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

https://docs.vmware.com/
Contents

About the VMware HCX User Guide 7

1 VMware HCX Overview 8

2 VMware HCX Services 10

3 VMware HCX Components 12

4 VMware HCX Deployment Types 15

5 Preparing for HCX Installations 17
   System Requirements for HCX 17
   Software Version Requirements 18
   HCX Support Policy for Vacating Legacy vSphere Environments 20
   Network Port and Protocol Requirements 20
   Using the HCX Interface 21
   HCX Activation and Licensing 21
      Activating or Licensing New HCX Systems 21
      Updating an HCX Evaluation License Key 23
      Removing or Adding the HCX Enterprise Upgrade Key 24
   NSX Requirements for HCX Deployments 25
      NSX Requirements for HCX Appliance Deployments 25
      NSX Requirements for the HCX Connector Installation 26

6 Installing the System 27
   HCX Installation Workflow 27
      HCX Installation Workflow for HCX Public Clouds 27
      HCX Installation Workflow for vSphere Private Clouds 29
      HCX Installation Workflow for vCloud Director Private Clouds 29
   Downloading the HCX OVAs 30
      Downloading the Installer OVA 30
      Downloading the HCX Connector OVA 31
   Deploying the Installer OVA in the vSphere Client 31
   Activating and Configuring HCX 32

7 Configuration and Service Limits for VMware HCX 42

8 Configuring and Managing the HCX Interconnect 43
Overview of the HCX Interconnect Services Deployment with Multi-Site Service Mesh 43
Configuring and Managing the HCX Interconnect with the Multi-Site Service Mesh 44
About the HCX Multi-Site Service Mesh 44
Adding a Site Pair 47
Creating a Network Profile 49
Creating a Compute Profile 52
Creating a Service Mesh 59
Synchronizing the Multi-Site Service Mesh 62
Sentinel Management 62
Downloading and Installing HCX Sentinel Agent Software 62
Uninstalling HCX Sentinel Agent Software 63
Upgrading HCX Sentinel Agent Software 64

9 Extending Networks with VMware HCX 66
About VMware HCX Network Extension 66
Requirements for Network Extension 67
Restrictions and Limitations for Network Extension 68
Network Extension to Destinations with Universal Distributed Logical Routers 69
Importing Routers for Network Extension with NSX-V 70
Extending Networks Using VMware HCX 70
Removing a Network Extension 72
HCX Network Extension with Mobility Optimized Networking for NSX-T 73
Understanding HCX Mobility Optimized Networking 74
Limitations for HCX Mobility Optimized Networking 75
Configuring HCX Mobility Optimized Networking 76
Configuring Policy Routing for Mobility Optimized Networking 78

10 Migrating Virtual Machines with VMware HCX 80
VMware HCX Migration Types 80
Understanding VMware HCX Bulk Migration 81
Understanding VMware HCX vMotion and Cold Migration 83
Understanding VMware HCX Replication Assisted vMotion 85
Understanding VMware HCX OS Assisted Migration 88
Architectural Considerations for OSAM Deployment 90
OS Assisted Migration Limitations 90
Migrating Virtual Machines with HCX 94
Monitoring Migrations with HCX 96
Canceling a Migration with HCX 96
Managing Failed or Canceled Migrations 97
Clearing the Migration History 97
Migrating Virtual Machines with Mobility Groups 98
<table>
<thead>
<tr>
<th>11 Protecting Virtual Machines with VMware HCX</th>
<th>105</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware HCX Disaster Recovery</td>
<td>105</td>
</tr>
<tr>
<td>Planning for HCX Protection</td>
<td>106</td>
</tr>
<tr>
<td>Enabling DR Protection for a Virtual Machine</td>
<td>109</td>
</tr>
<tr>
<td>Performing a Virtual Machine Test Recovery</td>
<td>111</td>
</tr>
<tr>
<td>Performing a Virtual Machine Recovery</td>
<td>111</td>
</tr>
<tr>
<td>VMware HCX Disaster Recovery - Protect Operations for VMs</td>
<td>112</td>
</tr>
<tr>
<td>HCX Integration with Site Recovery Manager</td>
<td>112</td>
</tr>
<tr>
<td>Enabling SRM Integration in HCX</td>
<td>113</td>
</tr>
<tr>
<td>Protecting VMs with SRM Integration Enabled</td>
<td>113</td>
</tr>
<tr>
<td>Performing Test and Recovery Operations Using SRM Integration</td>
<td>113</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12 Managing System Settings</th>
<th>115</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding the Appliance Management Dashboard</td>
<td>115</td>
</tr>
<tr>
<td>Updating the Time Settings</td>
<td>117</td>
</tr>
<tr>
<td>Updating the System Name</td>
<td>118</td>
</tr>
<tr>
<td>Managing CA and Self-Signed Certificates</td>
<td>118</td>
</tr>
<tr>
<td>Backing Up and Restoring the System</td>
<td>119</td>
</tr>
<tr>
<td>Backing Up HCX Manager</td>
<td>119</td>
</tr>
<tr>
<td>Restoring the System</td>
<td>120</td>
</tr>
<tr>
<td>Managing HCX Alerts</td>
<td>121</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>13 Updating VMware HCX</th>
<th>123</th>
</tr>
</thead>
<tbody>
<tr>
<td>About HCX Service Updates</td>
<td>123</td>
</tr>
<tr>
<td>Planning for HCX Updates</td>
<td>124</td>
</tr>
<tr>
<td>HCX Service Update Procedures</td>
<td>126</td>
</tr>
<tr>
<td>Upgrading the HCX Manager</td>
<td>126</td>
</tr>
<tr>
<td>Upgrading the HCX Service Mesh Appliances</td>
<td>127</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>14 Removing VMware HCX</th>
<th>129</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uninstalling VMware HCX</td>
<td>130</td>
</tr>
<tr>
<td>Uninstalling HCX in VMware Cloud on AWS Deployments</td>
<td>131</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>15 VMware HCX Troubleshooting</th>
<th>135</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling SSH on the VMware HCX Manager</td>
<td>135</td>
</tr>
<tr>
<td>Logging in to the VMware HCX Manager Shell</td>
<td>136</td>
</tr>
</tbody>
</table>
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. The guide that describes how to plan for and install VMware HCX for Telco Cloud in Telco environments is VMware HCX for Telco Cloud Deployment Guide.

To access the Telco guide, see VMware HCX for Telco Cloud Deployment Guide.

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.
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>Application Path Resiliency</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>TCP Flow Conditioning</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>
<tr>
<td>Mobility Optimized Networking (MON)</td>
<td>This service integrates HCX Network Extension with NSX Dynamic Routing to enable migrated virtual machines to reach other virtual machines and networks optimally, without a trombone or hairpin effect. MON can be enabled on new or existing network extensions to NSX-T 3.0 Data Centers.</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 HCX Network Extension service provides a low-touch operation for high performance (4–6 Gbps) Layer 2 Extension from environments that use a vSphere Distributed Switch, or NSX Networking. HCX Network Extension provides the ability to keep the same IP and MAC addresses during virtual machine migrations. HCX Network Extension with Mobility Optimized Networking eliminates tromboning between migrated virtual machines on different extended segments, and virtual machines on native NSX-T networks at the destination.
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 Gateway Appliance**

The HCX Sentinel Gateway (SGW) appliance is used to connect and forward guest workloads from the source environment to 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.

**Note** This section describes only VMware HCX deployment types. For information about deploying VMware HCX for Telco Cloud in Telco environments, see *VMware HCX for Telco Cloud Deployment Guide*.

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:
## Deployment 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 (Public Cloud to Public Cloud, SDDC to SDDC, or SDDC to Public 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. <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. **Configure the firewall access** for ports and protocols for inbound and outbound HCX connections
4. **Deploy the Interconnect Service Mesh** on the source site
5. **Configure and license the HCX Manager appliance**
6. **Initiate network extensions** from the source site
7. **Initiate HCX operations** (migration, replication) from the source site
8. **Perform site pairing**

---

VMware HCX User Guide
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
- HCX Support Policy for Vacating Legacy vSphere Environments
- Network Port and Protocol Requirements
- Using the HCX Interface
- HCX Activation and Licensing
- NSX Requirements for HCX Deployments

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>

Note: The storage requirement per appliance is doubled during the HCX upgrade and redeploy operations, as a second appliance is created for the duration of the operation.
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 supported software versions.

Software Version Requirements for the HCX Installations

Note In cloud-to-cloud deployments, the HCX Cloud environment requirements apply to both sides of a site pair.

<table>
<thead>
<tr>
<th>Component Type</th>
<th>HCX Connector Environment Requirements</th>
<th>HCX Cloud Environment Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere (vCenter Server and ESXi)</td>
<td>6.0+</td>
<td>6.5.x, 6.7.x, and 7.0</td>
</tr>
<tr>
<td>NSX</td>
<td>NSXv 6.4.4+ or NSX-T 2.4.0+</td>
<td>NSXv 6.4.5+ or NSX-T 2.5.0+</td>
</tr>
<tr>
<td></td>
<td>Interoperability with vSphere 7.0</td>
<td>Interoperability with vSphere 7.0</td>
</tr>
<tr>
<td></td>
<td>requires NSX-T 3.0.1</td>
<td>requires NSX-T 3.0.1+</td>
</tr>
<tr>
<td>vCloud Director</td>
<td>Not supported at the source site.</td>
<td>When the destination environment is integrated with vCloud Director, the minimum is 9.7.</td>
</tr>
</tbody>
</table>

Software 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</th>
<th>Destination Site Component Version Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>HCX Bulk Migration</td>
<td>vSphere 6.0+</td>
<td>vSphere 6.5+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NSXv 6.4.5+ or NSX-T 2.5.0+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vSphere 7.0+ with NSX-T 3.0.1+</td>
</tr>
<tr>
<td>HCX vMotion</td>
<td>vSphere 6.0+</td>
<td>vSphere 6.5+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NSXv 6.4.5+ or NSX-T 2.5.0+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vSphere 7.0+ with NSX-T 3.0.1+</td>
</tr>
<tr>
<td>HCX Cold Migration</td>
<td>vSphere 6.0+</td>
<td>vSphere 6.5+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NSXv 6.4.5+ or NSX-T 2.5.0+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vSphere 7.0+ with NSX-T 3.0.1+</td>
</tr>
<tr>
<td>Feature</td>
<td>Source Site Component Version Requirements</td>
<td>Destination Site Component Version Requirements</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>--------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>HCX Replication Assisted vMotion</td>
<td>vSphere 6.0+</td>
<td>vSphere 6.5 U3F+ or vSphere 6.7U3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NSXv 6.4.5+ or NSX-T 2.5.0+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vSphere 7.0+ with NSX-T 3.0.1+</td>
</tr>
<tr>
<td>HCX OS Assisted Migration</td>
<td>vSphere 6.0+</td>
<td>vSphere 6.5+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NSXv 6.4.5+ or NSX-T 2.5.0+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vSphere 7.0+ with NSX-T 3.0.1+</td>
</tr>
<tr>
<td></td>
<td>For a list of supported guest OS versions, see Understanding VMware HCX OS Assisted Migration.</td>
<td></td>
</tr>
<tr>
<td>Network Extension of vSphere Distributed Switch VM Networks</td>
<td>vSphere 6.0+</td>
<td>vSphere 6.5+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NSXv 6.4.5+ or NSX-T 2.5.0+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vSphere 7.0+ with NSX-T 3.0.1+</td>
</tr>
<tr>
<td>Network Extension for NSXv Logical Switches</td>
<td>vSphere 6.0+</td>
<td>vSphere 6.5+</td>
</tr>
<tr>
<td></td>
<td>NSX for vSphere 6.4.4+</td>
<td>NSXv 6.4.5+ or NSX-T 2.5.0+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vSphere 7.0+ with NSX-T 3.0.1+</td>
</tr>
<tr>
<td>Network Extension for NSX-T VLAN or Overlay Segments</td>
<td>vSphere 6.0+</td>
<td>vSphere 6.5+</td>
</tr>
<tr>
<td></td>
<td>NSX-T 2.4.0+</td>
<td>NSXv 6.4.5+ or NSX-T 2.5.0+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vSphere 7.0+ with NSX-T 3.0.1+</td>
</tr>
<tr>
<td>VMware HCX Disaster Recovery</td>
<td>vSphere 6.0+</td>
<td>vSphere 6.5+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NSXv 6.4.5+ or NSX-T 2.5.0+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vSphere 7.0+ with NSX-T 3.0.1+</td>
</tr>
<tr>
<td>Site Recovery Manager Integration</td>
<td>vSphere 6.5+</td>
<td>vSphere 6.5+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NSXv 6.4.5+ or NSX-T 2.5.0+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vSphere 7.0+ with NSX-T 3.0.1+</td>
</tr>
<tr>
<td>Mobility Optimized Networking</td>
<td>vSphere 6.0+</td>
<td>vSphere 6.5+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NSX-T 3.0+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vSphere 7.0+ with NSX-T 3.0.1+</td>
</tr>
<tr>
<td>Traffic Engineering</td>
<td>vSphere 6.0+</td>
<td>vSphere 6.5+</td>
</tr>
<tr>
<td>Application Path Resiliency</td>
<td></td>
<td>NSXv 6.4.5+ or NSX-T 2.5.0+</td>
</tr>
<tr>
<td>TCP Flow Conditioning</td>
<td></td>
<td>vSphere 7.0+ with NSX-T 3.0.1+</td>
</tr>
</tbody>
</table>

**Interoperability with External Software**

HCX can operate with other VMware services provided they meet the requirements for interoperability.
**Software Interoperability**

<table>
<thead>
<tr>
<th>Software Interoperability</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere Replication and HCX</td>
<td>For HCX and vSphere Replication installations to co-exist, vSphere Replication 8.1 or above is required. This allows both systems to manage replications without disrupting the other system's configurations. Any single virtual machine cannot be managed by both systems simultaneously.</td>
</tr>
<tr>
<td>vRealize Operations (VROPS) and HCX</td>
<td>VROPS 8.1.1+.</td>
</tr>
</tbody>
</table>

**HCX Support Policy for Vacating Legacy vSphere Environments**

One of the key use cases for VMware HCX is to give users a supported and consistent option for vacating legacy vSphere environments. Customers can use this option to avoid complex upgrades and accelerate the adoption of a modern vSphere based public or private cloud.

A legacy vSphere environment is defined as any vSphere installation that has exceeded the General Availability support phase but is within Technical Support Guidance. Refer to [VMware Product Lifecycle Matrix](#) for version-specific vSphere lifecycle information.

The following support policy applies:

- If the environment is under Technical Guidance
  - HCX supports migrations from legacy vSphere environments. (HCX Connector only.)
  - HCX does not support migration to legacy vSphere environments.
- If the environment is out of Technical Guidance
  - Legacy vSphere environments exceeding the End of Technical Guidance date are not supported under this policy.

This policy applies to all HCX deployments for any on-premises or cloud environment.

**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](https://www.vmware.com/support/robot.html).

**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 <a href="https://www.vmware.com/support/robot.html">Logging in to the VMware HCX Manager Shell</a>.</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](https://www.vmware.com/support/robot.html).

**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:
Activating the system requires network access from the HCX Manager system to https://connect.hcx.vmware.com and a valid activation key or license key.

To test connectivity from the HCX Manager, use SSH to connect to the HCX Manager shell.

```
curl -k -v https://connect.hcx.vmware.com
```

Network access from the HCX Manager system to https://connect.hcx.vmware.com when there is a proxy for outbound HTTPS connections.

If there is a proxy server in the environment, the proxy server must be configured on the HCX Manager. The proxy settings can be configured in the Administration interface. To resume the Initial Configuration Wizard, click the dashboard tab.

**Caution** 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.

Activating HCX systems when using a private vSphere or vCloud Director as the destination environment.

Use NSX Data Center Enterprise Plus licenses from my.vmware.com. Enter this license when prompted for the **HCX Advanced Key**.

NSX Data Center Enterprise Plus evaluation licenses may be used, but they must be updated to full keys for operations exceeding the trial limits.
### Activating HCX with VMware Cloud on AWS

Obtain the activation keys for the HCX system following the cloud provider’s procedures. Enter this activation key when prompted for the **HCX Advanced Key**.

- Obtain the activation keys for VMware HCX in VMware Cloud on AWS.
  - Log in to console.cloud.vmware.com.
  - Open VMware Hybrid Cloud Extension > Activation Keys > CREATE ACTIVATION KEYS.
  - Create an HCX Cloud key for VMware Cloud on AWS SDDC.
  - Create an HCX Enterprise key for the HCX on-premises system.

### Activate Later

This option allows HCX activation to be temporarily skipped. To complete the installation while waiting for proxy or firewall allow additions, choose this option. The activation keys can be entered in the Appliance Management Configuration interface.

### Grace Period

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.

### 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:
     - Click **REMOVE** to remove the existing license key.
   - Add an HCX Enterprise license key:
     - Enter the HCX Enterprise license, and click **ADD**.
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 6.4 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.
- When NSX-T is registered, both Overlay and VLAN segments can be used during the Network Profile creation.
- 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.
- In NSX-T deployments, HCX supports integration with networking objects created with the NSX Simplified UI/API only.
Deployment of HCX in environments with multiple Data Centers prepped for NSX and a single vCenter (sharing transport zones and datastores) is not supported.

**Note**  The HCX Network Extension service has additional NSX requirements. See [Requirements for Network Extension](#).

## 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](#).
Installing the System

This section describes how to install and activate the VMware HCX Cloud Manager and VMware HCX Connector components.

VMware HCX has two component services: HCX Cloud Manager and HCX Connector. These components work together to provide the VMware HCX services. In cloud-to-cloud environments, you deploy HCX Cloud Manager at both the source and destination sites. In legacy vSphere-to-cloud (private or public) deployments, you install HCX Connector at your on-premises or legacy site and HCX Cloud Manager at the destination cloud site.

This chapter includes the following topics:

- HCX Installation Workflow
- Downloading the HCX OVAs
- Deploying the Installer OVA in the vSphere Client
- Activating and Configuring HCX

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—3, 8, 9 must be performed for each SDDC.
- Steps 4—7 are only required once for each source site.
An HCX Connector installation can pair with many VMware Cloud on AWS 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 **Add Ons** tab of your VMware Cloud on AWS SDDC. See *Deploying HCX from the VMC Console*.

3. In the VMware Cloud on AWS SDDC Console go to the Network and Security tab to perform the following actions:
   a. Configure the Management Gateway to allow the HCX Cloud Manager (use the pre-defined HCX group as the destination) to receive inbound TCP-443 connections.
   b. If configuring HCX to use AWS Direct Connect with a Private Virtual Interface, see *Configuring VMware HCX for Direct Connect Private Virtual Interfaces*.

   For more details on the network port configuration, see *Network Port and Protocol Requirements*.

4. Download the HCX Connector for the Source on-premises installation and site pairing.
   a. On the **Add Ons** tab of your SDDC, click **Open HCX** on the HCX card.
   b. Navigate to the SDDC tab and click **Open HCX**.
      
      The browser redirects to hcx.sddc-*.vmwarevmc.com.
   c. Enter the cloudadmin@vmc.local user and password and click **Log In**.
   d. Under the Administration tab, select **System Updates** and click **Request Download Link**.
      
      An option is provided to download the HCX Connector OVA locally or copy the download link.

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

6. Configure the source site (on-premises) firewall to allow inbound and outbound connectivity based on the HCX services or features used. See [https://ports.vmware.com/home/VMware-HCX](https://ports.vmware.com/home/VMware-HCX).

7. Create and activate keys for the source site HCX Connector that will be paired with the HCX Cloud Manager in VMware Cloud on AWS.
   b. On the **Add Ons** tab of your SDDC, click **Open HCX** on the HCX card.
   c. Navigate to the **Activation Keys** tab.
   d. Create an Activation Key for the source HCX Connector.
   e. Enter the created activation key in the source HCX Connector and click **Activate**.

8. Pair HCX Connector with HCX Cloud. See *Adding a Site Pair*.
If the HCX Cloud system is prepared using the Multi-Site Service Mesh, see Adding a Site Pair.

Enable HCX services to deploy the HCX Interconnect.

See Configuring and Managing the HCX Interconnect with the Multi-Site Service Mesh.

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 Installer OVA.

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

4. Configure firewall rules at source and destination sites to allow inbound and outbound connectivity based on the HCX services or features used. See https://ports.vmware.com/home/VMware-HCX.

5. Activate and Configure the HCX Cloud system. See Activating and Configuring HCX.

6. 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.

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

8. Activate and Configure the HCX Connector system. See Activating and Configuring HCX.

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

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

4 Configure firewall rules at source and destination sites to allow inbound and outbound connectivity based on the HCX services or features used. See https://ports.vmware.com/home/VMware-HCX.

5 Activate and Configure the HCX Cloud system. See Activating and Configuring HCX.

During this step, select vCloud Director as the installation type and select the additional vCloud Director-specific details (for example, Public Access URL, AMQP).

6 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.

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

8 Activate and Configure the HCX Connector system. See Activating and Configuring HCX.

9 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.

10 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.

**Downloading the HCX OVAs**

You use separate OVA files to deploy HCX Connector and HCX Cloud Manager.

The installer OVA provides the image necessary to deploy HCX Cloud Manager. You obtain the installer OVA from the VMware downloads site. You obtain the HCX Connector OVA file by accessing the HCX Cloud Manager service interface after you have fully deployed and activated HCX Cloud Manager.

**Downloading the Installer OVA**

The installer OVA is used for deploying HCX Cloud Manager in a vSphere cloud environment.

In public cloud deployments, the cloud service provider may deploy HCX Cloud Manager.

Use this procedure to download the installer 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

Deploy the downloaded installer OVA in the vCenter Server. See Deploying the Installer OVA in the vSphere Client.

Downloading the HCX Connector OVA

The HCX Connector OVA is used when deploying VMware HCX at the legacy site in legacy-to-vSphere cloud environments.

You obtain the HCX Connector OVA from the System Updates selection in the HCX Cloud Manager service UI.

Prerequisites

Before you can download the HCX Connector OVA, you must install, activate, and configure the HCX Cloud Manager.

Procedure

1. Navigate to the HCX Cloud Manager service interface: 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

Deploy the downloaded HCX Connector OVA in the vCenter Server. See Deploying the Installer OVA in the vSphere Client.

Note

The same procedure for deploying the installer OVA applies to deploying the Connector OVA.

Deploying the Installer OVA 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 virtual machine that you are installing.
   - **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.
   - **Services Configuration**
     - NTP Server List.

10. Click **Next**.

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

**What to do next**

Allow up to 5 minutes for initialization, then browse to the appliance management interface for the initial activation using `https://hcx-ip-or-fqdn:9443`.

**Activating and Configuring HCX**

After you have deployed the OVA file, activate the system and perform the initial configuration immediately when you next open the appliance management interface.

**Note** You use this same procedure for both HCX Cloud Manager and HCX Connector deployments.
Prerequisites

- The OVA deployment must complete before you begin. Allow up to five minutes after the installer OVA deployment for the services to initialize.
- Configure firewall rules at source and destination sites to allow inbound and outbound connectivity based on the HCX services or features used. See https://ports.vmware.com/home/VMware-HCX.
- Obtain the activation key based on the HCX destination type. See Activating or Licensing New HCX Systems.

Procedure


After you log in, the installation welcome screen appears.

2. Click Continue.

The activation screen appears.
3 Enter the License Key.

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

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.

5 Click Activate.

The system prompts you to confirm the deployment type. The system detects the deployment type based on the license key and displays a graphic illustrating the installation component.

6 Click OK.

The Manage License Keys screen appears.
7 (Optional) If you have an HCX Enterprise License (upgrade) key, enter it in the HCX License Key field, and click **Add**.

The upgrade license key is added to the license key table with the activation key. The table includes information about each license key and its duration.

8 Click **Next**.

9 Observe the system download information.

After you enter the license information and confirm the deployment type, the system begins downloading the image file that is specific to the deployment type. If upgrades are available, they are applied before the download. The download process can take several minutes depending on your environment. A display screen provides the download status.

When the download is complete, the system reloads, and the log in screen appears.

10 To start the configuration wizard, log in to the system using the admin user credentials.

The system location screen appears.

11 Enter the location where you are deploying the system.

Select the nearest major city to where the HCX system is geographically located. HCX sites are represented visually in the Dashboard.
12 Click **Continue**.

A screen appears prompting you for a system name.

13 Enter the system name, and click **Continue**.

A screen appears prompting you to select the cloud instance type.

14 Select the cloud instance to which VMware HCX will be connected: vSphere, vCloud Director, or VMware Integrated OpenStack.

The HCX can connect to only one cloud instance per deployment.

**Note** Kubernetes is not available for VMware HCX.

15 Click **Continue**.

A series of screens appears, prompting you for the selection details.
Enter the configuration details for the selected cloud instance.

After entering the information, click **Continue** to proceed to the next screen.

<table>
<thead>
<tr>
<th>Cloud Instance</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere</td>
<td>a  vCenter Server and NSX details</td>
</tr>
<tr>
<td></td>
<td>1  vCenter Server</td>
</tr>
<tr>
<td></td>
<td>■  vCenter URL</td>
</tr>
<tr>
<td></td>
<td>■  User name</td>
</tr>
<tr>
<td></td>
<td>■  Password</td>
</tr>
<tr>
<td></td>
<td>2  NSX</td>
</tr>
<tr>
<td></td>
<td>■  NSX URL</td>
</tr>
<tr>
<td></td>
<td>■  User name</td>
</tr>
<tr>
<td></td>
<td>■  Password</td>
</tr>
<tr>
<td></td>
<td>b  SSO details</td>
</tr>
<tr>
<td></td>
<td>■  vCenter Server or Platform Services Controller URL</td>
</tr>
<tr>
<td></td>
<td>c  Public Access URL details</td>
</tr>
<tr>
<td></td>
<td>■  URL through which the HCX Manager is accessed.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This is typically the HCX Manager services UI: https://&lt;hcx-mgr-fqdn-or-ip&gt;.</td>
</tr>
<tr>
<td>vCloud Director</td>
<td>a  vCloud Director details</td>
</tr>
<tr>
<td></td>
<td>■  vCloud Director URL</td>
</tr>
<tr>
<td></td>
<td>■  System Administrator user name</td>
</tr>
<tr>
<td></td>
<td>■  System Administrator password</td>
</tr>
<tr>
<td></td>
<td>b  vCenter Server and NSX details</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The HCX Manager automatically fetches the vCenter Server and NSX URLs.</td>
</tr>
<tr>
<td></td>
<td>1  vCenter Server</td>
</tr>
<tr>
<td></td>
<td>■  User name</td>
</tr>
<tr>
<td></td>
<td>■  Password</td>
</tr>
<tr>
<td></td>
<td>2  NSX</td>
</tr>
<tr>
<td></td>
<td>■  User name</td>
</tr>
<tr>
<td></td>
<td>■  Password</td>
</tr>
<tr>
<td></td>
<td>c  AMQP details</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The HCX Manager automatically fetches the AMQP parameters.</td>
</tr>
<tr>
<td></td>
<td>Edit the parameters as appropriate.</td>
</tr>
<tr>
<td></td>
<td>■  AMQP Host name</td>
</tr>
<tr>
<td></td>
<td>■  Port</td>
</tr>
<tr>
<td></td>
<td>■  vHost</td>
</tr>
<tr>
<td></td>
<td>■  User name</td>
</tr>
<tr>
<td></td>
<td>■  Password</td>
</tr>
<tr>
<td></td>
<td>■  Use SSL</td>
</tr>
<tr>
<td>VMware Integrated OpenStack</td>
<td>a  VMware Integrated OpenStack (VIO) details</td>
</tr>
<tr>
<td></td>
<td>■  OpenStack Management Server (OMS) URL</td>
</tr>
<tr>
<td></td>
<td>■  User name</td>
</tr>
<tr>
<td>Cloud Instance</td>
<td>Configuration Parameters</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td></td>
<td>a  Password</td>
</tr>
<tr>
<td></td>
<td>b  Keystone details</td>
</tr>
<tr>
<td></td>
<td>■  Admin user name</td>
</tr>
<tr>
<td></td>
<td>■  Admin password</td>
</tr>
<tr>
<td></td>
<td>c  Domains and Projects details</td>
</tr>
<tr>
<td></td>
<td>Note  You can add Multiple VIO Domains and Projects.</td>
</tr>
<tr>
<td></td>
<td>1  Add New Domain</td>
</tr>
<tr>
<td></td>
<td>For each Domain, provide the following details.</td>
</tr>
<tr>
<td></td>
<td>■  Domain Name (select from the drop-down)</td>
</tr>
<tr>
<td></td>
<td>■  User name</td>
</tr>
<tr>
<td></td>
<td>■  Password</td>
</tr>
<tr>
<td></td>
<td>■  Projects (optional)</td>
</tr>
<tr>
<td></td>
<td>For each Domain, you can add multiple Projects.</td>
</tr>
<tr>
<td></td>
<td>■  Project Name (select from the drop-down)</td>
</tr>
<tr>
<td></td>
<td>■  User name</td>
</tr>
<tr>
<td></td>
<td>■  Password</td>
</tr>
<tr>
<td></td>
<td>d  vCenter and NSX details</td>
</tr>
<tr>
<td></td>
<td>1  vCenter Server</td>
</tr>
<tr>
<td></td>
<td>■  vCenter URL</td>
</tr>
<tr>
<td></td>
<td>■  User name</td>
</tr>
<tr>
<td></td>
<td>■  Password</td>
</tr>
<tr>
<td></td>
<td>2  NSX</td>
</tr>
<tr>
<td></td>
<td>■  NSX URL</td>
</tr>
<tr>
<td></td>
<td>■  User name</td>
</tr>
<tr>
<td></td>
<td>■  Password</td>
</tr>
<tr>
<td></td>
<td>e  AMQP details</td>
</tr>
<tr>
<td></td>
<td>■  AMQP Host name</td>
</tr>
<tr>
<td></td>
<td>■  Port</td>
</tr>
<tr>
<td></td>
<td>■  vHost</td>
</tr>
<tr>
<td></td>
<td>■  User name</td>
</tr>
<tr>
<td></td>
<td>■  Password</td>
</tr>
<tr>
<td></td>
<td>■  Use SSL</td>
</tr>
</tbody>
</table>

The system verifies the configuration and then generates a configuration summary.
17 Review the system summary information.

Summary information can vary depending on the cloud instance type.

18 To reload the system, click **Restart**.

It can take several minutes to reinitialize the system completely. During this process, the appliance management interface is not available.

After the system reloads, it displays the appliance management dashboard. For more information about the dashboard, see **Understanding the Appliance Management Dashboard**.
19 (vSphere instance only) Configure vSphere roles for the cloud instance.

a In the appliance management dashboard, navigate to **Configuration > vSphere Role-Mapping**.

b Assign the HCX Roles to the vCenter User Groups that are allowed to perform HCX operations.

The groups assigned must have the minimum privileges to perform the HCX-related operations in vCenter Server.

<table>
<thead>
<tr>
<th>vCenter Resource Type</th>
<th>User Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder/Datacenter</td>
<td>VirtualMachine.Inventory.Create</td>
<td>On the selected destination folder (vCenter Inventory), assign user privileges to create a virtual machine.</td>
</tr>
<tr>
<td>Folder/Datacenter</td>
<td>VirtualMachine.Interact.PowerOn</td>
<td>On the selected destination folder (vCenter Inventory), assign user privileges to power on a virtual machine.</td>
</tr>
<tr>
<td>Datastore</td>
<td>Datastore.UpdateVirtualMachineMetadata</td>
<td>On the selected destination datastore, assign user privileges to update virtual machine related files.</td>
</tr>
<tr>
<td>Datastore</td>
<td>Datastore.DeleteFile</td>
<td>On the selected destination datastore, assign user privileges to delete files.</td>
</tr>
<tr>
<td>DistributedVirtualPortgroup/Network</td>
<td>Network.Assign</td>
<td>On the selected destination Network, assign user privileges to connect NiCs.</td>
</tr>
<tr>
<td>VirtualMachine</td>
<td>VirtualMachine.Interact.PowerOn</td>
<td>On the selected virtual machine, assign user power-on privileges. This permission is required on source side. All the other permissions are required on destination side.</td>
</tr>
</tbody>
</table>

c Click **Save**.

**Results**

The system configuration is complete.
What to do next

Deploy additional HCX systems.
Configuration and Service Limits for VMware HCX

When you are configuring, deploying, and operating VMware HCX, you must stay within the supported limits.

VMware HCX maintains an updated list of system and operational limits in the following categories:

- Sites and Service Components
- Migrations
- Disaster Recovery and Site Recovery Manager
- Network Extension
- Migration-Centric Virtual Machine Limits

For a detailed list of the system limits, refer to the VMware Configurations Maximum tool.
Configuring and Managing the HCX Interconnect

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:
   a. Select a source and destination Compute Profile.
   b. Enable a Multi-Site 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 diagram.
- 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.

In HCX Connector to HCX Cloud deployments, the HCX Connector is deployed at the legacy or source vSphere environment. The HCX Connector creates a unidirectional site pairing to an HCX Cloud system. In this type of site pairing, all HCX Service Mesh connections, Migration and Network Extension operations, including reverse migrations, are always initiated from the HCX Connector at the source.
In HCX cloud-to-cloud deployments, site pairing can be unidirectional or bidirectional:

- In unidirectional site pairing, the HCX Cloud containing the virtual machine inventory and networks (similar to HCX Connectors) will site pair to the destination HCX Cloud. In this type of site pairing, all HCX Service Mesh connections, Migration and Network Extension operations, including reverse migrations, are always initiated from the source HCX Cloud system. In this case, an administrator may see the message URL not available when viewing site pairing from the destination site. This is expected behavior because HCX Connector to HCX Cloud site pairing is uni-directional.

- In bidirectional site pairing, the HCX Cloud systems are site paired with each other, share a common Service Mesh, and can initiate Migration and Network Extension operations from either HCX Cloud system.

In the case of unidirectional site pairing, an administrator may see the message URL not available when viewing site pairing from the destination site. This is expected behavior because HCX Connector to HCX Cloud site pairing is unidirectional. In the case of bidirectional site pairing, the URLs for the paired sites are visible from either the source or destination.

An HCX Connector cannot be the target for a site pairing.

**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**.
4. (Optional) To achieve bidirectional site pairing in cloud-to-cloud deployments, repeat this procedure at both cloud sites.

**Results**

If all validations succeed, the system displays the remote site in the list as a connected site. With bidirectional site pairing, both sites show up in the list.

**Example: Connected Site**

![Connected Site Screenshot]

**What to do next**

Create the Network and Compute Profiles, followed by the Multi-Site Service Mesh.

**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.

**Caution** Although a Network Profile can be assigned any of the functions during the Compute Profile configuration, consider creating a separate profile for each function as a best practice.

- 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.

  **Important** The HCX Interconnect uses a Network Profile configuration dedicated to vMotion traffic. This configuration does not include the vMotion NFC traffic. HCX always uses its Management interface for vMotion NFC traffic.

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

  **Important** In deployments where ESXi servers use a dedicated VMkernel configuration for vSphere Replication services, the HCX Interconnect uses a Network Profile configuration dedicated to the vSphere Replication traffic. This configuration does not include the vSphere Replication NFC traffic. HCX always uses its Management interface for vSphere Replication NFC traffic.

- **Guest Network for OS Assisted Migration**
  The Sentinel Gateway appliances use this vSphere network to connect with non-vSphere virtual machines.

  **Important** When creating a separate Network Profile for vMotion or vSphere Replication services, although the option is available to configure a GW as a standard Network Profile, traffic for those services will only use the default GW in the Management Network Profile to attempt to access resources in a different subnet. If ESXi resources are not L2 adjacent to the IX appliance on those networks, there is a requirement to configure “Static Routes” as part of the “Advance Configurations” option in the Compute Profile to ensure traffic is directed to the default GW on those networks.

Refer to Steps Step 9 and Step 10 in the section Creating a Compute 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**.

**Note**  To edit an existing Network Profile, navigate to the specific Network Profile and click **Edit**.

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**

- Install and configure HCX Manager.
- 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 plug-in > 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 **Create 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 the 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**.
      The Select Deployment Resources and Reservations screen appears.

6 Make your resource, and resource reservation selections.
   a From the **Select Resource** drop-down menu, and select each cluster or resource pool to be used when deploying HCX Interconnect appliances.
   b From the **Select Datastore** drop-down menu, and 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.
c  (Optional) From the Select Folder drop-down menu, and specify a folder in which to deploy the HCX appliances.

**Note**  This option requires VMware HCX release R137 or higher.

d  Using the slide bar, select the amount of CPU and memory to reserve for HCX operations. As a best practice, set the CPU and memory reservation to 100 percent.

For example, setting **Memory Reservation** to 100 percent ensures that all of the memory allocated for HCX appliances is always available for HCX operations.

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.

9 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 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 a network, or click Create Network Profile to create it.**

For additional information see **Creating a Network Profile**.

c **Expand the selected Guest Network Profile to view its details and free IP Addresses, and click Close.**

d **Click Continue.**

The Guest Network is depicted in the topology.
12 Select Network Containers Eligible for Network Extension:
   a  Click the Select Network Containers drop-down menu.
      The system displays the list of network containers found in the service resources selected in a previous step.
   b  Select entries with virtual machine networks. Click Close.
      You can select vDS, N-VDS, Transport Zones, or some combination for Network Extension. If only one network container is found in the previously selected service resources, it is pre-selected.

   **Note** Only the virtual machine networks on the selected switches or Transport Zones may be used during network extension operations.

   c  Optionally, use the Advanced Configurations to restrict the Network Extensions for your selection.
   d  Click Continue.
      The topology view is dynamically updated, depicting your selections.

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 Select Target Datastores.
      The menu contains a list of all the datastores present in the resource pool or cluster selected in Deployment cluster.
   b  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 Manager UI at the source site to create the Interconnect Service Mesh.

**Note** To edit an existing Compute Profile, navigate to the specific Compute profile, and click *Edit*.

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.

(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 is 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.

The HCX Service Mesh can use up to three HCX Uplinks, adding network path failover and improving overall resiliency for HCX services. Multiple HCX Uplinks are not aggregated for increased throughput capacity. The following specific behaviors apply:

- HCX attempts to load balance traffic on the Network Extension (HCX-NE) appliance based on characteristics of the flow and the performance of the uplinks.

- HCX does not load balance migration traffic on the Interconnect (HCX-IX) appliance. Additional uplinks may or may not be used.

c. Click Continue.

d. Optionally, repeat these steps for the destination site.
7  (Optional) Configure the Network Extension appliances deployed per switch or Transport Zone:

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

a  In Advanced Configuration - Network Network Extension Appliance Scale, review the default Extension appliances per Network Container.

b  For each entry, 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.

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.

What to do next

If it is necessary to make any direct changes to an existing Services Mesh, such enabling or disabling services and overriding uplinks, select Interconnect > Service Mesh > Edit. The editing
workflow includes a preview screen, listing the changes and describing the impact of those changes on related services prior to finishing the procedure. You can select to complete or cancel the update.

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 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.
   - **HCX Sentinel installation for Linux**
     a. Connect to your guest system using SSH.
     b. Copy the `linux-sentinel-installer.sh` file to the guest system.
     c. At the terminal, enter the command `bash linux-sentinel-installer.sh`.
        The software prompts you for permission to start the installation.
     d. 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 uninstall the Sentinel agent software manually, 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 the 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 the 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.
Extending Networks with VMware HCX

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 Network Extension with Mobility Optimized Networking for NSX-T

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 a VMware vSphere Distributed Switch.
- Extend NSX overlay 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 vSphere Distributed Switch 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:
  - vSphere Distributed Switch Version 5.1.0 or higher is required.

- Requirements for 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 in the vCenter Server where the network originates.
    - NSX-T Overlay and NSX-T VLAN networks can be extended.
  - NSX-T Overlay or VLAN Transport Zones must be configured in the destination vCenter Server or SDDC.
    - HCX will always create or connect to an existing NSX-T Overlay network during the network extension operation.

- Requirements when extending NSX for vSphere Logical Switches:
  - The NSX-V Manager must be registered during the HCX Manager deployment.
  - The NSX-V Manager must be Version 6.4 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.

Restrictions and Limitations for Network Extension
HCX Network Extension may be prevented, disallowed, or allowed under explicit conditions.

Detected and Restricted Source Network Types
The HCX Network Extension service detects and prevents several non-supported Network Extension scenarios (items are dimmed in the Network Extension UI):

- vSphere cluster infrastructure networks (ESXi VMkernel networks).
- HCX Network Profile networks (Distributed Port Groups or Segments selected in a Network Profile).
- Trunk networks (Distributed Port Groups with VLAN type Trunk).
- Untagged networks (Distributed Port Groups with VLAN type None, ID 0 or NULL).
- HCX Network Extension does not support Private VLAN (PVLAN) networks.
- HCX Network Extension does not support port groups configured with ephemeral binding.
- Virtual machine networks with shared or overlapping VLAN configurations should not be extended to the same destination router. This can result in a network outage.

Unsupported Source Configurations
HCX Network Extension does not support the following source configurations:

- vSphere Standard Switch (VSS) networks.
- Cisco NSX1000v or other third-party switches.
- Cisco Application Centric Infrastructure (ACI) with VMware Virtual Machine Monitor (VMM).
- vSphere Distributed Switches configured with LACP.
- Daisy-chaining a single network to three separate destination sites is not supported. For example, A to B to C to D is not supported.
- Virtual machine networks must only be extended with a single solution. HCX does not support Network Extension for networks already extended to the same NSX router by an external solution. For example, HCX Network Extension or NSX L2 VPN can be used to provide connectivity, but both must not be used simultaneously. Using multiple bridging solutions simultaneously can result in a network outage.

Unsupported Destination Configurations
HCX Network Extension does not support the following destination configurations:

- NSX-T Global Federation configurations.
  
  HCX does not integrate with the NSX Global Manager (only the NSX Local Manager).
- NSX-T environments without a Tier 1 Router.
- NSX-T environments without an Overlay Transport Zone.
- Destination environments without NSX-T.

**Additional Considerations**

- HCX supports one Network Extension to a maximum of 3 distinct destinations or routers.
- One HCX Network Extension configuration cannot be extended multiple times to the same destination/router.
- One HCX Network Extension appliance can only connect to one Distributed Virtual Switch or NSX Transport Zone.
- One HCX Network Extension configuration cannot use multiple HCX Network Extension appliances.
- HCX Network Extension does not detect or mitigate loops.
- Virtual machine networks that span more than one vCenter Server should not be extended from more than one vCenter to the same destination router. This can result in a network outage.
- HCX Network Extension does not detect or mitigate IP conflicts on the network.
- HCX Network Extension does not detect or mitigate MAC conflicts on the network.
- For a cloud/site pair, a given network can be extended through only one appliance and is subject to the resource and performance limitations of that appliance.
- When a network is extended using an incorrect gateway IP or Prefix List, unextending and re-extending with the correct information will fail due to the mismatch on the NSX gateway configuration at the destination. In this case, it is necessary to manually remove the previous network extension configuration from the NSX gateway.
- HCX Network Extension does not support clusters with multiple discontiguous vMotion subnets. For example, where some hosts in the cluster use vMotion network/subnet 1 and other hosts in the cluster use vMotion network/subnet 2. This configuration is not best practice, but may exist as a part cluster consolidation, or when clusters are designed to span various racks, and those racks are designed to be layer 3 boundaries.

**Network Extension to Destinations with Universal Distributed Logical Routers**

When working with destination environments with Cross-vCenter NSX configurations, HCX supports extending source networks to destination environments using a Universal Distributed Logical Router (UDLR). When a UDLR is selected during the network extension operation, HCX creates a Universal Logical Switch on the destination, across multiple vCenter Servers.
The following information and requirements apply for Network Extension when specifying a UDLR as the gateway.

- The HCX Cloud 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.
- HCX Network Extension does not support the local egress feature of UDLRs.

### 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 is an L2 bridging function initiated at the source.

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

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

**Note** For a list of restrictions regarding Network Extension, see Restrictions and Limitations for Network Extension.

For the operational limits supported with HCX Network Extension, see Chapter 7 Configuration and Service Limits for VMware HCX.
Procedure

1 If you are using the HCX Manager UI, follow these steps to select a network for extension:
   a In the HCX Services menu, select **Network Extension**.
      
      A summary screen appears displaying all configured site pairs. Expand a site pair to see
      the associated Service Mesh information. Expand a Service Mesh to see the associated
      Network Extensions.
   b At the top of the page, select **Extend Networks**.
      
      A screen appears prompting you for the target site network selections.
   c Select a Service Mesh.
      
      **Note** If you have only one Service Mesh, it is selected by default.
   d Select one or more Distributed Port Groups or NSX Logical Switches.
      
      You can use the available filters to hide networks that are ineligible for extension, hide
      networks that do not have virtual machines associated with them, or hide networks
      without extension.
   e Click **Next**.

2 If you are using the vSphere Client Networking interface, follow these steps to select a network for extension:
   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 Network to HCX Target Site**.
      
      A screen appears prompting you for the target site network selections.
   d Expand Remote Site Connection and select a site.
      
      **Note** If you have only one site pairing, it is selected by default.

3 Use the drop-down menu to select the Destination First Hop Router.

   If you are extending a network to a vCenter with NSXv, select an Edge Services Gateway
   (ESG) or Distributed Logical Router (DLR) from the drop-down menu.

   If you are extending a network to a vCenter with NSX-T, select a tier-1 router.

4 Provide the Gateway IP address 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, click the extended option drop-down menu and optionally specify the DNS configuration.

5 Select the Extension appliance.
6  (Optional) For each source network, expand **Settings - optional** and check the appropriate options:

**Allow Overlapping VLAN**

The HCX Manager prevents you from extending networks that have the same VLAN ID and Gateway IP address. Select this option to override system and allow duplicate VLAN IDs.

**DNS entries**

For a vCD target cloud, optionally specify the DNS configuration: **Primary DNS**, **Secondary DNS**, and **DNS Suffix**.

7  (Optional) Depending on the NSX version running in your data center, enable Mobility Optimized Networking for all workloads that require routing through the local gateway at the target site.

With MON, you can configure individual workloads for local routing, or create policy routes to control which networks are routed locally. For more information about MON and additional configuration settings, see [HCX Network Extension with Mobility Optimized Networking for NSX-T](#).

8  To finish, click **Extend**.

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 HCX Manager UI, select **Services > Network Extension**.

The system displays a list of extended networks.

2  Select the network or networks that must be unextended, and click the ellipsis menu to see a list of actions.

3  Select the action: **Unextend Network** or **Force Unextend Network**.

The interface opens and displays the selected network.

**Note**  To unextend multiple networks simultaneously, select the networks and click the **Unextend Networks** tab.
4 (Optional) Expand the network entry and select **Connect cloud network to cloud edge gateway after unextending** to connect the remote side gateway.

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 on-premises data center. Checking this check box will connect the network to the cloud edge gateway after unextension. If dynamic routing is enabled, the network is advertised from the cloud Edge Gateway and may cause a routing conflict. Refer to the [KB article](#) for more information on this option.

**Note** Unextending a network removes the HCX L2 bridged path without removing the NSX Segment or vSphere Port Group, or NSX interface. The NSX router interface remains disconnected when the option **Connect cloud network** is not used.

5 To confirm the operation, click **Unextend**.

**HCX Network Extension with Mobility Optimized Networking for NSX-T**

When extending networks to a remote VMware NSX-T Data Center, you can enable the HCX Mobility Optimized Networking service to route the network traffic based on the locality of the source and destination virtual machines.

**Note** Mobility Optimized Networking is fully supported for VMware Cloud on AWS, and available for Early Adoption (EA) in other environments. For EA, enablement is available upon request and approval for NSX Enterprise Plus environments. For additional information about HCX Mobility Optimized Networking with VMware Cloud on AWS, see [HCX Services for VMware Cloud on AWS](#).

This service ensures traffic from the local and remote data centers uses an optimal path to reach its destination, while all flows remain symmetric.

In the absence of Mobility Optimized Networking, all traffic from workloads on an extended network at the destination site is routed through the source environment router.

Network Extension with HCX Mobility Optimized Networking provides the following functionality:

- Enable or disable Mobility Optimized Networking at the time of stretching a network
- Enable or disable Mobility Optimized Networking for already extended networks
- Enable or disable Mobility Optimized Networking on an individual VM basis for VMs residing on extended networks in the SDDC
- Display which VMs are using Mobility Optimized Networking
- When using HCX to vMotion a VM, preserve existing network connections while providing an option to enable Mobility Optimized Networking on that VM after migration
Understanding HCX Mobility Optimized Networking

This section provides an overview of workload traffic flows using HCX Network Extension with and without Mobility Optimized Networking.

Virtual Machine Reachability on Extended Networks Without Mobility Optimized Networking

- In the following figure, Network A has been extended without enabling Mobility Optimized Networking.
- Virtual Machine B has been migrated. Reaching Virtual Machine B:
  - Traffic sourcing from Virtual Machine A in Data Center A traverses Local HCX-NET-EXT and Remote HCX-NET-EXT to reach Virtual Machine B in Data Center B, and conversely for Virtual Machine B to Virtual Machine A.
  - Traffic sourcing from Virtual Machine B in Data Center B traverses Remote HCX-NET-EXT and Local HCX-NET-EXT to reach Virtual Machine D in Data Center B.
  - 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-NET-EXT and Remote HCX-NET-EXT 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.

Virtual Machine Reachability on Extended Networks with Mobility Optimized Networking

- In the following figure, Network A has been extended with Mobility Optimized Networking enabled.
■ Virtual Machine B has been migrated. Reaching Virtual Machine B:
  ■ Traffic sourcing from Virtual Machine A in Data Center A traverses Local HCX-NET-EXT and Remote HCX-NET-EXT to reach Virtual Machine B in Data Center B, and conversely for Virtual Machine B to Virtual Machine A.
  ■ Traffic sourcing from VM-B to Network C is routed locally to gateway 192.168.10.1 in Data Center B.
  ■ Traffic sourcing from VM-B to VM-C is first routed locally to gateway 192.168.10.1 in Data Center B. Since the gateway has no connected or static routes for Network B, it matches the policy route before using the default. Because the address for VM-C matches the policy route, the traffic is redirected to the Data Center A (NET A Gateway) router through Remote HCX NET-EXT to Local HCX NET-EXT.

Limitations for HCX Mobility Optimized Networking

The HCX Mobility Optimized Networking feature routes network traffic based on locality of the source and destination virtual machines.

When using HCX Mobility Optimized Networking, the following limitations apply:
  ■ Virtual Machines need VMware Tools installed for the HCX management plane to learn their IP address.
  ■ Editing the Mobility Optimized Networking segment properties from VMware Cloud on AWS "Networking & Security" tab is not supported.
  ■ A virtual machine must have a unique IP address in the same subnet for the MON enabled segment it is connected to.
If the virtual machine has multiple vNICs with IP addresses in different subnets, those vNICs must be connected to other stretched segments without MON enabled or other cloud segments.

The current implementation of Mobility Optimized Networking provides functionality for site-to-site service mesh. It does not provide routing optimizations for multi-site extension.

Routes for migrated virtual machines are currently not advertised beyond the NSX-T routing boundaries. Connectivity beyond NSX-T requires a NAT configuration.

Configuring HCX Mobility Optimized Networking

For data centers using NSX-T, configure Mobility Optimized Networking for workloads that require routing through the local gateway.

Prerequisites

- The HCX Manager at both the source and destination site is upgraded to version R140 or higher.
- NSX-T 3.0 is required at the destination.
- The HCX Service Mesh component appliances are upgraded to the latest versions.

Note In VMware Cloud on AWS environments the SDDC must be upgraded to at least M8v2 for both the control and data plane.

Procedure

1. In the HCX Manager UI, navigate to Services > Network Extension.
2. In the Network Extension screen, expand a site pair to see the extended networks.

   Network Extensions enabled for MON are highlighted with an icon.
3  Expand each extension to display network details.

4  Select a Network Extension and enable the slider for Mobility Optimized Networking.

   Enabling Mobility Optimized Networking applies to all subsequent events, such as VM migrations and new VMs connected to the network. VMs in the source environment and VMs not having VM Tools, are ineligible for Mobility Optimized Networking.

   **Note**  Workloads that were connected to the network prior enabling Mobility Optimized Networking continue to be routed through the source site.

5  For existing VMs requiring Mobility Optimized Networking, complete the following steps:
   a  Select a VM and expand the row.

      You can select multiple VMs using the check box next to each workload.

      **Note**  Transition VMs to Mobility Optimized Networking in batches of 25 or less at a time. Maintain a gap of 30 seconds between the batches.

   b  Select **Target Router Location** and choose the cloud option from the drop-down menu.

   c  Select **Proximity Conversion Type**: **Immediate Switchover** or **Switchover on VM Event**.

      Immediate Switchover: This selection transfers the router location immediately. If a workload VM has ongoing flows to the source router, they are impacted.

      Switchover on VM Event: This selection transfers the router location upon VM events like NIC disconnect and connect operations, and VM power cycle operations.
6 Click **Submit**.

All selected VM workloads are configured for Mobility Optimized Networking.

**Note** VMs that have been set for Switchover on VM Event stay in a pending state until that event occurs.

### Configuring Policy Routing for Mobility Optimized Networking

With Mobility Optimized Networking, you have the option to control which traffic is routed locally using the cloud gateway versus traffic that goes out through the source gateway. Policy routes define which traffic is routed through the source gateway. All other traffic is routed through the cloud gateway.

#### Procedure

1. In the HCX Manager UI, navigate to **Network Extension**.
2. In the Network Extension screen, click the **Advanced** tab.
3. Click **Policy Routes**.

   A new screen appears with options to Add or Remove networks.

   ![Policy Routes](policy_routes.png)

4. Using the pull-down menu, select a destination site.
5. In the Network field, for which you want traffic routed through the source gate, click **Add**.
6. Complete the entries for **Network IP Address** and **Prefix Length**.

   By default, **Redirect to Peer** is selected.

7. (Optional) To specify a policy that blocks a network from being redirected, uncheck **Allow Redirect to Peer**.
8  Click **Submit**.

The policy is applied to the network.
Migrating Virtual Machines with VMware HCX

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

Organizations migrate application workloads for many reasons. From data center consolidation and evacuation to modernization and maintenance, migrating workloads requires analysis and planning. Administrators identify individual workloads for migration, or waves of workloads based on, for example, cluster, network, or application landscape. HCX provides an array of migration types for moving these workloads including cold, warm, and live migration.

HCX also provides procedures for migrating groups, or waves, of virtual machines. And through integration with VMware vRealize Network Insight, Application Group information can be exported to HCX for migration as Mobility Groups. HCX Mobility Groups and vRealize Network Insight integration with HCX are available with the HCX Enterprise license.

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
- HCX Integration with vRealize Network Insight

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 POSIX 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.
- Virtual machines using virtual NVMe (vNVME) Controllers cannot be migrated.
- If either the source or destination vCenter version is 6.0 or earlier, VMware vCenter tags attached to a virtual machine are not retained during migration. Tags can be created manually for those virtual machines after migration.

Understanding VMware HCX vMotion and Cold Migration

The VMware HCX Interconnect integrates with ESXi to perform vMotion migrations for powered on virtual machines, and with Cold Migration for 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 and Limitations 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.
- Forward vMotion based migrations are supported from source ESXi hosts running versions 5.5 to 6.7. Reverse vMotion based migration is only supported with vSphere 6.0 and higher. Reverse migrations to ESXi 5.5 hosts can be accomplished with HCX Bulk migration.
- VMware NFC is used as the primary protocol during Cold Migration and as a secondary protocol during HCX vMotion.

**Note**  
The HCX Interconnect uses a Network Profile configuration dedicated to the vMotion traffic. This configuration does not include the Cold and vMotion NFC traffic. HCX always uses its Management interface for Cold and vMotion NFC traffic. In deployments where ESXi servers use a dedicated Provisioning vmkernel for NFC traffic, the HCX continues to route Cold and vMotion NFC traffic through the Management interface.

**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.

If either the source or destination vCenter version is 6.0 or earlier, VMware vCenter tags attached to a virtual machine are not retained during migration. Tags can be created manually for those virtual machines after migration.

### 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.

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.
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.

As the final step in the switchover, the source VM is removed, and the migrated VM is connected to the network powered on.

Replication Assisted vMotion creates two folders at the destination site. One folder contains the virtual machine infrastructure definition, and the other contains the virtual machine disk information. This is normal behavior for RAV migrations and has no impact on the functionality of the virtual machine at the destination site.

Note In some cases, having two folders might impact other applications, such as back-up tools, that require access the virtual machines folders. If necessary, you can consolidate the contents of these two folders using VMware Storage vMotion.

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.
- VMware NFC is used as a secondary protocol during HCX Replication Assisted vMotion migration.

Note HCX always uses its Management interface NFC traffic. In deployments where ESXi servers use a dedicated Provisioning vmkernel for NFC traffic, the HCX continues to route NFC traffic through the Management interface.

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 to VMFS6 target datastores requires the following minimum vSphere version at the target site: vSphere 6.5U3f or vSphere 6.7U3.
- RAV migration from a source environment running vCenter Server 5.5 to any destination vCenter Server with VMFS6 datastore as the target, is not supported.
- When RAV migration is to environments with vSAN Datastores, an individual virtual machine disk (vmdk) cannot exceed 2 TB.
- 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.
- Virtual machines using virtual NVMe (vNVME) Controllers cannot be migrated.
- Virtual machine Snapshots cannot be migrated.
If either the source or destination vCenter version is 6.0 or earlier, VMware vCenter tags attached to a virtual machine are not retained during migration. Tags can be created manually for those virtual machines after migration.

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 virtual machine 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 virtual machine systems for migration and to help replication processes prepare the disks on the replica virtual machine 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 virtual machines 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 virtual machines and SGW in the compute profile.

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

Using the established connection between the SGW and SDR, replication connections are made between the Sentinel software on the guest virtual machines 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 virtual machine remains online during replication until the final delta synchronization.

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

   The OS Assisted Migration service quiesces the guest virtual machine on a best-effort basis. For example, it is possible for a Linux service running on the guest virtual machine to start immediately after OS Assisted Migration has quiesced the services and stopped all known processes. If some process starts after quiescing the system, it can potentially lead to final synchronization not completing and appear as though the switchover process is stuck.
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.

During scheduled migrations, HCX Sentinel performs continuous synchronization by transferring only the deltas since the previous sync cycle. For Windows HCX Sentinel, this synchronization is achieved by identifying the changed file system blocks, whereas for Linux HCX Sentinel this synchronization is achieved by monitoring the changed files. To improve time it takes to reach that final consistency point for Linux systems, a pre-determined set of files and directories listed in `/opt/vmware/hcx/osam/excluded_paths` is excluded from the continuous synchronization. If you have additional files that do not require monitoring, you can exclude them from continuous synchronization by editing the file. Excluding files requires a restart of the Sentinel service named `vmware-hcx-osam-sentinel` using service or `systemctl` commands.

**Note** Excluded files are always synchronized to the target virtual machine during the initial and final synchronization phases.

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 virtual machine 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.

As the final step in the switchover, the source is powered-off, the migrated replica is connected to the network, and the switchover completes. The vSphere target virtual machine reboots twice during the switchover phase.

If the synchronization process fails for any reason, such as a broken network connection, by default the synchronization is retried for eight hours. To improve the time it takes to reach a final consistency point for Switchover to begin, you can shorten the retry period to as little as one hour by editing the file `/opt/vmware/hcx/osam/etc/sync.params` and setting the `max_retry_interval` from one to eight hours. After setting the interval, restart the Sentinel service named `vmware-hcx-osam-sentinel` using service or `systemctl` commands.

HCX Manager names the replica virtual machine with the host name of the source virtual machine.
VMware Tools is installed on the migrated virtual machine and migration completes.

If the source does not power off, an attempt is made to power off the replica virtual machine.

If the replica virtual machine 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 virtual machine 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 virtual machine using vCenter, power-off source virtual machine (if not already), and power-on Migrated virtual machine.

**Architectural Considerations for OSAM Deployment**

The OS Assisted Migration (OSAM) service includes several components that work together for connecting and forwarding guest workloads in the source environment.

Refer to the following considerations when deploying and operating OS Assisted Migration in your environment.

- HCX deployments for OSAM migrations assume that there is (at minimum) a vSphere HA-compliant cluster to host the source HCX components (HCX-SGW).
- The HCX Sentinel Agents are installed in the non-vSphere (KVM or Hyper-V) workloads and automatically make connections to the HCX Sentinel Gateway.
- The HCX Sentinel Gateway that receives encrypted connections from the Sentinel Agents must be deployed in a vSphere environment, with the other HCX source appliances.
- For HCX Network Extension with OSAM deployments, VLANs in the non-vSphere environment must be made available to the Distributed Switch used for HCX Network Extension. This may require a network change.
- When the non-vSphere (KVM or Hyper-V) environment is collocated in the same data center or Metro area, it is an option to deploy the HCX Connector and source Service Mesh components at the destination vCenter Server.

**OS Assisted Migration Limitations**

The OS Assisted Migration service supports a variety of hypervisors and guest operating systems in both Linux and Windows environments with limitations and requirements that are both common and specific to these environments.

**OS Assisted Migration in Linux and Windows Environments**

The OS Assisted Migration service has limitations that are common to both Linux and Windows environments.
This section provides a list of service limitations common to any environment where OS Assisted Migration is deployed. For a list of limitations specific to Linux deployments, see OS Assisted Migration in Linux Environments. For a list of limitations specific to Windows deployments, see OS Assisted Migration in Windows Environments.

- Guest virtual machines with locale and UI language other than English US are not supported.
- An SDR appliance can support up to 50 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 50.
- Multiple Service Mesh deployment is supported since HCX release R144, Service Mesh, meaning you can create multiple SGW and SDR.
- Guest virtual machines can only be migrated to a datastore that is accessible by the SDR.
- Redeployment of SGW and SDR appliances is not allowed when any migration is in-progress.
- Linked mode VCs are not supported.
- VMC 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.
- Migration using PowerCLI 11.5 is not supported.
- The OSAM migration service applies the default storage policy to the migrated VMs and their disks. Currently, the OSAM service does not support a user-selected storage policy.
- UEFI-based source systems using legacy BIOS boot mode are not supported
- OSAM migrations with vCD as target are not supported using PowerCLI.
- Changes to source Guest virtual machine configurations while a migration is in progress may not take effect in migrated virtual machines and sometimes may lead to migration failure.
- Mobility Group migration is not supported through PowerCLI for vCD (all services)

OS Assisted Migration in Linux Environments

The OS Assisted Migration service has specific limitations in Linux environments.

This section provides a list of supported guest operating systems and service limitations specific to a to a Linux environment where OS Assisted Migration is deployed. For a list of limitations that are common to any OS Assisted Migration deployment, see OS Assisted Migration in Linux and Windows Environments.

Supported Guest Operating Systems

<table>
<thead>
<tr>
<th>Supported OS versions on KVM Hypervisor (BIOS and EFI)</th>
<th>Supported OS versions on Hyper-V Hypervisor (BIOS and EFI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS 6.1 - CentOS 6.10 (32-bit, 64-bit)</td>
<td>RHEL 7.1 - RHEL 7.8 64-bit (BIOS/GEN-1 &amp; UEFI/GEN-2)</td>
</tr>
<tr>
<td>RHEL 6.1 - RHEL 6.10 (32-bit, 64-bit)</td>
<td>RHEL 6.4 - RHEL 6.10 32-bit and 64-bit (BIOS/GEN-1 Only)</td>
</tr>
</tbody>
</table>
### Supported OS versions on KVM Hypervisor (BIOS and EFI)

<table>
<thead>
<tr>
<th>Supported OS versions on KVM Hypervisor (BIOS and EFI)</th>
<th>Supported OS versions on Hyper-V Hypervisor (BIOS and EFI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS 7.1 - CentOS 7.8 (64-bit)</td>
<td>CentOS 7.0 - CentOS 7.8 64-bit (BIOS/GEN-1 &amp; UEFI/GEN-2)</td>
</tr>
<tr>
<td>RHEL 7.1 - RHEL 7.8 (64-bit)</td>
<td>CentOS 6.4 - RHEL 6.10 32-bit and 64-bit (BIOS/GEN-1 Only)</td>
</tr>
<tr>
<td>Ubuntu 14.04 LTS (32-bit, 64-bit)</td>
<td>Ubuntu 14.04 LTS 32-bit (BIOS/GEN-1) and 64-bit (BIOS/GEN-1 &amp; UEFI/GEN-2)</td>
</tr>
<tr>
<td>Ubuntu 16.04 LTS (32-bit, 64-bit)</td>
<td>Ubuntu 16.04 LTS 32-bit and 64-bit (BIOS/GEN-1 &amp; UEFI/GEN-2)</td>
</tr>
<tr>
<td>Ubuntu 18.04 LTS (64-bit)</td>
<td>Ubuntu 18.04 LTS 64-bit (BIOS/GEN-1 &amp; UEFI/GEN-2)</td>
</tr>
</tbody>
</table>

### Linux Limitations

- Block devices (partitions) with unrecognized content will not be migrated to the destination.
  - Unsupported file systems (supported file systems: ext2, ext3, ext4, XFS).
  - Unmounted file systems (Linux specific).
  - Unknown content with a partition or a block device.
  - Encrypted file systems.
  - md devices (software RAID).
- Statics routes are not supported.
- VLAN interfaces are not supported.
- On RHEL/CentOS 7.0, 7.1, and 7.2, the XFS file system UUID is not restored to the original UUID for the file system where /boot resides because mkfs.xfs does not support the functionality (-m option). A new random UUID is generated. Modifying the UUID after the file system is created triggers RHEL bug 1579390.
- `/etc/fstab` entries for removable media (floppy, CD) are not supported; such entries must be commented-out before migration.
- 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.
- 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.

### OS Assisted Migration in Windows Environments

The OS Assisted Migration service has specific limitations in Windows environments.

This section provides a list of supported guest operating systems and service limitations specific to a Windows environment where OS Assisted Migration is deployed. For a list of limitations that are common to any OS Assisted Migration deployment, see OS Assisted Migration in Linux and Windows Environments.
Supported Guest Operating Systems

<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>Windows Server 2012</td>
<td>Windows Server 2012</td>
</tr>
<tr>
<td>Windows Server 2012 R2</td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td>Windows Server 2008 R2 (64-bit)</td>
<td>Windows Server 2008 R2 (64-bit)</td>
</tr>
</tbody>
</table>

Windows Limitations

- No support for syncing logical volumes.
- Only basic MBR and basic GPT disks are supported. Dynamic GPT and Dynamic MBR disks are not supported.
- 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 the 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 before migration are not usable on the migrated system.
- VLAN interfaces are not supported.
- 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.
- 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.
- Do not run Windows updates on the source system during a migration. If Windows updates are in progress, the migration can fail.
A Windows source system configured as a failover cluster node is not supported.

**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.

Migrations are always configured using the HCX Connector or Cloud system that initiated site pairing. In Cloud-to-Cloud deployments with bi-directional site pairing, HCX in both paired sites can initiate migrations. For more information, see Adding a Site Pair.

The HCX system automatically detects virtual machine disk additions or removals and reconfigures running migrations to accommodate these changes. These disk changes are honored only if the changes occur before the migration switchover phase. If disk changes occur during the switchover phase, the changes are not recognized, which can affect the success of the migration operation. Support for adding or removing disks is available only with Bulk and Replication Assisted vMotion migrations.

Taking snapshots of a VM during migration, either manually or via a third-party backup solution, it can disrupt the migration process. In order to prevent any impact, it is required to stop those services that may create or remove snapshots during migration. Refer to KB79220 for more information.

**Note** For the operational limits supported with HCX migrations, see Chapter 7 Configuration and Service Limits for VMware HCX.

**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.

3. 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 in-progress migrations.

For OSAM, the effect of canceling a migration depends on the state of the migration when selecting the Cancel 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.

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 Cancel Migration. This operation can take several minutes. When finished, the UI displays the message Migration cancelled.

Managing Failed or Canceled Migrations

Following a failed or canceled migration, you can use the Force Cleanup selection to clear internal operations and processes manually.

Sometimes following a failed or canceled migration, the system might not clean up migration-related processes that were started but did not complete. These processes occur on both the source and destination systems. If migration clean-up does not succeed, future migration operations can fail.

The Force Cleanup selection provides the method for manually cleaning up failed or canceled system migration processes.

Procedure

1  Navigate to Services > Migration > Tracking.

2  Review the Progress and Status columns for Cancelling Migration or Migration Failed messages.

   If the message is Migration Cancelled, the clean-up operation was successful and you can skip this procedure.

3  Expand the selection for the unsuccessful migration.

4  Click Force Cleanup.

   A pop-up window appears prompting you to confirm the clean-up operation.

   Note  Ignore the check box labeled Local Cleanup Only, which is provided only for special cases. It is a best practice always to clean up both the source and destination sides of a failed or canceled migration.

5  Click Yes.

What to do next

If the clean-up operation did not succeed, click Force Clean again. Repeat the clean-up operation until it succeeds.

Clearing the Migration History

You can clear the migration activity for a site using the Archive option.

Use the Archive option to clear failed, canceled, and completed migration activity. Clearing the migration history updates the HCX Dashboard migration counters but does not remove the migration-related details from the HCX log files.
Procedure

1. Navigate to the HCX dashboard.

2. Select the Service > Migration > Tracking.
   - The Tracking window displays a summary of virtual machine migrations for a site pair.

3. Select the migration entries that you want to clear from the display.
   
   **Note** You cannot clear migrations that are in progress.

4. Click Archive.
   - A pop-up screen appears prompting you to acknowledge the request to archive the migration entries.

5. Click Archive.
   - The selected entries are cleared from the migration history.

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.

Migrations are always configured using the HCX Connector or Cloud system that initiated site pairing. In Cloud-to-Cloud deployments with bidirectional site pairing, HCX in both paired sites can initiate migrations. For more information, see Adding a Site Pair.

The HCX system automatically detects virtual machine disk additions or removals and reconfigures running migrations to accommodate these changes. These disk changes are honored only if the changes occur before the migration switchover phase. If disk changes occur during the switchover phase, the changes are not recognized, which can affect the success of the migration operation. Support for adding or removing disks is available only with Bulk and Replication Assisted vMotion migrations.

Taking snapshots of a VM during migration, either manually or using a third-party backup solution, it can disrupt the migration process. To prevent any impact, it is required to stop those services that may create or remove snapshots during migration. Refer to KB79220 for more information.

**Note** For the operational limits supported with HCX migrations, see Chapter 7 Configuration and Service Limits for VMware HCX.

Prerequisites

The HCX Enterprise license is activated.
Procedure

1. Open the HCX plug-in 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>
</table>
| Edit Group               | To display the Workload Mobility window, click this option. From this window, you have several options:  
- Add additional virtual machines to the group.  
- Change the default migration profile for the group.  
- Change the migration profile of individual virtual machines.  
- Delete a specific virtual machine from the group.  
- Restart failed or canceled migrations. |
| Delete Group             | 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. |

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, schedule, or archive 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>
</tbody>
</table>
| Cancel                   | 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.  
For information about cleaning up failed or canceled migrations, see Managing Failed or Canceled Migrations. |
| Archive                  | Clears the migration entry from the display. Use the Archive option to clear failed, canceled, and completed migration activity. Clearing the migration history updates the HCX Dashboard migration counters but does not remove the migration-related details from the HCX log files. |

**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.
HCX Integration with vRealize Network Insight

You can export waves of VMware vRealize Network Insight discovered applications to HCX for migration as Mobility Groups. HCX integration with vRealize Network Insight is available through API calls.

In many cases, the relationships, dependencies, and boundaries among application workloads is complex, and knowing what application to migrate and in which order can be challenging. vRealize Network Insight uses Application Discovery and Dependency Analytics to identify migration waves. From this information, vRealize Network Insight defines Application Groups that are then exported using public APIs to HCX as established Mobility Groups.

After HCX creates the Mobility Groups, you prepare for migration using the HCX Mobility Group configuration procedures.

**Note** All limitations and requirements for HCX migrations and migration types apply to Mobility Groups created from vRealize Network Insight.

**Prerequisites**

Public APIs are available for exporting vRealize Network Insight Application Groups to HCX as Mobility Groups. To view the HCX API for creating Mobility Groups, log in to access the HCX API documentation: https://hcx_ip_or_fqdn/hybridity/docs. Navigate to Mobility > Migration Group APIs in the documentation.

**Procedure**

1. Import the vRealize Network Insight discovered application groups into HCX using API calls.
2. Navigate to Services > Migration and verify that HCX created the Mobility Groups.

   **Note** Mobility groups created by vRNI have a vRNI label and a timestamp to differentiate them from other Mobility Groups created by HCX admins.

3. Configure the Mobility Groups for migration.

   All Mobility Group operations are available for configuration, including setting the migration type, scheduling the migration, and editing the group information. See Migrating Virtual Machines with Mobility Groups.

4. Complete the migration.

**Results**

The workloads included in the API are created and migrated as Mobility Groups in HCX.
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.

Limitations

VMware HCX Disaster Recovery has the following limitations:

- HCX DR does not support using datastore clusters for VM protection operations.
- Guest customization is not available for HCX DR protection or recovery operations.

Benefits

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.**

**While workloads are being protected by HCX Disaster Recovery, the VMware HCX system automatically detects virtual machine disk additions or removals and reconfigures running protections to accommodate these changes. HCX keeps monitoring such disk changes until workloads are recovered, or protection is removed on them.**

**Taking snapshots of a VM while protected, either manually or using a third-party backup solution, it can disrupt the replication process. To prevent any impact, it is required to stop those services that may create or remove snapshots during replication. Refer to KB79220 for more information.**

**Planning for HCX Protection**

HCX Disaster Recovery service operation requires planning for the amount of storage consumed at the target location.

**HCX Protection Workflow**

Replication based operations such as HCX Bulk Migration, Replication Assisted vMotion and HCX Disaster Recovery use the vSphere Replication technologies to transfer virtual machine disk data. When a virtual machine protection operation is first run, the replication engine performs a full synchronization of all the data that makes up the virtual machine to the target location datastore. Following that baseline synchronization, the system performs a delta synchronization, meaning that only changed data blocks are replicated.
Delta synchronization occurs based on the recovery point objective (RPO) interval configured for the virtual machine, creating a replication instance. The selectable RPO ranges from 5 minutes to 24 hours. For example, setting the Recovery Point Objective (RPO) to 2 hours means that the maximum data loss that your organization can tolerate is 2 hours.

Setting an RPO does not mean replication occurs on a specific interval. A replication instance reflects the state of a virtual machine at the time the synchronization starts. The system schedules replications so that the RPO is not violated. For example, assuming a 15 minute RPO, if the synchronization starts at 12:00 and it takes five minutes to transfer to the target site, the instance becomes available on the target site at 12:05. That instance reflects the state of the virtual machine at 12:00. The next synchronization can start no later than 12:10 so that instance is available no later than 12:15.

**Note** To determine the replication transfer time, the replication scheduler uses the duration of the last few instances to estimate the next one.

Following a full synchronization, the HCX DR service prompts you to run a test recovery operation to verify the replication.

**Using Snapshots with HCX DR Protection**

HCX allows for multiple recovery points, or replica instances, which are converted to snapshots when you recover a virtual machine. You set a retention policy for these instances by configuring a snapshot interval along with the number of snapshots to retain for each protected virtual machine. Snapshot intervals range from 1 hour to 7 days. The maximum number of snapshots taken during that interval can range from 1 to 24. For example, setting the number of snapshots to 4 and the snapshot interval to 1 day, means you can restore that virtual machine to any of 4 recovery points over the past 24 hours. In another example, setting the number of snapshots to 24 and the snapshot interval to 3-hours results in 8 snapshots per day for 4 days.

**Note** The RPO interval and snapshot interval may not be the same. Snapshots are taken from the latest replication instance based on the RPO. The RPO must be set low enough to create the number of configured snapshots. For example, setting a retention policy of 6 snapshots per day means the RPO period must not exceed 4 hours to create at least 6 replication instances in 24 hours.

With snapshots, delta synchronizations are written to a new (replica) disk created for the snapshot in the same datastore as the baseline. Each new snapshot becomes the child of the previous version. For example, the first snapshot (replica 1) becomes the child and the baseline becomes the parent and all delta synchronization are written to replica 1. When a second snapshot (replica 2) is created, replica 2 becomes the child and replica 1 becomes the parent, and all delta synchronizations are written to replica 2.

**Best Practices for HCX Protection Planning**

Storage and bandwidth planning for replication at the target site depends on several factors:

**Data set size**
Consider the data set for replication and the capacity of the virtual disks (VMDK files) that make up the target site virtual machine. Consider whether the target site virtual disks are thick- or thin-provisioned. For example, a 100 GB virtual disk that is thick-provisioned always consumes 100 GB. A 100 GB disk that is thin provisioned will consume only the actual amount of data stored on the disk up to 100 GB. While a thin provisioned disk may initially use only a fraction of the provisioned storage, it can grow to the fill the total storage space.

**Data change rate**

Consider the amount of data replicated to the target location based on the rate of change in source virtual machine data. For example, a source virtual machine disk with 50 GB of data has an estimated daily change rate of 5 percent, meaning 2.5 GB of data is replicated each day.

Also, consider the maximum amount of data transferred for any one replication instance. Network bandwidth must be capable of meeting the RPO interval for the amount of data transferred.

**Recovery Point Objective interval**

Assuming consistent rate of change on the source virtual machine, a lower RPO generally means smaller delta synchronizations but higher bandwidth consumption to meet the lower RPO. Setting the RPO interval to the largest interval that your organization can tolerate can help to reduce network issues.

**Network bandwidth**

The replication network bandwidth must be sufficient to meet the RPO interval for the amount of data transferred. For example, if the RPO interval is 15 minutes, and the rate of change during that period is 1 GB, the network must capable of transferring that amount of data during the 15 minute interval. Set the number of recovery points as low as possible while still meeting business requirements.

**Retention policy**

Having multiple recover points means having a copy of the point in time changes for each snapshot, which increases storage requirements by the amount of changes over the RPO interval times the amount of snapshots configured.

**Protection concurrency with migration operations**

Ongoing HCX migrations use the HCX Interconnect (HCX-IX) appliance for virtual machine disk replications. Resources used during a Bulk or RAV transfer affect the total resources available for HCX Disaster Recovery (and vice versa) when the same service mesh appliances are used for both services.

**Recovery and recovery testing**
During recovery operations, or when testing a recovery plan with HCX Disaster Recovery, additional space is consumed by each recovered virtual machine. Normally, redo logs are consolidated into the replica base disk or into other redo logs if multiple recover points is enabled. During a test recovery, some or all of the redo logs may be in use until the test recovery is cleaned up (completed). If redo logs are in use, HCX cannot consolidate the redo logs. Replication continues during a test recovery, which generates additional redo logs. The actual amount of storage capacity consumed depends on factors such as data change rates, replication frequencies, and how long the test recovery lasts.

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.

**Note** For the number of concurrent virtual machine protections supported with HCX, see Chapter 7 Configuration and Service Limits for VMware HCX.

**Procedure**

1. In the **vSphere Web Client**, navigate to VMware HCX.
2. Navigate to the **Disaster Recovery** tab and click **Protect VMs**. The **Protection Configuration** screen appears.

**Note** For the number of concurrent VM protections supported with HCX, see Chapter 7 Configuration and Service Limits for VMware HCX.

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 minutes – 24 hours.
  
  **Note** The 5 minute RPO requires the source host to be ESXi 6.0 or later for vSAN, and ESXi 6.5 for other supported datastores.

- **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.
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 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 and 8.3.
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\vCenter Site Recovery Manager\config\vmware-dr.xml to add the HCX extensions:

   `<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
- Managing HCX Alerts

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>
</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


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 procedure allows you to manually import and trust certificates from remote systems on the HCX Manager appliance.


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

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

4. Select the certificate import option: **File**, **URL**, or **Content**.

5. Enter the information for the selected option.
For example, when selecting the URL option, enter the IP or FQDN that the source HCX Manager uses to reach the HCX Cloud Manager.

6. Click **Apply**.

**Backing Up and Restoring the System**

You can 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 or SFTP server for uploading the backup file:
   a. Click the FTP server setting tab.
   b. Click Add.

      **Note**  The best practice to use a Linux-based OpenSSH host for file transfer operations.

   c. Enter the FTP or SFTP server information and click Save.

4. (Optional) Configure a backup schedule:

   **Note**  The best practice is to schedule Daily backups. 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.

   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:

   **Note**  If you have scheduled backups, the system automatically generates the backup file at the scheduled time and saves the file to the FTP or SFTP server.

   - To save the generated file to an FTP or SFTP server, check the box Upload to server.
   - 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 a 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.

**Managing HCX Alerts**

The HCX generates alerts with different severity levels to flag events such as migration, network stretch failure, or reachability issues connecting to an endpoint or paired site.

Based on the type of alert, you can perform various actions to acknowledge, reset, or suppress the message.
<table>
<thead>
<tr>
<th>Alert Type</th>
<th>Action</th>
<th>Action Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Acknowledge</td>
<td>The alert has been noted and the corrective actions will be taken. The HCX records the user who acknowledged the alert, including a time stamp for the entry.</td>
</tr>
<tr>
<td></td>
<td>Reset to Green</td>
<td>Action has been taken to correct the alert. The HCX records the user who resets the alert, including a time stamp for the entry. The alert is removed from the display.</td>
</tr>
<tr>
<td>Warning</td>
<td>Acknowledge</td>
<td>The alert has been noted and the corrective actions will be taken. The HCX records the user who acknowledged the alert, including a time stamp for the entry.</td>
</tr>
<tr>
<td></td>
<td>Reset to Green</td>
<td>Action has been taken to correct the alert. The HCX records the user who resets the alert, including a time stamp for the entry. The alert is removed from the display.</td>
</tr>
<tr>
<td>Info</td>
<td>Suppress</td>
<td>Signifies that the alert has been reviewed. The alert is removed from the display.</td>
</tr>
</tbody>
</table>

**Procedure**

1. Log in to the HCX Manager Service UI:
   - The system displays the HCX Dashboard.
2. To locate the Alerts panel, scroll through the display.
3. Review the list of alerts.
   - a. (Optional) Expand an entry to see more information regarding an alert.
   - b. (Optional) To sort the list by **Status**, use the Status filter to select **Info**, **Warning**, or **Critical**.
   - c. (Optional) To sort the list by **Entity Name** or **Creation Date**, select the respective filter and enter the search information.
4. To take action on an alert, click the ellipsis next to the alert, and select the action.
Updating VMware HCX

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

**Important** For details on the support and upgrade requirements for HCX service updates, see VMware HCX Release Notes.

This chapter includes the following topics:

- About HCX Service Updates
- Planning for HCX Updates
- HCX Service Update Procedures

**About HCX Service Updates**

HCX service updates may include new features, software fixes and security patches.

- HCX service updates are published periodically as a set for HCX Connector and HCX Cloud types.
- For example, the service update R137 provides both HCX Connector and HCX Cloud 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 rebooting. If the Interconnect services do not return to service within that time frame, contact VMware Support.
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. If HCX must 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:

1. Stop all migrations and DR protections
2. Unstretch the network, which removes Network Extension (HCX-NET-EXT) appliances
3. Delete the Service Mesh, which removes Interconnect (HCX-IX) and WAN Optimization (HCX-WAN-OPT) appliances
4. Remove site pairing
5. Remove the HCX Manager
6. 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 the 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](https://console.cloud.vmware.com)
   b Select your organization and data center (SDDC).
   c Select **Add Ons**.
   d Navigate to the SDDC tab and click **Open HCX**.
   e Enter the clouadmin@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](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
- HCX Password Recovery

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

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.

2 Select the box next to one or more logs that you want to generate.

3 Click Request.

4 After the bundle is prepared, you are prompted to download them.

5 (Optional) To allow the HCX Admin to download logs from your HCX system for troubleshooting, locate the Settings section at the bottom of the page, and select Auto Approve.

   Note This setting is available only from the HCX Manager Service UI.

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

1 Log in to the HCX Appliance Management interface: https://hcx-ip-or-fqdn:9443.

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**.
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 web-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 the 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.

HCX Password Recovery

You can reset the admin or root password on either the HCX Connector or HCX Cloud Manager.

If an account password is lost or forgotten, a standard Linux password recovery procedure can be used to reset it.

The recovery procedure, which requires a reboot of the HCX Connector or Cloud manager, does not impact the following scenarios:

- Network Extensions actively forwarding.
- Virtual machine protections in continuous synchronization.
- Migration operations in the transfer phase or "waiting for switchover."

To reset the root or admin password, see the VMware KB article 79362.

Prerequisites

Active migration and configuration workflows may be impacted by a password reset. Allow those operations to complete before proceeding to recover the password.
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
- VMware vCenter HCX Alarms

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 of panels. You can 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 site pair, click New Site Pairing. To view detailed instructions for adding a site pair, see <a href="#">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>Panel</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Alerts</td>
<td>Provides a comprehensive list of logged Alert messages: Critical, Warning, Info. For a description of Alert messages and available actions, see Managing HCX Alerts.</td>
</tr>
</tbody>
</table>
| Activity Logs | For the selected source system, displays a historical log of system tasks:  
|              | - Job Type  
|              | - Entity Name  
|              | - Percentage of task completed.  
|              | - Task status  
|              | - Task Start Time  
|              | - Task Completion Time  
|              | To change the source site or to display tasks by status (All, Running, Failed), select from the pull-down menus. Use the search field to identify specific tasks or groups of tasks. |

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.
- vRealize Operations version 8.1.1 or above requires HCX Management Pack 5.1.
- 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.
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 > Repository**.

8 Click **Add/Upgrade**.

9 Browse to the downloaded an HCX Management Pack PAK file.

10 If you had previously installed an HCX Management Pack, check the box that prompts you to install the PAK files even if it is already installed.

11 Click **Upload**. After the upload completes, click **Next**.

12 Accept the EULA, click **Next**.

13 After the installation is finished, click **Finish**.

   The Management Pack is listed in the Repository.

14 Navigate to **Administration > Solutions > Other Accounts**.

15 Add an HCX account:

   **Note** For each HCX Connector and HCX Cloud Manager that uses vRealize Operations, you must add an account.

   a Click **Add Account**.
   b Select the account type **HCX adapter**.
   c Enter a Cloud Account name.
   d Enter the HCX Connector or HCX Cloud Manager IP address.
   e Click + to add the vCenter credentials.
   f Enter the **Collector/Group** information or use the default entry.
   g Click **Validate Connection**.
      If the connection is not successful, verify the credentials and try again.
   h Click **Save**.
   i If prompted, accept the certificate.
   j Repeat this procedure for each HCX Connector and HCX Cloud Manager.

16 Create the vCenter Server accounts:

   **Note** For each vCenter Server associated with an HCX Connector and HCX Cloud Manager, you must add an account.

   a Navigate to **Administration > Solutions > Cloud Accounts**.
   b Click **Add Account**.
c Select account type vCenter.
d Enter a Cloud Account Name.
e Enter the vCenter Server IP address.
f Enter the vCenter credentials.
g Enter the Collector/Group information or use the default entry.
h Click Validate Connection.
If the connection is not successful, verify the credentials and try again.

17 Click Save.
18 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 main folder and navigate to 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 an error state. - Critical
Outgoing Replication is in an 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>
<tr>
<td>Widget 4</td>
<td>Mobility Groups</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>
DICE Integration for HCX

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><strong>API Key</strong></td>
<td>Provides API key information for the REST authentication with the DICE portal. Obtain this key from the DICE website under Account Settings in your profile.</td>
</tr>
<tr>
<td><strong>API Secret</strong></td>
<td>Provides API secret key information for the REST authentication with the DICE portal. Obtain this secret from the DICE website under Account Settings in your profile.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you must change any of the DICE parameters in the future, you must reenter the secret key.</td>
</tr>
<tr>
<td><strong>Customer ID</strong></td>
<td>Obtain this ID from your account team.</td>
</tr>
<tr>
<td><strong>Model ID</strong></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><strong>Note</strong></td>
<td>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 vCenter HCX Alarms

The HCX service generates default vCenter Alarms that are reported to vCenter Server.

You can use these alarms to trigger additional actions or notifications.

<table>
<thead>
<tr>
<th>HCX Event Alarm in vCenter (Event Code)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HCX RAV Migration Error Encountered (65005)</td>
<td>The HCX RAV Migration did not succeed. See the HCX Migration Tracker for details.</td>
</tr>
<tr>
<td>HCX Bulk Migration Error Encountered (65006)</td>
<td>The HCX Bulk Migration did not succeed. See the HCX Migration Tracker for details.</td>
</tr>
<tr>
<td>HCX vMotion Migration Error Encountered (65007)</td>
<td>The HCX vMotion Migration did not succeed. See the HCX Migration Tracker for details.</td>
</tr>
<tr>
<td>HCX Cold Migration Error Encountered (65008)</td>
<td>The HCX Cold Migration did not succeed. See the HCX Migration Tracker for details.</td>
</tr>
<tr>
<td>HCX RAV Migration Cancelled (66001)</td>
<td>The HCX Replication Assisted vMotion migration is cancelled.</td>
</tr>
<tr>
<td>vSphere Bulk Migration Cancelled (66002)</td>
<td>The HCX Bulk migration is cancelled.</td>
</tr>
<tr>
<td>HCX vMotion Migration Cancelled (66003)</td>
<td>The HCX vMotion migration is cancelled.</td>
</tr>
<tr>
<td>HCX Cold Migration Cancelled (66004)</td>
<td>The HCX Cold migration is cancelled.</td>
</tr>
<tr>
<td>HCX Connector Database Upgrade Failed (com.vmware.hcx.enterprise.database.upgrade)</td>
<td>The HCX Connector database upgrade has failed. Contact VMware Support.</td>
</tr>
</tbody>
</table>
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:
- HCX Services for VMware Cloud on AWS
- Topology Overview of VMware HCX on VMware Cloud on AWS
- Deploying HCX from the VMC Console
- Configuring VMware HCX for Direct Connect Private Virtual Interfaces
- Scaling Out HCX Deployments in a Multi-Edge SDDC
- Configuring HCX for VMware Transit Connect

**HCX Services for VMware Cloud on AWS**

HCX for VMware Cloud on AWS includes support for all HCX Advanced services as well as select HCX Enterprise features and services with no additional license requirement and at no additional cost.

In addition to all HCX Advanced services, installing HCX for VMware Cloud on AWS provides support for these HCX Enterprise class services:
- Replication Assisted vMotion
- Mobility Optimized Networking
- Traffic Engineering features
  - Application Path Resiliency
  - TCP Flow Conditioning
- Mobility Groups

**Note** HCX Mobility Groups support integration with vRealize Network Insight, available as a separate license. This integration allows the creation of mobility groups from VMware vRealize Network Insight discovered applications to HCX for wave migration.
For a detailed description of HCX services, see Chapter 2 VMware HCX Services.

Requirements

- HCX Advanced services are available with all currently supported HCX releases.
- HCX for VMware Cloud on AWS Enterprise-class services require HCX release R145 or above at both the HCX Cloud (destination) site and HCX Connector (source) site.

  Note: For new installations or upgrades, the HCX Connector (source) site inherits the available services from the HCX for VMware Cloud on AWS license, and no additional license is required at the source site.

- Site paring with HCX Cloud Manager can be established through Internet network (INET), AWS Direct Connect, or VPN connections.
- HCX Interconnect and HCX Network Extension tunnels can be established through INET and AWS Direct Connect only. Connectivity through a VPN tunnel terminated on the NSX Edge for the SDDC is not supported.

HCX Replication Assisted vMotion for VMware Cloud on AWS

HCX Replication Assisted vMotion works the same in VMware Cloud on AWS SDDCs as it does in on-premises or private cloud environments.

- The service must be selected in the Compute Profile of both the source and destination sites.
- The service must be enabled in the Service Mesh deployed for the respective source and destination Compute Profiles.

To migrate virtual machines using Replication Assisted vMotion, see Chapter 10 Migrating Virtual Machines with VMware HCX.

HCX Mobility Optimized Networking for VMware Cloud on AWS

HCX Mobility Optimized Networking (MON) functions the same in VMware Cloud on AWS SDDCs as it does in on-premises or private cloud environments.

- Mobility Optimized Networking is disabled by default for an Extended Network.
- You must explicitly set Mobility Optimized Networking when extending a network.
- You can set Mobility Optimized Networking on an existing network extension.

  Note: For existing network extensions, the network may experience a brief outage while the system publishes routes corresponding to the migrated virtual machines residing on the MON enabled extended network.

To use HCX Mobility Optimized Networking, see HCX Network Extension with Mobility Optimized Networking for NSX-T.
HCX Traffic Engineering for VMware Cloud on AWS

The Application Path Resiliency and TCP Flow Conditioning features define the HCX Traffic Engineering services. These services function the same in VMware Cloud on AWS SDDCs as they do in on-premises or private cloud environments.

- For new installations, optionally select these services when creating the Service Mesh.
- For existing installations, edit the Service Mesh to select these features.
- For existing installations, updating the Service Mesh for Application Path Resiliency has the following operational impact:
  - Redeployment of both the Interconnect and Network Extension appliances.
  - Disruption of Bulk and vMotion migrations. Quiese migration operations prior to finishing the Service Mesh update.
  - Brief disruption of traffic over extended networks.

To configure the HCX Service Mesh for these features, see Creating a Service Mesh.

HCX Mobility Groups for VMware Cloud on AWS

HCX Mobility Groups function the same in VMware Cloud on AWS SDDCs as it does in on-premises or private cloud environments. Support for Mobility Groups includes integration with vRealize Network Insight.

- Mobility Groups support assembling one or more virtual machines into logical sets for execution and monitoring of migrations as a group.
- Migration management functionality allows you to edit and delete groups, initiate and stop migrations, and schedule migrations.
- Through integration with VMware vRealize Network Insight, you can export waves of discovered applications to HCX for migration as Mobility Groups.

For more information about Mobility Groups, see Migrating Virtual Machines with Mobility Groups.

For more information about Mobility Group integration with vRealize Network Insight, see HCX Integration with vRealize Network Insight.

Topology Overview of VMware HCX on VMware Cloud on AWS

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>VMware HCX WAN Optimization</td>
<td>- Deduplication, compression, and line conditioning of VMware HCX migration and protection network flows.</td>
</tr>
<tr>
<td>VMware HCX Network Extension</td>
<td>- A maximum of eight networks can be extended to the SDDC per VMware HCX Network Extension appliance.</td>
</tr>
<tr>
<td></td>
<td>- After a Network Extension operation, there is a five minute delay until the network is available for a migration operation.</td>
</tr>
<tr>
<td></td>
<td>- Network Extension with Mobility Optimized Networking is available with VMware Cloud on AWS NSX-T SDDCs.</td>
</tr>
<tr>
<td>VMware HCX over AWS Direct Connect</td>
<td>- VMware HCX supports connections over AWS Direct Connect with a Private Virtual Interface.</td>
</tr>
</tbody>
</table>

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 Click View Details.

The SDDC interface opens.

3 On the Add Ons tab of your SDDC, click Open HCX on the HCX card.

The VMware HCX interface opens.

4 Navigate to the SDDC 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.

5 Create a firewall rule to open the necessary ports to access the HCX Cloud Manager.

   a From the VMC Console, select Networking & Security.

   b Under Security go to Gateway Firewall and select Management Gateway.
Click **Add Rule** and create a new inbound firewall rule with these parameters:

- Source: Where the connection to the HCX manager is coming from.
- Destination: **HCX**
- Services: **HTTPS (TCP 443)**

**Note** HCX is already a system defined group that can be selected as a destination. A user-defined group can be created for the source.

to save the new rule, click **Publish**

6 On the **Add Ons** tab of your SDDC, click **Open HCX** on the **HCX** card.
A new browser tab opens.

7 Navigate to the SDDC tab and click **Open HCX**.
The VMware HCX Cloud service interface opens.

8 Enter the cloudadmin@vmc.local user and password and click **Log In**.

**Note** Use the vCenter password.

**Results**
The HCX Cloud Manager UI is available for HCX operations.

**What to do next**
Navigate to **Administration > System Updates** and download the HCX Connector OVA, which is needed for the on-premises HCX installation. Downloading the HCX Connector OVA is detailed in *Downloading the HCX Connector OVA*. For a complete installation workflow, see **HCX Installation Workflow for HCX Public Clouds**.

**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 the VMware Cloud on AWS management subnet CIDR block or any other IP range already in use for services in VMC. Overlap 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.

**Procedure**

1. Log in to the VMC Console at [vmc.vmware.com](http://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 SDDC 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 are reachable over the AWS Direct Connect.

**Figure 17-1. VMware HCX over Direct Connect Private Virtual Interface**
Scaling Out HCX Deployments in a Multi-Edge SDDC

An HCX Service Mesh configured with Multi-Edge traffic groups uses dedicated high-bandwidth network paths for HCX Network Extension and Migration operations.

About HCX with Multi-Edge SDDC

In the default configuration, an SDDC network has a single edge (T0) gateway through which all North-South traffic flows. You configure additional bandwidth for North-South traffic flows for direct-connect networks by creating one or more network traffic groups, each of which creates an additional T0 edge router in AWS. Traffic groups are created for each SDDC using the VMC Console.

When traffic groups are created in VMware Cloud on AWS, the HCX Cloud Manager at the destination site automatically detects those groups and adds them to the list of networks in the HCX Network Profile. HCX assigns a logical name to the traffic group, and the HCX Manager communicates any changes to the SDDC. HCX Manager can take advantage of the bandwidth provided by T0 routers to enhance HCX operations.

Requirements for HCX Multi-Edge Deployments

The HCX Multi-Edge solution requires AWS SDDCs configured with VMware Transit Connect.

Best Practices and Limitations

Review these best practices and systems limitations when scaling-out HCX deployments.

- It is a best practice to create a dedicated traffic group for HCX virtual machine migration.
  - The HCX-IX migration services cannot load balance across multiple traffic groups.
- It is a best practice to create a traffic group for HCX Network Extension.
  - If using a single traffic group for Network Extension, assign a /25 prefix to accommodate the maximum Network Extension appliance scale.
  - Create multiple traffic groups to distribute network extension traffic, which can be done using smaller prefixes.
  - The HCX enabled SDDC supports a maximum of 100 HCX Network Extension appliances.

Configuring SDDC Traffic Groups in HCX

You can configure HCX to associate a traffic group with an Uplink Network in the Multi-site Service Mesh for improved migration or workload bandwidth.
By default, VMware HCX uses the management network for all uplink traffic. By overriding the default Uplink Network for the destination site with a specific traffic group, you isolate traffic for the HCX service. By isolating network traffic in this way, you gain any performance advantage by separating the traffic and utilizing the available bandwidth of the T0 router. For example, you can isolate migration and workload traffic by creating one Service Mesh for Bulk Migration and one Service Mesh for Network Extension. Within each specific Service Mesh, you then configure a unique traffic group for the Uplink Network.

Prerequisites

- Each SDDC is configured with traffic groups.
- A separate Service Mesh exists for each HCX service that is using traffic groups. For more information about creating and modifying a Service Mesh, see Creating a Service Mesh.

Procedure

1. In the HCX Cloud Manger UI, Navigate to Interconnect > Network Profile. The system displays the available SDDC traffic groups.
2. Select a traffic group Network Profile, and click Edit. They system displays the profile information for the traffic group.
3. Enter a logical name for the Network Profile.
4. Under IP Pools, add a range of IP addresses and enter the network prefix.
   The HCX Manager communicates with the SDDC, updating the traffic group with an association map that includes the HCX network profile name and prefix list. At the same time, the traffic group becomes available in the Service Mesh for overriding the uplink networks at the destination site.
5. Click Update.
6. In the HCX Manager UI at the source site (HCX Connect), navigate to Interconnect > Service Mesh.
7. Select the Service Mesh in which to add the traffic group, and click Edit.
8. Step through the Service Mesh dialog until you come to Override Uplink Network profiles.
9. Expand the list of Destination Site Uplink Network Profiles.
10. Select the named network to associate with the traffic group for the Service Mesh, and click Continue.
11. Step through the rest of the Service Mesh dialog, and click Finish.
Results

The HCX services enabled in the Service Mesh are configured to use the T0 gateway created by the traffic group.

**Note** Before you can delete a traffic group from an SDDC, you must either delete the HCX Service Mesh that is using the traffic group or override the Uplink Network in the Service Mesh with a different network.

What to do next

Repeat this procedure to isolate traffic and enhance bandwidth for other HCX services.

Configuring HCX for VMware Transit Connect

You can configure VMware HCX to use VMware Transit Connect™ for migration and network extension traffic.

VMware Transit Connect connects your SDDCs and VPCs to provide high-bandwidth, low-latency connections between SDDCs in the group and to other VPCs in the same region. The Direct Connect network profile is used for Transit Connect. For instructions on how to configure Direct Connect, refer to the section "Configuring VMware HCX for Direct Connect Private Virtual Interfaces." Configuring VMware HCX for Direct Connect Private Virtual Interfaces