WHITE PAPER – **AUGUST 2018**

MULTICLOUD WORKLOAD MIGRATION STRATEGIES WITH VMWARE CLOUD FOUNDATION™

vmware®

Table of Contents

Introduction

We live in a multicloud world where application workloads require a highly resilient and flexible infrastructure: the kind of infrastructure that enables users to move those workloads freely between data centers, as well as between private and public clouds, with minimal downtime and without having to replatform. Business today demands the flexibility to choose where to run workloads as well as the option of the private or public cloud. VMware believes that the key to realizing this kind of highly resilient and flexible environment is in the adoption of a software-defined approach to IT infrastructure. We call this the Software-Defined Data Center (SDDC). The SDDC is the architecture for the modern hybrid cloud. The VMware SDDC is extensively tested, validated, and automated through VMware Cloud Foundation™ for a turnkey product approach. Cloud Foundation can be both deployed on premises, as part of a private cloud, and hosted by cloud providers, as a public cloud offering.

A Cloud Foundation deployment is only the start. Customers have large numbers of existing, mission-critical workloads already running in their data centers. As they work to transition their data centers into private clouds and possibly to look to adopt public clouds, they must be able to migrate these existing workloads off their legacy infrastructure and into the new SDDC. This white paper provides an overview of the available migration options and enables readers to understand the pros and cons of each option to help determine which is best suited to pursue the fastest path to the hybrid cloud.

Scope

The workload migration examples in this document are based on a migrating-to-multicloud operational model using the components of the VMware SDDC. This model enables users to run application workloads in any cloud based on the VMware SDDC, whether that cloud is on premises or with a public cloud service provider. Regardless of which cloud is chosen, this document provides an overview of the migration options available and the technical guidance to complete the installation, configuration, and operational procedures for migrating application workloads into a true hybrid cloud.

Migration Strategy

Business drivers—cost, data security, data locality, compliance, burst capacity, consolidation, mergers and acquisitions, and many others—ultimately impel placement decisions regarding application workloads. There is no "one size fits all" migration approach. Each customer is unique, and VMware gives users the freedom to choose where applications reside. We also understand that where a workload is placed today might not be where it is needed to run tomorrow. VMware aims to provide a highly secure, highly reliable infrastructure that gives users the flexibility to move workloads as needed to best meet business demands. This white paper considers all these factors to help users determine the best tool for a migration strategy.

Migration Types

There are two primary methods of migrating application workloads: *live migration* and *cold migration*. We will now review the meaning and assumptions for each.

Live Migration

Live migration, also referred to as *hot migration* or VMware vSphere® vMotion® migration, is the ability to relocate an application workload with no downtime. This means that virtual machines (VMs) are not powered off and the IP address does not change.

To determine whether hot migration is optimal, first consider network connectivity. The migration target location must be on the same layer 2 (L2) IP subnet. Although this is possible, it adds a level of complexity to the environment. Regarding L2 stretch, consider how to best manage the maintenance of these systems as well as all possible downtime scenarios. Review the "Appendix" at the end of this document to learn about many of the possible VM guest settings that can impact all migrations.

MIGRATION APPROACH	PROS	CONS
Live Migration	• No downtime • No changes to the guest OS or application	• Requires stretching the L2 IP network, which adds complexity

Table 1. Pros and Cons of Live Migration

Cold Migration

Cold migration is the most flexible option. With this approach, there is a brief outage as the VM guest is powered off while it is migrated. In addition, because the VM is powered down, it enables changing the IP address and subnet during the move. Workloads do not have to be offline for long periods of time during a cold migration. Very fast cold migrations with little downtime, sometimes less than a few minutes, can be achieved with careful planning and preparation by using the tools discussed in this paper. The following benefits of cold migration are not available with live migration:

- Cold migration enables upgrades of VM compatibility level and VMware Tools™ version.
- Application workloads can take advantage of new capabilities associated with newer virtual hardware.
- Moving to a newer-generation physical server can make new CPU instruction sets available to the operating system (OS) or application.
- NUMA boundaries and configuration can change, based on the new hardware.

See the "Appendix" for details on many of the settings that can be affected by migration.

MIGRATION APPROACH	PROS	CONS
Cold Migration	• Most flexible • Enables changing IPs as well as upgrading VM compatibility and VMware Tools versions • Enables use of new hardware features	• Requires downtime

Table 2. Pros and Cons of Cold Migration

Migration Direction

Migration is not a one-way street in a multicloud world. Business requirements change. Regulatory requirements change. These changes can require moving workloads migrated to the cloud back on premises or vice versa. Consider this when designing a migration strategy. This white paper is written with an understanding that migrations occur in both directions. This gives enterprises flexibility and choice with application workloads.

VMware Cloud Foundation Bill of Materials

This white paper is based on the use of Cloud Foundation version 2.3. Table 3 is the bill of materials included with Cloud Foundation. Features and functions discussed in this document are based on the capabilities of these components.

SOFTWARE COMPONENT	VERSION	DATE	BUILD NUMBER
VMware Cloud Foundation bundle	2.3.0	18-Jan-18	7597069
VMware SDDC Manager	2.3.0	11-Jan-18	7524634
Platform Services Controller™	6.5 U1e	9-Jan-18	7515524
VMware vCenter Server® on VMware vCenter Server Appliance™	6.5 U1e	9-Jan-18	7515524
VMware vSphere (VMware ESXi™)	6.5 P02	18-Jan-18	7388607
VMware vSAN™	6.6	11-Jan-18	7395176
VMware NSX® for vSphere® (NSX-V)	6.3.5	11-Jan-18	7119875
VMware vRealize Operations™	6.6.1	8-Aug-17	6163035
VMware vRealize Automation™	7.3	25-May-17	5610496
VMware vRealize® Log Insight™	4.3	3-Jun-17	5084751
VMware Tools	10.1.15	9-Sep-17	6677369
VMware Horizon® View™ Standard Edition	7.2	26-Jun-17	5748532
VMware App Volumes™	2.12	8-Dec-16	

Table 3. Cloud Foundation Bill of Materials

Cloud Foundation Network Topology

Cloud Foundation leverages the advanced automation capabilities of the VMware SDDC Manager to automate and simplify the deployment of the SDDC based on VMware Validated Designs (VVDs). An understanding of the underlying physical and virtual networking architecture implemented by Cloud Foundation is essential to designing a migration strategy and knowing how to route and control network traffic.

Figure 1 illustrates the physical network topology for Cloud Foundation version 2.3.

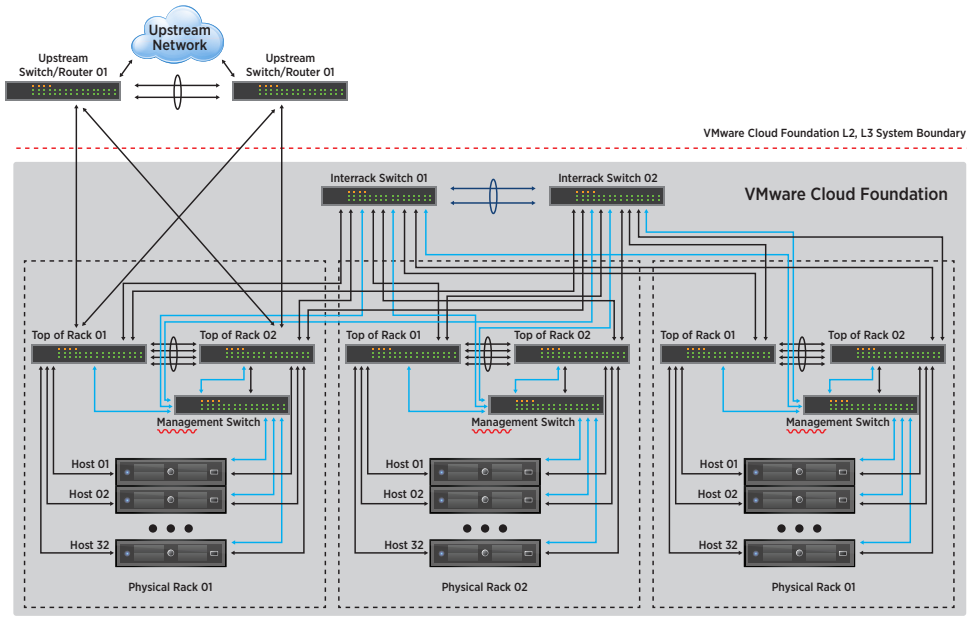


Figure 1. Physical Network Topology for Cloud Foundation Version 2.3

In this design, all north–south network traffic for Cloud Foundation egresses through the top-of-rack (ToR) switches in **Rack 01**. Access to and from any legacy vSphere system or public cloud provider is via these physical ports.

Layered on top of the physical network, Cloud Foundation leverages the software-defined networking capabilities provided by VMware vSphere Distributed Switch™ (VDS) together with NSX-V instance. Figure 2 depicts the Cloud Foundation software-defined logical network topology implemented with Cloud Foundation version 2.3.

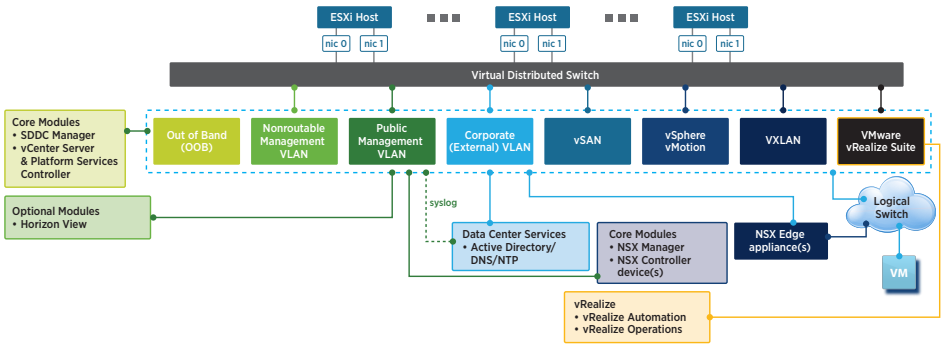


Figure 2. Software-Defined Logical Network Topology Implemented with Cloud Foundation Version 2.3

This logical network topology determines the migration methods that can be used with Cloud Foundation. This is because the nonroutable management VLAN is not routed out of the physical rack to the corporate uplinks. For security reasons, this VLAN is accessible only inside Cloud Foundation.

Migration Tool Options

Migration path can quickly be determined based on the two migration choices —live and cold—and by the version of legacy vSphere system that is running.

This white paper reviews five possible tools and methods for migration:

1. vSphere API using Microsoft Windows PowerShell and VMware vSphere PowerCLI™
2. Cross vCenter vMotion Migration Utility Fling
3. VMware vSphere Replication™
4. NAS third-party storage array
5. NSX Hybrid Connect

Figure 3 shows the five choices, and the legacy vSphere version(s) they support, for live migration. Live migration requires that the L2 VLAN that the VM currently runs on be extended to the Cloud Foundation site.

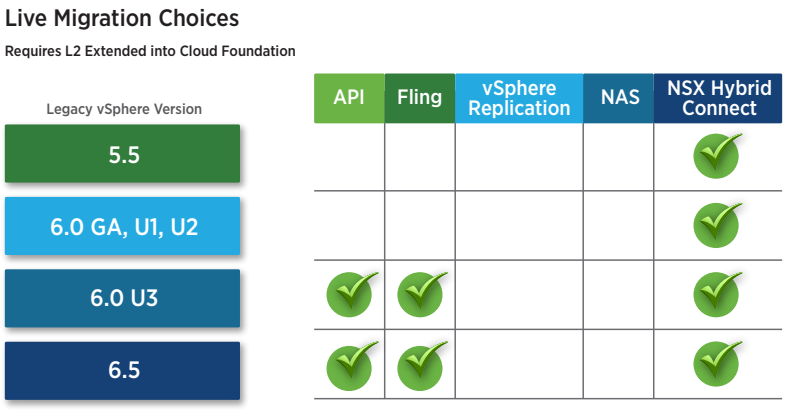


Figure 3. Five Choices for Live Migration

Figure 4 is a similar chart that again shows the five options. This time, support for cold or low-downtime migration is also shown.

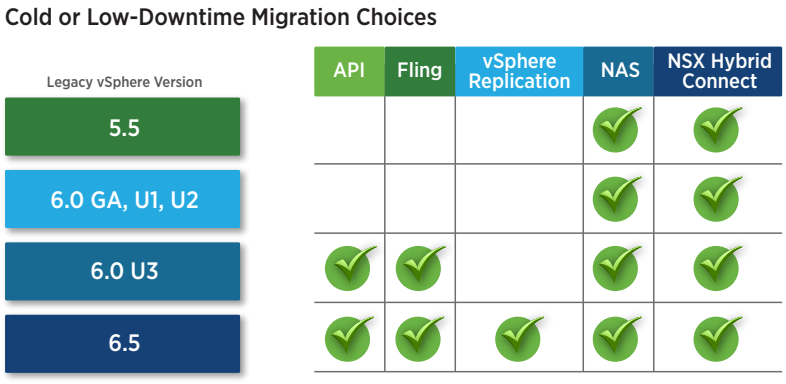


Figure 4. Five Choices for Cold or Low-Downtime Migration

This white paper next discusses the details of the tools, providing an overview, architecture, installation, and migration usage for each.

VMware API – vSphere PowerCLI – Cross vCenter vMotion

Overview

vSphere 6.0 introduced a new feature called Cross vCenter vMotion. This API or SDK feature enables an administrator to live-migrate or cold-migrate a VM from one vCenter Server instance to another without being connected to the same single sign on (SSO) domain. The Cross vCenter Migration Utility Fling uses this API, with an added simple user interface that makes it easy to use. Beginning with vSphere 6.5, vSphere PowerCLI added this feature to the Move-VM commandlet. For administrators who are comfortable using vSphere PowerCLI, this is an easy-to-use and free option for migrating VMs to a Cloud Foundation site.

Requirements

VMware Knowledge Base article 2106952 documents some restrictions with the API. Legacy vCenter Server instances running vSphere 6.0 U3 or later can use this vSphere PowerCLI command to migrate VMs. Both live migration and cold migration options are fully supported.

Architecture

The architecture for the API is straightforward and consists of just a few components. See Figure 5. The administrator must provide a client computer to run PowerShell with the vSphere PowerCLI plug-in installed. This client computer must have network access to both vCenter Server instances involved in the migration.

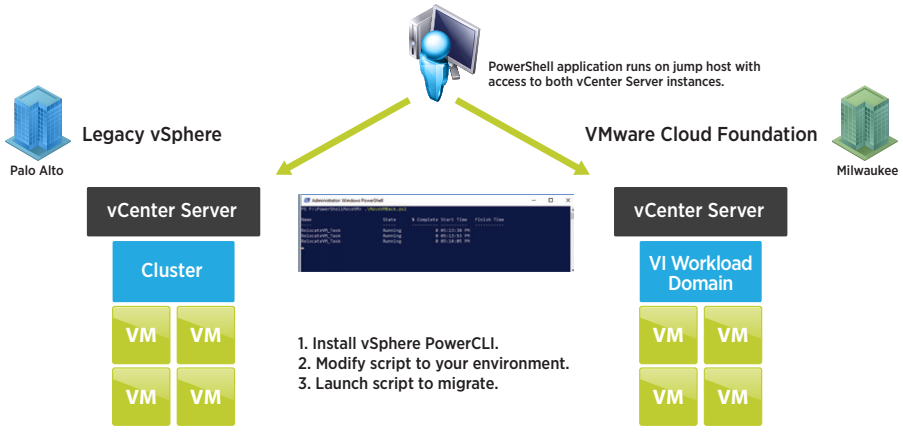


Figure 5. API Migration Architecture Overview

Figure 6 shows the network architecture for live migration. The same VLAN must be present in both sites, and the vSphere vMotion port groups must have layer 3 (L3) routes to each other as depicted in the diagram.

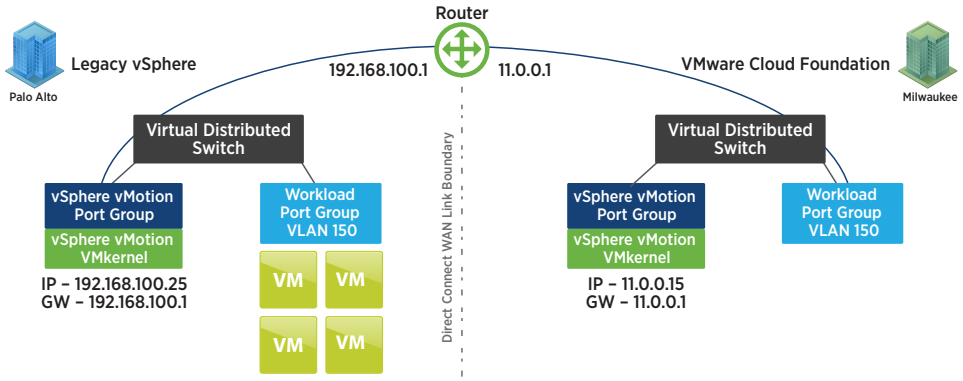


Figure 6. Network Architecture for API Live Migration

Installation

Follow the installation instructions for the vSphere PowerCLI plug-in.

Migration

With vSphere PowerCLI installed, see the following sample PowerShell script for migrating VMs from a legacy vCenter Server site to a Cloud Foundation site. It is easy to modify this sample code to suit individual needs. Included here is a sample for concurrently migrating multiple VMs with an array. Bulk migration is also possible with PowerShell.

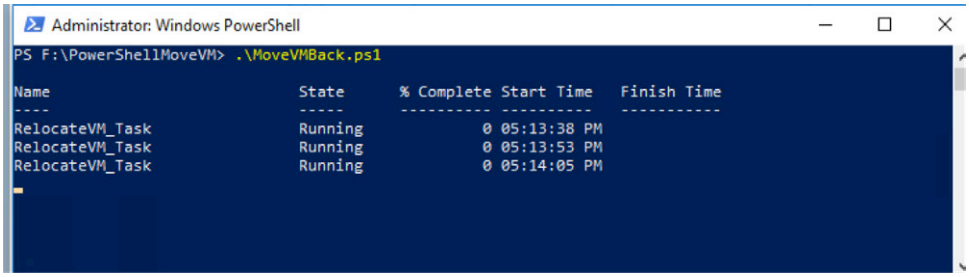
```
#Enter the Following Variables

##########Target Virtual Center##########

$targetVCname = "vcenter-1.sddc.lab.local"

$targetVCusername = "sddc-admin@vsphere.local"

$targetVCpassword = "VMware1!"

########################################


##########Source Virtual Center##########

$sourceVCname = "vc01.lab.local"

$sourceVCusername = "administrator@vsphere.local"

$sourceVCpassword = "VMware1!"

########################################
```

```
###########Target Information############
#####Enter the specific ESXi host you want to migrate to
$vmhost = "r1n0.sddc.lab.local"

#####Enter VM Names to migrate
$vm1 = "Tiny_Linux_VM_1"
$vm2 = "Tiny_Linux_VM_2"
$vm3 = "Tiny_Linux_VM_3"
$vm4 = "Tiny_Linux_VM_4"
$vmnames = $vm1,$vm2,$vm3,$vm4

#####Enter the Name of the virtual Switch to Migrate to
$TargetswitchName = "vRack-DSwitch"

#####Enter the Name of the PortGroup to migrate to
$Targetportgroup = "vDSMigrate"

#####Enter the Name of the DataStore to Migrate to
$TargetDatastore = "vsanDatastore1"

#####Enter the Disk Type for the target destination
# Thin, Thick, and EagerZeroedThick values
$TargetDiskType = "Thin"

Foreach ($vmname in $vmnames)
{
$targetVCconn = Connect-VIServer -Server $targetVCname -User
$targetVCusername -Password $targetVCpassword
$sourceVCconn = Connect-VIServer -Server $sourceVCname -User
$sourceVCusername -Password $sourceVCpassword
```

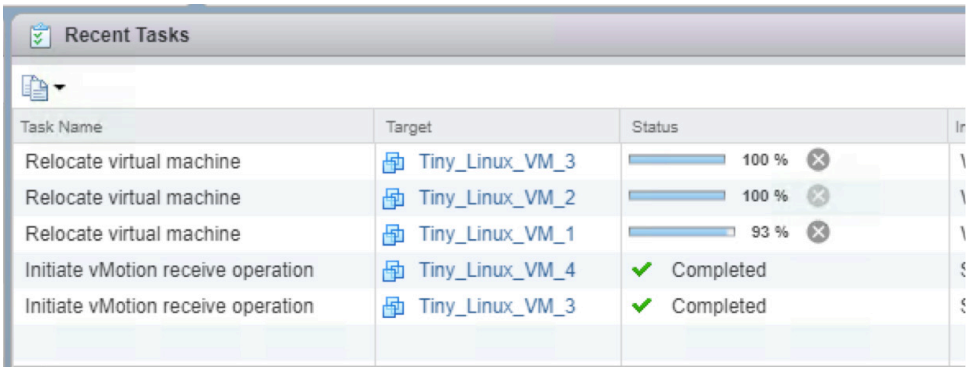
```
$vm = Get-VM -Server $sourceVCconn $vmname

$networkAdapter = Get-NetworkAdapter -VM $vm -Server $sourceVCconn

$destinationPortGroup = Get-VDPortgroup -VDSwitch $TargetswitchName
-Name $Targetportgroup -Server $targetVCconn


Move-VM -VM $vm -VMotionPriority High -Destination (Get-VMhost -Server
$targetVCconn -Name $vmhost) -RunAsync -NetworkAdapter $networkAdapter
-DiskStorageFormat $TargetDiskType -PortGroup $destinationPortGroup
-Datastore (Get-Datastore -Server $targetVCconn -Name $TargetDatastore )

}
```

Save this sample code into a text file. Save the text file with the .ps1 file extension.

Now execute the PowerShell script from the PowerShell interface.



From the VMware vSphere Web Client, monitor the migration tasks for the VMs moved with this script.



Summary

This small code sample demonstrates the ease of use. This API is fully supported by VMware. For code samples that contain more options for migration, see this article. It contains sample code that goes much deeper into using this powerful API.

Cross vCenter Workload Migration Utility Fling

Overview

The Cross vCenter Workload Migration Utility Fling provides easy migration between various vCenter Server infrastructures—that is, with different SSO domains—using the Cross vCenter vMotion feature built into vSphere 6.x. Shared storage is not required between sites because the Fling uses VMware vSphere Storage vMotion® to migrate the entire VM.

Flings are applications and tools built by VMware engineers and our community that are intended to be tested and explored. All Flings are officially unsupported, but many have become official VMware products.

The Cross vCenter Workload Migration Fling uses officially supported VMware APIs, and it consolidates them into a graphical user interface (GUI) for easy consumption. This migration Fling offers two options for migration: cold and live migration. Cold migration is more flexible, enabling migrations for mismatching vCenter Server versions and virtual switch types or versions. A few requirements must be met to complete the process successfully when choosing live migration. Live migration with Cloud Foundation requires that the source and target sites use the same switch type and version. Because Cloud Foundation uses VDS 6.0, a legacy vCenter Server instance must use the same.

Architecture

The Fling architecture is straightforward and consists of only a few components.

The administrator must provide a client computer to run the Fling Java application. This client computer must have network access to both vCenter Server instances involved in the migration, as depicted in Figure 7.

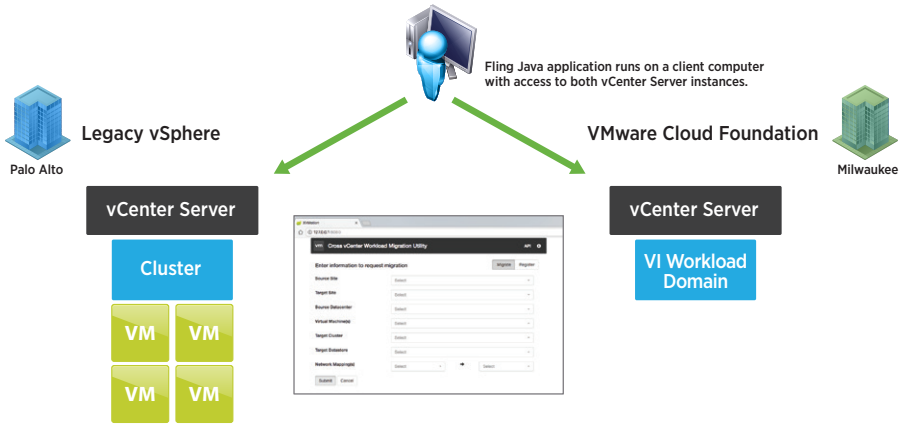


Figure 7. Architecture Overview Using Cross vCenter Workload Migration Utility Fling

For live migration, the same VLAN must be present in both sites, and the vSphere vMotion port groups must have reciprocal L3 routes as depicted in Figure 8.

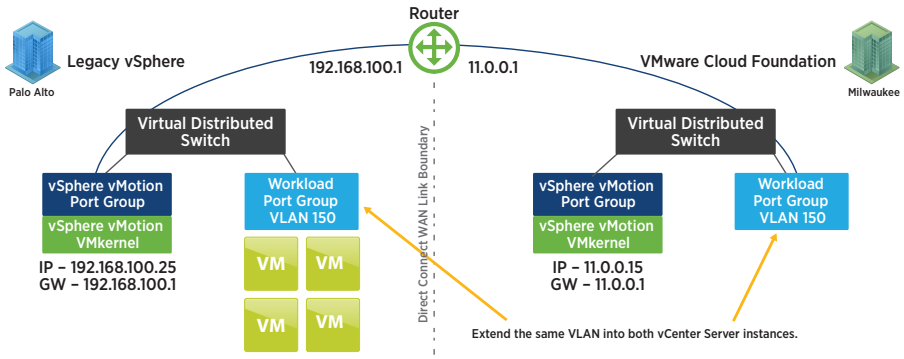
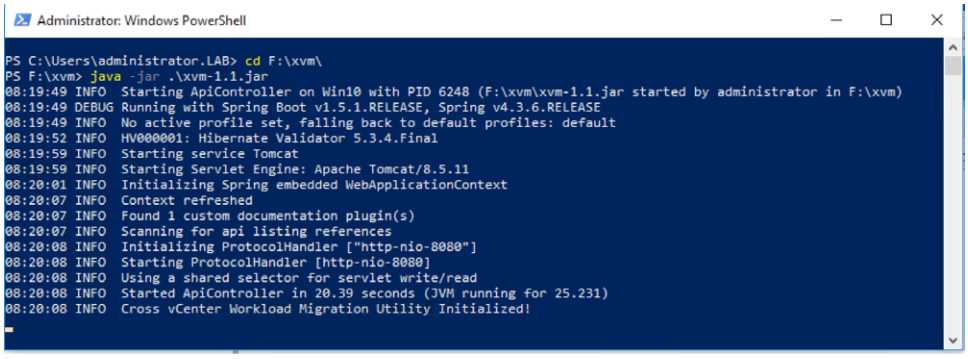


Figure 8. Network Architecture Showing VLANs and L3 Routes

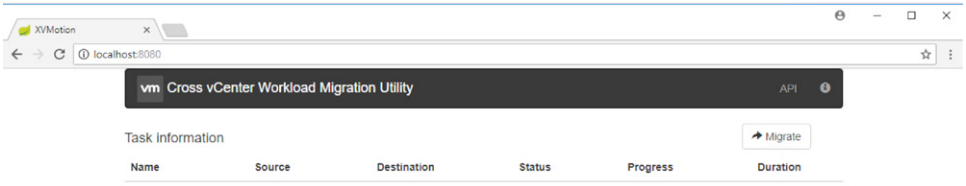
Installation on Cloud Foundation

Download the Fling from the Cross vCenter Workload Migration Utility Fling web page.

Review the requirements to ensure that the correct version of Java is installed on the client computer. Then launch the XVM#.#.jar file from a chosen shell. It is demonstrated here using Microsoft Windows PowerShell, as depicted in the following screenshot.

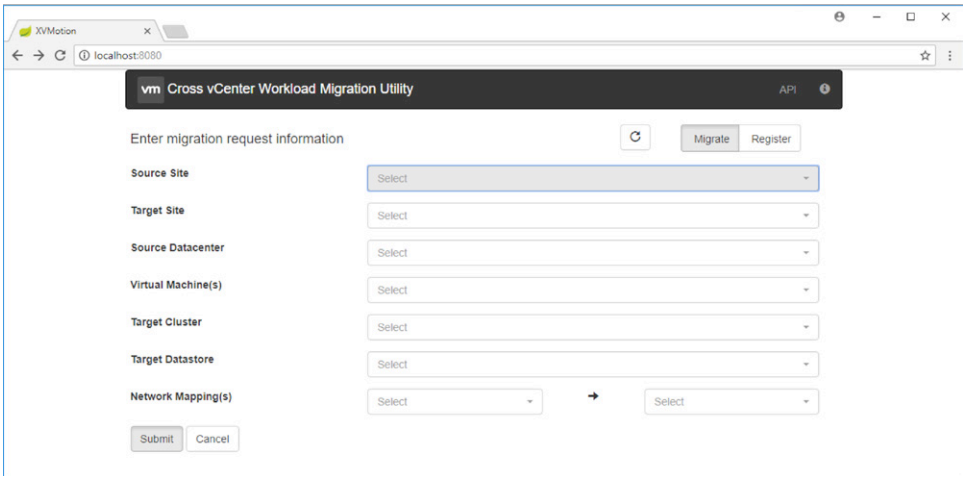


After the Java application has started successfully, open the web browser and direct it to http://localhost:8080. Connecting to the Fling web application prompts a greeting with the following user interface (UI).



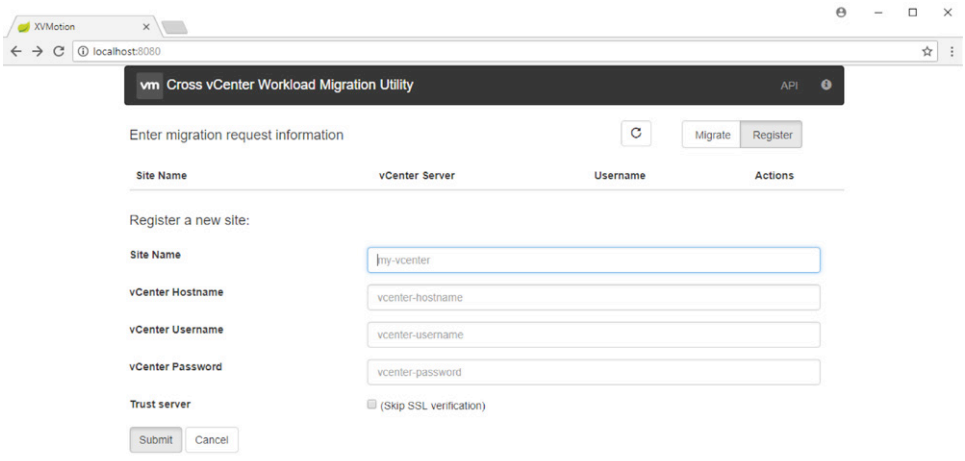
Click **Migrate**.

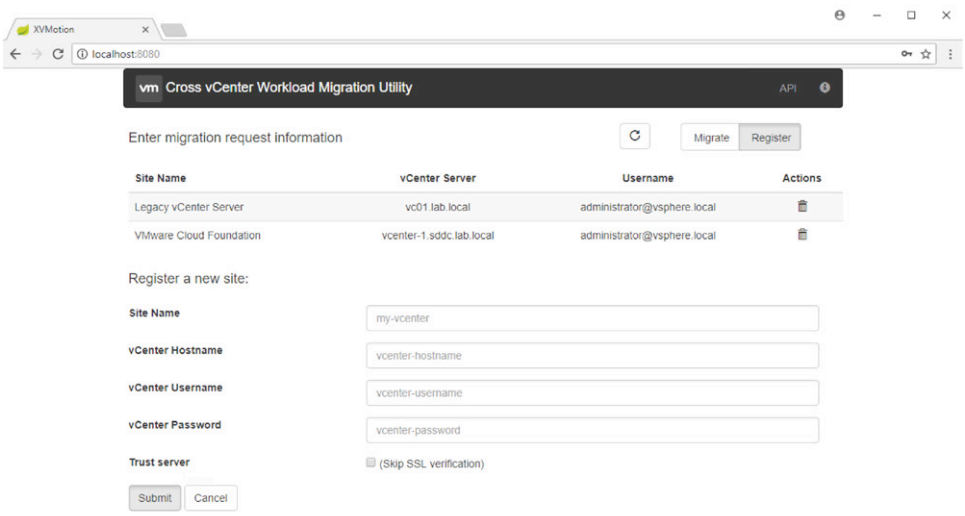
To begin registration of source and target vCenter Server instances, click **Register**.



Enter the legacy vCenter Server information in the registration form. Click **Submit**.

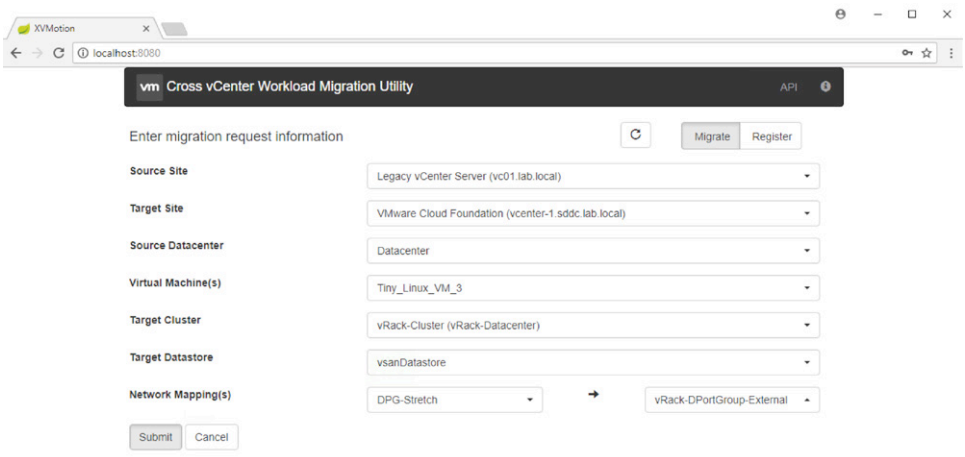
Repeat the process for the Cloud Foundation vCenter Server instance.



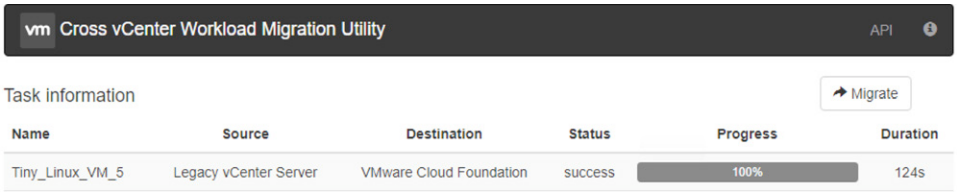


When both sites have successfully been registered, click **Migrate**. Complete the form to begin the migration process.

After selecting **Source Site**, **Target Site**, and **Virtual Machine(s)** information, click **Submit** to begin the migration process.



This leads to the **Task information** UI, where you can monitor the progress of the migration. As shown in the following screenshot, the VM migration has been successful.



The migration process is the same for both live and cold migrations. Multiple VMs can be selected concurrently to complete a bulk migration.

Summary

The Fling migration tool is free to download and provides a simple, easy-to-use interface for the Cross vCenter Migration features built into vSphere systems. This tool is a Fling and is not officially supported. For any issues with it, open a bug on the Fling website and post your log information.

vSphere Replication

vSphere Replication is a hypervisor-based, asynchronous replication solution for vSphere VMs. It is included at no extra cost with most vSphere versions. Originally designed for data protection and disaster recovery, it can also be used as a low-cost, easy-to-use vSphere migration tool.

Architecture

In this white paper, we install the vSphere Replication appliance on a Cloud Foundation instance with a private replication subnet so bandwidth usage can be controlled with VMware vSphere Network I/O Control. Using Network I/O Control ensures that migrations do not negatively impact production workloads. Cloud Foundation supports configuration of additional VMkernel adapters that are dedicated to vSphere Replication for network traffic isolation. Do not modify the VMkernel adapters created by the SDDC Manager.

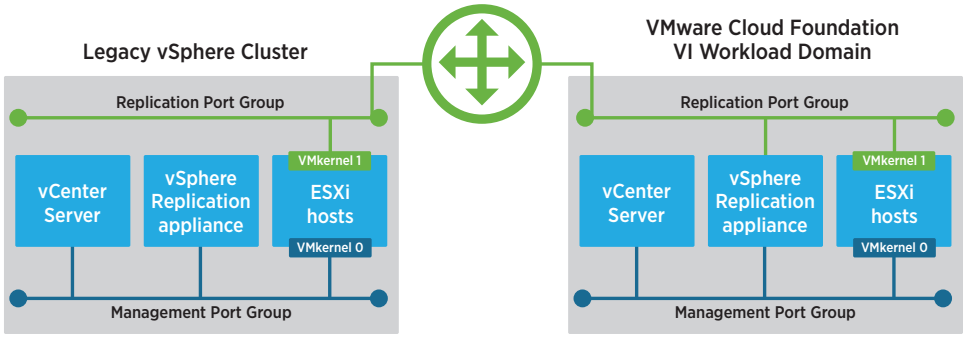


Figure 9. vSphere Replication Architecture Overview

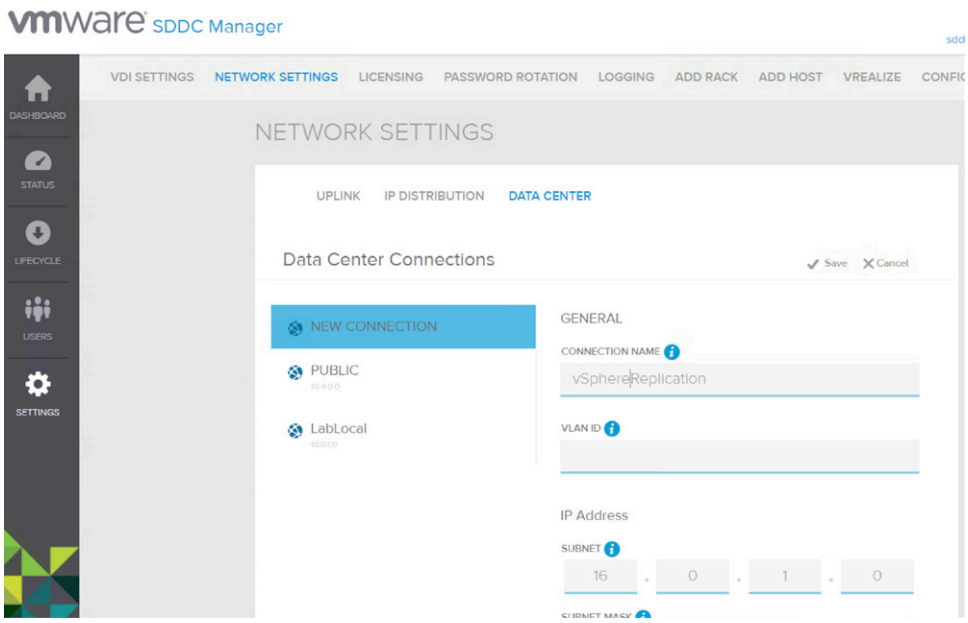
Installation

Cloud Foundation uses an architecture based on workload domains. By default, a single management workload domain is created for all Cloud Foundation management components. In addition, virtual infrastructure (VI) workload domains can be created for application workloads to maintain separation. When installing the vSphere Replication appliance, know in advance where application workloads will be run.

For a Cloud Foundation single-rack consolidated workload domain, the vSphere Replication appliance is installed in the management domain. This white paper explains how to install it. The same process can be followed for configuring a VI workload domain.

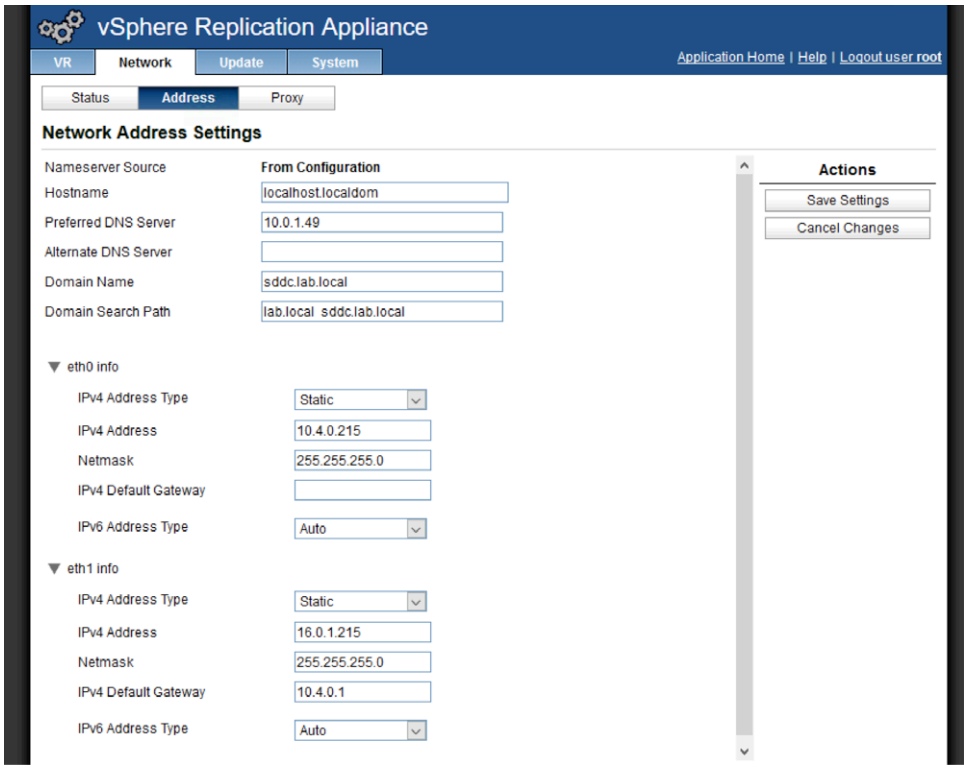
Migration – Target Site

Begin by creating a VLAN in the SDDC Manager for the vSphere Replication appliance.



After this has completed, this vSphere Replication VLAN will be available to all ESXi hosts.

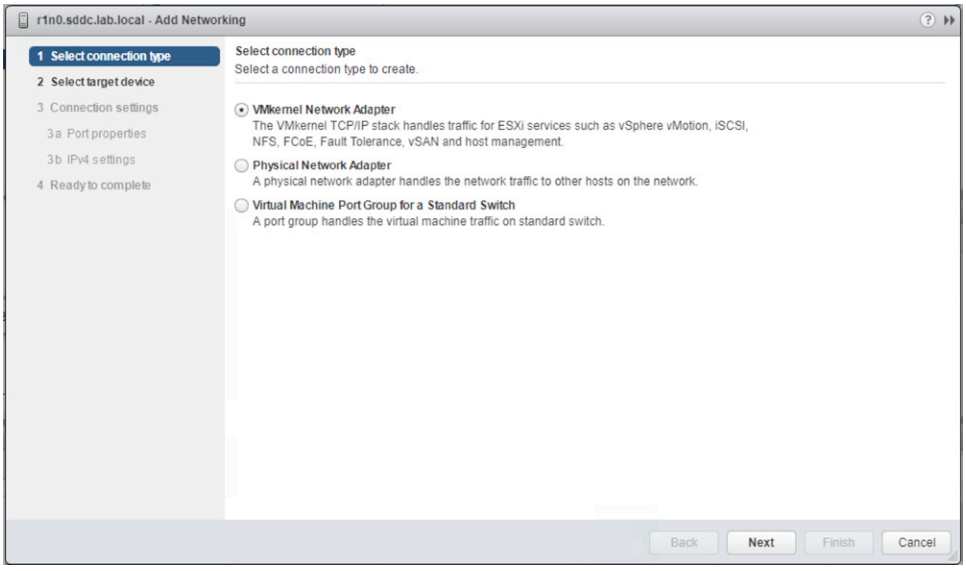
Install the vSphere Replication appliance on the Cloud Foundation instance with the default settings outlined in vSphere Replication documentation. After completing the appliance installation, power it on once to verify that it has configured its network adapter. Then power off the appliance and add a second virtual network adapter to it, connecting the second adapter to the vSphere Replication port group. Power it on again and proceed to the appliance management interface at https://<appliancename>:5480. Configure the IP on the second network adapter in the appliance. Provide an IP address for the vSphere Replication port group. Configure the default gateway for the appliance.



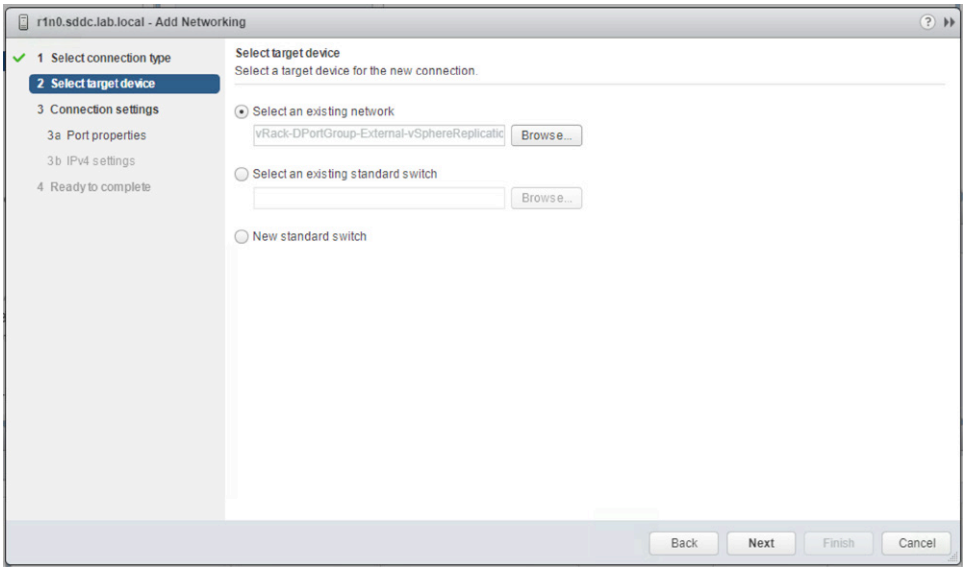
Next, configure the VMkernel adapters for the Cloud Foundation site to receive vSphere Replication traffic from the legacy environment.

Select the ESXi hosts to be used for the vSphere Replication appliance. Navigate to *Configure > VMkernel adapters*. Click to add a **VMkernel Network Adapter**. Follow the prompts from the wizard.

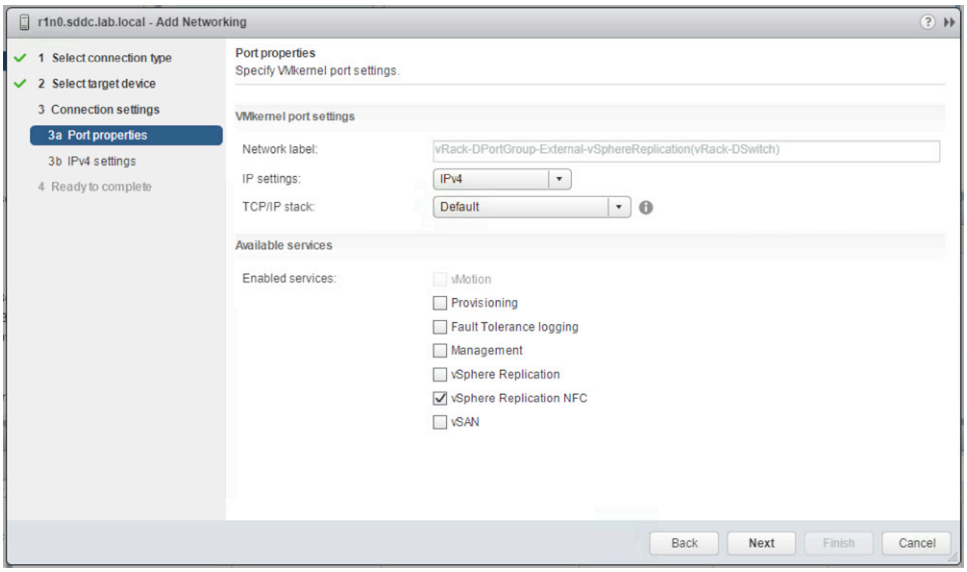
Use the defaults. Click **Next**.



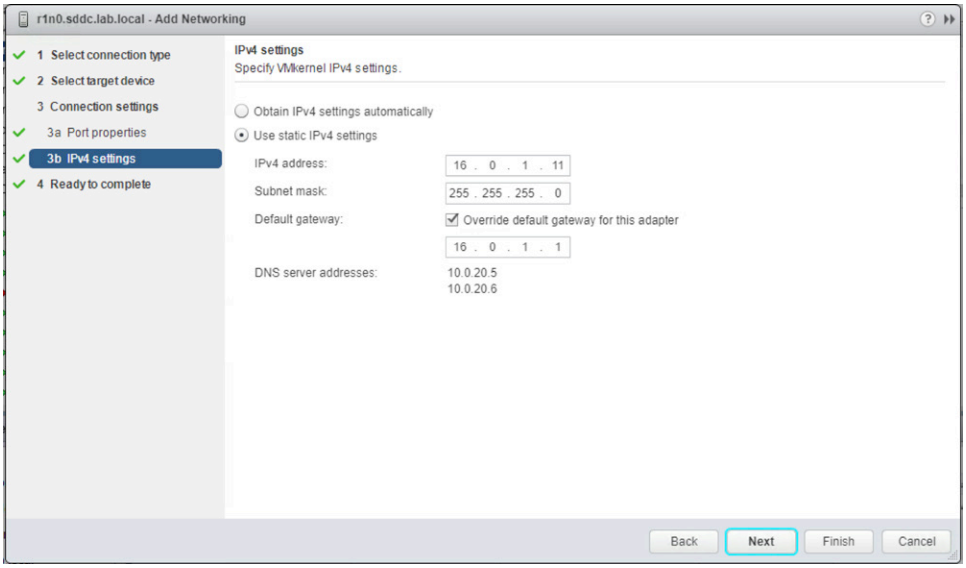
Select the newly created port group for the vSphere Replication appliance. Click **Next**.



This is used to receive vSphere Replication traffic in the Cloud Foundation site. Select **vSphere Replication NFC**.



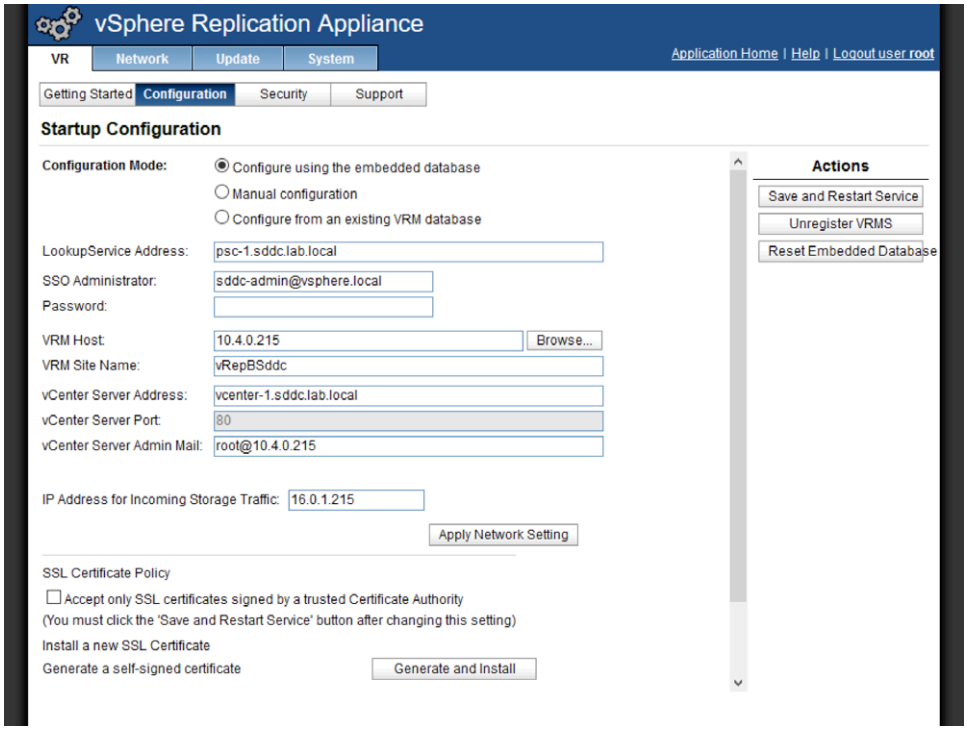
Set the IP address and click **Next**. Click **Finish**.



Complete this process for all ESXi hosts in Cloud Foundation that will be used as a vSphere Replication target.

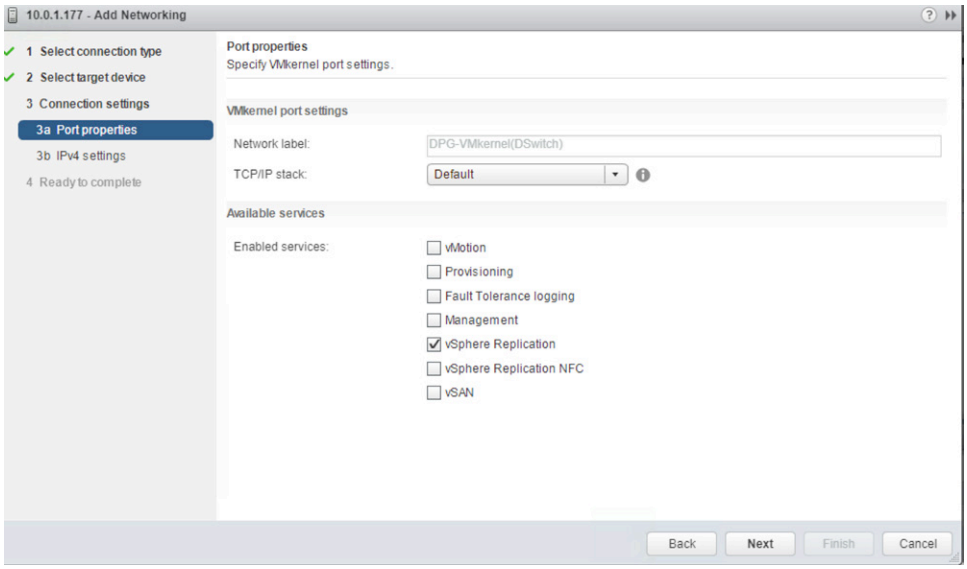
To finish the installation of the vSphere Replication appliance, return to its web interface and complete the **Configuration** page. Be sure to set the **IP address for Incoming Storage Traffic** to the IP you have configured for the second network adapter on this appliance.

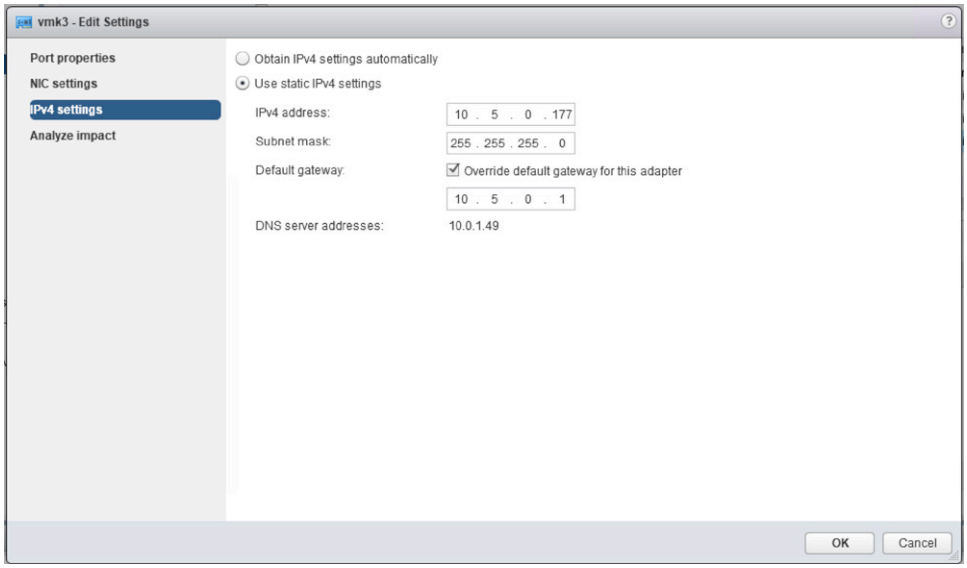
After filling out the required information, click **Save and Restart Service**. Installation in the Cloud Foundation site as the vSphere Replication target is now complete.



Migration – Source Site

Next, configure similar settings on the source site legacy ESXi hosts. There is one minor difference: The source site requires that the VMkernel adapter be set up to **send** vSphere Replication traffic with the setting shown in the following screenshots. Select **vSphere Replication** under **Enabled services**.





As shown in this screenshot, the default gateway for vSphere Replication traffic is set in the source site. This is required to force network traffic to use this gateway for vSphere Replication traffic. Without this setting, the default gateway of the ESXi host will be used.

NOTE: This default gateway setting is available only on vSphere 6.5 and later. For vSphere 6.0 legacy environments, a static route can be created using ESXCLI.

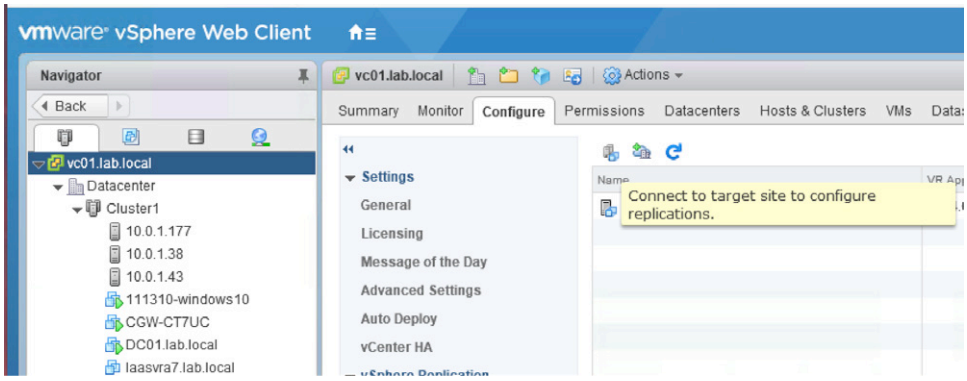
With ESXi hosts prepared in the source site, the vSphere Replication appliance can now be installed by following vSphere Replication documentation. The source site does not require a second network adapter because that is needed only for incoming traffic. All outbound vSphere Replication traffic originates from the ESXi host. After installation, complete configuration of the vSphere Replication appliance from the management web interface.

Configuration

With the appliances installed and configured in source and target sites, we now proceed to connect the two.

From the legacy source vCenter Server instance, navigate to *vCenter > Configure > vSphere Replication > Target Sites.*

Add the target Cloud Foundation site.



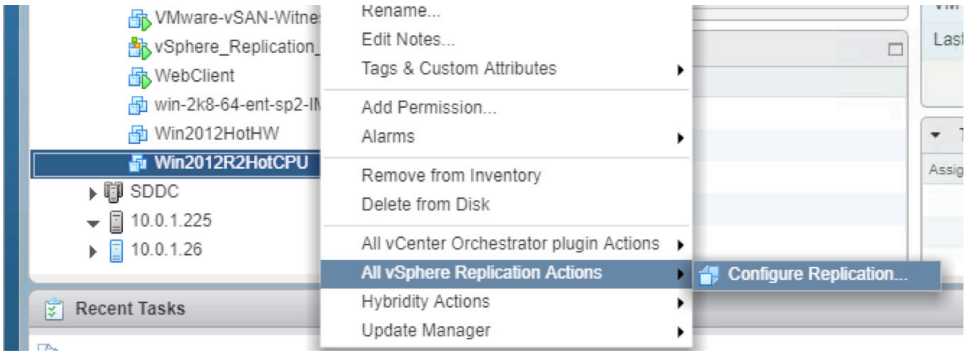
NOTE: Ensure that the DNS name for each site is resolvable from each site.

With the two sites now connected, begin replication.

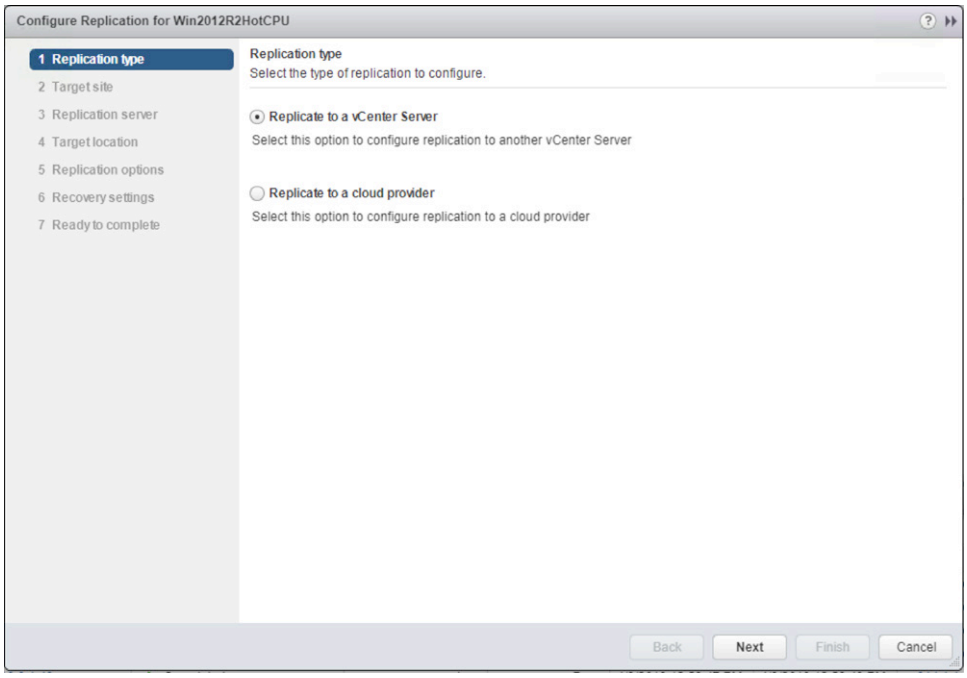
How to Use

After the vSphere Replication appliance has been installed, it is quite easy to use for migration.

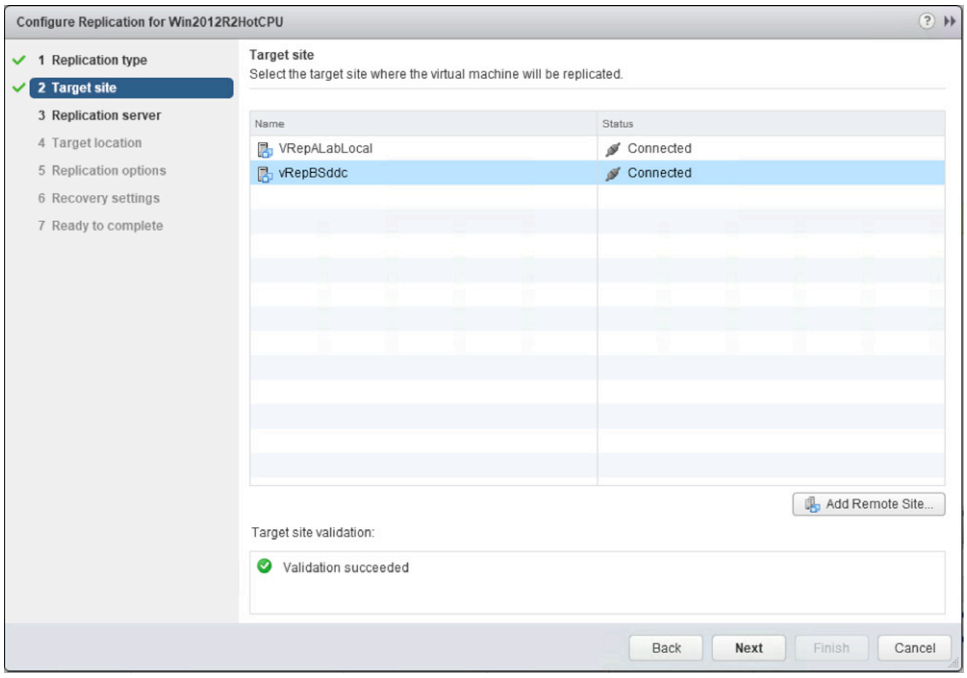
Right-click the VM to be migrated. Navigate to *All vSphere Replication Actions > Configure Replication*.



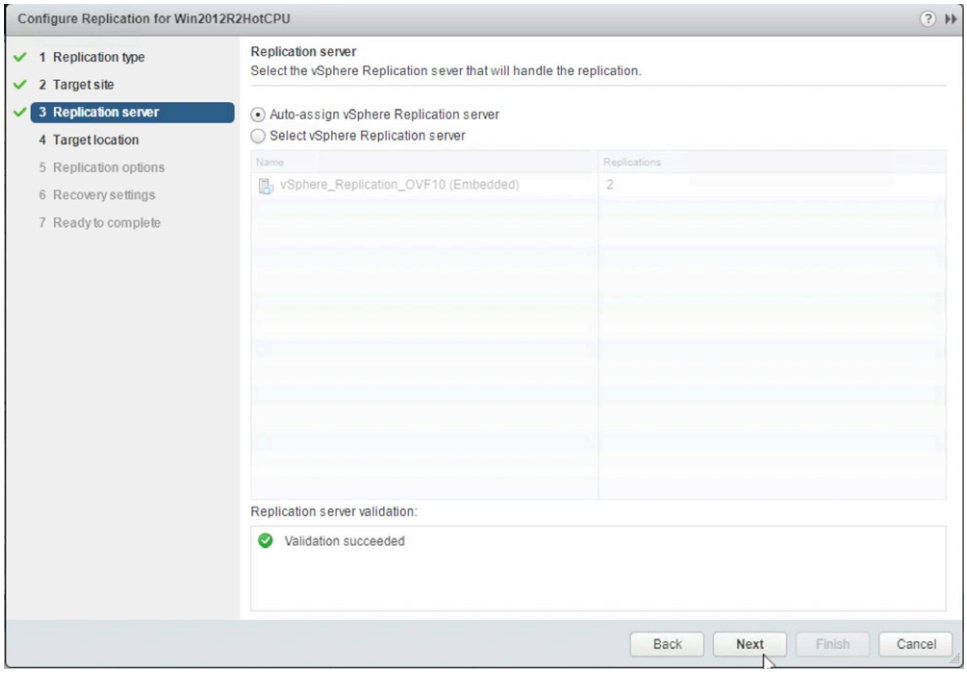
The wizard will appear for setting up replication of the guest VM. Select the **Replication type**.



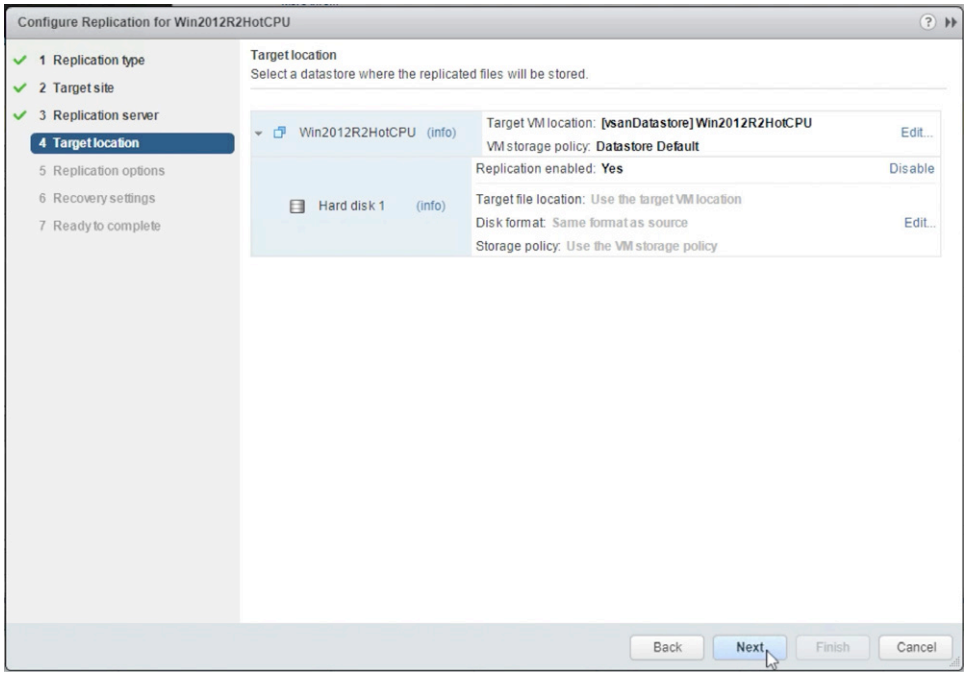
Select the **Target site** to replicate to.



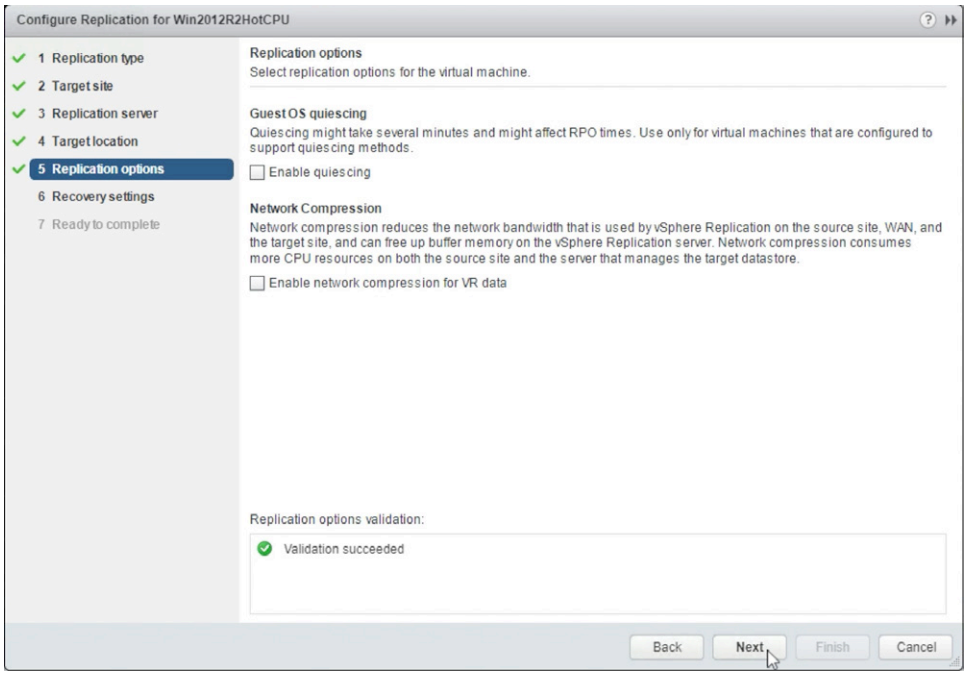
Select the **Replication server** to use in the target site.



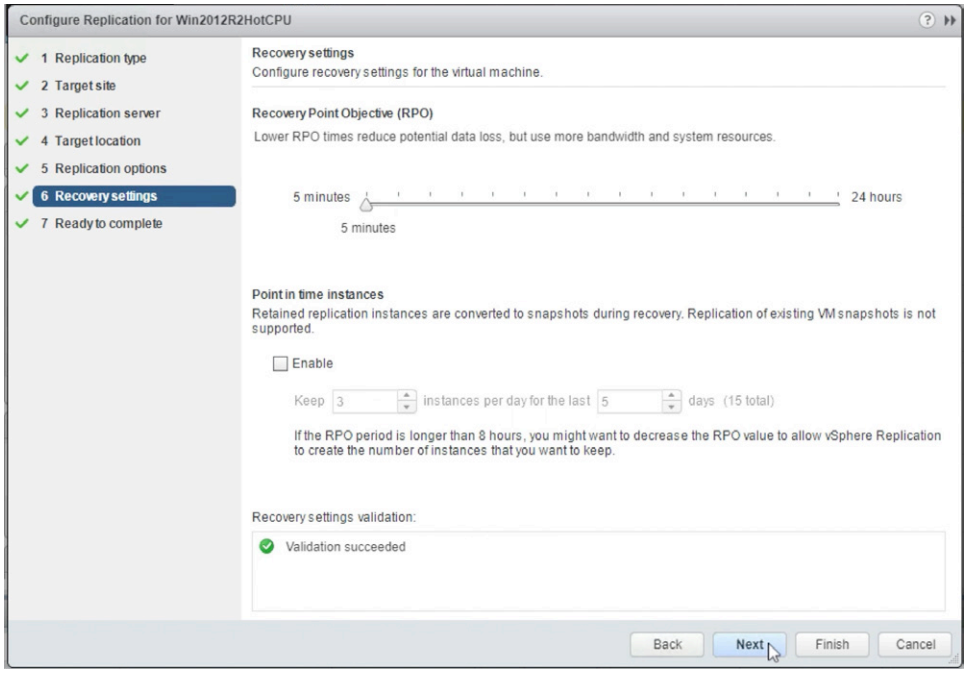
Select the **Target location**. For the Cloud Foundation site, select the vSAN datastore.



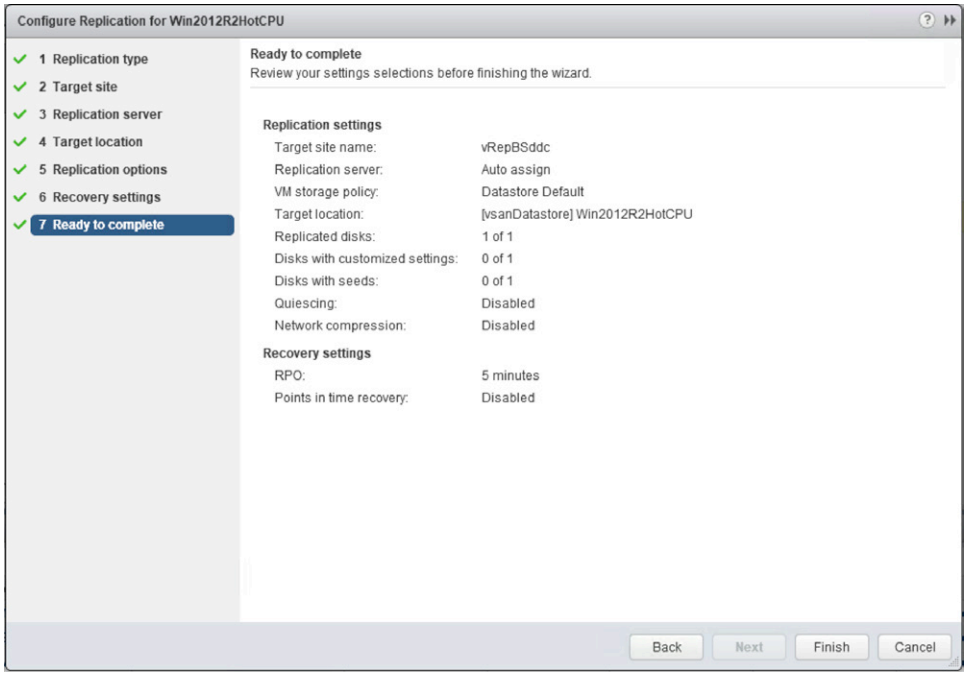
Select **Replication options**.



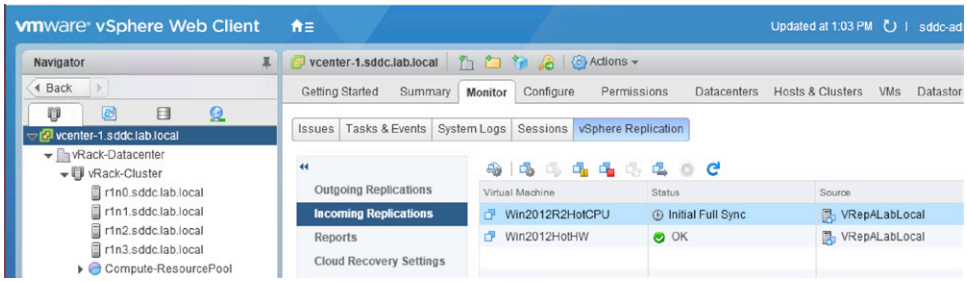
Set the **Recovery Point Objective (RPO)** for replication. If **Guest OS quiescing** was not previously selected, RPO can be set for as little as 5 minutes.



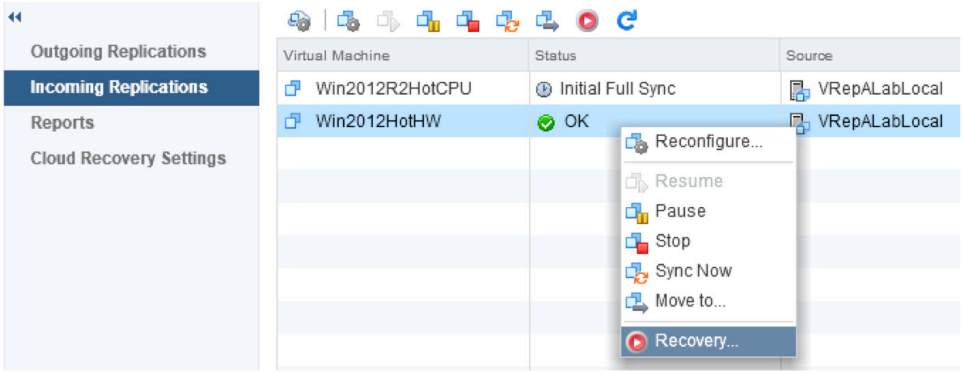
Review all **Replication settings** and **Recovery settings**.



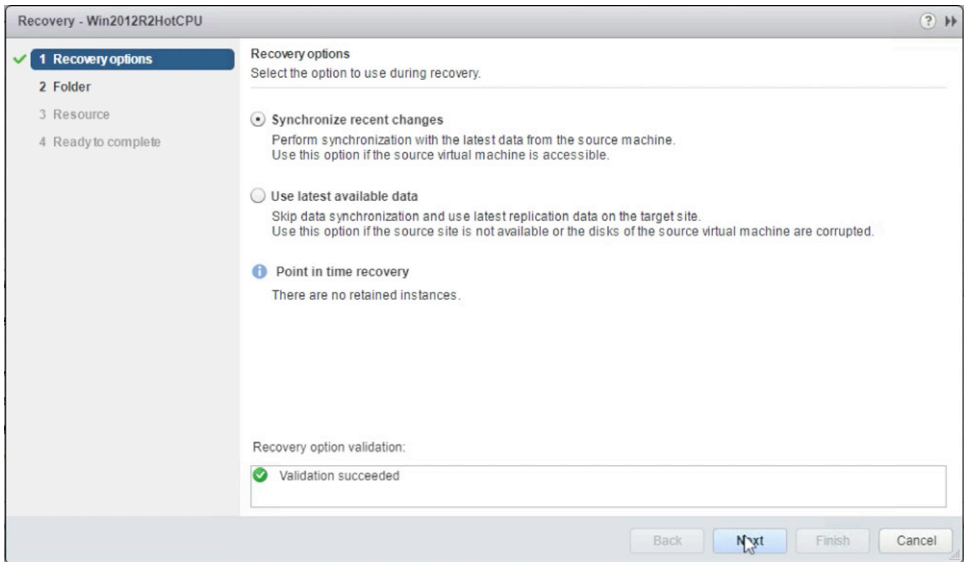
Go to the target vSphere Web Client instance and log in. Navigate to the vCenter Server instance in the navigation tree on the left. Navigate to *Monitor > vSphere Replication > Incoming Replications*.



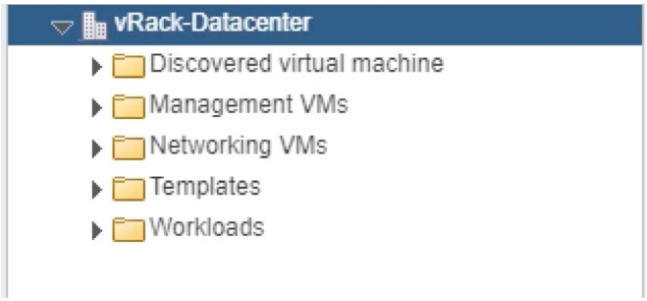
Replication has begun its **Initial Full Sync**. When the sync has completed, begin the migration process: Power off the guest VM. Click **Recovery**.



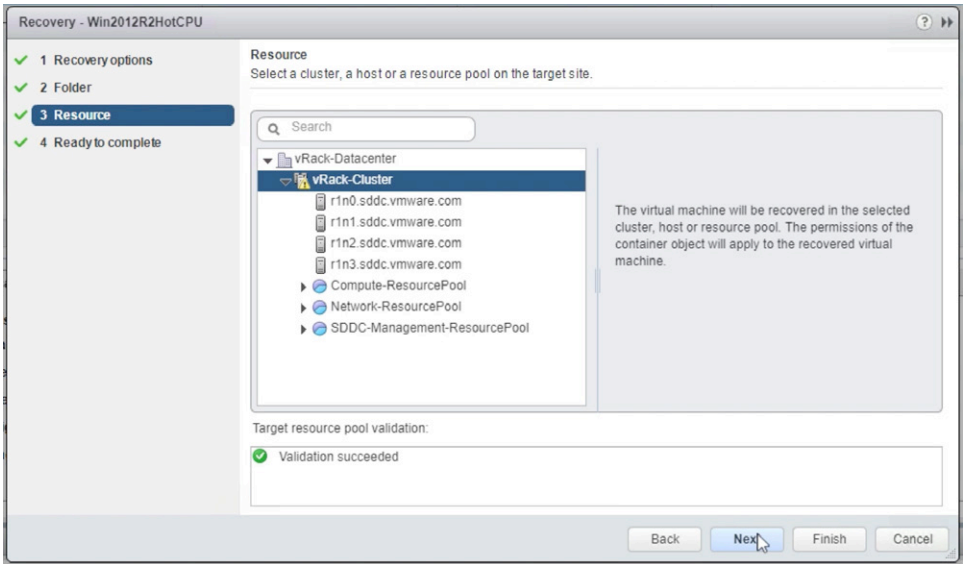
The recovery wizard appears. Work through the process of migrating the VM to the target site. Select the default to **Synchronize recent changes** since the last replication. Click **Next**.



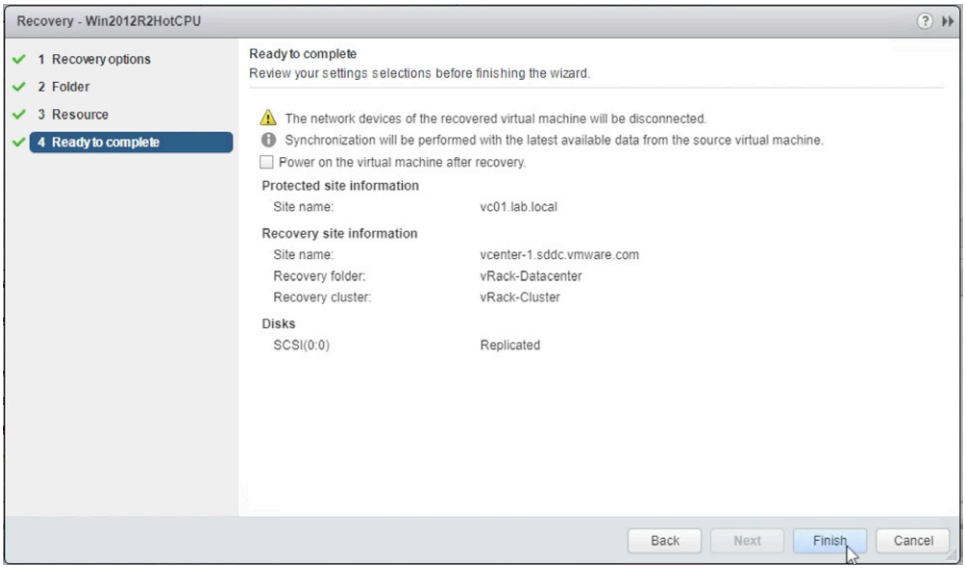
Select the target folder destination for the VM.



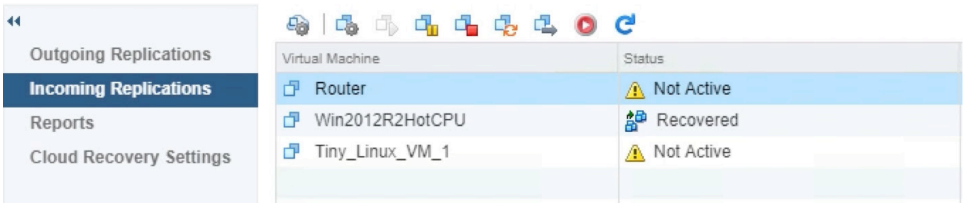
Select the **cluster** or **resource pool** in the target site



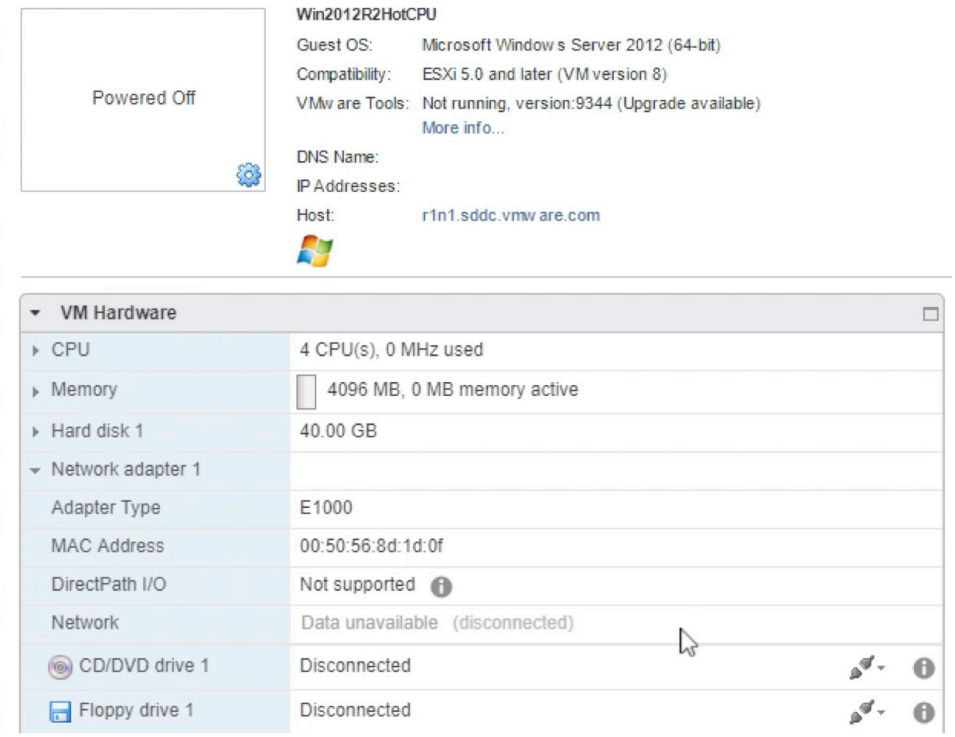
Review all selections. Click **Finish**.



After the final sync has completed, the VM will be registered with the target vCenter Server instance. Continue to configure the network settings for the target site.



The recovered VM has no connected network. Select the port group to use in the Cloud Foundation site.



After selecting the port group assignment, power on the VM. Migration to the Cloud Foundation site is now complete.

Summary

Using vSphere Replication as a migration tool is a very time-consuming process. There are no bulk migration tools built into the vSphere Replication appliance. It is a good option for moving only a small number of VMs. This option supports only cold migrations.

NOTE: VMware Site Recovery Manager™ is compatible with vSphere Replication and can enable bulk cold migration of VMs. Site Recovery Manager can be used with vSphere Replication to migrate VMs to a Cloud Foundation site.

Using Third-Party NAS Storage as Cold Migration Intermediary

Overview

Cloud Foundation supports the addition of NAS storage attached to ESXi hosts for third-party storage. After this storage has been installed and configured for both legacy vSphere and Cloud Foundation environments, it provides an easy path to migrate VM workloads. This method enables only cold migration through the process described herein. NAS storage can be used in conjunction with other live migration strategies presented in this white paper. It also can be used when migrating with the Fling or API. Doing so, time is saved by not having to migrate the storage and compute resources.

Architecture

The architecture for this migration process is straightforward and requires that the NAS storage be connected to both a legacy vSphere environment and a Cloud Foundation instance. An administrator must have vSphere access to both environments, as depicted in Figure 10.

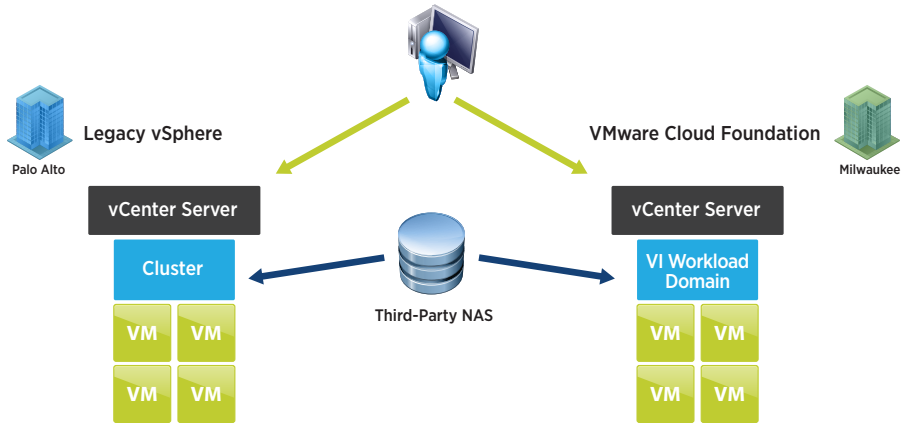


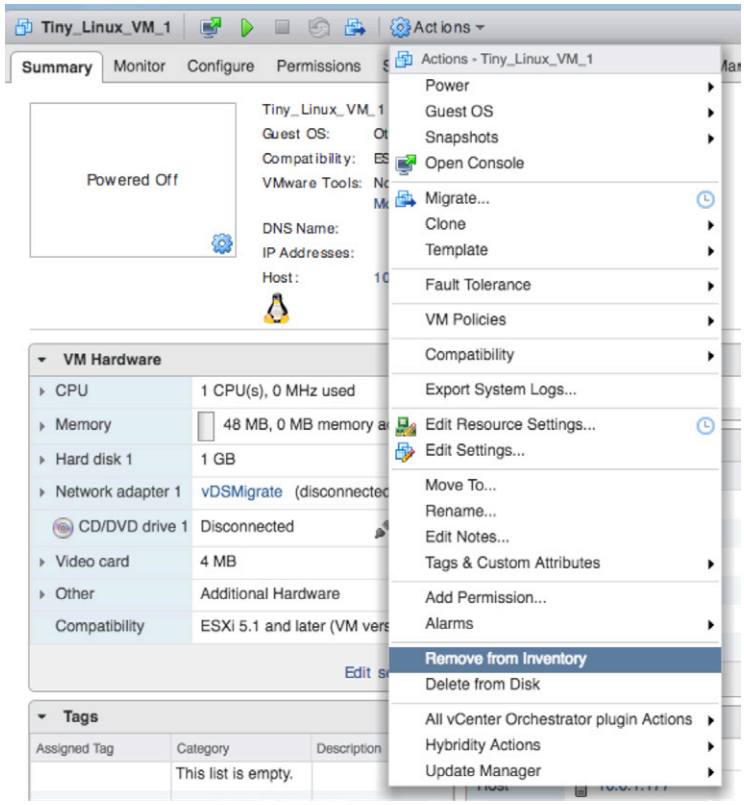
Figure 10. Architecture Overview – Migration Process

Installation

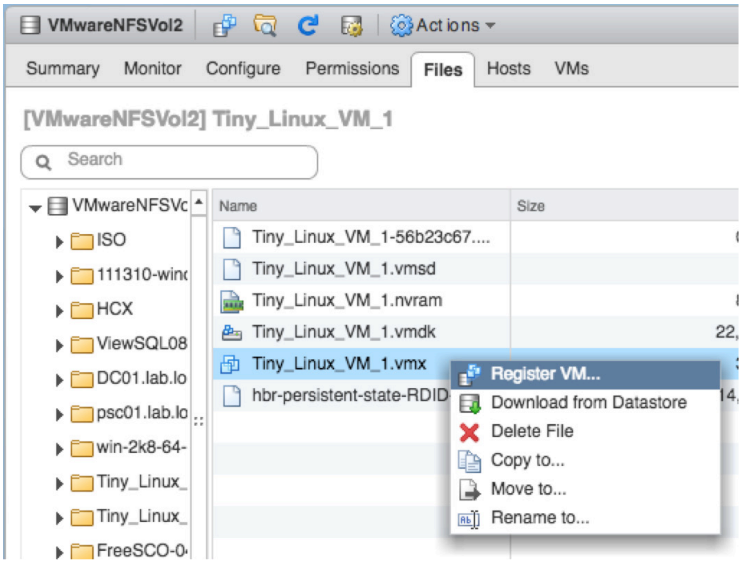
Refer to this white paper on how to install NAS storage into a Cloud Foundation environment.

Migration

Migration for this process begins with verifying the VM storage folder location. Make sure that all files associated with the VM are located on the NAS storage. After verifying and noting the location of all the VM files, power off the VM and unregister it from the legacy vCenter Server instance. Use the vSphere Web Client instance and click **Actions**. Choose **Remove from Inventory**.



From the Cloud Foundation vSphere Web Client instance, browse the NAS storage and find where the VM files are located. Select and right-click the **.vmx** file. Choose **Register VM**.



After the VM has been successfully registered to the Cloud Foundation vCenter Server instance, power on the VM.

Summary

This is a straightforward but manual migration process. There is little downtime when migrating a VM using this method. After the VM has powered on, use vSphere Storage vMotion migration to move the VM to the vSAN storage in the Cloud Foundation site.

NSX Hybrid Connect

Overview

NSX Hybrid Connect abstracts on-premises and cloud resources and presents them to applications as one continuous hybrid cloud. It provides high-performance, secure, and optimized multisite interconnects. The abstraction and interconnects create a highly secure infrastructure hybridity tunnel. With this hybridity tunnel, NSX Hybrid Connect facilitates secure and seamless application mobility and disaster recovery across on-premises vSphere platforms and VMware clouds.

NSX Hybrid Connect is the most feature-rich tool currently available for Cloud Foundation workload mobility. This document explains how to install, configure, and use NSX Hybrid Connect with a Cloud Foundation site when connecting to a legacy vSphere environment.

Architecture

The NSX Hybrid Connect process begins with two vSphere sites, a source and a target. Each site has its own requirements for software installation. The target site requires the use of NSX; for this document, the target is a Cloud Foundation site. This site requires installation of the NSX Hybrid Connect Manager components.

The source site must also install the NSX Hybrid Connect Manager components. However, the installation package for this site is different from that of the target site. After the NSX Hybrid Connect target site has been installed and configured, a link will be provided to download the software components for the source site. NSX Hybrid Connect Manager does not require NSX but can be used in conjunction with it if NSX is available.

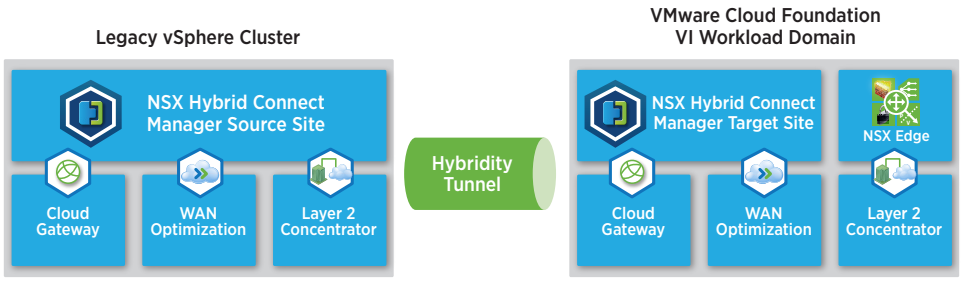


Figure 11. Architecture Overview – NSX Hybrid Connect

NSX Hybrid Connect comprises four appliances:

NSX Hybrid Connect Manager appliance

This appliance facilitates the management and control plane for NSX Hybrid Connect.

NSX Hybrid Connect Cloud Gateway appliance

This Cloud Gateway appliance is responsible for creating encrypted tunnels across enterprise sites for the vSphere vMotion traffic and the vSphere based replication traffic. The appliance makes it easy to connect the source and target sites and reduces the engineering time required to build a hybrid cloud infrastructure that enables workload mobility freedom.

WAN Optimization appliance

This high-performance appliance is built into NSX Hybrid Connect. The appliance provides data deduplication and compression. This improves the performance of the tunnel, creating a LAN-like experience.

Layer 2 Concentrator appliance

This appliance creates an L2 extension between vSphere environments, enabling workloads to maintain the same IP address during migration.

To create a hybridity tunnel between the Cloud Foundation site and the legacy vSphere site, first reserve three IP addresses within the Cloud Foundation infrastructure for installing three of the four NSX Hybrid Connect appliances. The WAN Optimization appliance does not require a reserved IP. The NSX Hybrid Connect Manager appliances must be network accessible to each other across both source and target sites. The remaining three NSX Hybrid Connect appliances must be installed with network adapters attached to the vSphere vMotion VLANs and management VLANs in both sites. With both sites installed and configured, the architecture will resemble that depicted in Figure 12.

NOTE: For the purposes of this white paper, it is assumed that both sites are available over a LAN connection and that there are no firewalls between them. If firewalls exist between the sites being connected, see the NSX Hybrid Connect documentation on the ports being used.

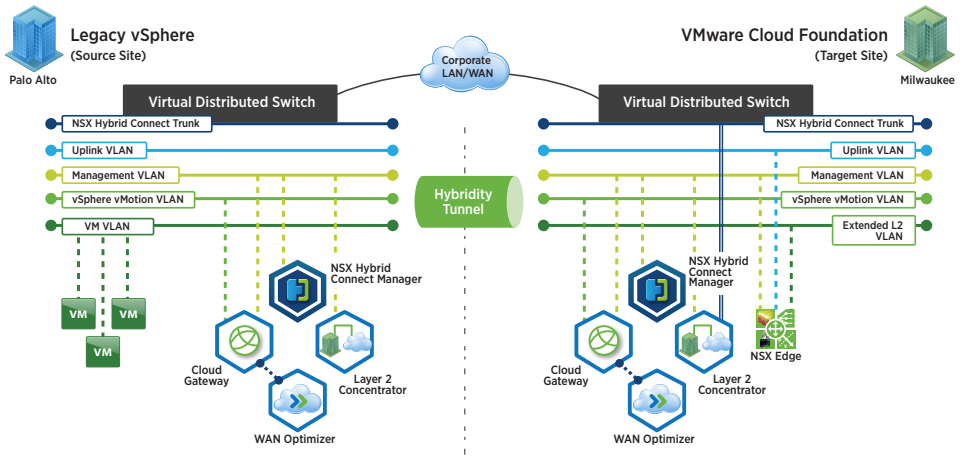


Figure 12. Architecture Overview – NSX Hybrid Connect

Installation – NSX Hybrid Connect Manager Target (Cloud Foundation Site)

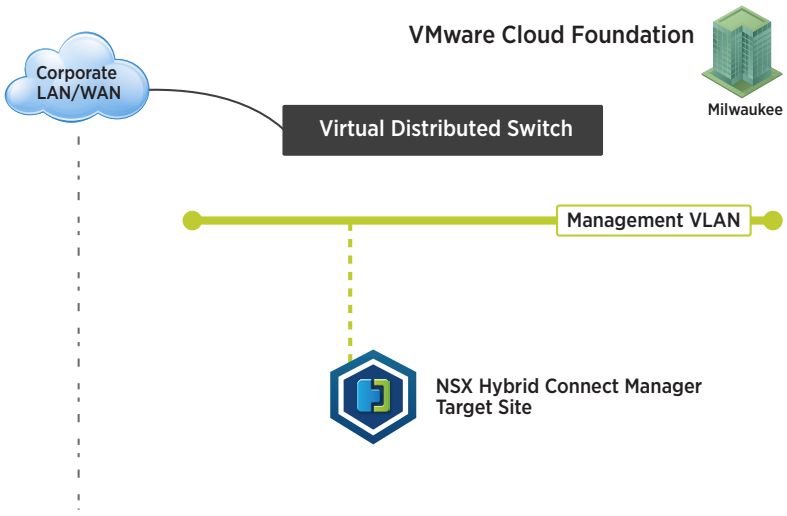
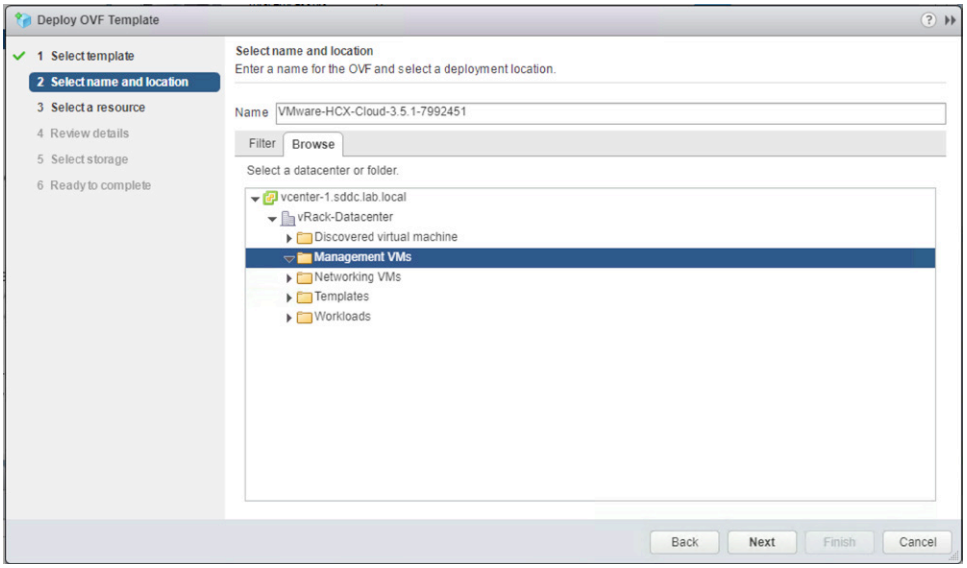


Figure 13. NSX Hybrid Connect Cloud Installation

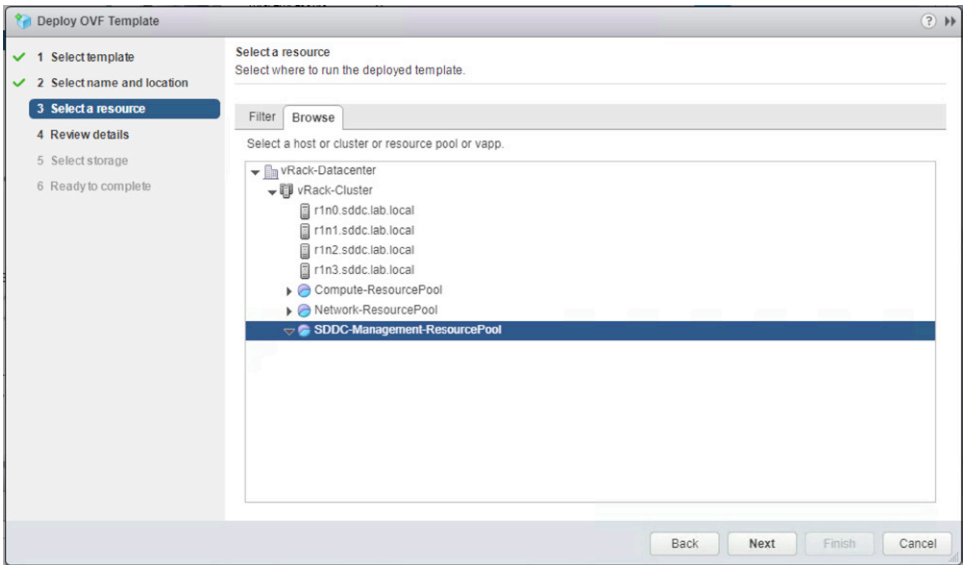
To deploy the NSX Hybrid Connect Manager target appliances in a target Cloud Foundation environment and configure the VLANs, begin by downloading the NSX Hybrid Connect Manager target Open Virtualization Appliance (OVA). Start the installation in the Cloud Foundation site as depicted in Figure 13.

First, determine where to install the NSX Hybrid Connect appliances in the Cloud Foundation site. If they are wanted, create any folders or resource groups now. In this document, we use the management folder and resource pool built into Cloud Foundation.

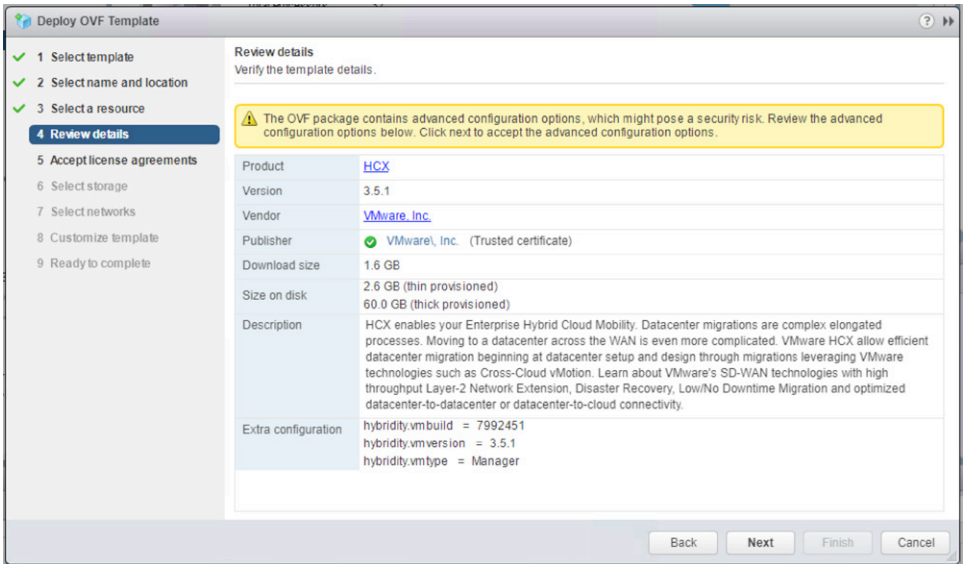
Log in to the management domain vCenter Server instance and install the OVA in the **Management VMs** folder.



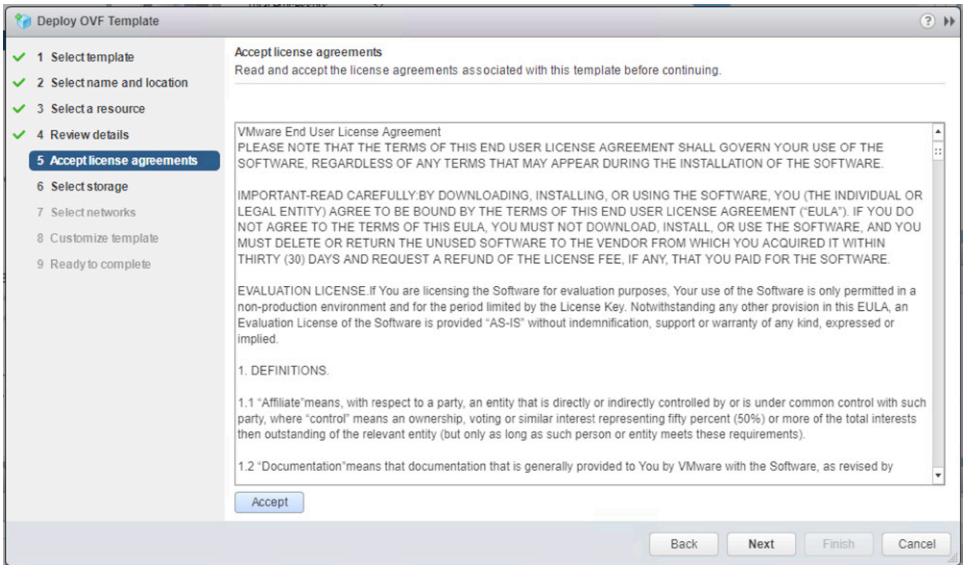
Select the **Management** resource pool.



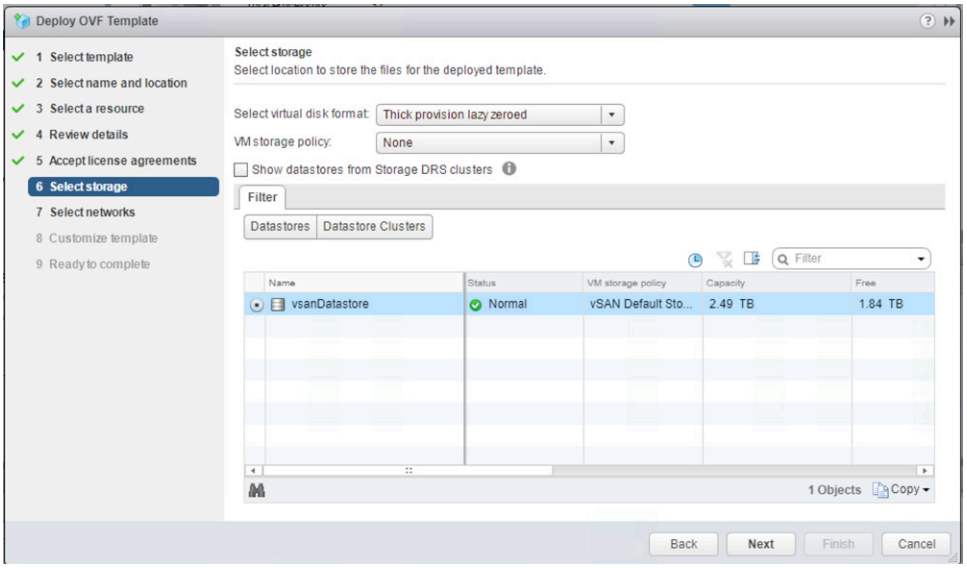
Click **Next**.



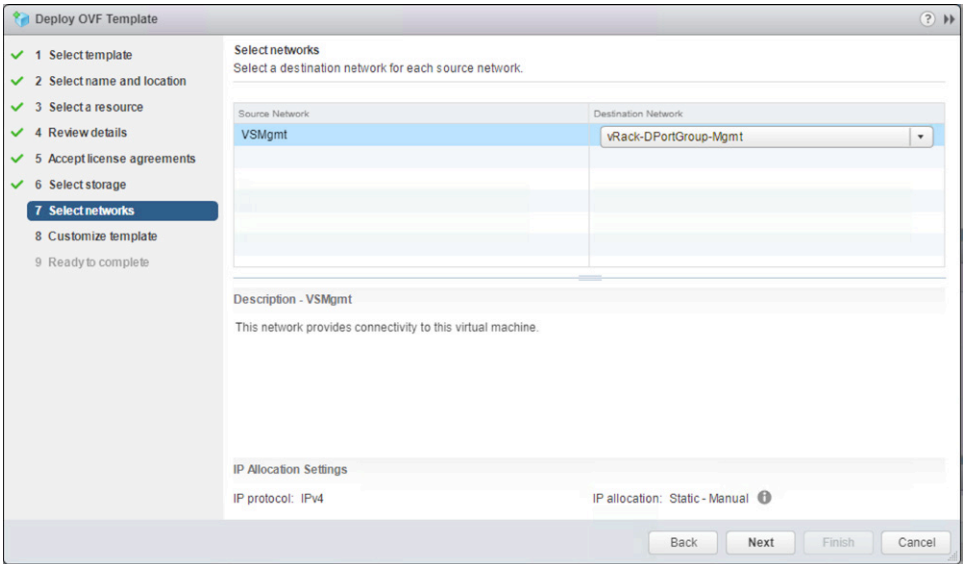
Accept the **VMware End User License Agreement** (EULA).



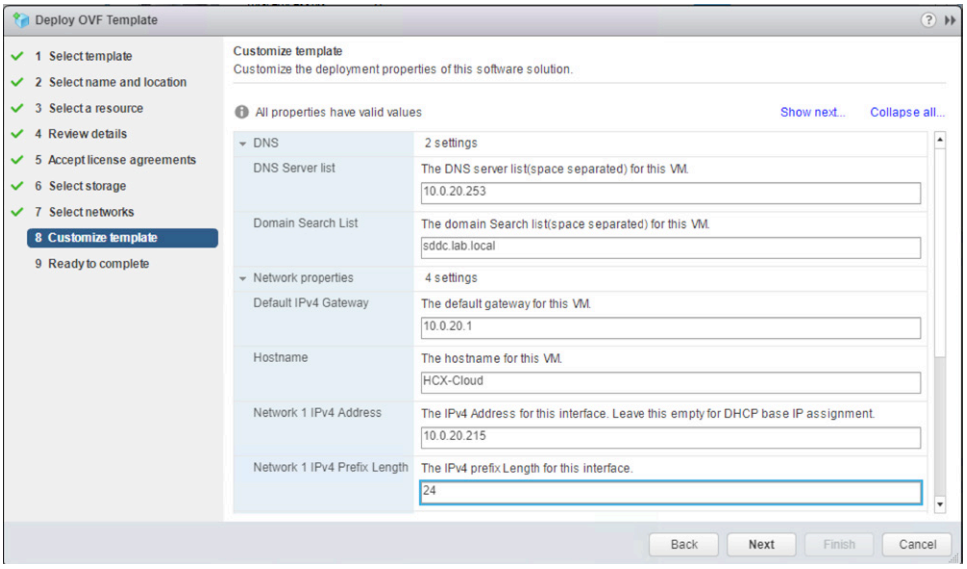
Select the Cloud Foundation **vSAN Datastore**.



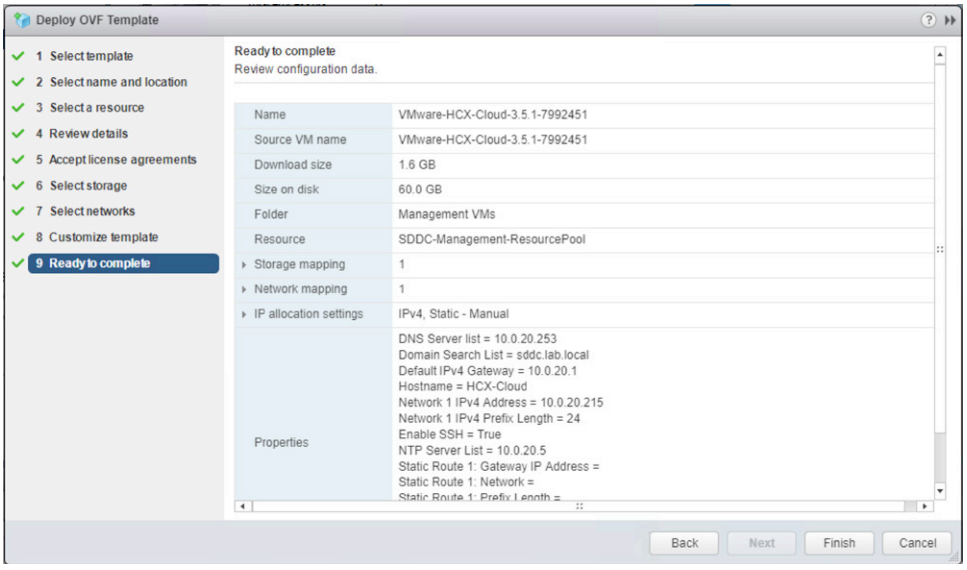
Select the port group where the NSX Hybrid Connect Manager instance is to reside.



Provide the IPs for the NSX Hybrid Connect management appliance.

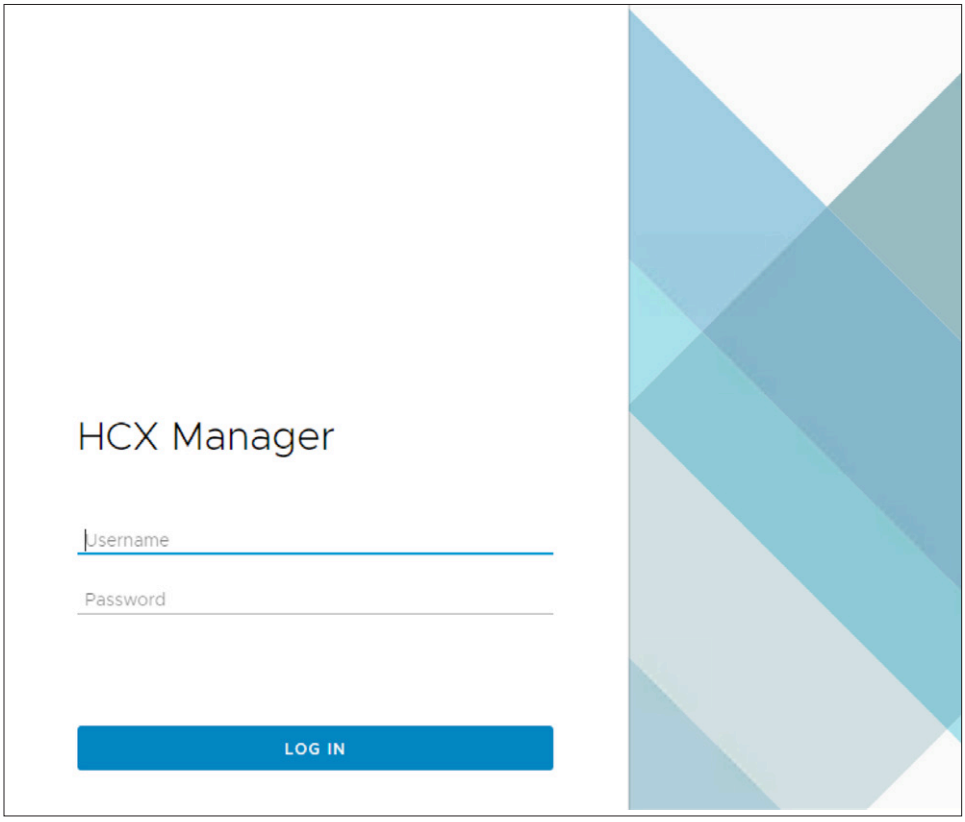


Review the details and complete the installation.

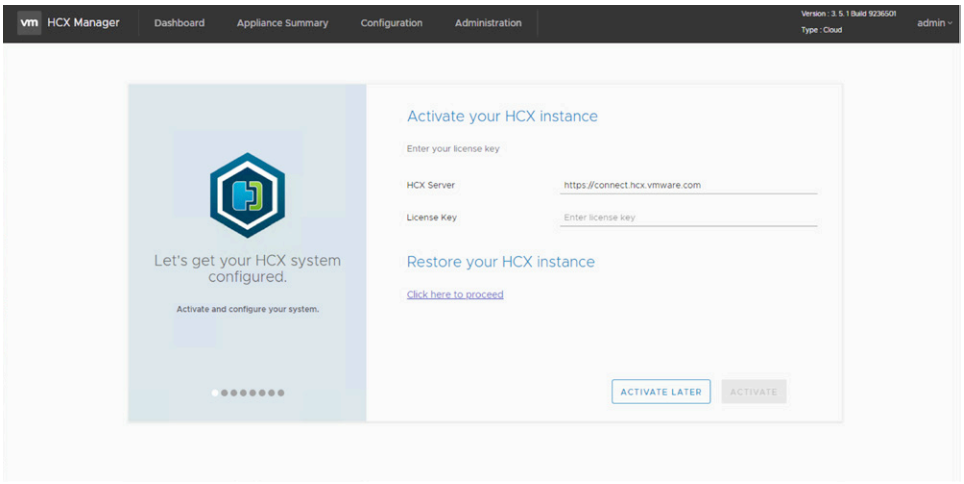


After installation of the OVA has been completed, power on the NSX Hybrid Connect Manager target site appliance.

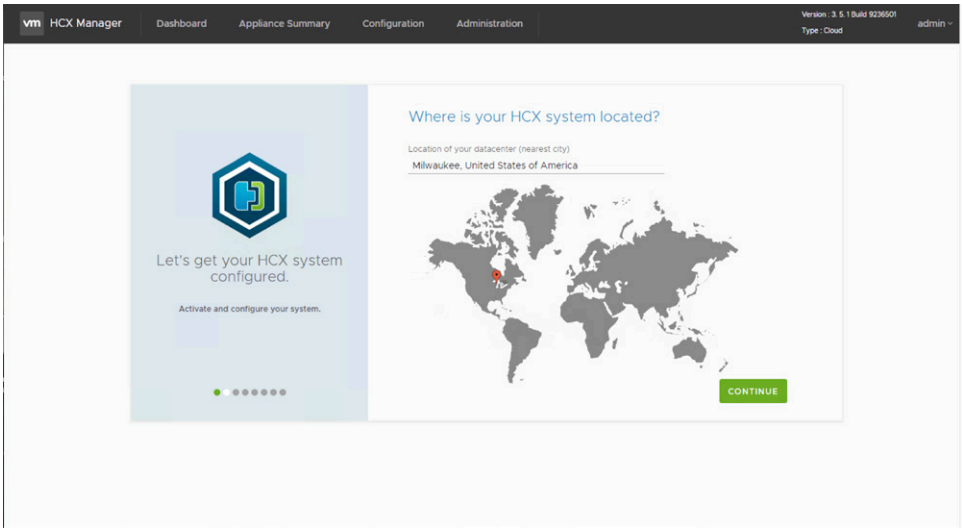
With the NSX Hybrid Connect Manager target site appliance installed, the next step is to register the appliance with the vCenter Server instance in the target site. To begin, log in to the appliance at https://<Hybrid Connect Manager target site >:9443 and enter the default username **Admin** and the password you set during installation of the OVA.



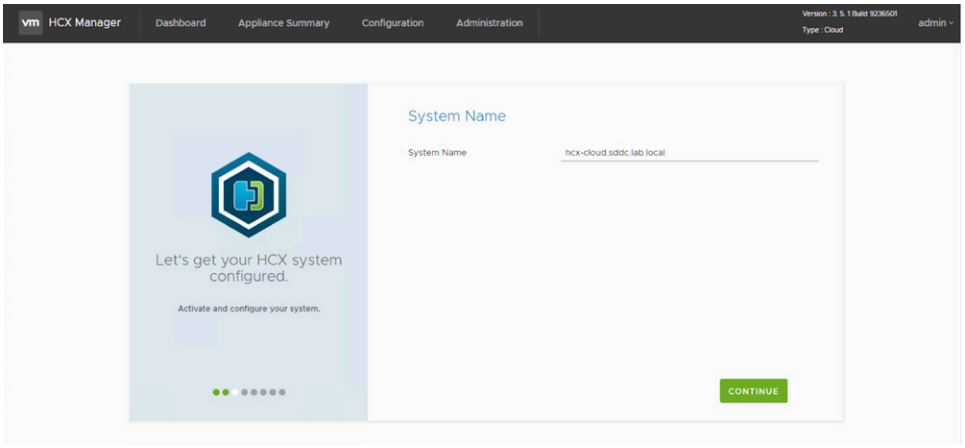
After login, the appliance will ask you to activate the target site instance. Enter the **License Key** and click **ACTIVATE**.



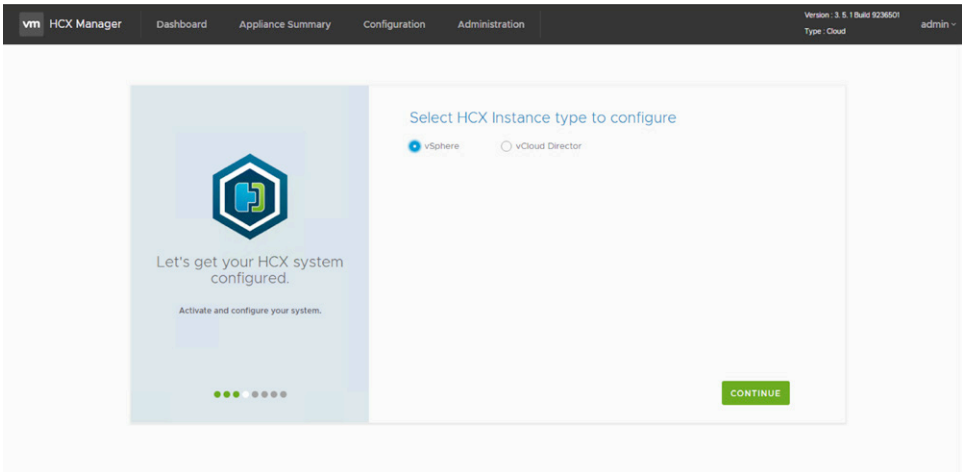
Set the cloud site geographic location.



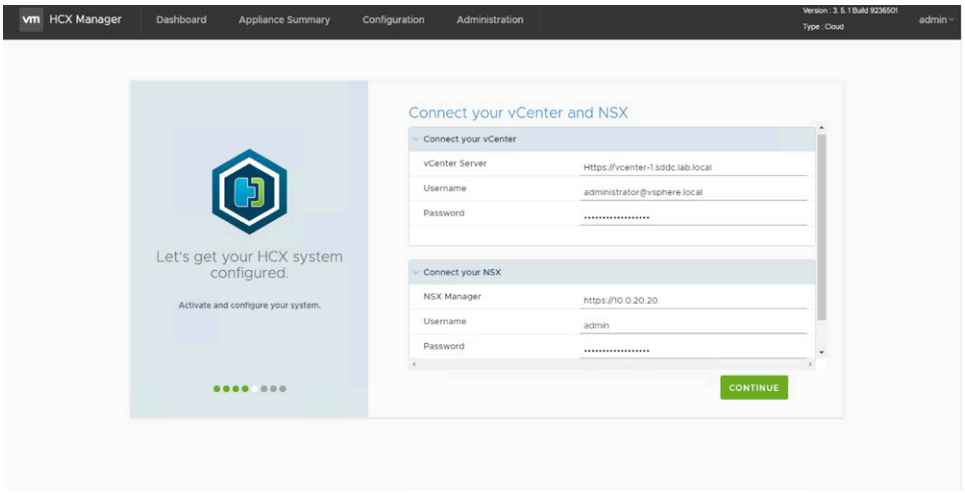
Enter the **System Name**.



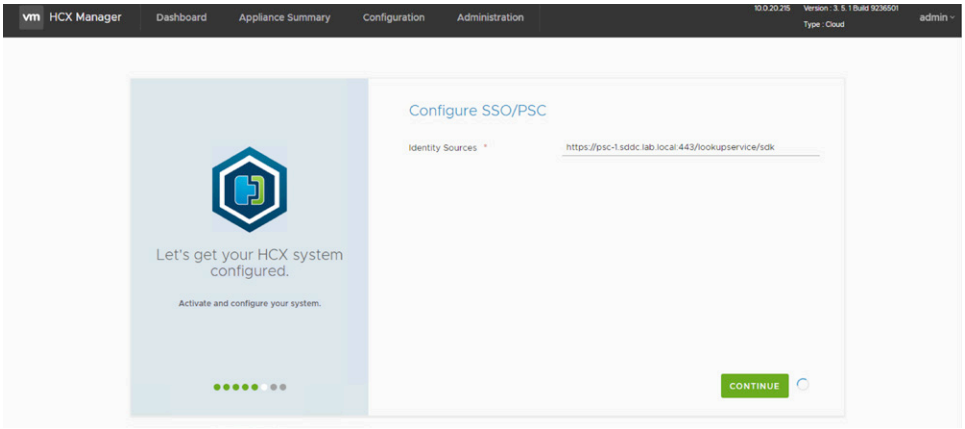
Select the vSphere installation option.



Configure the vCenter Server and NSX connection using the credentials from the target vSphere site.

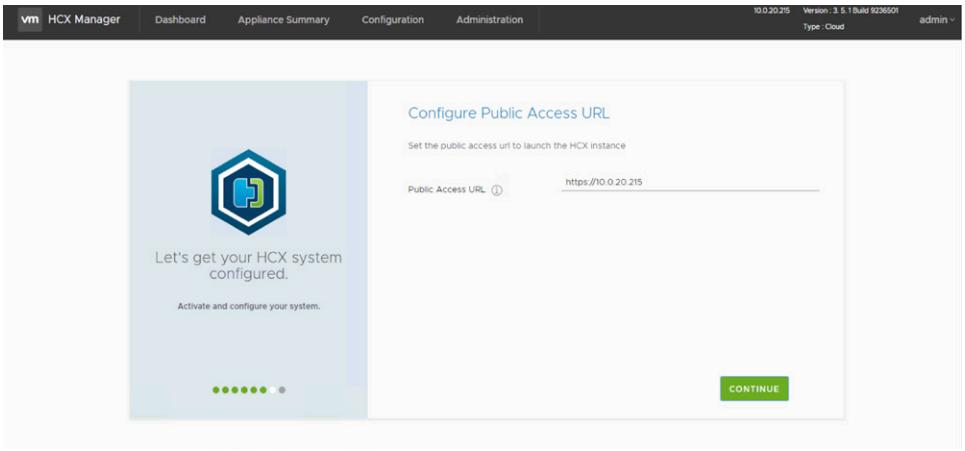


Enter the URL for the Platform Services Controller instance for the target site lookup service—example: https://<Target site PSC>:443/lookupservice/sdk.

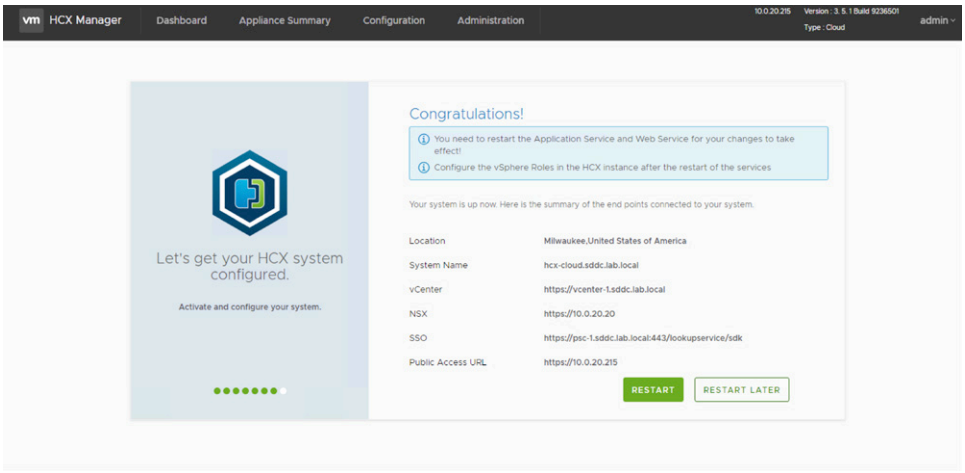


Enter the **Public Access URL** for the target site. This URL will be used later to complete the site pairing process.

NOTE: If this installation is not public Internet facing, an IP address can be used.



To complete the configuration, click **RESTART**.



The next step is to configure and install the remaining NSX Hybrid Connect appliance VMs in the NSX Hybrid Connect target site. This is referred to as the interconnect configuration. Figure 14 is a network diagram for reference. It shows each of the appliance VMs and which networks they are connected to.

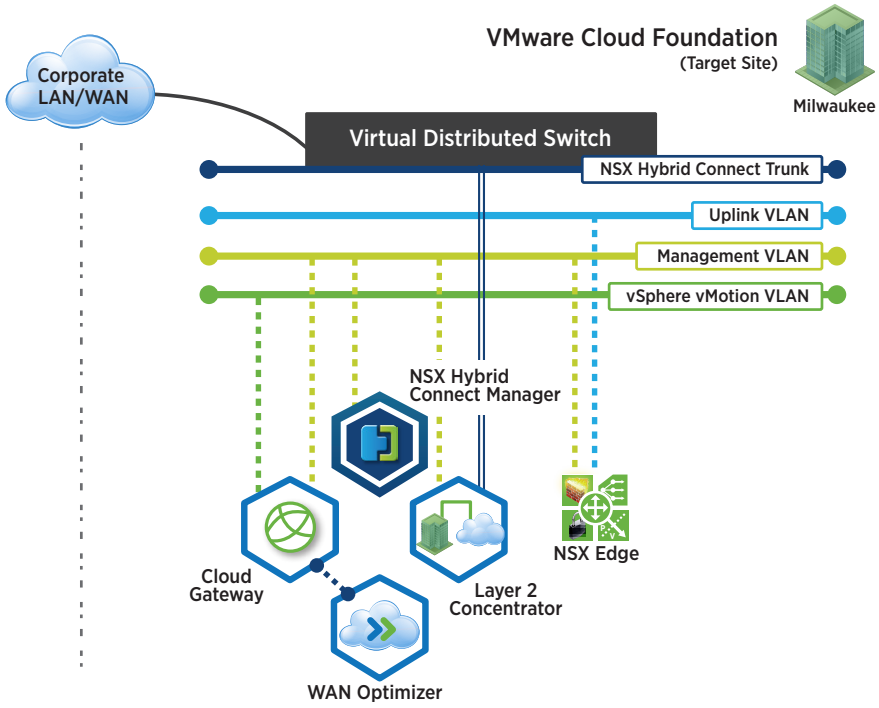
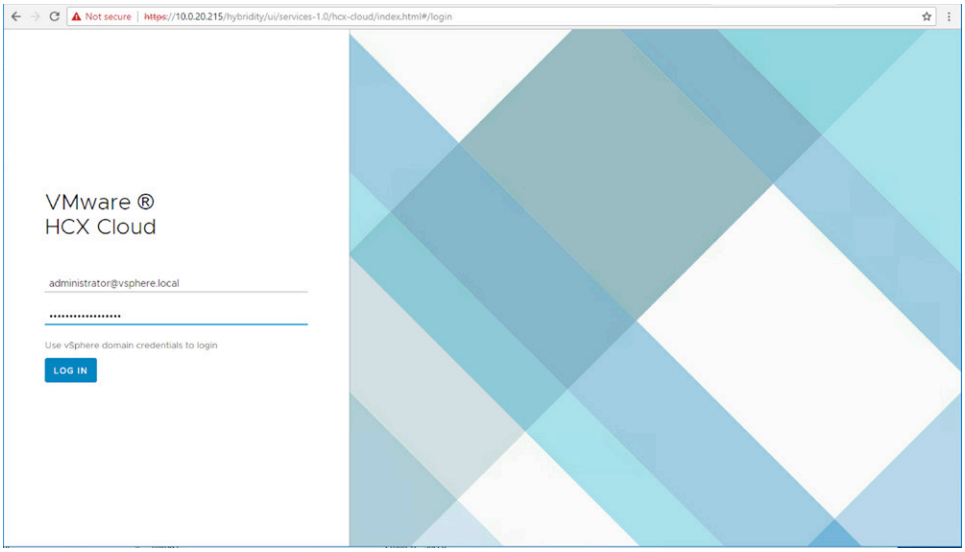
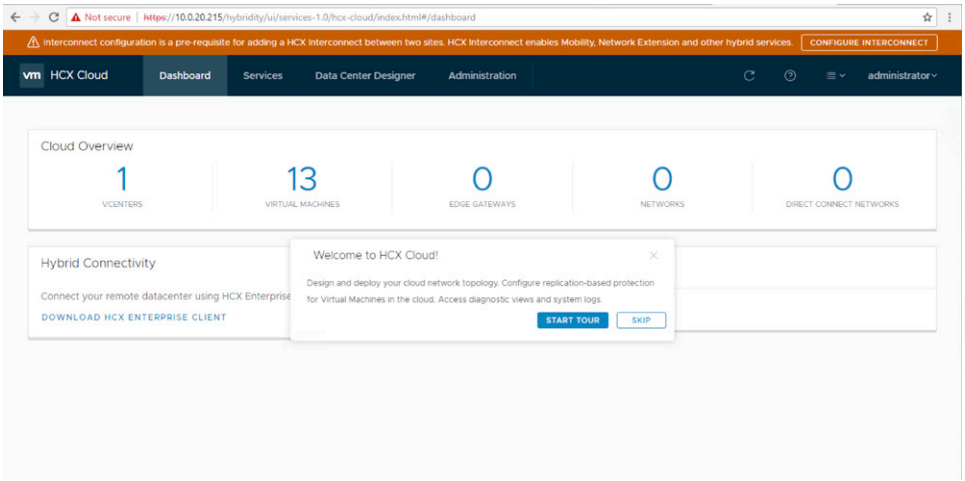


Figure 14. NSX Hybrid Connect Target Site Network Detail

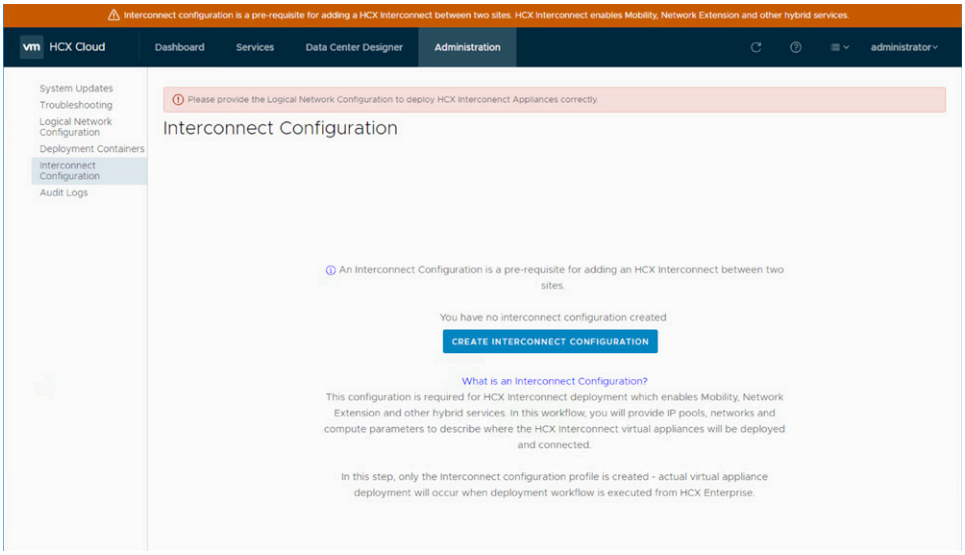
To begin the interconnect configuration, log in to https://<Hybrid Connect Manager> with your vSphere credentials.



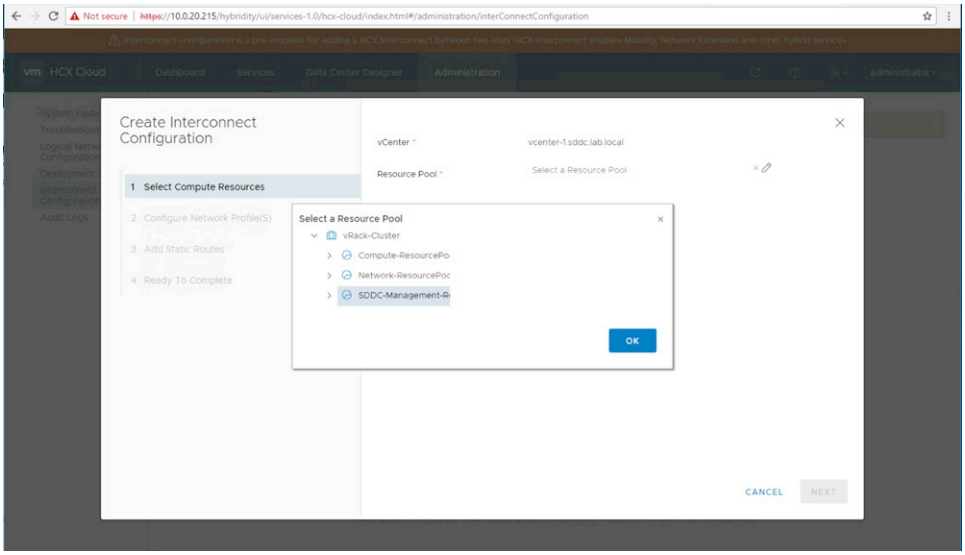
Upon login, the NSX Hybrid Connect Manager target dashboard appears. We see that the interconnect configuration must be completed. Click **CONFIGURE INTERCONNECT**.



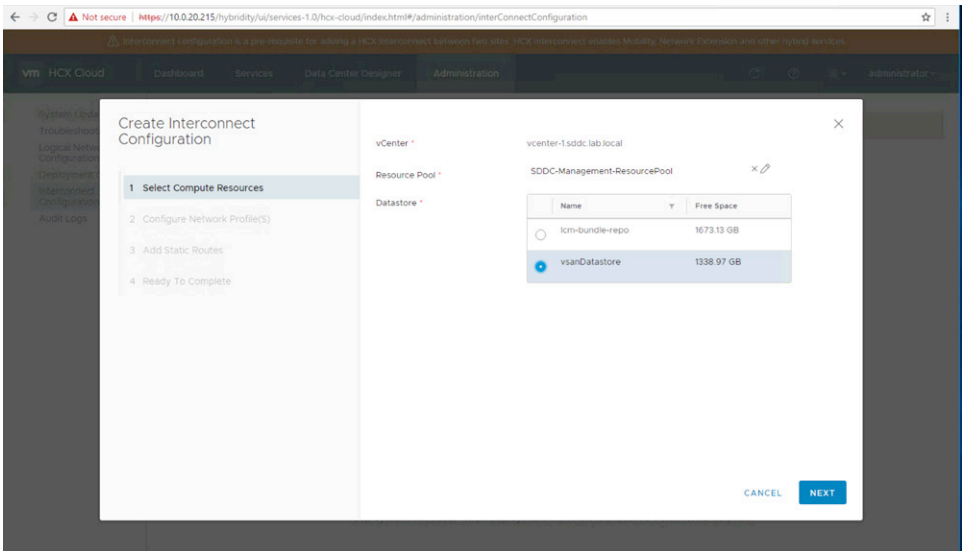
Click **CREATE INTERCONNECT CONFIGURATION**.



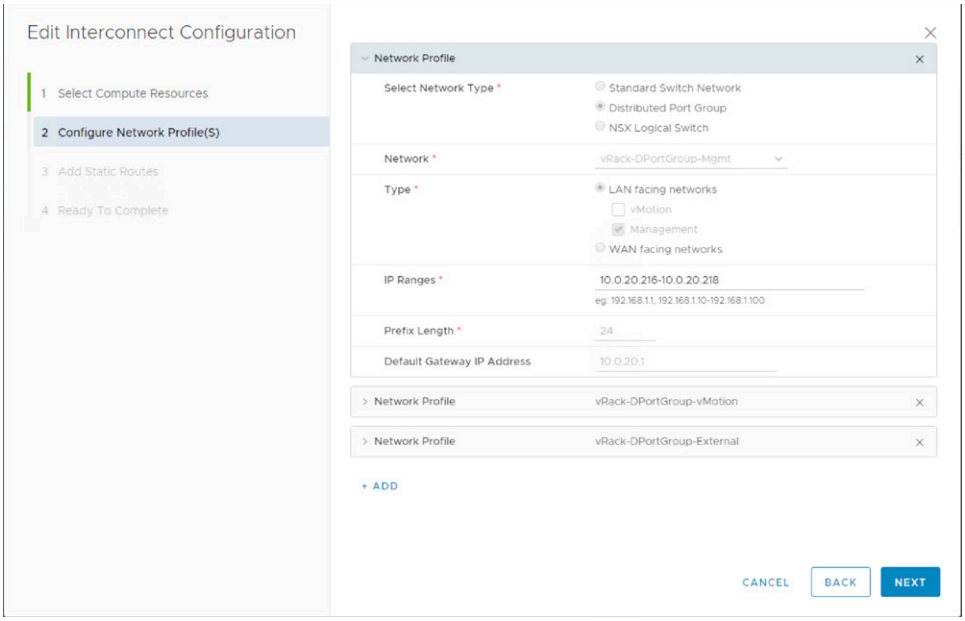
Select a Resource Pool into which to deploy the NSX Hybrid Connect appliances.



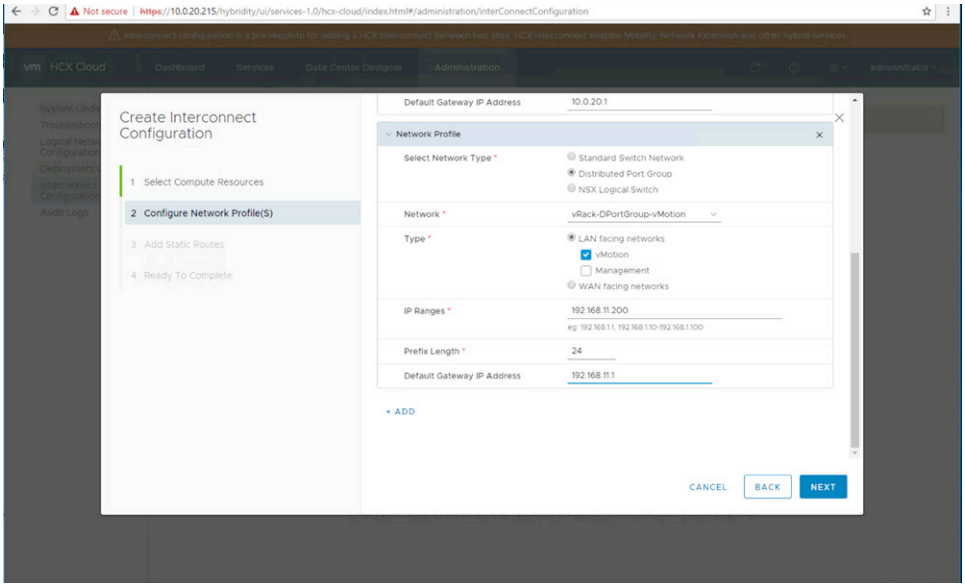
Select the vSAN datastore as the storage location of the NSX Hybrid Connect appliances.



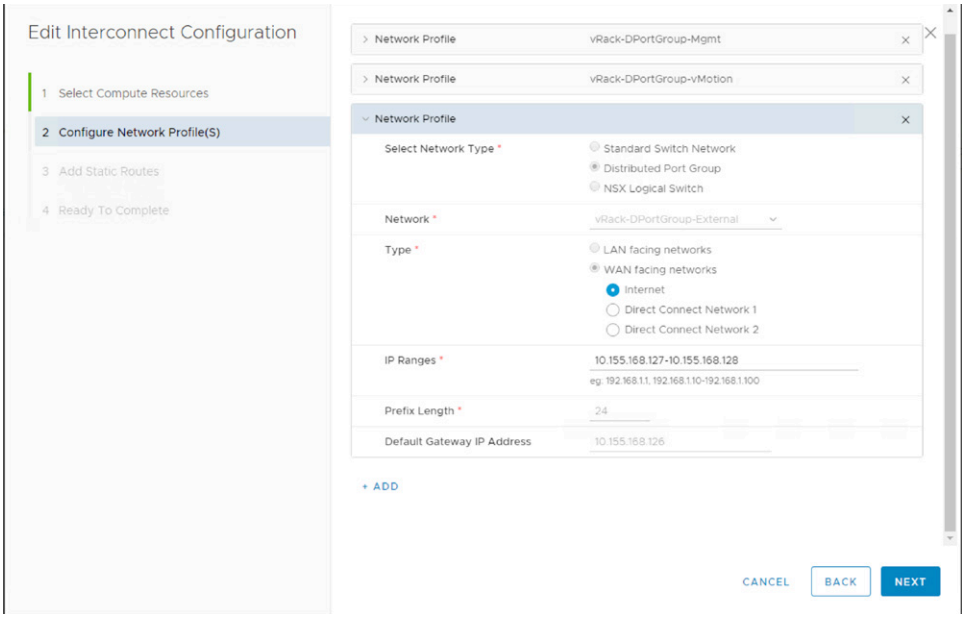
Next, create the network profiles for the NSX Hybrid Connect Cloud Gateway appliance. This defines the IP address pool for the Cloud Gateway and the Layer 2 Concentrator appliances. Later, when the hybridity tunnel has been built, the NSX Hybrid Connect Manager instance will automatically select an available IP from this pool and assign it to the appliances.



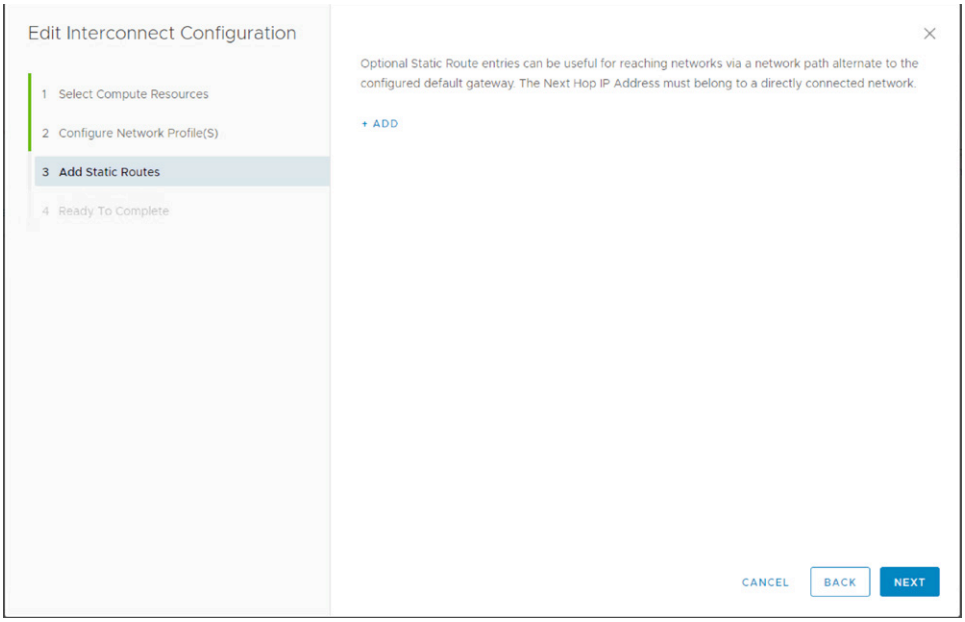
Add an available IP for the vSphere **vMotion** subnet in the Cloud Foundation site.



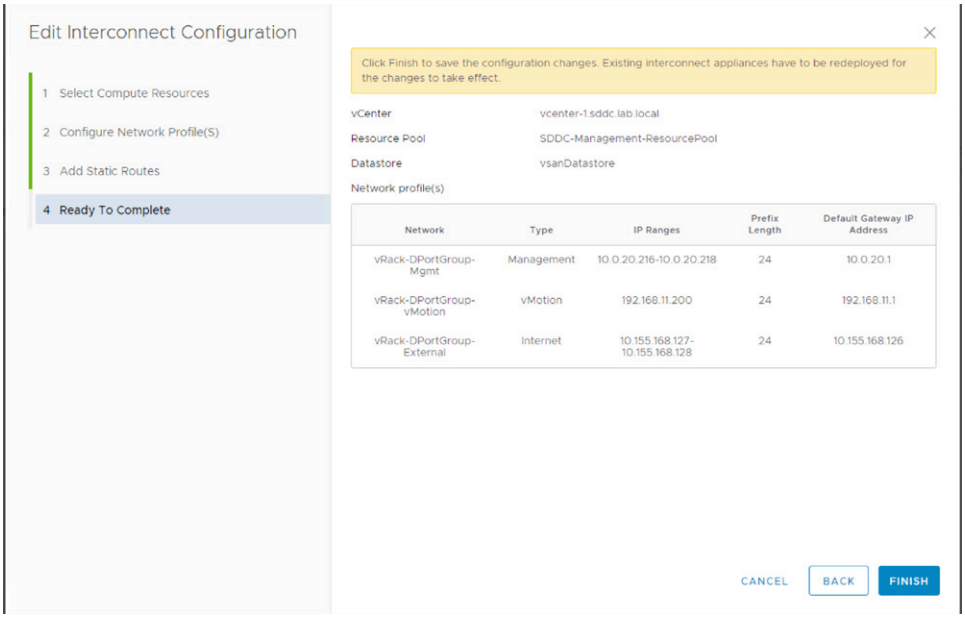
Add available IP addresses for the external WAN–facing networks. These IP addresses will be routed from the Cloud Foundation site and available on the external corporate network.



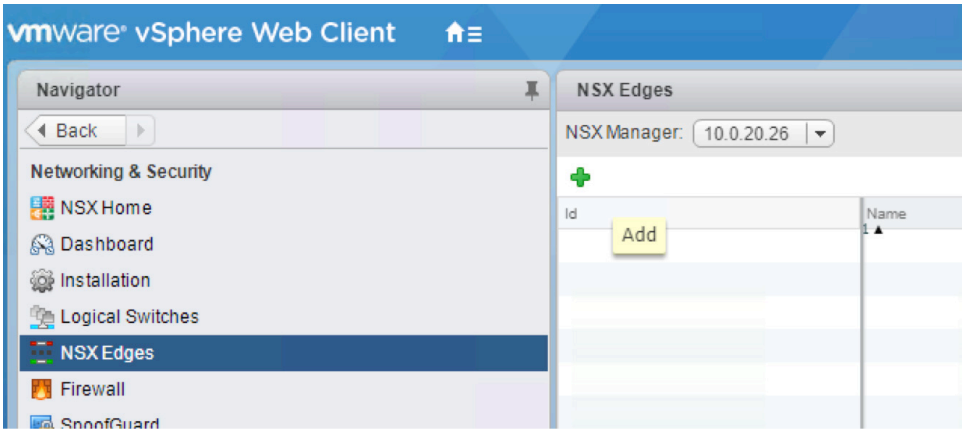
Add Static Routes if necessary.



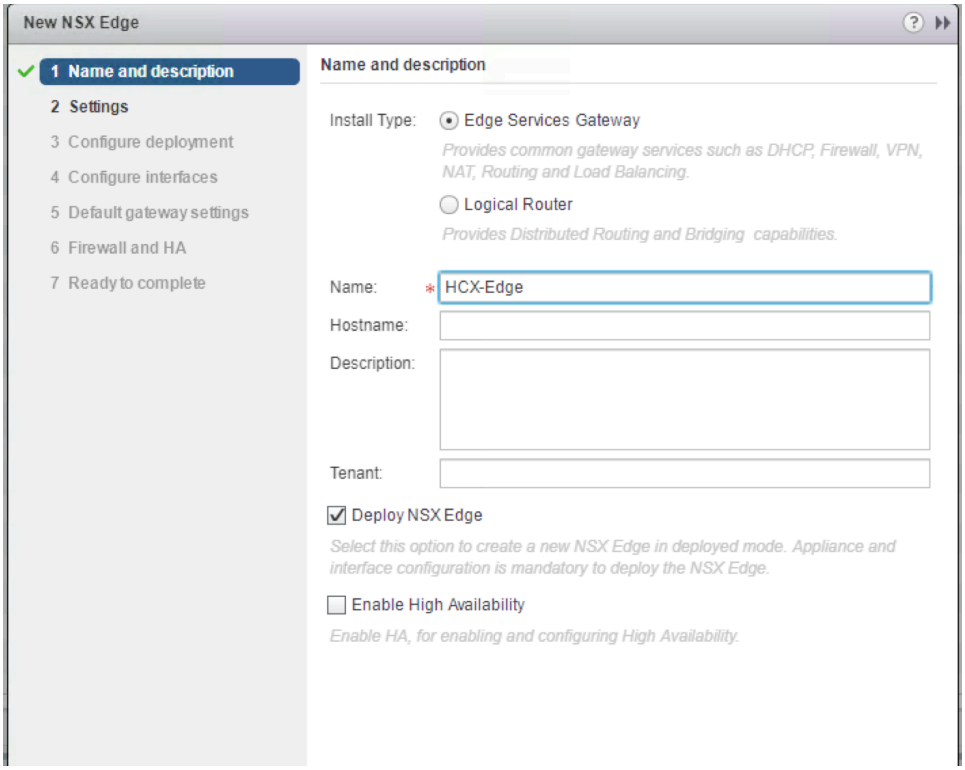
Review the settings for the interconnect configuration and click **FINISH**.



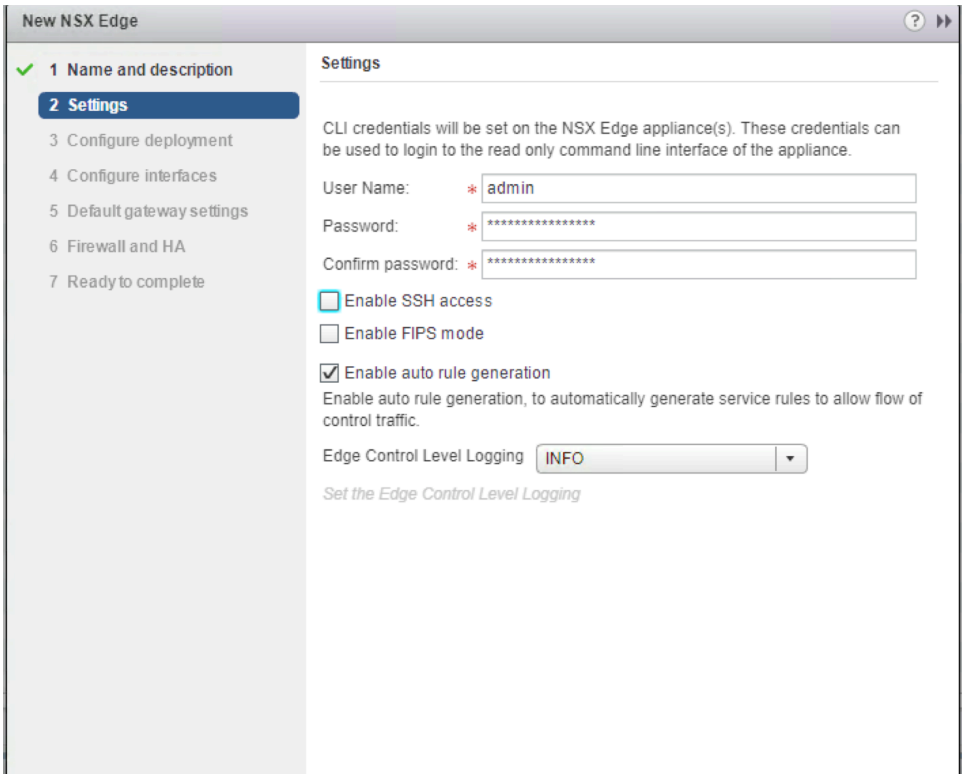
With the interconnect configuration now complete, configure an NSX router to enable L2 network extensions into the Cloud Foundation site. Log in to the Cloud Foundation vSphere Web Client instance. Navigate to the NSX home and select **NSX Edges**. Click the **green plus icon** to add a new NSX Edge instance.



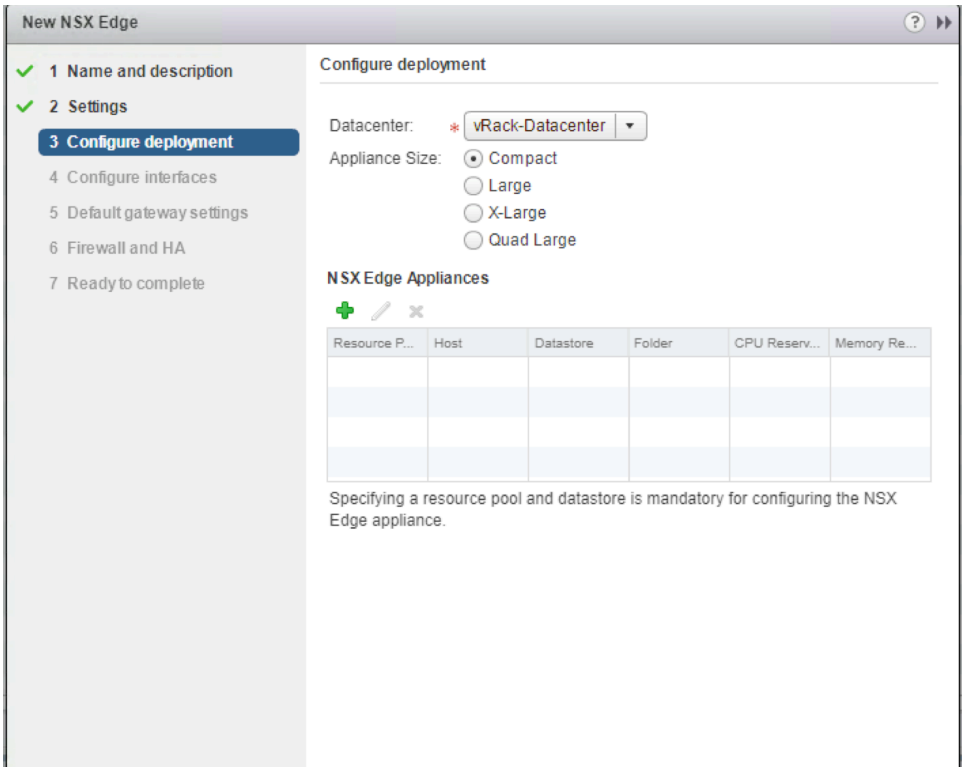
Give the NSX Hybrid Connect NSX Edge instance a **Name**. Click **Next**.



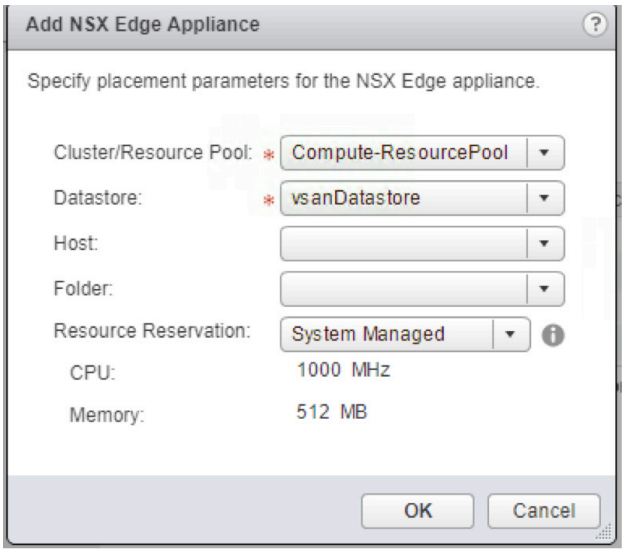
Set the **Password** for the NSX Edge instance.



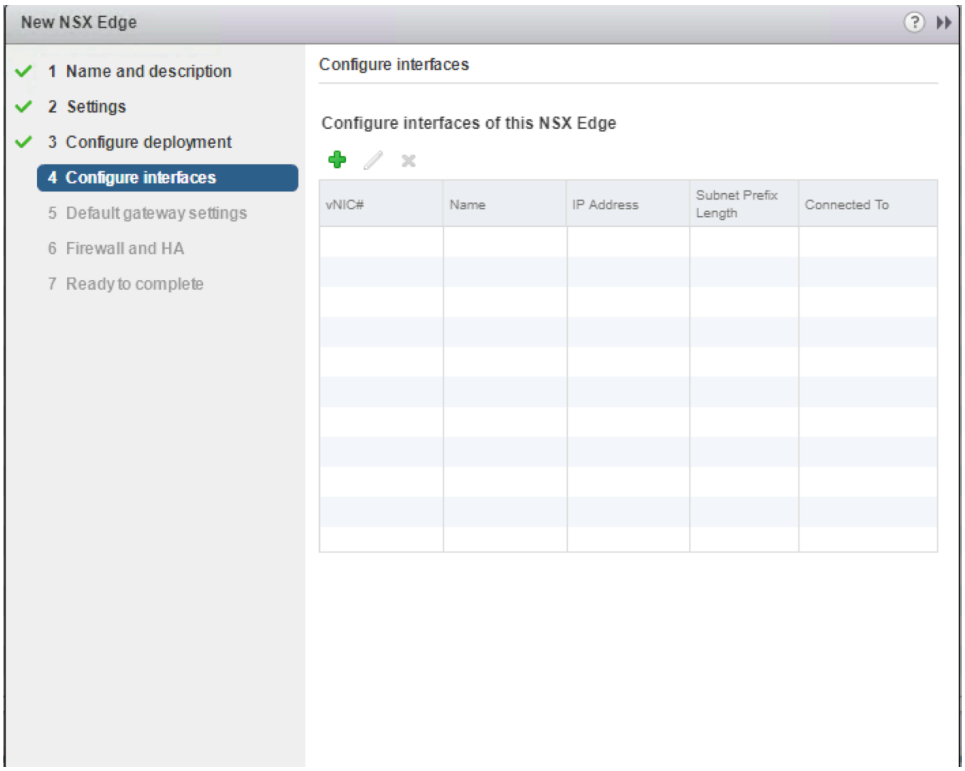
Select the **Appliance Size**. Then click the **green plus icon**.



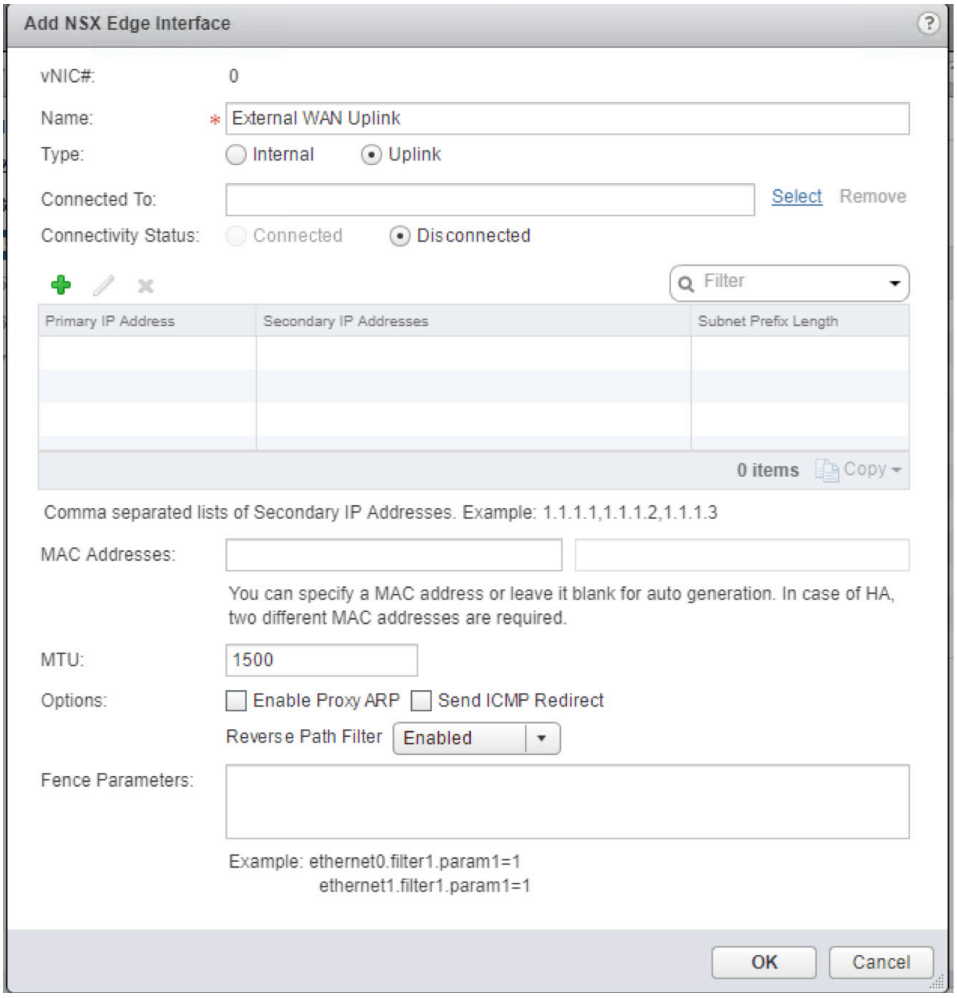
Select the **Resource Pool** and **Datastore**. Click **OK**. Then click **Next**.



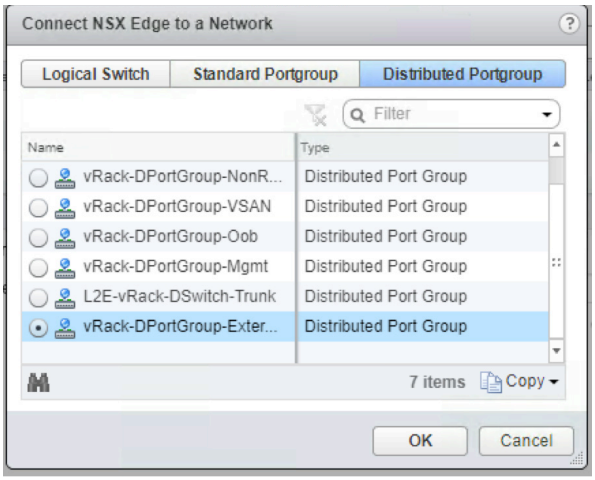
Click the **green plus icon** to add the **interfaces**.



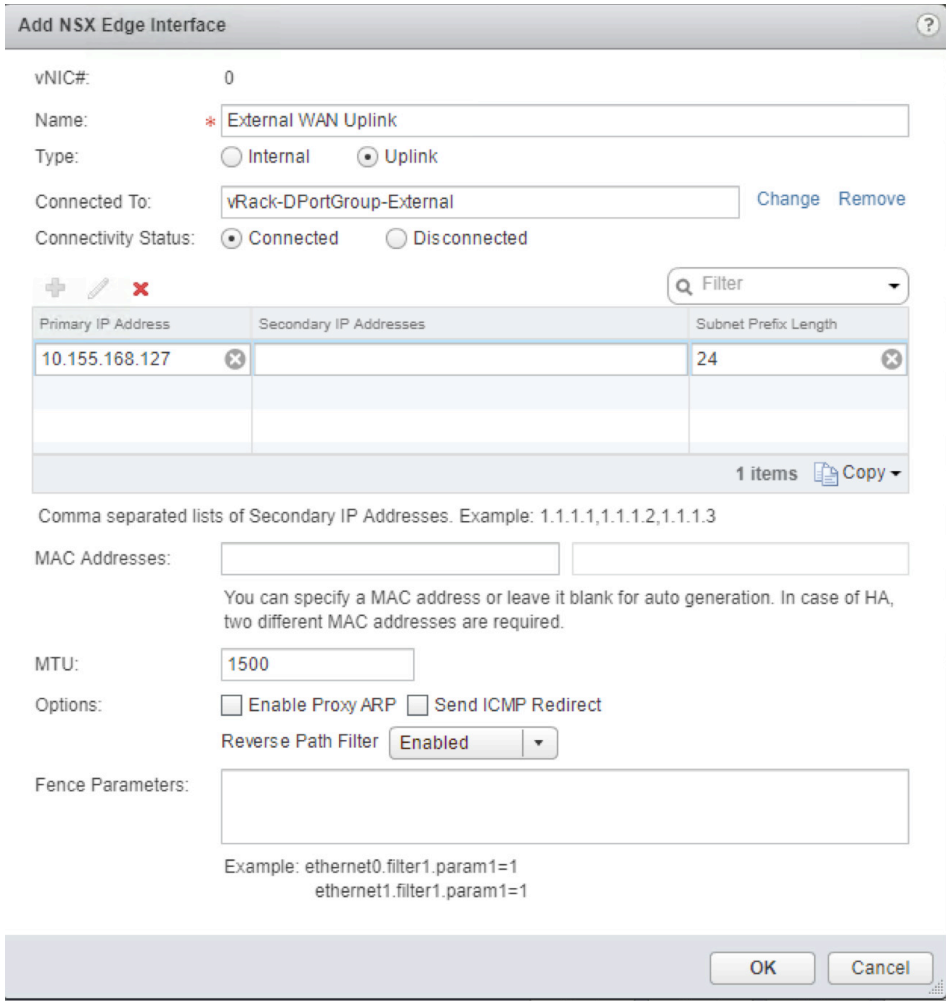
First connect the WAN uplink interface. Enter the **Name** and click the link to select the distributed switch port group for the external WAN uplink connected to the corporate data center.



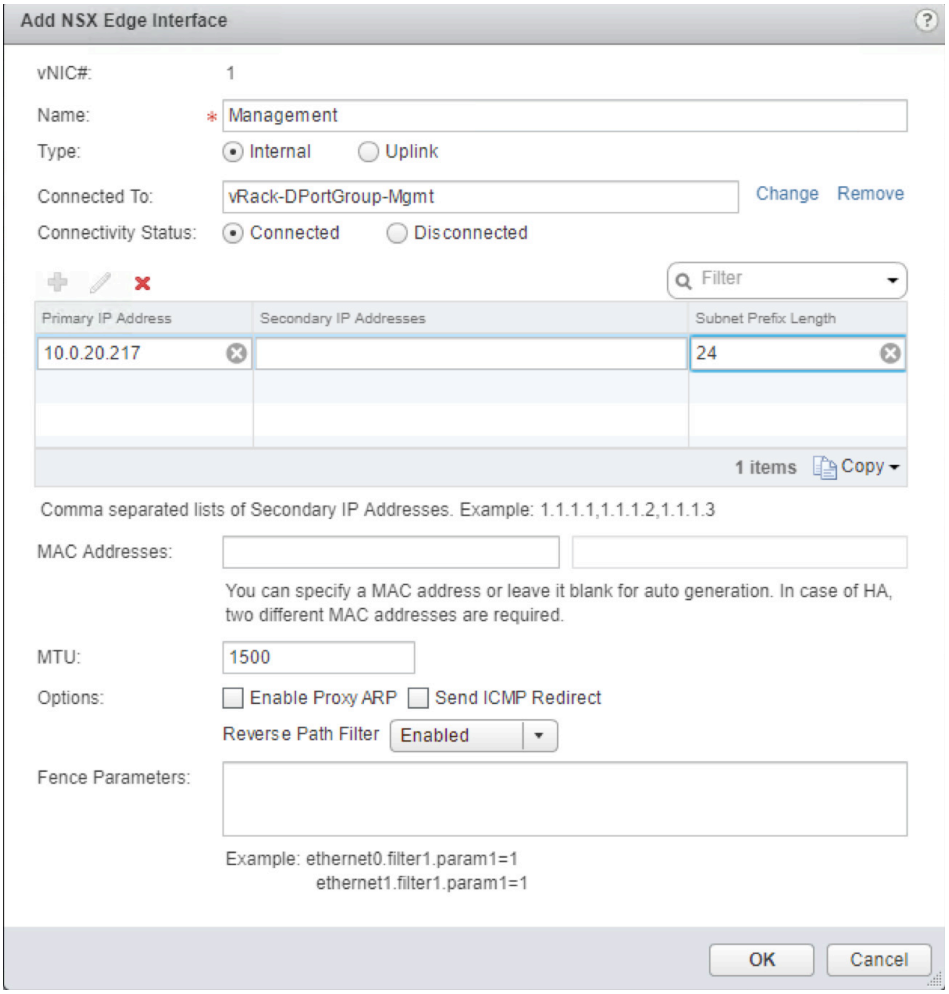
Select the **Port Group** and click **OK**.



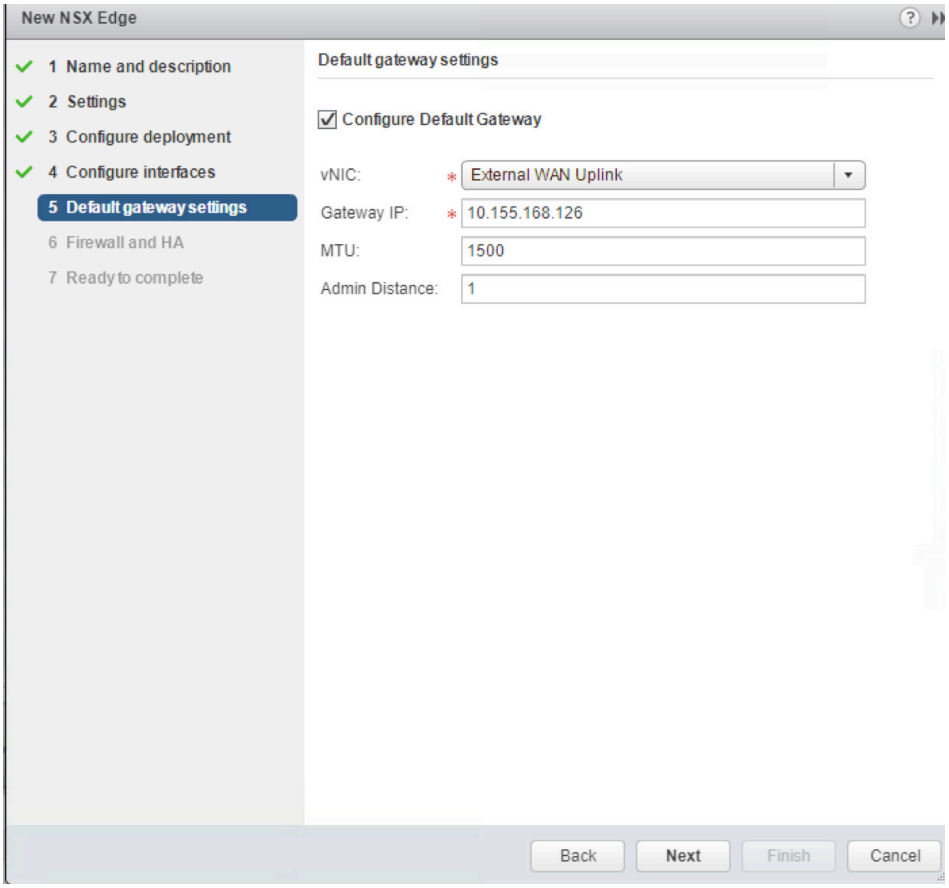
Click the **green plus icon** and enter an available **IP Address** for the **External WAN Uplink**.



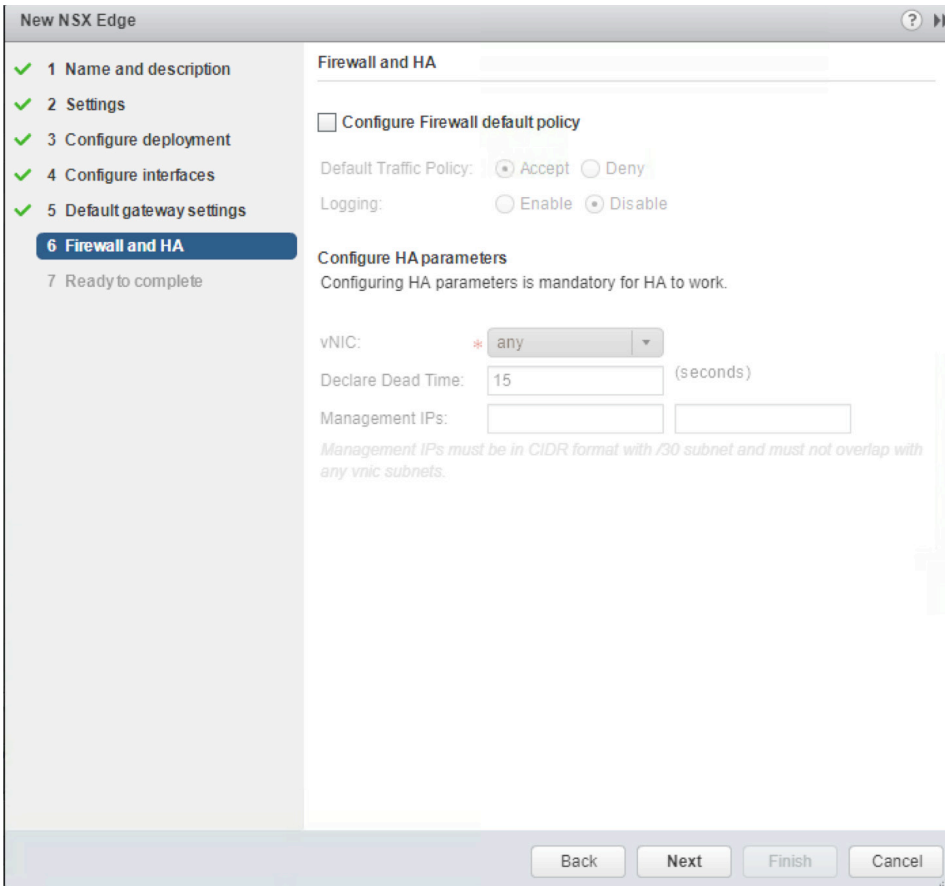
Click the **green plus icon** and add the interface for the Cloud Foundation **Management** port group as depicted in the following screenshot.



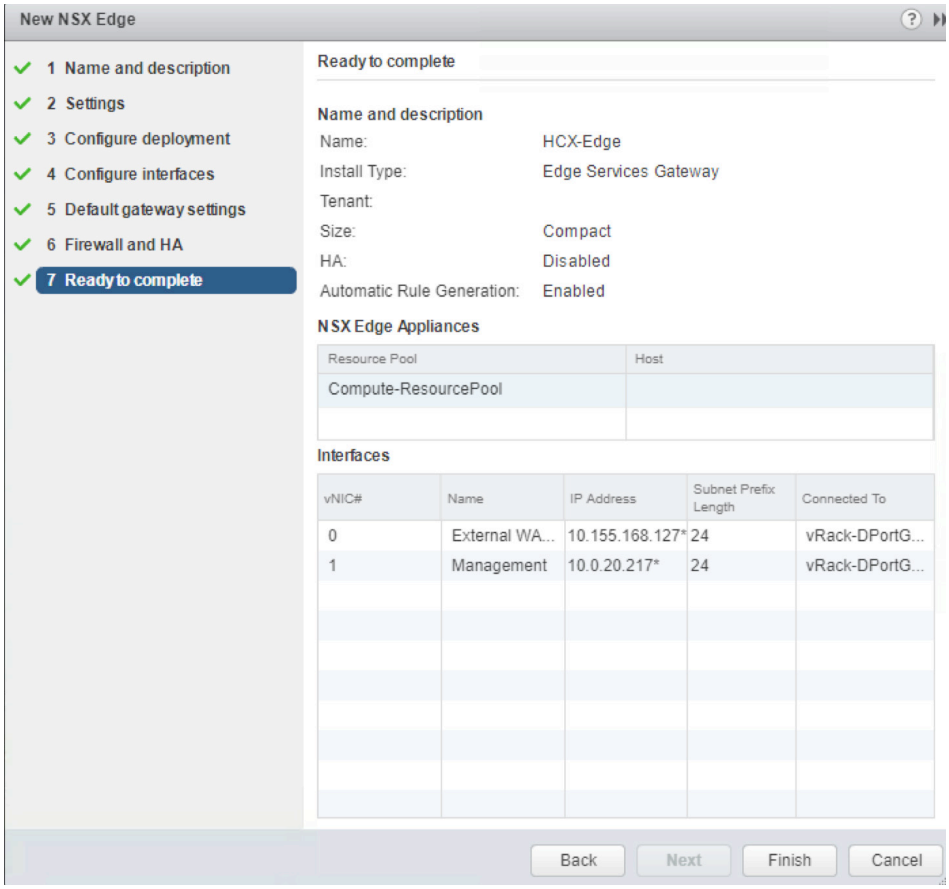
With both NSX Edge interfaces now connected, click **Next** to **Configure Default Gateway**.



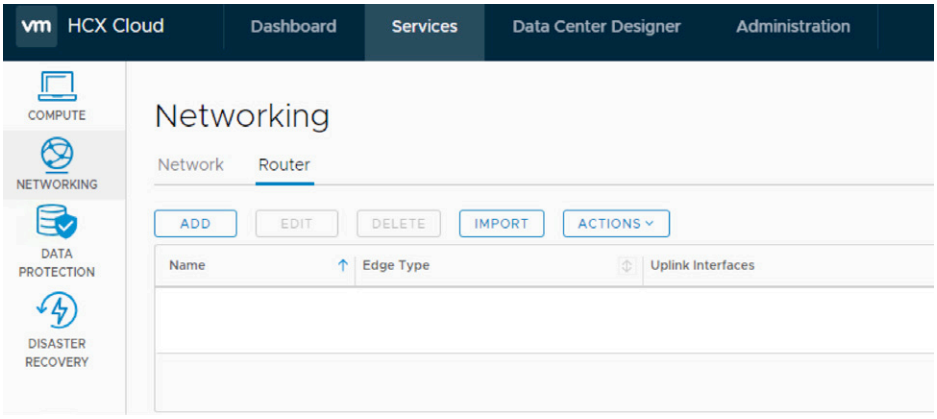
Configure Firewall default policy and click **Next**.



Review the configuration for the **NSX Edge Appliance** and click **Finish**.



When the NSX Edge appliance has been completely installed, import the appliance into the NSX Hybrid Connect Manager so it can be used later for L2 network extension. Log in to the https://<Hybrid Connect Manager> web interface. Navigate to *Services > Networking > Router*. Select **IMPORT** to import the new NSX Edge router.



The NSX Hybrid Connect target installation is now complete and ready for the installation of the NSX Hybrid Connect source site. Figure 15 shows that the NSX Hybrid Connect target appliance is installed and that the NSX instance is configured with an NSX Edge appliance.

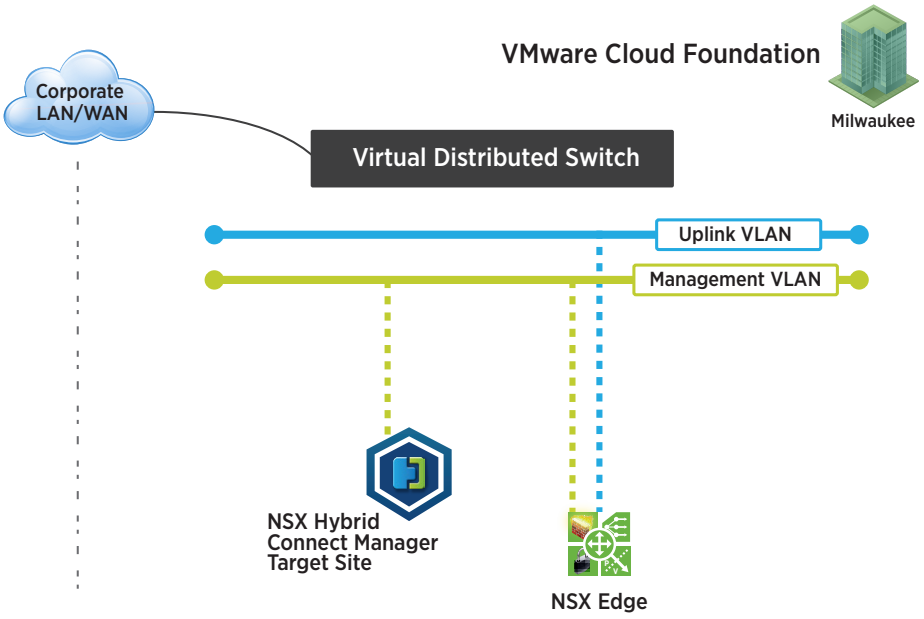
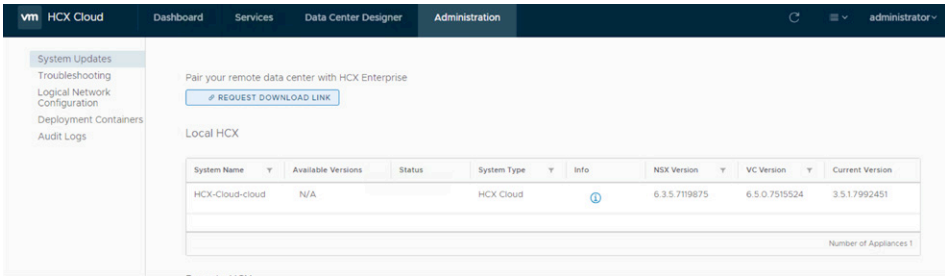


Figure 15. NSX Hybrid Connect Target Site Installation

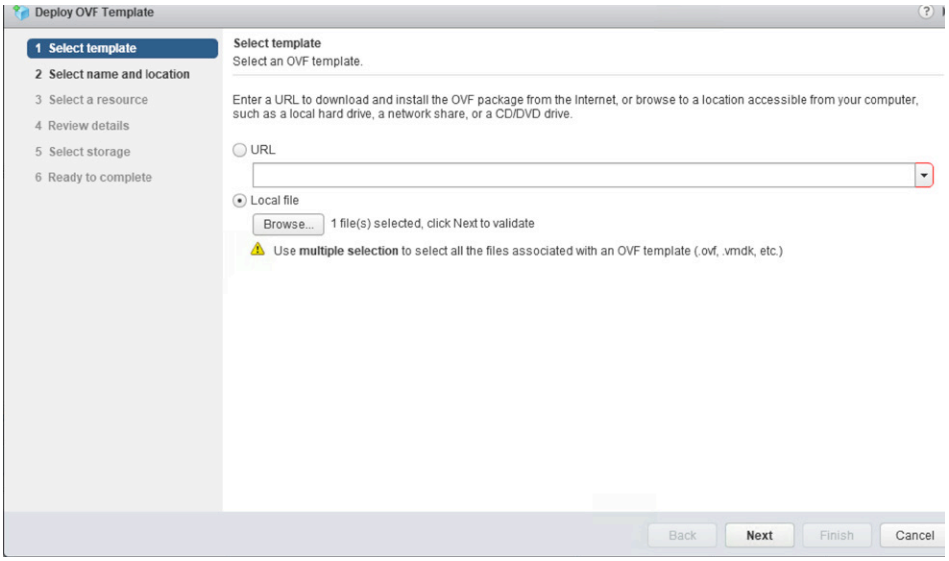
Installation – NSX Hybrid Connect Manager Source (Legacy vSphere Site)

From the NSX Hybrid Connect Manager target site web UI, https://<Hybrid Connect Manager>/, log in with vSphere administrator (administrator@vsphere.local) credentials and proceed to the **Administration** page. See **REQUEST DOWNLOAD LINK**. This link downloads the NSX Hybrid Connect Manager source site installer OVA for deployment into the legacy vSphere environment.

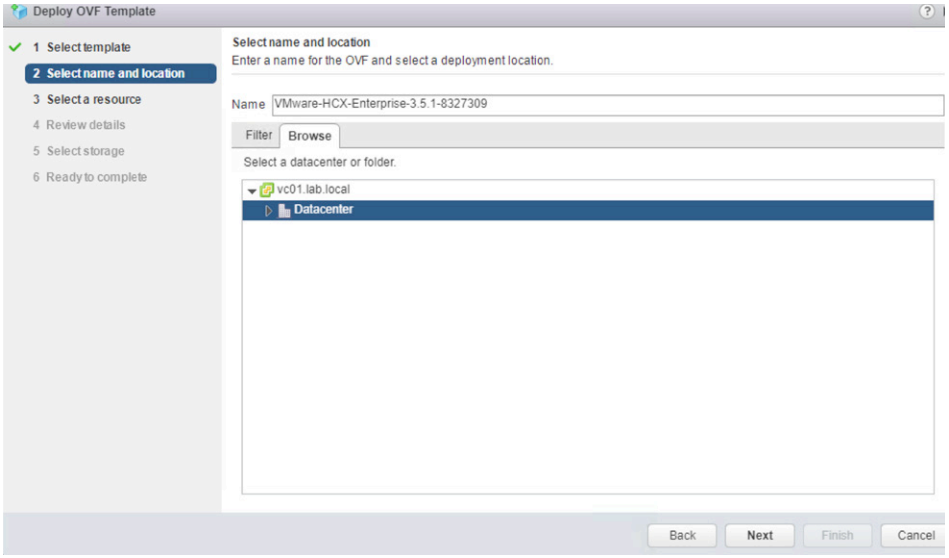
Click **REQUEST DOWNLOAD LINK**.



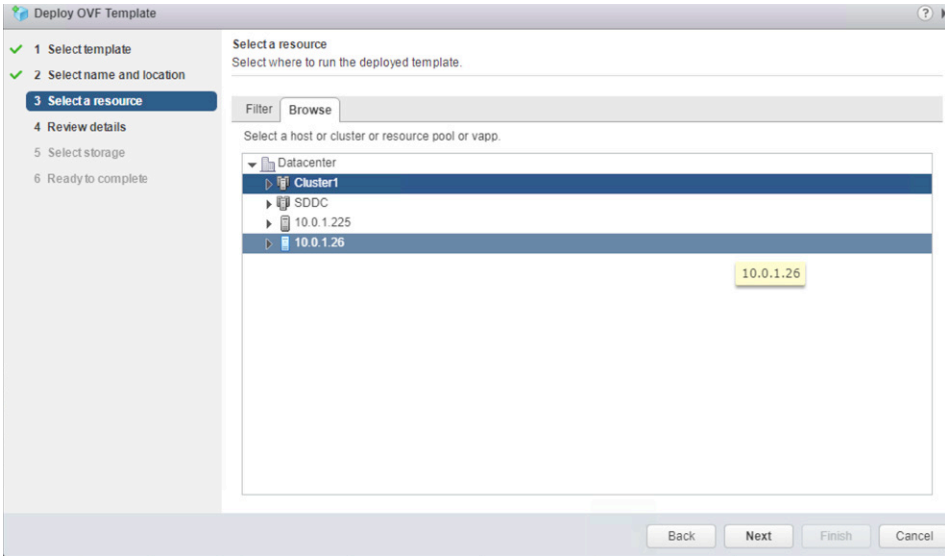
Select **Local file** and click **Browse** to find the downloaded OVA file. Click **Next**.



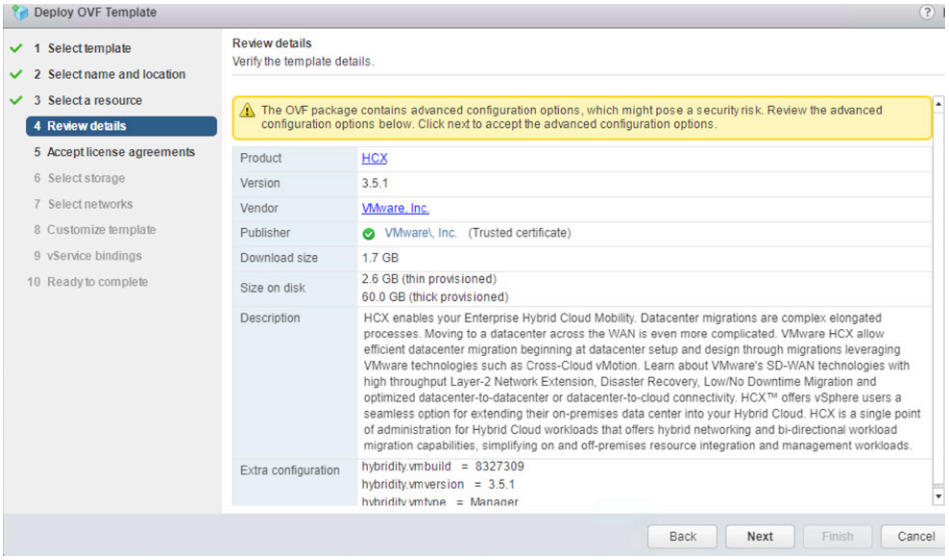
Enter a **Name** for the NSX Hybrid Connect Manager source site appliance and select the destination folder. Click **Next**.



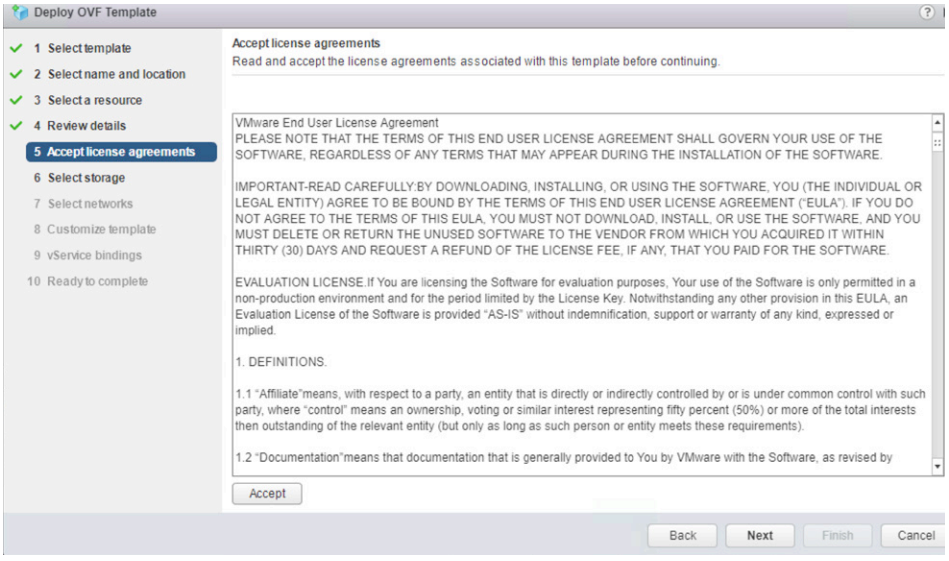
Select the destination cluster. Click **Next**.



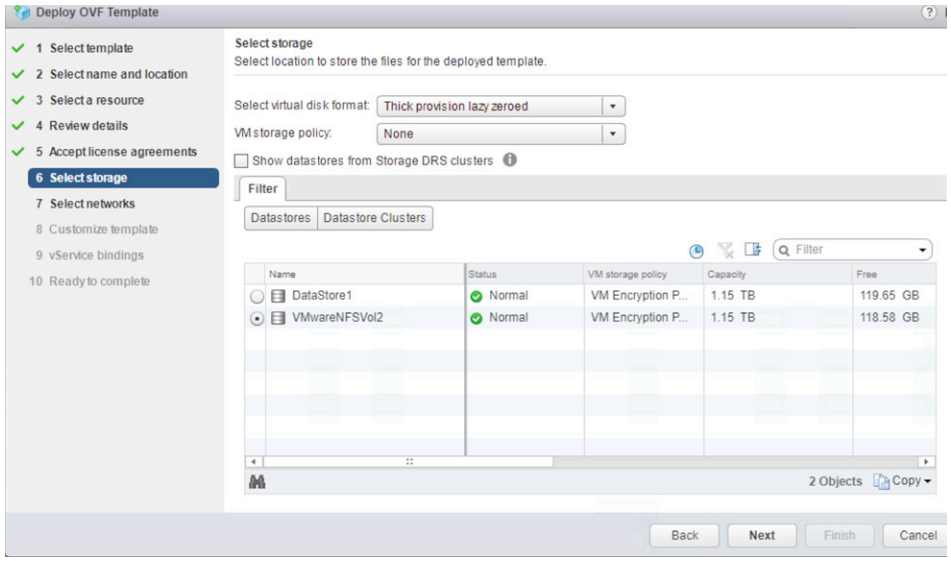
Review details and click **Next**.



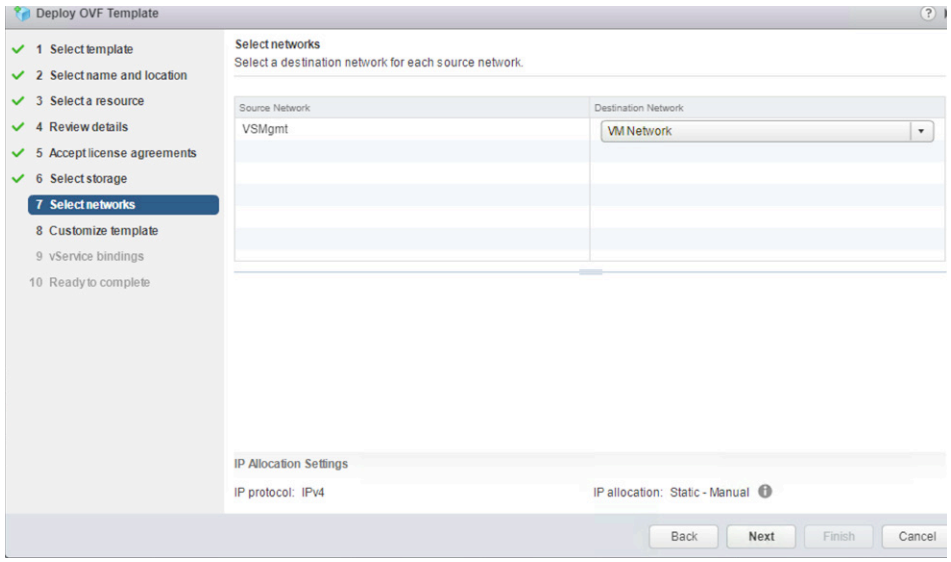
Review the EULA. Click **Accept**. Click **Next**.



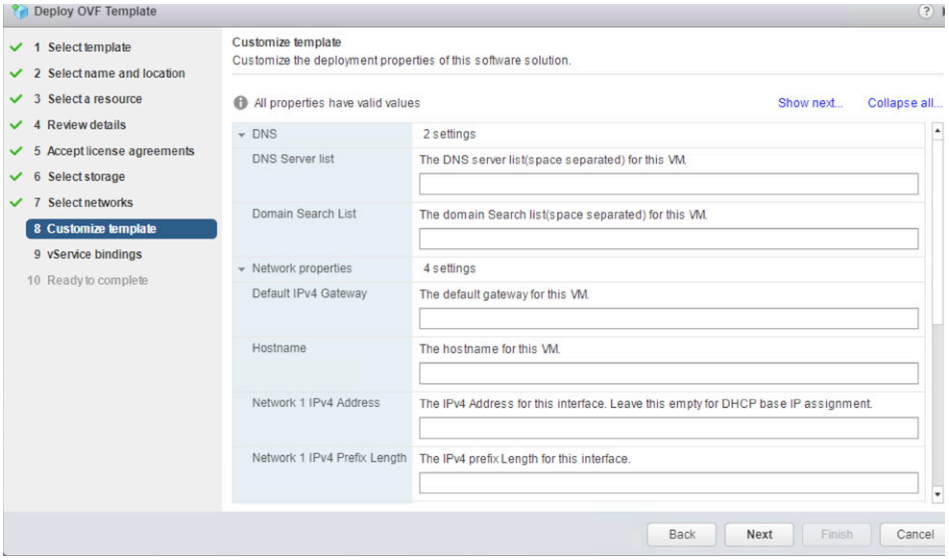
Select storage location. Click **Next**.



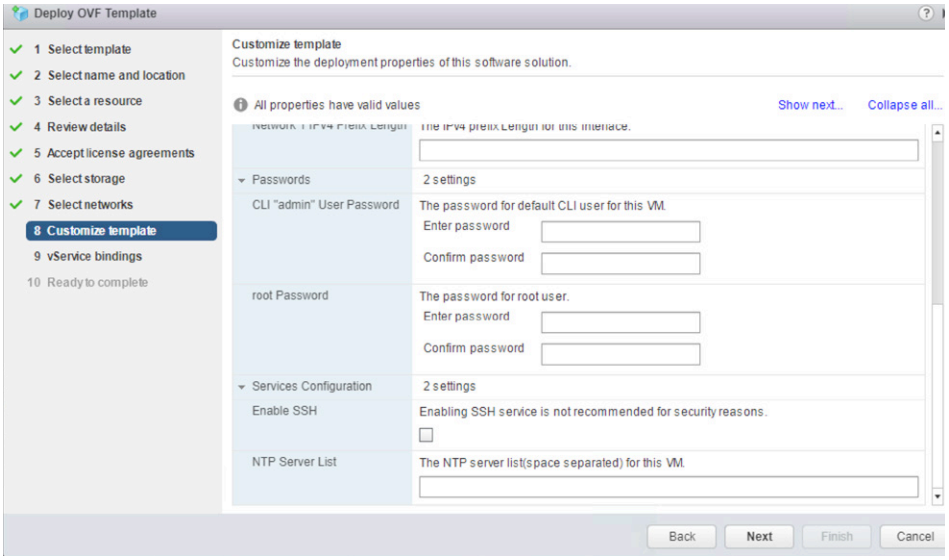
Select the **destination network** for installation of the NSX Hybrid Connect Manager source site appliance. Click **Next**.



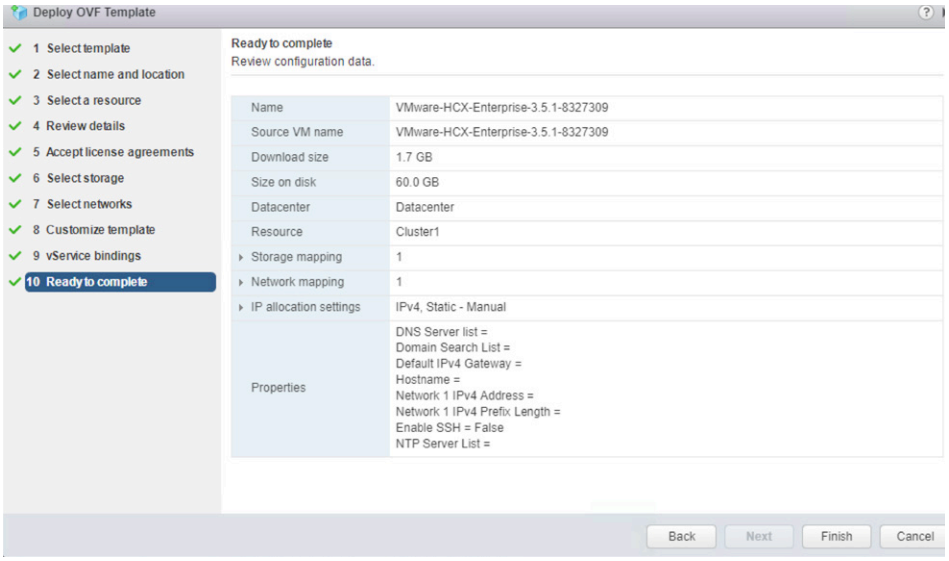
Enter the network settings for the appliance. Click **Next**.



Enter the **Passwords** and complete the appliance configuration. Click **Next**.



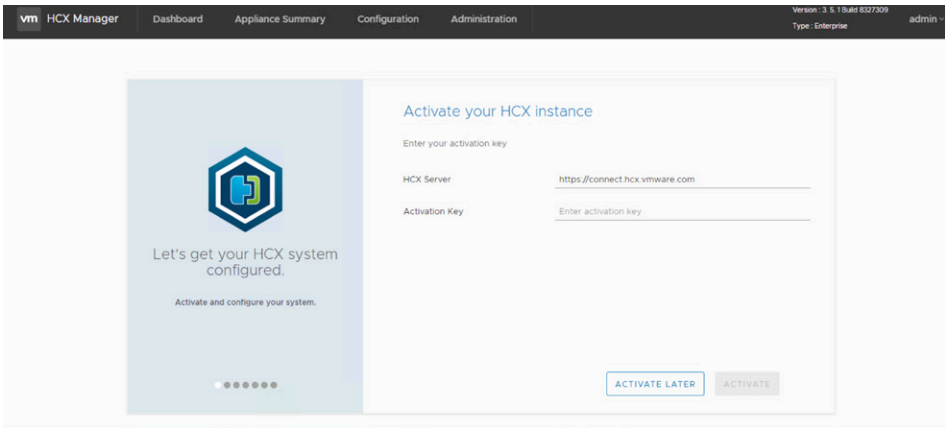
Review the installation settings and click **Finish**.



After the OVA deployment has completed, power on the NSX Hybrid Connect Manager source site VM.

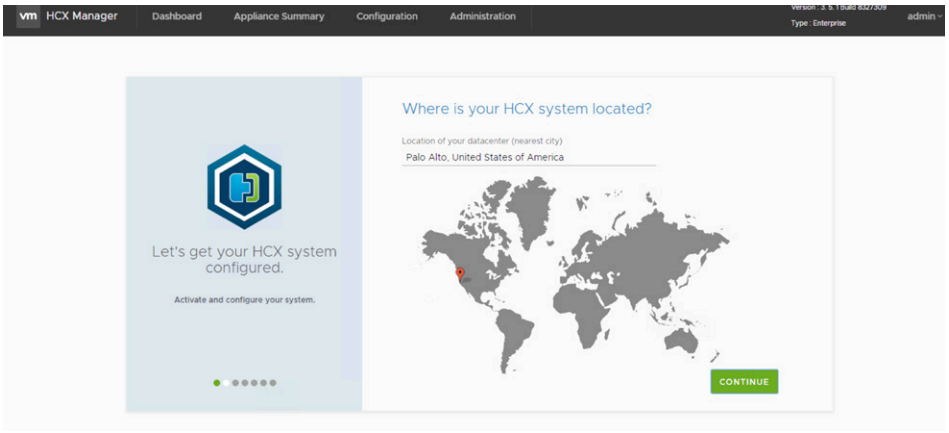
Now configure the NSX Hybrid Connect Manager source site appliance. Log in to the web UI of the appliance at https://<Hybrid Connect Manager Source Site>:9443/. Log in with the **Admin** username and password set while deploying the OVA.

After successful login, the appliance configuration wizard will appear.

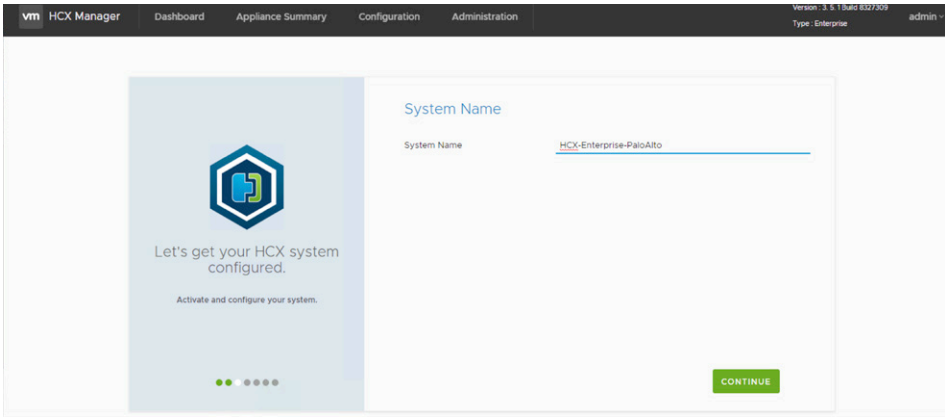


Obtain the NSX Hybrid Connect Manager source site activation key from your account at cloud.vmware.com. Apply the activation key to the appliance.

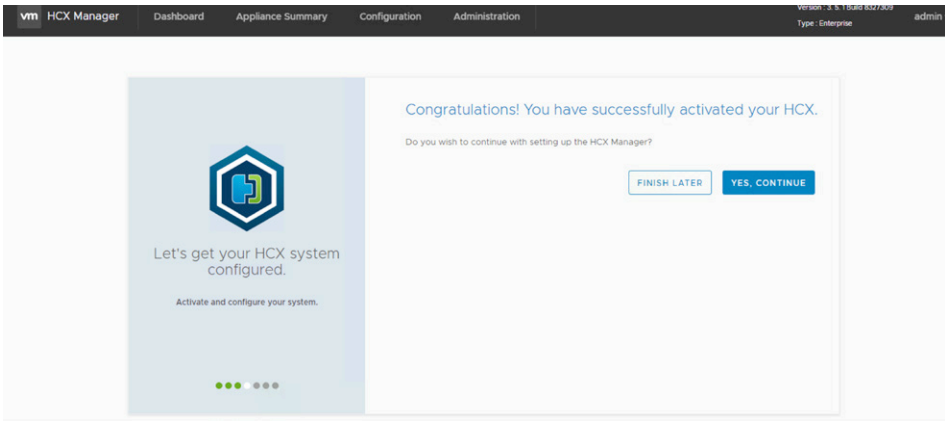
Select the data center location for the NSX Hybrid Connect Manager source site installation. Click **CONTINUE**.



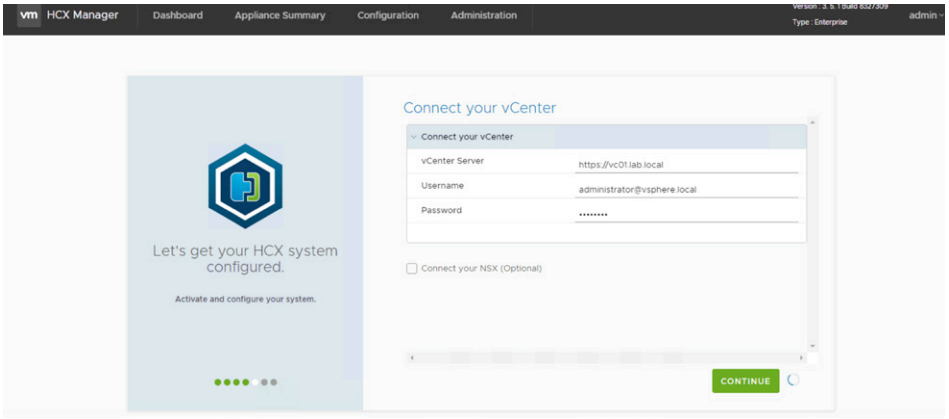
Provide a **System Name** for the NSX Hybrid Connect Manager source site system. Click **CONTINUE**.



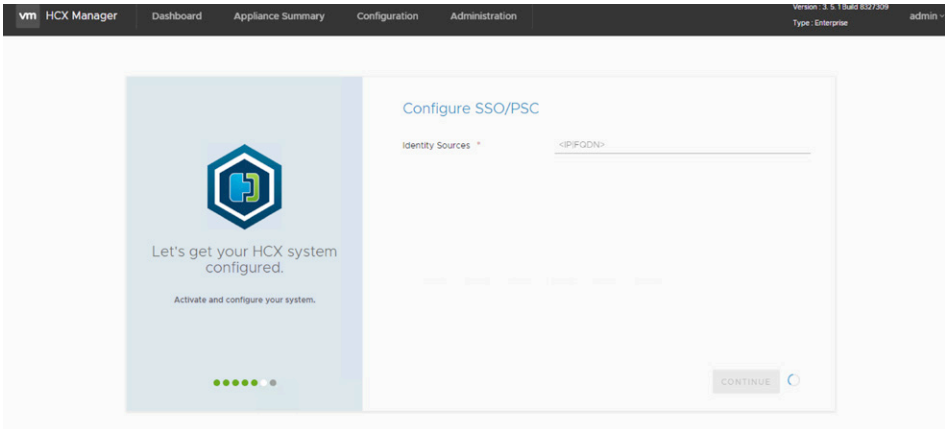
After completing the activation, select **YES, CONTINUE**.



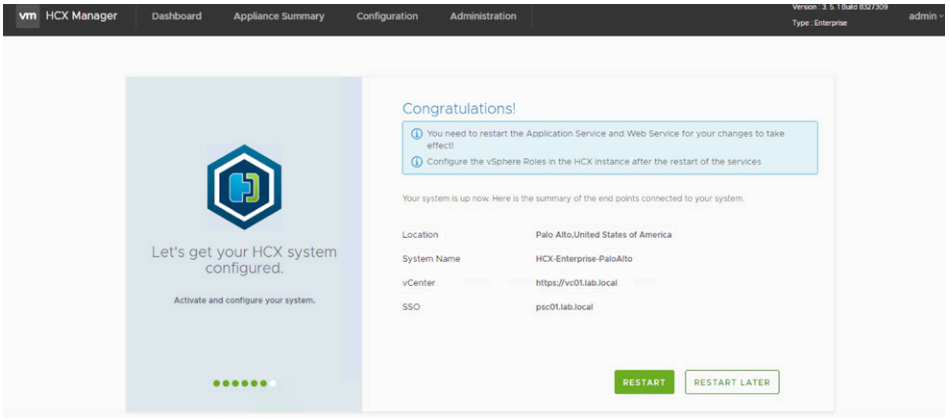
Now connect the NSX Hybrid Connect Manager source site appliance to the legacy vCenter Server system. Enter the web URL for the legacy vCenter Server system and provide the **Username** and **Password**.



If the Platform Services Controller instance is not internal to your vCenter Server system, direct the NSX Hybrid Connect Manager source site instance to the Platform Services Controller instance in your legacy vCenter Server system.

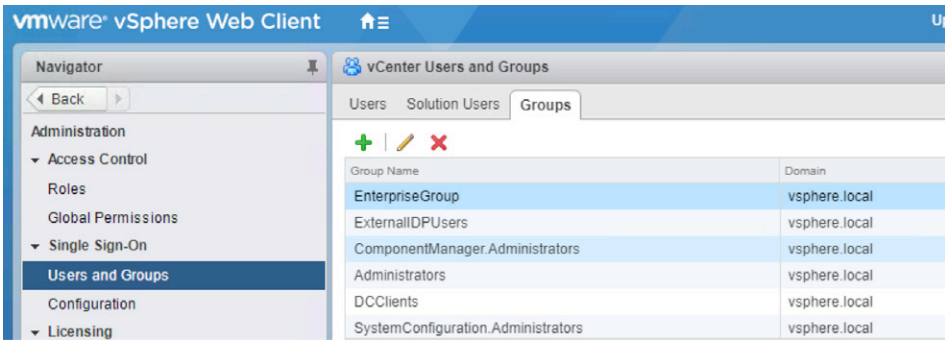


After a restart of NSX Hybrid Connect Manager source site services, the NSX Hybrid Connect Manager source site dashboard will reappear.

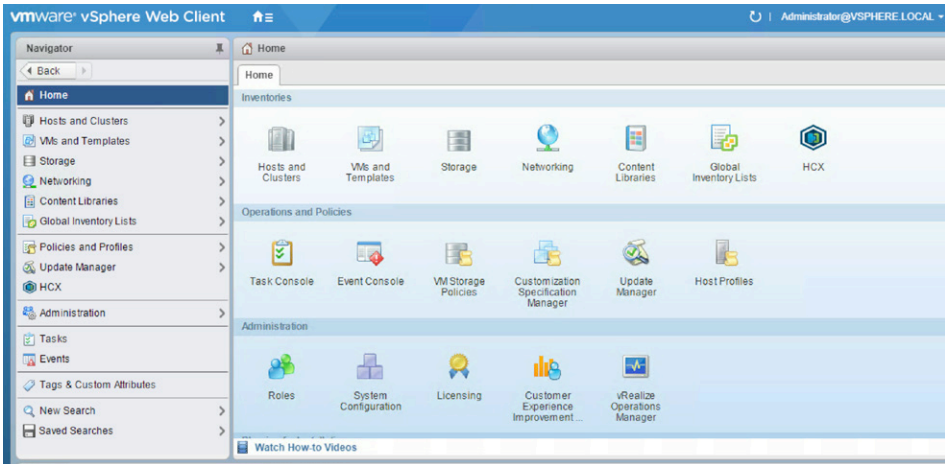


On the NSX Hybrid Connect Manager source site dashboard, configure the **EnterpriseGroup** account.

If you don't have an **EnterpriseGroup** in your SSO accounts for vCenter Server, create one via the vSphere Web Client instance.



Restart the vSphere Web Client instance. When it restarts, the **NSX Hybrid Connect [HCX] icon** will appear on its home screen.



The NSX Hybrid Connect Manager source site installation is now complete.

In the next section, we will complete the site pairing and begin the process of connecting the two sites with NSX Hybrid Connect.

Configuration

The NSX Hybrid Connect architecture environment now resembles Figure 16.

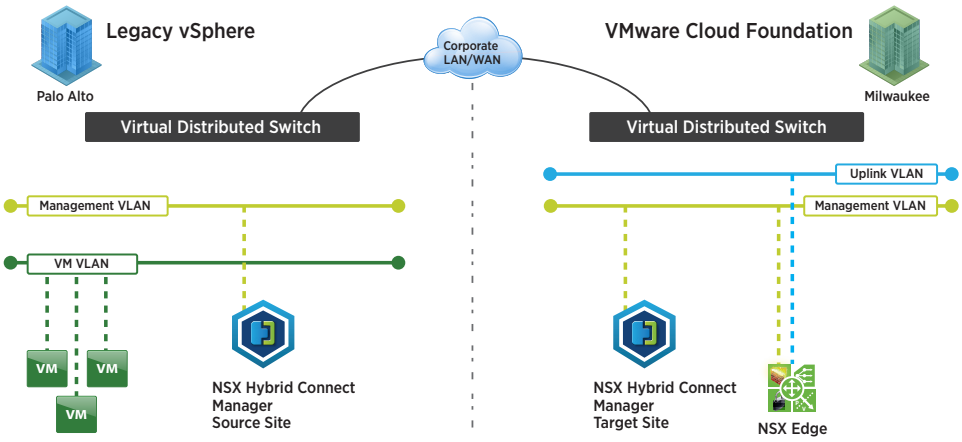
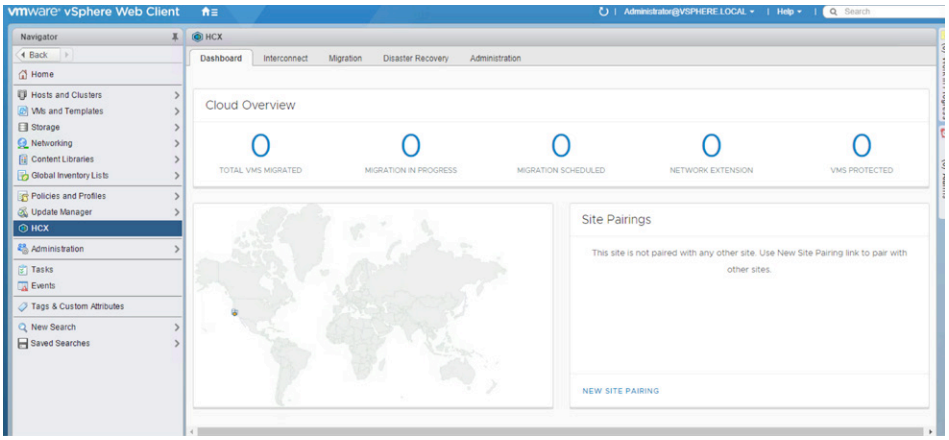


Figure 16. NSX Hybrid Connect Architecture Overview

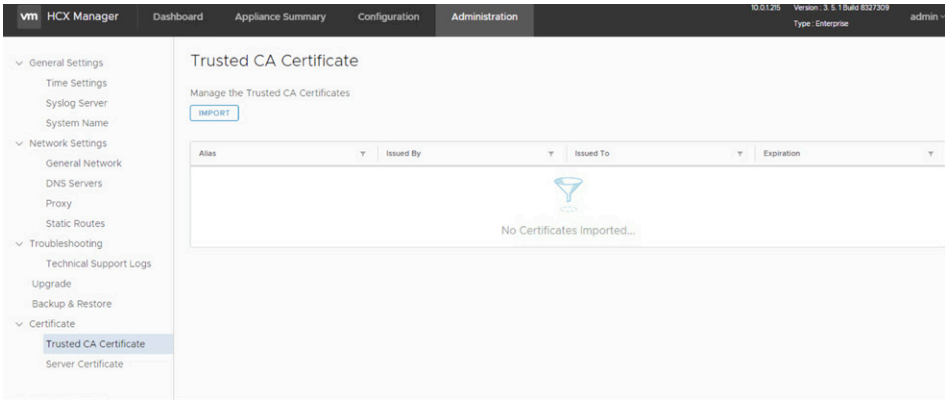
The two NSX Hybrid Connect Manager appliances are installed and connected to a VLAN that enables them to communicate with each other, over the LAN or WAN interface, and with the local vCenter Server environments.

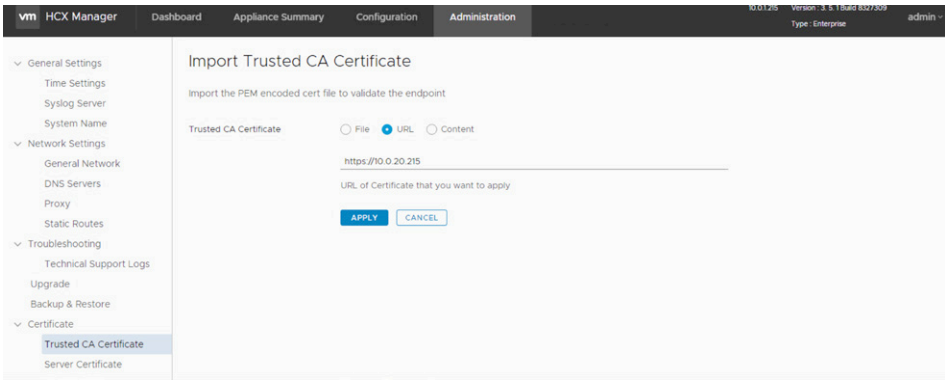
Access the **NSX Hybrid Connect [HCX]** dashboard from the vSphere Web Client instance in the legacy vSphere system. See **Site Pairings**. Site pairings occur when NSX Hybrid Connect Manager source and target instances are linked. The site pairing process includes the following steps.



Before enabling the new site pairing link, the NSX Hybrid Connect Manager source site must trust the SSL certificate of the NSX Hybrid Connect Manager target site. Log in to the NSX Hybrid Connect Manager source web UI and import the certificate, located at https://<Hybrid Connect Manager Source Site>:9443/.

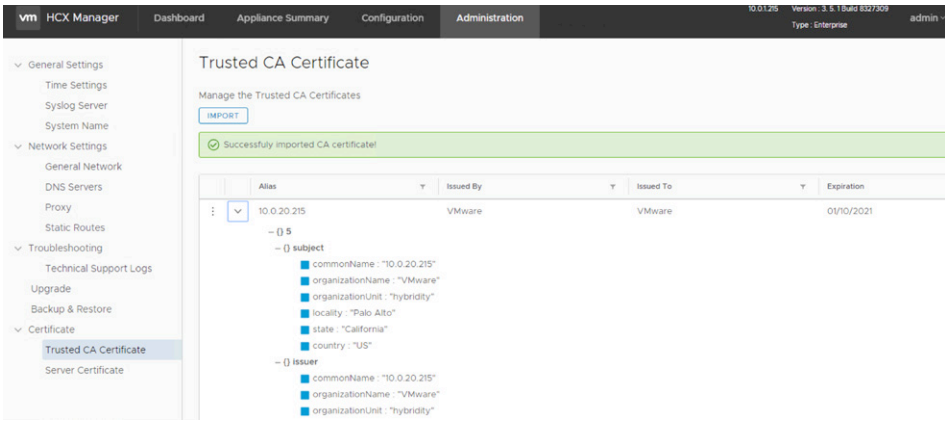
Click **Administration** in the NSX Hybrid Connect Manager source site and select **Trusted CA Certificate** on the left navigation bar. Click **IMPORT** and then select the URL. Enter the URL for the NSX Hybrid Connect Manager target site appliance installed in the Cloud Foundation site. Click **APPLY**.



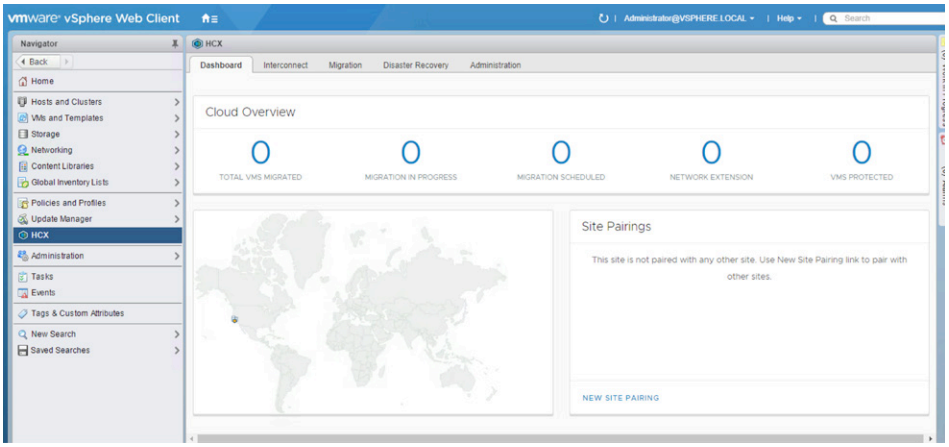


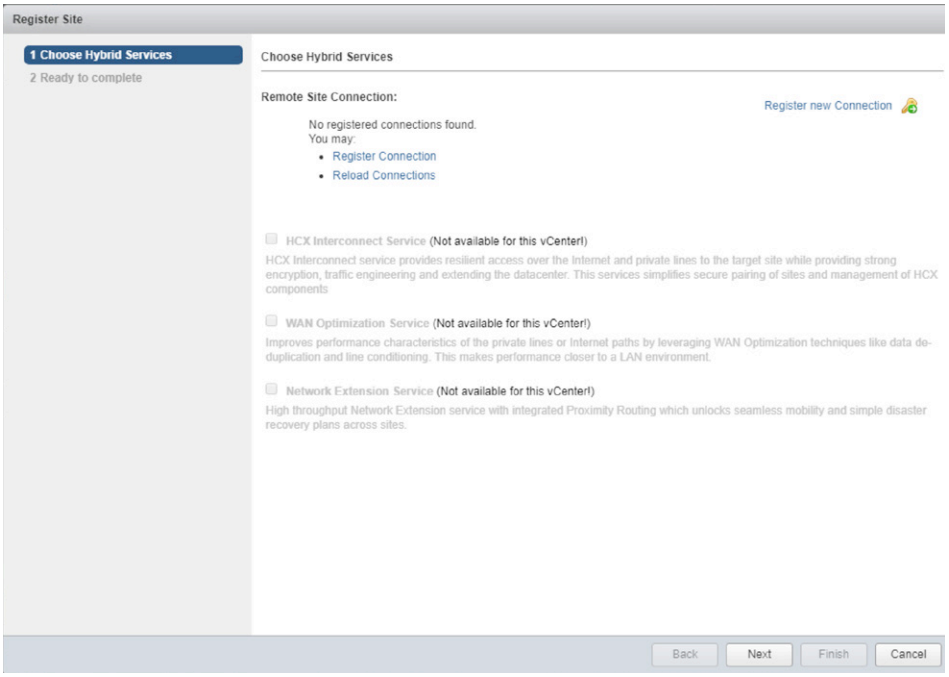
The site pairing process will not work if the common name (CN) in the SSL certificate does not match the name in the URL. In this white paper, we use the IP address in the CN name of the appliance and have updated the SSL certificate with this information.

The SSL certificate is now trusted and ready for site pairing.

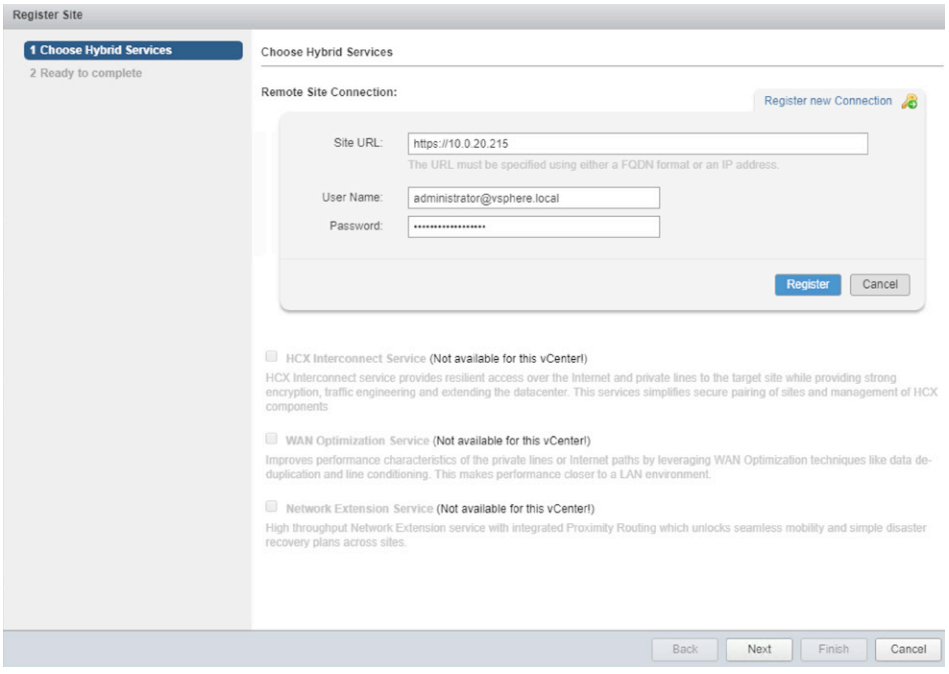


Return to the legacy vCenter Server vSphere Web Client NSX Hybrid Connect [HCX] dashboard. Click the **NEW SITE PAIRING** link. The register site wizard will appear. Click **Register new Connection**.





Enter the **Site URL** for the NSX Hybrid Connect Manager target appliance. Enter the administrator SSO **User Name** and **Password** for the Cloud Foundation installation. Click **Register**.



The site pairing process is now completed, as depicted in Figure 17. We are ready to begin the final process of creating a hybridity tunnel between the two sites.

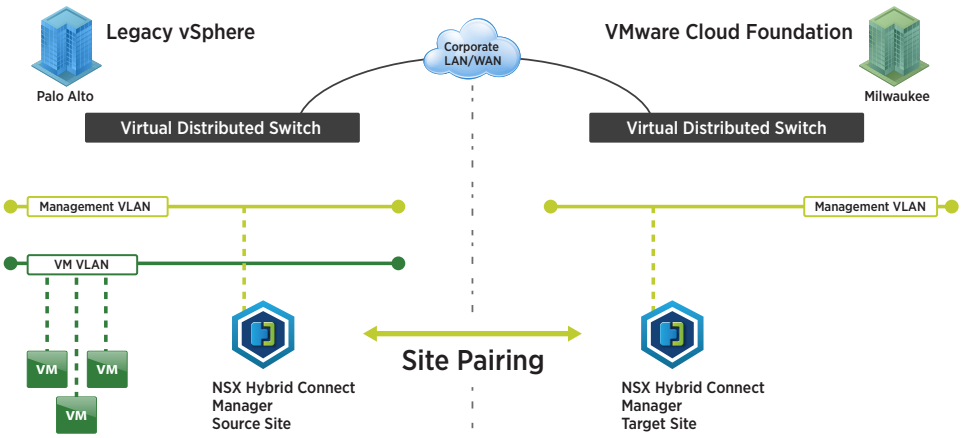
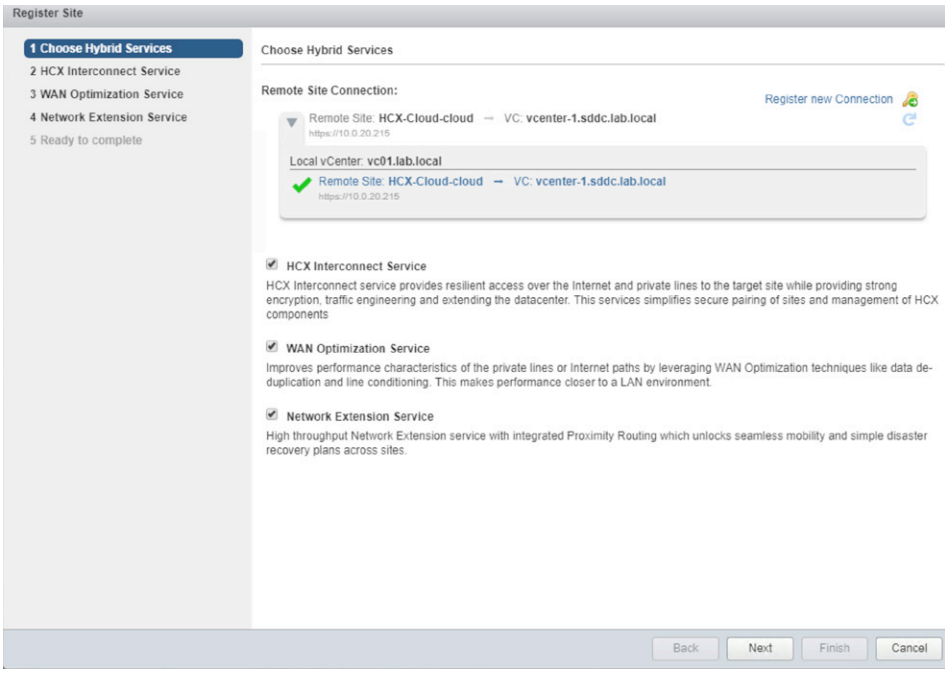


Figure 17. Site Pairing Process Completed

Creating the Hybridity Tunnel

On the vSphere Web Client instance for the NSX Hybrid Connect Manager source site, begin by selecting the three services used to create the hybridity tunnel.

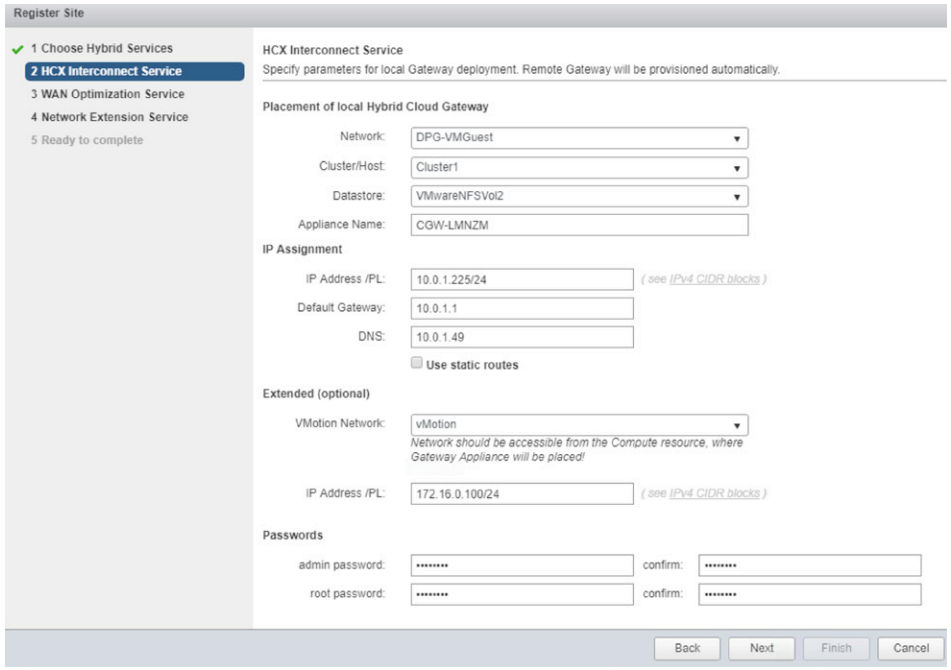
Select all three check boxes. Click **Next**.



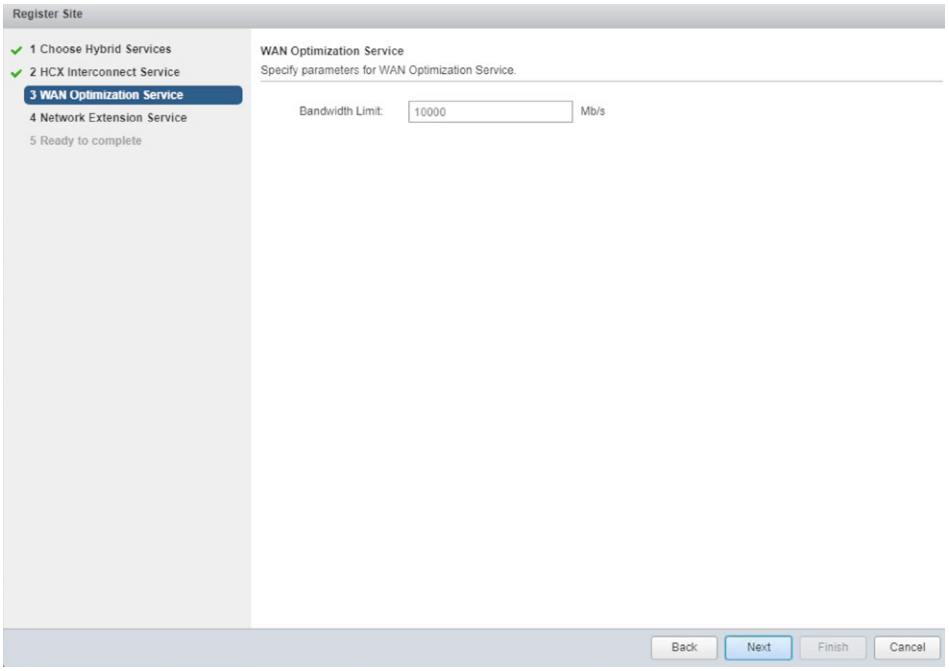
Next, provide information for the installation of the NSX Hybrid Connect service appliances.

Start with the **NSX Hybrid Connect [HCX] Interconnect Service**, which will be installed on the legacy vSphere source site. Select the **Network** that enables access across the LAN or WAN link to the Cloud Foundation site and also has access to the ESXi host management VMkernel interface subnet. Select a **Cluster/Host** and **Datastore** in which to install the appliance. Give the appliance a name that meets your naming conventions. Provide the **IP Address**, **Default Gateway**, and **DNS**.

To do live migrations, select the vSphere vMotion VMkernel subnet and provide the **Appliance Name** and **IP Address** on that subnet. Enter **admin password** and **root password** for the accounts on the appliance. Click **Next**.



The next component to configure is the **WAN Optimization appliance**. Set the **Bandwidth Limit** for the migrations. Click **Next**.

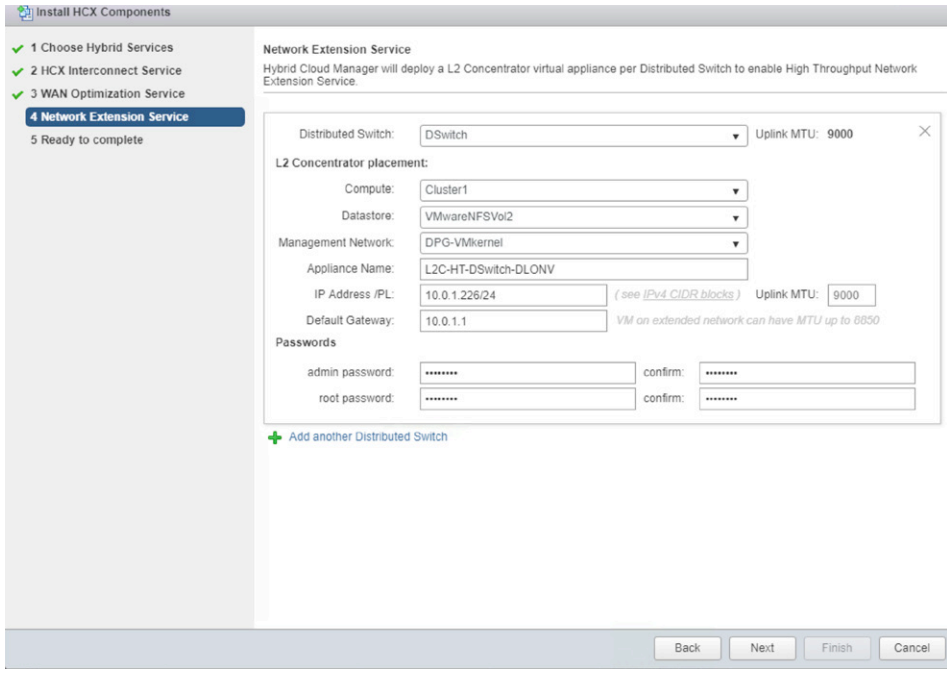


The last component to configure is the **Layer 2 Concentrator appliance**.

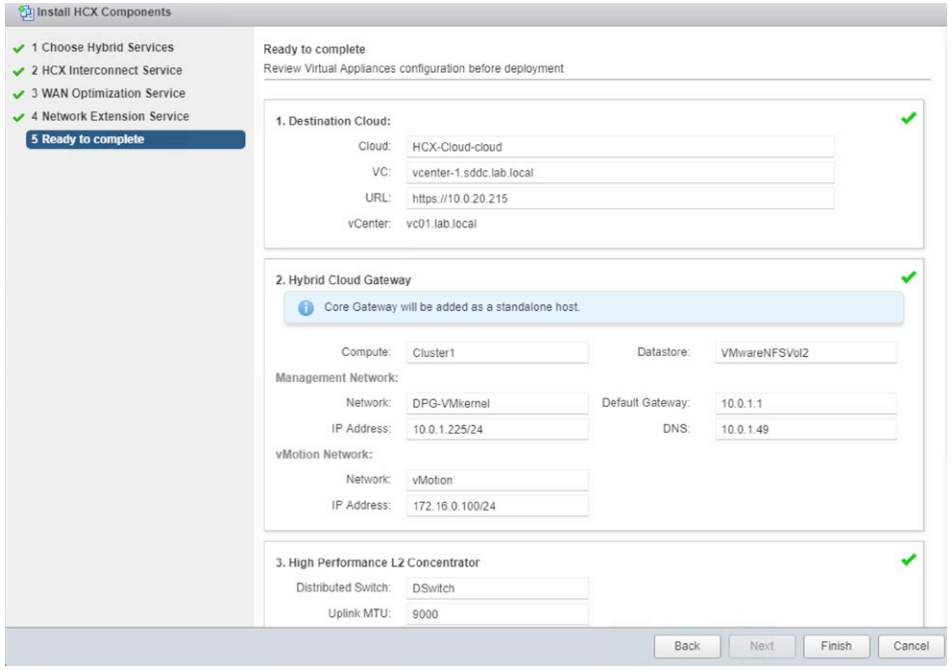
Select the placement for the installation of this Layer 2 Concentrator appliance. Select the cluster, datastore, and management port group in which to install the appliance.

Provide the **Appliance Name** and **IP Address** on the selected subnet. Enter the **Uplink MTU** supported across the LAN or WAN link boundaries.

Enter **admin password** and **root password** for the accounts on the appliance.

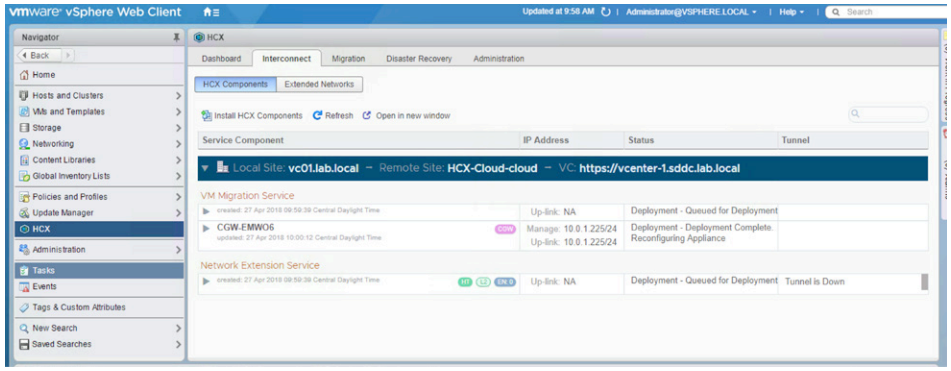


When completed, review your selections for accuracy. Click **Finish**.

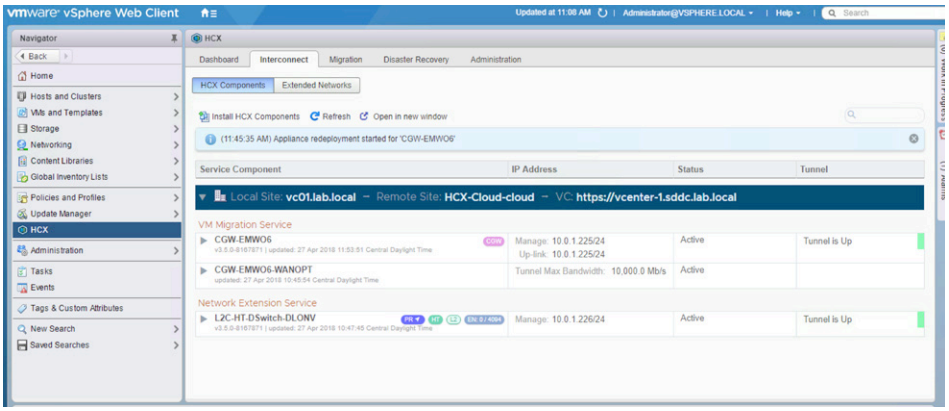


The NSX Hybrid Connect Manager appliances will automatically begin the installation of the service appliances.

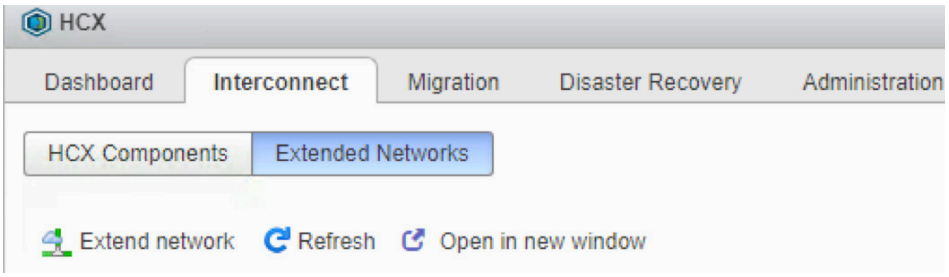
Monitor the installation of the appliances from the vSphere Web Client and watch the active tasks. Alternatively, watch the NSX Hybrid Connect **Interconnect** dashboard to check the status of the NSX Hybrid Connect appliance installation.



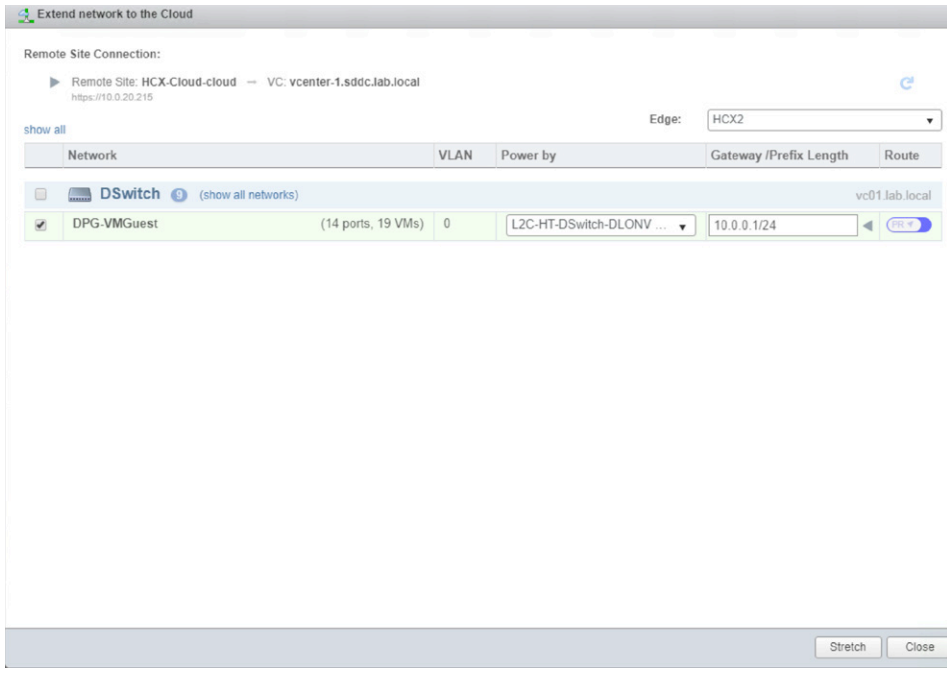
After completion of the automated installation of the NSX Hybrid Connect appliances, log in to the NSX Hybrid Connect **Interconnect** dashboard to verify that the appliances are active and that each hybridity **Tunnel is Up** and greenlit.



The last configuration element to enable live migration requires that the network port group be extended to the NSX Hybrid Connect Manager target site. On the NSX Hybrid Connect dashboard, click **Interconnect** and **Extended Networks**. Click **Extend network** to start the configuration.



Select the distributed port group you want to extend to the Cloud Foundation site. Enter the **Gateway** for that subnet. Then click **Stretch**. The NSX Hybrid Connect Manager will automatically create the distributed port group as a VXLAN inside the Cloud Foundation VDS. After the stretch process is completed, begin live migration to the Cloud Foundation site.



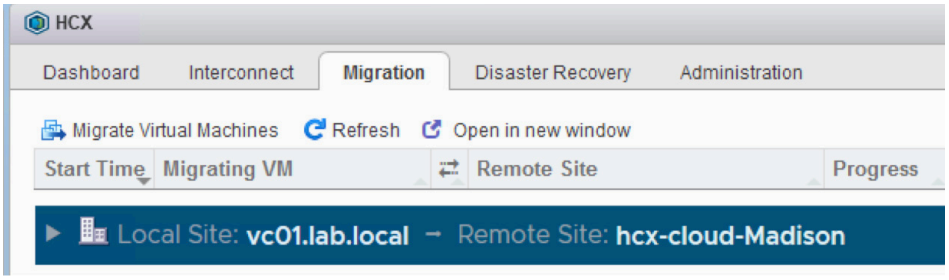
The configuration of both sites for the NSX Hybrid Connect hybridity tunnel is now complete. You are ready to begin migrating workloads to the Cloud Foundation site.

How to Migrate

Bulk Cold Migration

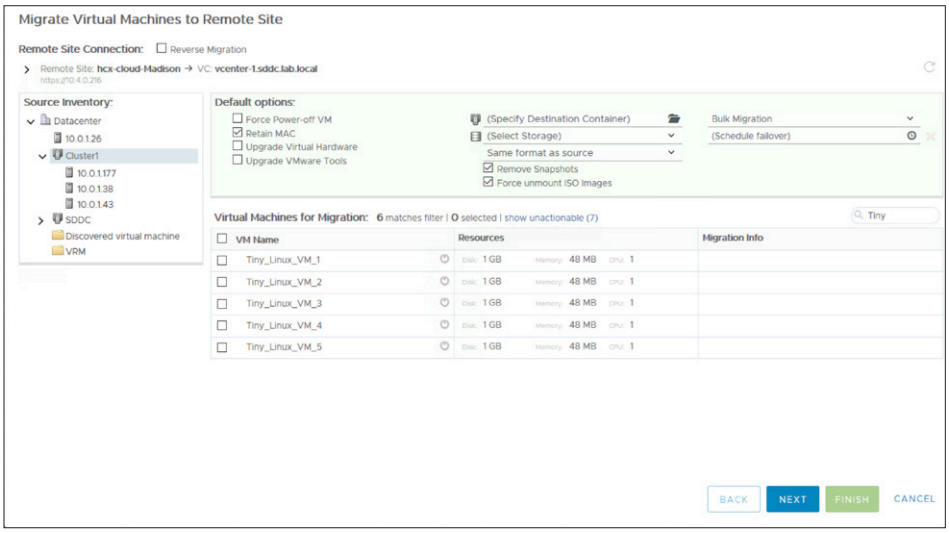
Begin with the **vSphere Web Client** instance for the source site—that is, the legacy vSphere system. On the home screen, click the **NSX Hybrid Connect [HCX] icon**.

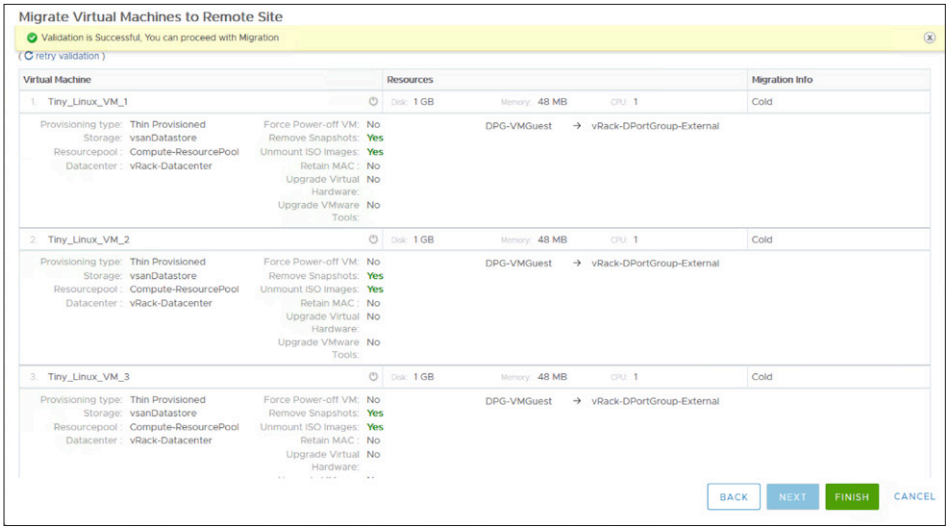
Click **Migration**. Then click **Migrate Virtual Machines**.



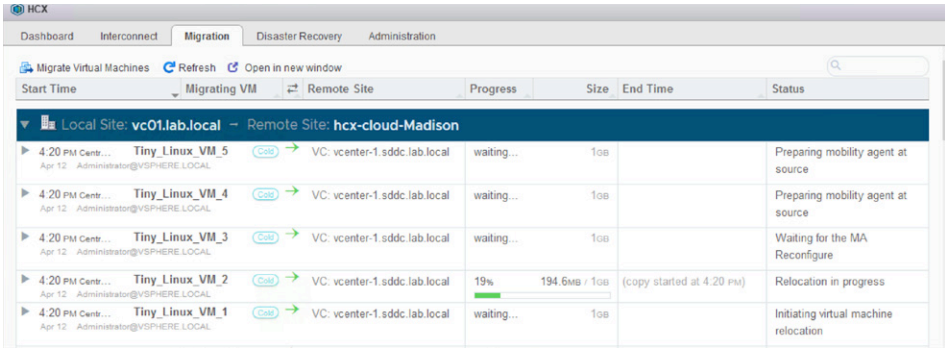
You can now begin the process of VM migration.

This simple-to-use web interface enables selection of either the **Default options** for each VM or unique ones. Click **Next** to verify the destination settings for each VM. Click **Finish** to begin migration.

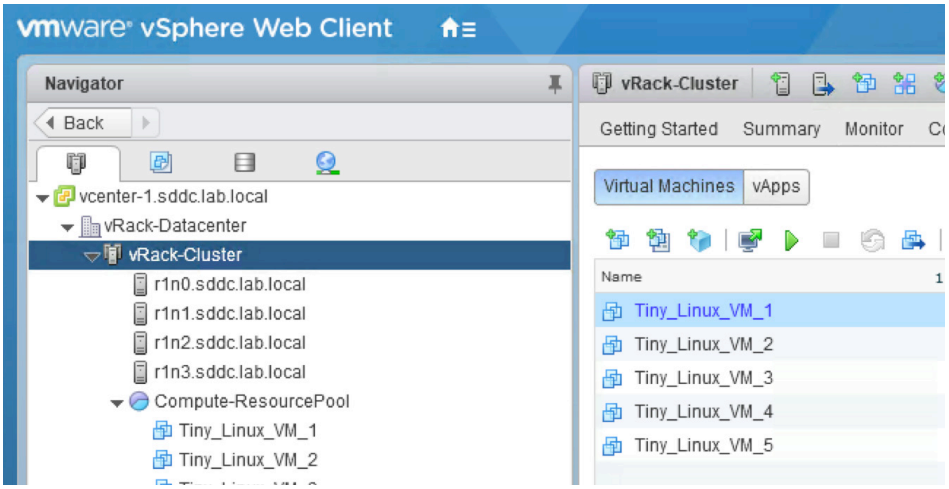




You can now monitor the migration progress for each VM.



When the migration is completed, log in to the vSphere Web Client instance in the Cloud Foundation site and see the migrated VMs.

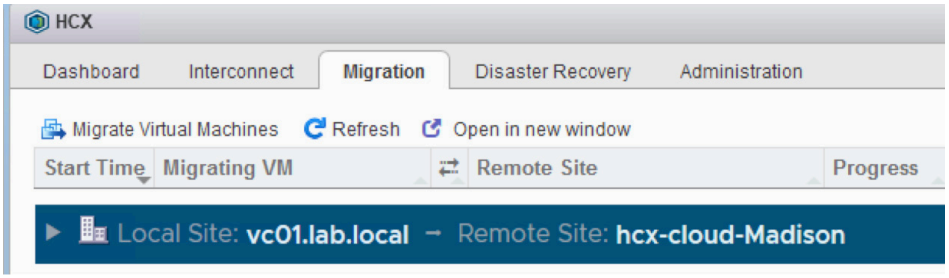


Live Migration

The live migration process is very similar to that for cold migration.

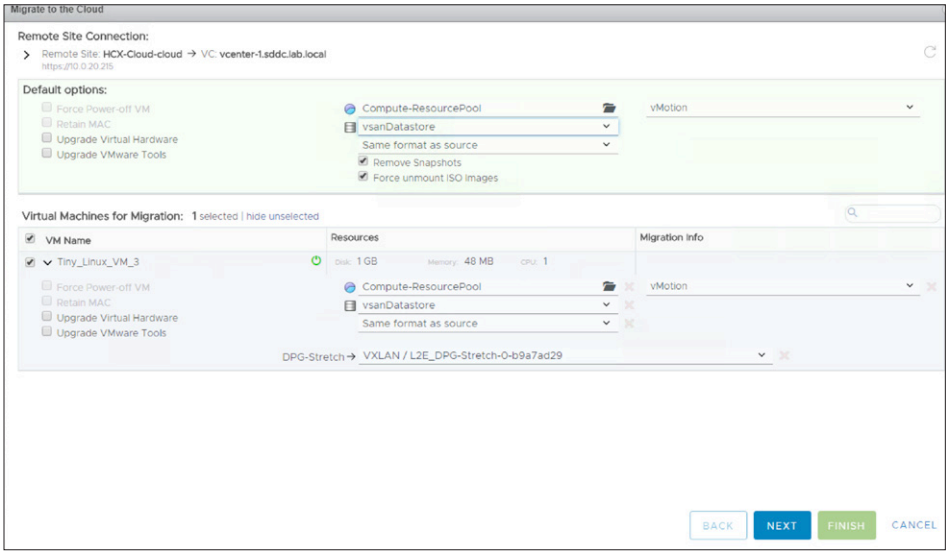
Begin with the vSphere Web Client instance for the source site—that is, the legacy vSphere system. On the home screen, click the **NSX Hybrid Connect [HCX] icon**.

Click **Migration**. Then click **Migrate Virtual Machines**.

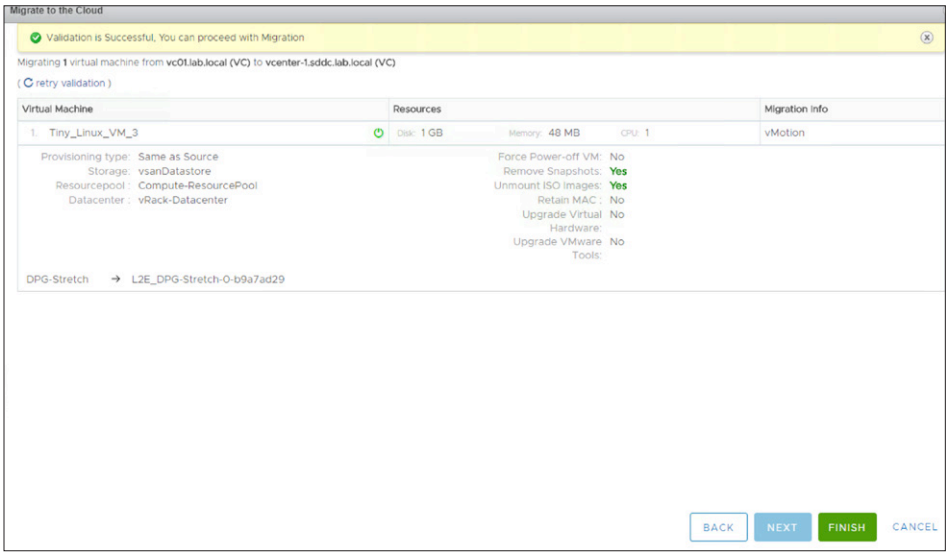


You can now begin the VM migration process. Select the VM(s) you want to live-migrate.

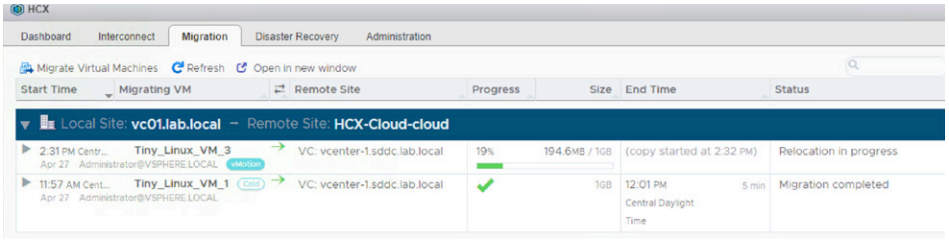
On the far right, select the vSphere **vMotion** option rather than bulk. Click **NEXT**.



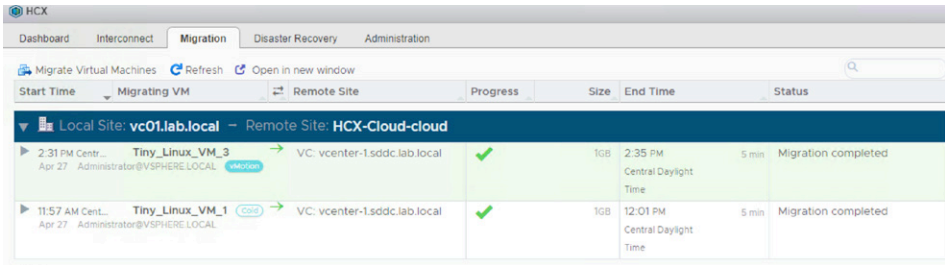
Verify the migration settings and click **FINISH**.



The live migration will now begin. On the NSX Hybrid Connect screen, click **Migration** to review the status.



When the live migration has completed, verify that the migrated VM(s) are now in the Cloud Foundation site.



NSX Hybrid Connect Summary

NSX Hybrid Connect is extremely powerful and easy to use. It enables live migrations and cold migrations to VMware Cloud Foundation sites without the need to re-engineer the physical network infrastructure. This tool quickly creates the hybrid cloud.

Appendix: VM Guest–Setting Considerations

Migrating a guest VM can impact many things. Research the following issues before beginning migration activities.

When migrating a VM to different hardware or different sites, the underlying type of physical hardware will probably change. Newer physical servers can have different CPU types, instruction sets, and core counts. Some customers have tuned their database VMs to the underlying physical CPU NUMA node boundaries. For applications that are NUMA aware, research some of the latest performance-tuning settings for VMs. This article dives deep into best-practice performance settings for VMs.

Enhanced vMotion Compatibility (EVC) mode is another thing to consider with the physical CPU. If EVC mode is turned on in the legacy site but not in the Cloud Foundation site, it is possible to live-migrate to the Cloud Foundation site, but it might not be possible to migrate back because the VM might have acquired a new instruction set from new CPUs. Consider enabling EVC mode in Cloud Foundation to enable migration to and from Cloud Foundation instances.

When migrating to another site, consider any other local application dependencies that the VM might communicate with. Cloud Foundation Enterprise includes vRealize Network Insight, which can enable development of application dependency maps to itemize entities a VM might be communicating with.

There are many things to consider before migrating a VM to a new site or infrastructure. The following list provides some guest settings to research that might be affected by their location when migrating VMs. This list might not be all inclusive, but it provides preliminary suggestions for migration planning.

Guest Settings

- NUMA awareness
- EVC mode
- Custom CPU instruction set masking
- DNS settings
- Gateway
- Microsoft Active Directory sites and services for Windows
- Backups
- Agents
- Governance
- Tags

- Firewall rules
- Affinity rules
- Media access control (MAC) address (might be tied to software licensing)
- VMware vSphere Network I/O Control
- VMware vSphere DirectPath I/O™
- ISO or CD-ROM attachments
- VMware vSphere virtual machine encryption (VM encryption)
- Fibre Channel NPIV
- Custom swap file location

About the Author

Heath Johnson is a senior technical marketing manager based in southern Wisconsin. He has been with VMware since 2015 and is a three-time vExpert. Heath has worked with VMware products since 2004 and started his virtualization journey as a customer with VMware ESXi version 2.1. When he is not working, he spends time with his family, flies airplanes and drones, cycles, and enjoys the outdoors. Follow Heath on his personal blog at www.FlyingVirtually.com or on Twitter @heathbarj.

Acknowledgments

For excellent sample code that contains more options for migration and goes much deeper into using the powerful Cross vCenter vMotion API, see William Lam's blog. And special thanks to William and to Vishal Gupta for all their work on the Fling migration tool.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

8/18