You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to
docfeedback@vmware.com
Contents

About the VMware HCX User Guide 7

1 VMware HCX Overview 8

2 VMware HCX Services 9

3 VMware HCX Components 11

4 VMware HCX Deployment Types 14

5 Preparing for HCX Installations 16
   System Requirements for HCX 16
   Software Version Requirements 17
   NSX Requirements for HCX Deployments 18
      NSX Requirements for HCX Appliance Deployments 18
      NSX Requirements for the HCX Connector Installation 19
   Network Port and Protocol Requirements 19
   Using the HCX Interface 20
   HCX Activation and Licensing 20
      Activating or Licensing New HCX Systems 20
      Updating an HCX Evaluation License Key 22
      Removing or Adding the HCX Enterprise Upgrade Key 23
   HCX Installation Workflow 24
      HCX Installation Workflow for HCX Public Clouds 24
      HCX Installation Workflow for vSphere Private Clouds 25
      HCX Installation Workflow for vCloud Director Private Clouds 25

6 Installing the System 27
   Downloading the HCX OVAs 27
      Downloading the HCX Cloud OVA 27
      Downloading HCX Connector OVA 28
   Deploying the Installer in the vSphere Client 28
   HCX Activation and Initial Configuration 29

7 Configuring and Managing the HCX Interconnect 32
   Overview of the HCX Interconnect Services Deployment with Multi-Site Service Mesh 32
   Configuring and Managing the HCX Interconnect with the Multi-Site Service Mesh 33
   About the HCX Multi-Site Service Mesh 33
Adding a Site Pair 36
Creating a Network Profile 38
Creating a Compute Profile 39
Creating a Service Mesh 46
Synchronizing the Multi-Site Service Mesh 48
Sentinel Management 49
  Downloading and Installing HCX Sentinel Agent Software 49
  Uninstalling HCX Sentinel Agent Software 50
  Upgrading HCX Sentinel Agent Software 51

8 Extending Networks with VMware HCX 53
  About VMware HCX Network Extension 53
  Requirements for Network Extension 54
  Requirements for Network Extension Using UDLR 55
  NSX Requirements in the Destination Environment for HCX Proximity Routing 55
  Importing Routers for Network Extension with NSX-V 55
  Extending Networks Using VMware HCX 56
  Removing a Network Extension 57
  HCX Proximity Routing with NSX for vSphere 58

9 Migrating Virtual Machines with VMware HCX 62
  VMware HCX Migration Types 62
  Understanding VMware HCX Bulk Migration 63
  Understanding VMware HCX vMotion and Cold Migration 65
  Understanding VMware HCX Replication Assisted vMotion 66
  Understanding VMware HCX OS Assisted Migration 68
  Migrating Virtual Machines with HCX 72
    Monitoring Migrations with HCX 73
    Canceling a Migration with HCX 74
  Migrating Virtual Machines with Mobility Groups 74
    Monitoring Migrations with Mobility Groups 76
    Managing Migrations with Mobility Groups 77
  Additional Migration Settings 78

10 Protecting Virtual Machines with VMware HCX 80
  VMware HCX Disaster Recovery 80
    Enabling DR Protection for a Virtual Machine 81
    Performing a Virtual Machine Test Recovery 83
    Performing a Virtual Machine Recovery 84
  VMware HCX Disaster Recovery - Protect Operations for VMs 84
  HCX Integration with Site Recovery Manager 84
15 Monitoring VMware HCX Systems  116
   Understanding the HCX Manager Dashboard  116
   vRealize Operations Management Pack for HCX  118
   Installing the HCX Management Pack  118
   Viewing the HCX Adapter Logs  119
   Management Pack for HCX Reference Topics  120
   DICE Integration for HCX  125

16 VMware HCX in the VMware Cloud on AWS  127
   Deploying HCX from the VMC Console  127
   Overview of VMware HCX on NSX for vSphere-Backed SDDCs  128
   Overview of VMware HCX on NSX-T Backed VMC SDDCs  130
   Configuring VMware HCX for Direct Connect Private Virtual Interfaces  132
About the VMware HCX User Guide

The VMware® HCX™ User Guide describes how to plan for, install, and operate VMware HCX services in a vSphere data center. The information includes step-by-step configuration instructions and operational procedures.

Intended Audience

This information is for anyone who wants to install, upgrade, or use VMware HCX. The information is for Windows or Linux system administrators who are familiar with virtual machine technology and data center operations.

VMware Technical Publications Glossary

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

VMware HCX is an application mobility platform that is designed for simplifying application migration, workload rebalancing, and business continuity across data centers and clouds.

VMware HCX enables:

- **Application migration**
  You can schedule and migrate thousands of vSphere virtual machines within and across data centers without requiring a reboot.

- **Change platforms or upgrade vSphere versions**
  With HCX, you can migrate workloads from vSphere 5.x and non-vSphere (KVM and Hyper-V) environments within and across data centers or clouds to current vSphere versions without requiring an upgrade.

- **Workload rebalancing**
  Workload rebalancing provides a mobility platform across cloud regions and cloud providers to allow customers to move applications and workloads at any time to meet scale, cost management, compliance, and vendor neutrality goals.

- **Business continuity and protection**
  Using HCX capabilities, administrators can protect workloads by replicating them to other HCX enabled sites. Workload migration is available on-demand, or it can be scheduled for business or maintenance planning.
VMware HCX Services

The HCX offers various services based on the type of license installed with the system.

The HCX is available with either an Advanced and Enterprise license. Advanced license services are standard with HCX and are included with the HCX Enterprise license.

<table>
<thead>
<tr>
<th>Advanced Services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interconnect</td>
<td>This service creates and secures connections between HCX installations, supporting management, migration, replication, and disaster recovery operations. This service is deployed as a virtual appliance.</td>
</tr>
<tr>
<td>WAN Optimization</td>
<td>The WAN Optimization service works with the HCX Interconnect service to improve the network performance through a combination of deduplication, compression, and line conditioning techniques. This service is deployed as a virtual appliance.</td>
</tr>
<tr>
<td>Network Extension</td>
<td>This service extends the Virtual Machine networks from an HCX-enabled source site to an HCX-enabled remote site. Virtual Machines that are migrated or created on the extended segment at the remote site are Layer 2 adjacent to virtual machines placed on the origin network. This service is deployed as a virtual appliance.</td>
</tr>
<tr>
<td>Bulk Migration</td>
<td>This service uses VMware vSphere Replication protocol to move virtual machines in parallel between HCX enabled sites.</td>
</tr>
<tr>
<td>vMotion Migration</td>
<td>This migration method uses the VMware vMotion protocol to move a single virtual machine between HCX enabled sites with no service interruption.</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>The HCX Disaster Recover service replicates and protects virtual machines to a remote data center.</td>
</tr>
<tr>
<td>Enterprise Services</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mobility Groups</td>
<td>This service supports assembling one or more virtual machines into logical sets for migration and monitoring as a group. Group migration provides the flexibility to manage migrations by application, network, or other aspects of your environment.</td>
</tr>
<tr>
<td>OS Assisted Migration</td>
<td>This migration service moves Linux- or Windows-based guest VMs from their host environment to a VMware vSphere enabled data center. This service comprises two appliances. The HCX Sentinel Gateway appliance is deployed the source site, and the HCX Sentinel Data Receiver appliance at the destination site. This service also requires the installation of HCX Sentinel software on each guest machine.</td>
</tr>
<tr>
<td>Replication Assisted vMotion (RAV)</td>
<td>This service uses both VMware Replication and vMotion technologies for large-scale, parallel migrations with no service interruption.</td>
</tr>
<tr>
<td>Site Recovery Manager (SRM) Integration</td>
<td>This service integrates HCX functionality with the VMware SRM for protection and recovery operations.</td>
</tr>
<tr>
<td>Traffic Engineering</td>
<td>VMware HCX provides settings for optimizing network traffic for HCX Interconnect and Network Extension services.</td>
</tr>
<tr>
<td></td>
<td>- The Application Path Resiliency service creates multiple tunnel flows, for both Interconnect and Network Extension traffic, those may follow multiple paths across the network infrastructure from the source to the destination data centers. The service then intelligently forwards traffic through the tunnel over the optimal path and dynamically switches between tunnels depending on traffic conditions.</td>
</tr>
<tr>
<td></td>
<td>- The TCP Flow Conditioning service adjusts the segment size during the TCP connection handshake between end points across the Network Extension. This optimizes the average packet size to reduce fragmentation and lower the overall packet rate.</td>
</tr>
</tbody>
</table>
VMware HCX Components

VMware HCX comprises a virtual management component at both the source and destination sites, and up to five types of VMware HCX Interconnect service appliances depending on the HCX license. VMware HCX services are configured and enabled at the source site, and then deployed as virtual appliances at the source site, with a peer appliance at the destination site.

HCX Connector and HCX Cloud Installations

In the HCX site-to-site architecture, there is notion of an HCX source and HCX destination environment. Depending on the environment, there is a specific HCX installer: HCX Connector (previously HCX Enterprise) or HCX Cloud. HCX Connector is always deployed as the source. HCX Cloud is typically deployed as the destination, but it can be used as the source in cloud-to-cloud deployments. In HCX-enabled public clouds, the cloud provider deploys HCX Cloud. The public cloud tenant deploys HCX Connector on-premises.

The source and destination sites are paired together for HCX operations.

**Note** An HCX Connector cannot be paired with another HCX Connector.

In both the source and destination environments, HCX is deployed to the management zone, next to each site's vCenter Server, which provides a single plane (HCX Manager) for administering VMware HCX. This HCX Manager provides a framework for deploying HCX service virtual machines across both the source and destination sites. VMware HCX administrators are authenticated, and each task authorized through the existing vSphere SSO identity sources. VMware HCX mobility, extension, protection actions can be initiated from the HCX User Interface or from within the vCenter Server Navigator screen's context menus.

In the NSX Data Center Enterprise Plus (HCX for Private to Private deployments), the tenant deploys both source and destination HCX Managers.
HCX-IX Interconnect Appliance

The HCX-IX service appliance provides replication and vMotion-based migration capabilities over the Internet and private lines to the destination site whereas providing strong encryption, traffic engineering, and virtual machine mobility.

HCX WAN Optimization Appliance

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

HCX Network Extension Virtual Appliance

The VMware HCX Network Extension service provides a late Performance (4–6 Gbps) Layer 2 extension capability. The extension service permits keeping the same IP and MAC addresses during a Virtual Machine migration. Network Extension with Proximity Routing provides the optimal ingress and egress connectivity for virtual machines at the destination site.
HCX Sentinel Gateway Appliance

Using VMware HCX OS Assisted Migration (OSAM), you can migrate guest (non-vSphere) virtual machines from on-premise data centers to the cloud. The OSAM service has several components: the HCX Sentinel software that is installed on each virtual machine to be migrated, a Sentinel Gateway (SGW) appliance for connecting and forwarding guest workloads in the source environment, and a Sentinel Data Receiver (SDR) in the destination environment.

HCX Sentinel Data Receiver Appliance

The HCX Sentinel Data Receiver (SDR) appliance works with the HCX Sentinel Gateway appliance to receive, manage, and monitor data replication operations at the destination environment.
VMware HCX Deployment Types

The HCX deployment type varies depending on the environments being connected.

HCX deployments use the following terminology:

**Software Defined Data Center (SDDC)**

Software Defined Data Center (SDDC) refers to an environment using current VMware software. An SDDC can refer to a private (on-premise) cloud or public cloud that meets the requirements of the HCX destination. The SDDC is typically the destination for HCX migrations and network extension. See Software Version Requirements.

**Legacy vSphere**

A legacy environment uses vSphere Version 5.0 or higher and optionally uses NSX. These environments typically contain the workloads to migrate and the networks to extend.

**Public Cloud**

An SDDC that is offered as a service by HCX-enabled public cloud providers. For example, VMware Cloud on AWS (VMC). A public cloud is typically the destination for migrations and network extension.

*Note*  VMC uses the term “SDDC” to describe a compute instance in the cloud.

HCX deployments fall into several types:
<table>
<thead>
<tr>
<th>Deployment</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy vSphere to SDDC</td>
<td>In this deployment type, the HCX Connector at the Legacy site initiates Site Pairing, and the Service Mesh appliances initiate the Interconnect tunnels. The HCX Cloud Manager and Service Mesh appliances at the SDDC site are the receivers.</td>
</tr>
<tr>
<td>Legacy vSphere to Public Cloud</td>
<td>In this deployment type, the HCX Connector at the Legacy site initiates Site Pairing, and the Service Mesh appliances initiate the Interconnect tunnels. The HCX Cloud Manager and Service Mesh appliances at the Public Cloud are the receivers.</td>
</tr>
<tr>
<td>Cloud-to-Cloud</td>
<td>In this deployment type, the HCX Manager at the SDDC or Public Cloud can initiate or receive Site Pairing requests and act as the initiator or receiver during the HCX Interconnect tunnel creation.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Cloud-to-cloud deployment is not available for VMware Cloud Director (vCD) and VMware Integrated OpenStack (VIO).</td>
</tr>
</tbody>
</table>

In any of these deployment types, HCX is functionally the same, and the same general workflow applies:

1. **Deploy HCX Manager at the legacy, SDDC, or Public Cloud sites**
2. **Create Network and Compute Profiles on both source and destination sites**
3. **Deploy the Interconnect Service Mesh on the source site**
4. **Initiate network extensions from the source site**
5. **Initiate HCX operations (migration, replication) from the source site**
6. **Configure the firewall access for ports and protocols for inbound and outbound HCX connections**
7. **Configure and license the HCX Manager appliance**
8. **Perform site pairing**
Preparing for HCX Installations

This section describes the system requirements, network ports, and protocols that must be allowed and various other requirements, like software versions and feature interoperability requirements.

This chapter includes the following topics:

- System Requirements for HCX
- Software Version Requirements
- NSX Requirements for HCX Deployments
- Network Port and Protocol Requirements
- Using the HCX Interface
- HCX Activation and Licensing
- HCX Installation Workflow

System Requirements for HCX

Before installing or deploying HCX, consider the required resources for both the source and destination environments.

Hardware Requirements for HCX Appliances

<table>
<thead>
<tr>
<th>Appliance</th>
<th>vCPU</th>
<th>Memory</th>
<th>Disk Space/IOPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>HCX Manager</td>
<td>4</td>
<td>12 GB</td>
<td>60 GB</td>
</tr>
<tr>
<td>HCX-IX</td>
<td>8</td>
<td>3 GB</td>
<td>2 GB</td>
</tr>
<tr>
<td>HCX-NE</td>
<td>8</td>
<td>3 GB</td>
<td>2 GB</td>
</tr>
<tr>
<td>HCX-WAN-OPT</td>
<td>8</td>
<td>14 GB</td>
<td>100 GB / 5000 IOPS</td>
</tr>
<tr>
<td>HCX-SGW (source only)</td>
<td>8</td>
<td>3 GB</td>
<td>10 GB</td>
</tr>
<tr>
<td>HCX-SDR (destination only)</td>
<td>8</td>
<td>3 GB</td>
<td>10 GB</td>
</tr>
</tbody>
</table>

Scaling the HCX Deployment

HCX Manager is deployed per vCenter Server.
The other HCX virtual appliances deploy per service mesh.

The network extension appliance (HCX-NE) has a one-to-one relationship to a distributed virtual switch (DVS).

**Software Version Requirements**

Infrastructure components must be running the required minimum version.

**Minimum Software Version Requirements for the HCX Installations**

*Note*  In cloud-to-cloud deployments, the destination requirements apply to all sites.

<table>
<thead>
<tr>
<th>Component Type</th>
<th>Source Environment Requirements</th>
<th>Destination Environment Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server</td>
<td>5.1 If using 5.5 U1 or earlier, use the standalone HCX User Interface for HCX operations.</td>
<td>6.0 U2 and above</td>
</tr>
<tr>
<td>ESXi</td>
<td>5.0</td>
<td>ESXi 6.0 and above</td>
</tr>
<tr>
<td>NSX</td>
<td>For HCX Network Extension of Logical Switches at the Source: NSXv 6.2+ or NSX-T 2.4+</td>
<td>NSXv 6.2+ or NSX-T 2.4+ For HCX Proximity Routing, NSXv 6.4+ (Proximity Routing not supported with NSX-T)</td>
</tr>
<tr>
<td>vCloud Director</td>
<td>Not required/Not applicable. There is no interoperability with vCloud Director at the source site.</td>
<td>When the destination environment is integrated with vCloud Director, the minimum is 9.1.0.2.</td>
</tr>
</tbody>
</table>

**Source Environment Version Requirements Listed by HCX Feature**

*Note*  Listed VMware HCX Interoperable versions must also meet VMware Product Interoperability Matrix compatibility requirements.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Source Site Component Version Requirements (see the preceding table for Destination Environment Requirements).</th>
</tr>
</thead>
</table>
| HCX Bulk Migration          | ■ vCenter Server 5.1 and above.  
                                 | ■ ESXi 5.0 and above. |
| HCX vMotion                 | ■ vCenter Server 5.5 and above.  
                                 | ■ ESXi 5.5 and above. |
| HCX Cold Migration          | ■ vCenter Server 5.5 and above.  
                                 | ■ ESXi 5.5 and above. |
| HCX Replication Assisted vMotion | ■ vCenter Server 5.1 and above.  
<pre><code>                                | ■ ESXi 5.1 and above. |
</code></pre>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Source Site Component Version Requirements (see the preceding table for Destination Environment Requirements).</th>
</tr>
</thead>
</table>
| HCX OS Assisted Migration (Guest VM supported OS versions on KVM Hypervisor). |  - RHEL 6.x (64-bit, 32-bit)  
- RHEL 7.x (64-bit)  
- CentOS 6.x (64-bit, 32-bit)  
- CentOS 7.x (64-bit)  
- Ubuntu 14.04 LTS (64-bit, 32-bit)  
- Ubuntu 16.04 LTS (64-bit, 32-bit)  
- Ubuntu 18.04 LTS (64-bit)  
- Windows Server 2012  
- Windows Server 2012 R2  
- Windows Server 2016  
- Windows Server 2008 R2 (64-bit)  
- Windows Server 2008 SP2 (64-bit, 32-bit) |
| HCX OS Assisted Migration (Guest VM supported OS versions on Hyper-V Hypervisor). |  - Windows Server 2012  
- Windows Server 2012 R2  
- Windows Server 2016  
- Windows Server 2008 R2 (64-bit)  
- Windows Server 2008 SP2 (64-bit, 32-bit) |
| Network Extension of vSphere Distributed Switch VM Networks |  - vCenter Server 5.1 and above.  
- ESXi 5.1 and above.  
- vSphere or third-party Distributed Switch must be installed. |
| Network Extension for NSX Logical Switches (overlay networks) |  - NSX for vSphere 6.2 and above or NSX-T 2.4+. |
| HCX Network Extension with Proximity Routing for NSXv |  - vCenter Server 5.1 and above with ESXi 5.1 and above.  
- vSphere Distributed Switch must be installed. |
| VMware HCX Network Extension of Cisco Nexus 1000v Networks |  - vCenter Server 5.0 and above. |
| VMware HCX Disaster Recovery |  - vCenter Server 5.1  
- ESXi 5.0 and above. |

**NSX Requirements for HCX Deployments**

In VMware HCX installations connecting private environments, NSX must be installed and configured before deploying HCX. This section details the requirements.

**NSX Requirements for HCX Appliance Deployments**

NSX must be installed and configured, including integration with the target vCenter Server, before deploying the HCX appliance.

- In the destination environment, NSX Manager must be installed and integrated with the target vCenter Server. Minimum supported NSX versions:
  - NSX for vSphere 6.2 and higher.
- NSX-T 2.4 and higher.
- An NSX Data Center Enterprise Plus license is required. This license is used to activate the HCX systems, and provides access to HCX Advanced features.
- The NSX Manager must be registered during the HCX install with the admin user.
  - If the NSX Manager IP or FQDN uses self-signed certificates, it may be necessary to trust the NSX system manually using the Import Cert by URL interface in the HCX Appliance Management interface.
- The HCX Deployment Cluster (selected during the Compute Profile creation) must be NSX Prepared:
  - NSX Data Center for vSphere - Preparing Clusters for NSX.
  - NSX-T Data Center - Host Preparation.
- NSX requires a Transport Zone capable of creating overlay networks:
  - NSX Data Center for vSphere - Add a Transport Zone.
  - NSX-T Data Center - Create Transport Zones.
- In multi-vCenter deployments using NSX for vSphere, where HCX is connected with primary and secondary NSX Managers, the secondary NSX Manager must have a local transport zone. Otherwise, HCX is not able to use the transport zone to deploy the Interconnect appliances.

**NSX Requirements for the HCX Connector Installation**

NSX is not required for HCX Connector installation, but requirements apply if NSX overlay networks are extended with HCX.

- For more information, see [NSX Requirements for HCX Appliance Deployments](#).

**Network Port and Protocol Requirements**

HCX deployments require setting various ports for communication between services on the HCX appliance itself and between HCX pairs at the source and destination sites.

The following ports must be allowed in HCX deployments:

- The source site firewalls must be configured to allow outbound connections to the destination HCX systems.
- The destination site firewalls must be configured to allow inbound connections from the source HCX system.
- Connections initiated from the source HCX to the destination HCX.
- Connections within a single HCX site, either at the source or destination environment. These connections never traverse from source to destination or from destination to source.
- Connections made when the HCX is added as a solution in a vRealize Operations installation.

For a complete list of network port and protocol requirements, see [VMware Ports and Protocols](#).
Using the HCX Interface

You access HCX services and appliances through one of several interfaces.

VMware HCX has the following user interfaces:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere Client</td>
<td>You can perform all operations related to HCX services from the HCX Plug-in in the vSphere Client. This interface is not available in vCD clouds.</td>
</tr>
<tr>
<td>HCX Manager UI</td>
<td>At both the source or destination site, you perform all operations related to HCX services by logging in to the HCX Manager at <a href="https://hcx-ip-or-fqdn:443">https://hcx-ip-or-fqdn:443</a>.</td>
</tr>
<tr>
<td>HCX Appliance Management</td>
<td>At both the source or destination site, you perform system management, licensing, and upgrade operations by logging in to the HCX Manager at <a href="https://hcx-ip-or-fqdn:9443">https://hcx-ip-or-fqdn:9443</a>.</td>
</tr>
<tr>
<td>Central CLI</td>
<td>You access the CCLI for debugging or troubleshooting HCX issues with VMware representatives. For access to the CCLI, see Logging in to the VMware HCX Manager Shell.</td>
</tr>
</tbody>
</table>

HCX Activation and Licensing

The HCX service features are available based on the installed license.

HCX licenses are available in two types: Advanced and Enterprise. The Advanced license is packaged with NSX Data Center Enterprise Plus, VMware Cloud on AWS, VCF Enterprise and from VMware Cloud Provider Partners. The HCX Enterprise license is available for purchase to NSX Enterprise Plus customers. For a list of services available with each license type, see Chapter 2 VMware HCX Services.

Activating or Licensing New HCX Systems

Activation requirements refer to any information required to activate a newly deployed HCX system.

HCX Activation Requirements

The HCX system must be activated before services like migration and extension can be triggered.

During the initial configuration of the HCX Manager, the wizard displays an activation screen:
### Requirement

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activating the system requires network access from the HCX Manager system</td>
<td>To test connectivity from the HCX Manager, use SSH to connect to the HCX Manager shell.</td>
</tr>
<tr>
<td>to <a href="https://connect.hcx.vmware.com">https://connect.hcx.vmware.com</a> and a valid activation key or license key.</td>
<td>curl -k -v <a href="https://connect.hcx.vmware.com">https://connect.hcx.vmware.com</a></td>
</tr>
<tr>
<td>Network access from the HCX Manager system to <a href="https://connect.hcx.vmware.com">https://connect.hcx.vmware.com</a></td>
<td>If there is a proxy server in the environment, the proxy server must be configured on the HCX Manager.</td>
</tr>
<tr>
<td>when there is a proxy for outbound HTTPS connections.</td>
<td>The proxy settings can be configured in the Administration interface. To resume the Initial Configuration Wizard, click the dashboard tab.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution</strong> By default, when you configure a proxy server, the system uses that server for all HTTPS connections, including the local vCenter Server, ESXi, NSX, and HCX-IX. For a successful deployment, define all related proxy exceptions when you configure a proxy server.</td>
</tr>
<tr>
<td>Activating HCX systems when using a private vSphere or vCloud Director as</td>
<td>Use NSX Data Center Enterprise Plus licenses from my.vmware.com. Enter this license when prompted for the <strong>HCX Advanced Key</strong>.</td>
</tr>
<tr>
<td>the destination environment.</td>
<td>NSX Data Center Enterprise Plus evaluation licenses may be used, but they must be updated to full keys for operations exceeding the trial limits.</td>
</tr>
</tbody>
</table>
## Activating HCX with VMware Cloud on AWS

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activating HCX with VMware Cloud on AWS.</td>
<td>Obtain the activation keys for the HCX system following the cloud provider's procedures. Enter this activation key when prompted for the <strong>HCX Advanced Key</strong>. Obtaining the activation keys for VMware HCX in VMware Cloud on AWS.</td>
</tr>
<tr>
<td></td>
<td>- Log in to console.cloud.vmware.com.</td>
</tr>
<tr>
<td></td>
<td>- Open VMware Hybrid Cloud Extension &gt; Activation Keys &gt; CREATE ACTIVATION KEYS.</td>
</tr>
<tr>
<td></td>
<td>- Create an HCX Cloud key for VMware Cloud on AWS SDDC.</td>
</tr>
<tr>
<td></td>
<td>- Create an HCX Enterprise key for the HCX on-premises system.</td>
</tr>
</tbody>
</table>

## Activate Later

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate Later</td>
<td>This option allows HCX activation to be temporarily skipped. To complete the installation while waiting for proxy or firewall allow additions, choose this option.</td>
</tr>
<tr>
<td></td>
<td>The activation keys can be entered in the Appliance Management Configuration interface.</td>
</tr>
</tbody>
</table>

## Grace Period

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grace Period</td>
<td>A small grace period allows the installation of HCX components. After the grace period expires, the system stops all associated services and operations. After the installation, the HCX systems must maintain an outbound connection to the central service URL, connect.hcx.vmware.com.</td>
</tr>
</tbody>
</table>

## Updating an HCX Evaluation License Key

You can update VMware HCX installations using evaluation or trial activation keys to use a standard HCX Advanced License key.

**Note**  This procedure is applicable to both the source and destination HCX systems activated with NSX Data Center Enterprise Plus trial licenses (or expiring licenses).

This procedure, however, does not apply for HCX systems connecting with a VMware HCX-enabled public cloud.

### Prerequisites

- Administrative access to the HCX system.
- NSX Data Center Enterprise Plus purchased license.

### Procedure

2. Navigate to the **Configuration** tab.
3. Select **License** on the side menu and click **Edit**.
4. Enter the new HCX Advanced license (NSX Enterprise Plus key), and click **UPDATE**.
Removing or Adding the HCX Enterprise Upgrade Key

You can update evaluation or trial activation keys to use a premium HCX Enterprise license, or if no license exists, you can add the HCX Enterprise license.

This procedure is applicable to both the source and destination HCX Manager systems.

Prerequisites

- Administrator access to the HCX Manager system.
- HCX Enterprise purchased license.

Procedure

2. Navigate to the Configuration tab.
3. Select License on the side menu and click Edit.
4. Remove or add the HCX Enterprise license key:
   - **Remove an HCX Enterprise license key:**
     1. Click REMOVE to remove the existing license key.
   - **Add an HCX Enterprise license key:**
     1. Enter the HCX Enterprise license, and click ADD.
HCX Installation Workflow

This section provides an overview of the HCX installation flow for supported installation scenarios.

HCX Installation Workflow for HCX Public Clouds

A sample public installation workflow using HCX on the VMware Cloud on AWS.

**Important** Follow the HCX installation procedures provided by your public cloud service.

This section provides an example procedure demonstrating how to use HCX with the VMware Cloud on AWS. Not all these steps must be repeated for each source and destination site pair:

- Steps 1—4, 8, 9 must be performed for each SDDC.
- Steps 5—7 are only required once for each source site.

An HCX Connector installation can pair with many VMC SDDCs when the Network Profiles are configured to support them.

1. Prepare the deployment configurations using Checklist B in Getting Started with VMware HCX.
2. Enable HCX in the VMware Cloud on AWS. See Deploying HCX from the VMC Console.
3. Use the VMC SDDC console to perform the following actions:
   - a. Note the HCX Cloud Manager and Interconnect EIPs. If configuring HCX to use AWS Direct Connect with a Private Virtual Interface, see Configuring VMware HCX for Direct Connect Private Virtual Interfaces.
   - b. Configure the VMC Firewall to allow the HCX Cloud manager to receive inbound TCP-443 connections.
   - c. Configure the VMC Firewall to allow the HCX Interconnect addresses to receive UDP-500 and UDP-4500 connections.

   See Network Port and Protocol Requirements for more details on the network port configuration details pertinent to Steps B and C.
4. Create HCX Activation Keys for the source site. See Activating or Licensing New HCX Systems.
5. Download the Enterprise Client for the source site. See Deploying HCX from the VMC Console.
6. Deploy HCX Manager in the source environment using the HCX Connector OVA. See Deploying the Installer in the vSphere Client.
7. Activate and Configure the HCX Connector system. See HCX Activation and Initial Configuration.
8. Pair HCX Connector with HCX Cloud. See Adding a New Site Pair.
   - If the HCX Cloud system is prepared using the Multi-Site Service Mesh, see Adding a Site Pair.
9. Enable HCX services to deploy the HCX Interconnect.
   - See Configuring and Managing the HCX Interconnect with the Components Interface.
If the HCX Cloud system is prepared using the Multi-Site Service Mesh, see Configuring and Managing the HCX Interconnect with the Multi-Site Service Mesh.

**HCX Installation Workflow for vSphere Private Clouds**

This topic summarizes a fully private HCX installation, where both the destination/modernized environment and the source/legacy environments must be considered.

1. Prepare the deployment configurations using Checklist A in Getting Started with VMware HCX.

2. Download the HCX Installer for the destination site first. See Downloading the HCX Cloud OVA.

3. Deploy HCX Manager in the destination environment using the HCX Cloud OVA. See Deploying the Installer in the vSphere Client.

4. Activate and Configure the HCX Cloud system. See HCX Activation and Initial Configuration.

5. Configure the Compute Profile on the HCX Cloud system, see: Configuring and Managing the HCX Interconnect with the Multi-Site Service Mesh.

   Compute Profiles are defined in both HCX Connector and HCX Cloud systems. Later in the workflow, the Multi-Site Service Mesh wizard is used to deploy HCX Interconnect services.

6. Deploy the HCX Manager in the source environment using the HCX Connector OVA. See Deploying the Installer in the vSphere Client.

7. Activate and Configure the HCX Connector system. See HCX Activation and Initial Configuration.

8. Pair HCX Connector with HCX Cloud. See Adding a Site Pair.

9. To deploy the HCX Interconnect, enable HCX services at the source site. See Configuring and Managing the HCX Interconnect with the Multi-Site Service Mesh.

**HCX Installation Workflow for vCloud Director Private Clouds**

This topic summarizes a fully private HCX installation, where both the destination/modernized environment and the source/legacy environments must be considered. In this workflow, the destination system is integrated with vCloud Director.

1. Prepare the deployment configurations using Checklist A in Getting Started with VMware HCX.

2. Download the HCX Installer for the destination site first. See Downloading the HCX Cloud OVA.

3. Deploy HCX Manager in the destination environment using the HCX Cloud OVA. See Deploying the Installer in the vSphere Client.

4. Activate and Configure the HCX Cloud system. See HCX Activation and Initial Configuration.

   During this step, select vCloud Director as the installation type and select the additional vCloud Director-specific details (for example, Public Access URL, AMQP).
5 Prepare the destination site’s HCX Cloud system for Interconnect Deployments using the Multi-Site Service Mesh, see: Configuring and Managing the HCX Interconnect with the Multi-Site Service Mesh. Define Compute and Network Profiles.

6 Deploy HCX Connector in the source environment using the HCX Connector OVA. See Deploying the Installer in the vSphere Client.

7 Activate and Configure the HCX Connector system. See HCX Activation and Initial Configuration.

8 Pair HCX Connector with HCX Cloud. See Adding a Site Pair. Note the vCloud Director-specific information when connecting a vCloud Director-based target site.

9 To deploy the HCX Interconnect, enable HCX services at the source site. See Configuring and Managing the HCX Interconnect with the Multi-Site Service Mesh.
Installing the System

This section describes how to install and activate the system.

This chapter includes the following topics:

- Downloading the HCX OVAs
- Deploying the Installer in the vSphere Client
- HCX Activation and Initial Configuration

Downloading the HCX OVAs

The HCX Installer is an OVA file used for deploying HCX in either or both of the source and destination vSphere environments.

Downloading the HCX Cloud OVA

The HCX Cloud OVA is used when deploying HCX in a private destination environment. In public cloud deployments, the HCX Cloud system may be deployed automatically by the cloud service provider.

Use this procedure to download the HCX Cloud OVA.

Procedure

2. Search for HCX.
3. Select VMware HCX.
4. Click Download Now.

Results

This installer updates itself to the most current service updates.

What to do next

Use the downloaded HCX Cloud OVA file to install HCX in the destination environment.
Downloading HCX Connector OVA

The HCX Connector OVA is used when deploying HCX at the source site.

Prerequisites

The HCX Cloud manager system must be installed and activated, and have SSO configured before downloading the HCX Connector OVA.

Procedure

1. Navigate to https://hcxcloudmgr-ip-or-fqdn.
2. Log in using the vSphere SSO user credentials (or vCloud Directory system administrator in VCD-integrated HCX Managers).
3. Navigate to the Administration tab.
4. Navigate to System Updates using the left-side menu.
5. Click Request Download Link.

What to do next

Use the downloaded HCX Connector OVA file to install HCX at the source environment.

Deploying the Installer in the vSphere Client

Deploying the installer OVA requires a standard OVA template installation through the vSphere Client.

Procedure

1. Connect to the vCenter Server client and deploy the OVF Template.
2. Browse and select the <filename>.ova file, and click Next.
3. Enter a virtual machine name and the inventory location, and click Next.
4. Select a compute resource location, and click Next.
5. Review the Deploy OVF Template Details and click Next.
6. Read and accept the VMware End User License Agreement, and click Next.
7. Select the virtual disk format, Storage Policy, storage name, and then click Next.
8. Select the Destination Network, and click Next.
9. Set the appropriate properties.
   - Passwords
     - Provide an admin password.
     - Provide a root password.
- **Network Properties**
  - Enter a host name for the HCX Manager virtual machine.

- **Static Route**
  - Optionally, provide the IPv4 Network, the Prefix Length, and Gateway IP address for any networks that cannot be accessed through the default gateway.

- **DNS**
  - Enter the DNS server. (Required)

- **Services Configuration**
  - NTP Server List (Required)

10. Click **Next**.

11. Review the deployment settings and click **Finish**.

**What to do next**

Allow up to 5 minutes for the HCX appliance to initialize, then browse to the appliance management interface for the initial configuration using **https://hcx-ip-or-fqdn:9443**. Proceed to "HCX Activation and Initial Configuration."

**HCX Activation and Initial Configuration**

After you have deployed HCX Manager, activate the system immediately when you next open the Appliance Management interface.

**Prerequisites**

- The HCX OVA deployment must complete fully before you begin. Allow up to five minutes after the HCX OVA deployment for the services to initialize.

**Procedure**

1. Browse to the HCX appliance management interface and authenticate using the admin user.

   Browse to **https://hcx-ip-or-fqdn:9443**.
2 Enter the Activation Key.

3 (Optional) If there is a proxy server in the environment in the path for outbound HTTPS connections, click Configure Proxy (Optional).

   If a proxy server is entered, add the local vCenter, ESXi, NSX, SSO, and HCX-IX systems as exceptions not to be sent to the proxy server.

4 Click Activate.

5 (Optional) Enter the HCX Enterprise License Key and click Add.

   You can skip this step and add the Enterprise License Key later.
6 Select the nearest major city to where the HCX Manager system is geographically located. HCX sites are represented visually in the Dashboard.

7 Click **Continue**.

8 Click **Yes** and continue to acknowledge a successful activation.

9 Enter the vCenter Server FQDN, user name, and password.

10 The NSX registration is mandatory for HCX Cloud and optional for HCX Connector.
   a Select **Connect your NSX**.
   b Enter the NSX Manager URL, NSX administrator account name, and the password for that account.

11 Click **Continue**.

12 Enter the SSO server details, user name, and password and then click **Continue**.
   The SSO URL must be entered exactly as displayed by the vCenter Server system.

13 Verify the information. To reinitialize the HCX services, click the **RESTART** item. VMware HCX requires up to five minutes to reinitialize the system completely, and during this process the Appliance Management interface is not available. After the HCX Manager system finishes the restart process, it displays the HCX Manager Dashboard.

14 Browse to the vSphere Role-Mapping section in the Configuration tab.

15 Assign the VMware HCX Roles to the vCenter User Groups that are allowed to perform VMware HCX operations. The groups assigned must have sufficient privileges to perform the VMware HCX-related operations in vCenter Server.

16 Click **Save**.

17 Log into the vSphere Web Client and look for the VMware HCX plugin in the Navigator.
   Log out first if an active session existed during the VMware HCX configuration.
The VMware HCX Interconnect provides a secure pipeline for migration, extension, and Virtual Machine protection between two connected VMware HCX sites.

This chapter includes the following topics:

- Overview of the HCX Interconnect Services Deployment with Multi-Site Service Mesh
- Configuring and Managing the HCX Interconnect with the Multi-Site Service Mesh
- Sentinel Management

Overview of the HCX Interconnect Services Deployment with Multi-Site Service Mesh

HCX services are deployed and managed using the Multi-Site Service Mesh.

The following steps use the Interconnect Multi-Site Service Mesh interface. Configuration preparation steps are symmetrical.

1. Site Pairing: Register the destination HCX system at the source.
2. Create a Compute Profile in the source and destination HCX environments.
3. Add the Service Mesh at the source:
   - Select a source and destination compute profile, and enable a Service Mesh.
Configuring and Managing the HCX Interconnect with the Multi-Site Service Mesh

The Multi-Site Service mesh is used to create a secure optimized transport fabric between any two sites managed by HCX.

About the HCX Multi-Site Service Mesh

When HCX Migration, Disaster recovery, Network Extension, and WAN Optimization services are enabled, HCX deploys Virtual Appliances in the source site and corresponding "peer" virtual appliances on the destination site. The Multi-Site Service Mesh enables the configuration, deployment, and serviceability of these Interconnect virtual appliance pairs.
Multi-Site Service Mesh Benefits

New Configuration Options:

- Uniformity: the same configuration patterns at the source and remote sites.
- Reusability: Once a compute profile is created, it can be used to connect to multiple HCX sites.
- Multisite ready: Compute Profiles and Network Profiles can be shared across multiple sites.
- Ease of reconfiguration: New capability to pool datastores or modify them after deploying an Interconnect network structure.
- Scale-out deployment: The HCX-IX can be deployed per cluster or a single HCX-IX can be shared across multiple clusters.

Performance Enhancements:

- Parallel execution ensures faster Interconnect deployments (in under 5 minutes).
- The new lockless model ensures parallel configuration of network stretches.

Usability Enhancements:

- Improved interfaces display a clear deployment diagrams.
- New task-tracking features provide incremental details for each step of the progress of operations.
- Preview of required firewall rules to avoid configuration difficulties.

Multi-Site Service Mesh Site Pairs

You register the destination HCX system in the Site Pairing Interface at the source site. Pairing the source and destination sites is a requirement for creating a Service Mesh.
Compute and Network Profiles

The compute profile defines the structure and operational details for the virtual appliances used in a Multi-Site Service Mesh deployment architecture. The compute profile:

- Provisions the infrastructure at the source and destination site.
- Provides the placement details (Resource Pool, Datastore) where the system places the virtual appliances.
- Defines the networks to which the virtual appliances connect.

The following conditions apply when deploying a service mesh network:

- The integrated compute profile creation wizard can be used to create the compute and network profiles (or Network Profiles can be pre-created).
- HCX Interconnect service appliances are not deployed until a service mesh is created.
Service Mesh

A Service Mesh specifies a local and remote Compute Profile pair. When a Service Mesh is created, the HCX Service appliances are deployed on both the source and destination sites and automatically configured by HCX to create the secure optimized transport fabric.

Sentinel Management

You must install HCX Sentinel on all guest virtual machines requiring migration using HCX OS Assisted Migration. Sentinel gathers the system configuration from the guest VM and assists with the data replication.

The source system information is used by various HCX OS Assisted Migration service processes. In part, the information is used to create an inventory of guest VM systems for migration and to help replication processes prepare the disks on the replica VM for replication and migration.

Sentinel also helps with the data replication by reading data written to the source disks and passing that data to the SDR appliance at the destination site.

Adding a Site Pair

A Site Pair establishes the connection needed for management, authentication, and orchestration of HCX services across a source and destination environment.

Prerequisites

- HCX Manager installed and configured in the source and destination environments.
- The Site URL and User:
  - When the destination is a private vSphere-based private cloud, the Site URL refers to the HCX Cloud Manager at the target site:
    https://hcx-cloud-ip-or-fqdn
Provide a user from the destination site's SSO configuration. The user must be included in the HCX Role-Mapping Group configuration.

The administrator@vsphere.local user is included by default.

- When the destination system is a Public Cloud, the Site URL may use a trusted domain name pre-created by the cloud provider.
  
  HCX for VMC SDDC uses the following Site URL format:
  
  https://hcx.sddc.*.vmwarevmc.com
  
  Use a cloud administrative account. For example, when registering a VMware Cloud on AWS SDDC, use the cloudadmin@vmc.local user.

- When registering a vCloud Director Organization as the HCX destination endpoint, the Site URL refers to the HCX Cloud system with a suffix referencing the Org:
  
  https://hcx-cloud-ip-or-fqdn/cloud/org/<orgname>
  
  Provide a Local or LDAP Organization User with the Organization Administrator role. Use the format username@orgname.

- The destination Site URL must use a CA signed trusted certificate or be manually trusted on the source HCX system. See Managing CA and Self Signed Certificates.

Procedure

1. From the HCX dashboard, go to Infrastructure > Site Pairs.
2. Click Add a Site Pairing.
3. Enter the Remote HCX URL and credentials, then click Connect.

Results

If all validations succeed, the system displays the remote site in the list as a connected site.

Example: Connected Site

What to do next

An Interconnect Service Mesh can only be enabled on connected Site Pairs.
Creating a Network Profile

The Network Profile is an abstraction of a Distributed Port group, Standard Port group, or NSX Logical Switch, and the Layer 3 properties of that network. A Network Profile is a subcomponent of a complete Compute Profile.

Create a Network Profile for each network you intend to use with the HCX services. The extension selects these network profiles when creating a Compute Profile and assigned one or more of four Network Profile functions:

- **Management Network:**
  The HCX Interconnect appliances use this network to communicate with management systems like the HCX Manager, vCenter Server, ESXi Management, NSX Manager, DNS, NTP.

- **Uplink Network:**
  The HCX Interconnect appliances use this network for WAN communications, like TX/RX of transport packets.

- **vMotion Network:**
  The HCX Interconnect appliances use this network for the traffic exclusive to vMotion protocol operations.

- **vSphere Replication Network:**
  The HCX Interconnect appliances use this network for the traffic exclusive to vSphere Replication.

**Caution** A Network Profile can be assigned any of the functions during the Compute Profile Configuration. Consider each role when planning each network profile.

**Prerequisites**

- The HCX Manager must be installed and configured.
- Use the planned network configurations prepared using the checklist described in Getting Started with VMware HCX.

**Procedure**

1. Navigate to the Network Profiles interface:
   a. In the vSphere Client, navigate To HCX > Interconnect > Multi-Site Service Mesh > Network Profiles.
   b. At the destination site, navigate to https://hcx-cloud-ip-or-fqdn > Multi-Site Service Mesh > Network Profiles.
2 Click Create Network Profile.

3 Select a vCenter Server and existing Network.
   a Select a vCenter Server from the drop-down menu.
   b Select Distributed Port Group, Standard Switch Port Group, or NSX Logical Switch to filter the available networks by type.
   c Select one of the available networks.

4 Name the Network Profile.

5 Provide the IP address details for the network profile.
   a Provide an IP address range available for the HCX appliances. Use a comma to separate multiple discontiguous ranges within the same subnet.
   b Enter the Prefix Length for the network containing the IP ranges provided.
   c Enter the Default Gateway Address for the network.

6 To complete the Network Profile configuration, click Create.

What to do next

Created Network Profiles are designated to one or more specific functions during a Compute Profile configuration, or when to override default Network Profiles when creating a Service Mesh.

Creating a Compute Profile

A Compute Profile contains the compute, storage, and network settings that HCX uses on this site to deploy the Interconnect-dedicated virtual appliances when a Service Mesh is added.

Create a Compute Profile in the Multi-Site Service Mesh interface in both the source and the destination HCX environments using the planned configuration options for each site, respectively.
Prerequisites

- The HCX Manager must be installed and configured.
- To obtain the optimum system usage, assign resource configurations based on HCX deployment considerations.
- Use the planned configurations collected using the checklist described in Getting Started with VMware HCX.

Procedure

1. Navigate to the Compute Profiles interface:
   a. At the source site, open vSphere Client and navigate to the HCX plugin > Interconnect > Multi-Site Service Mesh > Compute Profiles.
   b. At the destination site, navigate to https://hcx-cloud-ip-or-fqdn > Multi-Site Service Mesh > Compute Profiles.

   The system displays all the defined Compute Profiles. If no profiles have been configured, the system highlights the Create Compute Profile option.

2. Click Add Compute Profile.

3. Name the Compute Profile:
   a. Enter a name for the Compute Profile
   b. Click Continue.
4 Select the HCX services to be enabled. Click **Continue**.

**Note** Premium services require an additional HCX Enterprise license.

5 Select the Service Resources:
   a Click the **Select Resources** drop-down menu.
   b Select each cluster to be enabled for HCX services.
      If there is only one cluster, it is selected automatically.
   c Click **Continue**.

6 Select the Deployment Resource Pools:
   a Click the **Select Resource** drop-down menu.
   b Select each cluster or resource pool to be used when deploying HCX Interconnect appliances.
c  Click the **Select Datastore** drop-down menu.

d  Select the datastore to be used when deploying HCX Interconnect appliances.

When multiple compute resources or datastores are selected, HCX uses the first selection until its capacity is exhausted.

<table>
<thead>
<tr>
<th>Create Compute Profile</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
</table>

**Select Deployment Resources**

Select each compute and storage resource for deploying the HCX Interconnect appliances. When multiple resources are selected, HCX will use first resource selected until its capacity is exhausted.

7  **Select the Management Network Profile:**

a  Click the **Select Management Network Profile** drop-down menu.

b  Select an existing Network Profile or click **Create Network Profile** to create it.

Reference the [Creating a Network Profile](#) topic for more details.

c  Expand the selected Management Network Profile to view its details and free IP Addresses. Click **Close** when done reviewing.

d  Click **Continue**.

8  **Select the Uplink Network Profile:**

- The **Network Profile** previously selected for another function, like Management can also be assigned as the **Uplink Network Profile**.
Multiple Network Profiles can be selected.

a. Click the Select Uplink Network Profile drop-down menu.

b. Select one or more existing Network Profile, or click Create Network Profile to create it.

   Reference the Creating a Network Profile topic for more details.

c. Expand the selected Uplink Network Profile to view its details and free IP Addresses. Click Close when done reviewing.

d. Click Continue.

HCX Manager now updates the topology view to depict the configured Network Profile. As shown in the diagram, the Compute Profile configuration tool displays a symbolic map of the network links between the Interconnect appliance virtual machines to be deployed for the selected Uplink network.

Select the vMotion Network Profile:

a. Click the Select vMotion Network Profile drop-down menu.

b. Select an existing Network Profile or click Create Network Profile to create it.

   Reference the Creating a Network Profile topic for more details.

c. Expand the selected vMotion Network Profile to view its details and free IP Addresses. Click Close when done reviewing.

d. Click Continue.

The Network Profile tool now displays a topology view that shows how the selected vMotion Network connects the HCX Interconnect appliances assigned to the profile.
10 Select the vSphere Replication Network Profile:

Assigning a vSphere Replication Network Profile is useful when there is a VMkernel interface for the network traffic that is exclusive to vSphere Replication operations. If the Management Network Profile is used for Replication operations, click Continue to skip this step.

a Click the Select vSphere Replication Network Profile drop-down menu.

b Select an existing Network Profile or click Create Network Profile to create it.

Reference the Creating a Network Profile topic for more details.

c Expand the selected vSphere Replication Network Profile to view its details and free IP Addresses. Click Close when done reviewing.

d Click Continue.

11 Select Distributed Switches for Network Extension:

a Click the Select Distributed Switches for Network Extensions drop-down menu.

b Select the Distributed Switches with virtual machine networks. Click Close.

Only the virtual machine networks on the selected Distributed Switches may be used during network extension operations.

c Optionally use the Advanced Configurations to restrict the Network Extensions for the Distributed Switch.

d Click Continue.

The topology view is dynamically updated, depicting the selected Distributed Switches.
12 If HCX OS Assisted Migration is enabled, select the Guest Network Profile:

- This is the network on which guest virtual machines communicate with the HCX SGW for OS Assisted Migration.
- The **Network Profile** previously selected for another function, like Management can also be assigned as the **Guest Network Profile**.

**Note**  This step appears on only the source Compute Profile interface, and only if you have selected OS Assisted Migration from the list of available services.

a Click the Select Guest Network Profile drop-down menu.
b Select one or more existing **Network Profile**, or click Create Network Profile to create it.
Reference the Creating a Network Profile topic for more details.
c Expand the selected **Guest Network Profile** to view its details and free IP Addresses. Click Close when done reviewing.
d Click Continue.

13 If HCX OS Assisted Migration is enabled, select **Target Datastores**.

**Note**  This step appears only on the destination Compute Profile interface, and only if you have selected OS Assisted Migration from the list of available services.

a Click the Select Target Datastores drop-down menu.

b The menu contains a list of all the datastores present in the resource pool or cluster selected in Deployment cluster.
c Select the datastore and click **Continue**.

14 Pre-Deployment Validation:

HCX checks whether the selected configurations are valid for interconnect deployments.
a Address any errors reported by the validation.
b To see which firewall rules may be required if the service mesh uses this service profile, click Review Connection Rules.
c To export the rules, click COPY ALL to copy them to the clipboard in the JSON format.
d Click **Next**.

15 Ready to Complete:

a Review the configuration. The topology diagram depicts the selected configurations.
b To create the Compute Profile, click **Finish**.

**Results**

A Compute Profile is created, and can be used when creating a service mesh.
What to do next

Once there are valid Compute Profiles in the source and destination environments, use the HCX plug-in at the source site to create the Interconnect Service Mesh.

Creating a Service Mesh

An HCX Service Mesh is the effective HCX services configuration for a source and destination site. A Service Mesh can be added to a connected Site Pair that has a valid Compute Profile created on both of the sites.

Adding a Service Mesh initiates the deployment of HCX Interconnect virtual appliances on both of the sites. An interconnect Service Mesh is always created at the source site.

Prerequisites

Creating a Service Mesh requires:

- A connected Site Pair.
- A valid compute profile at the HCX Source site.
- A valid compute profile at the HCX destination site.

Procedure

1. Navigate to the Service Mesh interface:
   a. In the vSphere Client, navigate to HCX > Interconnect > Multi-Site Service Mesh > Service Mesh tab.

   Created Service Mesh configurations are listed.

2. Click Create Service Mesh:

3. Select Sites:
   a. Click each drop-down and select a source and destination site. Only connected Site Pairs are displayed.
   b. Click Continue.
Select Compute Profiles:

a. Click the **Select Source Compute Profile** drop-down and select a **Compute Profile**.
b. Click the **Select Remote Compute Profile** drop-down and select a **Compute Profile**.
c. Click **Continue**.

Select the HCX services to be enabled, and click **Continue**:

**Note** Premium services require an additional HCX Enterprise license.

6. **(Optional) Override the default Uplink Network Profile:**

   By default, the HCX interconnect uses the Uplink Network Profiles defined in the Compute Profile for the source and destination sites. You can override the default As an example, an override can be useful in vCloud Director-based deployments where an uplink network that deviates from a common configuration created for an Organization to consume during the Service Mesh creation.

   a. Click the **Select Source Uplink Network Profile** drop-down.
b. Select one or more networks. Click **Close**.
c. Click **Continue**.
d. Optionally, repeat these steps for the destination site.

7. **(Optional) Configure the Network Extension appliances deployed per switch:**

   As an example, this advanced configuration can be useful when deploying Network Extension appliances to extend high volume source networks.

   a. Click **Configure the Network Extension Appliance Scale**.
b. For each selected vSphere Distributed Switch, set the number of Network Extension appliances that HCX deploys when it enables a service mesh configuration. Click **OK**.
c. Click **Continue**.
8  (Optional) Configure HCX Traffic Engineering features:

   The Application Path Resiliency and TCP Flow Conditioning features are available with the HCX Enterprise license.

   a  To create multiple transport tunnels for directing the HCX traffic to a destination site, check Application Path Resiliency.

   Note  To view the available tunnels after completing the Multi-Site Service Mesh configuration, navigate to Interconnect > Multi-Site Service Mesh > Service Mesh > View Appliances and expand the HCX-WAN-IX appliance.

   b  To dynamically manage the TCP segment size and optimize the transport performance for the HCX Network Extension service traffic, check TCP Flow Conditioning.

   This option is available only after enabling the HCX Network Extension service.

   c  To manage the bandwidth consumed for migrations across all uplink networks, use the up and down arrows to change the bandwidth setting.

   This option is available only after enabling the HCX WAN Optimization service.

   Note  It is a best practice to retain the default setting of 10000 Mb/S.

9  Review Topology Preview:

   a  Review the selected clusters and resources.

   b  Click Continue.

10 Ready to Complete:

   a  To view a summary of the Service Mesh selections, click the here link.

   b  Name the Service Mesh.

   c  To create the service mesh, click Finish.

Synchronizing the Multi-Site Service Mesh

The Multi-Site Service Mesh is the effective HCX service configuration between a source and destination site and must be kept in synchronization between the pair.

Synchronizing the Multi-Site Service Mesh is necessary whenever there is an update to the Compute or Network configurations at either the HCX source or destination site.

Note  Synchronizing the Service Mesh is available from the HCX Manager where the Service Mesh was created.

Procedure

1  Log in to the HCX Manager at the source site: <https://hcxmgr-ip-or-fqdn>.

2  Go to Interconnect > Multi-Site Service Mesh > Service Mesh.
3  Click RESYNC.

4  Verify that the changes appear in the Compute Profile though the HCX Interconnect interface UI.

**Sentinel Management**

You must download and install HCX Sentinel on all guest virtual machines requiring migration using HCX OS Assisted Migration. Sentinel gathers the system configuration from the guest VM and assists with the data replication.

The guest VM information is used by various HCX OS Assisted Migration service processes. In part, the information is used to create an inventory of guest VM systems for migration and to help replication processes prepare the disks on the replica VM for replication and migration.

Sentinel also helps with the data replication by reading data written to the source disks and passing that data to the SDR appliance at the destination site.

The Sentinel Management tab, which provides access to downloading the Sentinel software, appears in the HCX Interconnect interface when an HCX Enterprise license is activated, and you have a deployed a service mesh with an SGW/SDR pair deployed. For more information about OS Assisted Migration, see Understanding VMware HCX OS Assisted Migration.

**Downloading and Installing HCX Sentinel Agent Software**

When performing migrations from non-vSphere virtual machines, you must install the HCX Sentinel on all guest virtual machines requiring migration using HCX OS Assisted Migration. The sentinel agent gathers the system configuration from the guest virtual machine and assists with the data replication.

**Prerequisites**

HCX Enterprise license is activated.

HCX OS Assisted Migration is enabled in Service Mesh.

**Procedure**

1  In the vCenter Server for the HCX Connector, navigate to Interconnect > Multi-Site Service Mesh > Sentinel Management.

2  Download the software bundle appropriate for the environment that you are migrating.

   The Sentinel software bundle is downloaded to the local machine with the name linux-sentinel-installer.sh or windows-sentinel-bundle.zip.

3  Install the Linux or Windows software on all guest VMs that require migration.

   a  Connect to your guest system using SSH.

   b  Copy the linux-sentinel-installer.sh file to the guest system.
At the terminal, enter the command `bash linux-sentinel-installer.sh`.

The software prompts you for permission to start the installation.

Enter `yes`, and press Enter.

- HCX Sentinel installation for Windows
  a Log in to the guest system.
  b Copy the `windows-sentinel-bundle.zip` file to the guest system.
  c Unzip the bundle.
  d To run the installer, double-click `install-sentinel.exe`.
  e Click Next to continue.
  f Accept the license agreement and click Next to continue.
  g Choose the location where you to install the software and click Next.
  h Click Finish.

### Uninstalling HCX Sentinel Agent Software

The HCX OS Assisted Migration (OSAM) service automatically uninstalls the Sentinel software from the guest system after a successful migration. Alternatively, you can manually remove the software using the Sentinel Management interface.

Following a successful migration, the OSAM service automatically sends instructions to the guest virtual machine to power off and uninstall the Sentinel agent software upon reboot. The OSAM service then removes the VM from the inventory of non-vSphere virtual machines on the HCX.

You can manually uninstall the software from a source VM using the Uninstall button in the Sentinel Management interface. The action taken by the OSAM service to uninstall the Sentinel software depends on whether the service has access to the source system:

- **OSAM service has a connection to the source VM**—OSAM uninstalls the Sentinel software from the source VM. Also, OSAM removes the source VM from the inventory of non-vSphere virtual machines on the HCX.

- **OSAM service has no connection to the source VM**—OSAM removes the source VM from the inventory of non-vSphere virtual machines on the HCX, but the Sentinel software remains installed on the source VM. In this case, if a connection to the source VM is reestablished with the OSAM service, the source VM reappears in the inventory of non-vSphere virtual machines on the HCX. To remove the Sentinel agent software and delete the source VM from the inventory, repeat the uninstall the procedure.

**Note** The OSAM service prevents you from uninstalling the HCX Sentinel software during the source VM migration.

To manually uninstall the Sentinel agent software, use the following procedure.
Procedure

1. Go to Interconnect > Multi-Site Service Mesh > Sentinel Management.
   The system displays the list of source VMs installed with the Sentinel agent software.

2. Select the source systems.

3. Click Uninstall.
   The system prompts you to verify the action.

4. Click Yes.
   The OSAM service begins the process of uninstalling the software from the source VM.

5. In the Sentinel Management interface, verify that the entry is removed from the inventory of non-vSphere virtual machines.

Upgrading HCX Sentinel Agent Software

To maintain compatibility with OS Assisted Migration (OSAM) service appliances, update HCX Sentinel agent software on guest virtual machines.

The OS Assisted Migration (OSAM) upgrade bundle includes the HCX Sentinel agent, Sentinel Gateway (SGW) appliance, and Sentinel Data Receiver (SDR) appliance software. This software is downloaded to the HCX only after you upgrade the HCX Manager. This means you must upgrade to the latest HCX software to get the latest OSAM updates.

The OSAM upgrade bundle has two versions depending on the HCX deployment: On-premise or Cloud. The Sentinel agent software is only downloaded with on-premise HCX deployment upgrades.

Prerequisites

The Sentinel Gateway and Sentinel Data Receiver appliances are updated to the latest version as described in Upgrading the HCX Service Mesh Appliances.

Procedure

1. Navigate to the HCX Dashboard, and select Interconnect > Multi-Site Service Mesh > Sentinel Management.
   The system displays the inventory of guest virtual machines. Each entry lists the current Sentinel software version and the available software version installed after upgrading the HCX Manager.

2. Select the guest VMs to update:
   It is a best practice to update all guest virtual machines to the same version at the same time.
   - To update all guest VMs, check the box at the top of the Hostname column.
   - To update individual VMs, check the box next to each VM.
3 Click **Upgrade**.

The upgrade begins for the selected guest VMs. For the upgrade status, review **Task Details**.

**Note**  Sentinel upgrade is allowed only when the migration is not in switchover phase for that guest virtual machine. An attempt to upgrade Sentinel on a guest virtual machine that has a switchover in progress results in an upgrade request failure.
The HCX Network Extension can be used to create bridged multi-gigabit network segments at the destination HCX data center. The new stretched network is automatically bridged/aggregated with the vSphere Network at the source HCX data center.

This chapter includes the following topics:

- About VMware HCX Network Extension
- Importing Routers for Network Extension with NSX-V
- Extending Networks Using VMware HCX
- Removing a Network Extension
- HCX Proximity Routing with NSX for vSphere

About VMware HCX Network Extension

You can bridge local network segments between HCX-enabled data centers with HCX Network Extension.

With VMware HCX Network Extension (HCX-NE), a High-Performance (4–6 Gbps) service, you can extend the Virtual Machine networks to a VMware HCX-enabled remote site. Virtual Machines that are migrated or created on the extended segment at the remote site are Layer 2 next to virtual machines placed on the origin network. Using Network Extension a remote site's resources can be quickly consumed. With Network Extension, the default gateway for the extended network only exists at the source site. Traffic from virtual machines (on remote extended networks) that must be routed returns to the source site gateway.

Using VMware HCX Network Extension with VMware HCX Migration you can:

- Retain the IP and MAC addresses of the Virtual Machine and honor the existing network policies.
- Extend VLAN networks from VMware’s vSphere Distributed Switch.
- Extend NSX overlay networks.
- Extend Cisco’s Nexus 1000v networks.
- VMware HCX deploys the Remote Site HCX-NE appliance automatically whenever a local appliance is deployed. The HCX-NE service appliance is always deployed as a pair.
Requirements for Network Extension

The HCX appliance supports extending networks from VMware’s vSphere Distributed Switch, third-party virtual switches, and NSX overlay networks.

The following information and requirements apply when extending networks:

- Requirements in deployments using NSX for vSphere at the destination:
  - Use a Distributed Logical Router (DLR) or Edge Services Gateway (ESG) to connect the extended network.
  - If a single Edge Services Gateway is used for more than 8 networks, use a trunk interface.

- Requirements in deployments using the NSX-T Data Center at the destination:
  - HCX connects to Tier-1 Gateways and Segments created in the Networking tab (simplified UI). NSX configurations created in the Advanced Networking & Security tab cannot be used with HCX Network Extension and Migration operations.
  - Additional network extension appliances may be required when extending more than 8 networks.

- Requirements when extending Virtual Distributed Switch networks:
  - To avoid creating a network loop, never extend the same VLAN to the same Target Site more than once. This misconfiguration is common in environments where distinct vSphere networks share a common VLAN ID backing.
  - vSphere Distributed Switch Version 5.1.0 or higher is required.

- Requirements when extending NSX-T networks:
  - The NSX-T Manager must be registered during the HCX Manager deployment.
  - The NSX-T Manager must be Version 2.4 or higher.
  - NSX-T Overlay or VLAN Transport Zones must be configured.

  **Note** The HCX Service Mesh deployment cluster must be deployed to an Overlay Transport Zone.

- Requirements when extending NS for vSphere Logical Switches:
  - The NSX-V Manager must be registered during the HCX Manager deployment.
  - The NSX-V Manager must be Version 6.2 or higher.

- Requirements when extending vSphere Standard Switch networks:
  - Not supported.

- General requirements:
  - Never extend the networks used to create the network profiles.
  - Never use HCX to extend the vSphere Management network or other VMkernel networks (for example: vMotion, vSAN, replication) to the remote site.
Requirements for Network Extension Using UDLR

The HCX appliance supports extending a network with a Universal Distributed Logical Router (UDLR) on the destination side. Extending the network using a UDLR creates a universal virtual wire on the destination side, which is present across multiple vCenters if NSX managers are connect and pair with multiple vCenters.

The following information and requirements apply for Network Extension when specifying a UDLR as the gateway.

- The HCX Manager configuration includes all secondary NSX systems as specified in Configuration > NSX. Each secondary NSX listed must have the administrative credentials of its associated vCenter Server.
- If proximity routing is enabled, the HCX automatically adds a static route in the UDLR and ESG for every migrated VM. After the static routes are added, the VM will be proximity routed and will use the destination side gateway for any egress traffic to other networks. If the static routes are not added, the VM is non-proximity routed and uses the source side gateway for any egress traffic to other networks.
  - For bulk migration, the static route will be added immediately after the migration.
  - For HCX vMotion, the static route will be added after the VM is power-cycled.
- The HCX does not support local egress for UDLRs.

NSX Requirements in the Destination Environment for HCX Proximity Routing

Network Extension with Proximity Routing ensures that forwarding between virtual machines connected to extended and routed networks, both on-premises and in the cloud, is symmetrical.

HCX Proximity Routing integrates with NSX in the destination environment and performs Host Route Injection for bulk migrated, and DR recovered virtual machines. When using Network Extension with proximity routing, the following information and requirements apply:

- NSX Data Center for vSphere version 6.4 or higher is required.
- NSX-T Data Center does not support the Proximity Routing feature.
- For proximity routing to work:
  - A dynamic routing protocol like BGP or OSPF must be configured between the source and destination gateway.
  - Configure the NSX router where network extensions are connected to advertise static routes.

Importing Routers for Network Extension with NSX-V

Extending networks to a destination site that is running NSX-V may require importing the NSX-V Edge router information if it is not present in the HCX Cloud Manager inventory.
Without the NSX-V Edge router information, network extension operations can fail.

**Note** When extending networks to an NSX-T supported destination, the Edge router information is imported automatically.

**Procedure**

1. Log in to the destination HCX Cloud Manager: <https://hcxcloudmgr-ip-or-fqdn>.
2. Go to Services > Networking and click Router.
3. Click IMPORT.
   
   A window appears for entering vCenter and NSX gateway information.
4. Using the pull-down menus, select the vCenter Server and gateway required for network extension.
5. Click OK.

**Extending Networks Using VMware HCX**

VMware HCX Network Extension can be initiated from either the vSphere Client Networking view or from the HCX User Interface.

If you are using the vSphere Client Networking view, you can select a single Distributed virtual Port Group and extend it.

If you are using the HCX user interface (stand alone or vSphere Client plug-in), you can extend networks by selecting one or more Distributed Port Groups or NSX Logical Switches in the HCX User Interface. When you extend a network, the corresponding NSX Logical Switch will be created at the destination site.

**Procedure**

1. If you are using the vSphere Client, follow these steps to extend a Distributed Port Group:
   a. From the vSphere menu, select Networking.
   b. Right-click a Distributed Port Group.
   c. Locate HCX Actions near the bottom of the list, and select Extend Networks to HCX Target Site.
      
      The Extend Network to HCX Target Site interface opens with the network selected.

2. If you are using the HCX user interface, follow these steps to extend one or more Distributed Port Groups:
   a. In the HCX dashboard, select Network Extension.
   b. At the top of the page, select Extend Network.
   c. Select one or more Distributed Port Groups or NSX Logical Switches.

3. Select the Remote Site Connection.

**Note** If you have only one site, it is selected by default.
4 At the top right, select an Edge Services Gateway (ESG), Distributed Logical Router (DLR), or Universal DLR (UDLR) from the Edge drop-down menu:
   a If you are extending a network to a single vCenter, select an ESG or DLR from the drop-down menu.
   b If you are extending a network for to multiple vCenters at the destination site and require a universal virtual wire to be created, select a UDLR from the drop-down menu.

5 Select the Extension appliance in the Power by column.

6 Provide the Gateway IP and Prefix Length for the network being extended in the format <gateway IP/Prefix Length>. For example: 192.168.10.1/24.
   For a vCD target cloud, you can click the extended option drop-down menu and optionally specify the DNS configuration.
   For a vCenter target cloud, leave the DNS information blank.

7 (Optional) To enable Proximity Routing, toggle the PR switch.

8 Click **Extend** to finish.

To view the task status, navigate to the HCX Dashboard and scroll down to the Activity Logs display.

### Removing a Network Extension

Unextending a network prevents further cross-site communications between virtual machines residing on that network. This operation is typical when the source side network is vacated.

**Procedure**

1 In the vSphere Web Client navigator, select **HCX**.

2 Navigate to the **NetworkExtension** tab. You can see a list of currently extended port groups.

3 Locate the network that must be unextended and expand the selection.

4 Click **Unstretch**.

   The Un-Extend Network interface opens. Review the information.

5 Optionally, select the **Connect cloud network to cloud edge gateway after unstretching** option to connect the remote side gateway. To view this selection, expand **Cloud Network column**.

   Using this option enables the gateway for the stretch network. Ideally, perform this operation after the stretched network has been fully evacuated from the source site. Not selecting this option results in a network segment at the target site that is not connected to a gateway for routing.

6 To confirm the operation, click **Unstretch**.
HCX Proximity Routing with NSX for vSphere

VMware HCX Proximity Routing optimizes connectivity for VMs that are migrated in and out of Proximity Routed Networks. Proximity Routing builds on VMware HCX Network Extension by integrating with NSX Routers at the VMware HCX Cloud destination site. By dynamically injecting Virtual Machine routes into the existing routed topology, proximity routed network traffic always traverses a symmetric path to the network target.

VMware HCX-PR allows extended VMs to route traffic optimally through the cloud-side, first-hop gateway. By dynamically injecting VM routes into the routing protocols, incoming traffic from the local and remote data centers use an optimal path to reach the extended Virtual Machine, while ensuring all flows remain symmetric. The Proximity Routing feature is toggled on during the VMware 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 Proximity Routing

- In the following figure, Network A has been extended without enabling Proximity Routing. Virtual Machine B has been migrated.

- Reaching Virtual Machine B:
  - Traffic sourcing from Virtual Machine A in data center A traverses Local HCX-NE and Remote HCX-NE to reach Virtual Machine B in data center B, and conversely for Virtual Machine B to Virtual Machine A.
  - Traffic sourcing from Network B, Network C, or any other network, must first travel to the Network A gateway in data center A. It then traverses Local HCX-NE and Remote HCX-NE to reach VM-B in data center 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.
VMware HCX Proximity Routing In Action

The following events take place when VMware HCX-PR is used, with VMware HCX Migrations.

Prerequisites

Requirements and Restrictions for HCX Proximity Routing

- Dynamic Routing
  - The HCX Connector site (on-premises data center) must be configured to learn routes from the VMware HCX target site dynamically. A routing protocol like BGP or OSPF must be configured between the two sites.
  - The VMware HCX-enabled Cloud target site must be running NSX 6.3GA+ (allows host routes to learn from the dynamic routing protocol).
- Private Lines/Direct Link/ Direct Connect Networks
  - Private lines are typically implemented as the transport for the Dynamic Routing configuration (if there is OSPF, to meet security requirements, and adjacency requirements).
- VMware HCX-Cloud Providers and Proximity Routing
  - VMware HCX is available for IBM Clouds, OVH Private Cloud, and the VMware Cloud on AWS (VMC). The IBM and OVH cloud services can be configured to meet all VMware HCX-PR requirements. If the Cloud is configured to use NSX Distributed Logical Router for virtual machine networking, there are additional requirements in the following section that must be met.
At the time, of this writing, the VMC cloud cannot be configured to meet the VMware HCX-PR requirements.

After all requirements are met, Proximity Routing can simply be enabled during the Network Extension operations.

Additional Configuration Requirements for VMware HCX Proximity Routing when NSX Distributed Logical Router (DLR or UDLR) is present.

- Dynamic Routing Between the Cloud Site Edge Gateway and the Cloud Site DLR
  - Cloud destination site NSX Edge Services Gateway Configuration
    - Enable BGP.
    - Add the Cloud Site DLR as a Neighbor.
    - Add the on-premises peer as a neighbor.
    - Configure Redistribution of Static routes.
  - Cloud destination site NSX DLR Configuration
    - Enable BGP.
    - Add the Cloud Site NSX Edge as a Neighbor.
    - Add BGP Filters (in this specific order):
      - Deny Out Network Extended/Stretch Prefix Lists.
      - Permit Out Any (this filter advertises native Virtual Machine networks).
      - Deny Any In (The NSX DLR must be configured to reach the ESG using its default route).

Procedure

1. VMware HCX Network Extension is triggered at the source site.
   - The extended subnet's details are provided, including the extended subnet's gateway IP. The system enables VMware HCX-PR for the extension.
   - Upon completion, a routed port group and isolated port group are created for the extended network, at the cloud site.
   - The VMware HCX Network Extension appliance becomes connected to both the routed and isolated extended port groups.
   - VMware HCX creates the extended subnet's gateway on the Cloud destination site DLR using the same IP as the on-premises gateway. ARP filters are applied to prevent the new gateway from being reached from the source site.
2 A Virtual Machine is migrated into the PR-Extended Network.

- A virtual machine is migrated to the extended network with VMware HCX Proxy vMotion placed into the ISO segment. The ARP table shows the on-premises gateway's MAC address, the VM continues sending routing requests to the on-premises gateway mac address.

**Note** VMware HCX handles virtual machine membership in the isolated "ISO" network as an internal configuration operation. Virtual machine membership in the ISO port groups is not reflected in the vCenter Network view.

- Whenever the vMotion VM is rebooted (at the administrator's discretion), VMware HCX connects the VM to the routed (non-ISO) version of the network. Post-reboot, the VM ARP table shows the Cloud Site DLR MAC address for its gateway and being routing locally, without hair-pinning.

**Note** Rewiring into the non-ISO/routed port group requires VM tools to be running and detecting the virtual machine's IP address.

- A Virtual Machine migrated to the extended network with VMware HCX Bulk Migration is placed directly on the non-ISO tagged/routed extended network. The ISO tagged isolated network is not used in this case.

**Results**

- VMware HCX Injected Routes
  - After the system places the virtual machine on the non-ISO/routed extended network, VMware HCX adds a /32 host route for the VM. The VM is then added to the destination site NSX Edge Gateway with the destination site DLR Uplink IP as the next hop.
  - Also, VMware HCX adds exclusion static routes covering every IP from the extended subnet that does not belong to migrated VMs to the destination site DLR. With the destination site NSX Edge Gateway Downlink IP as the next hop.
Migrating Virtual Machines with VMware HCX

Workloads can be migrated bi-directionally between data centers using various VMware HCX migration technologies.

This chapter includes the following topics:

- VMware HCX Migration Types
- Understanding VMware HCX Bulk Migration
- Understanding VMware HCX vMotion and Cold Migration
- Understanding VMware HCX Replication Assisted vMotion
- Understanding VMware HCX OS Assisted Migration
- Migrating Virtual Machines with HCX
- Migrating Virtual Machines with Mobility Groups
- Additional Migration Settings

**VMware HCX Migration Types**

Virtual Machines can be moved to and from VMware HCX-enabled data centers using multiple migration technologies.

**VMware HCX Bulk Migration**

This migration method uses the VMware vSphere Replication protocols to move the virtual machines to a destination site.

- The Bulk migration option is designed for moving virtual machines in parallel.
- This migration type can set to complete on a pre-defined schedule.
- The virtual machine runs at the source site until the failover begins. The service interruption with the bulk migration is equivalent to a reboot.

**VMware HCX vMotion**

This migration method uses the VMware vMotion protocol to move a virtual machine to a remote site.

- The vMotion migration option is designed for moving single virtual machine at a time.
Virtual machine state is migrated. There is no service interruption during the VMware HCX vMotion migration.

**VMware HCX Cold Migration**

This migration method uses the VMware NFC protocol. It is automatically selected when the source virtual machine is powered off.

**VMware HCX Replication Assisted vMotion**

VMware HCX Replication Assisted vMotion (RAV) combines advantages from VMware HCX Bulk Migration (parallel operations, resiliency, and scheduling) with VMware HCX vMotion (zero downtime virtual machine state migration).

**VMware HCX OS Assisted Migration**

This migration method provides for the bulk migration of guest (non-vSphere) virtual machines using OS Assisted Migration to VMware vSphere on-premise or cloud-based data centers. Enabling this service requires additional HCX licensing.

**Understanding VMware HCX Bulk Migration**

Bulk migration uses the host-based replication to move a virtual machine between HCX data centers.

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

A Bulk Migration request triggers the following actions:

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 original VM using a binary timestamp suffix to avoid a naming conflict with the migrated VM. If you have not enabled the Retain MAC option, the migrated VM obtains a new MAC address.

7. The migration completes.
VMware HCX copies the original VM to the Migrated VMs folder in the vSphere Templates view. You can recover a saved VM.

**Note**  There are two uses for these copies:

1. The copy can act as seed, in the event the VM on Site B must be protected on Site A.
2. Protect against any VM corruption (due to external factors) during migration.

### Requirements for HCX Bulk Migration

- The Hybrid Interconnect Service and Bulk Migration Service must be enabled and in a healthy state in the relevant service mesh.
- The resources to create, power on and use the virtual machine must be available in the destination environment.
- Virtual machines must be running Hardware Version 7 or higher.
- Virtual machines must have VMware Tools installed.
- Virtual machines must reside in a Service Cluster (defined in the Compute Profile).
- Network Extension is required for low downtime migration operations.
- Personalization Scripts and System Identity changes (Hostname, IP, SID) require the system to be rebooted one additional time during the switchover phase.
- Bulk Migration potential throughput can vary depending on bandwidth available for migrations, latency, available CPU/MEM/IOPS, and disk read speed. For successful switchover phase, the bandwidth and network conditions must be sufficient to satisfy the operation considering the dataset and virtual machine data change rate. For more information about how to determine bandwidth requirements, see [Bandwidth Requirements for vSphere Replication](#).

### Restrictions for HCX Bulk Migration

- Virtual machines with Raw Device Mappings (RDM) in Physical Compatibility mode cannot be bulk migrated.
- Virtual machines with mounted ISO images cannot be migrated. The HCX bulk migration operation can be used for force unmount ISO images.
- Virtual machine snapshots will not be migrated. The HCX bulk migration operation has an option to remove the snapshots.
- Virtual machines with DirectPath I/O configurations cannot be migrated without first removing the DirectPath device.
- Virtual machines with Multi-Writer or FT-enabled virtual machines can be migrated, but the multi-writer configuration will no longer be functional.
- Virtual machines with SCSI bus sharing cannot be migrated.
Virtual machines that cannot be gracefully powered off cannot be migrated. HCX can override with the Force Power-off VM option.

NSX Security tags and configurations related to the virtual machine will not be migrated. vSphere tags will be migrated.

With the Bulk migration option, new disk UUIDs are generated at the destination environment. Use HCX vMotion when the application has disk UUID-related dependencies.

Understanding VMware HCX vMotion and Cold Migration

The VMware HCX Interconnect integrates with ESXi to perform migrations based on the vMotion protocol for live powered on virtual machines, and with VMware NFC for cold migrations on powered off virtual machines.

HCX vMotion

VMware HCX vMotion can transfer a live Virtual Machine from a VMware HCX-enabled vCenter Server to a VMware HCX-enabled destination site (or from the VMware HCX-enabled destination 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 depends on the connectivity, including both the bandwidth available and the latency between the two sites.

HCX Cold Migration

Cold migration uses the same network path as VMware HCX vMotion to transfer a powered-off virtual machine. During a cold migration, the Virtual Machine IP address and MAC address are preserved. Cold migrations must satisfy the vMotion requirements.

Requirements for VMware HCX vMotion and Cold Migration

- VMware HCX Interconnect Tunnels must be up/active.
- VMware HCX 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.

Virtual Machine Restrictions for HCX vMotion

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

- Shared VMDK files.
- Attached virtual media or ISOs.
- Virtual Machine Hardware Version 8 or below.
Although concurrent VMware HCX vMotion migrations can be initiated up to the vSphere limits, VMware only supports serial VMware HCX vMotion migrations between a source and destination site. For simultaneous migrations in parallel, select VMware HCX Bulk Migration.

VMware HCX vMotion defaults to Opportunistic mode for per-VM vMotion Encryption if it is set to Required. During the migration operation - the mode is changed to Opportunistic during the migration initialization, and then set back to Required after the migration is completed.

Virtual Machines with Change Block Tracking (CBT) can be migrated, but HCX disables CBT.

Understanding VMware HCX Replication Assisted vMotion

VMware HCX Replication Assisted vMotion (RAV) uses the HCX Interconnect appliance along with replication and vMotion technologies to provide large scale, parallel migrations with zero downtime.

HCX RAV provides the following benefits:

- Large-scale live mobility: Administrators can submit large sets of VMs for a live migration.
- Switchover window: With RAV, administrators can specify a switchover window.
- Continuous replication: Once a set of VMs is selected for migration, RAV does the initial syncing, and continues to replicate the delta changes until the switchover window is reached.
- Concurrency: With RAV, multiple VMs are replicated simultaneously. When the replication phase reaches the switchover window, a delta vMotion cycle is initiated to do a quick, live switchover. Live switchover happens serially.
- Resiliency: RAV migrations are resilient to latency and varied network and service conditions during the initial sync and continuous replication sync.
- Switchover larger sets of VMs with a smaller maintenance window: Large chunks of data synchronization by way of replication allow for smaller delta vMotion cycles, paving way for large numbers of VMs switching over in a maintenance window.
- Legacy version support: Migrating VMs with RAV is supported for vSphere 5.1 at the source site. For destination environment requirements, see "Software Version Requirements."

HCX RAV migration triggers the following events:

1. Replication begins with a full synchronization (replication) of the virtual machine’s disks to the destination site.
2. Migrated VMs enter a continuous synchronization cycle until a switchover is triggered.
3. You can have the switchover process start immediately following the initial sync or delay the switchover until a specific time using the scheduled migration option. If the switchover is scheduled, the synchronization cycle continues until the switchover begins.
4. The final delta synchronization begins when the switchover phase starts. During this phase, vMotion is engaged for migrating the disk delta data and virtual machine state.
5. As the final step in the switchover, the source VM is removed, and the migrated VM is connected to the network powered on.
Requirements for HCX Replication Assisted vMotion

- VMware HCX Interconnect tunnels must be up/active.
- VMware HCX vMotion requires 100 Mbps or above throughput capability.
- The virtual machine hardware version must be 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.
- The Hybrid Interconnect, Bulk Migration, vMotion, and Replication Assisted vMotion services must be enabled and in a healthy state in the relevant service mesh.
- The resources to create, power on and use the virtual machine must be available in the destination environment.
- Virtual machines must reside in a Service Cluster (defined in the Compute Profile).
- RAV uses vSphere Replication whose potential throughput can vary depending on bandwidth available for migrations, latency, available CPU/MEM/IOPS, and disk read speed. For more information about how to determine bandwidth requirements, see Bandwidth Requirements for vSphere Replication.

Restrictions for HCX Replication Assisted vMotion

- Virtual machines with the following attributes are not supported for migration.
  - Shared VMDK files.
  - Attached virtual media or ISOs.
  - Virtual Machine Hardware Version 8 or below.
- Live switchover of concurrent RAV migrations is run serially.
- VMware HCX vMotion defaults to Opportunistic mode for per-VM vMotion Encryption if it is set to Required. During the migration operation - the mode is changed to Opportunistic on the migration initialization, and then set back to Required after the migration is completed.
- VMware HCX Replication Assisted vMotion does not support migration of workloads with Independent persistent and Independent non-persistent disks.
- Virtual machines with Raw Device Mappings (RDM) in Physical Compatibility mode cannot be bulk migrated.
- Virtual machines with DirectPath I/O configurations cannot be migrated without first removing the DirectPath device.
- To migrate FT-enabled VMs, temporarily turn off Fault Tolerance, and perform RAV. When this operation is complete, turn Fault Tolerance back on.
- Virtual machines with SCSI bus sharing cannot be migrated.
- Virtual machines that cannot be gracefully powered off cannot be migrated. HCX can override with the Force Power-off VM option.
- NSX Security tags and configurations related to the virtual machine are not migrated. vSphere tags are migrated.
- Virtual Machines with Change Block Tracking (CBT) can be migrated, but HCX disables CBT.
- With the RAV migration option, new disk UUIDs are generated at the destination environment. Use HCX vMotion when the application has disk UUID-related dependencies.
- VIO and vCD cloud types are not supported.
- RAV migration using VMFS6 target datastores requires the following minimum vCenter version at the target site: vCenter Server 6.5U3f or vCenter Server 6.7U3.
- RAV migration for virtual machines with any disk in independent persistent mode is not supported as taking a snapshot of such a virtual machine does not produce delta disks, which are required for the underlying RAV migration technology.

**Understanding VMware HCX OS Assisted Migration**

The HCX OS Assisted Migration service uses the Sentinel software that is installed on Linux- or Windows-based guest virtual machines to assist with communication and replication from their environment to a VMware vSphere SDDC.

You must install HCX Sentinel on all guest virtual machines requiring migration using HCX OS Assisted Migration. Sentinel gathers the system configuration from the guest VM and assists with the data replication. The source system information is used by various HCX OS Assisted Migration service processes. In part, the information is used to create an inventory of guest VM systems for migration and to help replication processes prepare the disks on the replica VM for replication and migration.

Sentinel also helps with the data replication by reading data that is written to the source disks and passing that data to the SDR appliance at the destination site.

Guest VMs connect and register with an HCX Sentinel Gateway (SGW) appliance at the source site. The SGW then establishes a forwarding connection with an HCX Sentinel Data Receiver (SDR) appliance at the destination vSphere site. You specify the network connections between the guest VMs and SGW in the compute profile.

You must install the HCX Sentinel software on each guest VM requiring migration to enable the guest VM discovery and data replication. After Sentinel is installed, a secure connection is established between the guest VM and the HCX SGW. HCX builds an inventory of candidates for migration as the Sentinel software is installed on the guest VMs.

Using the established connection between the SGW and SDR, replication connections are established between the Sentinel software on the guest VMs and the SDR, with one connection each for control operations and data replication.
An OS Assisted Migration request triggers the following events:

1. Replication begins a full synchronization transfer to the destination site. The guest VM remains online during replication until the final delta synchronization.

2. Before the final delta synchronization, the OS Assisted Migration service quiesces the guest VM.

3. HCX performs a hardware mapping of the replicated volumes to ensure proper operation, including updates of the software stack on the replica. This fix-up process includes adding drivers and modifying the OS configuration files at the destination. The migrated VM reboots during this process.

   **Note** When migrating Windows systems, HCX OS Assisted Migration software creates a temporary local user on the migrated Windows system during the switchover phase. This user gets deleted after the fix-up process is completed.

   **Note** When migrating Linux systems, HCX OS Assisted Migration software uses an independent software stack residing on a separate disk for the fix-up process. This fix-up boot disk is detached and deleted at the end of the switchover process.

4. When the delta synchronization finishes, a switchover is triggered. You can have the switchover process start immediately following the initial sync 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. The final delta synchronization begins when the switchover phase starts.

5. As the final step in the switchover, the source is powered-off, the migrated replica is connected to the network, and the switchover completes.

   If the source does not power off, an attempt is made to power off the replica VM. If the replica VM successfully powers off, it remains connected to the NICs. In this case, you can manually power off the source and power on the replica. If the replica does not power off, both the guest VM and the replica remain on, but the replica is not connected to the network. In this case, you enable the NICs manually that are attached to the replica VM using vCenter, power-off source VM (if not already), and power-on Migrated VM.

6. HCX Manager names the replica VM with the hostname of the source VM.

7. VMware Tools is installed on the migrated VM and migration completes.

**VMware HCX OS Assisted Migration Requirements**

- **Supported OS versions:**

<table>
<thead>
<tr>
<th>Supported OS versions on KVM Hypervisor</th>
<th>Supported OS versions on Hyper-V Hypervisor</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL 6.x, 7.x (64-bit)</td>
<td>Windows Server 2012</td>
</tr>
<tr>
<td>RHEL 6.x (32-bit)</td>
<td>Windows Server 2012R2</td>
</tr>
<tr>
<td>CentOS 6.x, 7.x (64-bit)</td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>CentOS 6.x (32-bit)</td>
<td>Windows Server 2008 R2 (64-bit)</td>
</tr>
<tr>
<td>Supported OS versions on KVM Hypervisor</td>
<td>Supported OS versions on Hyper-V Hypervisor</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Ubuntu server 16.04 (32-bit and 64-bit)</td>
<td></td>
</tr>
<tr>
<td>Ubuntu server 18.04 (64-bit)</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2012</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2012 R2</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2016</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2008 R2 (64-bit)</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2008 SP2 (32-bit and 64-bit)</td>
<td></td>
</tr>
</tbody>
</table>

- Linux workload migration limitations:
  - Unsupported filesystems (supported file systems: ext2, ext3, ext4, XFS).
  - Unmounted filesystems (Linux specific).
  - Unknown content with a partition or a block device.
  - Encrypted filesystems.
  - md devices (software RAID).

- Windows workload migration limitations:
  - Basic disks (MBR and GPT) are migrated to the destination. Dynamic disks, including logical volumes, are not migrated to the destination.
    - If the boot disk is dynamic, migration is not supported.
    - If the data disks are dynamic, the data on the disks is not migrated, and the disks appear as raw disks on the migrated system.
  - Only NTFS formatted volumes are supported. ESP (EFI system partition) with the FAT32 file system is an exception.
  - No support for non-Windows service applications from system quiescing perspective during the final sync.
  - Systems with more than 64 volumes are not supported since VSS allows a maximum of 64 snapshots on a system.
  - Any VSS snapshots present on the source Windows system prior to migration are not be usable on the migrated system.
  - Sentinel software is not automatically updated.

- An SDR appliance can support up to 57 active replica disks. This support limits the number of VMs that can be migrated at the same time. In other words, the total number of disks among all active migrating VMs cannot exceed 57.

- Only one SGW and one SDR deployment is supported per Service Mesh, meaning that multi-site service mesh is not supported.

- Guest VMs can only be migrated to a datastore that is accessible by the SDR.
- For Linux systems, interface bonding is only supported for Ubuntu Linux.
- For Linux systems, static routes are not supported.
- VLAN interfaces on Linux and Windows are not supported.
- Redeployment of SGW and SDR appliances is not allowed when any migration is in-progress.
- For Windows systems, in general the pre-requisites for the VMware Tools installation have to be satisfied on the source system. The pre-requisites for the VMware Tools installation can vary based on: the target VC and ESX version, and Windows OS version on the source system. For example, if the target ESXi version is 6.5.0 (or higher), VMware Tools version is 10.3.x. The prerequisites based on different Windows OS versions are listed at: https://kb.vmware.com/s/article/55798.
- On RHEL/CentOS 7.0, 7.1, and 7.2, the XFS filesystem UUID is not restored to the original UUID for the filesystem where /boot resides because mkfs.xfs does not support the functionality (-m option). A new random UUID is generated. Modifying the UUID after the filesystem is created triggers RHEL bug 1579390.
- Linked Mode VCs are not supported.
- VMC, vCD, and VIO cloud types are not supported.
- Only “thin” and “thick” disk provisioning types are supported as the disk provision type for the migrated system. The "Same as Source" option is not supported.
- OSAM migration service applies the default storage policy to the migrated VMs and their disks. Currently, user selected storage policy is not supported by OSAM service.
- /etc/fstab entries for removable media (floppy, CD) are not supported; such entries must be commented-out before migration.
- When migrating Windows systems, the HCX OS Assisted Migration software creates a temporary local user on the migrated Windows system during the switchover phase. This user gets deleted after the fix-up process is completed.
- When migrating Linux systems, the HCX OSAM software uses an independent software stack residing on a separate disk for the fix-up process. This fix-up boot disk is detached and deleted at the end of the switchover process.
- When migrating Windows systems, the HCX OS Assisted Migration software applies only the IPv4 configurations to the migrated system based on source system interface configuration. All the other network settings have the default Windows configuration values.
- The configuration files of Linux system services (for example, dhcpd) that reference network interface names are not modified. You must manually modify these files on the migrated system.
- Do not run Windows updates on the source system during a migration. If Windows updates are in progress, the migration can fail.
- Source systems with legacy BIOS are not supported. Most UEFI implementations include a BIOS compatibility(legacy) mode.
RHEL/CentOS 7.x Virtual Machines running under Hyper-V is supported for both Gen 1/BIOS and Gen 2/UEFI.

Migrating Virtual Machines with HCX

Through the HCX Migration interface, you can configure multiple virtual machine migrations, including reverse migrations.

This section describes migration operations using HCX Advanced License functionality. For information about migration operations using HCX Mobility Groups, which is available as an HCX Enterprise License feature, see Migrating Virtual Machines with Mobility Groups.

Reverse migration refers to the migration of virtual machines from an HCX-enabled remote site to a local site.

All HCX migration operations, including reverse migrations, are initiated from the local site.

Prerequisites

- The migration service is enabled in both the source and destination site Compute Profile.
- The migration service is enabled in the HCX Service Mesh.
- For RAV or OSAM migrations, the HCX Enterprise license is activated.
- Sentinel software is installed on all guest virtual machines requiring OSAM migration. See Sentinel Management.

Procedure

1. Navigate to the HCX dashboard.
2. Select the Service > Migration.
   The Migrate Tracking window displays a summary of virtual machine migrations.
3. Select Migrate Virtual Machines.
4. Select the Remote Site Connection.
   The list of virtual machines available for migration appears in the display.

   **Note** For OSAM, select Non vSphere Inventory > Remote connections to display the list of guest virtual machines on which you installed HCX Sentinel.

5. (Optional) To display the list remote site virtual machines available for the reverse migration, click the Reverse Migration check box.
6. Select the virtual machines you want to migrate.

   **Note** Click hide unselected to keep only selected virtual machines on the screen.
7 Set the Transfer and Placement, Switchover, and Extended options.

- To apply default settings for all selected virtual machines, use the green area of the interface at the top of the window.
- To set machine-specific Transfer, Placement, and Switchover options, select a specific virtual machine and expand the entry.

**Note**
- For Bulk, RAV, and OSAM migrations, you can schedule the migration date and time as part of the Switchover settings. Scheduling vMotion migrations is not available.
- If the VM is powered off, Cold Migration is set by default.
- Extended Options provide additional settings based on the selected migration type.
- For additional information, see Additional Migration Settings.

8 Select the destination network for each virtual machine to be migrated.

In most cases, the stretched network between the source and destination sites is automatically selected. You can change this selection as needed.

a Expand each virtual machine selection.

b Next to each guest virtual machine NIC name, click the folder for a list of available target networks.

c Click the check box next to the network you want the guest virtual machine to map to, and then click Select.

d (Optional) To specify a new guest OS IP address for the virtual machine at the target network, expand the NIC entry and enter the new IP address, gateway, and subnet mask.

9 Click Finish.

The HCX Manager validates your selections and starts the migrations. If a warning is generated, click Finish again to proceed.

**Monitoring Migrations with HCX**

The HCX Migration Tracking page displays a summary of migrations reporting the status and progress of individual virtual machine migrations.

**Procedure**

1 In the HCX dashboard, select Services > Migration.

The Migration Tracking interface displays a summary of migration information.

2 To determine the migration status, review the summary information.

   The UI groups all migrations by connection. While migrations are underway, the Progress column displays a progress bar with information about the number of bytes synced to the destination and the percentage of replication completed.
To sort the information in the list, use the filter option provided in each column of the display. You can use the filter option at the top right corner of the display to narrow down the list of migrations. You can filter by virtual machine name, state message, migration type, or other attributes.

**Canceling a Migration with HCX**

The HCX Migration interface includes an option for canceling migrations.

For OSAM, the effect of canceling a migration depends on the state of the migration when selecting the abort option:

- Canceling a migration while the HCX appliance is replicating data to the destination site deletes the associated resources created at the destination site with no effect on the source VM.
- Canceling a migration when the source system is in the final sync phase reboots the source system and deletes the associated resources.
- Canceling a migration after the target VM has been created deletes the destination virtual machine and the associated resources.
- Canceling a migration after the source virtual machine is powered down requires you to restart the virtual machine at the source site. Also, the HCX deletes the associated resources at the destination site.

For Bulk Migration, you can cancel a migration at any point with no effect on the source site virtual machine. Replication is canceled on the source site VM, and replicated data is deleted from the destination site.

Canceling a migration is not available for vMotion, Cold Migration, and Replication Assisted vMotion (RAV) migration types.

**Procedure**

1. In the HCX dashboard, select Services > Migration.
   
   The Migration Management interface displays a summary of migration information.
2. Identify the virtual machine on which to cancel migration, and expand the entry.
3. In the Status column, select Abort Migration.
   
   This operation can take several minutes. When finished, the UI displays the message Migration aborted.

**Migrating Virtual Machines with Mobility Groups**

Mobility Groups is an HCX Enterprise License feature that supports assembling one or more virtual machines into logical sets, for execution and monitoring of migrations as a group.

With Mobility Groups, you have the flexibility to manage migrations for sets of virtual machines by application, network, pod, or other aspects of your environment.

All HCX migration operations, including reverse migrations, are initiated from the source site.
Prerequisites

HCX Enterprise license is activated.

Procedure

1. Open the HCX plugin in the vSphere Client.

2. Select Services > Migration.

   The Migration Management interface displays a summary of groups and provides the group migration progress. For detailed group information, you can expand each group.

3. Click Migrate and select Remote Site Connection.

   The Workload Mobility interface displays a list of virtual machines (workloads) that are available for migration and that can be added to a group. You can select the Networks or Hosts and Clusters icon to update the list of virtual machines. In addition, you can use a regular expression search to filter the list of virtual machines by name.

   **Note** If you have only one site pair, it is selected by default. For OS Assisted Migrations, select Non vSphere Inventory > Remote connections to populate the list of guest virtual machines on which you installed HCX Sentinel.

4. (Optional) To display a list of remote site virtual machines available for the reverse migration, click the Reverse Migration check box.

   **Note** Reverse migration refers to the migration of virtual machines from an HCX-enabled destination site to a source site.

5. Specify a Group Name.

   **Note** If no group name is provided, the system automatically assigns a five character identifier as the group name. You can change this name later by editing the group information. See Managing Migrations with Mobility Groups.

6. Select the set of virtual machines to include in the group and click ADD.

   **Note** You can add additional virtual machines to the group at any time.
7 Select the group Transfer and Placement, Switchover, and Extended options.

The settings you provide are applied to all members of the group by default. To override the default settings for specific virtual machines in the group, select and expand the virtual machine entry, and set different options.

**Note**
- For Bulk, Replication Assisted vMotion (RAV), or OS Assisted Migration (OSAM) type migrations, you can schedule the migration. Scheduling migrations for vMotion is not supported.
- If the VM is powered off, Cold Migration is set by default.
- Extended Options provide additional settings.
- For additional information, see Additional Migration Settings.

8 Select the destination network for each virtual machine to be migrated.

In most cases, the stretched network between the source and destination sites is automatically selected. You can change this selection as needed.

a Expand each virtual machine selection.

b Next to each guest virtual machine NIC name, click the folder for a list of available target networks.

c Click the check box next to the network you want the guest virtual machine to map to, and then click Select.

d (Optional) To specify a new guest OS IP address for the virtual machine at the target network, expand the NIC entry and enter the new IP address, gateway, and subnet mask.

9 To complete the Mobility Group migration operation, select Go, Validate, Save, or Close to complete the Mobility Group migration operation:

<table>
<thead>
<tr>
<th>Migration operation</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Go</td>
<td>Validates your virtual machine migration selections, saves the group, and then starts the migration.</td>
</tr>
<tr>
<td>Validate</td>
<td>Validates readiness of selected virtual machine for migration without starting the migration. Validation can be done at any time on selected virtual machines or a group.</td>
</tr>
<tr>
<td>Save</td>
<td>Saves migration selections as drafts for future editing or scheduling without starting the migration.</td>
</tr>
<tr>
<td>Close</td>
<td>Cancels your selections without creating a group or starting a migration.</td>
</tr>
</tbody>
</table>

**Monitoring Migrations with Mobility Groups**

The HCX Migration interface provides a summary of group migration progress and the progress of individual virtual machine in a group.
Procedure

1. Navigate to Services > Migration.

The Migration Management window displays Mobility Group information for each site pair. The window displays both forward and reverse migration information.

2. To display a summary of migration information for the virtual machines in a group, expand the group.

3. To display an overall summary of group migration progress, including the migration phase, click the Group Info icon.

   Migration phase information includes the base synchronization and switchover percentages.

4. To display the Transfer and Placement, and Switchover information associated with a virtual machine in the group, expand the migration entry.

5. To display a list of virtual machine migrations and migration progress, select the Migration Tracking tab.

   The Migration Tracking window provides a list of ongoing or recent migrations for all site pairs.

   Sort the tracking information using the filter option provided in each column heading.

6. To return to the Migration Management window, click Migration Management.

Managing Migrations with Mobility Groups

From the HCX Migration interface, you can edit any group, delete groups, initiate and stop migrations, and schedule migrations.

Procedure

1. Navigate to Services > Migration.

   The Migration Management window displays a summary of Mobility Group information for each site pair. The window displays both forward and reverse migration information.

   **Note** You can switch between Migration Management (group migration) and Migration Tracking (individual migration) displays at any time using the menu button.

2. From the migration management window, you can edit or delete any group.

<table>
<thead>
<tr>
<th>Mobility Group Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Group</td>
<td>To display the Workload Mobility window, click this option. From this window, you have several options:</td>
</tr>
<tr>
<td></td>
<td>■ Add additional virtual machines to the group.</td>
</tr>
<tr>
<td></td>
<td>■ Change the default migration profile for the group.</td>
</tr>
<tr>
<td></td>
<td>■ Change the migration profile of individual virtual machines.</td>
</tr>
<tr>
<td></td>
<td>■ Delete a specific virtual machine from the group.</td>
</tr>
<tr>
<td></td>
<td>■ Restart failed or canceled migrations.</td>
</tr>
<tr>
<td>Delete Group</td>
<td>To delete a group entry, click this option. You can delete a group only when all entries in the group are in the Draft state.</td>
</tr>
</tbody>
</table>
3 To show information about all members of the group, expand the group.

The system displays a list of virtual machines in a group with their migration status.

4 From the expanded group, you can also start, cancel, or schedule one or more selected migrations.

<table>
<thead>
<tr>
<th>Mobility Group Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Go</td>
<td>Validates your virtual machine migration selections and then prompts you to start the migration. After the migration starts, the migration progress changes with each phase of the migration.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Provides an option to reschedule a switchover for the migration.</td>
</tr>
<tr>
<td>Abort</td>
<td>Cancels a migration that is in progress. This operation is supported only for Bulk, Replication Assisted vMotion, and OS Assisted Migration (OSAM) migrations types. For information about the effects of canceling an OSAM migration, see Canceling a Migration with HCX.</td>
</tr>
</tbody>
</table>

Additional Migration Settings

The VMware HCX migration interface provides a set of options that 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, VMware HCX attempts to shut down the Virtual Machine guest gracefully during the VMware HCX Bulk migration operation. If the OS interrupts the termination process, the migration operation fails. Checking this option allows VMware 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 VMware 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 VMware 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 VMware 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 VMware HCX to consolidate snapshot files before migrating the Virtual Machine. If there are snapshots present, the system enables the option by default.

Force Unmount Container
This option allows VMware HCX to remove mounted ISO images before migrating the Virtual Machine.

Select Destination Container
This drop-down option is for selecting a compute container (cluster, host, resource pool) that the VMware HCX migrated Virtual Machine uses at the destination site.

Select Destination Storage
This drop-down option is for selecting a storage location that the VMware HCX migrated Virtual Machine uses at the destination site.

Select Virtual Disk Format
This drop-down option allows VMware HCX to set the Virtual Disk Format that the migrated Virtual Machine uses at the destination site.

Select the Destination Network
This drop-down option is for selecting the network that the extension uses to connect the VMware HCX migrated Virtual Machine at the destination site. If the Virtual Machine resides on a network that has been extended with VMware HCX, the system selects that network automatically.
Protecting Virtual Machines with VMware HCX

VMware HCX provides various services for protecting virtual machines based on the type of license installed.

The HCX Disaster Recovery service, standard with HCX, replicates and protects virtual machines to a remote data center. The HCX Integration with the Site Recovery Manager service is available with Enterprise licensing. HCX with SRM takes advantage of the HCX Interconnect and Network Extension components for protection and recovery operations from the SRM interface.

This chapter includes the following topics:

- VMware HCX Disaster Recovery
- HCX Integration with Site Recovery Manager

VMware HCX Disaster Recovery

Virtual Machine replication-based protection with a nimble architecture that uses existing VMware HCX mobility components.

VMware 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. VMware 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 VMware HCX Disaster Recovery. VMware HCX Disaster Recovery provides the following benefits:

- Simple and easy to use the 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 an 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 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 depends on the available bandwidth from the source site to the destination site.

- Multiple points in time recovery snapshots that allow you to recover back up to 24 previous replication point in time.
- Optimized replication throughput by use of Wan Optimizer.
- Routing replication traffic through a customer preferred direct connect network
- On-premises monitoring and management with the fully integrated vSphere Web Client.
- Access to production-level support from VMware.

**Prerequisites**

- Enabled Disaster Recovery services through VMware HCX.

**Enabling DR Protection for a Virtual Machine**

The VMware HCX virtual machine protection operation is used to configure the disaster recovery settings for a virtual machine, with specific remote site resources and recovery point objectives.

**Procedure**

1. In the **vSphere Web Client**, navigate to VMware HCX.
2. Navigate to the **Disaster Recovery** tab and click **Protect VMs**.
   
   Protection Configuration screen appears.
3. Set these options as appropriate:
   
   - Replication Destination Site – When selected, the site loads the virtual machine Inventory for Site B. When deselected (default), Site B’s virtual machine inventory is loaded.
   - Remote Site – The 2 Sites that are paired and the current direction of Protection.
   - Source Inventory
- Default Replication options – Global Setting Policy for all VMs within the DC or Cluster, Resource Pool, or Host.
- Virtual Machine Replication Options:
  - Enable Compression – Helps during the seeding process of the VM. Helps if there is a low throughput LAN/WAN connectivity.
  - Enable Quiescence – Pauses the virtual machine to ensure that the most consistent copy of the virtual machine is protected on Site B.
  - Seed Virtual Machine – Used when a previous action created a copy of the VM, for example, a Bulk Migration of a virtual machine.
  - Specify Destination Container – data center, Cluster, or Resource Pool where the protected copy of the virtual machine is going to live.
  - Storage – Datastore on which the protected copy of the virtual machine resides. The Storage Policy drop-down menu lists all compatible datastores. Default Storage Policy and the corresponding datastore are used if there is no selection.
  - RPO – Recovery Point Objective for the VM. With VMware HCX, it can go from 5 mins – 24 hours. The synchronization interval between the Source virtual machine and the Protected virtual machine.
  - Snapshots Interval – Interval between Snapshots. In the event, a corrupted change was synchronized to the protect site, providing an option to recover from an earlier point in time. The event provides a Multiple Point in the Time Recovery plan for the protected VM.
  - No. of Snapshots – Total number of snapshots within the established snapshot interval.
  - Network Port group – Corresponding port group that the protected virtual machine uses. In the illustration used, the port group that the source virtual machine is using has been stretched to Site B, as a result it is automatically populated.

**Note** Always verify the Storage Policy and associated datastore selection, and evaluate the expected storage usage at the DR site. The settings cannot be changed once the protection is in place. Storage Policy selection is NOT available during Recovery or Test Recovery operations.

4 Click **Next**. A validation of the configuration for protection is performed.

5 Click **Finish**. The DR Dashboard is displayed. You can monitor the progress of virtual machine protection.

6 The dashboard now shows the virtual machine being protected. Expand the dashboard.
- Local VMs – Reflects the total # of VMs on Site B that are protected. In the preceding illustration, it shows that one local virtual machine is being protected.
- Remote VMs – Reflects the total # of VMs on Site B that are being protected from other Sites.
- Activity – To monitor any ongoing Disaster Recovery related operations.
- Green Shield – DR protection is active.
Yellow triangle – Protection has not been tested.

In/Out – Direction of protection between a local site and a remote site.

7 Log in to Site B.

8 Go to Services > Disaster Recovery.

The Protected virtual machine is displayed. This process shows how a virtual machine on Site A is protected on Site B using VMware HCX.

Performing a Virtual Machine Test Recovery

A VMware HCX Disaster Recovery protection configuration can be tested by bringing the virtual machine online with a test recovery operation, which does not disrupt the ongoing replication.

Prerequisites

- An initial full synchronization of the protected virtual machine is required. The interface dims the virtual machine test recovery option while the initial synchronization is in progress, to indicate that the option is disabled until the initial synchronization procedure completes.
- When working with protected virtual machines on extended networks:
  - Do not connect a test-recovered virtual machine to the extended network. Doing so may impact the original protected virtual machine due to the duplicate IP address.
  - To test the recovery, create or use a test network at the Disaster Recovery site.

Procedure

1 Log in to the vSphere Web Client and access the VMware HCX plugin.

2 Go to the Disaster Recovery tab.

3 Select the virtual machine and under Actions, click Test Recovery.

4 If the Protected virtual machine is on a stretched network, an error similar to the illustration shows up. The option to use none is available for Test Recovery operations.

5 Clicking Test.

  After the test 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.

6 Select the VM, click Actions, and then click Test Cleanup.

7 Click Cleanup on the next screen.

Results

The test is now cleaned up. The solid yellow triangle disappears.
Performing a Virtual Machine Recovery

Using the VMware HCX Disaster Recovery's Virtual Machine recovery operation, you can enable the Virtual Machine replica at the HCX destination site.

Prerequisites

This procedure applies when a protected virtual machine has become unavailable due to a disaster event. This unavailable state is indicated with a red lightning bolt status in the Services - Disaster Recovery interface.

Procedure

1. Open the VMware HCX Cloud interface at the destination site.
2. Navigate to Services > Disaster Recovery.
3. Click (colon icon) and click Recover.

The recovery process starts. After the recovery completes, the Virtual Machine is visible in the VMware HCX Disaster Recovery destination site's vSphere Inventory.

VMware HCX Disaster Recovery - Protect Operations for VMs

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

Available Operations include:

1. Reverse – After 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 virtual machine selected.
3. Resume - Pause the current replication policy associated with the virtual machine selected.
4. Remove - Remove the current replication policy associated with the virtual machine selected.
5. Sync Now – Out of bound sync source virtual machine to the protected VM.

HCX Integration with Site Recovery Manager

The HCX integration with the Site Recovery Manager (SRM) enables protection and recovery operations from the SRM interface.

SRM DR backup and recovery operations use the HCX hybrid interconnect to optimize the bandwidth and connectivity, secure VMs in transit, and stretch networks to simplify the IP address management for recovered VMs.

Requirements

The HCX Integration with the Site Recovery Manager service has the following requirements:

- It is supported with HCX private cloud (NSX Enterprise Plus) deployments.
- Tested with SRM 8.2.
Enabling SRM Integration in HCX

Enabling SRM integration in HCX requires adding the SRM Integration Service in the Compute Profile and preparing the system configuration file on the SRM server.

Prerequisites

HCX Enterprise license is activated.

SRM is installed successfully for both the source and destination sites.

Procedure

1. On both the source and destination HCX, select the SRM Integration Service when creating or updating the Compute Profile. See Creating a Compute Profile.

2. On both the source and destination HCX, check that the SRM Integration Service is included in the Service Mesh. See Creating a Service Mesh.

3. On both the source and target SRM server, edit the file C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml to add the HCX extensions:

   ```xml
   <extension>
     <hmsType>com.vmware.hcx</hmsType>
     <hmsKey>com.vmware.vcHcx</hmsKey>
   </extension>
   ```

4. Restart the SRM client service followed by the SRM server.

   The plugin com.vmware.hcx appears in the vCenter Managed Object Browser.

Protecting VMs with SRM Integration Enabled

You must configure the HCX disaster recovery protection for a virtual machine, with specific remote site resources and recovery point objectives, before they are available in Site Recovery Manager.

Procedure

1. For each virtual machine you want to manage in SRM, configure the protection settings as described in Enabling DR Protection for a Virtual Machine.

2. In Site Recovery Manager, verify that all protected virtual machines are available.

Performing Test and Recovery Operations Using SRM Integration

The HCX Interconnect with Site Recovery Manager (SRM) makes available the suite of features and tools provided by SRM for virtual machines protected by HCX.

The HCX integration with the Site Recovery Manager service takes advantage HCX Interconnect and Network Extension components for protection and recovery operations from the SRM interface. VMware SRM provides resources that help you to plan, test, and run recovery of virtual machines between a protected vCenter Server site and a recovery vCenter Server site.
For information about test and recovery operations available in SRM, see the VMware Site Recovery Manager documentation.
Managing System Settings

Use the appliance management interface for viewing, configuring, and managing system-level functions.

The appliance management interface is reached by navigating to the management port: <https://hcx-ip-or-fqdn:9443>. This interface uses the system administration credentials set up during the OVA deployment.

The appliance management interface provides access to the system Dashboard, Appliance Summary, Configuration, and Administration information.

Note  Appliance management operations may be done by your cloud service provider.

This chapter includes the following topics:

- Understanding the Appliance Management Dashboard
- Updating the Time Settings
- Updating the System Name
- Managing CA and Self Signed Certificates
- Backing Up and Restoring the System

Understanding the Appliance Management Dashboard

The system Dashboard provides access to status and services, configuration settings, and system-level administration tasks.

The Dashboard is the first screen that appears after you log in to the appliance management interface port (:9443).
The Dashboard provides access to various system management settings through a set of tabs at the top of the display.

**Note** For installations where the vCenter Servers are in linked-mode, the Dashboard includes information from all vCenter Servers registered to a system.

<table>
<thead>
<tr>
<th>Tab Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>Displays the appliance status as a set of summary panels:</td>
</tr>
<tr>
<td></td>
<td>- System information and resource usage</td>
</tr>
<tr>
<td></td>
<td>- NSX status</td>
</tr>
<tr>
<td></td>
<td>- vCenter status</td>
</tr>
<tr>
<td></td>
<td>- SSO status</td>
</tr>
<tr>
<td></td>
<td>- Public Access URL status</td>
</tr>
<tr>
<td></td>
<td>The panels that are visible in the display depend on the HCX installation type. To change the configuration settings for a panel, click <strong>Manage</strong>. The system redirects you to the Configuration tab, where you can update the settings.</td>
</tr>
<tr>
<td>Appliance Summary</td>
<td>Displays the status of services running on the system:</td>
</tr>
<tr>
<td></td>
<td>- Hybridity Services</td>
</tr>
<tr>
<td></td>
<td>- Common Services</td>
</tr>
<tr>
<td></td>
<td>- System Level Services</td>
</tr>
<tr>
<td></td>
<td>Options are provided to stop and restart services. The list of services in the display varies based on the installation type.</td>
</tr>
<tr>
<td>Tab Entry</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configuration</td>
<td>Displays the list of service configuration settings.</td>
</tr>
<tr>
<td></td>
<td>- Licensing</td>
</tr>
<tr>
<td></td>
<td>- vCenter</td>
</tr>
<tr>
<td></td>
<td>- SSO</td>
</tr>
<tr>
<td></td>
<td>- Public Access URL</td>
</tr>
<tr>
<td></td>
<td>- vSphere Role Mapping</td>
</tr>
<tr>
<td></td>
<td>- Data Center location</td>
</tr>
<tr>
<td></td>
<td>Click an item in the list to display the current settings. To modify the current settings, click <strong>Edit</strong>.</td>
</tr>
<tr>
<td>Administration</td>
<td>Displays the list of system-level configuration settings.</td>
</tr>
<tr>
<td></td>
<td>- General Settings</td>
</tr>
<tr>
<td></td>
<td>- Time Settings</td>
</tr>
<tr>
<td></td>
<td>- Syslog Server</td>
</tr>
<tr>
<td></td>
<td>- System Name</td>
</tr>
<tr>
<td></td>
<td>- Network Settings</td>
</tr>
<tr>
<td></td>
<td>- General Network</td>
</tr>
<tr>
<td></td>
<td>- DNS Servers</td>
</tr>
<tr>
<td></td>
<td>- Proxy</td>
</tr>
<tr>
<td></td>
<td>- Static Routes</td>
</tr>
<tr>
<td></td>
<td>- Troubleshooting</td>
</tr>
<tr>
<td></td>
<td>- Technical Support</td>
</tr>
<tr>
<td></td>
<td>- Logs</td>
</tr>
<tr>
<td></td>
<td>- Upgrade</td>
</tr>
<tr>
<td></td>
<td>- Backup &amp; Restore</td>
</tr>
<tr>
<td></td>
<td>- Certificate</td>
</tr>
<tr>
<td></td>
<td>- Trusted CA Certificate</td>
</tr>
<tr>
<td></td>
<td>- Server Certificate</td>
</tr>
<tr>
<td></td>
<td>Click an item to display or edit the settings.</td>
</tr>
</tbody>
</table>

**Updating the Time Settings**

The system provides initial NTP Server settings during the OVA deployment in the vCenter Server. These settings can be updated in the appliance management interface.

**Caution**  Editing NTP Settings requires restarting the Appliance Management Service. You can restart this service from within the Appliance Summary tab.

**Editing and Removing the NTP Server Configuration**

NTP Settings can be modified in the appliance management interface.

HCX requires a valid NTP server synchronized time for integrated systems operations.

2. Navigate to the **Administration** tab.
3 Select Time Settings on the side menu, click Edit (or Unconfigure NTP Servers).

4 Enter the NTP server.
   Multiple servers can be specified using a separated comma-separated list.

5 Navigate to the Appliance Summary tab in the dashboard, locate the Appliance Management Service, and click Restart.

**Updating the System Name**

The initial Hostname is provided during the OVA deployment. The system name can be updated in the Appliance Management interface.

**Editing the System Name**

1 Navigate to the Appliance Management interface `https://hcx-ip-or-fqdn:9443`.

2 Navigate to the Administration tab.

3 Select System Name on the side menu, then click Edit.

4 Enter the System Name. Click Save.

### Managing CA and Self Signed Certificates

The appliance management interface can be used to add or remove certificates from the system certificate store.

**Importing Certificates with a Remote Site URL**

This operation is required for successful site pairing when the remote system is using self-signed certificates.

1 Navigate to the appliance management interface `https://hcx-ip-or-fqdn:9443`.

2 Navigate to the Administration tab.

3 Select Certificate > Trusted CA Certificate on the side menu.

4 Select the URL option.
5 Enter the URL for the target HCX system: https://hcx-manager-ip-or-fqdn

Use the IP or FQDN that the source HCX Manager uses to reach the HCX Cloud Manager.

Back up and restore the appliance from the appliance management interface.

Backup and restore operations are available in the appliance management interface except when restricted by a cloud service provider. You first use the appliance management interface to generate a configuration file and then use that file to restore to a healthy system.

The HCX service appliances, which include HCX-IX and HCX-NE, do not require individual backups. A restored HCX Manager reconnects to existing service appliances that were created within the backup time frame. If the service appliances are no longer functional, the HCX Manager deploys new appliance virtual machines based on the backed-up configuration.

**Backing up HCX Manager**

You use the appliance management interface to create a backup file.

This operation backs up the following information:

- Inventory data
- Configuration files
- Certificates
- System UUID

The backup file is saved in tar.gz format.

**Procedure**

1 Log in to the appliance management interface: <https://hcx-ip-or-fqdn:9443>.
2 Navigate to Administration > Troubleshooting > Backup & Restore.

3 (Optional) Set up an FTP server for uploading the backup file:
   a. Click the FTP server setting tab.
   b. Click Add.
   c. Enter the FTP server information and click Save.

4 (Optional) Configure a backup schedule:
   a. Click the Scheduling tab.
   b. Click Add.
      The scheduling window appears.
   c. Select the Backup Frequency.
   d. Enter the hour and minute of the backup.
   e. Click Save.

5 Click the Backup and Restore tab.

6 Click Generate.
   If a backup schedule is configured, the system creates the backup file at the scheduled time.

7 For manual backups, save the backup file:
   a. To save the generated file to an FTP server, check the box Upload to server.
   b. To download the generated file to the client browsing system, click Download.

Restoring the System

You use the appliance management interface to restore the system from a backup file. The restore operation is used in cases where the system has become corrupt or unusable due to resource or system failures.

This operation restores the appliance to the state it was in at the time of the backup. The contents of the backup file supersede configuration changes made before restoring the appliance.

Note: A restored HCX Manager cannot connect to HCX service appliances that were created during a time after the backup file was generated.
Prerequisites

You have deployed an replacement system that is clean of prior configuration settings. The replacement system has the same software version and IP address as the original system.

**Note**  A clean system deployment requires only the minimum configuration to be manageable and that the system is network reachable from the operator or client system.

Procedure

1. Log in to the appliance management interface: <https://hcx-ip-or-fqdn:9443>.
2. Navigate to **Administration > Troubleshooting > Backup & Restore**.
3. Within the **Restore** section, browse to the backup file and open it.

   **Note**  Restoring from backup files that are more than two days old is not supported due to potential inventory changes from the backup time to present.

4. Click **Continue**.

   The system verifies the uploaded file.

5. Click **Restore**.

   The restoration begins. This process can take several minutes to complete.

6. Verify that the system is operating properly:
   a. Navigate to the Dashboard tab and confirm that the NSX and vCenter Server status is green.
   b. Navigate to the Appliance Summary tab and verify that the Hybridity Services, Common Services, and System Level Services are running.
Updating VMware HCX

The information includes step-by-step instructions for updating HCX components.

This chapter includes the following topics:

- About HCX Service Updates
- Planning for HCX Updates
- HCX Service Update Procedures
- Converting Legacy Interconnect to Multi-Site Service Mesh

About HCX Service Updates

HCX service updates, with new features and software fixes, are released in a bi-weekly interval.

- HCX service updates are published periodically as a set for HCX Connector and HCX Cloud types.
- For example, the service update R123, contains HCX Connector R123 and HCX Cloud R123 builds.

Overview of HCX Component Updates

- HCX service updates can be summarized in the following steps:
  - During a new HCX implementation, the latest updates are applied automatically.
  - When VMware releases a service update, metadata for the release is published to the HCX client systems. The HCX Manager displays a notification banner noting the update.
  - The HCX admin identifies site paired HCX client systems, and applies the new service updates to the paired HCX Manager systems. You can update HCX Connector and HCX Cloud systems during separate maintenance windows, but for optimal compatibility update both systems together.
  - Apply service updates during a maintenance window where no new HCX operations are queued up.
    - The HCX Manager and Service Mesh can be upgraded independently, during separate maintenance windows.
    - The upgrade window accounts for a brief disruption to the Network Extension service, while the appliances are redeployed with the updated code.
During the window, the Interconnect service components are updated to the new release.

Component updates are triggered for each Interconnect or Service Mesh using the source side HCX plugin, but are run symmetrically at the source and destination site.

Planning for HCX Updates

As part of HCX update planning, and to ensure that HCX components are updated successfully, review the service update considerations and requirements.

Service Update Requirements

- HCX Manager systems periodically connect to connect.hcx.vmware.com and query the server for published service updates. A continuous connection is required. The VMware HCX UI displays a banner when an updated HCX release is available.
- VMware HCX client systems must be able to reach connect.hcx.vmware.com using HTTPS throughout the entire lifecycle of the system. When this connection is not available, the VMware HCX client system cannot display updates available to other VMware HCX systems.
- If the connection is not maintained, the client system can miss a published update.
- A client system without a maintained connection to connect.hcx.vmware.com is placed out of support if the connection is not restored. Also, the system displays a banner stating that the system will be deactivated.
- If the HCX service update is not reflected on all site paired HCX systems, contact VMware Support. Partial updates are not supported.
- VMware HCX client systems must be able to reach hybridity-depot.vmware.com using HTTPS for the download of update files, without connectivity to the depot, the Update Download fails.
- HCX Site Pairing must reflect healthy connections before applying the service update.
- Unless directed by VMware Support to upgrade to resolve a known issue, HCX components reporting degraded state must be restored to a healthy state before the update.

Service Update Considerations

- The HCX service update file can be downloaded to the HCX Manager systems before the upgrade to reduce the time of the maintenance windows.
  - If Site A is paired with Site B, and Site A is also paired with Site C, plan the updates for Site A, B and C for the maximum compatibility across all environments. The environments can be updated in separate windows.
- Applying a service update causes the HCX Manager system to be rebooted:
  - Existing Network Extensions continue to work during the HCX Manager reboot. New Network Extensions cannot be configured while the HCX Manager is rebooting.
Existing VM Protections continue to work during the HCX Manager reboot. New replications cannot be configured while the manager is rebooting.

Because upgrading the HCX Managers does not disrupt the Interconnect Service Mesh, the HCX team encourages installing updated releases when they become available to ensure that systems have the most recent fixes and security patches.

HCX Interconnect (Migration, WAN Optimization, and Network Extension) service component upgrades are performed independently to the manager upgrades:

- Upgrade the Service Mesh appliances only after all Site Paired HCX Managers are upgraded.
- Updating the Interconnect service components disrupts those services while the updates are being applied.
  - Ensure that migrations are not running or new migrations or replications are scheduled when updating the IX/CGW or WAN-OPT appliances.
  - Updating the HCX-NE (L2C) appliances disrupts connectivity that crosses the Network Extension path. The tunnel state re-converges in less than one minute after triggering the update.
  - Update the Network Extension components during a maintenance window.

- HCX client systems to be running within the latest three releases to be eligible for support.

**Service Update Sequence**

1. When a published update is available:
   - Identify the environments connected through HCX Site Pairing. The paired systems are displayed in the two tables in the Administration tab.
   - Connect to all paired HCX Managers and ensure that the update is available.
   - Download the update on all the paired HCX Managers.
   - Ensure that no new migrations, protections, or network extensions are configured during the update.
   - Ensure that all ongoing migrations have finished.
   - Ongoing synchronizations for Disaster Recovery are supported.
   - Ensure that there are no failovers scheduled during the upgrade.

2. Initiate the Upgrade task on all paired HCX Connector and HCX Cloud systems:
   - The HCX Manager system reboots during the upgrade procedure.
   - Allow the system several minutes to complete the initialization process.
   - Use the System Updates view to verify that the current version is updated.
3  The HCX Service Mesh can be upgraded once all paired HCX Manager systems are updated and all services have returned to a fully converged state.
   - HCX Interconnect service components can be upgraded from the source HCX system. Use the Service Mesh interface to redeploy or upgrade the VMware HCX Interconnect service appliances:
     - Upgrade or redeploy the HCX-IX (CGW) and HCX-WAN-OPT together.
     - Verify that the required tunnels are functional before resuming services or proceeding to the next component.
     - Upgrade or redeploy the HCX-NE (L2C) appliance.
     - Verify that the required tunnels are functional before resuming services or proceeding to the next component.
     - If the HCX topology has multiple source sites paired to a destination environment, the components upgrade has to be triggered at each source site.

**HCX Service Update Procedures**

Updating a VMware HCX system installs the latest features, problem fixes, and security patches.

**Upgrading the HCX Manager**

The HCX update is applied to the HCX Manager systems first.

*Note*  It is a best practice to back up the HCX Manager prior to upgrading. See [Backing Up and Restoring the System](#). This back up option may not be available in some Public Clouds where HCX is managed by the cloud service provider.

### Prerequisites

- Verify the HCX Manager system reports healthy connections to the connected (vCenter Server, NSX Manager (if applicable), vCloud Director/RMQ (if applicable).
- Verify the HCX Manager system reports healthy connections to the HCX Interconnect service components.
- Verify that Site Pair configurations are healthy.

### Procedure

1. Open the HCX Manager Service UI.

   *Note*  You can update site-paired HCX Managers simultaneously.

2. Navigate to the **Administration** tab.

3. Navigate to the **System Updates** section.
4 In the Local HCX section, under **Available Service Update Versions**, click **Check for Updates**.

In normal operation, the HCX automatically receives the latest service update. But if the HCX is offline or unable to access the Internet when a service update is pushed out, the HCX can miss the update. This selection checks for the latest version and adds it to your available service updates.

5 Right-click the available version link and select one of the operations from the drop-down menu.

If Service Updates have not been installed for more than one release, older updates are displayed. The newest updates are shown on top.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download.</td>
<td>The upgrade file is downloaded, but not installed.</td>
</tr>
<tr>
<td>Upgrade.</td>
<td>The file previously downloaded is used during the upgrade. If there is no file available, the option is dimmed.</td>
</tr>
<tr>
<td>Download &amp; Upgrade.</td>
<td>The upgrade file is downloaded. The upgrade begins immediately after the download completes.</td>
</tr>
</tbody>
</table>

6 To begin the selected process, click **OK**.

The system reports that the upgrade is underway. After the upgrade file is downloaded and installed, the HCX system reboots. Allow a few minutes for the system to reinitialize.

7 Open the HCX Appliance management interface in a browser tab.

This option may not be available in HCX enabled Public Clouds.

https://hcx-ip-or-fqdn:9443.

8 Navigate to the dashboard and verify the registered systems display a healthy connected state.

9 Open the **System Updates** interface and confirm the **Current Version** is updated.

Results

With the HCX Managers upgraded, the HCX Service Mesh reflects that an update is available.

The HCX Managers will apply the updates, reboot, and become operational in less than five minutes after rebooting. If the HCX Manager does not return to service within that time frame, contact VMware Support.

**Upgrading the HCX Service Mesh Appliances**

The Service Mesh appliances are upgraded independently of the managers. These appliances are flagged for new available updates anytime the HCX Manager has newer software available.

**Prerequisites**

- The site-paired HCX Managers are updated.
- Service Mesh appliances must be initiated using the HCX plug-in at the source site.
- While Service Mesh appliances are upgraded independently to the HCX Manager, they must be upgraded.
Procedure

1. Open the HCX plugin in the vSphere Client.
2. Navigate to the Interconnect tab > Multi-Site Service Mesh > Service Mesh tab.
3. Click View Appliances.
   - Interconnect appliances show a green flag in the Available Versions column if there is an update available.
4. Select each Interconnect appliance that needs to be upgraded.
5. Click Update Appliance.
   - The Update Appliance option is not displayed when there are no available updates.
6. Verify the Current and Available versions are valid.
7. To confirm the operation, click Update.
8. The selected component and its peer component at the destination site are upgraded at the same time. Use the Tasks tab to view the upgrade progress details.

Results

When the Service Mesh appliances reconverge to a Tunnel Up state, the upgrade is complete.

The Interconnect service appliances will apply the updates, reboot, and become operational in less than two minutes after reboots. If the Interconnect services do not return to service within that time frame, contact VMware Support.

Converting Legacy Interconnect to Multi-Site Service Mesh

With the introduction of HCX Multi-Site Service Mesh, support for managing the HCX Interconnect using the HCX Components interface is deprecated.

The HCX Interconnect Multi-Site Service Mesh, introduced in the HCX R121 service update, provides a foundation for the latest features. Upgrading to Multi-site Service Mesh is a requirement for supporting current and future HCX deployments. VMware provides a conversion tool for migrating existing Interconnect deployments to the Multi-Site Service Mesh.

**Note** HCX Multi-Site Service Mesh is unrelated to NSX Service Mesh.

Before Multi-Site Service Mesh, the HCX Interconnect provisioning process included two main steps:

- Creating the Interconnect Configuration (a definition of Compute, Storage, Network resources) on the HCX Cloud Manager in the destination environment.
- Enabling and configuring all the required parameters separately, and then following the deployment of those services to completion.
All this provisioning was done as one monolithic operation using the HCX plugin in the source environment.

Multi-Site Service Mesh improves the provisioning process in many ways:

- Separate configurations are deprecated, replaced by Compute Profiles, Network Profiles, and HCX Service definitions.
- Compute Profile creation is decoupled from the Service Mesh creation (the instantiation of the Interconnect), so deployment configurations can be better planned.
- A Compute Profile can be used with multiple Service Mesh configurations. Connecting to a new HCX remote site can be done by using a previously planned deployment allocation.
- Service Mesh deployments are symmetrical. Compute Profile creation is the same in the HCX Connector and HCX Cloud Manager systems.
- Parallel execution makes provisioning faster (Less than 5 minutes; previously, 15 minutes).

For more information about the benefits of HCX Multi-Site Service Mesh, see About the HCX Multi-Site Service Mesh.

Important Considerations

- All HCX appliances in a Service Mesh MUST be in the same management network. Previously, administrators might deploy appliances in multiple management networks, in which case the conversion might fail. The recommendation is to remove appliances in the legacy HCX Interconnect environment before conversion. Since that implies a service disruption, selection of which appliances to keep depend on how many appliances share the same management network or service priority. Service priority means that layer 2 concentrators (L2C) that extend more VLANs are preferred over concentrators with fewer VLANs or the CGW. After conversion, all the removed services and appliances are redeployed in the new Service Mesh.
- vCloud Foundation may have a limit on the number of hosts, so the addition of the HCX WAN Interconnect (HCX IX) appliance with vMotion services requires an extra host.
- Since Multi-Site Service Mesh is cluster-centric, verify the cluster affinity to ensure that datastores are available on all the hosts targeted for the HCX appliance conversion.
- Conversion to Multi-Site Service Mesh requires a redeployment of the appliance, so a minimal service disruption is expected.
- Distributed firewall rules must be reinstated to allow communication between all the new HCX components, vCenter, and all the ESXi hosts in the cluster.

Converting to Multi-Site Service Mesh

For HCX sites that have been deployed using the HCX Component interface, upgrading to HCX Multi-Site Service Mesh provides enhanced usability, performance, and uniformity for deployments across multiple HCX sites.
The conversion tool creates the Network and Compute Profiles, and Service Mesh configuration. After all Service Mesh related configuration are created, the Interconnect Appliances are converted to Service Mesh and the appliances are redeployed.

Prerequisites

- HCX is running a supported version. All HCX components are upgraded before converting. Refer to the HCX Release Notes.
- System-to-system connections (HCX to vCenter Server, NSX, VCD, or RMQ as applicable) are green, as indicated in the HCX Appliance Management interface (https://hcx-ip-or-fqdn:9443).
- Site pairs are connected as identified using the vCenter HCX Plug-in.
- Appliances are connected as indicated by running the HCX CCLI list command. See Using Central CLI to Connect to VMware HCX Services.
- No upgrade or redeployment operations are running.
- Migration, DR, and Network Extension operations that were in progress are completed, quiesced, or halted.
- In a vCD environment, paired org have a single orgvdc.

Procedure

1. From the HCX plug-in, select Interconnect > HCX Components.
2. Click Upgrade to the Multi-Site Service Mesh.
   The HCX displays a message indicating that the upgrade transforms the current HCX components’ configuration into a Multi-Site Service Mesh configuration. This operation is not reversible.
   The message states that the upgrade operation may require redeploying the service appliances and mentions that there are no migration, DR, Network Extension operations in progress before proceeding with the upgrade.
3. To continue, click YES.
   The Interconnect upgrade begins, displaying each transition state:
   Initiated upgrade of compute and network configuration on endpoints...
   Created service meshes.
   Initiated upgrade of appliances configuration on endpoints...
   Backing up HCX Components and removing...
   Upon completion, the HCX Component interface displays Upgrade Successful, and the Interconnect services disappear from the interface.
5. Verify that the interface displays the converted appliances.
   If all appliances appear in the interface, the upgrade was successful.
Removing VMware HCX

You can remove the HCX service from your environment by uninstalling the site-paired HCX Managers.

HCX supports on-going operations, including application migration and workload rebalancing while servicing the deployment. In the event that HCX needs to be removed, stop all ongoing operations.

The procedure for uninstalling HCX may vary based on your environment and privileges. For deployments involving public clouds, uninstalling HCX may require actions from your cloud service provider.

Uninstalling HCX from VMware Cloud on AWS (VMC) deployments requires removing the service from both source and destination site. It is a self-serviceable process and there are no actions required from VMC.

The process for removing HCX has the following general workflow:

- Stop all migrations and DR protections
- Unstretch the network, which removes Network Extension (HCX-NET-EXT) appliances
- Delete the Service Mesh, which removes Interconnect (HCX-IX) and WAN Optimization (HCX-WAN-OPT) appliances
- Remove site pairing
- Remove the HCX Manager
- Remove the HCX plug-in from the vCenter Server

This chapter includes the following topics:

- Uninstalling VMware HCX
- Uninstalling HCX in VMware Cloud on AWS Deployments
Uninstalling VMware HCX

Uninstalling HCX requires removing the service from both source and destination site.

**Note**  This procedure applies to non-VMC deployments. To uninstall HCX in VMC environments, see Uninstalling HCX in VMware Cloud on AWS Deployments.

A graceful uninstall of HCX appliances is always initiated from the source side. The process requires that HCX is fully functional, including site pairings and communication between source and destination site appliances.

**Prerequisites**

All migrations and replications, including DR operations, are finalized.

**Procedure**

1. Navigate to the HCX Manager Service UI.
2. Verify that no migration or protection operations are running.
3. To remove all network extensions from source-site data centers, complete the following substeps:
   a. Go to **Services > Network Extension**.
   b. Review each stretched network and decide whether you want the network to be connected on the destination site after uninstalling HCX.
   c. Expand each extended network and click **Unextend**.
      The system displays information about the Unextend Network.
   d. Under **Cloud Network**, expand the network entry.
      **Note**  By default, the cloud network is disconnected from the cloud Edge Gateway after the network is unextended. This disconnection is done to prevent an edge gateway with dynamic routing enabled from advertising the route of the network and causing a potential routing conflict with the network in the source site.
   e. (Optional) Use the check boxes to keep the cloud network connected or force unextend the network.
   f. Click **Unextend**.
4. In the HCX system containing the Service Mesh configuration, complete the following substeps to delete all Service Mesh instances:
   a. Go to **Interconnect > Multi-Site Service Mesh > Service Mesh**.
   b. For each Service Mesh, click **DELETE**.
      **Note**  Removing the Multi-Service Mesh from the source site also deletes it from the destination site.
5 To disconnect all HCX site pairings, complete the following substeps:
   a From the HCX dashboard, navigate to Site Pairing.
      For HCX release R131 and earlier, go to Infrastructure > Interconnect > Service Mesh.
      In HCX release R132 and higher, go to Infrastructure > Site Pair.
   b For each site pair, click DISCONNECT.

6 To remove the HCX Manager, complete the following substeps:

   Note For public cloud deployments, contact your cloud service provider to remove HCX.

   a At the destination site, navigate to the vCenter Hosts and Clusters tab.
   b Expand the cluster where the HCX Manager is deployed and locate the virtual machine.
   c Right-click on the HCX entry and power off the selection.
   d Right-click on the HCX entry and select Delete from Disk.
   e Repeat this procedure at the source site.

7 Unregister the HCX Plug-in from the vCenter Server using the instructions on how to remove or disable unwanted plug-ins using the KB article, https://kb.vmware.com/s/article/1025360.

   Note Remove all HCX extensions that include com.vmware.hybridity in the path. Also, remove the following extensions:
      - com.vmware.hcsp.alarm
      - com.vmware.vca.marketing.ngc.ui

Uninstalling HCX in VMware Cloud on AWS Deployments

Uninstalling HCX from VMware Cloud on AWS (VMC) deployments requires removing the service from both source and destination site.

A graceful uninstall of HCX appliances is always initiated from the source side. The process requires that HCX is fully functional, including site pairings and communication between source and destination site appliances.

Prerequisites

All migrations and replications, including DR operations, are finalized.

Procedure

1 Navigate to the HCX Manager Service UI.
2 Verify that no migration or protection operations are running.
3 To remove all network extensions from source-site data centers, complete the following substeps:
   a Go to Services > Network Extension.
   b Review each stretched network and decide whether you want the network to be connected on the cloud side gateway after uninstalling HCX.
   c Expand each extended network and click Unextend. The system displays information about the Unextend Network.
   d Under Cloud Network, expand the network entry.
      Note By default, the cloud network is disconnected from the cloud Edge Gateway after the network is unextended. This disconnection is done to prevent an edge gateway with dynamic routing enabled from advertising the route of the network and causing a potential routing conflict with the network in the source site.
   e (Optional) Use the check boxes to keep the cloud network connected or to force the network to unextend.
   f Click Unextend.

4 For any of the unextended networks that are unused, complete the following substeps to remove them from the destination site:
   Note Unextending networks does not remove them from the destination.
   a Access the VMC management interface: https://console.cloud.vmware.com
   b Select your organization and data center (SDDC).
   c Select Network & Security > Network > Segments.
   d Select the unextended network from the list and click Delete.

5 In the HCX Manager containing the Service Mesh configuration, complete the following substeps to delete all Service Mesh instances:
   Note Removing a Multi-Service Mesh from the source site also deletes it from the destination site.
   a Go to Interconnect > Multi-Site Service Mesh.
   b For each Service Mesh, click Delete.
   c Before proceeding to the next step, check that the Service Mesh no longer appears in the HCX Manager Service UI.
6 To disconnect all HCX site pairings, complete the following substeps:
   a From the HCX dashboard, navigate to **Site Pairing**.
      For HCX release R131 and earlier, go to **Infrastructure > Interconnect > Service Mesh**.
      In HCX release R132 and higher, go to **Infrastructure > Site Pair**.
   b For each site pair, click **Disconnect**.

7 (DX only) To remove direct connect private interfaces from the destination (VMC) site, complete the following substeps:
   a Access the VMC management interface: `https://console.cloud.vmware.com`
   b Select your organization and data center (SDDC).
   c Select **Add Ons**.
   d Navigate to the SDDCs tab and click **Open HCX**.
   e Enter the `cloudadmin@vmc.local` user and credentials and click **Log In**.
   f Navigate to the **Infrastructure > Interconnect**.
   g Click the **Network Profiles** tab.
   h Select the direct connect network profile and click **Edit**.
   i Clear the IP ranges, Prefix length, and Gateway address.
   j Click **Update**.

8 To remove HCX Manager from the destination (VMC) site, complete the following substeps:

   **Note** For deployments between HCX enabled clouds on VMC (cloud-to-cloud), repeat this procedure at the source site.
   a Access the VMC management interface: `https://console.cloud.vmware.com`
   b Select your organization and data center (SDDC).
   c Click **Add Ons**.
      The system displays all SDDCs with HCX deployed.
   d Click **Undeploy HCX**.
      VMC automation cleans up SDDC HCX Manager services and removes the HCX Cloud Manager.

9 To remove HCX Connector on-premise, complete the following substeps:

   **Note** For cloud-to-cloud deployments using VMC, skip this step. This step applies only in on-premise to VMC deployments.
   a Navigate to the vCenter **Hosts and Clusters** tab.
   b Expand the cluster where the HCX Manager is deployed and locate the virtual machine.
c  Right-click on the HCX Manager virtual machine and power off the selection.

d  Right-click on the HCX Manager virtual machine and select **Delete from Disk**.

10  Unregister the HCX Plug-in from the vCenter Server using the instructions on how to remove or disable unwanted plug-ins using the KB article, [https://kb.vmware.com/s/article/1025360](https://kb.vmware.com/s/article/1025360).

Remove all HCX extensions that include com.vmware.hybridity in the path. Also, remove entries with the following extensions:

- com.vmware.hcsp.alarm
- com.vmware.vca.marketing.ngc.ui
The following sections contain common VMware HCX troubleshooting scenarios, troubleshooting methodology, general information collection, and how to use built in diagnostic tools like the VMware HCX Central CLI.

This chapter includes the following topics:

- Enabling SSH on the VMware HCX Manager
- Logging in to the VMware HCX Manager Shell
- Locating the VMware HCX System IDs Using VMware HCX Manager Shell
- Locating the VMware HCX System IDs Using VMware HCX Plug-In
- Using Central CLI to Connect to VMware HCX Services
- Gathering VMware HCX Technical Support Logs from the VMware HCX Plug-In
- Gathering VMware HCX Technical Support Logs from the VMware HCX Appliance Management
- Viewing Logs in the VMware HCX Manager Shell
- VMware HCX Manager Services from the VMware HCX Appliance Management Interface
- VMware HCX Manager Services from the VMware HCX CLI
- Viewing VMware HCX System State
- Viewing VMware HCX-Related Entries in the vSphere Task Console
- Enabling the VMware HCX Central CLI

### Enabling SSH on the VMware HCX Manager

This section describes how to enable the **SSH Service** on the HCX Manager to access to the command-line interface.

To access to the HCX Manager shell, use a VMware Remote Console session in the vSphere Client or establish an SSH session. If the **SSH Service** was not enabled during the initial HCX Manager installation, you must first enable it:

**Procedure**


---

VMware, Inc.
2. Go to **Appliance Summary**.
3. Under System Level Services, locate the **SSH Service**.
4. Click **Start**.

---

**Logging in to the VMware HCX Manager Shell**

This topic contains information on how to connect to the HCX Manager shell.

**Prerequisites**

You can log in to the HCX Manager shell using VMRC or an SSH session. The first-level access uses the admin account created during the initial installation of the HCX Manager. If requested to do so by support, you can switch the User to root once you log in with the admin account.

**Procedure**

1. Connect to the HCX Manager using VMRC or SSH.
2. When prompted for credentials, enter `admin` as the user name and password.
3. Switch to root by typing `su root` and providing the `root password`. 
Locating the VMware HCX System IDs Using VMware HCX Manager Shell

When working with support, you may have to provide the VMware HCX System IDs. You can get the IDs from the VMware HCX plug-in and from the HCX Manager shell.

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

Locating the VMware HCX System IDs Using VMware HCX Plug-In

When working with support, you may have to provide the VMware HCX System IDs. The IDs can be obtained from the VMware HCX plug-in and from the HCX Manager shell.

Procedure
1. In the vSphere Web Client, navigate to the VMware HCX plug-in > Administration > System Updates.
2. Under Local HCX, in the Info column, click the (information) icon. Doing so copies the System ID to your clipboard. Do the same to obtain the Remote HCX System ID.
3. Note the IDs and provide them to VMware when requested.
Using Central CLI to Connect to VMware HCX Services

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

Procedure

1. Enable CCLI on the HCX Manager: ccli.
2. Type list to view a list of VMware HCX nodes.
3. Identify the VMware HCX Node ID for the VMware HCX service to which you want to connect.
4. Type go # where # is the node ID.
5. Type ssh.
6. Use the help command to display available commands.

Gathering VMware HCX Technical Support Logs from the VMware HCX Plug-In

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

Procedure

1. From the HCX Manager Service UI, navigate to the log options at > Administration > Troubleshooting > Download Log Bundles.

Note From the HCX Appliance Management interface, navigate to Administration > Troubleshooting > Technical Support Logs.
Gathering VMware HCX Technical Support Logs from the VMware HCX Appliance Management

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

**Procedure**

2. Navigate to **Administration > Troubleshooting > Technical Support Logs**.
3. Select the box next to one or more logs that you want to generate.
4. Click **Generate**.
5. After the bundle is prepared, you are prompted to download them.

Viewing Logs in the VMware HCX Manager Shell

VMware HCX service logs are useful when troubleshooting failures.

**Prerequisites**

There are two key logs in 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 VMware HCX Web Engine service. The process requires a good understanding of the VMware HCX system so it is best to review with a VMware support engineer.

**Procedure**

1. Use VMRC or SSH to connect to the HCX Manager shell.
2. Switch user to root: `su -`.
3. Change directory to `/common/logs/admin`.
4. From within this directory, you can open the relevant logs using standard Linux text commands.
5. When troubleshooting failures, search using keywords such as Fail, ERROR, exception, migration.
VMware HCX Manager Services from the VMware HCX Appliance Management Interface

Managing HCX services from the Appliance Management interface.

Prerequisites

There are several HCX Manager services critical for VMware HCX operations. Two key services to observe are the Application Engine and the Web Engine.

When working with support, you may have to confirm that these services running or may have to restart them. The HCX Manager services can be viewed and restarted in several places.

**Important** Do not restart services unless directed to do so by VMware Global Support Services.

Procedure

2. Navigate to **Appliance Summary**.
3. You can find all services and can monitor or restart them. The only two services that are optional are the SNMP and SSH services. All others must always be running.

VMware HCX Manager Services from the VMware HCX CLI

You can manage the HCX service using the VMware HCX CLI.

Procedure

1. VMRC or SSH into the HCX Manager.
2. Switch user to root: `su -`. 
3 Type `systemctl action service_name`.
   - Action can be status, stop, start, restart.
   - Service name can be that of a web-engine or an app-engine.

```
systemctl status web-engine
systemctl status app-engine
systemctl stop web-engine
systemctl restart web-engine
```

### Viewing VMware HCX System State

You can view the HCX system state from the appliance management dashboard.

**Prerequisites**

For HCX to run properly, it is important that it has sufficient available resources. You can view the key system resources such as CPU, memory, and storage from the Dashboard section in the HCX Appliance Management interface. The dashboard section also provides other useful information such as 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: `https://<hcx-ip-or-fqdn>:9443`
2. Navigate to **Dashboard**.
3. Review the CPU, Memory, Storage, Uptime, and Version.
Viewing VMware HCX-Related Entries in the vSphere Task Console

Most VMware HCX Operations such as the initial appliance deployment, extending a network, or a migration can be monitored from the vSphere Web Client Task Console.

Procedure

1. Open the vSphere Web Client and navigate to **Home**.
2. Navigate to **Tasks**.
3. In the Task Console, filter the results by using **HCX** in the search filter.
4. Look for any failures or errors. If you see an error, you can review the logs to find additional details.

Enabling the VMware HCX Central CLI

The VMware HCX Central CLI is used for diagnostic information collection and secure connections to the Service Mesh.

The Central CLI on VMware HCX allows you to run commands available centrally on the HCX Manager to view run time state for HCX services. The Central CLI reduces troubleshooting time by providing centralized diagnostics and improves the security posture of the Service Mesh appliances by eliminating the need to run the SSH service on them. To use it, first you must enable the Central CLI on the VMware HCX Manager.

Procedure

1. Use VMRC or SSH to connect to the VMware HCX Manager shell.
2. Switch user to root: **su -**.
3. Type **ccli**.
   - The VMware HCX Central CLI is now enabled.
4. Begin using it by exploring the **p** command output.
Monitoring VMware HCX Systems

VMware HCX native tools and views can be used to collect the current state of the system and general system health. Also, VMware HCX can be integrated with vRealize Log Insight and vRealize Operations using Management Pack.

This chapter includes the following topics:

- Understanding the HCX Manager Dashboard
- vRealize Operations Management Pack for HCX
- DICE Integration for HCX

Understanding the HCX Manager Dashboard

The Dashboard provides a summary of HCX operations, data center locations, resource usage, status, and activity.

The Dashboard is the first screen that appears when you open the HCX Service UI.
The Dashboard highlights various HCX functions in a set panels, and in some cases allows you to change settings related to those panels.

**Note** For HCX installations where the vCenter Servers are in linked-mode, the Dashboard includes information from all vCenter Servers registered to an HCX system.

<table>
<thead>
<tr>
<th>Panel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Overview</td>
<td>Lists HCX operations:</td>
</tr>
<tr>
<td></td>
<td>- Number of virtual machines migrated</td>
</tr>
<tr>
<td></td>
<td>- Number of migrations in progress</td>
</tr>
<tr>
<td></td>
<td>- Number of scheduled migrations not started</td>
</tr>
<tr>
<td></td>
<td>- Number of extended networks</td>
</tr>
<tr>
<td></td>
<td>- Number of protected virtual machines for business continuity</td>
</tr>
<tr>
<td>Site Pairs</td>
<td>Displays connected site pairs and lists the pair status, Up or Down.</td>
</tr>
<tr>
<td></td>
<td>To create a new site pair, click New Site Pairing. To view detailed instructions for adding a site pair, see <a href="#unique_112">Adding a Site Pair</a>.</td>
</tr>
<tr>
<td>Active Migrations</td>
<td>Displays ongoing migrations for the selected HCX system.</td>
</tr>
<tr>
<td></td>
<td>Use the pull-down menu to change the source site.</td>
</tr>
<tr>
<td>Migrations Overview</td>
<td>Summarizes completed migrations for the selected HCX system.</td>
</tr>
<tr>
<td></td>
<td>Use the date pull-down menu to display migrations for a specified period:</td>
</tr>
<tr>
<td></td>
<td>- Last 6 Months</td>
</tr>
<tr>
<td></td>
<td>- Last 3 Months</td>
</tr>
<tr>
<td></td>
<td>- This Month</td>
</tr>
<tr>
<td>Cloud Resource Usage</td>
<td>For the selected source system, provides a summary view of resource usage for the site pair.</td>
</tr>
<tr>
<td></td>
<td>Use the pull-down menu to change the source site.</td>
</tr>
<tr>
<td>Alerts</td>
<td>Provides a comprehensive list of logged Alert messages: Critical, Warning, Info.</td>
</tr>
<tr>
<td></td>
<td>For a description of Alert messages and available actions, see #unique_112.</td>
</tr>
<tr>
<td>Activity Logs</td>
<td>For the selected source system, displays a historical log of system tasks:</td>
</tr>
<tr>
<td></td>
<td>- Job Type</td>
</tr>
<tr>
<td></td>
<td>- Entity Name</td>
</tr>
<tr>
<td></td>
<td>- Percentage of task completed.</td>
</tr>
<tr>
<td></td>
<td>- Task status</td>
</tr>
<tr>
<td></td>
<td>- Task Start Time</td>
</tr>
<tr>
<td></td>
<td>- Task Completion Time</td>
</tr>
<tr>
<td></td>
<td>Select from the pull down menus to change the source site or display tasks by status (All, Running, Failed).</td>
</tr>
<tr>
<td></td>
<td>Use the search field to identify specific tasks or groups of tasks.</td>
</tr>
</tbody>
</table>
vRealize Operations Management Pack for HCX

The Management Pack (MP) for HCX adds monitoring capabilities with integrated dashboards and reports. It triggers problem alerts for the HCX services.

The Management Pack for HCX extends the Operations Management capabilities of vRealize Operations for HCX Hybrid Mobility, Interconnect Management and Data Center and Cloud Migrations.

Installing the HCX Management Pack

The Management Pack for HCX is downloaded from the VMware Solutions Exchange and added to an existing vRealize Operations installation.

Prerequisites

- You have a my.vmware.com account to download the management pack.
- The MP requires vRealize Operations version 6.6.1 or above. See the VMware Interoperability Matrix.
- The vRealize Operations Manager connects to HCX Manager systems using TCP-443 when they are added with the VROPS HCX Management Pack.

Procedure

1. Navigate to the VMware Solutions Exchange.
2. Locate the Management Pack for HCX version 5.0.
3. Log in using my.vmware.com credentials.
4. To download the Management Pack, click the Try button.
5. On the Download window, click Proceed.
6. Log in to the vRealize Operations Manager user interface with administrator privileges.
7. Navigate to Administration > Solutions.
8. On the Solutions tab, click the plus icon.
10. Click Upload. After the upload, click Next.
11. Accept the EULA, click Next.
12. After the installation is finished, click Finish.

The Management Pack is listed as a solution.
13 Use the cogs icon to Manage the HCX Solution.

14 Use the green plus icon to add an HCX adapter instance.

15 Connect the Management Pack to the HCX Manager system using its IP or FQDN.

16 Authenticate to the HCX system using a vSphere SSO-integrated user with access to HCX.

After sufficient metrics are collected, the vRealize Operations dashboards are populated with views based on enabled HCX services.

Viewing the HCX Adapter Logs

Adapter Logs are useful when diagnosing issues with the Management Pack for HCX.

Prerequisites

- Administrative access to the vRealize Operations Manager.
- The Management Pack for HCX is listed in Solutions.

Procedure

1 In the vRealize Operations Manager, navigate to the Administration tab.

2 On the left side navigator, expand Support and click Logs.

3 In the file navigator, expand the MASTER folder > Collector > Adapter > HCXAdapter.
4 Select the log and click GO.

What to do next

To download logs, use Support Bundles on the left side navigator.

Management Pack for HCX Reference Topics

The Management Pack dashboards, alerts, and metrics are listed for reference.

HCX MP Alerts

List of possible HCX Alerts, and their severity.

HCX services are using trial period limits. To remove the limits, activate HCX. – Warning

The HCX trial period has ended. To continue using services, activate HCX. - Critical

The HCX Manager is unable to reach https://connect.hcx.vmware.com. This connection is required for authorization, critical updates, and support. - Warning

The HCX Manager has failed to reach https://connect.hcx.vmware.com beyond the grace period. To resume HCX services, restore this connection . - Critical

Site Pair Link Status is not OK. - Immediate

Site Pair Remote Status is not OK. - Immediate

Interconnect Service Status is Down. - Critical

vMotion Service Status is Down. - Critical

Disaster Recovery Service Status is Down. - Critical

Bulk Migration Service Status is Down. - Critical

Network Extension Service Status is Down. - Critical

WANOPT Service Status is Down. - Critical

VM Migration status is Failed. - Immediate

Hybrid Interconnect Service Pipeline Status is down. - Critical
Hybrid Interconnect Service Transport Status is down. - Critical
Hybrid Interconnect Service Encryption Tunnel Status is down. - Critical
Hybrid Interconnect Service service is not running. - Critical
Hybrid Interconnect Service System State is Fatal. - Critical
Hybrid Interconnect Service System State is Critical. - Critical
High Throughput Network Extension service is not running. - Critical
Network Extension Service System State is Fatal. - Critical
Network Extension Service System State is Critical. - Critical
Network Extension Service Pipeline Status is down. - Critical
Network Extension Service Transport Status is down. - Critical
Network Extension Service Encryption Tunnel Status is down. - Critical
WAN Optimization Service is not running.- Critical
Hybrid Interconnect Service Tunnel is down. - Warning
High Throughput Network Extension Tunnel is down. - Warning
All tunnels on Hybrid Interconnect Service are down. - Critical
All tunnels on High Throughput Network Extension are down. - Critical
Hybrid Interconnect Service status is degraded. - Info
Hybrid Interconnect Service Pipeline Status is degraded. - Info
Hybrid Interconnect Service Transport Status is degraded. - Info
Hybrid Interconnect Service Encryption Tunnel Status is degraded. - Info
Network Extension Service status is degraded. - Info
Network Extension Service Pipeline Status is degraded. - Info
Network Extension Service Transport Status is degraded. - Info
Network Extension Service Encryption Tunnel Status is degraded. - Info
Hybrid Interconnect Service Tunnel status is degraded. - Info
Network Extension Service Tunnel status is degraded. - Info
WAN Optimization Service is degraded. - Info
Hybrid Interconnect Service status is unknown. - Warning
Hybrid Interconnect Service Pipeline Status is unknown. - Warning
Hybrid Interconnect Service Transport Status is unknown. - Warning
Hybrid Interconnect Service Encryption Tunnel Status is unknown. - Warning
High Throughput Network Extension service status is unknown. - Warning
Network Extension Service Pipeline Status is unknown. - Warning
Network Extension Service Transport Status is unknown. - Warning
Network Extension Service Encryption Tunnel Status is unknown. - Warning
Hybrid Interconnect Service Tunnel status is unknown. - Warning
High Throughput Network Extension Tunnel status is unknown. - Warning
WAN Optimization Service status is unknown. - Warning
Incoming replication is in error state. - Critical
Outgoing Replication is in error state. - Critical
Incoming Replication has an RPO violation. - Warning
Outgoing Replication has an RPO violation. - Warning

**HCX MP Dashboards**

Descriptions for the vROPS HCX dashboards added when the MP for HCX is installed.

**HCX Environment Overview**

<table>
<thead>
<tr>
<th>Widget 1</th>
<th>HCX Environments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Widget 2</td>
<td>Interconnect Topology</td>
</tr>
<tr>
<td>Widget 3</td>
<td>Metrics</td>
</tr>
<tr>
<td>Widget 4</td>
<td>Alerts</td>
</tr>
</tbody>
</table>

**HCX Extended Networks**

<table>
<thead>
<tr>
<th>Widget 1</th>
<th>HCX Environments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Widget 2</td>
<td>Extended Networks Topology</td>
</tr>
<tr>
<td>Widget 3</td>
<td>Metrics</td>
</tr>
</tbody>
</table>

**HCX Migrations**

<table>
<thead>
<tr>
<th>Widget 1</th>
<th>Recent Completed Migrations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Widget 2</td>
<td>Ongoing Migrations</td>
</tr>
<tr>
<td>Widget 3</td>
<td>Recent Error Migrations</td>
</tr>
</tbody>
</table>

**HCX Disaster Recovery**

<table>
<thead>
<tr>
<th>Widget 1</th>
<th>Incoming Replications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Widget 2</td>
<td>Outgoing Replications</td>
</tr>
<tr>
<td>Widget 3</td>
<td>Replications by Status</td>
</tr>
<tr>
<td>Widget 4</td>
<td>Replications with RPO Violation</td>
</tr>
</tbody>
</table>
## HCX MP Metrics

Descriptions for the vROPS HCX Metrics available with the MP for HCX.

### Resource: Site Pairing (HCX Adapter)

<table>
<thead>
<tr>
<th>Metric Group</th>
<th>Metric Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration</td>
<td>Average Rate of Data Migrated</td>
</tr>
<tr>
<td>Migration</td>
<td>Average Time Taken per Migration (mins)</td>
</tr>
<tr>
<td>Migration</td>
<td>Distribution of Successful Migrations</td>
</tr>
<tr>
<td>Migration</td>
<td>Distribution of Failed Migrations</td>
</tr>
</tbody>
</table>

### Resource: Migration (HCX Adapter)

<table>
<thead>
<tr>
<th>Metric Group</th>
<th>Metric Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>LWD, LWD In Progress, NFC, NFC In Progress</td>
<td>Received Traffic</td>
</tr>
<tr>
<td>LWD, LWD In Progress, NFC, NFC In Progress</td>
<td>Received Operations</td>
</tr>
<tr>
<td>LWD, LWD In Progress, NFC, NFC In Progress</td>
<td>Received Throughput</td>
</tr>
<tr>
<td>LWD, LWD In Progress, NFC, NFC In Progress</td>
<td>Transmitted Traffic</td>
</tr>
<tr>
<td>LWD, LWD In Progress, NFC, NFC In Progress</td>
<td>Transmitted Operations</td>
</tr>
<tr>
<td>LWD, LWD In Progress, NFC, NFC In Progress</td>
<td>Transmitted Throughput</td>
</tr>
<tr>
<td>LWD, LWD In Progress, NFC, NFC In Progress</td>
<td>Error Count</td>
</tr>
<tr>
<td>Progress Info</td>
<td>Progress</td>
</tr>
<tr>
<td>Progress Info</td>
<td>Rate of Transfer</td>
</tr>
<tr>
<td>Progress Info</td>
<td>Checksum Total</td>
</tr>
<tr>
<td>Progress Info</td>
<td>Checksum Compared</td>
</tr>
<tr>
<td>Summary</td>
<td>Instances Completed</td>
</tr>
<tr>
<td>Summary</td>
<td>Instances Aborted</td>
</tr>
<tr>
<td>Summary</td>
<td>Images Created</td>
</tr>
<tr>
<td>Summary</td>
<td>Disks Configured</td>
</tr>
<tr>
<td>Summary</td>
<td>Group Errors</td>
</tr>
<tr>
<td>Summary</td>
<td>Source Migration State</td>
</tr>
<tr>
<td>Summary</td>
<td>Destination Migration State</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Migration Start Time</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Migration End Time</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Source Datacenter Name</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Destination Datacenter Name</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Time Taken (minutes)</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>VM Size</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Status</td>
</tr>
<tr>
<td>Metric Group</td>
<td>Metric Name</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Protocol</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Latest State at Source</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Latest State at Destination</td>
</tr>
</tbody>
</table>

**Resource: vMotion (HCX Adapter)**

<table>
<thead>
<tr>
<th>Metric Group</th>
<th>Metric Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Progress Info</td>
<td>Progress</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Migration Start Time</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Migration End Time</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Source Datacenter Name</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Destination Datacenter Name</td>
</tr>
<tr>
<td>Summary</td>
<td>Time Taken (minutes)</td>
</tr>
<tr>
<td>Summary</td>
<td>VM Size</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Estimated Completion Time</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Status</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Protocol</td>
</tr>
</tbody>
</table>

**Resource: RAV Migration (HCX Adapter)**

<table>
<thead>
<tr>
<th>Metric Group</th>
<th>Metric Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Progress Info</td>
<td>Progress</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Migration Start Time</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Migration End time</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Source Datacenter Name</td>
</tr>
<tr>
<td>Summary</td>
<td>Time Taken (minutes)</td>
</tr>
<tr>
<td>Summary</td>
<td>VM Size</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Estimated Completion Time</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Status</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Protocol</td>
</tr>
</tbody>
</table>

**Resource: OsAssistedMigration (HCX Adapter)**

<table>
<thead>
<tr>
<th>Metric Group</th>
<th>Metric Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Progress Info</td>
<td>Progress</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Migration Start Time</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Migration End Time</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Source Datacenter Name</td>
</tr>
<tr>
<td>Summary (P)</td>
<td>Destination Datacenter Name</td>
</tr>
</tbody>
</table>
The Data Integrated Customer Engagement (DICE) tool uses customer utilization data to model the business benefits of VMware software-defined data center (SDDC) products. Through integration with DICE, you can upload the host and virtual machine inventory of the vCenter Server registered with an HCX.

Contact your account team for help with configuring and using this feature.
Prerequisites

Firewall rules allow access to the DICE portal through port 443.

Procedure

1. Navigate to the HCX Dashboard and select Administration > DICE.

The system displays the DICE configuration page.

2. Enter the DICE configuration parameters:

<table>
<thead>
<tr>
<th>DICE Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Key</td>
<td>Provides API key information for REST authentication with the DICE portal. Obtain this key from the DICE website under Account Settings in your profile.</td>
</tr>
<tr>
<td>API Secret</td>
<td>Provides API secret key information for REST authentication with the DICE portal. Obtain this secret from the DICE website under Account Settings in your profile.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you must change any of the DICE parameters in the future, you must reenter the secret key.</td>
</tr>
<tr>
<td>Customer ID</td>
<td>Obtain this ID from your account team.</td>
</tr>
<tr>
<td>Model ID</td>
<td>(Optional) Assigned by DICE after the first time you upload the inventory. The Model ID is unique to each HCX.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the Model ID is deleted from the DICE inventory, edit the configuration to remove the Model ID, and upload the inventory again.</td>
</tr>
</tbody>
</table>

3. Click **Save**.

4. Click **Upload VC Inventory to DICE**.

The HCX uploads the vCenter virtual machine and host inventory. In the DICE portal, a new model is created in the Library, and this Model ID is displayed in the HCX screen.

**Note** The time it takes to complete the upload depends on the size of the vCenter inventory. To refresh the inventory for the Model ID in the future, click **Upload VC Inventory to DICE** again.

What to do next

Conduct periodic updates once migrations and project milestones are completed to show the overall transformation progress. To compare results before and after, navigate to **Value Realization > Infrastructure Tracking**. Work with your account team for performing analysis on the Model in the DICE portal.
VMware HCX in the VMware Cloud on AWS

VMware HCX enables cloud on-boarding without retrofitting your source infrastructure, supporting migration from vSphere 5.0+ to VMware Cloud on AWS (VMC) without introducing application risk and complex migration assessments.

This chapter includes the following topics:

- Deploying HCX from the VMC Console
- Overview of VMware HCX on NSX for vSphere-Backed SDDCs
- Overview of VMware HCX on NSX-T Backed VMC SDDCs
- Configuring VMware HCX for Direct Connect Private Virtual Interfaces

Deploying HCX from the VMC Console

VMware HCX is an add-on to the VMC SDDC. After enabling the add-on from the VMC console, the HCX Cloud components are deployed and the HCX plug-in is available in the vSphere Client.

Prerequisites

- The user performing this procedure must have access to the VMC Console.

Procedure

1. Log in to the VMC Console at vmc.vmware.com.
2. On the Add Ons tab of your SDDC, click Open HCX on the HCX card.

   The VMware HCX interface opens.
3. Navigate to the SDDCs tab and click Deploy HCX and click Confirm to initiate the deployment.

   The VMC activation is created and displayed, and the deployment begins. This step takes several minutes to complete. After the deployment is complete, hcx_cloud_manager appears in the vCenter console.
4. On the Add Ons tab of your SDDC, click Open HCX on the HCX card.
5. Navigate to the SDDCs tab and click Open HCX.

   The VMware HCX Cloud service interface opens, the URL reads https://hcx.sddc.*.vmwarevmc.com.
6 Enter the cloudadmin@vmc.local user and credentials and click Log In.

Results

The Administration tab System Updates can now be used to download the HCX Connector OVA, which is needed for the on-premises HCX installation. The on-premises deployment is detailed in Chapter 6 Installing the System.

Overview of VMware HCX on NSX for vSphere-Backed SDDCs

VMware Cloud on AWS SDDCs backed by NSX for vSphere and SDDCs backed by NSX-T support different sets of features. This section describes the behavior and features of VMware HCX services on the SDDCs employing the network support functionality provided by NSX for vSphere.
Supported VMware HCX Features with NSXv SDDCs

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
</table>
| VMware HCX Virtual Machine Migrations | - VMware HCX vMotion for serial migrations.  
                                        - VMware HCX Bulk Migration for scheduled, replication-based, parallel migrations.  
                                        - VMware HCX Cold Migrations for powered-off virtual machines.  
                                        - VMware HCX Replication-Assisted vMotion is available with VMware HCX on VMC. |
<p>| VMware HCX WAN Optimization      | - Deduplication, compression, and line conditioning of VMware HCX migration and protection network flows. |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware HCX Network Extension</td>
<td>- Network Extension with Proximity Routing is not currently available with VMware Cloud on AWS NSXv or NSX-T SDDCs.</td>
</tr>
<tr>
<td>VMware HCX over AWS Direct Connect</td>
<td>- VMware HCX supports connections over AWS Direct Connect only by employing a Public Virtual Interface.</td>
</tr>
<tr>
<td></td>
<td>- VMware HCX does not require a special configuration to deploy connectivity to a Public Virtual Interface. The relevant AWS region subnets, which are communicated to the premises router, contain the required VMware HCX component EIPs.</td>
</tr>
<tr>
<td></td>
<td>- For more detail, see Using AWS Direct Connect with VMware Cloud on AWS.</td>
</tr>
</tbody>
</table>

### Overview of VMware HCX on NSX-T Backed VMC SDDCs

This section describes the behavior and features of VMware HCX services on the SDDCs operating with a set of network connectivity features provided by NSX-T.

### Summary of Changes to VMware HCX for NSX-T Operations in Support of VMC SDDCs

- Updated component architecture uses the NSX Service Insertion Framework.
- The AWS Direct Connect with Private Virtual Interface is now supported. User-defined Private IP Subnets can be used during the VMware HCX Interconnect configuration.
- Network Extension L2 bridging is done with MAC Address learning on the Network Extension L2 switch port.
VMware HCX Architecture of SDDCs Supported by NSX-T

VMware HCX Features of SDDCs Supported by NSX-T

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware HCX Virtual Machine Migrations</td>
<td>- VMware HCX vMotion for serial migrations.</td>
</tr>
<tr>
<td></td>
<td>- VMware HCX Bulk Migration for scheduled, replication-based, parallel migrations.</td>
</tr>
<tr>
<td></td>
<td>- VMware HCX Cold Migrations for powered-off virtual machines.</td>
</tr>
<tr>
<td></td>
<td>- VMware HCX Replication-Assisted vMotion is available with VMware HCX on VMC.</td>
</tr>
<tr>
<td>VMware HCX WAN Optimization</td>
<td>- Deduplication, compression, and line conditioning of VMware HCX migration and protection network flows.</td>
</tr>
</tbody>
</table>
### Feature Details

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
</table>
| VMware HCX Network Extension | - A maximum of eight networks can be extended to the SDDC per VMware HCX Network Extension appliance.  
- After a Network Extension operation, there is a five minute delay until the network is available for a migration operation.  
- Network Extension with Proximity Routing is not currently available with NSX-T SDDCs. |
| VMware HCX over AWS Direct Connect | - VMware HCX supports connections over AWS Direct Connect with a Private Virtual Interface. |

### Configuring VMware HCX for Direct Connect Private Virtual Interfaces

The private virtual interface allows VMware HCX migration and network extension traffic to flow over the Direct Connect connection between your on-premises or cloud source environment and your destination SDDC.

**Caution** Ensure the IP Address Range configured does NOT overlap with any other IP range already in use for any other service in VMC. This can cause routing and network reachability issues for those other components.

### Prerequisites

- The AWS Direct Connect with Private Virtual Interface is only supported on VMC SDDC backed by NSX-T networking.
- The SDDC must be configured to use the Direct Connect Private Virtual Interface.
  
  See [Using AWS Direct Connect with VMware Cloud on AWS](#).
- A private subnet that can be reached from on-premises over the Direct Connect with Private VIF, ideally reserved for VMware HCX component deployments.
- Existing VMware HCX Interconnect, Optimization Network Extension appliances must be removed before beginning this configuration.
  
  See [Removing VMware HCX Interconnect Virtual Appliances](#).

### Procedure

1. Log in to the VMC Console at vmc.vmware.com.
2. Select your organization and data center (SDDC).
3. Select Add Ons.
4. Click OPEN HCX on the HCX card.
5. Navigate to the SDDCs tab and click OPEN HCX.
6. Enter the cloudadmin@vmc.local user and credentials and click LOG IN.
7. Navigate to the Infrastructure > Interconnect.
8. Click the **Network Profiles** tab.

9. In the Direct Connect network profile template, click **Edit**.

10. Enter the private IP address ranges reserved for VMware HCX.

11. Enter the Prefix Length and the Gateway IP address.

12. Click **Update**.

**Results**

When the Service Mesh is deployed, it uses the Uplink Network Profile, private IP addresses assigned by the user. The assigned IPs will be reachable over the AWS Direct Connect.

**Figure 16-1. VMware HCX over Direct Connect Private Virtual Interface**