components
2. Existing Site connections are displayed. Select a single site.
3. Check all of the services that will be enabled.
4. Click Next

### 3.2.3 Configuring the HCX WAN Interconnect Component

The HCX Interconnect (HCX-WAN-IX) component provides migration and cross-cloud vmotion capabilities over the internet and private lines to the target site while providing strong encryption, traffic engineering and virtual machine mobility.

The HCX Interconnect Service (HCX-WAN-IX) appliance is always in the path for replication-based and vmotion-based operations. The Remote Site HCX Interconnect (HCX-WAN-IX) appliance is created automatically when a local appliance is deployed.

### HCX WAN Interconnect (CGW) Deployment Considerations

- The HCX WAN Interconnect service appliance should be deployed in a cluster where the HCX appliance will not be CPU/Memory resource constrained.

- It is recommended to have 100Mbit of WAN bandwidth available for the HCX WAN Interconnect’s migration services.

![HCX WAN Interconnect Connections](image)

**Fig 3.2-3** HCX WAN Interconnect Connections Summary

### Procedure

1. In the vSphere Web Client, navigate to HCX > Interconnect > HCX Components.
2. Click Install HCX Components. The Install HCX Components wizard is displayed
3. In the **Remote Site Connection > Select Connection** section, registered remote sites are displayed. Select a single site.

4. Check the HCX Interconnect Service, click Next
   Note: The service will be grayed out if the selected remote site is unavailable or deactivated, or if the service is already installed.

5. Populate the **HCX Interconnect Service** (IX) form for the local appliance deployment. Refer to the **HCX Deployment Checklist**, if completed during planning. The fields are explained below:

**Placement of local Hybrid Cloud Gateway**

a. **Network**  Select a distributed port group. The interface connected to the selected network will be used for management of the appliance, for HCX internal communications, and for the migration protocols. Selecting the ESX Management network is recommended.

b. **Cluster/Host**  Select a resource to deploy the service VM. Ensure the appliance is not resource constrained for maximum migration performance.

c. **Datastore**  Use flash/high performance tier datastore for maximum migration performance. HCX Interconnect disks are approximately 1.5GB.

d. **IP Address/Prefix Length**  Provide an available IP address and prefix length (e.g 255.255.255.128 = PL 25) for the network selected above.

e. **Default Gateway**  The network gateway IP address for the network specified above.

f. **DNS**  Provide the local DNS server IP address.

g. **vMotion Network**  Select the vMotion distributed portgroup. If the management network defined in step 1 is also used for vMotion, this can be left blank.

h. **vMotion IP Address/PL**  Provide an available IP address and prefix length (e.g 255.255.255.128 = PL 25) for the network selected above. Skip if 7 was left blank.

i. **Passwords**  Set the admin and root passwords.

6. Click **Next** and configure the other checked services, or proceed to the **Ready to Configure** screen.

7. Verify the Information and click **Finish**. Follow the vCenter tasks pane for appliance deployment progress.
3.2.4 Configuring the HCX WAN Optimization Component

The HCX WAN Optimization (HCX-WAN-OPT) service improves performance characteristics of the private lines or internet paths by leveraging WAN optimization techniques like data deduplication and compression. This makes performance closer to a LAN environment. It accelerates on-boarding to the cloud using Internet/VPN- without waiting for Direct Connect/MPLS circuits.

The HCX-WAN-OPT appliance is deployed “at-the-hip” of the HCX Interconnect. When deployed - the component is always in the path for virtual machine migrations.

HCX WAN Optimization Deployment Considerations

- The HCX WAN Optimization service appliance should be deployed to the compute zone, or network services cluster (or in a cluster where the HCX appliance will not be CPU/Memory resource constrained.

- The HCX WAN Optimization service appliance should be deployed in performance tier storage to ensure deduplication and WAN conditioning services operate optimally.

The HCX WAN Optimization appliance does not need an IP address; HCX will use an internal addressing configuration & network to service chain the WAN-OPT

Fig 3.2-4 HCX Service Chained WAN Optimization
**Procedure**

1. In the vSphere Web Client, navigate to **HCX > Interconnect > HCX Components**.
2. Click **Install HCX Components**. The Install HCX Components wizard is displayed.
3. In the **Remote Site Connection > Select Connection** section, registered remote sites are displayed. Select a single site.
4. Select the **WAN Optimization** checkbox, click **Next**.
5. The HCX WAN Optimization service appliance is also an enterprise-grade traffic shaper. Configure the setting only if there is a need to restrict the bandwidth available for HCX.
6. Click **Next** and configure the other checked services, or proceed to the **Ready to Configure** screen.

**3.2.5 Configuring the HCX Network Extension Component**

HCX Network Extension (HCX-NET-EXT) provides a High Performance (4-6Gbps) Layer 2 extension capability.
- Use Extension with Migration to keep Virtual Machine IP and MAC addresses during migration.
- Extend VLANS from VMware’s vSphere Distributed Switch.
- Extend VXLANs (Requires NSX integration in the HCX Appliance Management interface)
- Extend Cisco’s Nexus 1000v networks

Deploying the Network Extension Service appliance will allow networks to be extended in the vSphere Web Client. The **Remote HCX-NET-EXT** appliance is created automatically whenever a local appliance is deployed. The HCX-NET-EXT service appliance is always deployed as a pair.

**Scaling the HCX Extension Service**

A Single Network Extension Appliance for the HCX Source Site

If a single HCX-NET-EXT/L2E appliance is deployed, the ESXi host it resides on must be connected to every VDS for those networks to be displayed in the HCX interface.

One Network Extension Appliance per Site per Virtual Distributed Switch

The HCX-NET-EXT/L2E can be deployed per Distributed Switch to achieve isolation in environments where business zones are segregated by Distributed Switch.
One Network Extension Appliance per Extended Network
For high density environments with very high bandwidth network usage; the HCX-NET-EXT/L2E component can be deployed for each extended network, providing about 4-6 Gbps per extended network.

Fig 3.2-5 Network A Stretched with the HCX Network Extension Service

Procedure
1. In the vSphere Web Client, navigate to HCX > Interconnect > HCX Components.
2. Click Install HCX Components. The Install HCX Components wizard is displayed
3. In the Remote Site Connection > Select Connection section, registered remote sites are displayed. Select a single site.
4. Select the Network Extension Service checkbox, click Next
5. Populate the Network Extension Service form for the local appliance deployment. Refer to the HCX Deployment Checklist, if completed during planning. The fields are explained below:
   a. **Compute** Select a resource to deploy the service VM; please consider the Deployment Options implications when selecting the resource. See the Deployment Options section above for details.
   b. **Datastore** Select a datastore for deploying the Extension appliance. Network Extension appliance disks are about 1.5GB total.
   c. **Network** Select a distributed port group. The interface connected to the selected network will be used for management of the appliance and HCX internal communications with the HCX Manager.
   d. **VM Hostname** Specify a friendly name for the HCX Network Extension VM.
   e. **IP Address/Prefix Length** Provide an available IP address and prefix length (e.g. 255.255.255.128 = PL 25) for the network selected above.
f. **Default Gateway**  The network gateway IP address for the network specified above.

g. **Passwords**  Set the admin and root passwords.  Click **Next** and configure the other checked services, or to the **Ready to Configure** screen.

6. Click **Next** and configure the other checked services, or to the **Ready to Configure** screen.

7. Verify the Information and click **Finish**.

### 3.2.6 Verifying HCX Appliance Deployment Progress

The deployment of the HCX services appliances takes a few minutes to complete.  The vSphere Web Client and HCX interface can be used to track the status of deployments.

**Tracking HCX Deployment Progress In the vSphere Web Client**

1. In the vSphere Web Client, navigate to **Tasks**
2. Look for **HCX Service Initialization** in the Task Console

**Tracking HCX Deployment Progress In the HCX client**

1. In the vSphere Web Client, navigate to **HCX > Interconnect > HCX Components**.
2. The Status column will display the current step during the appliance deployment:
   - Queued for Deployment
   - Deployment In Progress
   - Deployment Complete
   - Reconfiguring Appliance

**Verify HCX Tunnel States**

1. In the vSphere Web Client, navigate to **HCX > Interconnect > HCX Components**.
2. Configuration has converged when the Tunnel column reads "**Active**" and "**Tunnel is Up**".
3.3 Managing a Configured HCX Interconnect

3.3.1 Editing a Registered Remote HCX Site
1. In the vSphere Web Client, navigate to HCX > Dashboard tab > locate the Site Pairings pane. Click > to expand the Site Pair that will be modified.
2. Click Edit Site Pairing.
3. Modify the URL, user or password settings.
4. Click Update to apply the changes.

3.3.2 Removing a Registered Remote HCX Site
1. In the vSphere Web Client, navigate to HCX > Dashboard tab > locate the Site Pairings pane. Click > to expand the Site Pair that will be removed.
2. Click Remove Site Pairing.
3. In the confirmation screen, click Remove

3.3.3 Removing HCX Appliances
1. In the vSphere Web Client, navigate to HCX > Interconnect > HCX Components.
2. In the Service Component column click the ► to display the expanded appliance view.
3. Click X Remove.
3.4 HCX Backup & Restore

3.4.1 About HCX Backup & Restore

The **HCX Enterprise Manager backups** can be initiated natively from the HCX Appliance Management Interface. The HCX system's configuration will be generated as a file that can be used to restore to a healthy system. The remote **HCX Cloud Manager** system (often managed by the infrastructure provider) can be backed up with the same mechanism.

**HCX Service Appliances don not require individual backups.** A restored HCX Manager will reconnect to existing service VMs that were created within the backup time frame, or if the service VMs are no longer functional, the manager can deploy VMs based on the backed up configuration.

3.4.2 HCX Backup

**Backup Requirements**

- A backup file of the HCX Manager system's configuration is generated in tar.gz format.
  - Hostname, IP, User Passwords
- Any configuration entered prior to restoring will be superseded by what is contained within the backup file.

**Procedure**

1. Log in to the HCX Appliance Management interface ([https://hcx-ip-or-fqdn:9443](https://hcx-ip-or-fqdn:9443))
2. Navigate to **Administration > Troubleshooting > Backup & Restore**
3. Click **Generate**. The system will create the backup file.
4. Click **Download**.
   - The backup (tar.gz) file will be downloaded to the client browsing system.
3.4.3 HCX Restore

The restore function can be used in cases where the HCX Manager system has become corrupt or unusable due to resource or system failures.

**Restore Requirements**

- A restore should only be performed on a clean deployed HCX system of the same version.
- A restored HCX Manager system cannot connect to HCX service appliances that were created during a time after the backup file was generated.
- A clean deployed HCX system requires only minimum deployment configuration to be manageable and network reachable from the Operator/client system.

**Procedure**

1. Log in to the HCX Appliance Management interface (https://hcx-ip-or-fqdn:9443)
2. Navigate to Administration > Troubleshooting > Backup & Restore
3. Within the Restore section, click Choose File. Select your HCXsystem-backup-date-time.tar.gz file.
4. Click Continue.
Chapter 4. Operating VMware HCX

4.1 Extending Networks with VMware HCX

4.1.1 About HCX Network Extension

HCX Network Extension (HCX-NET-EXT) is a High Performance (4-6Gbps) service that allows Virtual Machine networks to be extended to an HCX enabled remote site. Virtual Machines that are migrated or created on the extended segment at the remote site will be Layer 2 adjacent to virtual machines placed on the origin network. Network extension allows a remote site’s resources to be very quickly consumed. With Network Extension, the default gateway for the extended network only exists at the origin site. Traffic from Virtual Machines (on remote extended networks) that needs to be routed will returns to the origin site gateway.

Fig 4.1-1 Virtual Machine 192.168.10.20 is L2/ARP adjacent to Virtual Machine 192.168.10.21 in the Remote Site

- Using HCX Network Extension in conjunction with HCX Migration allows Virtual Machine to retain their IP and MAC addresses and allows existing network policies to be honored.
- Extend VLAN networks from VMware’s vSphere Distributed Switch.
- Extend VXLANs (Requires NSX integration at the origin site)
- Extend Cisco’s Nexus 1000v networks
- HCX deploys the Remote Site HCX-NET-EXT appliance automatically whenever a local appliance is deployed. The HCX-NET-EXT service appliance is always deployed as a pair.
4.1.2 Extending Networks from the vSphere Networking Context Menu

Procedure
1. In the vSphere Web Client, navigate to the Networking view.
2. Right click on a Distributed Portgroup.
3. Locate Hybridity Actions near the bottom of the menu.
4. Select Extend Networks to the Cloud.
5. The Extend Network to the Cloud HCX interface opens with the network selected.
6. In the top right, select the Edge from the drop down.
7. Select the Extension appliance in the Power by column.
8. Provide the Gateway IP and Prefix Length for the network being extended.
9. Extending the configuration displays optional DNS configuration. This should be left blank unless required by a vCD target cloud.
10. The PR switch enables Proximity Routing (covered in section 4.1.5, in detail).
11. Click Stretch to finish.

Note: The HCX enabled target site will have at least one NSX Edge Services Gateway deployed. The Gateway IP specified should duplicate the network's local gateway IP (this is very important when networks are migrated after the source/origin network is vacated).

4.1.3 Extending Networks from the HCX Interface

This approach allows multiple network extensions to be configured in a single operation. The interface will load all Distributed Switches connected to the HCX Network Extension services and all of the networks under each Distributed switch. Networks that were previously extended will be grayed out.

Procedure
1. In the vSphere Web Client, navigate to the HCX > Interconnect > Extended Networks.
2. Click Extend Network.
3. In the top right, select the Edge from the drop down (1).
4. Select each network that will be extended.
5. For each selected network:
   o Provide the Gateway IP and Prefix Length for the network being extended. (2)
   o Select the Extension appliance in the Power by column.

Extending the Gateway/PL configuration displays optional DNS configuration. This should be left blank unless required by a vCD target cloud (3).

6. Toggle the PR switch to enable Proximity Routing (covered in section 4.1.5, in detail).

7. Click Stretch to finish.

**Note:** The HCX enabled target site will have at least one NSX Edge Services Gateway deployed. The Gateway IP specified should duplicate the network's local gateway IP (this is very important when networks are migrated after the source/origin network is vacated).

### 4.1.4 Verifying Network Extension Operations

**In the HCX Interface**

1. In the vSphere Web Client, navigate to the **HCX > Interconnect > Extended Networks**.
2. Locate the **Status** column
3. The status will display **Extension Complete** when the operation finalizes.

**In vSphere Tasks Interface**

1. In the vSphere Web Client, navigate to **Tasks**
2. Look for Network Stretch V2 in the Tasks Console
3. The task will show **Completed** when the stretch operation finalizes.

**In the HCX Cloud Interface**

1. Open the HCX Cloud portal, and navigate to Services > Networking
2. Locate the extended network. The status will display **Success** when the extension operation finalizes.
4.1.5 HCX Network Extension with Proximity Routing

HCX Proximity Routing (HCX-PR) represents the progression of HCX Network Extension technology; HCX-PR optimizes connectivity to-and-from HCX migrated Virtual Machines by integrating HCX Network Extension and Migration state changes with the NSX Dynamic Routing configuration at the HCX-Enabled Cloud. HCX-PR allows extended VMs to route optimally on egress via the cloud side first hop gateway. By dynamically injecting VM routes into the routing protocols, ingress traffic from the local and remote datacenter will use an optimal (non-hairpinning/non-tromboning) path to reach the extended Virtual Machine, while ensuring all flows remain symmetric. The HCX-PR feature is toggled on during the HCX Network Extension operation, but it carries distinct requirements and results in enhanced traffic patterns, which are covered in this section.

Virtual Machine Reachability on Extended Networks without HCX-PR

- In figure 4.1.5-1 below, Network A has been extended without enabling HCX-PR. VM-B has been migrated.
- Reaching VM-B:
  - Traffic sourcing from VM-A in Datacenter A traverses Local HCX-NET-EXT and Remote HCX-NET-EXT to reach VM-B in Datacenter B, and vice-versa for VM-B to VM-A traffic.
  - Traffic sourcing from Network B, Network C or any other network, must first travel to the Network A gateway in Datacenter A, then traverses Local HCX-NET-EXT and Remote HCX-NET-EXT to reach VM-B in Datacenter B.
  - Traffic sourcing from VM-B to Network B, Network C or any other network, must first travel to the Network A gateway to be routed to its destination.

Fig 4.1-2 Network A is Extended from Datacenter A to Datacenter B
Virtual Machine Reachability on Extended Network with HCX-PR Enabled

- In figure 4.1.5-2 below, Network A has been extended with HCX-PR enabled. VM-B has been migrated and rebooted (in a pre-reboot state, the VM will use the on-premises gateway).
- Reaching VM-B:
  - Traffic sourcing from VM-A in Datacenter A traverses Local HCX-NET-EXT and Remote HCX-NET-EXT to reach VM-B in Datacenter B, and vice-versa for VM-B to VM-A traffic.
  - Traffic sourcing from Network B and other Datacenter A networks will traverse the Local First Hop Gateway and route to VM-B the Cloud Site NSX Router.
  - Traffic sourcing from Network C or other cloud side networks will route to VM-B locally within Datacenter B.
  - Traffic sourcing from VM-B destined to Network B, Network C or any other network, will route locally via the Cloud Site's NSX Router.

Fig 4.1-3 Network A is Extended from Datacenter A to Datacenter B with Proximity Routing Enabled

Requirements for HCX Proximity Routing

Dynamic Routing Requirements

The HCX Enterprise site must be configured to learn routes from the HCX Cloud target site, meaning that a dynamic routing protocol like BGP or OSPF must be configured between the two HCX sites.

The HCX-enabled Cloud target site must be running current NSX releases. NSX 6.2.x and older...
are not able to accept/learn of host routes injected by HCX.

Procedure (Without DLR)
1. Ensure the HCX target site is peered or has neighbor adjacencies with the on-premises HCX site.
2. Extend Networks with Proximity Routing enabled.
3. Migrate VMs to a network with HCX-PR enabled.
4. After reboot, the VM will use the local router and HCX route injection will take place.

Procedure (With DLR)
1. Ensure the HCX target site is peered or has neighbor adjacencies with the on-premises HCX site.
2. On the target site Edge Services Gateway:
   - add the Cloud Site DLR as a Neighbor/Peer.
   - Configure Redistribution of Static routes.
3. On the Cloud Site NSX DLR:
   - Add the Cloud Site NSX Edge as a Neighbor/Peer
   - Add the following Filters (in this specific order):
     1. Deny Out Extended/Stretch Network Prefix Lists (subnets of stretched networks)
     2. Permit Out Any Connected (this advertises native/non-stretched vm networks.)
     3. Deny Any In (DLR should be configured to reach the ESG via its default route).
4.1.6 Removing a Network Extension

Network Extension and Migration Progression without Proximity Routing
(Example scenario with a source site VM network that is being evacuated)

1. The on-premises/origin site’s VM network is extended to an HCX-enabled target site.
   1. The extended network’s gateway remains at the origin unchanged.
2. The workloads are migrated to the new extended on the target site in waves, until
   the source network is vacated.
   1. During the migration phase, network traffic from VMs on the extended network (at the target site)
      always returns to the network origin’s gateway to reach targets that are not in the extended
      network. This becomes less optimal as the VM location ratio prefers the target site.

When the source network is fully evacuated the Network Gateway Swing Over takes
4.2 Migrating Virtual Machines with VMware HCX

HCX enables bi-directional virtual machine mobility. Virtual Machines can be migrated to/from an HCX-enabled target site. The migration capability for both live (Powered-on) and cold (Powered-off) virtual machines. For Live VMs HCX offers two Migrations options.

**HCX Bulk Migration**

Replication-based low-downtime migration option for powered-on Virtual Machines; recommended for simultaneous migration of dozens of virtual machines.

**HCX Cross-Cloud vMotion**

vMotion-protocols based zero-downtime migration option. Cold and Hot Virtual Machine migrations. Recommended for critical workloads that have low downtime tolerance.

![HCX Interconnect Appliance Connections](image)

**Fig 4.2-1 HCX Interconnect Appliance Connections**

### 4.2.1 About HCX Bulk Migration

Bulk migration uses host-based replication to move a live virtual machine to and from HCX-enabled Cloud sites or datacenters.

To reduce downtime, the source VM remains online during the replication and is bootstrapped on the destination ESX host after replication completes.
**Bulk Migration Sequence:**

1. Replication begins a full synchronization transfer to the remote site. The time it takes to replicate is a function of the size of the VM and available bandwidth.
2. Replication bandwidth consumption varies depending on how the workload changes blocks on the disk.
3. When full synchronization finishes, a delta synchronization occurs.
4. When the delta synchronization finishes, a switchover is triggered. You can start immediately or delay the switchover until a specific time using the scheduled migration option. By using the scheduled migration option, the switchover can occur during a maintenance window.
5. Following the switchover, the source VM is powered-off, and the migrated replica is powered-on. If for some reason the VM cannot power on, the new VM is powered off (or remains powered off) and the original is powered on. You must have sufficient resources to power on the VM.
6. HCX Manager renames the powered off original VM to avoid a naming conflict with the migrated VM. HCX Manager appends a binary timestamp to the original VM name. If you have not enabled “Retain MAC,” the migrated VM obtains a new MAC address.

The migration is done.
HCX copies the original VM to the “Migrated VMs” folder in the vSphere Templates view. You can recover a saved VM.

**Note:** There are 2 uses for these copies.
1. The copy would act as seed, in the event the VM on Site B needed to be protected on Site A.
2. Protect against VM corruption (due to external factors) during migration.

### 4.2.2 About HCX Cross-Cloud vMotion

**Hot Migration**

HCX Cross-cloud vMotion can transfers a live Virtual Machine from an HCX enabled vCenter to a HCX enabled Remote Site (or from the HCX-enabled target site towards the local site. The vMotion transfer captures the virtual machine’s active memory, its execution state, its IP address, and its MAC address. Migration duration is dependent on the connectivity (bandwidth available for HCX migration / Latency between the 2 sites).
4.2.3 About HCX Cold Migration

Cold Migration

HCX Cold migration uses the VMware Network File Copy (NFC) protocol to transfer a powered-off virtual machine. During a cold migration, the Virtual Machine IP address and MAC address is preserved. Virtual Like a hot migration, a cold migration must meet satisfy vMotion requirements.

Pre-Requisites for HCX Cross-Cloud vMotion

- HCX Interconnect tunnels must up/active.
- Cross-cloud vMotion requires 100 Mbps or above throughput capability.
- The virtual machine hardware version must be at least version 9 or higher.
- The underlying architecture, regardless of OS, must be x86.
- VMs with Raw Disk Mapping in compatibility mode (RDM-V) can be migrated.

HCX Cross-Cloud vMotion Restrictions

Virtual machines with the following attributes are not supported for migration.

- Disk size exceeds 2 TB.
- Shared VMDK files.
- Attached virtual media or ISOs.
- Virtual Machine Hardware Version 8 or below.
- Concurrent vMotion migrations can be configured up to the documented vSphere limits.

4.2.4 HCX Migration Options

The options below appear in checkboxes or dropdowns in the HCX migration interface, these options can be used to tailor the behaviors and conditions of the Virtual Machine before, or after the migration operation.

Force Power-off VM

By default, HCX will attempt to gracefully shutdown the Virtual Machine guest during the HCXBulk migration operation. If the OS interrupts the graceful shutdown, the migration operation will fail. Checking this option allows
HCX to force the power-off. This option is not available for vMotion migrations.

**Retain MAC**
This option allows a virtual machine to keep its current MAC address during HCX bulk migration operation, allowing communications to resume gracefully, and allows for MAC based security policies to be honored. This option is not available for vMotion migrations.

**Upgrade Virtual Hardware**
This option allows HCX to upgrade Virtual Machine Hardware to the latest supported version as part of the migration operation, making current Virtual Machine Hardware features immediately available to the migrated Virtual Machine.

**Upgrade VMware Tools**
This option allows HCX to upgrade VMware Tools to the latest supported version as part of the migration operation, making current VMware Tools features immediately available to bulk migrated Virtual Machine.

**Remove Snapshots**
This option allows HCX to consolidate snapshot files prior to migrating the Virtual Machine. If there are snapshots present, the option will be checked by default.

**Force Unmount ISO Images**
This option allows HCX to remove mounted ISO images prior to migrating the Virtual Machine.

**Select Destination Container**
This dropdown option is for selecting a compute container (cluster, host, resource pool) that the HCX migrated Virtual Machine will use at the target site.

**Select Destination Storage**
This dropdown option is for selecting a storage location that the HCX migrated Virtual Machine will use at the target site.

**Select Virtual Disk Format**
This dropdown option allows HCX to set the Virtual Disk Format that the migrated Virtual Machine will use at the target site.

**Select the Destination Network**
This dropdown option is for selecting the network that will be used to connect the HCX migrated Virtual Machine at the target site. If the Virtual Machine resides on a network that has been extended with HCX, that network will be pre-selected.
4.2.5 Migrating a Virtual Machine from the Context Menu

When HCX is installed, the capabilities are integrated into the vSphere Web Client. This is the ideal method for kicking off single Virtual Machine Forward Migrations. These can be initiated directly from the Virtual Machine context menu.

Procedure

1. In the vSphere Web Client, search for a virtual machine and select it, or select it directly in the VMs and Templates navigator tab.
2. Right click the virtual machine > Hybridity Actions > Migrate to the Cloud
3. The Migrate to the Cloud wizard is displayed. Select the desired migration options:
   - Force Power-off VM
   - Retain MAC
   - Upgrade Virtual Hardware
   - Upgrade VMware Tools
   - Remove Snapshots
   - Force unmount ISO Images
4. Select the Target Site Resources
   a. Select Destination Container
   b. Select Storage
   c. Select Virtual Disk Format
   d. Select the Destination Network
5. Set the Migration Info
   a. Select Migration Type (vMotion, Bulk Migration)
   b. If Bulk Migration was selected, a schedule can be set.
6. Click Next. HCX will perform a validation.
7. Click Finish to begin the Migration

---

2 Forward Migration refers to the HCX Migration of Virtual Machines from the Local Site to an HCX-Enabled Remote Site. The operation is initiated at the local site.
4.2.6 Migrating Virtual Machines from the HCX Interface

The HCX interface is used for configuring multiple migrations, or for configuring Reverse Migrations.

Procedure

1. In the vSphere Web Client, navigate to the HCX > Migration > Click Migrate Virtual Machines
2. The Migrate Virtual Machines to Remote Site wizard is displayed.
3. Select the desired migration options. Use the Default Options pane to make the options apply to all selected Virtual Machines.
   Note: each of the options is explained in section 4.2.3 of this manual.
   - Force Power-off VM
   - Retain MAC
   - Upgrade Virtual Hardware
   - Upgrade VMware Tools
   - Remove Snapshots
   - Force unmount ISO Images
4. Select the Target Site Resources
   e. Select Destination Container
   f. Select Storage
   g. Select Virtual Disk Format
   h. Select the Destination Network
5. Set the Migration Info
   c. Select Migration Type (vMotion, Bulk Migration)
   d. If Bulk Migration was selected, a schedule can be set.
6. Click Next. HCX will perform a validation.
7. Click Finish to begin the Migration

---

Reverse Migration refers to the HCX Migration of Virtual Machines in HCX-Enabled Remote to the Local Site. The operation is initiated at the local site.
4.2.7 HCX Migration Status

After a migration operation is initiated; it will be displayed as an entry in the HCX UI > Migration tab - Status column. A healthy migration event will transition sequentially through the statuses detailed below, until the operation is complete.

Status Transitions During HCX Bulk Migration

- Queueing Migration
- Initiating Migration
- Validating Migration parameters
- Collecting source virtual machine details
- Creating placeholder disk(s) at destination
- Configuring replication
- Enabling replication on source virtual machine
- Replication in progress
- Initiating online sync
- Online sync in progress
- Powering off virtual machine
- Retrieve power status of virtual machine
- Monitor virtual machine power status
- Powering off virtual machine completed
- Initiating offline sync
- Offline sync in progress
- Instantiating virtual machine at target site to complete the migration
- Importing migrated virtual machine at the target site
- Virtual machine is migrated to the target site
- Unconfiguring replication
- Disabling replication on the source site
- Replication disabled
- Initiating rollback
- Rollback completed
- Archiving a timestamped copy of virtual machine image at source site (VMs migrated to cloud folder)
- Migration completed
In case of scheduled migrations:

- Waiting for schedule failover window to start
4.3 Protecting Virtual Machines with VMware HCX

4.3.1 About HCX Disaster Recovery

HCX Disaster Recovery is a service intended to protect virtual workloads managed by VMware vSphere that are either deployed in a private or a public cloud. It is simple to set-up, manage, and costs less than the traditional disaster recovery solutions. HCX Disaster Recovery can accommodate the most demanding business critical applications and allows you to scale your protection capacity to meet variable demands. This user guide addresses configuration, setup, and management aspects of HCX Disaster Recovery.

HCX Disaster Recovery provides the following benefits:

- Simple and easy to use management platform that allows secure (enterprise to cloud and cloud to cloud) asynchronous replication and recovery of virtual machines.
- Introduces major efficiency gains over traditional business continuity and disaster recovery (BC/DR) practices.
- Allows for improved recovery point objective (RPO) and recovery time objective (RTO) policy compliance while reducing total cost of ownership (TCO).
  - Note: RPO is the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds your BC/DR maximum allowable threshold. Whereas, RTO is the duration of time and a service level within which data must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.
- Reverse failover of workflows to your source site.
- Self-service RPO settings from 5 minutes to 24 hours per virtual machine.
  - Note: RPO policy compliance is dependent on available bandwidth from the source site to the destination site.
- Multiple point in time recovery snapshots that allows you to recover back up to 24 previous replication point in time.
- Optimized replication throughput by usage of Wan Optimizer.
- Routing replication traffic through customer preferred direct connect network
- On-premises monitoring and management with the fully integrated vSphere Web Client.
- Access to VMware’s production-level support.
Pre-requisites

- Requires compute on secondary site
- Enabled Interconnect services through HCX
- HCX Disaster Recovery uses the IPsec tunnel established between sites as the data path for replications. For proper communication ensure that the KB Article 2087769 is adhered to.

4.3.2 Enabling DR Protection for a Virtual machine

Below is an example workflow to enable DR Protection for a VM. Screenshots are for illustrative purposes only.

1. Login to the local vSphere web client and go to the HCX services plug-in.
2. Go to the Disaster Recovery Tab and click on Protect VMs.
3. The protection configuration screen is presented. This screen is similar to the migration configuration screen. From the top -
   1. Replication Destination Site - When checked, this loads the VM Inventory for Site B. When unchecked (default) Site B's VM inventory is loaded.
   2. Remote Site - The 2 Sites that are paired and the current direction of Protection.
   3. Source Inventory
   4. Default Replication options - Global Setting Policy for all VMs within the DC or Cluster, Resource Pool or Host.
   5. VM replication -
      1. Enable Compression - Helps during the seeding process of the VM. Assists in the event of low throughput LAN/WAN connectivity.
      2. Enable Quiescence - Pauses the VM to ensure the most consistent copy of the VM is protected on Site B.
      3. Seed Virtual Machine - Used when a previous action created a copy of the VM, for e.g., a Bulk Migration of a VM.
      4. Specify Destination Container - Datacenter, Cluster or Resource Pool where the protected copy of the VM is going to live.
      5. Storage - Datastore on which the protected copy of the VM would live.
6. RPO – Recovery Point Objective for the VM. With HCX, it can go from 5 mins – 24 hours. The interval between synchs of the Source VM and the Protected VM.

7. Snapshots Interval – Interval between Snapshots. In the event that a ‘corrupted’ change was synched over to the protect site, this will provide an option to recover from an earlier point in time. This provides a Multiple Point in Time Recovery plan for the protected VM.

8. No. of Snapshots – Total no. of snapshots within the established snapshot interval.

9. Network Portgroup – Corresponding portgroup that the protected VM will be using. In the illustration used, the portgroup that the source vm is using has been stretched to Site B, thus its automatically populated.

4. Hitting Next does a validation of the configuration for protection.

5. Hit Finish.

6. This action causes the DR Dashboard to be brought up. Here progress can be monitored on the protection of the VM.

7. The dashboard now shows the VM being protected. Expanding on the dashboard -
   1. Local VMs – Reflect the total # of VMs on Site B that are protected. In the above illustration, it shows that 1 local VMs is being protected.
   2. Remote VMs – Reflects the total # of VMs on Site B that are being protected from other Sites.
   3. Activity – To monitor any ongoing Disaster Recovery related operations.
   4. Green Shield – DR protection is active.
   5. Yellow triangle – Protection has not been tested.
   6. In/Out – Direction of protection between local site and remote site.

8. Log on to Site B

9. Go to Services -> Disaster Recovery

10. The Protected VM is now shown here. As can be seen, the DR screen is similar to Site A. In the above illustration, it shows there is 1 VM being protected locally.

This is how a VM on Site A is protected on Site B using HCX

4.3.3 Recovering a Protected VM
Below is an example workflow to Recover DR Protection for a VM. Screenshots are for illustrative purposes only.

There are 2 Recovery Operations available to a Protected VM.

1. Test Recovery Operations
2. Recover Operations

4.3.4 Test Recovery Operations

Below is workflow for testing the recovery of the VM on Site B. The action of testing can be raised on either from Site A or Site B. In the illustrations below, we will test the recovery from Site A.

Procedure

- Login to the vSphere Web Client and access the HCX plugin.
- Go to the Disaster Recovery Tab.
- Select the VM and either expand on : or under Actions, click on Test Recovery.
- If the Protected VM is on a stretched network, an error similar to the illustration will show up. The option to use none is available for test recovery.
- Go forward by clicking on test.
- Testing will go progress forward.
- Once the testing completes, the yellow triangle changes to a certificate to show a test been completed. The solid yellow triangle shows that a test cleanup is needed.
- To Clean up, Click on Actions after selecting the VM and click on Test Cleanup.
- Hit cleanup on the next screen.
- The test has now been completely cleaned up. Notice the solid yellow triangle has disappeared.

4.3.5 Recover Operations

Below is workflow for testing the recovery of the VM on Site B. In the illustrations below, we will recover a protected VM on Site B.
1. Protected VM on Site A is unavailable due to a disaster.
2. Log onto HCX on Site B.
3. Under Services – Disaster Recovery, the status for the protected VM is now a red lightning bolt.
4. Expand on the : and click on Recover.
5. A similar screen to test is up. In the illustration above, the source VM’s was on a stretched portgroup, so to ensure the VM comes up and is able to communicate to other VMs that could be on the same network path, following the recommendation in blue is best.
6. This now kicks off the recovery process.
7. As the process completes, the VM is brought up on Site B.

This is how a Protected VM is tested using HCX.

4.3.6 HCX Disaster Recovery - Protect Operations for VMs

HCX provides various operations that provide more control and granularity in replication policies.

Available Operations are

1. Reverse - Once a disaster has occurred. Reverse helps make Site B the source site and Site A where the protected VM now lives.
2. Pause - Pause the current replication policy associated with the VM selected.
3. Resume - Pause the current replication policy associated with the VM selected.
4. Remove - Remove the current replication policy associated with the VM selected.
5. Sync Now - Out of bound sync of source VM to the protected VM.
Chapter 5. Updating HCX

This chapter describes how to plan and execute updates of HCX service components.

5.1 Planning for HCX Updates

5.1.1 HCX Update Considerations & Requirements

HCX updates with new features and security fixes are bundled, published and automatically delivered to the HCX Manager at the Enterprise/source and Cloud/target sides. The HCX team recommends applying the published updates to the HCX service components at all sites. When a new update is delivered a notification in the form of an orange banner will be visible in the HCX plug-in.

Before updating HCX make sure there are no active tasks such as migrations, HCX service installations or network stretches. During the HCX Manager update procedure, existing stretched networks and protected virtual machines are not affected.

HCX Updates should be installed on both sides, the Enterprise/source and the Cloud/target sides.

It is recommended that you take a snapshot of the HCX Managers prior to starting the update.
Updates to Multi-Site Topologies

- HCX Services operate across 2 or more connected sites. HCX Enterprise/source, Cloud/Target pairs must run compatible HCX software builds.
- Published HCX Updates include the pair of compatible builds in the release notes.
- HCX to HCX site topologies can be one-to-one, one-to-many, many-to-many. Whenever a site's HCX Manager update is planned - the connected sites should also be upgraded to ensure the compatible builds requirement is met.

Compatible Builds

- HCX updates will always include compatible builds
- Build numbers for updates are listed in the release notes.
- HCX requires compatible builds to be running at the source site (HCX Enterprise) and remote (HCX Cloud Sites).
- In one-to-many and many-to-many HCX topologies, care should be taken to ensure all HCX sites are upgraded during the same change event.

5.1.2 Release Notes

Release notes for new updates can be found in the System Updates section of the HCX Manager plug-in.

Procedure

1. In the vSphere Web client on the Enterprise/Source side, navigate to the HCX plug-in > Administration > System Updates
2. Under the Local HCX section right-click the available version 3.5.### and select Readme. This will display the release notes for the new update.

Fig 5.1-2 Locating the HCX Release Notes
3. Release Notes for the current HCX version are located in the Current Version column, simply click on the clipboard next to the current version.

5.1.3 Downloading the HCX Update Software

The HCX update file can be downloaded in preparation for update execution. Downloading (without updating) is a recommended option for large scale deployments with many HCX sites, or sites with strict change control requirements. This allows the download to be decoupled from the update execution.

The HCX Manager will download the required software from hybridity-depot.vmware.com

Procedure

In the vSphere Web Client, navigate to the HCX > Administration > System Updates. In the Local HCX section (If an update is available), click the dropdown arrow, choose the Download operation. After the Download operation completes, the standalone Update operation will become available.

Fig 5.1-3 Downloading the HCX Update file
<table>
<thead>
<tr>
<th>System Name</th>
<th>Available Versions</th>
<th>Status</th>
<th>System Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>d2pv1mgmt-nsa-cloud</td>
<td>V3.5.1.7992451</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Choose Operation

Download
5.2 Performing the HCX Update

The HCX updates can be summarized in three overall steps:

1. HCX Manager Update - Enterprise/Source side: no data plane interruption
2. HCX Manager Update - Cloud/Target side: no data plane interruption
3. HCX Services: data plane services briefly interrupted.

The first step upgrades the HCX Manager on the Enterprise/source side, followed by upgrading the Cloud/Target side HCX Manager. The last step is to update the HCX Services (HCX Interconnect, HCX Network Stretch, HCX WAN Optimizer).

During steps 1 and 2 there is no data plane interruption to the HCX services. The last step can be updated subsequently per your maintenance schedule as this will incur in a brief (seconds) service interruption while the services go through a fast reboot.

5.2.1 HCX Manager Update (Enterprise/Source)

Procedure

1. In the vSphere Web client on the Enterprise/Source side, navigate to the HCX plug-in > Administration > System Updates
2. Under the Local HCX section right-click the available version 3.5.X.XXXXXX and select Download and Upgrade. Note down the available version for later confirmation.

Fig 5.2-1 Download and Upgrade HCX Operation
3. Click OK to confirm you want to start the update. During this step there is no HCX data plane interruption. The status column will show the current state of the update, from downloading the update bundle, to extracting it. When the update has been extracted the HCX Manager will be rebooted. Please allow up to 5 minutes for the HCX Manager to fully initialize.

![System will start upgrading](image)

4. Depending on your browser, you may need to refresh your session. Once the HCX Manager is back up confirm the Current Version column shows the newly updated version.

### 5.2.2 HCX Manager Update (Cloud/Target)

**Procedure**

1. In the HCX Cloud page on the Cloud/Target side, navigate to Administration > System Updates
2. Under the Local HCX section right-click the available version 3.5.##### and select Download and Upgrade. Note down the available version for later confirmation.

![Image of HCX System Update](image)
3. Click OK to confirm you want to start the update. During this step there is no HCX data plane interruption. The status column will show the current state of the update, from downloading the update bundle, to extracting it. When the update has been extracted the HCX Manager will be rebooted.

![Fig 5.2-4 System Unavailable Notification - Update in progress](image)

4. Log back in to the VMware HCX Cloud page once the HCX Manager is back up. Confirm the Current Version column shows the newly updated version located in Administration > System Updates.

### 5.2.3 HCX Services Update

**Procedure**

The final step in the HCX update procedure is to redeploy the HCX services. This will ensure that the new update is pushed to the HCX Interconnect, Network Extension and WAN Optimizer.

During this time, data plane services are briefly interrupted while the services go through a quick reboot so it is recommended that this is done during a maintenance window. Existing network stretches and protected virtual machines will remain in place after the update is done.

1. Confirm both HCX Managers are running the new version.
2. In the vSphere Web client on the Enterprise/Source side, navigate to the HCX plug-in > Interconnect > HCX Components
3. Expand the Network Extension Service and click Redeploy.
4. Expand the Hybrid Interconnect and the WAN-OPT and redeploy both.
5. Use the vSphere Task Console to track the redeploy task for all 3 services. Once they are redeployed, wait a few minutes until the tunnels for the Network Extension service and the Hybrid Interconnect are back up / green.
### Figure 5.2-5 Redeploying the HCX Service Appliances

#### Network Extension Service
- **Appliance**: L2C_HIT
- **Distributed Switch**: EqSwitch
- **Extended Networks**: 10.255.255.0/24
- **Network**: d695f17-e844-222
- **Host/Cluster**: Resources
- **DataStore**: z_d9b5f1e5a92e9a08e01c550a8
- **Version**: 3.6.0-732598
- **Created**: 7 Jan 2017 21:11:47 Coordinated Universal Time
- **Last update**: 10 Jan 2018 00:54:19 Coordinated Universal Time

#### VM Migration Service
- **Appliance**: GATEWAY
- **Network**: d695f17-e844-222
- **Host/Cluster**: CLS
- **DataStore**: z_d9b5f1e5a92e9a08e01c550a8
- **Version**: 3.6.0-732636
- **Created**: 30 Aug 2017 19:47:25 Coordinated Universal Time
- **Last update**: 13 Jan 2018 14:31:38 Coordinated Universal Time

- **Appliance**: WANOPT
- **Max Bandwidth**: Mb/s
- **Network**: d695f17-e844-222
- **Host/Cluster**: CLS
- **DataStore**: z_d9b5f1e5a92e9a08e01c550a8
- **Version**: 3.6.0-732636
- **Created**: 30 Aug 2017 19:47:25 Coordinated Universal Time
- **Last update**: 10 Jan 2018 00:57:34 Coordinated Universal Time
Chapter 6. Troubleshooting HCX

This chapter covers troubleshooting basics as well as some of the more common issues observed when installing and using HCX.

6.1 HCX Troubleshooting Basics

6.1.1 Enabling SSH on the HCX Manager

It is important to know how to gain access to the HCX Manager and its services. This can be done via a VMware Remote Console session using vSphere or by establishing an SSH session. For this you will have to first enable SSH on the HCX Manager if this was not enabled during the initial HCX Manager installation.

Procedure

1. Log in to the HCX Appliance Management interface
2. Go to Appliance Summary
3. Under System Level Services locate the SSH Service
4. Click Start

6.1.2 Logging in to the HCX Manager CLI

When logging in to the HCX Manager command line interface, either via VMRC or an SSH session, the first level access is with the admin account created during the initial installation of
the HCX Manager. Once you log in with the admin account you are able to switch the user to root if requested to do so by support.

**Procedure**

1. VMRC or SSH to the HCX Manager, at the `login as` prompt type `admin` and provide the password.
2. If required you can switch to root by typing `su -` and providing the root password.

### 6.1.3 Locating the HCX System IDs

When working with support you may be asked to provide the HCX System IDs. These can be obtained from the HCX plug-in as well as from the HCX Manager CLI.

**Procedure Using HCX Manager CLI**

This procedure only allows you to obtain the local HCX System ID.

1. VMRC or SSH into the HCX Manager
2. Switch user to root: `su -`
3. Type `cat /common/location`
4. Note the System ID

```
[root@usphcxmgr01 ~]# cat /common/location
20180214233611705-9242afbe-985a-44b0-b282-49f381ae0e2
[root@usphcxmgr01 ~]# 
```
Procedure Using HCX plug-in

1. In the vSphere Web Client, navigate to the HCX plug-in > Administration > System Updates
2. Under Local HCX, in the Info column click on the i information icon, this will copy the System ID to your clipboard. Do the same to obtain the Remote HCX System ID.
3. Note these down and provide them to VMware when requested.

6.1.4 Enabling Central CLI

The Central CLI on HCX allows you to run commands available centrally on the HCX Manager to query all your HCX services, including the HCX Interconnect and Network Extension Service. This reduces troubleshooting time from a central location. To use it you first need to enable the Central CLI on the HCX Manager.

Procedure

1. VMRC or SSH into the HCX Manager
2. Switch user to root: su -
3. Type ccli
4. CCLI is now enabled and you can issue commands such as help or connect to other HCX services
6.1.5 Using Central CLI to connect to HCX Services

From the HCX Manager Central CLI you can connect to the various HCX services for troubleshooting or gathering information.

**Procedure**

1. Enable CCLI on the HCX Manager: `ccli`
2. Type list to get a list of HCX nodes
3. Identify the HCX Node ID for the HCX service you want to connect to
4. Type `go #` where `#` is the node ID
5. Type `ssh`

![CLI Command Example]

6.1.6 Gathering HCX Technical Support Logs

Locating the HCX logs for review as well as knowing how to gather them is an important part of the troubleshooting process. It is very helpful to include at least the HCX Manager Technical Support log when experiencing an issue and reaching out to support.

**Procedure from the HCX Plug-in**

This procedure will allow you to generate the Core HCX Manager logs including a Heap Dump if one exists and the HCX Manager database. You can also include logs for the other HCX services.

Support will let you know which logs you need to include in the Technical Support log bundle.
1. In the vSphere Web Client, navigate to the HCX plug-in > Administration > Troubleshooting > Download Log Bundles
2. Check the box next to the log(s) that you want to generate
3. Click Request
4. When the bundle has been prepared you will be prompted to download them

Procedure from the HCX Appliance Management

5. Log in to the HCX Appliance Management interface
6. Navigate to Administration > Troubleshooting > Technical Support Logs
7. Check the box next to the log(s) that you want to generate
8. Click Generate
9. When the bundle has been prepared you will be prompted to download them
6.1.7 HCX Manager Logs in the Console

There are two key logs on the HCX Manager that can be reviewed and used when troubleshooting problems or to monitor system activities. Both are located in `/common/logs/admin` and they are the Application log (`app.log`) which logs all activities for the App-engine service and Web log (`web.log`) which logs all activities for the Web-engine service. This requires a good understanding of the HCX system so it is best to review along with a VMware support engineer.

Procedure

1. VMRC or SSH into the HCX Manager
2. Switch user to root: `su -`
3. Change directory to `/common/logs/admin`
4. From here you can tail the logs if monitoring the logs as you monitor an HCX job or you can use VI to review the logs.
5. When reviewing look out for any obvious errors. Some of the keywords to search for are: FAIL, ERROR, exception, migration
6.2 HCX Appliance Health

6.2.1 HCX Manager Services

The HCX Manager requires several key services to be running in order for HCX operations to function normally. There are several services that are required but the two most important ones which you should monitor and become familiar with are the App-engine and the Web-engine services.

When working with support you may be asked to confirm if these services are running or even to restart them. The HCX Manager Services are located and can be viewed and restarted in several places.

Do not restart services unless a support engineer request this to be done.

Procedure from the HCX Appliance Management Interface

1. Log in to the HCX Appliance Management interface
2. Navigate to Appliance Summary
3. From here you can find all services and have the ability to monitor or restart them. The only 2 services that are optional are the SNMP and SSH services, all others should always be running.
Procedure from the HCX CLI

1. VMRC or SSH into the HCX Manager
2. Switch user to root: su -
3. Type systemctl <action> <service name>
   a. action can be status, stop, start, restart
   b. service name: web-engine or app-engine

Example:
systemctl status web-engine
systemctl stop web-engine
systemctl restart web-engine

6.2.2 HCX System Resources

For HCX to run smoothly it is important that it has enough available resources in order to do its job. Key system resources such as CPU, Memory and Storage can be reviewed from the Dashboard section in the HCX Appliance Management Interface. Other useful information that can be found here are the version that the HCX Manager is running, the uptime, its IP address and current time. All useful information when reviewing logs or required by support.

Procedure

1. Log in to the HCX Appliance Management interface
2. Navigate to Dashboard
3. Review the CPU, Memory, Storage, Uptime, Version
6.2.3 HCX Operations in the vSphere Task Console

HCX operations like: initial appliance deployment, extending a network, or a migration can be monitored from the vSphere Web Client Task Console.

**Procedure**

1. In the vSphere Web Client, navigate to Home > Tasks
2. In the Task Console review the HCX operations. You can use the search function by typing hcx as a search term to only show HCX operations.
3. Look out for any failures or errors. If you do see an error you can review the logs to find additional details.
Appendices

Appendix I – HCX Network Ports

A high-resolution network diagram can be downloaded at hcx.vmware.com.

### HCX WAN Connections (HCX Components to Remote Targets)

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol/Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>HCX Enterprise Manager</td>
<td>connect.hcx.vmware.com</td>
<td>TCP-443</td>
<td>Activation, Updates</td>
</tr>
<tr>
<td></td>
<td>hybridity-depot.vmware.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HCX Enterprise Manager</td>
<td>HCX Cloud Manager</td>
<td>TCP-443</td>
<td>HCX Multisite Management</td>
</tr>
<tr>
<td>HCX-WAN-IX (CGW)</td>
<td>Remote HCX-WAN-IX (CGW)</td>
<td>UDP-500, UDP-4500</td>
<td>HCX WAN Transport Suite B Crypto; IKEv2</td>
</tr>
<tr>
<td>HCX-NET-EXT (L2C)</td>
<td>Remote HCX-NET-EXT (L2C)</td>
<td>UDP-500, UDP-4500</td>
<td>HCX WAN Transport Suite B Crypto; IKEv2</td>
</tr>
</tbody>
</table>

### HCX LAN Connections (Within the vSphere Datacenter)

Often these East-West intra-DC flows will not be firewall restricted. Use the table below the environment restricts intra-datacenter traffic.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol/Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>HCX Enterprise Manager</td>
<td>HCX-WAN-IX (CGW)</td>
<td>TCP-8123, TCP-443</td>
<td>HCX Bulk Migration Control, HCX Cross-Cloud Control</td>
</tr>
<tr>
<td>HCX Enterprise Manager</td>
<td>HCX-WAN-IX (CGW), HCX-NET-EXT (L2C)</td>
<td>TCP-9443</td>
<td>HCX Internal Control</td>
</tr>
<tr>
<td>HCX Enterprise Manager</td>
<td>vCenter</td>
<td>TCP-443, TCP-9443, TCP-7444</td>
<td>vSphere API, Web Client/Plugin (vSphere 5.5 SSO)</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>HCX Enterprise Manager</td>
<td>TCP-443</td>
<td>HCX HTTPS</td>
</tr>
<tr>
<td>HCX Enterprise Manager</td>
<td>ESXi Management IPs</td>
<td>TCP-80, TCP-902</td>
<td>OVH Import</td>
</tr>
<tr>
<td>Source</td>
<td>Destination</td>
<td>Protocol/Port</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>HCX Enterprise Manager</td>
<td>NSX Manager</td>
<td>TCP-443</td>
<td>NSX API (Only if integrating NSX for VXLAN Extension)</td>
</tr>
<tr>
<td>HCX-WAN-IX (CGW)</td>
<td>vCenter Server</td>
<td>UDP-902</td>
<td>HCX Cross-Cloud Control</td>
</tr>
<tr>
<td>HCX-WAN-IX (CGW)</td>
<td>ESXi Management IPs</td>
<td>TCP-80</td>
<td>ESX Authentication</td>
</tr>
<tr>
<td>HCX-WAN-IX ESXi Management IPs</td>
<td>ESXi Management IPs</td>
<td>TCP-902</td>
<td>HCX Cold Migration (Bi-directional)</td>
</tr>
<tr>
<td>HCX-WAN-IX ESXi-vMotion</td>
<td>ESXi-vMotion</td>
<td>TCP-8000</td>
<td>HCX Cross-Cloud vMotion</td>
</tr>
<tr>
<td>ESXi Management IPs</td>
<td>HCX-WAN-IX (CGW)</td>
<td>TCP-31031, TCP-44046</td>
<td>HCX Bulk Migration</td>
</tr>
<tr>
<td>HCX Operator</td>
<td>HCX Enterprise Manager</td>
<td>TCP-9443</td>
<td>HCX Appliance Management</td>
</tr>
</tbody>
</table>

**Enterprise Management Connections**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol/Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>HCX Enterprise Manager</td>
<td>DNS Server</td>
<td>TCP/UDP 53</td>
<td>Name Resolution</td>
</tr>
<tr>
<td>HCX Enterprise Manager</td>
<td>NTP Server</td>
<td>UDP-123</td>
<td>Synchronized Time</td>
</tr>
<tr>
<td>HCX Enterprise Manager</td>
<td>Central Syslog Collector</td>
<td>TCP/UDP 514</td>
<td>Centralized Syslog Collection</td>
</tr>
</tbody>
</table>