Getting Started with VMware HCX

05 AUG 2021
VMware HCX 4.2

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

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About Getting Started with VMware HCX

1

This guide describes how to plan for installation and operatation of VMware HCX services in a vSphere data center.

Information in this guide includes key concepts necessary to planning for deployment in your environment. The guide provides a series of checklists. These checklists help you to gather the information necessary deployment by identifying the compute and network details used during the system installation and configuration. For actual installation and operational details, see VMware HCX User Guide.

Intended Audience

This information is for anyone who wants to deploy 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

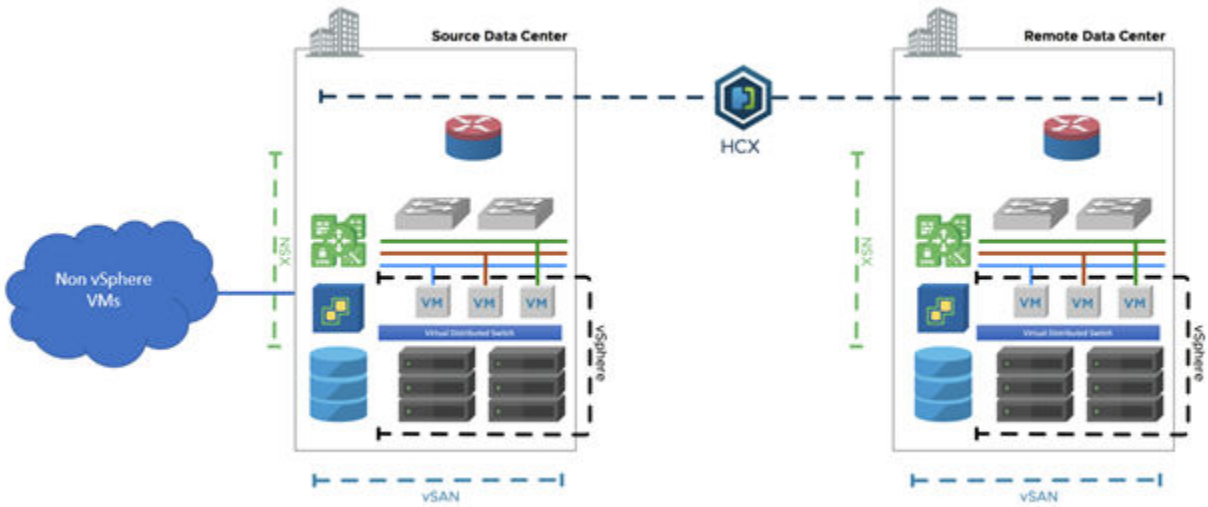
VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms used in the VMware technical documentation, go to http://www.vmware.com/support/pubs.

Introduction to HCX Deployments 2

Deploying VMware HCX requires information about your vSphere sites, networks, and configurations. Collecting the required configuration details and making some design choices in advance can greatly reduce the time and resources to deploy. Install checklists are provided in this document to help with configuration planning. Deployment concepts, considerations, and practices are explored.

Note This document supplements the information found in the VMware HCX User Guide. Operational procedures for HCX are not included in this document.

Overview



HCX provides services between two or more distinct environments. The environments might be running legacy vSphere, or they might be running modern vSphere SDDC, they might also be VMware-based public cloud instances. With OS Assisted Migration, HCX provides services to migrate non-vSphere workloads. See VMware HCX Deployment Types.

This chapter includes the following topics:

- HCX Connector and HCX Cloud Installations

HCX Connector and HCX Cloud Installations

In HCX , there is a notion of an HCX source and HCX destination environment. There is a specific HCX installer that should be used depending on the environments.

The table highlights the differences between the two HCX Manager/Installation types:

	HCX Connector (previously Enterprise)	**HCX Cloud**
When to use:	Use the HCX Connector with the vCenter Server containing the virtual machines that will be migrated. The HCX Connector is always an HCX source that connects to an HCX Cloud. **Note** If the environment is also used as a destination for site pairing and Network Extension, use the HCX Cloud instead. Installations using OS Assisted Migration require HCX Connector at the source.	Use the HCX Cloud installer with the vCenter Server that is the target of site pairing requests, network extensions, and virtual machine migrations. The HCX Cloud can also serve as the source of a site pair in HCX cloud-to-cloud installations. **Note** OS Assisted Migration does not support cloud-to-cloud installations. For OS Assisted Migration, you must have HCX Connector installed as the source.
Installer	Option 1 - Use a download link from a deployed HCX Cloud system. Option 2 - Use the Download Link API to get a download link for the latest HCX Connector build.	In a public cloud deployment, HCX Cloud is automatically installed when the service is enabled. In private cloud installations: Option 1 - Use the installer in downloads.vmware.com. This installer updates itself to the latest release. Option 2 - Use the Download Link API to get a download link for the latest HCX Cloud build.
Supports legacy vSphere (within Technical Guidance)	Yes	No
Requires Generally available version of vSphere	N/A	Yes
Requires NSXv or NSX-T	No	Yes
Endpoint for Site Pairing (The HCX destination)	No	Yes
Can initiate Site Pairing (the HCX source)	Yes	Yes* * Cloud to Cloud.
Licensing/Activation	No* * Uses HCX Cloud-based activation/ license.	Yes * * Public cloud HCX systems are activated through the cloud service. * Private cloud HCX systems are licensed based on NSX Enterprise + or VCF bundle.

More About the HCX Cloud Environments

The environment that is running HCX Cloud is generally the destination for HCX site pairing, for network extensions and workload migration (but they can also be the source site when connecting to another private or public HCX cloud system). The HCX Cloud site is always a Software Defined Data Center like VMware Cloud Foundation or similar environments with new vSphere and NSX, built a la carte. HCX public clouds like VMware Cloud on AWS, IBM Cloud, Azure VMware Solution by CloudSimple are all HCX Cloud environments. These are characteristics of the HCX destination environment:

- The destination environment and can be the target for Site Pairing, Network Extension, and virtual machine migrations with HCX.
- HCX at the destination is always deployed using the HCX Cloud Manager OVA.
- HCX requires the destination environment to use current vSphere. See Software Version Requirements (destination environment).
- HCX requires the destination environment to use current NSX-T (or NSX for vSphere) that meets at minimum all the NSX Requirements for HCX Appliance Deployments. Additional Requirements for Network Extension may apply.
- When the destination is an HCX enabled Public Cloud provider (like the VMware Cloud on AWS):
  - The public cloud provider installs and configures the HCX Cloud Manager on behalf of the tenant (the process varies slightly by public cloud provider).
  - The public cloud provider activates HCX or provides activation keys.
- When the destination is on-premises or private cloud:
  - VMware Cloud Foundation Enterprise meets all the destination environment and licensing requirements for HCX.
  - The user installs and configures HCX Cloud Manager.
  - The HCX Cloud Manager is licensed using NSX Data Center Enterprise plus.
- The HCX Cloud Manager installation carries higher requirements, but it can be both the source and the target for Site Pairing, HCX Network Extension operations and Service Mesh deployments.

  Note OS Assisted Migration does not support cloud-to-cloud installations. For OS Assisted Migration, you must install HCX Connector as the source.

More About the HCX Connector Environments

In public cloud-based deployments (for example, HCX with VMware Cloud on AWS), the HCX Connector is deployed on-premises (the cloud instance runs HCX Cloud).

In private cloud deployments (for example, Legacy to a modern migration), the legacy environment will use the HCX Connector (the modern private cloud environment runs HCX Cloud).

- An HCX Connector environment is always the source for **Site Pairing**, for **Service Mesh** deployments.
- An HCX Connector cannot be the target for HCX **Site Pairing**.
- HCX Connector cannot site pair with another HCX Connector, the destination must always be a private or public cloud with HCX Cloud.
- The HCX Connector's IX and NE appliances are always the Tunnel initiators when a Service Mesh is created.
- HCX Connector supports lower software versions found in out of support environments that cannot be upgraded.
- An HCX Connector installation does not require NSX to be present, except when extending NSX networks.
- A legacy vSphere environment is always considered the source HCX system, and is installed using the HCX Connector OVA. See Software Version Requirements (Source Environment Requirements).
- For source environments using OS Assisted Migration, HCX Connector is required.
- When the HCX Connector environment also meets the destination site requirements, consider installing HCX Cloud. See Software Version Requirements (destination environment).
- HCX supports interoperability with legacy environments for migration or evacuation, there is no support for migrating to a legacy environment.

Install Checklist A - HCX with a Private Cloud Destination Environment

3

This install checklist is written for fully private deployments, where HCX has to be prepared in each environment (in public cloud HCX deployments, the provider handles HCX installation and bootstraps an configuration using public IPs).

This document presented in a source vSphere to destination vSphere format:

- It is assumed that the source vSphere contains the existing workloads and networks that will be migrated. This environment can be legacy vSphere (within Technical Guidance) or modern (Generally Available versions).
- It is assumed that destination is a modern private cloud, or a VMware Cloud Foundation deployment that is the target for HCX network extensions, migrations, and services.
- Deployment variations like multi-vCenter Server, multi-cloud, vCloud Director, OS-Assisted or performance-centric implementations are outside the scope of this checklist.
- For checklist items specific to using OS Assisted Migration, see Checklist C.

Use Cases and POC Success Criteria

"How am I doing with HCX? How will I define a success in my proof of concept?"

▢ What defines the success criteria for the HCX proof of concept?	Clearly define how the success criteria. For example: ■ Extend 2 test networks. ■ Live migrate virtual machine. ■ Test HCX L2 connectivity using over the extended network. ■ Reverse migrate a VM. ■ Bulk Migrate a VM.
▢ Ensure features are available with the trial or full licenses obtained.	The core migration services (vMotion, Bulk, Optimization, and Network Extension) are available with HCX Advanced licensing. OSAM, RAV, and SRM integration require HCX Enterprise licensing. Trial license allows up to 20 migrations.
▢ Understand technology-specific restrictions.	For any HCX technologies that are used, have awareness of possible restrictions and requirements. For example, if a zero downtime application must be migrated, HCX vMotion or RAV should be used. In this case, one should note that "vMotion based migrations require Virtual Machine Hardware Version 9 or above." Restrictions like this one are documented in the About section for the specific migration type in the HCX User Guide.

Collect vSphere Environment Details

This section identifies vSphere related information that should be known about the environments that is relevant for HCX deployments.

Environment Detail	Source Environment	Destination Environment
▢ vSphere Version	■ vSphere version must be within Technical Guidance.	■ vSphere version must be generally available.
▢ Distributed Switches and Connected Clusters	■ Understand the relationships between clusters and the Distributed Switches. ■ Imported Distributed Switches are not supported for the HCX-NE service.	■ Understand the relationships between clusters and the NSX Transport Zone. HCX only deploys and extends networks to clusters included in the Transport Zone.
▢ ESXi Cluster Networks	■ Identify the ESXi Management, vMotion, and Replication (if it exists). VSS PG or DPG Names, VLANs, and Subnets. ■ If these networks vary from cluster to cluster, additional configuration will be needed. ■ Identify available IPs (HCX participates in these networks)	■ Identify the ESXi Management, vMotion, and Replication (if it exists). VSS PG or DPG Names, VLANs, and Subnets. ■ If these networks vary from cluster to cluster, additional configuration will be needed. ■ Identify available IPs (HCX will participate in these networks)
▢ NSX version and configurations:	■ NSX is not required at the source, but is supported for NSX Network Extension. See NSX Requirements for the HCX Connector Installation.	■ Must be NSX-T or NSX-V . See NSX Requirements for HCX Appliance Deployments. ■ NSX-T T1 or NSX-V ESG or DLR is required for Network Extension.
▢ Review and ensure all Software Version Requirements are satisfied.		

Environment Detail	Source Environment	Destination Environment
▢ vCenter Server URL:	■ https://vcenter-ip-or-fqdn	■ https://vcenter-ip-or-fqdn
▢ administrator @vsphere.local or equivalent account.		
▢ NSX Manager URL:	■ NSX is optional. It is only required when HCX is used to extend NSX networks	■ https://nsxmgr-ip-or-fqdn
▢ NSX admin or equivalent account.	■ If HCX is used to extend NSX networks, know the administrator account for the NSX registration step.	■ A full access Enterprise Administrator user is required when registering the NSX Manager.
▢ Destination vCenter SSO URL :	■ Use the SSO FQDN as seen in the vCenter Advanced Configurations (config.vpxd.sso.admin.uri)	■ Use the SSO FQDN as seen in the vCenter Advanced Configurations (config.vpxd.sso.admin.uri).
▢ DNS Server:	■ DNS is required.	■ DNS is required.
▢ NTP Server:	■ NTP server is required.	■ NTP server is required.
▢ HTTP Proxy Server:	■ If there is an HTTPS proxy server in the environment, it should be added to the configuration.	■ If there is an HTTPS proxy server in the environment, it should be added to the configuration.

Planning for the HCX Manager Deployment

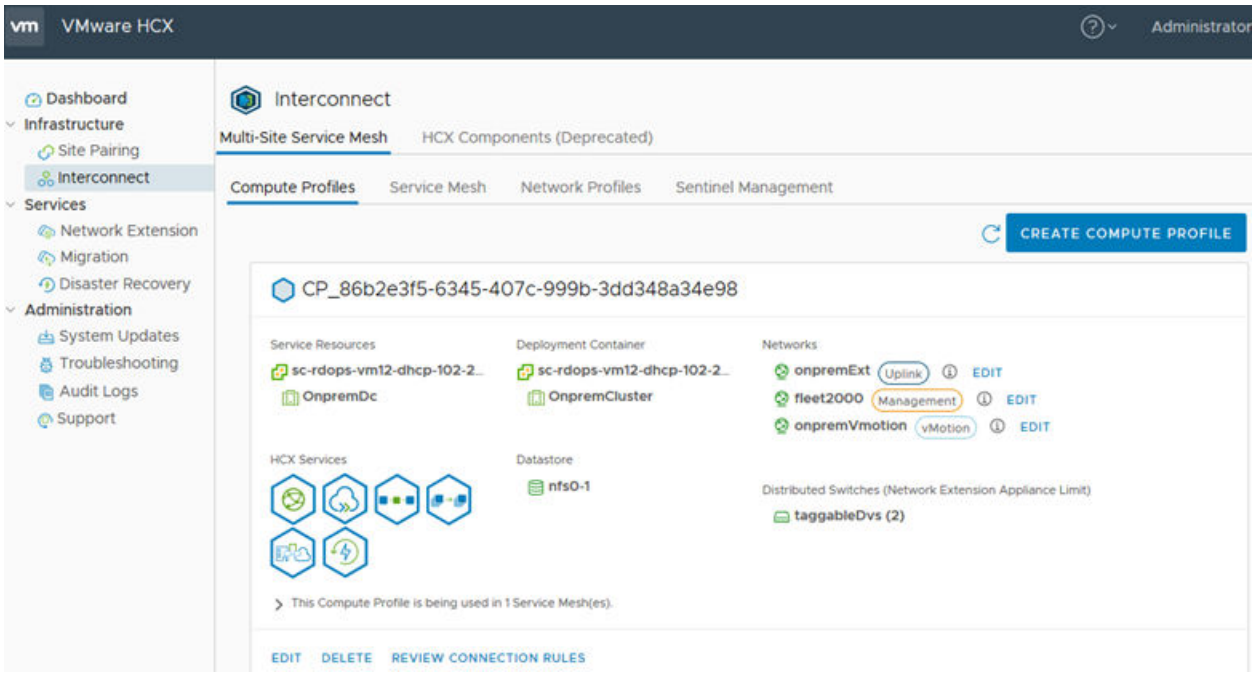
This section identifies information that should be known before deploying the source and destination HCX Manager systems.

	Source HCX Manager (type: Connector or Enterprise)	Destination HCX Manager (type: Cloud)
▢ HCX Manager Placement/ Zoning:	■ The HCX Manager can be deployed like other management components (like vCenter Server or NSX Manager). ■ It does not have to be deployed where the migration workloads reside.	■ The HCX Manager can be deployed like other management components (like vCenter Server or NSX Manager). It does not have to be deployed where the migration workloads reside.
▢ HCX Manager Installer OVA:	■ The HCX Manager download link for the source is obtained from the destination HCX Manager, in the System Updates UI. ■ If OVA download links were provided by the VMware team, the file for the source is named `VMware-HCX-Connector-x.y.z-########.ova`.	[The OVA has been downloaded.] ■ HCX Manager installer OVA can be obtained from downloads.vmware.com. ■ If OVA download links were provided by the VMware team, the file for the destination is named `VMware-HCX-Cloud-x.y.z-########.ova`. **Note** The file `VMware-HCX-Installer-x.y.z-########.ova` is a generic installer that will update itself to the latest version during the installation.
▢ HCX Manager Hostname:		

	Source HCX Manager **(type: Connector or Enterprise)**	**Destination HCX Manager** **(type: Cloud)**
▢ HCX Manager Internal IP Address:	■ The HCX Manager vNIC IP address, typically an internal address from the environment's management network.	■ The HCX Manager vNIC IP address, typically an internal address from the environment's management network.
▢ HCX Manager External Name / Public IP Address:	■ The source HCX Manager initiates the management connection to the destination, it does not need a dedicated public IP address. ■ The source HCX Manager supports outbound connections using Network Address Translation (Source NAT).	■ Only required when the paired environments do not have a private connection and will connect over the Internet. ■ The external name record should resolve to a public IP address. ■ The destination HCX Cloud Manager supports load balanced inbound connections or Network Address Translation (DNAT) .
▢ HCX Manager admin / root password:		
▢ Verify external access for the HCX Manager:	■ HCX Manager makes outbound HTTPS connections to `connect.hcx.vmware.com` and `hybridity-depot.vmware.com`. ■ The source HCX Manager will make outbound HTTPS connections to the site paired destination HCX Manager systems.	■ HCX Manager makes outbound HTTPS connections to `connect.hcx.vmware.com` and `hybridity-depot.vmware.com`. ■ The destination HCX Manager will receive HTTPS connections from the site paired source HCX Manager systems.
▢ HCX Activation / Licensing:	■ In private cloud, private data center, or VFC deployments, HCX Advanced features are licensed using the NSX Enterprise plus licenses from the destination NSX environment. See Activating or Licensing New HCX Systems for more details.	■ In private cloud, private data center, or VFC deployments, HCX Advanced features are licensed using the NSX Enterprise plus licenses from the destination NSX environment. See Activating or Licensing New HCX Systems for more details.
Proxy requirements	If a proxy server is configured, all HTTPS connections are sent to the proxy. An exclusion configuration is mandatory to allow HCX Manager to connect to local systems. The exclusions can be entered as supernets and wildcard domain names. The configuration should encompass: ■ vSphere Management Subnets. ■ NSX Manager if present. ■ Internally addressed site pairing targets. ■ Generally, the RFC 1918 IP block, along with the internal domain name, can be used as the exception configuration. For example: `10.0.0.0/8, *.internal_domain.com`	Not applicable.
Configuration and Service limits	Review the HCX configuration and operational limits: VMware Configurations Maximum.	Review the HCX configuration and operational limits: VMware Configurations Maximum.

Planning the Compute Profile Configurations

A **Compute Profile** contains the catalog of HCX services and allows in-scope infrastructure to be planned and selected before deploying the **Service Mesh**. The **Compute Profile** describes how HCX will deploy services and services appliances when a **Service Mesh** is created.



	Source Compute Profile	Destination Compute Profile
▢ Compute Profile Name	■ Using meaningful names simplify operations in multi-CPs deployments.	■ Using meaningful names simplify operations in multi-CPs deployments.
▢ Services to activate	■ Services are presented as a catalog, showing available capabilities based on licensing. ■ This can be used to restrict the individual HCX services that will be activated.	■ Services are presented as a catalog, showing available capabilities based on licensing. This can be used to restrict the individual HCX services that will be activated.
▢ Service Resources (Data Center or Cluster)	[legacy-dev cluster] ■ Every cluster that contains virtual machines is used as a **Service Cluster** in the **Compute Profile**.	[Compute-1 , Compute-2] ■ Every cluster that is a valid target should be included as a **Service Cluster** in the **Compute Profile**.
▢ Deployment Resources (Cluster or Resource Pool)	■ The **Deployment Cluster** hosts HCX appliances. ■ It must be connected to DVS for HCX L2 and can reach the service cluster networks for HCX migration.	■ The **Deployment Cluster** hosts HCX appliances. ■ It must be connected to the NSX Transport Zone for L2 and can reach the service cluster networks for HCX migration.

	Source Compute Profile	Destination Compute Profile
▢ Deployment Resources (Datastore)	■ Select the datastore to use with HCX service mesh deployments.	■ Select the datastore to use with HCX service mesh deployments.
▢ Distributed Switches or NSX Transport Zone for Network Extension	■ Select the virtual switch(es) or transport zone that contains virtual machine networks that will be extended. ■ The deployment cluster hosts must be connected to the selected switches.	■ Select the transport zone that will be used with HCX Network Extension operations.

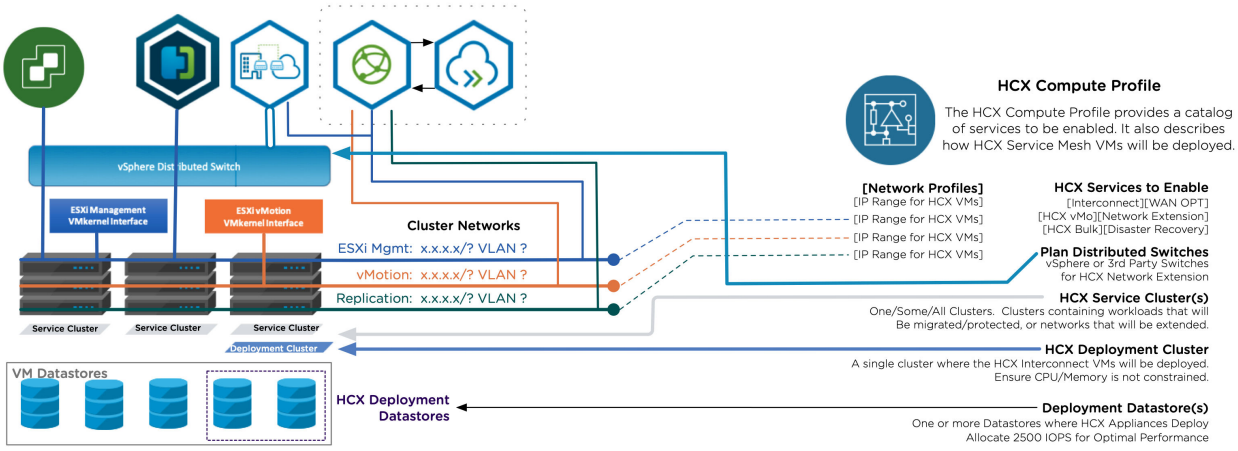
Planning the Network Profile Configurations

A **Network Profiles** contains information about the underlying networks and allows networks and IP addresses to be pre-allocated before creating a **Service Mesh**. Review and understand the information in Network Profile Considerations and Concepts before creating **Network Profiles** for HCX .

Network Profile Type	Source Network Details	Destination Network Details
▢ HCX Uplink	■ It is typical to use the Management and Uplink Networks to use the same backing at the source. If a dedicated network is used, collect the following: ■ VLAN, Port Group ■ VSS|DVS|NSX Network Name ■ Gateway IP ■ Range of available IPs for HCX to use.	■ When connecting environments over Internet, assign the Public IPs networks as the HCX Uplink. ■ VLAN, Port Group ■ VSS|DVS|NSX Network Name ■ Gateway IP ■ Range of available IPs for HCX to use.
▢ HCX Management	■ The ESX Management network (typically). ■ VLAN, Port Group ■ VSS|DVS|NSX Network Name ■ Gateway IP ■ Range of available IPs for HCX to use.	■ The ESX Management network (typically). ■ VLAN, Port Group ■ VSS|DVS|NSX Network Name ■ Gateway IP ■ Range of available IPs for HCX to use.
▢ HCX vMotion	■ The vMotion network ■ VLAN, Port Group ■ VSS|DVS|NSX Network Name ■ Gateway IP ■ Range of available IPs for HCX to use.	■ The vMotion network ■ VLAN, Port Group ■ VSS|DVS|NSX Network Name ■ Gateway IP ■ Range of available IPs for HCX to use.
▢ HCX Replication	■ The ESX Replication network. This is the same as the Management network when a dedicated Replication network doesn't exist or when using vSphere Replication NFC (required). ■ VLAN, Port Group ■ VSS|DVS|NSX Network Name ■ Gateway IP ■ Range of available IPs for HCX to use.	■ The ESX Replication network. This is the same as the Management network when a dedicated Replication network doesn't exist or when using vSphere Replication NFC (required). ■ VLAN, Port Group ■ VSS|DVS|NSX Network Name ■ Gateway IP ■ Range of available IPs for HCX to use.

Service Mesh Planning Diagram

The illustration summarizes HCX service mesh component planning.



Site to Site Connectivity

▢ Bandwidth for Migrations	■ A minimum 100 Mbps of bandwidth is required for HCX migration services. The requirement may be higher depending on the volume of migration.
▢ Public IPs & NAT	■ HCX automatically enables strong encryption for site to site service mesh communications. It is typical for customers to begin migration projects over the Internet (while private circuits are not available, or won't become available). ■ HCX supports outbound SNAT at the source. The HCX Uplink can be a private/internal IP address at the source environment. The SNAT of all HCX components to a single Public IP address. ■ Public IP addresses must be assigned directly in the Uplink Network Profile at the destination HCX configuration. ■ Inbound DNAT is not supported at the destination.
▢ Source HCX to Destination HCX Network Ports	■ The source HCX Manager connects to the HCX Cloud Manager using port TCP-443. ■ The source IX (HCX-IX-I) connects to the peer IX (HCX-IX-R) using port UDP-4500. ■ The source NE (HCX-NE-I) connects to the peer NE (HCX-NE-R) using port UDP-4500. ■ The source HCX appliances initiate the connections.
▢ Other HCX Network Ports	■ A full list of port requirements for HCX can be found in ports.vmware.com.

Figure 3-1. Network Ports at the Source

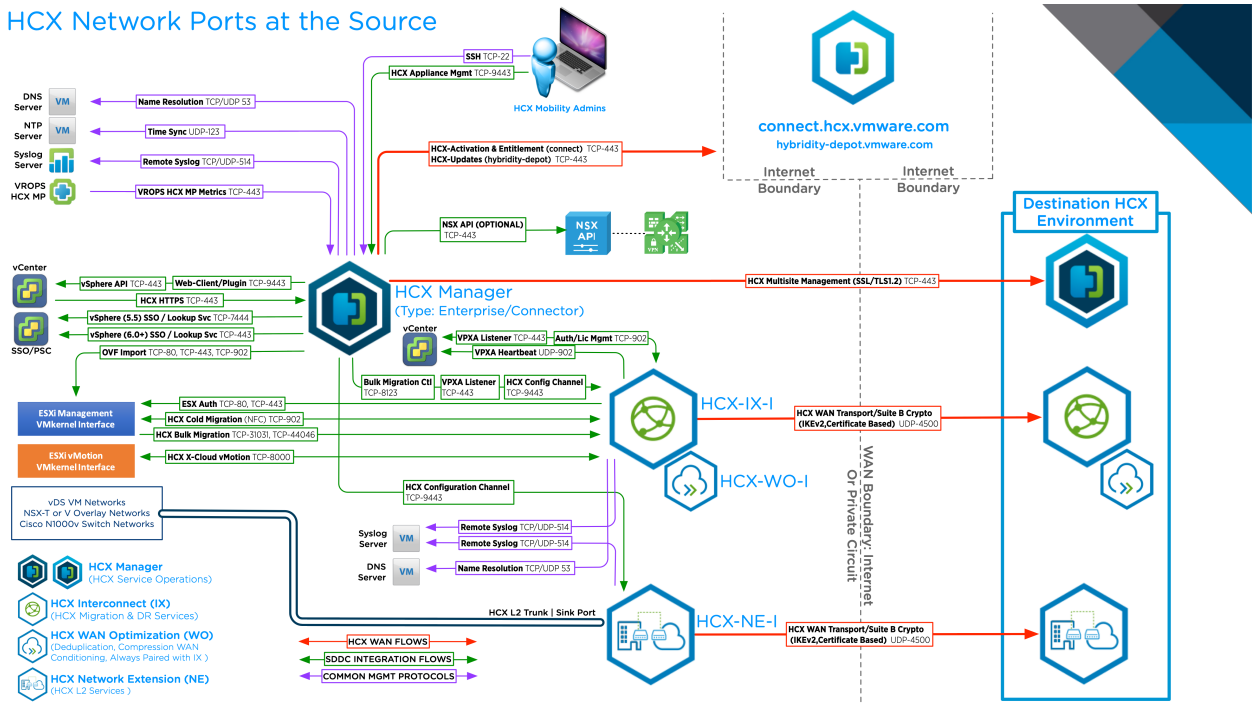
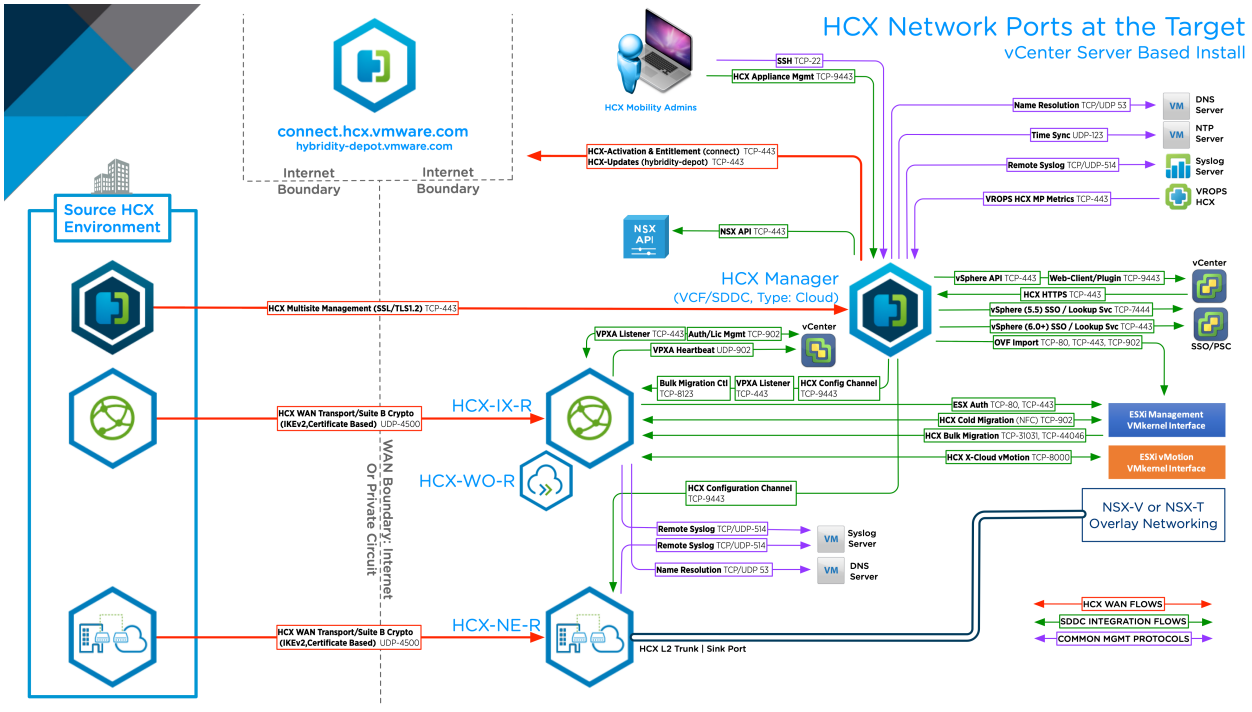


Figure 3-2. Network Ports at the Destination



Install Checklist B - HCX with a VMC SDDC Destination Environment

4

This install checklist is written for HCX deployments with VMware Cloud on AWS as the target, where HCX is automatically installed by enabling the service (in private cloud HCX deployments, the user handles full HCX deployment and configuration for the destination environment.

This document presented in using on-prem as the source to VMC SDDC as the destination. All the checklist tables follow this format:

- It is assumed that the on-prem vSphere contains the existing workloads and networks that will be migrated. This environment can be legacy vSphere or modern.
- It is assumed that destination is a VMC SDDC instance.

HCX Use Cases and POC Success Criteria

"How am I doing with HCX? How will I define a success in my proof of concept?"

▢ What defines the success criteria for the HCX proof of concept?	Clearly define how the success criteria. For example: ■ Extend 2 test networks to VMC. ■ Live migrate a virtual machine. ■ Test HCX L2 connectivity using over the extended network. ■ Reverse migrate a VM. ■ Bulk Migrate a VM.
▢ Ensure features will be available with the trial or full licenses obtained.	■ HCX is an available add-on included with a VMC SDDC. ■ The add-on gives access to the HCX Advanced features. ■ The add-on gives access to select HCX Enterprise-class services: Replication Assisted vMotion, Mobility Optimized Networking, Application Path Resiliency, TCP Flow Conditioning, and Mobility Groups. See VMware HCX Services.

Collect vSphere Environment Details

This section identifies vSphere related information that should be known about the environments that is relevant for HCX deployments.

Environment Detail	On-premises Environment	VMC SDDC
▢ vSphere Version:	■ vSphere version must be within Technical Guidance.	■ N/A. SDDC instances run supported software versions.
▢ Distributed Switches and Connected Clusters	■ Understand the relationships between clusters and the Distributed Switches. ■ Imported Distributed Switches are not supported for the HCX-NE service.	■ N/A. The SDDC compute profile will automatically include the workload clusters.
▢ ESXi Cluster Networks	■ Identify the ESXi Management, vMotion and Replication (if it exists). VSS PG or DPG Names, VLANs and Subnets. ■ If these networks vary from cluster to cluster, additional configuration will be needed. ■ Identify available IPs (HCX will participate in these networks)	■ N/A. In VMC the HCX is automatically installed.
▢ NSX version and configurations:	■ NSX is not required on-premises, but is supported for the purpose of extending NSX Networks. See NSX Requirements for HCX Connector Installation if NSX networks will be extended to VMC.	■ N/A. In VMC the HCX is automatically installed.
▢ Review and ensure all Software Version Requirements are satisfied.		
▢ vCenter Server URL:	■ https://vcenter-ip-or-fqdn	■ The VMC URLs are listed in vmc.vmware.com, under SDDCs > Settings.
▢ Administrative accounts	■ Know the administrator @vsphere.local or equivalent account for the vCenter Server registration step.	■ In VMC, know how to locate the cloudadmin@vmc.local account details.
▢ NSX Manager URL:	■ N/A. See the NSX versions column above.	■ N/A. Networking & Security features are managed using the VMC user interface.
▢ NSX admin or equivalent account.	■ If HCX will be used to extend NSX networks, know the administrator account for the NSX registration step.	■ N/A. Networking & Security features are managed using the VMC user interface.
▢ Destination vCenter SSO URL :	■ Use the SSO FQDN as seen in the vCenter Advanced Configurations (config.vpxd.sso.admin.uri)	■ The VMC URLs are listed in vmc.vmware.com, under SDDCs > Settings.
▢ DNS Server:	■ DNS is required.	■ N/A. Automatically configured.
▢ NTP Server:	■ NTP server is required.	■ N/A. Automatically configured.
▢ HTTP Proxy Server:	■ If there is an HTTPS proxy server in the environment, it should be added to the configuration.	■ N/A. Automatically configured.

Planning for the HCX Manager Deployment

This section identifies information that should be known prior to deploying the HCX Manager system on-premises. HCX Manager at the VMC SDDC is deployed automatically when the service is enabled.

	Source HCX Manager (type: Connector)	**Destination HCX Manager (type: Cloud)**
▢ HCX Manager Placement/Zoning:	■ The HCX Manager can be deployed like other management components (like vCenter Server or NSX Manager). ■ It does not have to be deployed where the migration workloads reside.	■ The VMC HCX Cloud Manager is deployed automatically in the SDDC management cluster whenever the HCX add-on service is enabled on the SDDC.
▢ HCX Manager Installer OVA:	■ The HCX Manager download link for the source is obtained from the destination HCX Manager, in the System Updates UI. ■ If OVA download links were provided by the VMware team, the file for the source will be named `VMware-HCX-Connector-x.y.z-########.ova`.	■ N/A.
▢ HCX Manager Hostname / FQDN:		■ The VMC URLs are listed in vmc.vmware.com, under SDDCs > Settings.
▢ HCX Manager Internal IP Address:	■ The HCX Manager vNIC IP address, typically an internal address from the environment's management network.	■ The SDDC HCX Cloud system uses an IP address based on the provided subnet for SDDC management. This address is not required for site pairing with the SDDC.
▢ HCX Manager External Name / Public IP Address:	■ The source HCX Manager initiates the management connection to the destination, it does not need a dedicated public IP address. ■ The source HCX Manager supports outbound connections using Network Address Translation (Source NAT).	■ The SDDC Management firewall will reflect entries allowing TCP-443 connections to the HCX Cloud Manager public IP address.
▢ HCX Manager admin / root password:		■ In VMC, know how to locate the cloudadmin@vmc.local account details.
▢ Verify external access for the HCX Manager:	■ HCX Manager makes outbound HTTPS connections to `connect.hcx.vmware.com` and `hybridity-depot.vmware.com`. ■ The source HCX Manager will make outbound HTTPS connections to the site paired destination HCX Manager systems.	■ The VMC URLs are listed in vmc.vmware.com, under SDDCs > Settings. ■ Ensure the VMC management firewall allows inbound HTTPS connections from the on-prem HCX Connector and from the User systems that will access the interface.

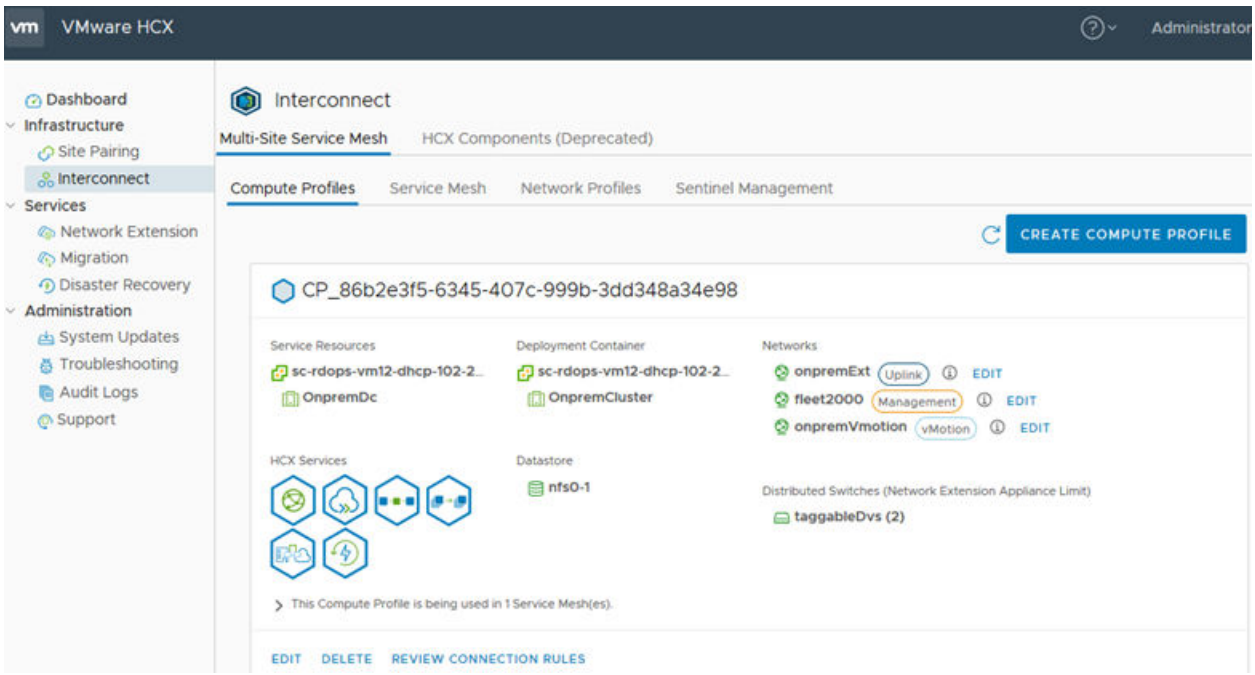
	Source HCX Manager (type: Connector)	Destination HCX Manager (type: Cloud)
▢ HCX Activation / Licensing:	■ Activation keys for the HCX Connector system on-premises are generated in VMC. ■ To generate a key, open add-ons tab to open HCX. Use Activation Keys > Create Activation Key > HCX Connector to generate a key for the on-premises HCX system.	■ The HCX in the VMC SDDC instance is activated when the service is enabled.
Proxy requirements	If a proxy server is configured, all HTTPS connections are sent to the proxy. An exclusion configuration is mandatory to allow HCX Manager to connect to local systems. The exclusions can be entered as supernets and wildcard domain names. The configuration should encompass: ■ vSphere Management Subnets. ■ NSX Manager if present. ■ Internally addressed site pairing targets. ■ Generally, the RFC 1918 IP block, along with the internal domain name, can be used as the exception configuration. For example: `10.0.0.0/8, *.internal_domain.com`	Not applicable.
Configuration and Service limits	Review the HCX configuration and operational limits: VMware Configurations Maximum.	Review the HCX configuration and operational limits: VMware Configurations Maximum.

Planning the Compute Profile Configuration

A **Compute Profile** contains the catalog of HCX services and allows in-scope infrastructure to be planned and selected prior to deploying the **Service Mesh**. The **Compute Profile** describes how HCX will deploy services and services appliances when a **Service Mesh** is created.

A **Compute Profile** is required in the on-premises HCX Connector.

A **Compute Profile** is pre-created in the VMC SDDC as part of enabling the HCX Add-on.



	On-premises Compute Profile	SDDC Compute Profile
▢ Compute Profile Name	■ Using meaningful names simplify operations in multi-CPs deployments.	■ The Compute Profile configuration is created automatically in the SDDC HCX system when HCX is enabled.
▢ Services to activate	■ Services are presented as a catalog, showing available capabilities based on licensing. ■ This can be used to restrict the individual HCX services that will be activated.	■ All HCX services are activated in the SDDC Compute Profile.
▢ Service Resources (Data Center or Cluster)	■ Every cluster that contains virtual machines will be used as a **Service Cluster** in the **Compute Profile**.	■ The SDDC Compute Cluster is assigned as the HCX Service Cluster. ■ The SDDC Management Cluster is a Service Cluster.
▢ Deployment Resources (Cluster or Resource Pool)	■ The **Deployment Cluster** hosts HCX appliances. ■ It needs to be connected to DVS for HCX L2 and can reach the service cluster networks for HCX migration.	■ The SDDC Management Cluster is assigned as the HCX Deployment Cluster.
▢ Deployment Resources (Datastore)	■ Select the datastore to use with HCX service mesh deployments.	■ The SDDC Management Datastore is used.
▢ Distributed Switches or NSX Transport Zone for Network Extension	■ Select the virtual switch(es) or transport zone that contains virtual machine networks that will be extended. ■ The deployment cluster hosts must be connected to the selected switches.	■ The SDDC Transport zone is used in the configuration.

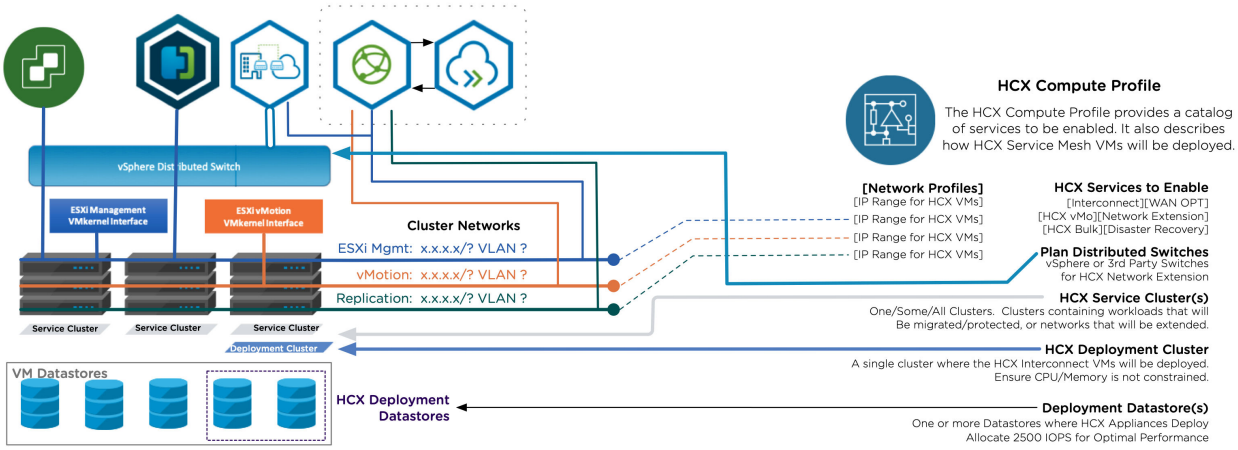
Planning the Network Profile Configurations

A **Network Profiles** contains information about the underlying networks and allows networks and IP addresses to be pre-allocated prior to creating a **Service Mesh**. Review and understand the information in Network Profile Considerations and Concepts before creating **Network Profiles** for HCX .

Network Profile Type	On-Prem Details	VMC SDDC Details
▢ HCX Uplink	■ It is typical to use the Management and Uplink Networks to use the same backing at the source. If a dedicated network is used, collect the following: ■ VLAN, Port Group ■ VSS|DVS|NSX Network Name ■ Gateway IP ■ Range of available IPs for HCX to use.	■ By default, the SDDC instance uses Public IP-based EIPs in the Uplink configuration. ■ If a DX private VIF will be used for connecting the on-prem environment to the SDDC, configure a unique private IP network.
▢ HCX Management	■ The ESX Management network (typically). ■ VLAN, Port Group ■ VSS|DVS|NSX Network Name ■ Gateway IP ■ Range of available IPs for HCX to use.	■ Network Profiles are configured automatically when the HCX service is enabled using a portion of the SDDC management network.
▢ HCX vMotion	■ The vMotion network ■ VLAN, Port Group ■ VSS|DVS|NSX Network Name ■ Gateway IP ■ Range of available IPs for HCX to use.	■ Network Profiles are configured automatically when the HCX service is enabled using a portion of the SDDC management network.
▢ HCX Replication	■ The ESX Replication network. This will be the same as the Management network when a dedicated Replication network doesn't exist. ■ VLAN, Port Group ■ VSS|DVS|NSX Network Name ■ Gateway IP ■ Range of available IPs for HCX to use.	■ Network Profiles are configured automatically when the HCX service is enabled using a portion of the SDDC management network.

Service Mesh Planning Diagram

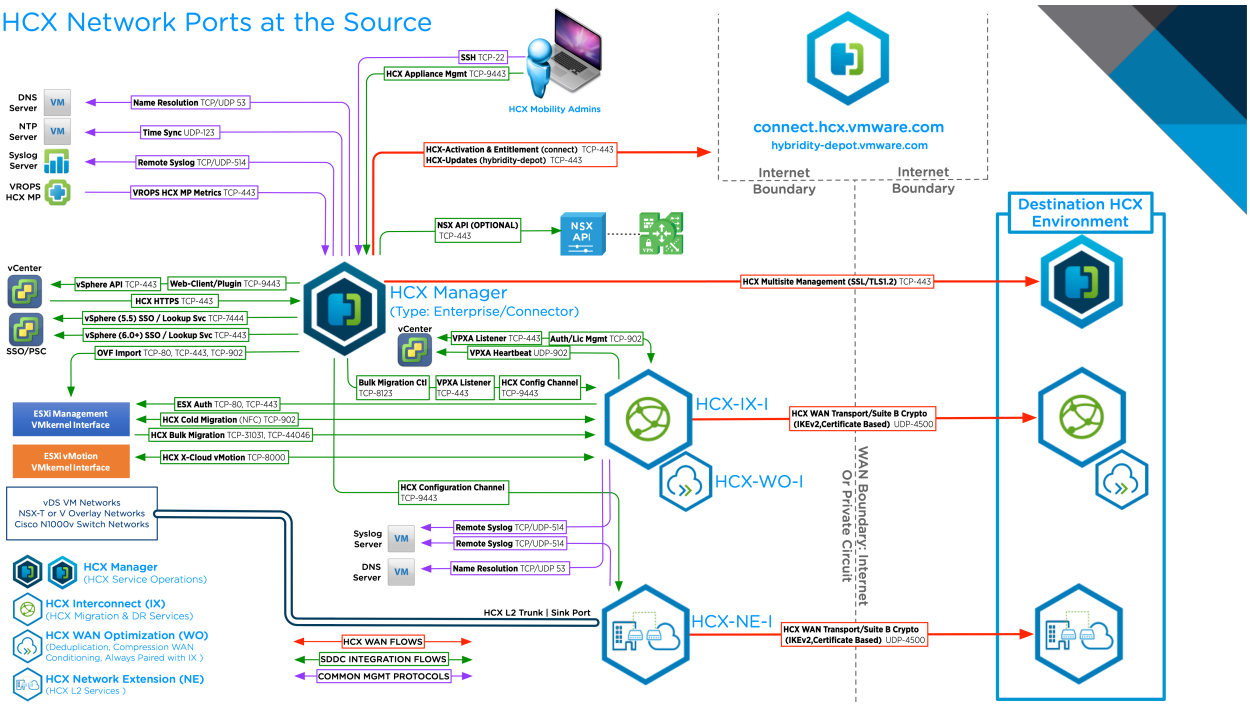
The illustration summarizes HCX service mesh component planning.



Site to Site Connectivity

▢ Bandwidth for Migrations	■ A minimum 100 Mbps of bandwidth is required for HCX migration services.
▢ Public IPs & NAT	■ HCX automatically enables strong encryption for site to site service mesh communications. It is typical for customers to begin migration projects over the Internet (while private circuits are not available, or won't become available). ■ HCX supports outbound SNAT at the source. The HCX Uplink can be a private/internal IP address at the source environment. The SNAT of all HCX components to a single Public IP address. ■ Inbound DNAT is not supported at the destination. A VMC HCX deployment automatically assigns public IP addresses to the HCX components
▢ Source HCX to Destination HCX Network Ports	■ The source HCX Manager connects to the HCX Cloud Manager using port TCP-443. ■ The on-prem IX (HCX-IX-I) connects to the VMC SDDC IX (HCX-IX-R) using port UDP-4500. ■ The on-prem NE (HCX-NE-I) connects to the VMC SDDC NE (HCX-NE-R) using port UDP-4500. ■ The source HCX appliances always initiate the transport tunnel connections.
▢ Other HCX Network Ports	■ A full list of port requirements for HCX can be found in ports.vmware.com.

HCX Network Ports On-Premises



Install Checklist C - HCX with OS Assisted Migration

5

HCX OS Assisted Migration allows for the migration of guest (non-vSphere) virtual machines from on-premise data centers to private or public cloud vSphere destinations.

OS Assisted Migration requires the HCX Enterprise license.

To use OS Assisted Migration, HCX must be prepared according to Install Checklist A, with additional preparation for non-vSphere (KVM or Hyper-V) virtual machine migration. For all OS Assisted Migration deployments, you must have HCX Connector deployed at the on-premises site.

HCX OS Assisted Migration has three components: Sentinel Gateway (SGW) appliance for connecting and forwarding guest workloads in the source environment, Sentinel Data Receiver (SDR) in the destination environment, and Sentinel software that must be installed on each guest virtual machine.

This section supplements Install Checklist A with specific information related to OS Assisted migration.

Collect the non-vSphere Environment Details

This section identifies information that should be known about the KVM or Hyper-V environments that is relevant for HCX deployments with OS Assisted Migration.

Environment Detail	Description
Hypervisor	OS Assisted Migration is available only for KVM or Hyper-V workloads.
Guest Network for OS Assisted Migration	This is the network on which guest virtual machines communicate with the HCX SGW for OS Assisted Migration. This can be the same network used by another HCX function, such as Management.
Guest virtual machines	Identify the set of KVM or Hyper-V virtual machines to migrate. You must install Sentinel software on each virtual machine for communication, inventory, and replication processes. For a detailed list of supported guest virtual machine operating systems, see Understanding VMware HCX OS Assisted Migration.
KVM or Hyper-V VLAN for Network Extension	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.

Planning for HCX OS Assisted Migration

This section identifies checklist information that applies to deploying HCX with OS Assisted Migration.

Checklist Item	Source HCX Manager (type: Connector or Enterprise)	Destination HCX Manager (type: Cloud)
Checklist A preparation	Review the Source HCX Manager items provided in Checklist A.	Review the HCX Cloud Manager items provided in Checklist A.
Port requirements	Review the OS Assisted Migration requirements at the source site for firewall access: VMware Ports and Protocol. Filter by Purpose, "OSAM."	Review the OS Assisted Migration port requirements at the destination site for firewall access: VMware Ports and Protocol. Filter by Purpose, "OSAM."
Sentinel software	Install Sentinel software on each KVM or Hyper-V workload requiring migration. Sentinel software is only available for download from the Sentinel tab in the HCX Service Mesh UI.	Sentinel software is not available for download from the HCX Cloud Manager.

Planning the Compute Profile Configuration

The same items called out in Install Checklist A apply to the Compute Profile configuration when using HCX with OS Assisted. For OS Assisted Migration, additional items may apply.

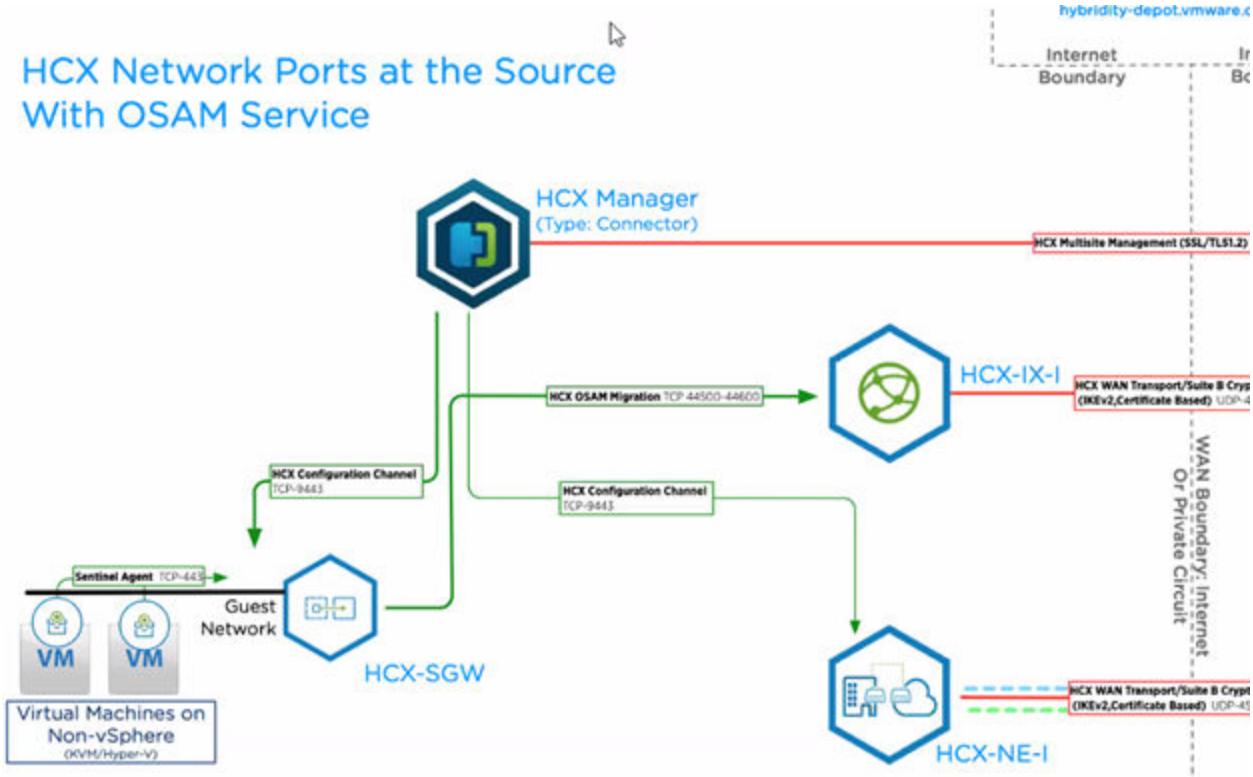
Checklist Item	Source Compute Profile	Destination Compute Profile
WAN Optimizaton and Network Extension Services	When migrating KVM or Hyper-V virtual machines to a VMware environment which resides in a different data center geographically, you must activate WAN Optimization and Network Extension services in the source Compute Profile. When migrating KVM or Hyper-V virtual machines to a VMware environment where both the non-vSphere and vSphere environment reside in the same data center, it is not necessary to activate WAN Optimization. It may not be necessary to activate Network Extension services depending on the diameter of the L2 switching domain in the data center.	When migrating KVM or Hyper-V virtual machines to a VMware environment which resides in a different data center geographically, you must activate WAN Optimization and Network Extension services in the destination Compute Profile. When migrating KVM or Hyper-V virtual machines to a VMware environment where both the non-vSphere and vSphere environment reside in the same data center, it is not necessary to activate WAN Optimization. It may not be necessary to activate Network Extension services depending on the diameter of the L2 switching domain in the data center.
Guest Network Profile	Use the Guest Network Profile when setting up the Compute Profile. **Note** If no Guest Network is set up in the Network Profile, this can be the same network used by another HCX function, such as Management.	Not applicable.

Planning the Network Profile Configuration

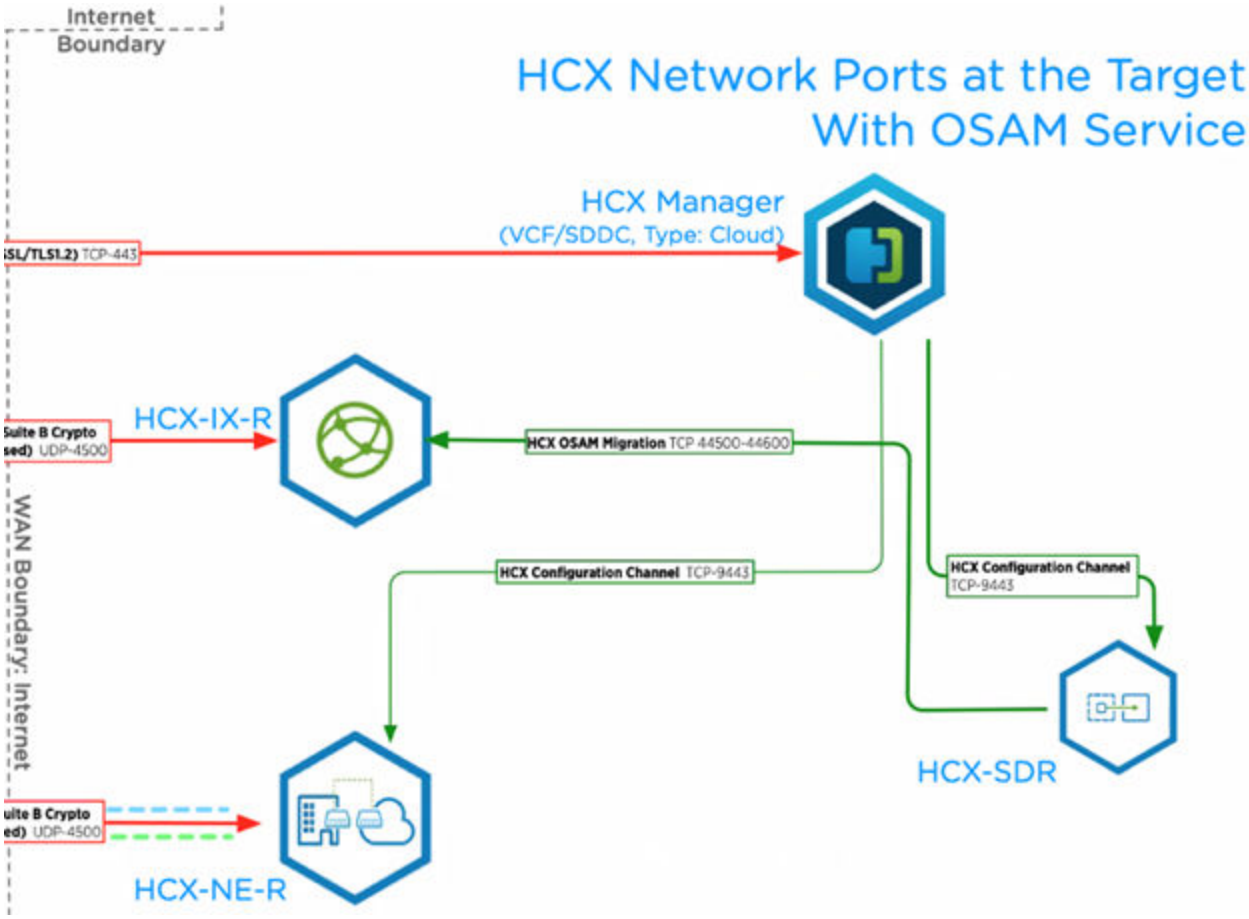
The same items called out in Install Checklist A apply to the Network Profile configuration when using HCX with OS Assisted. For OS Assisted Migration, additional items may apply.

Checklist Item	Source Compute Profile	Destination Compute Profile
Create a Network Profile for the Guest Network selection during the Compute Profile configuration.	This is the network on which guest virtual machines with Sentinel software communicate with the HCX Sentinel Gateway.	Not applicable in the Destination Compute Profile.

Network Ports at the Source with OS Assisted Migration



Network Ports at the Destination with OS Assisted Migration



Example - Completed Install Checklist A

6

This version of the checklist is prepared using a fictional migration scenario. The entries are completed using the scenario information.

The planning tables in this document are organized assuming there is one source environment and one destination environment:

- It is assumed that the source vSphere contains the existing workloads and networks that are migrated. This environment can be legacy or relatively modern. See Software Version Requirements (Source Requirements).
- It is assumed that the destination is a private cloud deployment, and is the target for HCX network extensions, migrations, and services. See Software Version Requirements (Destination Requirements).

Explanations are included in the regular pre-install checklists. This checklist omits them for brevity.

Scenario - XYZ Migration from Legacy DC to SDDC

The XYZ Widget Company plans to evacuate the XYZ Legacy DC into a newly built XYZ SDDC (in a new physical data center). HCX enables the evacuation of all workloads and the decommissioning of EOL hardware and EOS software without upgrades.

The objective for the HCX POC is to test core VMware HCX capabilities that enable the evacuation of the legacy data center. The proof of concept follows this success criteria:

- Deploy the HCX Service Mesh, configured to provide services for the DEV environment.
- Extend the prepared test network (virtual machine VLAN 10 backed DPG).
- Successfully perform HCX vMotion and Bulk migration for a test virtual machine from Legacy DC to the SDDC.
  - Understand the time to migrate VM data for each protocol.
  - Understand the ability to use bandwidth for migrations under the POC configuration.
- Test Network Extension:
  - Verify Legacy VM to SDDC VM connectivity over the HCX L2 path.
  - Understand Legacy to SDDC latency.

- Successfully perform reverse HCX migrations from SDDC to Legacy.
- Successfully complete the Bulk migration of 3-5 VMs in parallel from Legacy DC to SDD in parallel.
  - Test the Bulk migration failover scheduler.
  - Upgrade VM Hardware / VM Tools.

Scenario Environment Details

Fictional environment details for the XYZ-Legacy and the XYZ-SDDC.

Environment Facts	Source - Legacy DC	Destination - XYZ-SDDC
vSphere	■ vSphere 6.0 U1 ■ Mgmt Cluster ■ Dev Cluster ■ Prod Cluster ■ Legacy DVS	■ vSphere 7.0 U1 ■ Mgmt Cluster ■ Compute-1 Cluster ■ Compute-2 Cluster ■ Mgmt DVS ■ Compute DVS
Cluster Networks	■ ESXi Management 192.168.100.0 prefix-24 VSS-VLAN-100 ■ ESXi vMotion 192.168.101.0 prefix-24 VSS-VLAN-101	■ ESXi Management 10.0.100.0 prefix-22 ■ ESXi vMotion 10.0.104.0 prefix-22 ■ ESXi Replication 10.0.108.0 prefix-22
VM Networking	■ Single Legacy DC DVS. ■ DPG Test-VM-NET-10 192.168.10.0 prefix-24 VLAN 10. ■ 5 Test-VMs deployed for the POC.	■ NSX-T Overlay TZ Configured ■ NSX-T T1 Router Created.
Storage	■ Block Storage Central Array	■ vSAN Storage
Site to Site Connectivity	■ 1 Gbps Internet / WAN. ■ No dedicated Public IPs required for HCX (HCX will NAT outbound).	■ 10 Gbps Internet / WAN. ■ 3 Public IPs reserved for HCX.

Collect vSphere Environment Details

Collect the relevant environment details in preparation for the installation. The bulleted entries may provide context, or about requirements related to the Environment Detail entry.

XYZ Widget Company Scenario information is [in brackets].

Environment Detail	Source Environment	Destination Environment
▢ vSphere Version:	[XYX Legacy is 6.0]	[XYZ SDDC is 7.0 U1]
▢ Distributed Switches and Connected Clusters	[Shared DVS : Mgmt, Dev, Prod]	[Mgmt DVS: Mgmt Cluster Compute DVS: Compute-1, Compute-2]
▢ ESXi Cluster Networks	[ESXi Management 192.168.100.0/24 VSS-VLAN-100 ESXi vMotion 192.168.101.0/24 VSS-VLAN-101]	[ESXi Management 10.0.100.0/22 ESXi vMotion 10.0.104.0/22 ESXi Replication 10.0.108.0/22]
▢ NSX version and configurations:	[No NSX in Legacy DC]	[XYZ SDDC is running NSX-T 3.1, with an overlay Transport Zone that includes Compute-1 and Compute-2 clusters]
▢ Verify all Software Version Requirements are satisfied.	[Verified XYZ Legacy DC meets all documented version requirements]	[Verified XYZ SDDC meets all documented version requirements]
▢ vCenter Server URL:	[https://legacy-vcenter]	[https://sddc-1-vcenter.xyz.com]
▢ vCenter administrator@vsphere.local or equivalent account.	[Verified administrator access to the vCenter Server]	[Verified administrator access to the vCenter Server]
▢ Destination NSX Manager URL:	[N/A]	[https://sddc-1-nsxm.xyz.com]
▢ NSX admin or equivalent account.	[N/A]	[Verified the NSX admin account]
▢ Destination vCenter SSO URL :	[embedded]	[sddc-1-psc.xyz.com]
▢ DNS Server:	[legacy-dns.xyz.com]	[dns.xyz.com]
▢ NTP Server:	[legacy-ntp.xyz.com]	[ntp.xyz.com]
▢ HTTP Proxy Server:	[proxy.xyz.com]	[Verified xyz does not use HTTP proxy servers]

Planning for the HCX Manager Deployments

XYZ Widget Company Scenario information is [in brackets].

	HCX Manager Deployment at Source	HCX Manager Deployment at Destination
▢ HCX Manager Placement:	[HCX Manager is deployed in the xyz-sddc1]	[HCX Manager is deployed in the XYZ-SDDC-1 Mgmt cluster]
▢ HCX Manager Installer OVA:	[The OVA is downloaded from the SDDC-1 HCX Manager once that is online]	[The OVA has been downloaded.]
▢ HCX Manager Hostname:	[legacy-hcxm.xyz.com]	[sddc-1-hcxm.xyz.com]
▢ HCX Manager Internal IP Address:	[192.168.100.50]	[10.0.100.50]
▢ HCX Manager External Name / Public IP Address:	[External Name/Pub IP assignment is not applicable]	[sddc1-hcx.xyz.com , Pub IP assignment 192.0.2.50]

	HCX Manager Deployment at Source	HCX Manager Deployment at Destination
▢ HCX Manager admin / root password:		
▢ Verify outbound access for the HCX Manager:	[Verified outbound NAT will allow outbound connections for legacy-hcxm]	[Verified the HCXM network can reach *.vmware.com using . HTTPS]
▢ HCX Activation / Licensing:	[The licenses for the sddc-1-hcx are used at the source)	[The XYZ HCX POC uses trial licenses, which allows testing up to 20 migrations]

Planning the Compute Profile Configurations

XYZ Widget Company Scenario information is [in brackets].

Note In the XYZ Widget Company POC scenario, a single Compute Profile is used.

In production deployments, one can create additional Compute Profiles to scale out the HCX services or to achieve connectivity when there are things like per-cluster vMotion or DVS isolation in the environment.

	Source Compute Profile	Destination Compute Profile
▢ Compute Profile Name	[Legacy-DC-CP]	[sddc-1-CP]
▢ Services to activate	[All services activated]	[All services activated]
▢ Service Resources (Data Center or Cluster)	[legacy-dev cluster]	[Compute-1 , Compute-2]
▢ Deployment Resources (Cluster or Resource Pool)	[legacy-dev cluster]	[sddc-1-compute-1]
▢ Deployment Resources (Datastore)	[legacy-block-array]	[sddc-1-vsan-datastore]
▢ Distributed Switches or NSX Transport Zone for Network Extension	[legacy-shared-dvs]	[sddc-1-nsxt-overlay-tz, includes compute clusters]

Planning the Network Profile Configurations

The Network Profiles abstract Network consumption during HCX service deployments. See Network Profile Considerations and Concepts.

XYZ Widget Company Scenario information is [in brackets].

Network Profile Type	Source Network Details	Destination Network Details
HCX Uplink	[Using Mgmt]	[xyz-sddc-ext-net 192.0.2.11 - 192.9.2.15]
HCX Management	[legacy-mgmt, 192.168.100.0/24, gw: .1 HCX range: 192.168.100.201 - 192.168.100.205]	[xyz-sddc-mgmt, 10.0.100.0/22, gw: .1 10.0.100.201 - 10.0.100.205]
HCX vMotion	[legacy-vmotion, 192.168.101.0/24, gw: .1 HCX range: 192.168.101.201 - 192.168.101.205]	[xyz-sddc-vmo, 10.0.104.0/22, gw: .1 10.0.104.201 - 10.0.104.205]
HCX Replication	[Using Mgmt]	[xyz-sddc-repl, 10.0.108.0/22, gw: .1 10.0.108.201 - 10.0.108.205]

Source HCX to Destination HCX IP Connectivity

XYZ Widget Company Scenario information is [in brackets].

Bandwidth for Migrations	[XYZ Legacy DC has 1 Gbps Internet uplinks, 500 can be used for migrations. XYZ-SDDC has 10 Gbps available.]
Public IPs & NAT	[XYZ Legacy DC HCX components will SNAT. XYZ Legacy DC Public IP addresses have been allocated as follows : One for the HCX Manager (it is configured as an inbound DNAT rule). Two for HCX Uplink NP (one for the IX appliance and one for the NE appliance)]
Source HCX to Destination HCX Network Ports	[XYZ Legacy DC perimeter firewall has been configured to allow UDP-4500 and HTTPS outbound XYX SDDC perimeter firewall has been configured to allow HT]
HCX Network Ports	■ A full list of port requirements for HCX can be found in ports.vmware.com.

HCX Deployment Considerations

7

Several aspects of HCX deployments are presented and explored in the sections that follow.

This chapter includes the following topics:

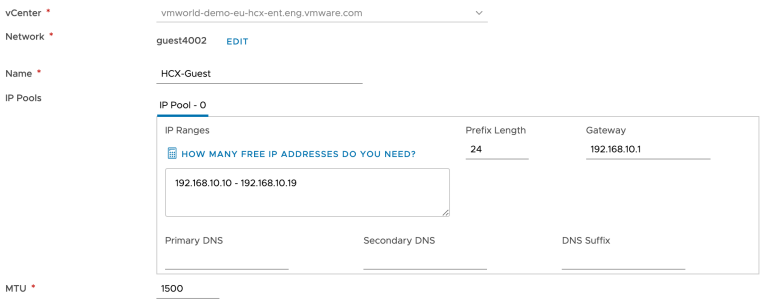
Network Profile Considerations and Concepts

Network Profiles are a subcomponent of the Compute Profile. When a service mesh is created, the network profile configurations are used to connect the deployed HCX appliances.

Introduction to Network Profiles

Network Profiles can be pre-created in the **Network Profile** tab or they can be created during the **Compute Profile** configuration. A **Network Profile** contains:

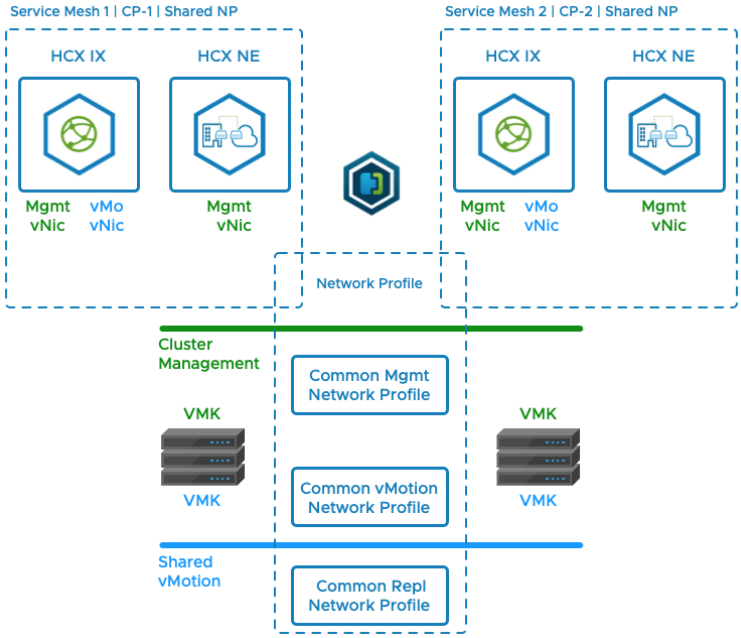
- One underlying vSphere Port Group (VSS or VDS) or NSX-based network.
- IP address information: The gateway IP, the network prefix and MTU, and DNS.
- A pool of IP addresses reserved for HCX to use during **Service Mesh** deployments.



Characteristics of Network Profiles

- **Network Profile** configurations are only used during **Service Mesh** deployments (IP addresses assigned to the IX and NE, and OSAM appliances).

- The HCX Manager only uses a Management interface, it does not use other **Network Profile** networks.
- A **Compute Profile** will always include one or more **Network Profile**.
- When **Service Mesh** is deployed, every **Network Profile** that is included in the **Compute Profile** configuration is used.
- When a **Network Profile** network is used in a **Service Mesh**, the HCX appliance will consume a single IP address out of the configured IP pool.
- When a **Network Profile** is assigned to a specific HCX traffic type (the traffic types are explained in the next section), a single IP address is used. For example, if the same **Network Profile** is assigned for HCX Management and HCX Uplink, one IP address is used, not two.
- A **Network Profile** can be used with multiple **Compute Profiles**.



HCX Traffic Types

Consider the **Network Profile** traffic types are like a router's uplinks and downlinks. The HCX-IX (mobility) and the HCX-NE (extension) have "uplinks" and "downlinks". The HCX "uplink" is used to connect the IX or NE to its remote peer, the "downlink" traffic types (Management, vMotion, Replication) connect the IX or NE to the local environment.

HCX Network Profile Types	Description
HCX Uplink	Used by **Service Mesh** components to reach their peer appliances. **Important** When destination HCX systems need to be reachable over the Internet, use the Uplink Network Profile to assign the Public IP addresses. Destination NAT configurations are not supported. The source HCX systems don't need Public IP addresses, they can be configured using traditional SNAT.
HCX Management	Used by **Service Mesh** components to connect to HCX Manager, vCenter Server, NTP, DNS.
HCX vMotion	Used by **Service Mesh** components to connect to the ESXi cluster for vMotion-based services.
HCX Replication	Used by **Service Mesh** components connect to the ESXi cluster for Replication-based services. **Note** This NP type is compatible with ESXi vSphere Replication VMkernel traffic but cannot be used for vSphere Replication NFC VMkernel traffic.
HCX Guest Network	In OSAM deployments, used by the **Service Mesh** Sentinel Gateway to connect to the Sentinel agents.

HCX Traffic Types and HCX Appliances

The table describes which NP traffic types are used by the different HCX appliances.

Important - One IP address is assigned for uniquely backed traffic type.

(For example, if all HCX-IX traffic types are configured to use a single network, a single vNIC with a single IP address is assigned. If a dedicated network is configured for each possible IX traffic type, then the HCX-IX will use four vNICs with an IP in each network. These wiring variations are described in the examples section, after the table.

HCX Appliance	Traffic Types Used
HCX-IX (Migrations, DR)	■ HCX Uplink ■ HCX Management ■ HCX vMotion ■ HCX Replication
HCX-NE (Network Extension)	■ HCX Uplink ■ HCX Management
HCX-WO (WAN Optimization)	■ HCX Management
HCX-Sentinel Gateway (OSAM)	■ HCX Management ■ HCX Guest Network
HCX-Sentinel Data Receiver	■ HCX Management

Network Profile Configuration Examples

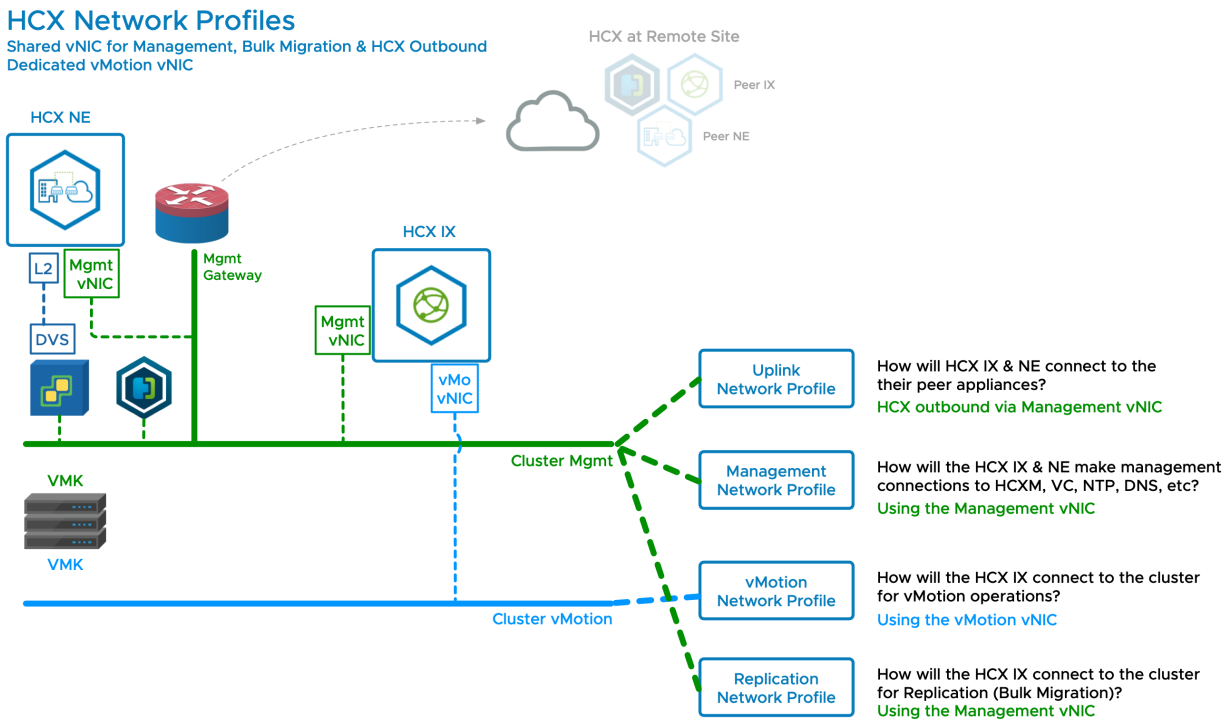
The examples below depict how the HCX Service Mesh appliances might be wired up.

In fully private HCX deployments where the environments are inside of the same private network, it is typical for the source HCX and destination HCX network profiles to be structured identically.

It is possible (and common) for the Network Profile configurations to differ at the source and destination when they are separated by the Internet. The reason for this is that the destination HCX Service Mesh appliances must have an HCX Uplink network profile with Public IP assignments (this requirement is not true at the source, where internal addresses can use source NAT for Internet access).

HCX Network Configuration 1 - Shared Management, Replication and Uplink with Dedicated vMotion

- This configuration trades the benefits gained from separation of traffic to simplify deployments. The same network is selected for Management, Uplink and Replication traffic.
- This configuration requires the management IP addresses assigned to destination HCX appliances at the destination to be fully reachable from the source HCX appliances without NAT translation. Because of this requirement - this configuration is most typical in HCX deployments fully within a private network.

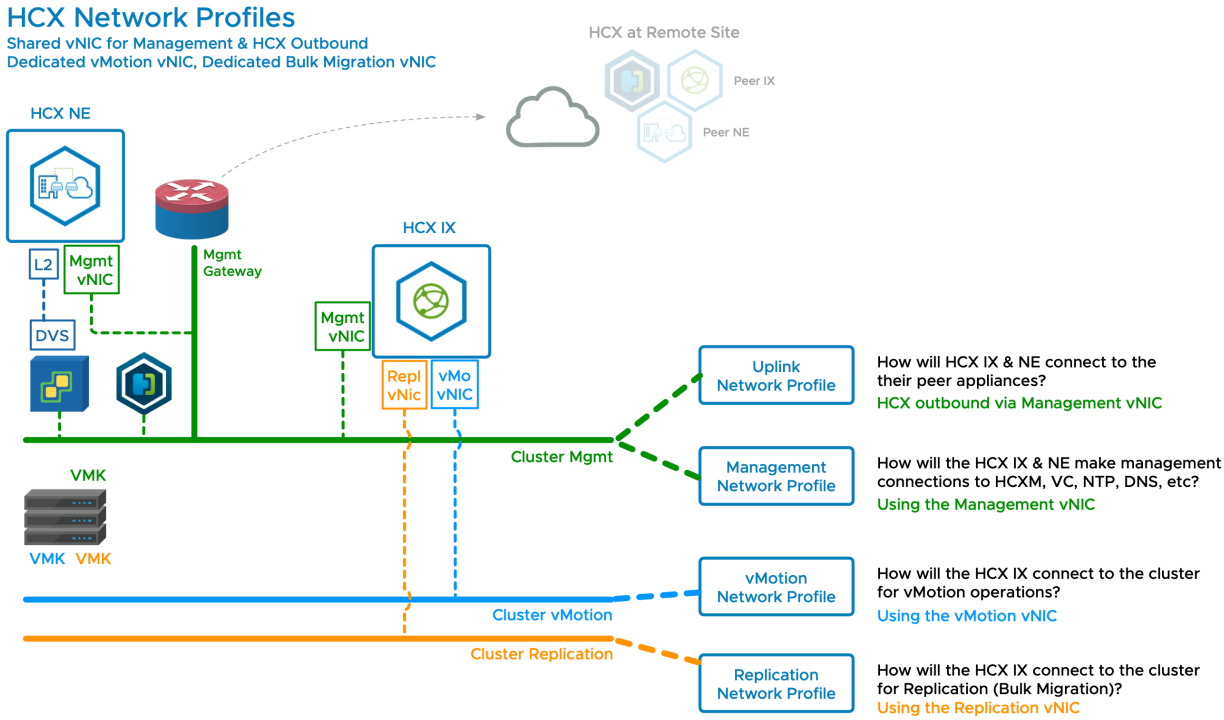


HCX Network Configuration 2 - Dedicated Replication Network

- Configuration 2 adds a dedicated network for the Replication traffic (HCX Bulk Migration).
- This configuration variation is only possible when the cluster hosts use a dedicated Replication VMkernel network (the option to add a Replication VMkernel adapter was added in vSphere 6.0, so it is not as common as having a vMotion VMkernel adapter).

- Separating the replication traffic is a recommended practice. This configuration should be used when a dedicated replication VMkernel interface is available.

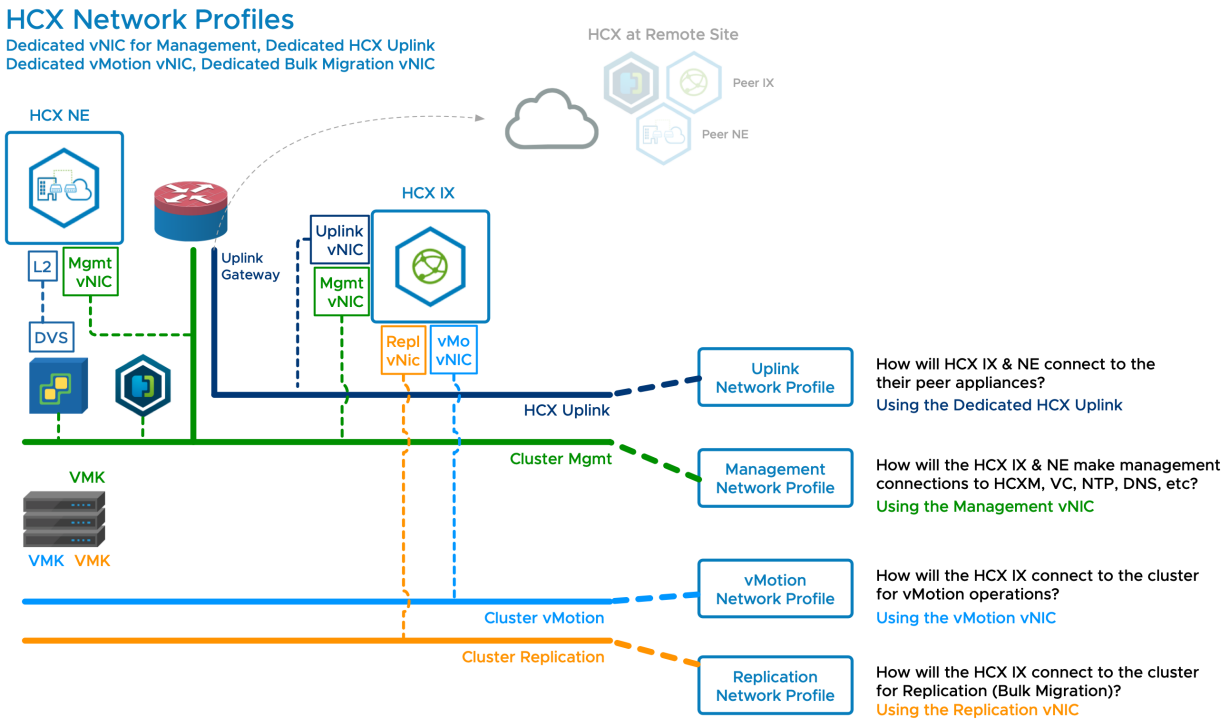
- **Important** In deployments where ESXi servers use a dedicated VMkernel configuration for vSphere Replication services, the HCX Interconnect uses a Network Profile configuration dedicated to the vSphere Replication traffic. This configuration does not include the vSphere Replication NFC traffic. HCX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



HCX Network Configuration 3 - Dedicated Uplink Network

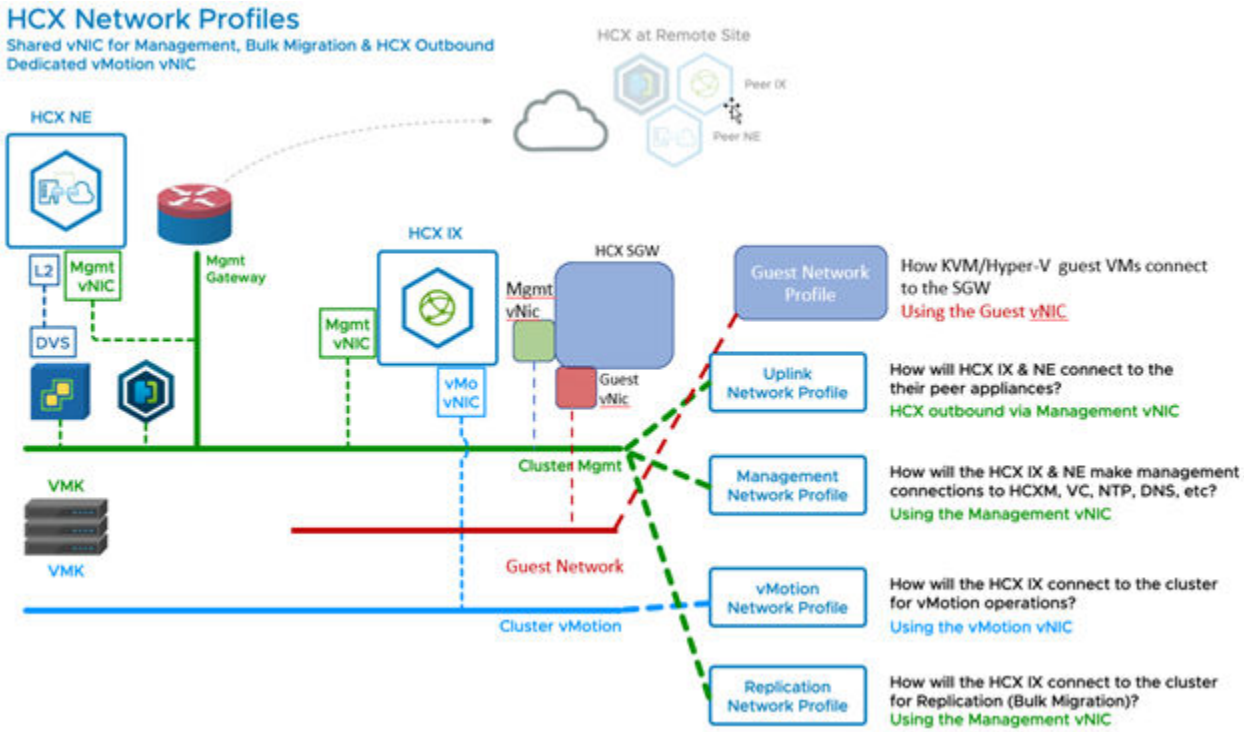
- Configuration 3 adds a dedicated network for HCX Uplink traffic (HCX Service Mesh Transport traffic).
- This configuration trades simplicity of deployment (see configuration 1) for the benefits of separating the uplink and management traffic.
- A dedicated uplink network is a good way to isolate the migration traffic for applying QOS or to control the outbound path.
- A dedicated uplink can be used to consume bandwidth/networks dedicated to the migration project.
- For deployments over the Internet:
  - Public IP addresses should be assigned at the destination using the HCX Uplink network profile.

- The source HCX appliances can use traditional Internet SNAT to securely connect to the destination public IP addresses using strong encryption.
- Public cloud providers leverage this configuration to make HCX services easy to deploy before dedicated private circuits become available.



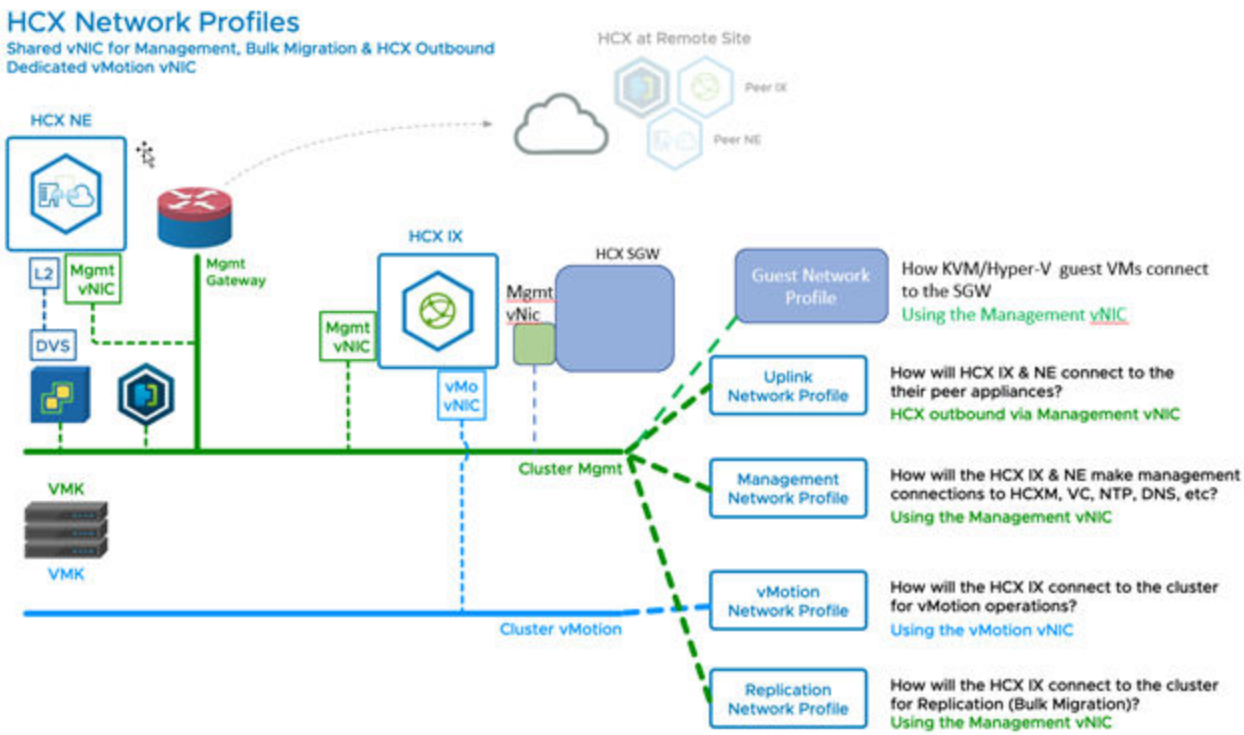
HCX Network Configuration 4 - OS Assisted Migration Using Guest Network

Configuration shows OS Assisted Migration networking when using a dedicated Guest Network for migrations.



HCX Network Configuration 5- OS Assisted Migration Using Management Network

Configuration shows OS Assisted Migration networking when using the Management Network for the Guest Network function.



Compute Profile Considerations and Concepts

A Compute Profile is a subcomponent of the Service Mesh. A Compute Profile describes which HCX services run, and how they are deployed when the Service Mesh is created.

Introduction to Compute Profiles

A **Compute Profile** configuration required for **Service Mesh** deployments. It defines deployment parameters, and allows service. See Creating a Compute Profile for configuration procedures. A **Compute Profile** is constructed of the following elements:

Services

The HCX services that are activated when a **Service Mesh** is created (only licensed services can be activated).

Service Cluster(s)

At the HCX source, the **Service Cluster** hosts should contain the virtual machines that will be migrated. For Network Extension, only Distributed Switches connected to selected **Service Clusters** are displayed. A **Datacenter** container can be used to automatically include clusters within the **Datacenter** container. Clusters are automatically adjusted in the **Compute Profile** when clusters are removed or added to the **Datacenter** container.

At the HCX destination, the **Service Clusters** can be used as the target for migrations.

Deployment Cluster(s)

The Cluster(or Resource Pool) & Datastore that will host the **Service Mesh** appliances.

For migrations to be successful, the **Deployment Cluster** must be connected such that the **Service Cluster(s)** vMotion and Management/Replication VMkernel networks are reachable to the HCX-IX appliance.

For Network Extension to be successful, the **Deployment Cluster** must be connected to a Distributed Switch that has full access to the VM network broadcast domains.

Management Network Profile

The **Network Profile** that HCX uses for management connections.

Uplink Network Profile

The **Network Profile** that HCX uses for HCX to HCX traffic.

vMotion Network Profile

The **Network Profile** that HCX uses for vMotion-based connections with the ESXi cluster.

Replication Network Profile

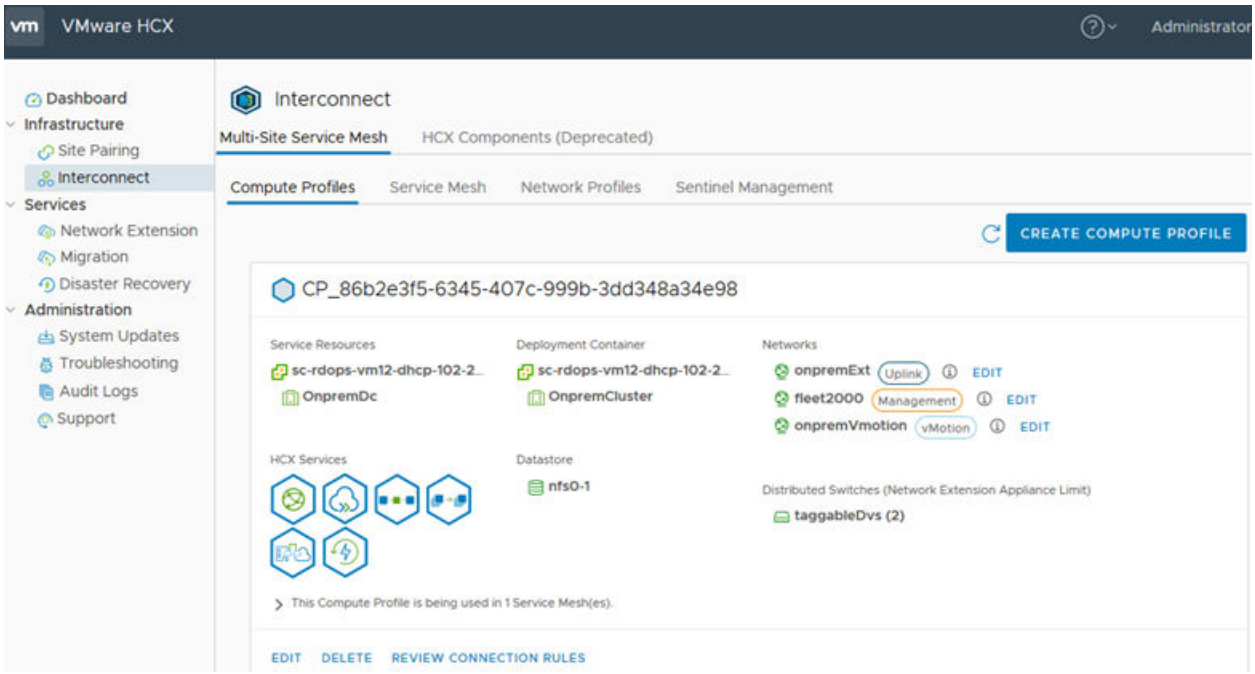
The **Network Profile** that HCX uses for Replication-based connections with the ESXi cluster.

Distributed Switches for Network Extension

The Distributed Switches containing the virtual machine networks that will be extended.

Guest Network Profile for OSAM

The **Network Profile** that HCX uses to receive connections from the Sentinel agents.



Characteristics of Compute Profiles

- An HCX Manager system must have one **Compute Profile**.
- **Compute Profile** references clusters and inventory within the vCenter Server that is registered in HCX Manager (other vCenter Servers require their own HCX Manager).
- Creating a **Compute Profile** does not deploy the HCX appliances (**Compute Profiles** can be created and not used).
- Creating a **Service Mesh** deploys appliances using the settings defined in the source and destination **Compute Profiles**.
- A **Compute Profile** is considered "in use" when it is used in a **Service Mesh** configuration.
- Changes to a **Compute Profile** profile are not effected in the **Service Mesh** until a **Service Mesh** a Re-Sync action is triggered.

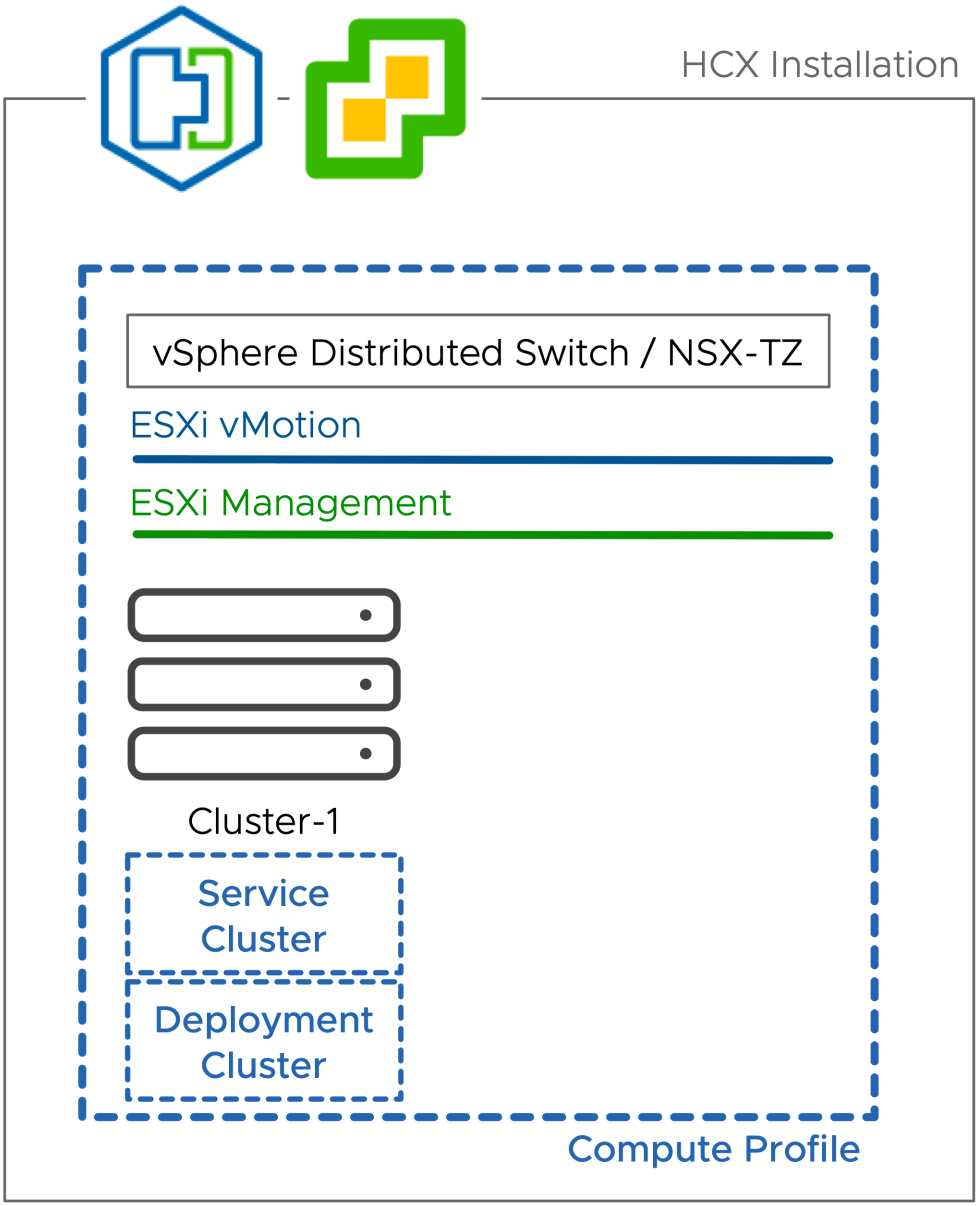
Compute Profiles and Clusters

The examples that follow depict the configuration flexibility when using Compute Profiles to design HCX Service Mesh deployments. Each example is depicted in the context of inventory within a single vCenter Server connected to HCX. The configuration variations are decision points that can be applied uniquely to each environment.

CP Configuration 1 - Single Cluster Deployments

In the illustrated example, Cluster-1 is both the **Deployment Cluster** and **Service Cluster**.

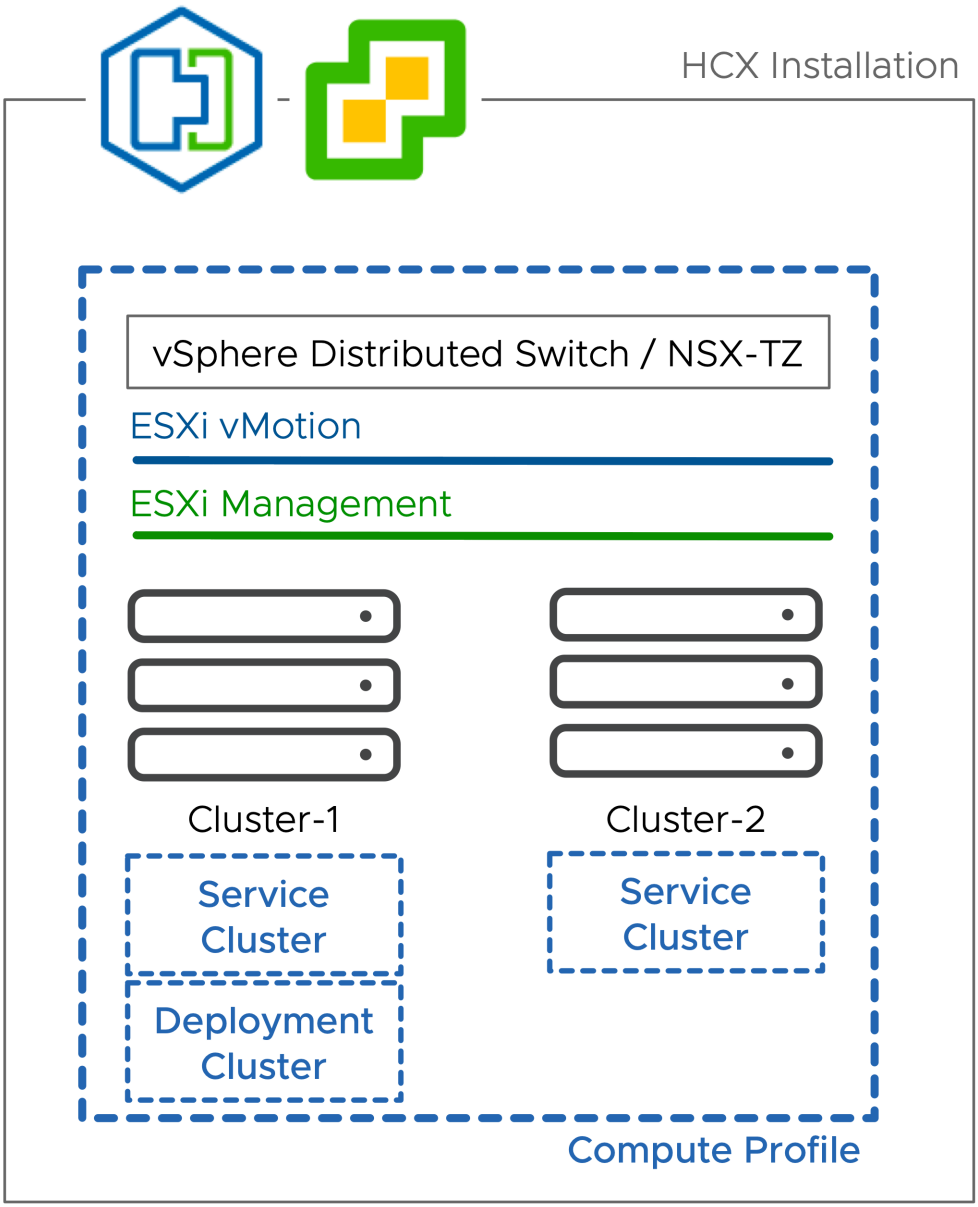
- Single cluster deployments use a single **Compute Profile** (CP).
- In the CP, the one cluster is designated as a **Service Cluster** and as the **Deployment Cluster**.



CP Configuration 2 - Multi Cluster (Simple CP)

In the illustrated example, Cluster-1 is the **Deployment Cluster**. Both Cluster-1 and Cluster-2 are **Service Clusters**.

- In this CP configuration, one cluster is designated as the **Deployment Cluster**, and all clusters (including the **Deployment Cluster**) are designated as **Service Clusters**.
- All the **Service Clusters** must be similarly connected (i.e. Same vMotion/Replication networks).
- When the **Service Mesh** is instantiated, one HCX-IX is deployed for all clusters.
- In larger deployments where clusters may change, a **Datacenter** container can be used (instead of individual clusters) so HCX will automatically manage the **Service Clusters**.



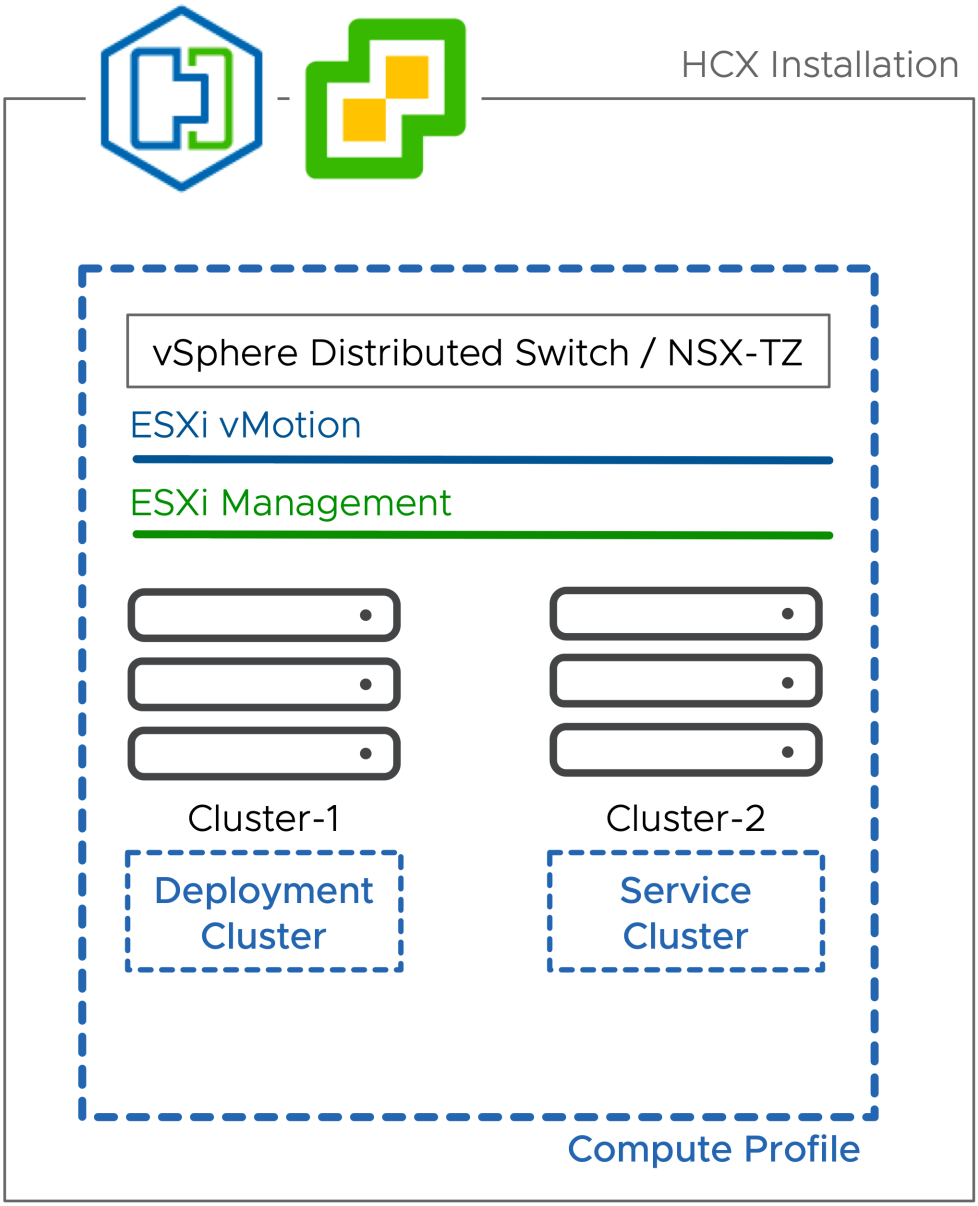
CP Configuration 3 - Multi Cluster (Dedicated Deployment Cluster)

In the illustrated example, Cluster-1 is the **Deployment Cluster** and Cluster-2 is the **Service Cluster**.

- In this CP configuration, one cluster is designated as the **Deployment Cluster** and is not a **Service Cluster**. All other clusters are designated as **Service Clusters**:
  - This CP configuration can be used to dedicate resources to the HCX functions.
  - This CP configuration can be used to control site-to-site migration egress traffic.

- This CP configuration can be used to provide a limited scope vSphere Distributed Switch in environments that heavily leverage the vSphere Standard Switch.

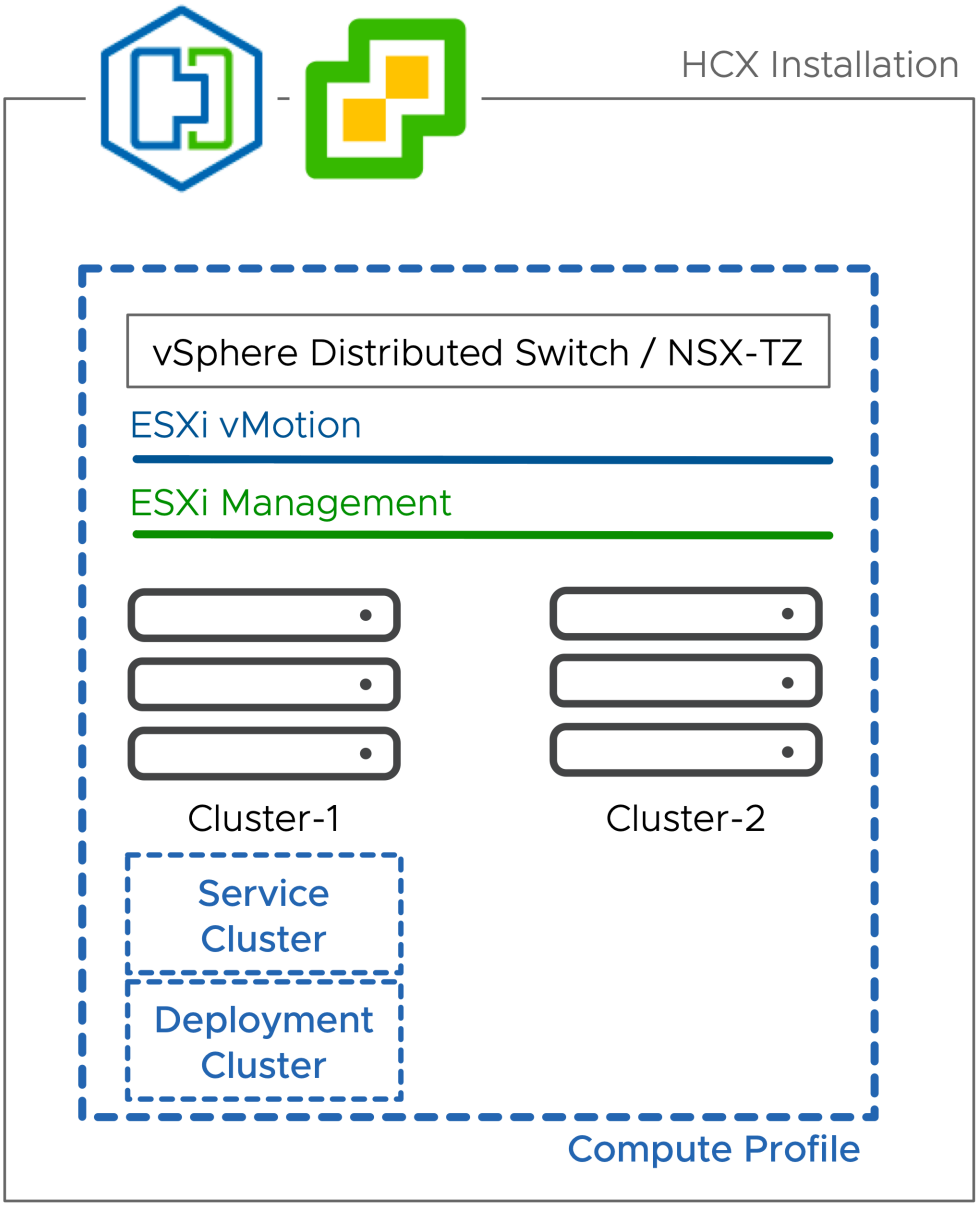
- For HCX migrations, this CP configuration requires the **Service Cluster** VMkernel networks to be reachable from the **Deployment Cluster**, where the HCX-IX is deployed.
- For HCX extension, this CP configuration requires the **Deployment Cluster** hosts to be within workload networks' broadcast domain (**Service Cluster** workload networks must be available in the **Deployment Cluster** Distributed Switch).
- When the **Service Mesh** is instantiated, one HCX-IX is deployed for all clusters.



CP Configuration 4 - Cluster Exclusions

In the illustrated example, Cluster-2 is not included as a **Service Cluster**.

- In this CP configuration, one or more servers have been excluded from the **Service Cluster** configuration.
- This can be used to prevent portions of infrastructure from being eligible for HCX services. Virtual machines in clusters that are not designated as a **Service Cluster** cannot be migrated using HCX (migrations will fail).

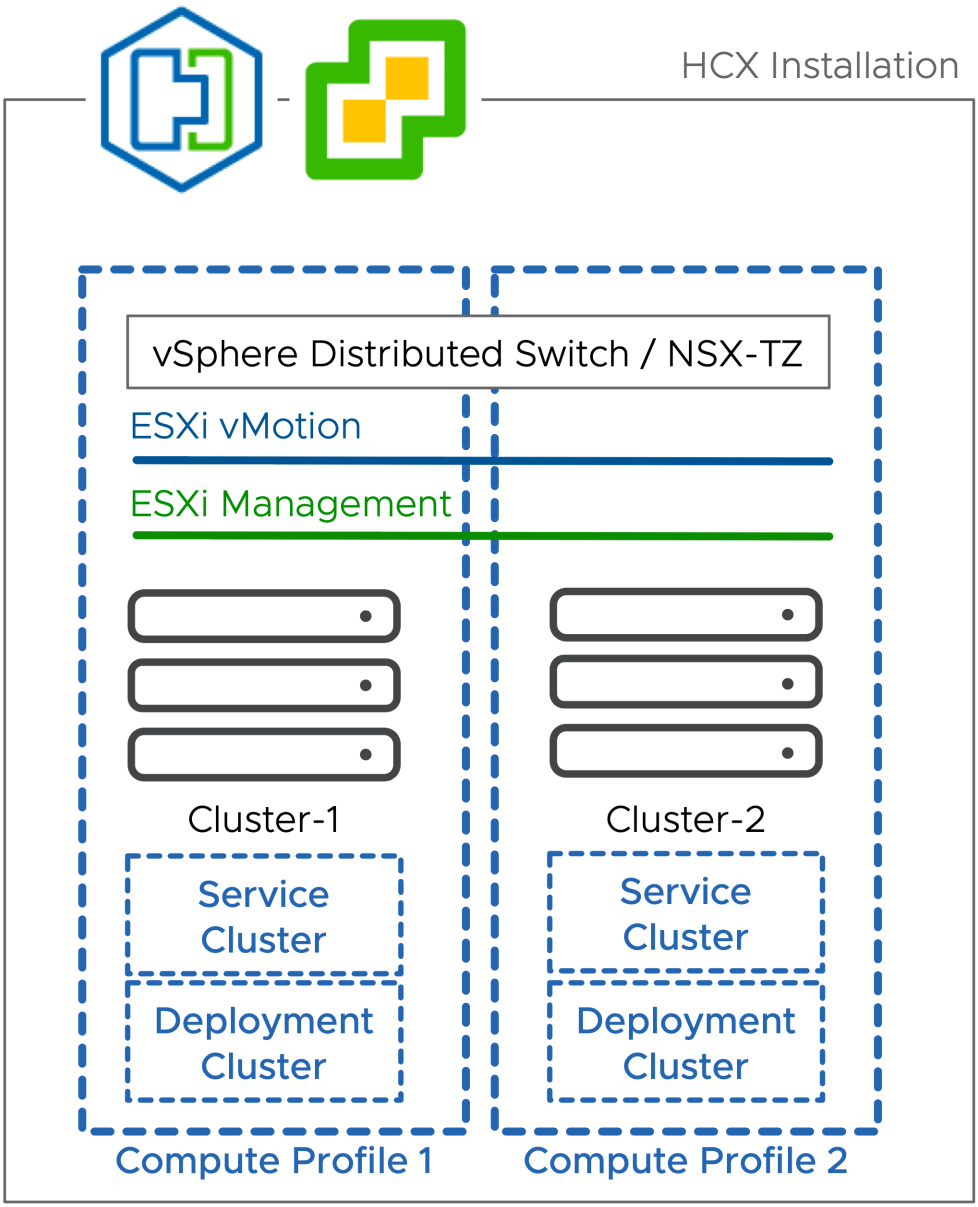


CP Configuration 5 - Multiple Compute Profiles (Optional, for Scale)

In the illustrated example, Compute Profile (CP) 1 has been created for Cluster-1 and CP-2 has been created for Cluster-2.

In the illustrated example, the VMkernel networks are the same. Creating additional CPs is optional (for scaling purposes).

- In this CP configuration ,**Service Clusters** are 'carved' into **Compute Profiles**.
- Every **Compute Profile** requires a **Deployment Cluster**, resulting in a dedicated **Service Mesh** configuration for each **Compute Profile**.
- As an expanded example, if there were 5 clusters in a vCenter Server, you might have **Service Clusters** carved out as follows:
  - CP-1: 1 Service Cluster , CP-2: 4 Service Clusters
  - CP-1 2 Service Clusters, CP-2: 3 Service Clusters
  - CP-1: 1 Service Cluster, CP-2: 2 Service Clusters, CP-3: 2 Service Clusters
  - CP-1: 1 Service Cluster, CP-2: 1 Service Cluster, CP-3: 1 Service Cluster, CP-4: 1 Service Cluster, CP-5: 1 Service Cluster
- It is worthwhile noting that the distinct **Compute Profile** configurations can leverage the same **Network Profiles** for ease of configuration.



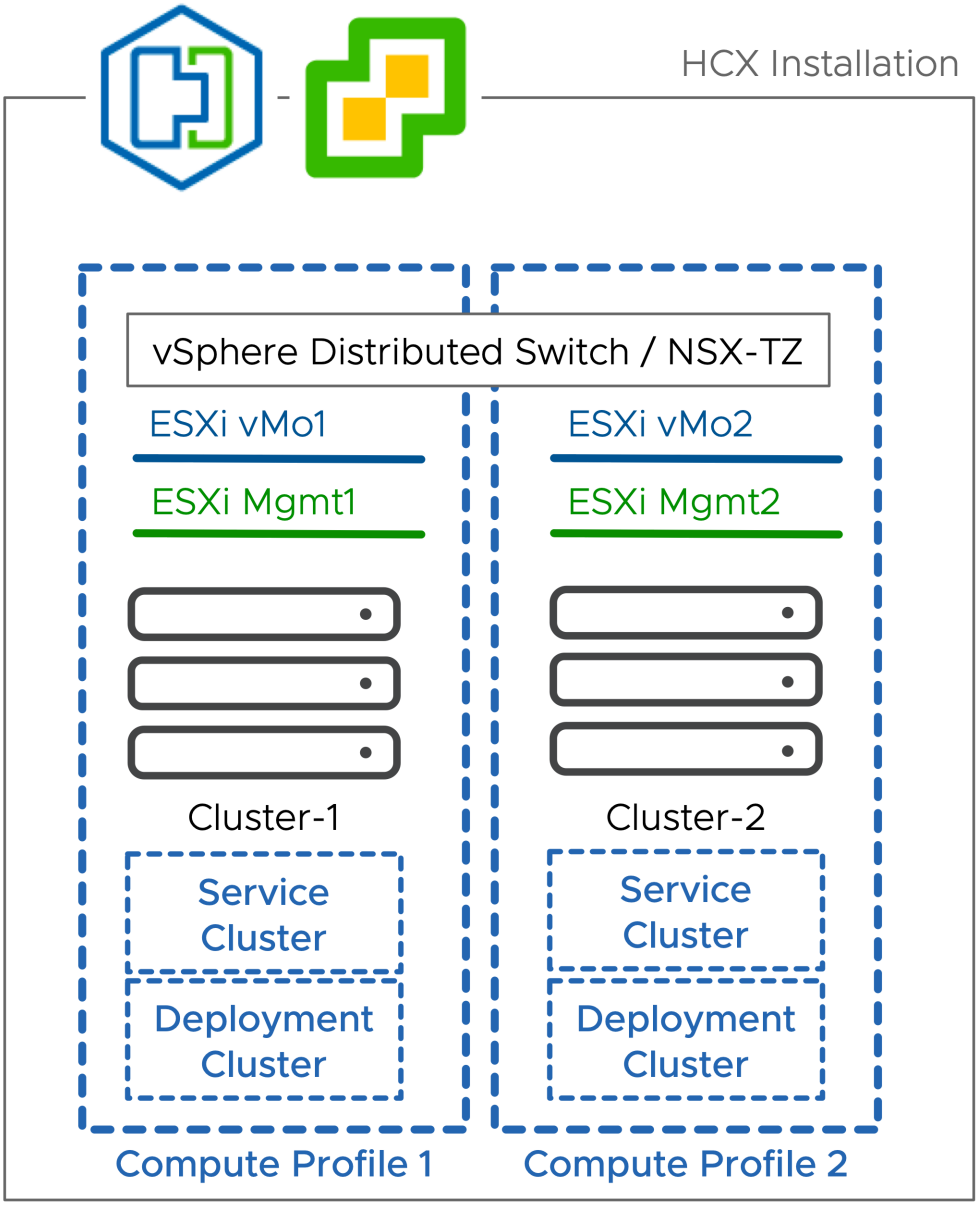
CP Configuration 6 - Multiple Compute Profiles (with Dedicated Network Profiles)

In the illustrated example, Cluster-1 uses vMotion and Mgmt network 1. Cluster-2 uses vMotion and Mgmt network2.

In the illustrated example, the VMkernel networks are different, and isolated from each other. Creating dedicated Network Profiles (NPs) and dedicated Compute Profiles (CPs) is required.

- In this CP configuration, the **Service Clusters** are 'carved up' into distinct **Compute Profiles**. The **Compute Profiles** reference cluster-specific **Network Profiles**.

- Because the **Service Mesh** HCX-IX appliance connects directly to the cluster vMotion network, anytime the cluster networks for Replication and vMotion are different, cluster-specific **Network Profiles** should be created, and assigned to cluster-specific **Compute Profiles**, which will be instantiated using cluster-specific **Service Mesh**.



Appendix - HCX Installation Summary Steps

8

This reference lists all the steps involved when deploying an HCX Connector, or HCX Cloud system. The steps are listed here as a quick reference. Requirements are not listed here. Use the checklists in this publication to prepare for the installation.

Install (or Enable) HCX Cloud at the Destination

1 Enable the HCX Service (in a public cloud), or Install HCX Cloud Manager at the destination:

   a If the destination is a Public Cloud instance, the provider may deploy HCX Cloud automatically when the service is enabled. If not, continue to step b.

   b If the destination environment is a Private Cloud:

      1 Use the HCX-Cloud-Manager-########.OVA to deploy the HCX Manager in the vSphere Client.

      2 Browse to the HCX Appliance Management (9443) interface and activate or license HCX and set the Location.

      3 Register the vCenter Server & NSX Manager.

      4 Define Role Mapping (this setting defines the groups can perform HCX operations).

      5 Restart the HCX Services

2 In the destination environment HCX Cloud Manager, create a Compute Profile:

   a If the destination is VMware Cloud Foundation or a private SDDC installation:

      1 Browse to the HCX UI (443) or use the HCX Plug-in in vSphere to create a Compute Profile. The compute profile defines how HCX Services Mesh components is deployed in the destination environment.

   b If the destination is a Public Cloud instance, review the existing Compute Profile and Uplink Network Profile configurations.

3 Configure firewalls to allow the inbound HCX traffic:

   a Allow TCP-443 inbound from the planned source HCX Manager to the HCX Cloud Manager at the destination (this may be a NAT Public IP if the environments are separated by Internet).

b Allow UDP-4500 inbound from the source HCX IX and NE planned IP addresses (this may be a NAT IP if the environments are separated by Internet).

4 Configure any other firewalls as needed. Reference ports.vmware.com for the complete list of HCX network ports.

5 Install HCX at the source environment:

Install the HCX Connector Source

1 Use the HCX-Connector-Manager-########.OVA to deploy the HCX Manager system in the vSphere Client. After the OVA is deployed and the system is initialized:

a Browse to the HCX Appliance Management interface (:9443), authenticate with the Admin user.

b Activate HCX.

c Register the vCenter Server, SSO, and optionally the NSX Manager.

d Configure Role Mapping (this defines the SSO user groups can perform HCX operations).

2 Create a Compute Profile:

a Browse to the the HCX Connector service UI (:443), authenticate with a user that is part of the role-mapping group. Or use the HCX plug-in to create a Compute Profile.

3 Create a Site Pairing:

a The HCX Connector service UI (:443) registers the remote HCX Cloud system using the SSO group from the destination environment (or Cloud admin if the target is a VMC SDDC)

4 Create a Service Mesh:

a The HCX Connector service UI (:443) uses the Service Mesh wizard to instantiate services.

1 In the service mesh interface you select a Compute Profile for the HCX Connector environment, and a Compute Profile for the destination environments.

2 Service mesh creation deploys HCX components in parallel at the source and the destination environments.

3 The source HCX service components are Initiators, and will automatically attempt to establish HCX tunneling connections to the destination side.

4 The destination HCX service components are Receivers that will only accept tunneling request from the Initiators.