

MULTICLOUD WORKLOAD MIGRATION STRATEGIES WITH VMWARE CLOUD FOUNDATION™

Table of Contents

Introduction	4
Scope	4
Migration Strategy	4
Migration Types	5
Live Migration	5
Cold Migration	5
Migration Direction	6
VMware Cloud Foundation Bill of Materials	6
Cloud Foundation Network Topology	7
Migration Tool Options	8
VMware API – vSphere PowerCLI – Cross vCenter vMotion	10
Overview	10
Requirements	10
Architecture	10
Installation	11
Migration	11
Summary	13
Cross vCenter Workload Migration Utility Fling	14
Overview	14
Architecture	14
Installation on Cloud Foundation	15
Summary	18
vSphere Replication	18
Architecture	18
Installation	19
Migration – Target Site	19
Migration – Source Site	24

Configuration.....	25
How to Use	25
Summary.....	34
Using Third-Party NAS Storage as Cold Migration Intermediary	34
Overview.....	34
Architecture	34
Installation.....	35
Migration.....	35
Summary.....	36
NSX Hybrid Connect	37
Overview.....	37
Architecture	37
Installation – NSX Hybrid Connect Manager Target (Cloud Foundation Site)	39
Installation – NSX Hybrid Connect Manager Source (Legacy vSphere Site).....	67
Configuration.....	77
Creating the Hybridity Tunnel.....	81
How to Migrate	88
Bulk Cold Migration.....	88
Live Migration.....	90
NSX Hybrid Connect Summary	92
Appendix: VM Guest-Setting Considerations	93
Guest Settings.....	93
About the Author	94
Acknowledgments	94

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	<ul style="list-style-type: none"> • No downtime • No changes to the guest OS or application 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Most flexible • Enables changing IPs as well as upgrading VM compatibility and VMware Tools versions • Enables use of new hardware features 	<ul style="list-style-type: none"> • 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.

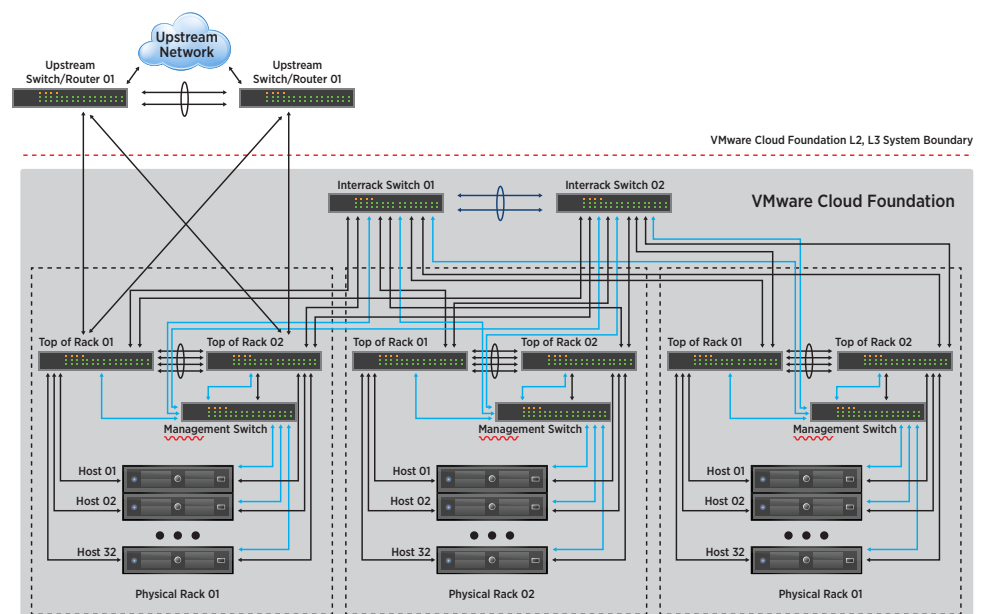


Figure 1. Physical Network Topology for Cloud Foundation Version 2.3

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.

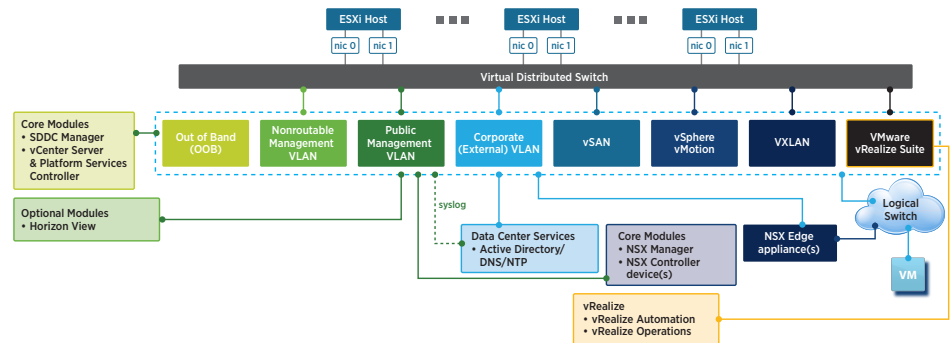


Figure 2. Software-Defined Logical Network Topology Implemented with Cloud Foundation Version 2.3

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.

Live Migration Choices

Requires L2 Extended into Cloud Foundation

Legacy vSphere Version	API	Fling	vSphere Replication	NAS	NSX Hybrid Connect
5.5					✓
6.0 GA, U1, U2					✓
6.0 U3	✓	✓			✓
6.5	✓	✓			✓

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.

Cold or Low-Downtime Migration Choices

Legacy vSphere Version	API	Fling	vSphere Replication	NAS	NSX Hybrid Connect
5.5				✓	✓
6.0 GA, U1, U2				✓	✓
6.0 U3	✓	✓		✓	✓
6.5	✓	✓	✓	✓	✓

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.

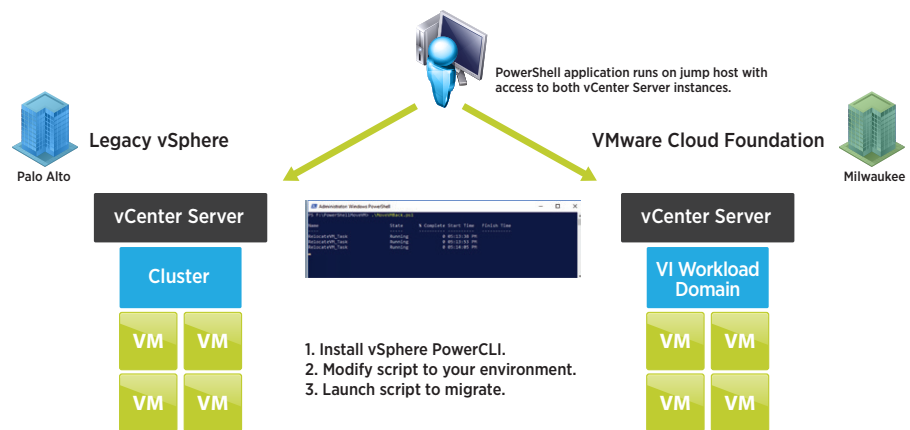


Figure 5. API Migration Architecture Overview

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.

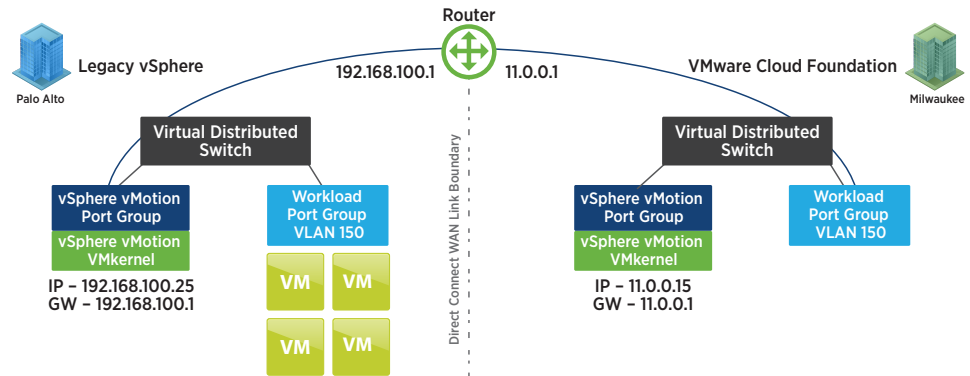


Figure 6. Network Architecture for API Live Migration

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"
$targetVCPasssword = "VMware!"
#####

#####Source Virtual Center#####
$sourceVCName = "vc01.lab.local"
$sourceVCUsername = "administrator@vsphere.local"
$sourceVCPasssword = "VMware!"
#####
```

```
#####Target Information#####
####Enter the specific ESXi host you want to migrate to
$vmhost = "rln0.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.

```
Administrator: Windows PowerShell
PS F:\PowerShellMoveVM> .\MoveVMBack.ps1

Name                               State      % Complete Start Time   Finish Time
----                               -
RelocateVM_Task                    Running    0 05:13:38 PM
RelocateVM_Task                    Running    0 05:13:53 PM
RelocateVM_Task                    Running    0 05:14:05 PM
```

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

Recent Tasks			
Task Name	Target	Status	
Relocate virtual machine	Tiny_Linux_VM_3	100 %	✕
Relocate virtual machine	Tiny_Linux_VM_2	100 %	✕
Relocate virtual machine	Tiny_Linux_VM_1	93 %	✕
Initiate vMotion receive operation	Tiny_Linux_VM_4	✓ Completed	
Initiate vMotion receive operation	Tiny_Linux_VM_3	✓ Completed	

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.

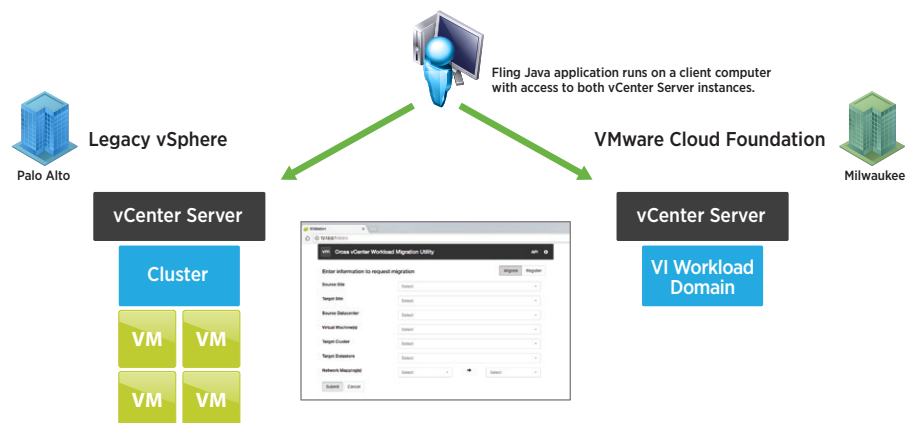


Figure 7. Architecture Overview Using Cross vCenter Workload Migration Utility Fling

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.

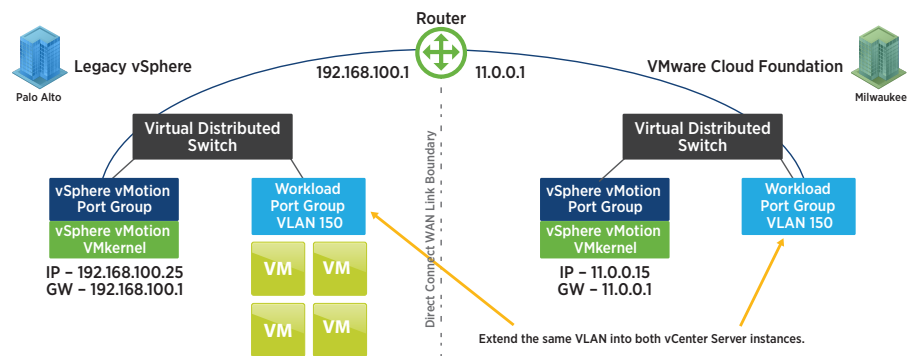


Figure 8. Network Architecture Showing VLANs and L3 Routes

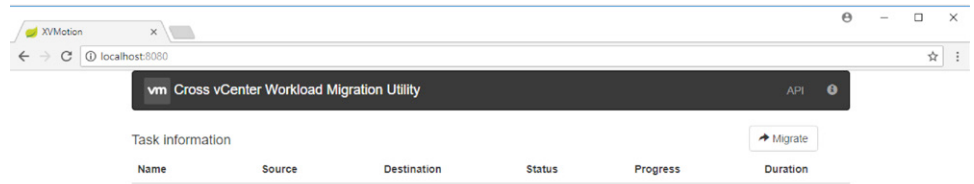
Installation on Cloud Foundation

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.

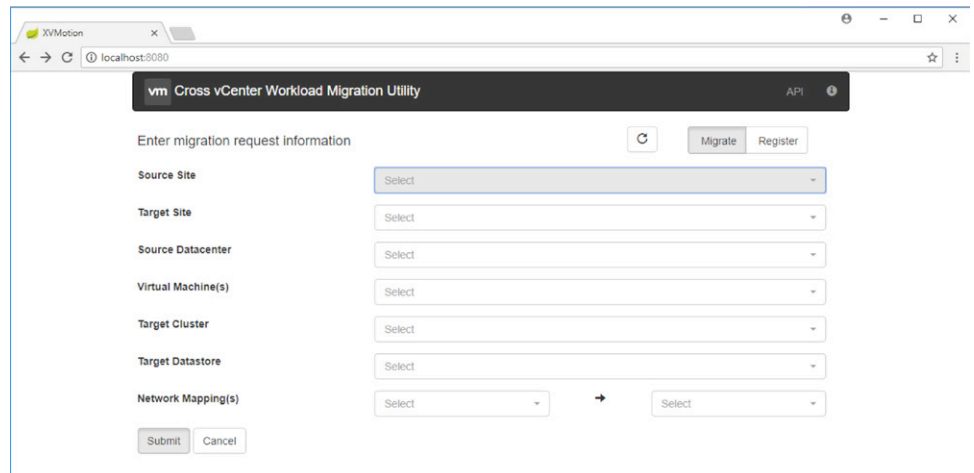
```
Administrator: Windows PowerShell
PS C:\Users\administrator.LAB> cd F:\xvm\
PS F:\xvm> java -jar .\xvm-1.1.jar
08:19:49 INFO Starting ApiController on Win10 with PID 6248 (F:\xvm\xvm-1.1.jar started by administrator in F:\xvm)
08:19:49 DEBUG Running with Spring Boot v1.5.1.RELEASE, Spring v4.3.6.RELEASE
08:19:49 INFO No active profile set, falling back to default profiles: default
08:19:52 INFO HV000001: Hibernate Validator 5.3.4.Final
08:19:59 INFO Starting service Tomcat
08:19:59 INFO Starting Servlet Engine: Apache Tomcat/8.5.11
08:20:01 INFO Initializing Spring embedded WebApplicationContext
08:20:07 INFO Context refreshed
08:20:07 INFO Found 1 custom documentation plugin(s)
08:20:07 INFO Scanning for api listing references
08:20:08 INFO Initializing ProtocolHandler ["http-nio-8080"]
08:20:08 INFO Starting ProtocolHandler [http-nio-8080]
08:20:08 INFO Using a shared selector for servlet write/read
08:20:08 INFO Started ApiController in 20.39 seconds (JVM running for 25.231)
08:20:08 INFO Cross vCenter Workload Migration Utility Initialized!
```

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).



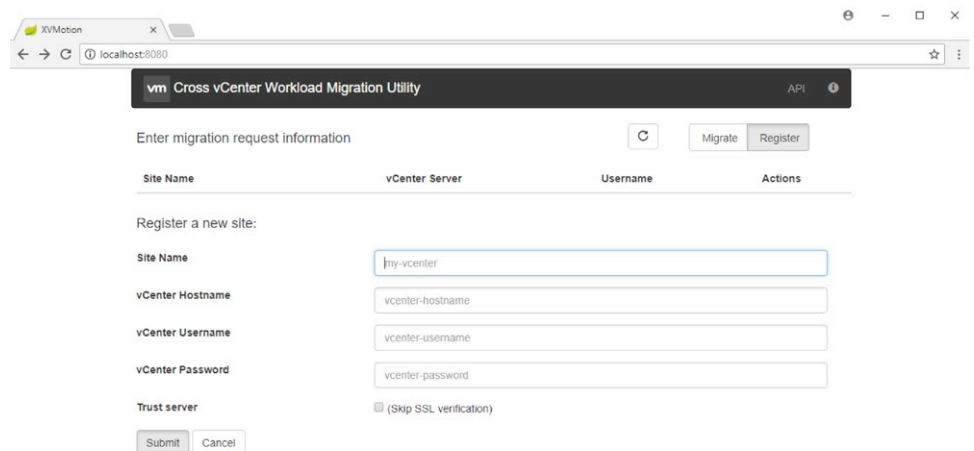
Click **Migrate**.

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.



The screenshot shows the 'Cross vCenter Workload Migration Utility' interface. At the top, there's a header with the VMware logo and the title. Below the header, there's a section titled 'Enter migration request information' with a 'Refresh' button and 'Migrate' and 'Register' buttons. A table lists registered sites:

Site Name	vCenter Server	Username	Actions
Legacy vCenter Server	vc01.lab.local	administrator@vsphere.local	[Icon]
VMware Cloud Foundation	vcenter-1.sddc.lab.local	administrator@vsphere.local	[Icon]

Below the table, there's a 'Register a new site:' section with input fields for 'Site Name' (my-vcenter), 'vCenter Hostname' (vcenter-hostname), 'vCenter Username' (vcenter-username), and 'vCenter Password' (vcenter-password). There's also a 'Trust server' checkbox labeled '(Skip SSL verification)'. At the bottom are 'Submit' and 'Cancel' buttons.

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.

The screenshot shows the 'Cross vCenter Workload Migration Utility' interface with the migration configuration form. The 'Enter migration request information' section has 'Migrate' and 'Register' buttons. The form fields are:

- Source Site:** Legacy vCenter Server (vc01.lab.local)
- Target Site:** VMware Cloud Foundation (vcenter-1.sddc.lab.local)
- Source Datacenter:** Datacenter
- Virtual Machine(s):** Tiny_Linux_VM_3
- Target Cluster:** vRack-Cluster (vRack-Datacenter)
- Target Datastore:** vsanDatastore
- Network Mapping(s):** DPG-Stretch (selected) and vRack-DPortGroup-External (available)

At the bottom are 'Submit' and 'Cancel' buttons.

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.

vm Cross vCenter Workload Migration Utility						API	
Task information						Migrate	
Name	Source	Destination	Status	Progress	Duration		
Tiny_Linux_VM_5	Legacy vCenter Server	VMware Cloud Foundation	success	100%	124s		

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.

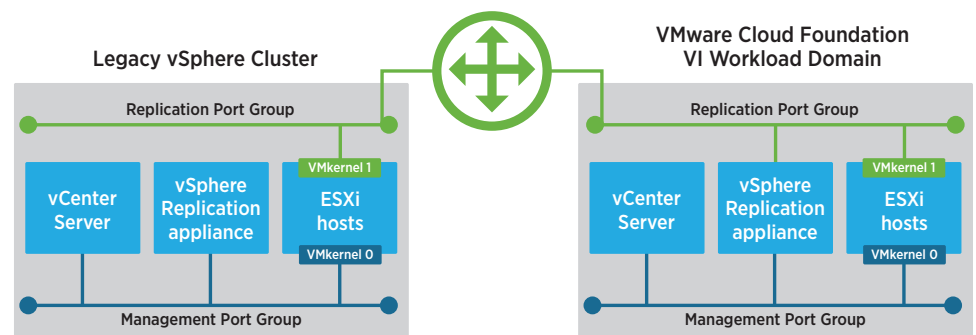


Figure 9. vSphere Replication Architecture Overview

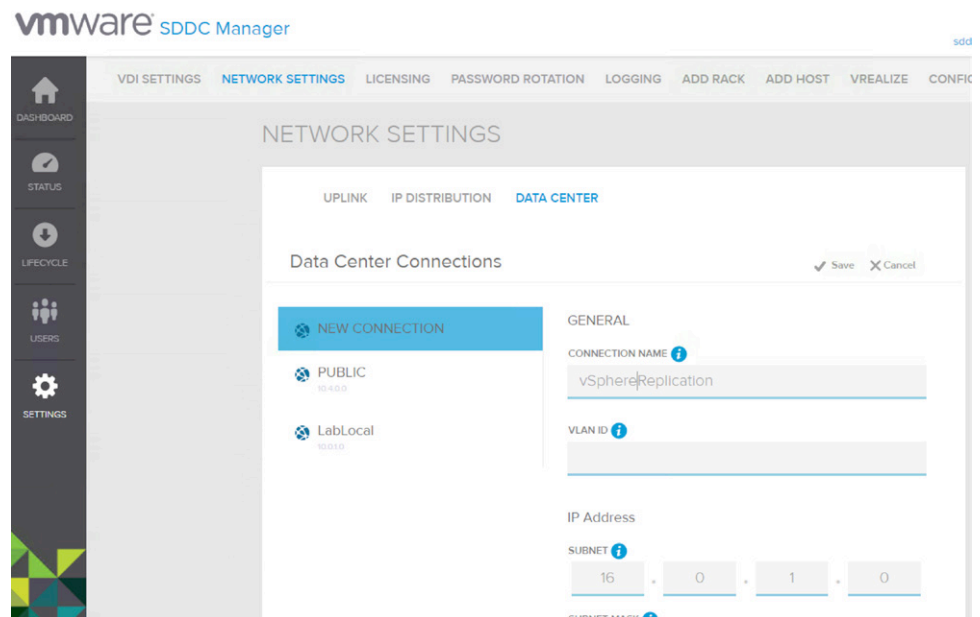
Installation

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.

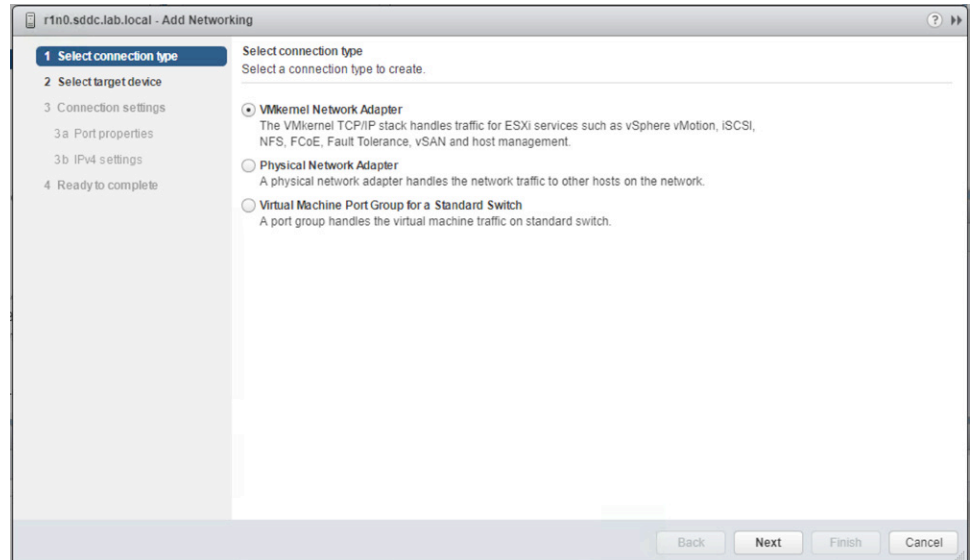
Install the vSphere Replication appliance on the Cloud Foundation instance with the default settings outlined in vSphere Replication documentation. After completing the appliance installation, power it on once to verify that it has configured its network adapter. Then power off the appliance and add 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.

The screenshot shows the 'vSphere Replication Appliance' management interface. The 'Network' tab is selected, and the 'Address' sub-tab is active. The 'Network Address Settings' section is displayed, showing configuration for the 'eth0' interface. The 'Nameserver Source' is set to 'From Configuration'. The 'Hostname' is 'localhost.localdom'. The 'Preferred DNS Server' is '10.0.1.49'. The 'Domain Name' is 'sddc.lab.local'. The 'Domain Search Path' is 'lab.local sddc.lab.local'. The 'eth0 info' section shows the 'IPv4 Address Type' set to 'Static', the 'IPv4 Address' as '10.4.0.215', the 'Netmask' as '255.255.255.0', and the 'IPv4 Default Gateway' as empty. The 'IPv6 Address Type' is set to 'Auto'. The 'eth1 info' section shows the 'IPv4 Address Type' set to 'Static', the 'IPv4 Address' as '16.0.1.215', the 'Netmask' as '255.255.255.0', and the 'IPv4 Default Gateway' as '10.4.0.1'. The 'IPv6 Address Type' is set to 'Auto'. On the right, the 'Actions' panel contains 'Save Settings' and 'Cancel Changes' buttons.

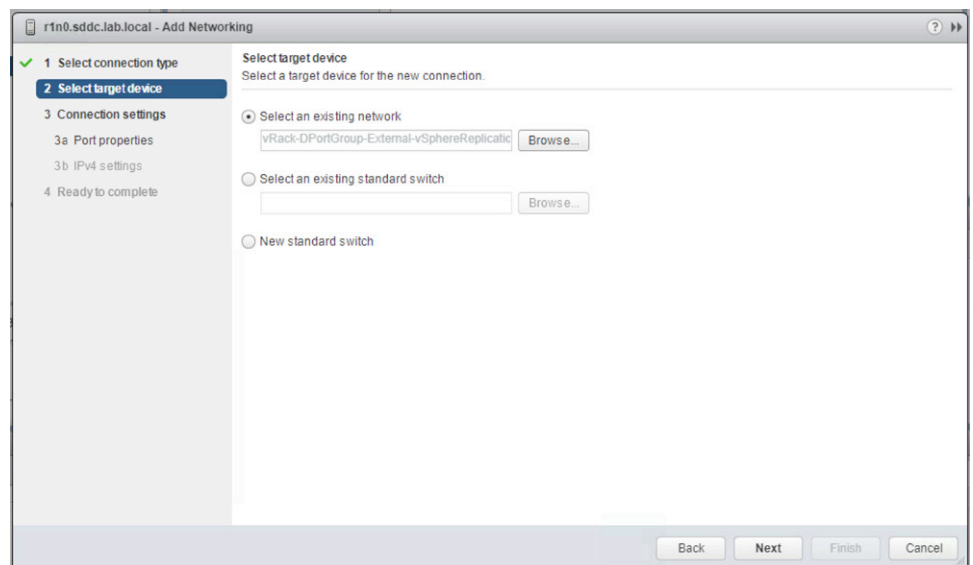
Next, configure the VMkernel adapters for the Cloud Foundation site to receive vSphere Replication traffic from the legacy environment.

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.

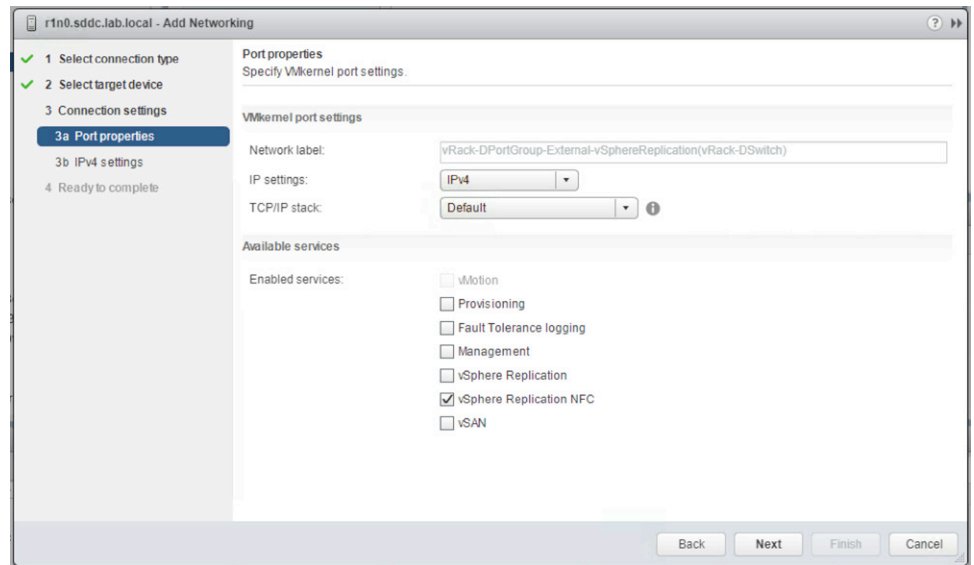
Use the defaults. Click **Next**.



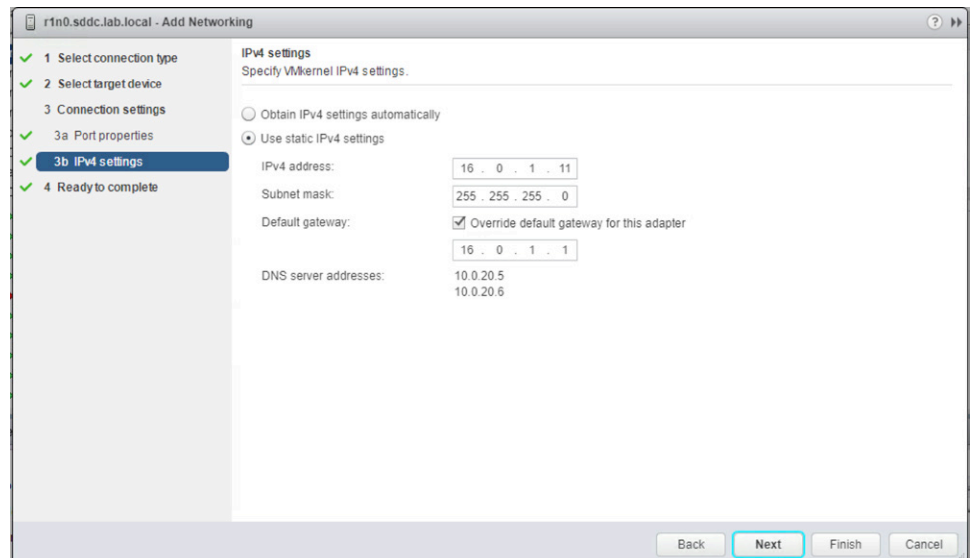
Select the newly created port group for the vSphere Replication appliance. Click **Next**.



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.

vSphere Replication Appliance

VR | Network | Update | System | Application Home | Help | Logout user root

Getting Started | **Configuration** | Security | Support

Startup Configuration

Configuration Mode:

- ☒ Configure using the embedded database
- ☐ Manual configuration
- ☐ Configure from an existing VRM database

LookUpService Address:

SSO Administrator:

Password:

VRM Host:

VRM Site Name:

vCenter Server Address:

vCenter Server Port:

vCenter Server Admin Mail:

IP Address for Incoming Storage Traffic:

SSL Certificate Policy

☐ Accept only SSL certificates signed by a trusted Certificate Authority
(You must click the 'Save and Restart Service' button after changing this setting)

Install a new SSL Certificate

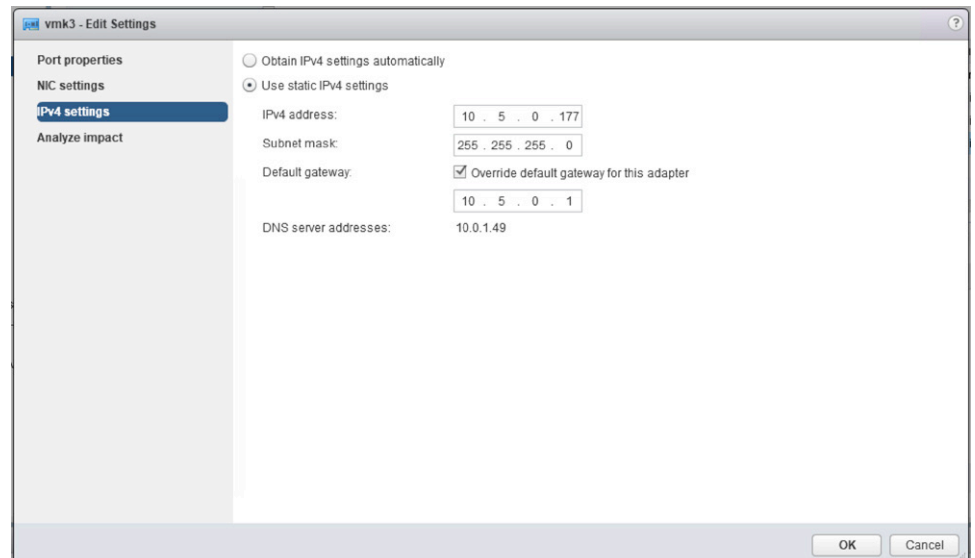
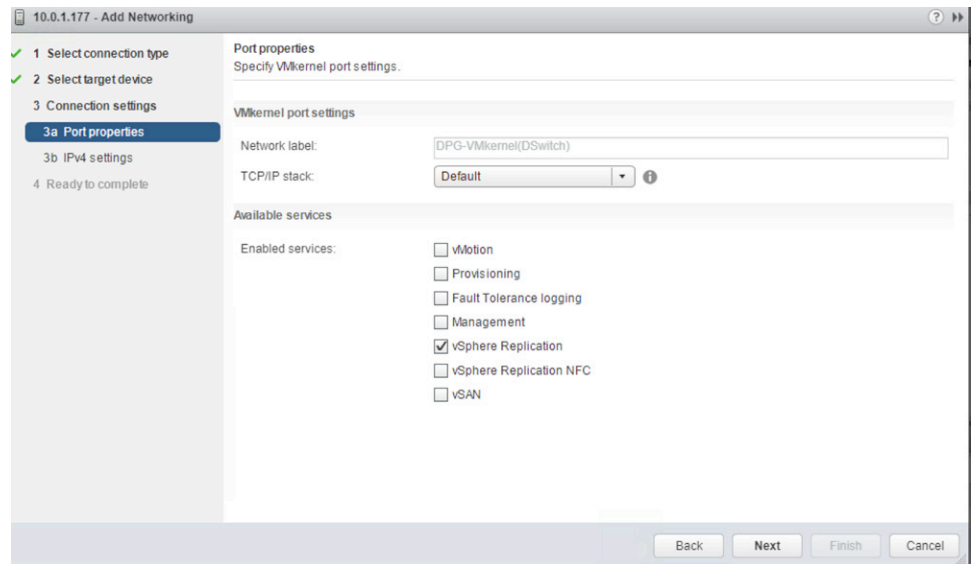
Generate a self-signed certificate

Actions

-
-
-

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.

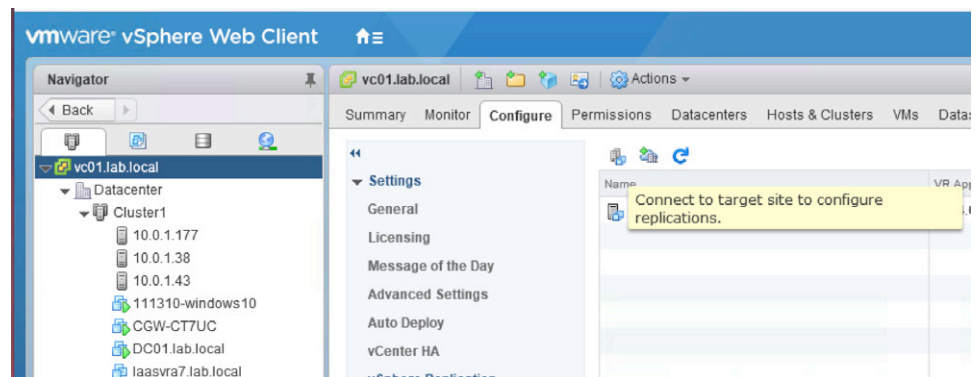
With ESXi hosts prepared in the source site, the vSphere Replication appliance can now be installed by following vSphere Replication documentation. The source site does not require a second network adapter because that is needed only for incoming traffic. All outbound vSphere Replication traffic originates 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.



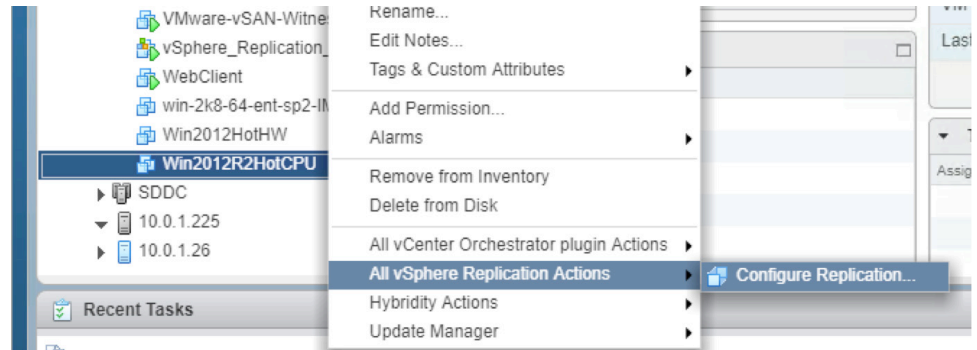
NOTE: Ensure that the DNS name for each site is resolvable from each site.

With the two sites now connected, begin replication.

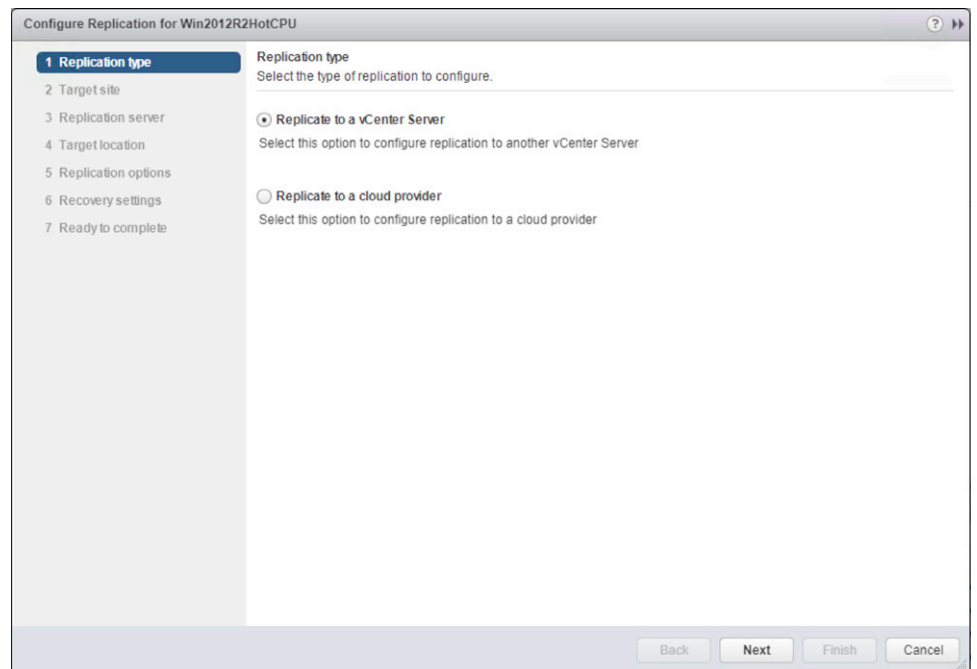
How to Use

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.

The screenshot shows the 'Configure Replication for Win2012R2HotCPU' wizard at Step 2, 'Target site'. The left sidebar shows a progress list with '1 Replication type' and '2 Target site' marked as complete. The main area is titled 'Target site' with the instruction 'Select the target site where the virtual machine will be replicated.' Below this is a table with two columns: 'Name' and 'Status'. Two sites are listed: 'VRepALabLocal' and 'vRepBSddc', both with a status of 'Connected'. The 'vRepBSddc' row is highlighted in blue. At the bottom right of the table area is a button labeled 'Add Remote Site...'. Below the table is a 'Target site validation:' section showing a green checkmark and the text 'Validation succeeded'. At the bottom of the wizard are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

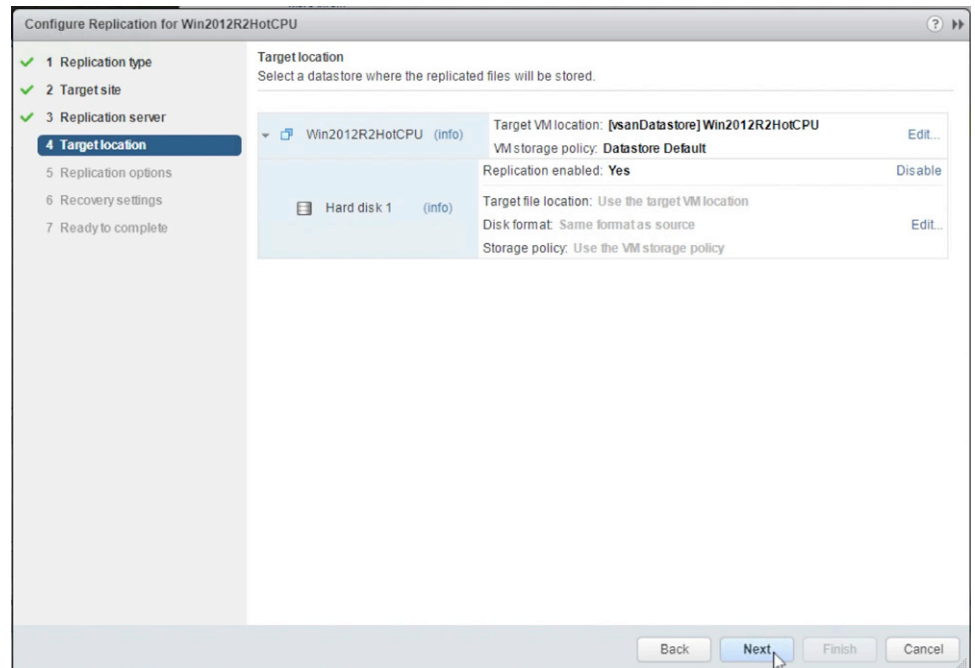
Name	Status
VRepALabLocal	Connected
vRepBSddc	Connected

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

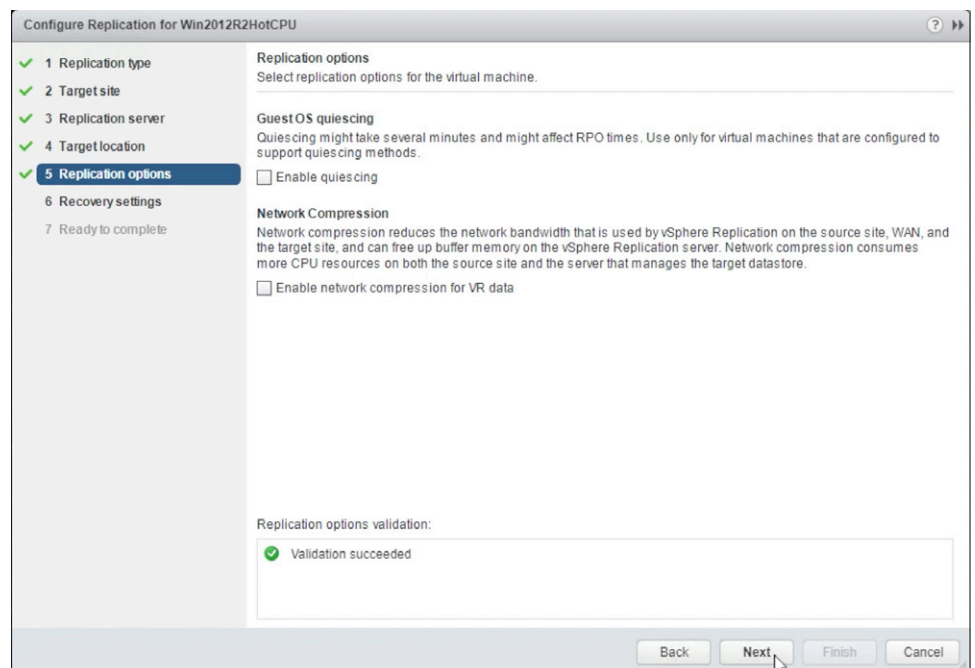
The screenshot shows the 'Configure Replication for Win2012R2HotCPU' wizard at Step 3, 'Replication server'. The left sidebar shows a progress list with '1 Replication type', '2 Target site', and '3 Replication server' marked as complete. The main area is titled 'Replication server' with the instruction 'Select the vSphere Replication sever that will handle the replication.' Below this are two radio buttons: 'Auto-assign vSphere Replication server' (which is selected) and 'Select vSphere Replication server'. Below the radio buttons is a table with two columns: 'Name' and 'Replications'. One entry is listed: 'vSphere_Replication_OVF10 (Embedded)' with a value of '2' in the 'Replications' column. At the bottom of the table area is a 'Replication server validation:' section showing a green checkmark and the text 'Validation succeeded'. At the bottom of the wizard are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

Name	Replications
vSphere_Replication_OVF10 (Embedded)	2

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.

The screenshot shows the 'Configure Replication for Win2012R2HotCPU' wizard at step 6, 'Recovery settings'. The left sidebar shows steps 1 through 7, with step 6 highlighted. The main area is titled 'Recovery settings' and contains the following sections:

- Recovery settings**: Configure recovery settings for the virtual machine.
- Recovery Point Objective (RPO)**: Lower RPO times reduce potential data loss, but use more bandwidth and system resources. A slider is set to 5 minutes, with a range from 5 minutes to 24 hours.
- Point in time instances**: Retained replication instances are converted to snapshots during recovery. Replication of existing VM snapshots is not supported.
 - ☐ Enable
 - Keep 3 instances per day for the last 5 days (15 total)
 - Note: If the RPO period is longer than 8 hours, you might want to decrease the RPO value to allow vSphere Replication to create the number of instances that you want to keep.
- Recovery settings validation**: Validation succeeded (indicated by a green checkmark).

At the bottom, there are buttons for 'Back', 'Next' (highlighted with a mouse cursor), 'Finish', and 'Cancel'.

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

The screenshot shows the 'Configure Replication for Win2012R2HotCPU' wizard at step 7, 'Ready to complete'. The left sidebar shows steps 1 through 7, with step 7 highlighted. The main area is titled 'Ready to complete' and contains the following sections:

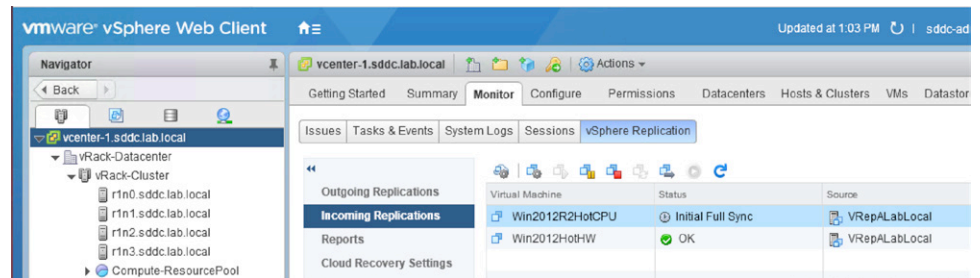
- Ready to complete**: Review your settings selections before finishing the wizard.
- Replication settings**:

Target site name:	vRepBSddc
Replication server:	Auto assign
VM storage policy:	Datastore Default
Target location:	[vsanDatastore] Win2012R2HotCPU
Replicated disks:	1 of 1
Disks with customized settings:	0 of 1
Disks with seeds:	0 of 1
Quiescing:	Disabled
Network compression:	Disabled
- Recovery settings**:

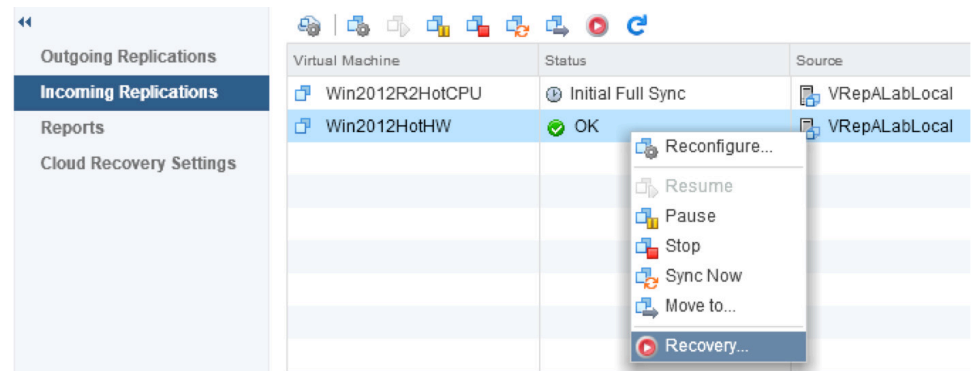
RPO:	5 minutes
Points in time recovery:	Disabled

At the bottom, there are buttons for 'Back', 'Next', 'Finish', and 'Cancel'.

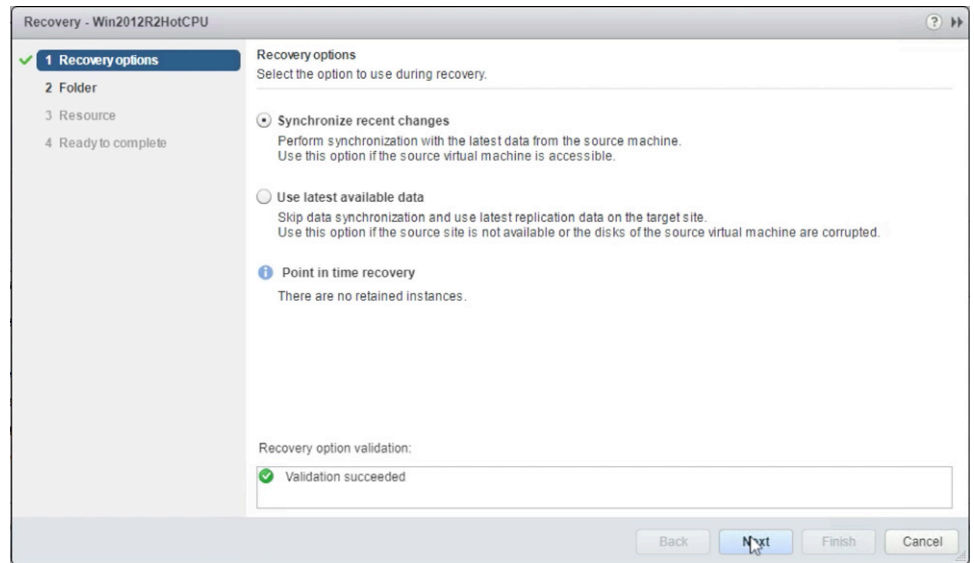
Go to the target vSphere Web Client instance and log in. Navigate to the vCenter Server instance in the navigation tree on the left. Navigate to **Monitor > vSphere Replication > Incoming Replications**.



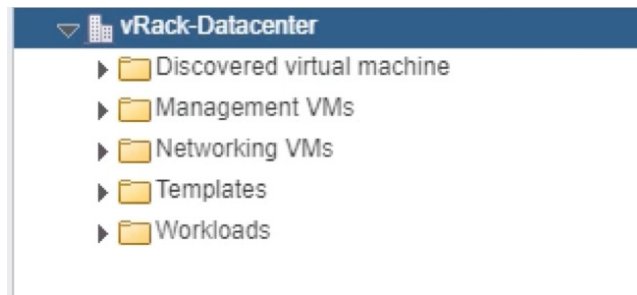
Replication has begun its **Initial Full Sync**. When the sync has completed, begin the migration process: Power off the guest VM. Click **Recovery**.



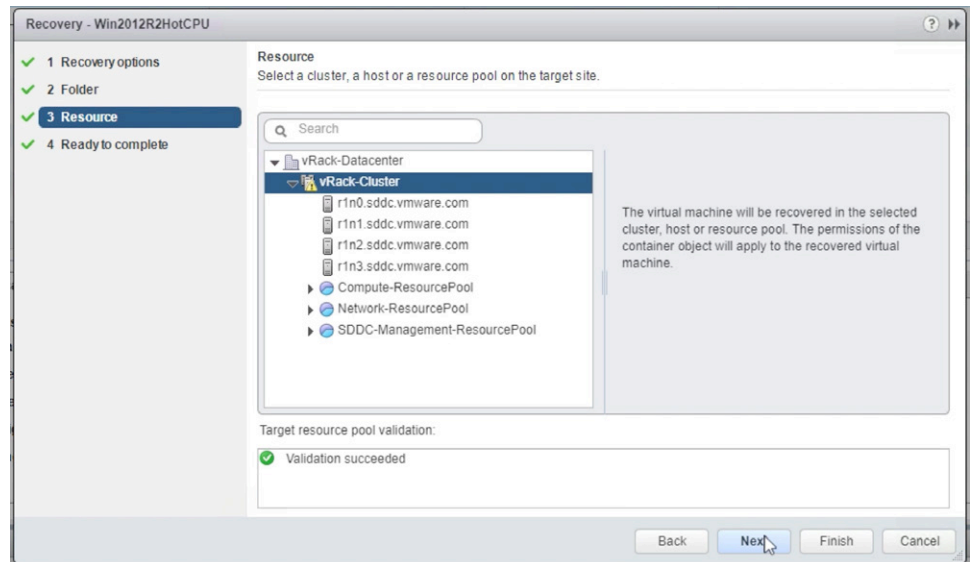
The recovery wizard appears. Work through the process of migrating the VM to the target site. Select the default to **Synchronize recent changes** since the last replication. Click **Next**.



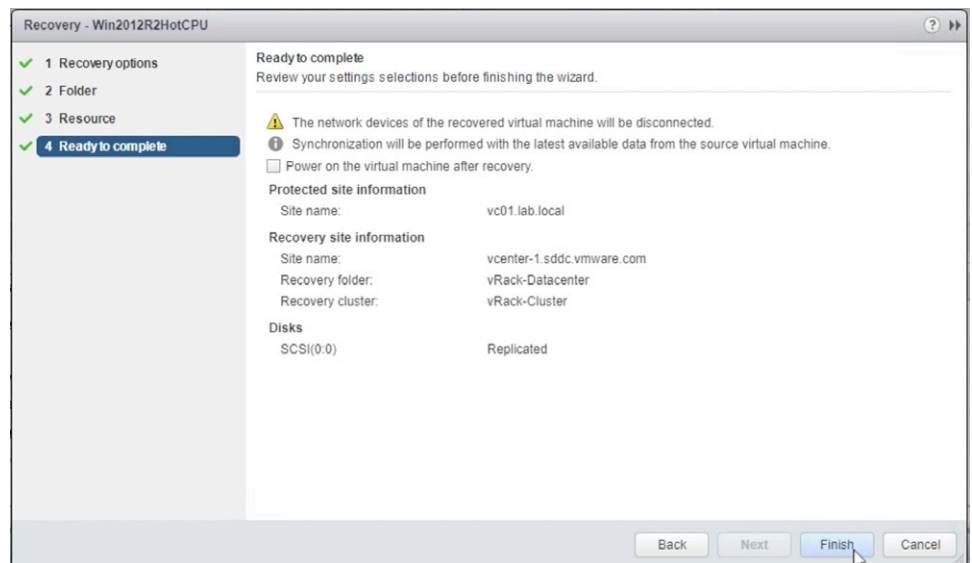
Select the target folder destination for the VM.



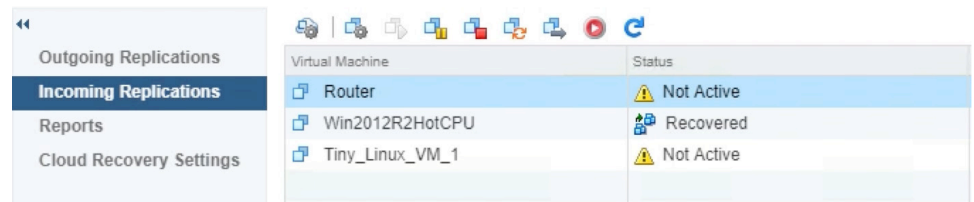
Select the **cluster** or **resource pool** in the target site



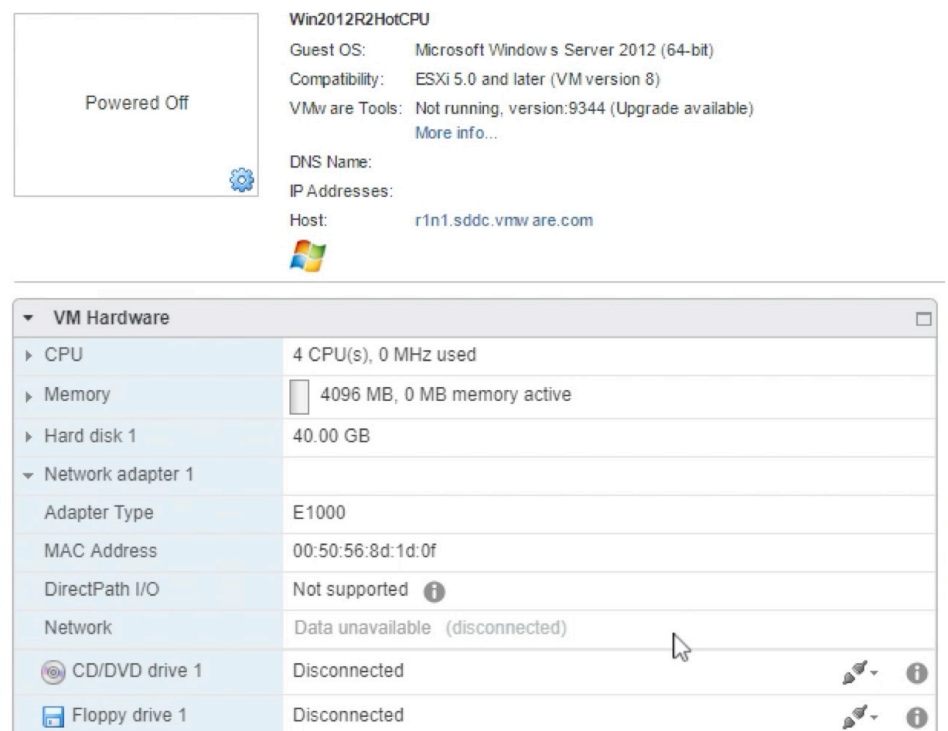
Review all selections. Click **Finish**.



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.

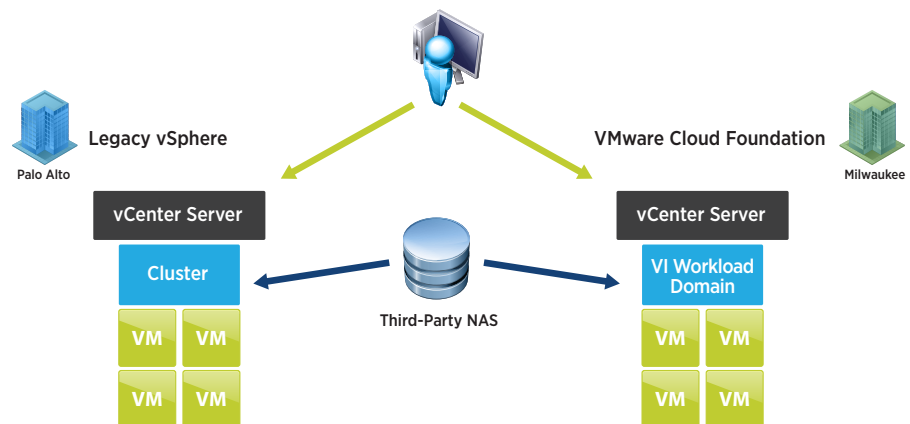


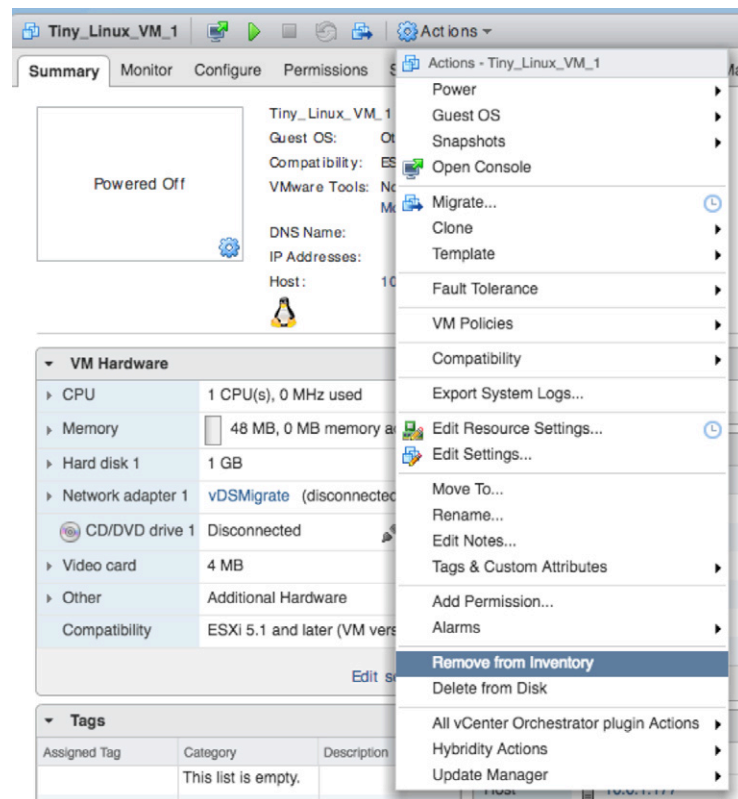
Figure 10. Architecture Overview – Migration Process

Installation

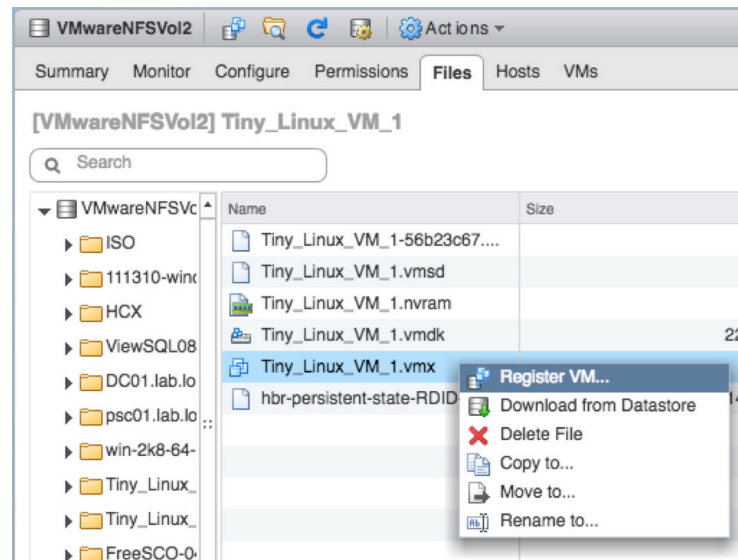
Refer to this [white paper](#) on how to install NAS storage into a Cloud Foundation environment.

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.

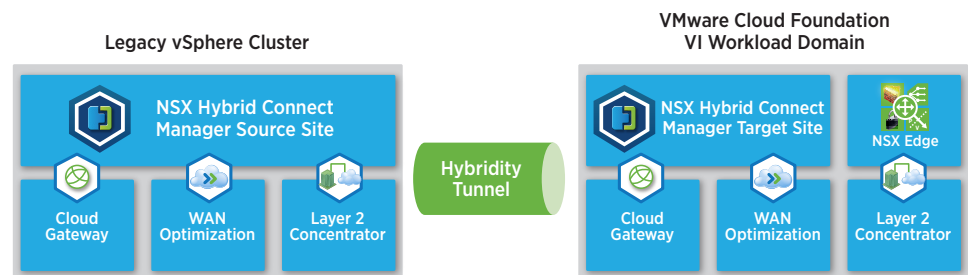


Figure 11. Architecture Overview – NSX Hybrid Connect

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.

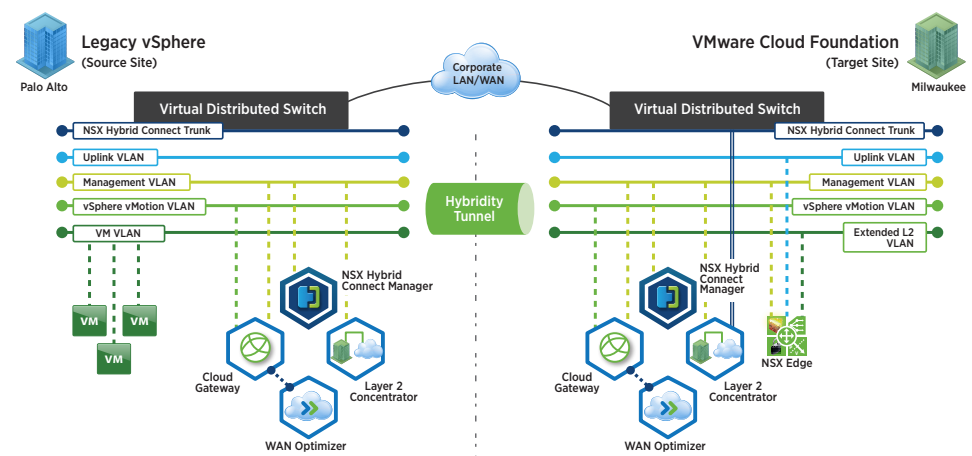


Figure 12. Architecture Overview – NSX Hybrid Connect

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

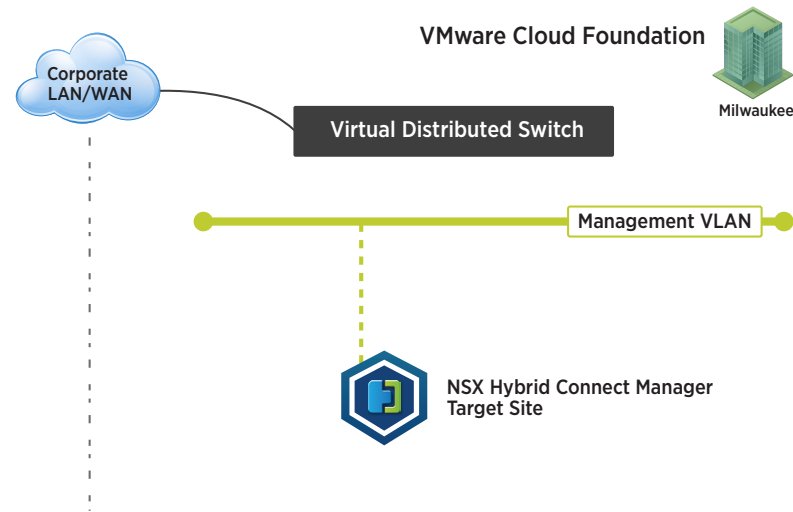
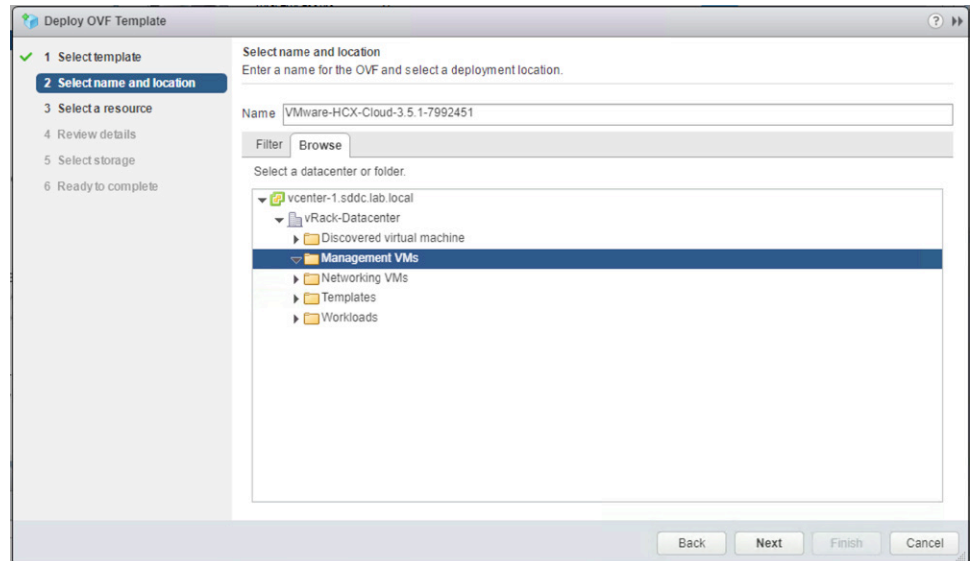


Figure 13. NSX Hybrid Connect Cloud Installation

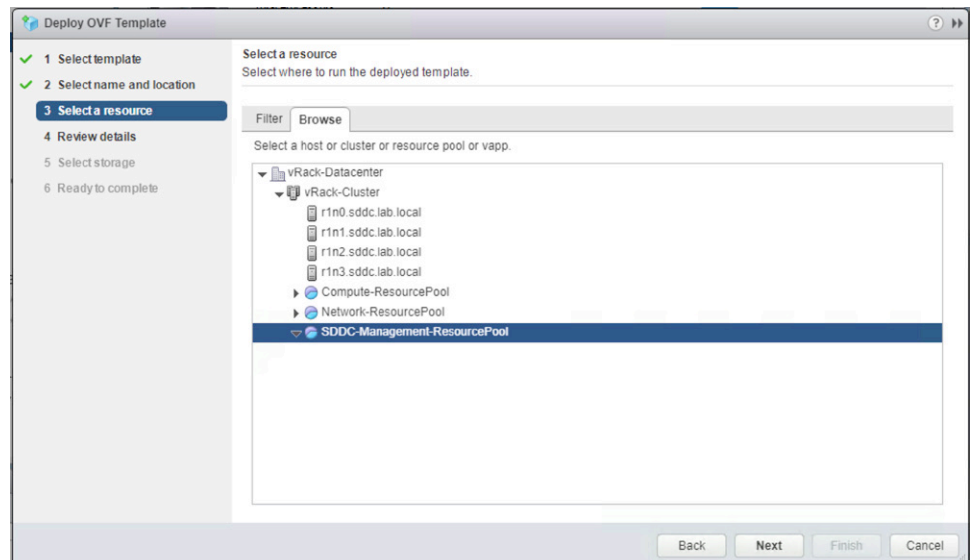
To deploy the NSX Hybrid Connect Manager target appliances in a target Cloud Foundation environment and configure the VLANs, begin by downloading the NSX Hybrid Connect Manager target Open Virtualization Appliance (OVA). Start the installation in the Cloud Foundation site as depicted in Figure 13.

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.

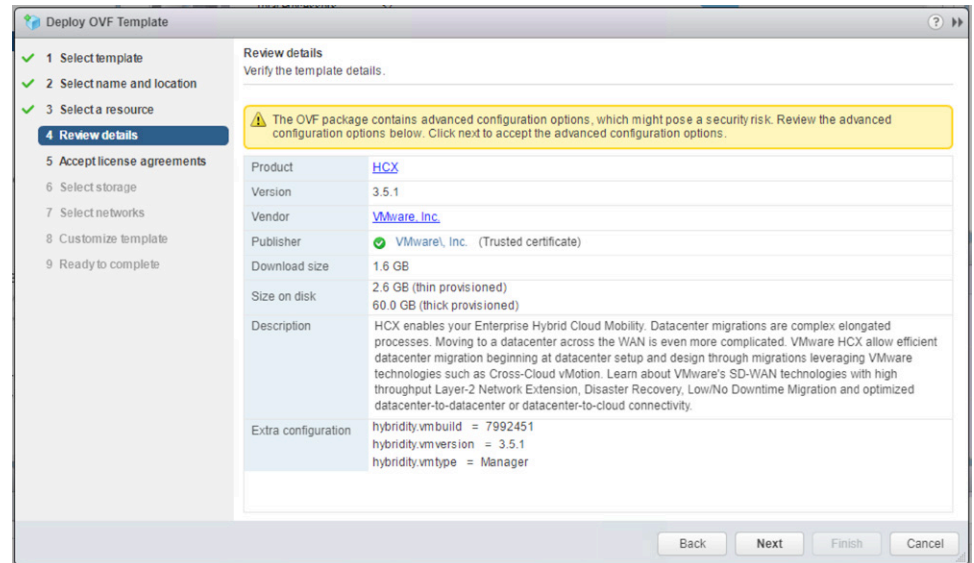
Log in to the management domain vCenter Server instance and install the OVA in the **Management VMs** folder.



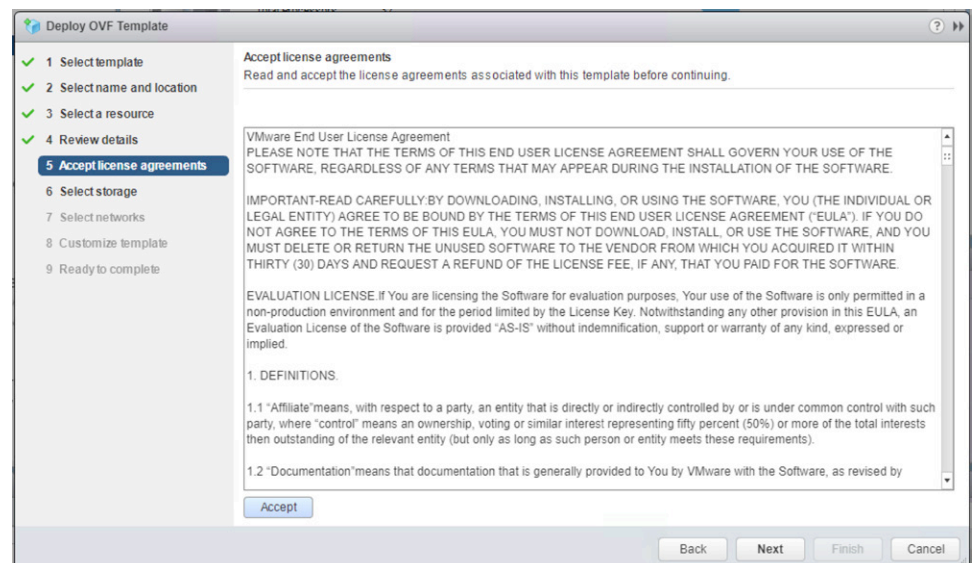
Select the **Management** resource pool.



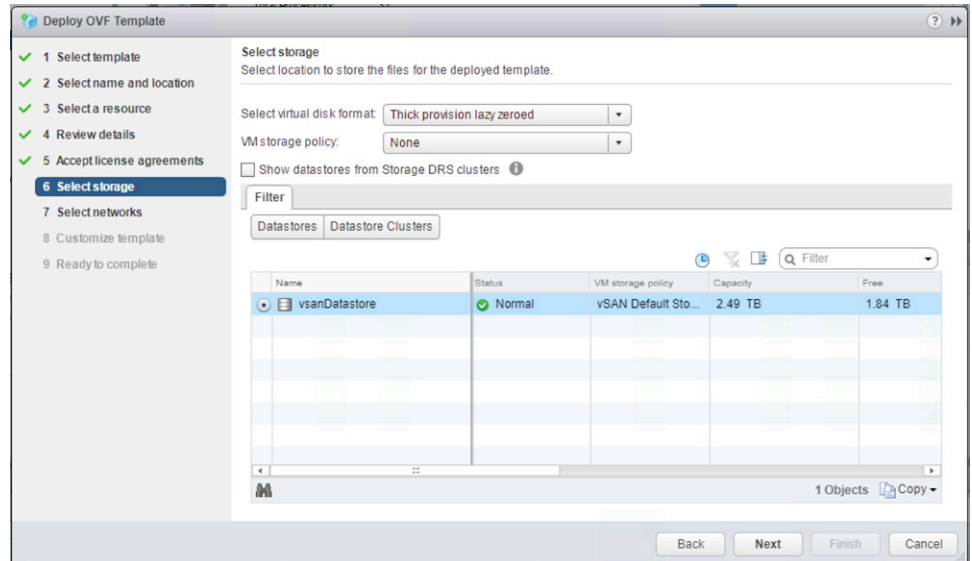
Click **Next**.



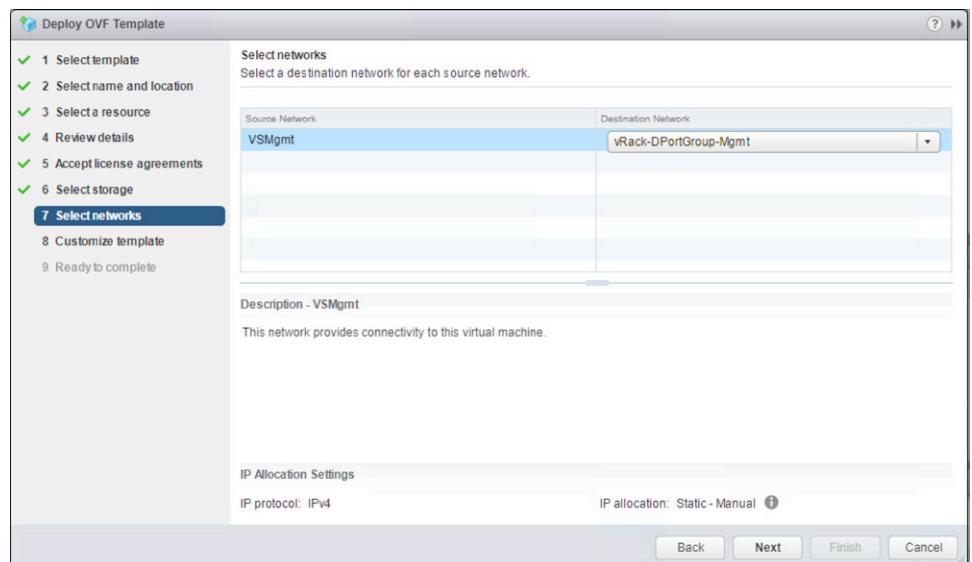
Accept the **VMware End User License Agreement (EULA)**.



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.

Deploy OVF Template

- 1 Select template
- 2 Select name and location
- 3 Select a resource
- 4 Review details
- 5 Accept license agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template**
- 9 Ready to complete

Customize template
Customize the deployment properties of this software solution.

All properties have valid values [Show next...](#) [Collapse all...](#)

Property	Value
DNS (2 settings)	
DNS Server list	The DNS server list(space separated) for this VM. 10.0.20.253
Domain Search List	The domain Search list(space separated) for this VM. sddc.lab.local
Network properties (4 settings)	
Default IPv4 Gateway	The default gateway for this VM. 10.0.20.1
Hostname	The hostname for this VM. HCX-Cloud
Network 1 IPv4 Address	The IPv4 Address for this interface. Leave this empty for DHCP base IP assignment. 10.0.20.215
Network 1 IPv4 Prefix Length	The IPv4 prefix Length for this interface. 24

Back Next Finish Cancel

Review the details and complete the installation.

Deploy OVF Template

- 1 Select template
- 2 Select name and location
- 3 Select a resource
- 4 Review details
- 5 Accept license agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete**

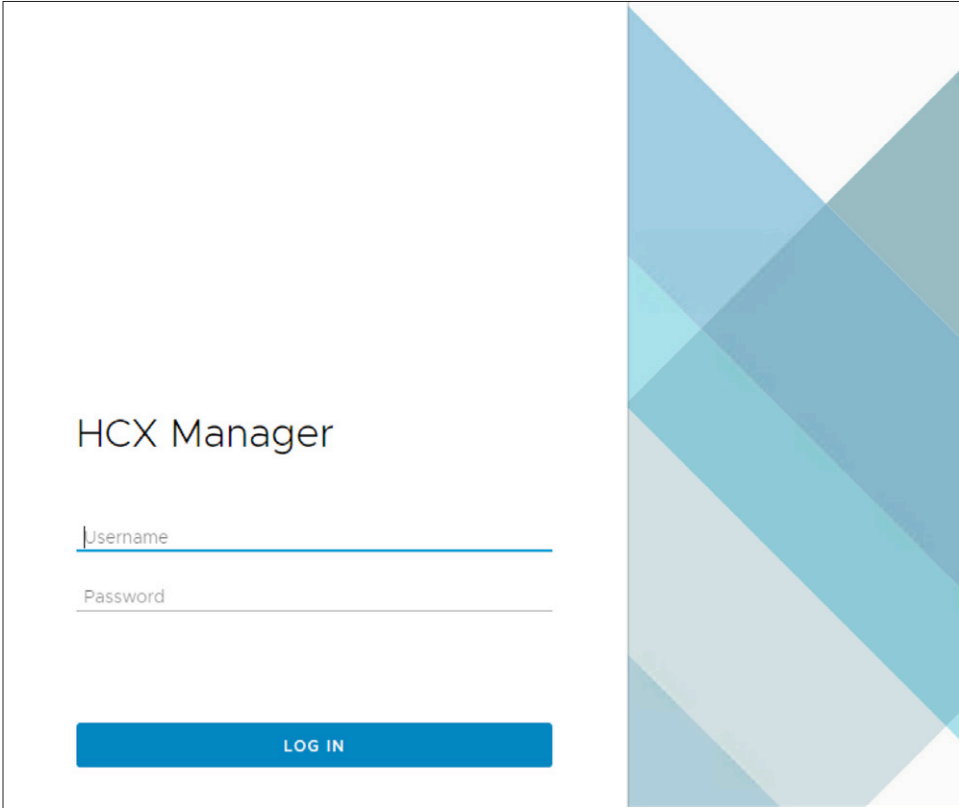
Ready to complete
Review configuration data.

Property	Value
Name	VMware-HCX-Cloud-3.5.1-7992451
Source VM name	VMware-HCX-Cloud-3.5.1-7992451
Download size	1.6 GB
Size on disk	60.0 GB
Folder	Management VMs
Resource	SDDC-Management-ResourcePool
Storage mapping	1
Network mapping	1
IP allocation settings	IPv4, Static - Manual
Properties	DNS Server list = 10.0.20.253 Domain Search List = sddc.lab.local Default IPv4 Gateway = 10.0.20.1 Hostname = HCX-Cloud Network 1 IPv4 Address = 10.0.20.215 Network 1 IPv4 Prefix Length = 24 Enable SSH = True NTP Server List = 10.0.20.5 Static Route 1: Gateway IP Address = Static Route 1: Network = Static Route 1: Prefix Length =

Back Next Finish Cancel

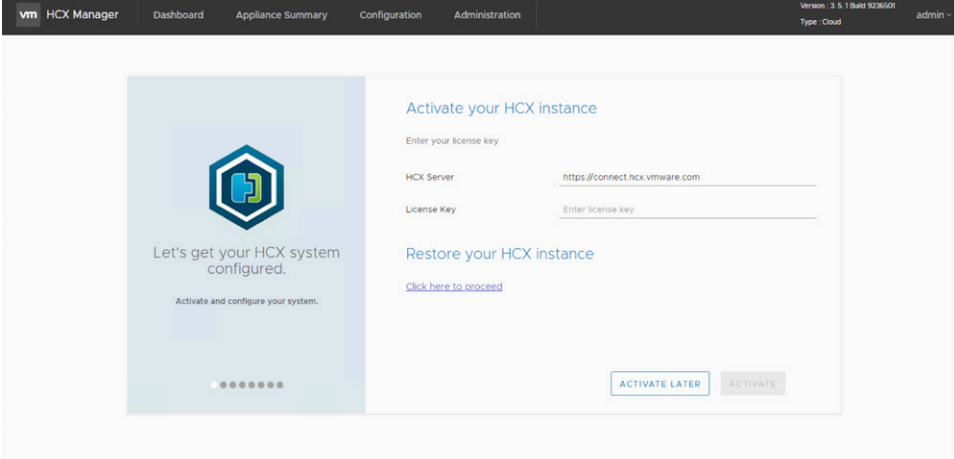
After installation of the OVA has been completed, power on the NSX Hybrid Connect Manager target site appliance.

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.



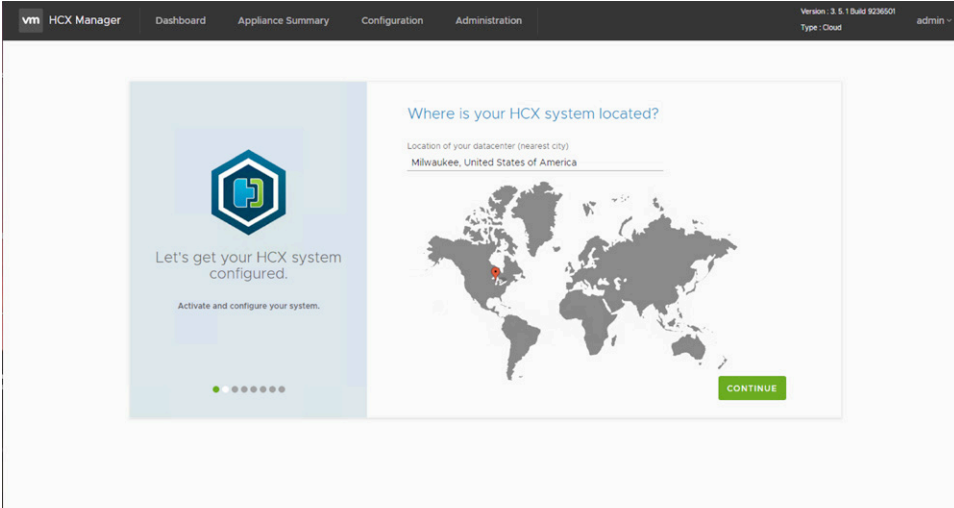
The screenshot displays the login page for HCX Manager. The page has a clean, modern design with a white background and a decorative geometric pattern of overlapping blue and teal triangles on the right side. The text 'HCX Manager' is centered in a large, black, sans-serif font. Below the title, there are two input fields: 'Username' and 'Password', each with a thin blue underline. At the bottom, there is a prominent blue rectangular button with the text 'LOG IN' in white, uppercase letters.

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



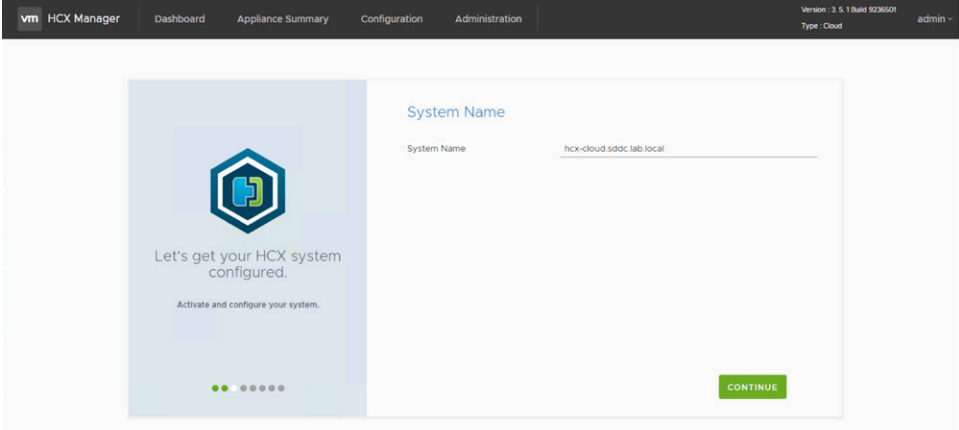
The screenshot shows the HCX Manager web interface. The top navigation bar includes 'vm HCX Manager', 'Dashboard', 'Appliance Summary', 'Configuration', and 'Administration'. On the right, it displays 'Version: 3.5.1 Build 9236501', 'Type: Cloud', and a user profile 'admin'. The main content area is split into two panels. The left panel features the HCX logo and the text 'Let's get your HCX system configured.' with a progress indicator showing the first step is active. The right panel is titled 'Activate your HCX instance' and contains a form with fields for 'Enter your license key', 'HCX Server' (pre-filled with 'https://connect.hcx.vmware.com'), and 'License Key' (with a placeholder 'Enter license key'). Below the form are links for 'Restore your HCX instance' and 'Click here to proceed'. At the bottom right are 'ACTIVATE LATER' and 'ACTIVATE' buttons.

Set the cloud site geographic location.



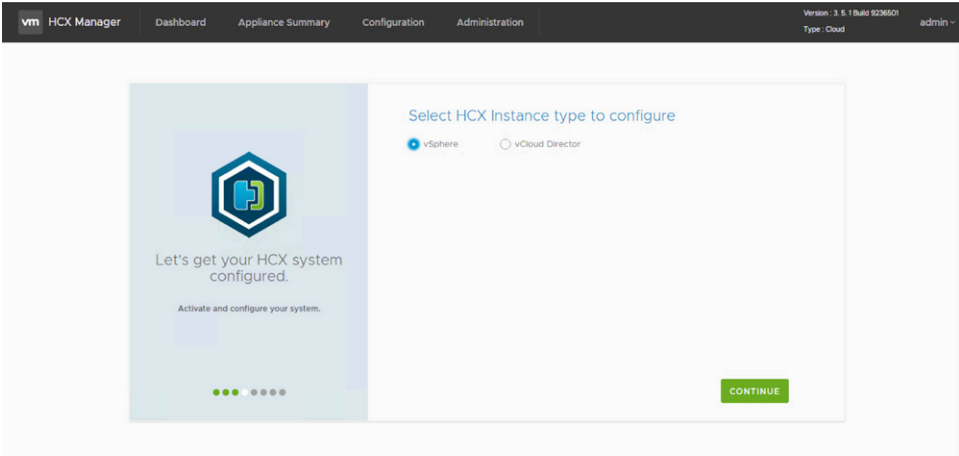
The screenshot shows the next step in the HCX Manager configuration. The navigation bar and version information remain the same. The left panel is identical to the previous screen. The right panel is titled 'Where is your HCX system located?' and asks for the 'Location of your datacenter (nearest city)'. The text 'Milwaukee, United States of America' is entered in the field. Below the text is a world map with a red pin indicating the location in North America. A green 'CONTINUE' button is located at the bottom right of the panel.

Enter the **System Name**.



The screenshot shows the HCX Manager web interface. The top navigation bar includes 'vm HCX Manager', 'Dashboard', 'Appliance Summary', 'Configuration', and 'Administration'. On the right, it displays 'Version: 3.5.1 Build 9236501', 'Type: Cloud', and a user profile 'admin'. The main content area is titled 'System Name'. On the left, there is a blue box with the HCX logo and the text 'Let's get your HCX system configured. Activate and configure your system.' Below this is a progress indicator with five dots, the second of which is filled. On the right, there is a text input field labeled 'System Name' containing the text 'hcx-cloud-sddc-lab-local'. A green 'CONTINUE' button is located at the bottom right of the configuration area.

Select the vSphere installation option.



The screenshot shows the same HCX Manager web interface as the previous one. The main content area is titled 'Select HCX Instance type to configure'. It features two radio button options: 'vSphere' (which is selected) and 'vCloud Director'. The same blue box with the HCX logo and configuration instructions is on the left, and the green 'CONTINUE' button is at the bottom right.

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

The screenshot shows the HCX Manager web interface. The top navigation bar includes 'vm HCX Manager', 'Dashboard', 'Appliance Summary', 'Configuration', and 'Administration'. The right side of the bar shows 'Version: 3.5.1 Build 9236501', 'Type: Cloud', and a user profile 'admin'. The main content area is titled 'Let's get your HCX system configured. Activate and configure your system.' with a progress indicator showing four steps, the second of which is active. The right panel is titled 'Connect your vCenter and NSX' and contains two sections: 'Connect your vCenter' and 'Connect your NSX'. The 'vCenter' section has fields for 'vCenter Server' (https://vcenter-1.sddc.lab.local), 'Username' (administrator@vsphere.local), and 'Password' (masked). The 'NSX' section has fields for 'NSX Manager' (https://10.0.20.20), 'Username' (admin), and 'Password' (masked). A green 'CONTINUE' button is at the bottom right.

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

The screenshot shows the HCX Manager web interface at the 'Configure SSO/PSC' step. The top navigation bar is identical to the previous screenshot. The main content area shows the same progress indicator. The right panel is titled 'Configure SSO/PSC' and has a section 'Identity Sources' with a single text input field containing the URL 'https://psc-1.sddc.lab.local:443/lookupservice/sdk'. A green 'CONTINUE' button is at the bottom right.

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.

vm HCX Manager Dashboard Appliance Summary Configuration Administration 10.0.20.215 Version: 3.5.1 Build 9236501 admin ~
Type: Cloud

Let's get your HCX system configured.
Activate and configure your system.

Configure Public Access URL
Set the public access url to launch the HCX instance

Public Access URL

CONTINUE

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

vm HCX Manager Dashboard Appliance Summary Configuration Administration 10.0.20.215 Version: 3.5.1 Build 9236501 admin ~
Type: Cloud

Let's get your HCX system configured.
Activate and configure your system.

Congratulations!

You need to restart the Application Service and Web Service for your changes to take effect!
Configure the vSphere Roles in the HCX instance after the restart of the services

Your system is up now. Here is the summary of the end points connected to your system.

Location	Milwaukee,United States of America
System Name	hcx-cloud.sddc.lab.local
vCenter	https://vcenter-1.sddc.lab.local
NSX	https://10.0.20.20
SSO	https://psc-1.sddc.lab.local:443/lookupservice/sdk
Public Access URL	https://10.0.20.215

RESTART RESTART LATER

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.

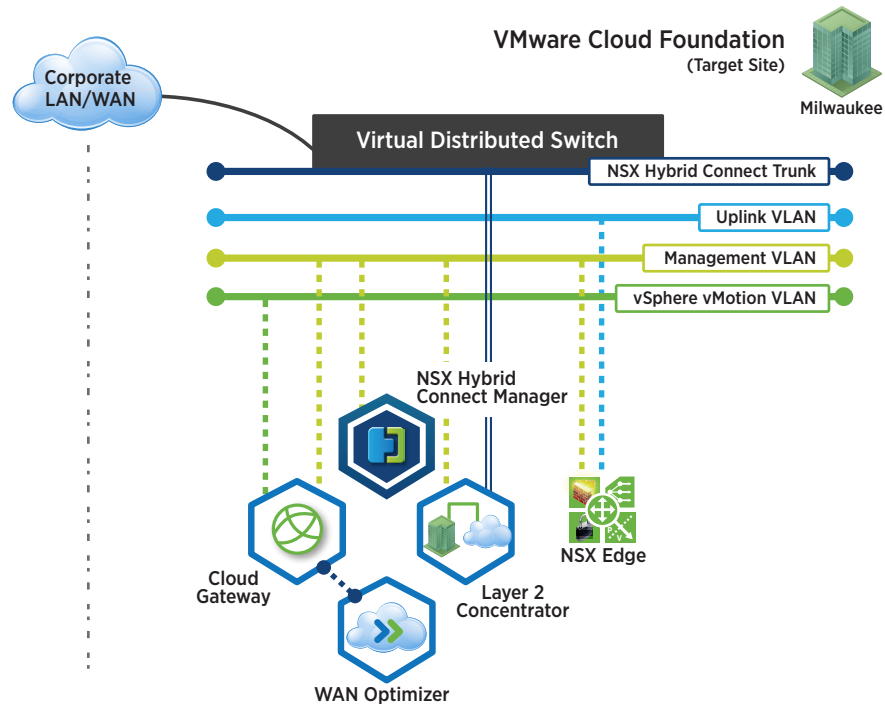
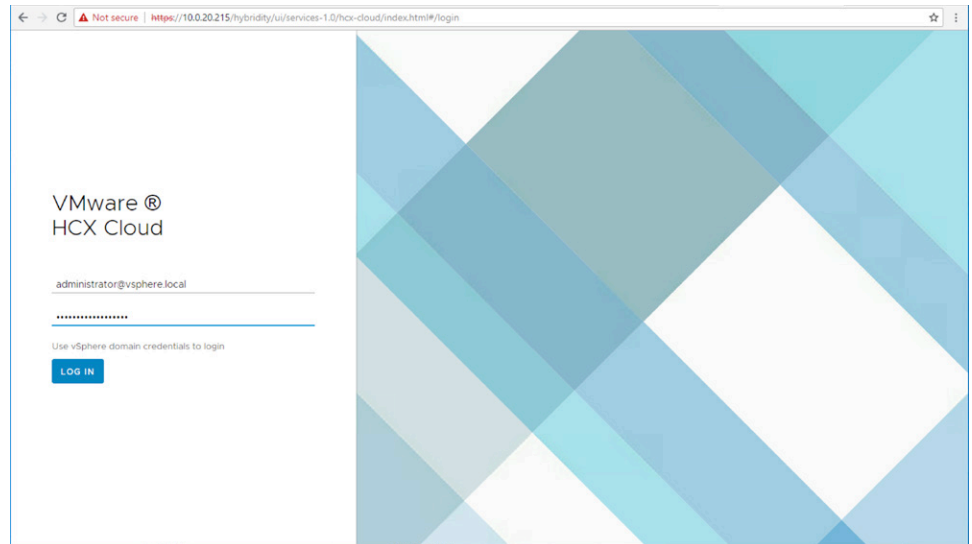
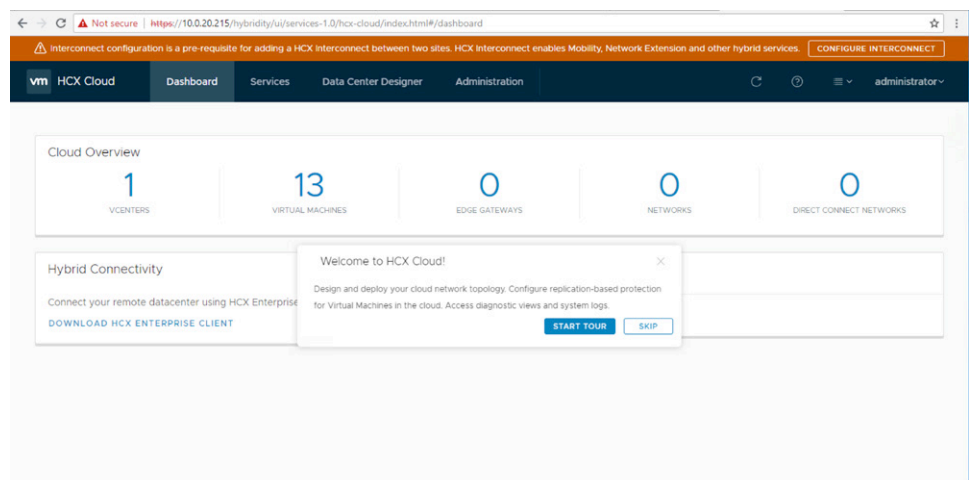


Figure 14. NSX Hybrid Connect Target Site Network Detail

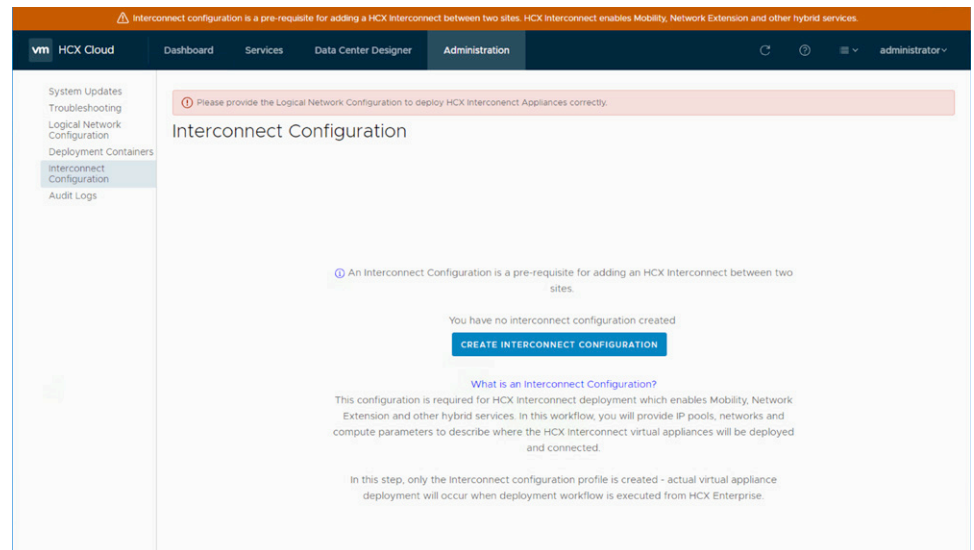
To begin the interconnect configuration, log in to <https://<Hybrid Connect Manager>> with your vSphere credentials.



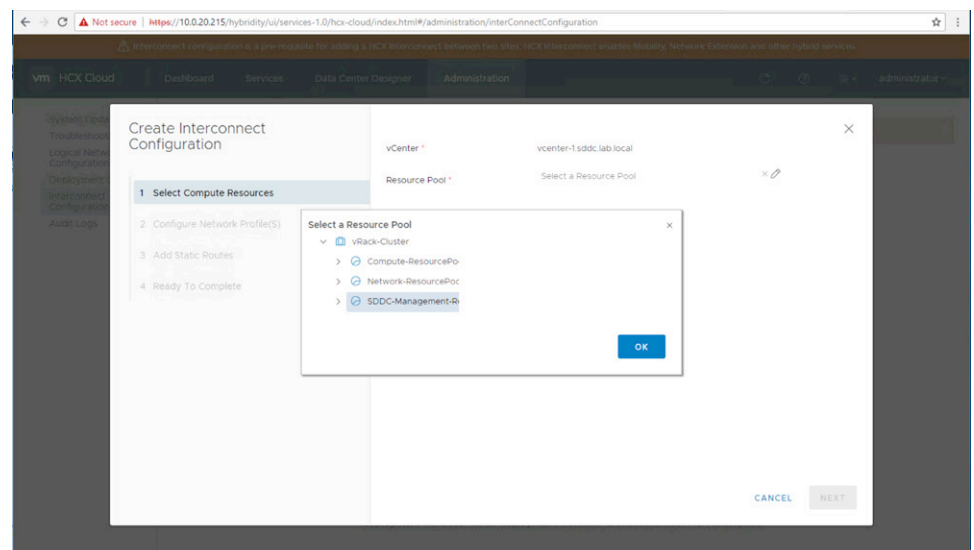
Upon login, the NSX Hybrid Connect Manager target dashboard appears. We see that the interconnect configuration must be completed. Click **CONFIGURE INTERCONNECT**.



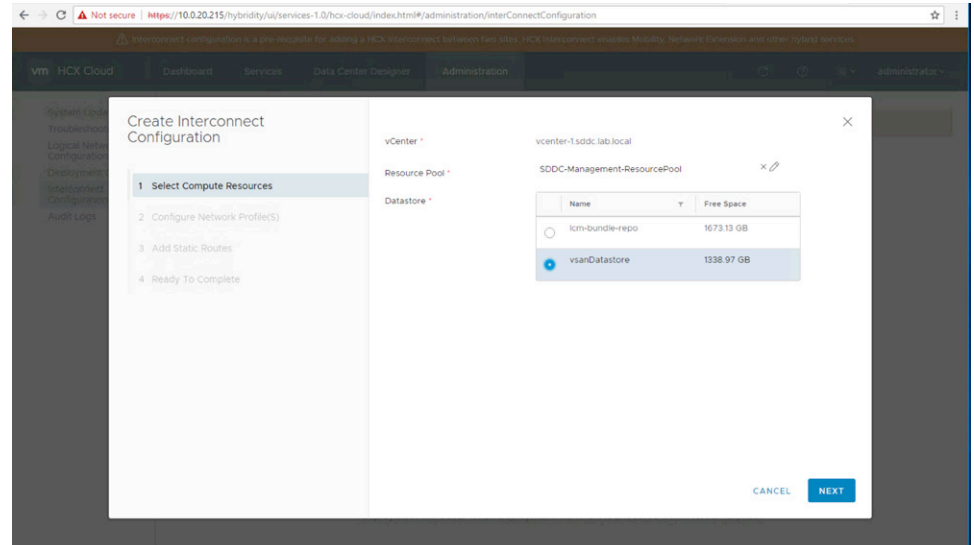
Click **CREATE INTERCONNECT CONFIGURATION**.



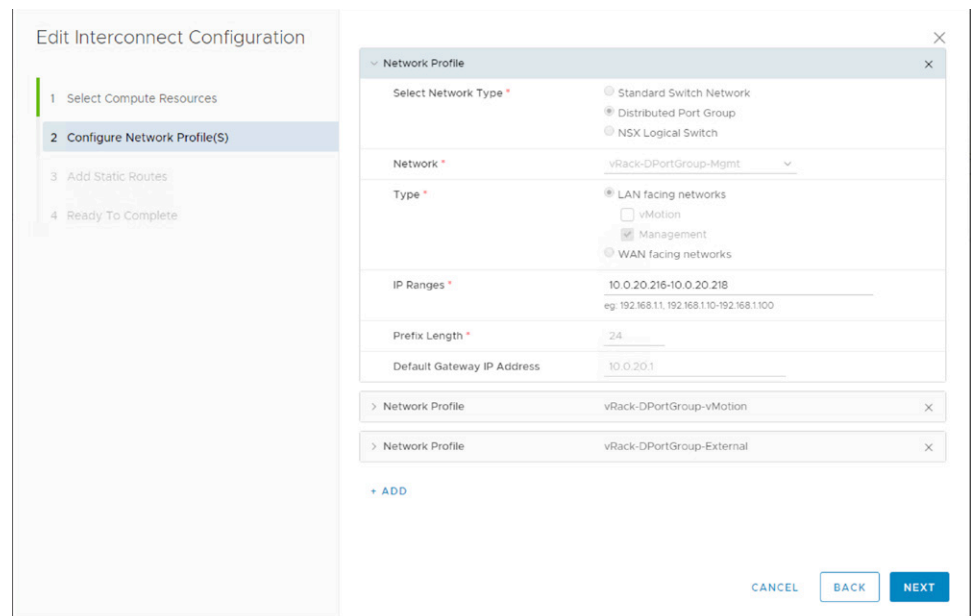
Select a **Resource Pool** into which to deploy the NSX Hybrid Connect appliances.



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.

Edit Interconnect Configuration

- Select Compute Resources
- Configure Network Profile(S)
- Add Static Routes**
- Ready To Complete

Optional Static Route entries can be useful for reaching networks via a network path alternate to the configured default gateway. The Next Hop IP Address must belong to a directly connected network.

[+ ADD](#)

CANCEL

BACK

NEXT

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

Edit Interconnect Configuration

- Select Compute Resources
- Configure Network Profile(S)
- Add Static Routes
- Ready To Complete**

Click Finish to save the configuration changes. Existing interconnect appliances have to be redeployed for the changes to take effect.

vCenter vcenter-1.sddc.lab.local
Resource Pool SDDC-Management-ResourcePool
Datastore vsanDatastore
Network profile(s)

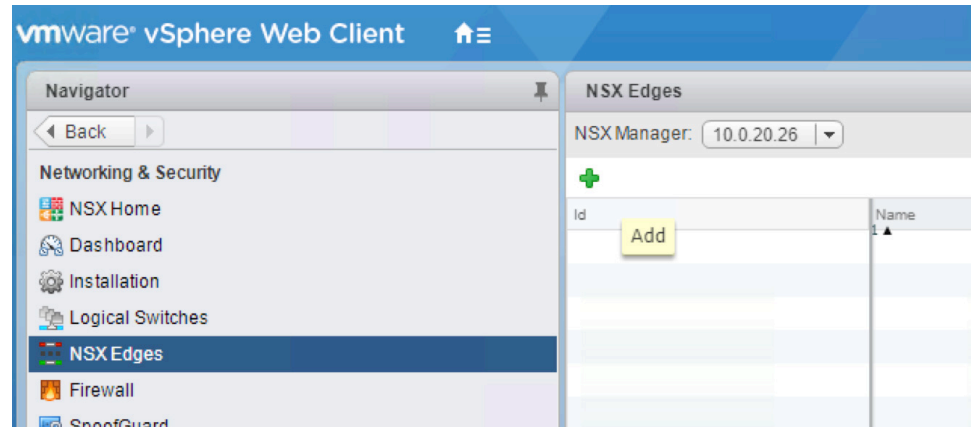
Network	Type	IP Ranges	Prefix Length	Default Gateway IP Address
vRack-DPortGroup-Mgmt	Management	10.0.20.216-10.0.20.218	24	10.0.20.1
vRack-DPortGroup-vMotion	vMotion	192.168.11.200	24	192.168.11.1
vRack-DPortGroup-External	Internet	10.155.168.127-10.155.168.128	24	10.155.168.126

CANCEL

BACK

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**.

New NSX Edge

1 Name and description

2 Settings

3 Configure deployment

4 Configure interfaces

5 Default gateway settings

6 Firewall and HA

7 Ready to complete

Name and description

Install Type: ☒ Edge Services Gateway
Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.

☐ Logical Router
Provides Distributed Routing and Bridging capabilities.

Name: * HCX-Edge

Hostname:

Description:

Tenant:

☒ Deploy NSX Edge
Select this option to create a new NSX Edge in deployed mode. Appliance and interface configuration is mandatory to deploy the NSX Edge.

☐ Enable High Availability
Enable HA, for enabling and configuring High Availability.

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

New NSX Edge

✓ 1 Name and description

2 Settings

3 Configure deployment

4 Configure interfaces

5 Default gateway settings

6 Firewall and HA

7 Ready to complete

Settings

CLI credentials will be set on the NSX Edge appliance(s). These credentials can be used to login to the read only command line interface of the appliance.

User Name: * admin

Password: *

Confirm password: *

☐ Enable SSH access

☐ Enable FIPS mode

☒ Enable auto rule generation

Enable auto rule generation, to automatically generate service rules to allow flow of control traffic.

Edge Control Level Logging INFO

Set the Edge Control Level Logging

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

New NSX Edge

- 1 Name and description
- 2 Settings
- 3 Configure deployment**
- 4 Configure interfaces
- 5 Default gateway settings
- 6 Firewall and HA
- 7 Ready to complete

Configure deployment

Datacenter: * vRack-Datacenter

Appliance Size: ☒ Compact
☐ Large
☐ X-Large
☐ Quad Large

NSX Edge Appliances

+ ✎ ✕

Resource P...	Host	Datastore	Folder	CPU Reserv...	Memory Re...

Specifying a resource pool and datastore is mandatory for configuring the NSX Edge appliance.

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

Add NSX Edge Appliance

Specify placement parameters for the NSX Edge appliance.

Cluster/Resource Pool: * Compute-ResourcePool

Datastore: * vsanDatastore

Host:

Folder:

Resource Reservation: System Managed ⓘ

CPU: 1000 MHz

Memory: 512 MB

OK Cancel

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

New NSX Edge

- ✓ 1 Name and description
- ✓ 2 Settings
- ✓ 3 Configure deployment
- 4 Configure interfaces**
- 5 Default gateway settings
- 6 Firewall and HA
- 7 Ready to complete

Configure interfaces

Configure interfaces of this NSX Edge

+ ✎ ✕

vNIC#	Name	IP Address	Subnet Prefix Length	Connected To

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.

?

Add NSX Edge Interface

vNIC#: 0

Name: * External WAN Uplink

Type: ☐ Internal ☒ Uplink

Connected To:

Select Remove

Connectivity Status: ☐ Connected ☒ Disconnected

+

✎

✕

Q Filter

▼

Primary IP Address	Secondary IP Addresses	Subnet Prefix Length

0 items

Copy ▼

Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.1.1.2,1.1.1.3

MAC Addresses:

You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.

MTU:

1500

Options: ☐ Enable Proxy ARP ☐ Send ICMP Redirect

Reverse Path Filter

Enabled ▼

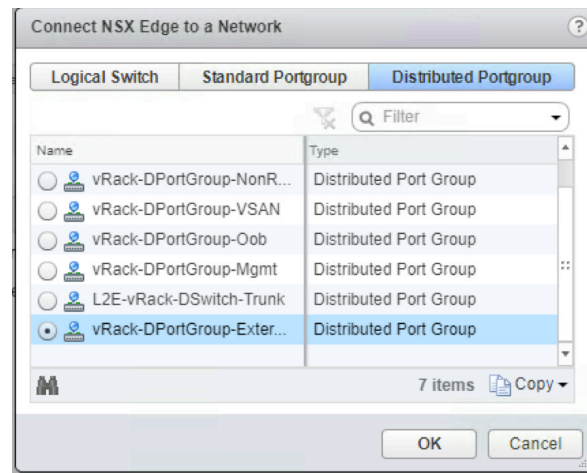
Fence Parameters:

Example: ethernet0.filter1.param1=1
ethernet1.filter1.param1=1

OK

Cancel

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



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

?

Add NSX Edge Interface

vNIC#:

0

Name:

* External WAN Uplink

Type:

☐ Internal
 ☒ Uplink

Connected To:

vRack-DPortGroup-External

Change Remove

Connectivity Status:

☒ Connected
 ☐ Disconnected

+

✖

Filter

▼

Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
10.155.168.127 ✖		24 ✖

1 items Copy ▼

Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.1.1.2,1.1.1.3

MAC Addresses:

You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.

MTU:

1500

Options:

☐ Enable Proxy ARP
 ☐ Send ICMP Redirect

Reverse Path Filter

Enabled ▼

Fence Parameters:

Example: ethernet0.filter1.param1=1
ethernet1.filter1.param1=1

OK

Cancel

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

Add NSX Edge Interface

vNIC#: 1

Name: * Management

Type: ☒ Internal ☐ Uplink

Connected To: vRack-DPortGroup-Mgmt [Change](#) [Remove](#)

Connectivity Status: ☒ Connected ☐ Disconnected

Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
10.0.20.217		24

1 items [Copy](#)

Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.1.1.2,1.1.1.3

MAC Addresses:

You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.

MTU:

Options: ☐ Enable Proxy ARP ☐ Send ICMP Redirect

Reverse Path Filter:

Fence Parameters:

Example: ethernet0.filter1.param1=1
ethernet1.filter1.param1=1

[OK](#) [Cancel](#)

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

The screenshot shows the 'New NSX Edge' configuration wizard. The left sidebar lists the steps: 1 Name and description, 2 Settings, 3 Configure deployment, 4 Configure interfaces, 5 Default gateway settings (selected), 6 Firewall and HA, and 7 Ready to complete. The main panel is titled 'Default gateway settings' and contains a checkbox 'Configure Default Gateway' which is checked. Below this are four fields: 'vNIC:' with a dropdown menu showing 'External WAN Uplink', 'Gateway IP:' with the value '10.155.168.126', 'MTU:' with the value '1500', and 'Admin Distance:' with the value '1'. At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

New NSX Edge

✓ 1 Name and description
✓ 2 Settings
✓ 3 Configure deployment
✓ 4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete

Default gateway settings

☒ Configure Default Gateway

vNIC: * External WAN Uplink

Gateway IP: * 10.155.168.126

MTU: 1500

Admin Distance: 1

Back Next Finish Cancel

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

New NSX Edge

1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete

Firewall and HA

☐ Configure Firewall default policy

Default Traffic Policy: ☒ Accept ☐ Deny

Logging: ☐ Enable ☒ Disable

Configure HA parameters
Configuring HA parameters is mandatory for HA to work.

vNIC: * any

Declare Dead Time: 15 (seconds)

Management IPs:

Management IPs must be in CIDR format with /30 subnet and must not overlap with any vnic subnets.

Back Next Finish Cancel

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

New NSX Edge

1 Name and description

2 Settings

3 Configure deployment

4 Configure interfaces

5 Default gateway settings

6 Firewall and HA

7 Ready to complete

Ready to complete

Name and description

Name: HCX-Edge

Install Type: Edge Services Gateway

Tenant:

Size: Compact

HA: Disabled

Automatic Rule Generation: Enabled

NSX Edge Appliances

Resource Pool	Host
Compute-ResourcePool	

Interfaces

vNIC#	Name	IP Address	Subnet Prefix Length	Connected To
0	External WA...	10.155.168.127*	24	vRack-DPortG...
1	Management	10.0.20.217*	24	vRack-DPortG...

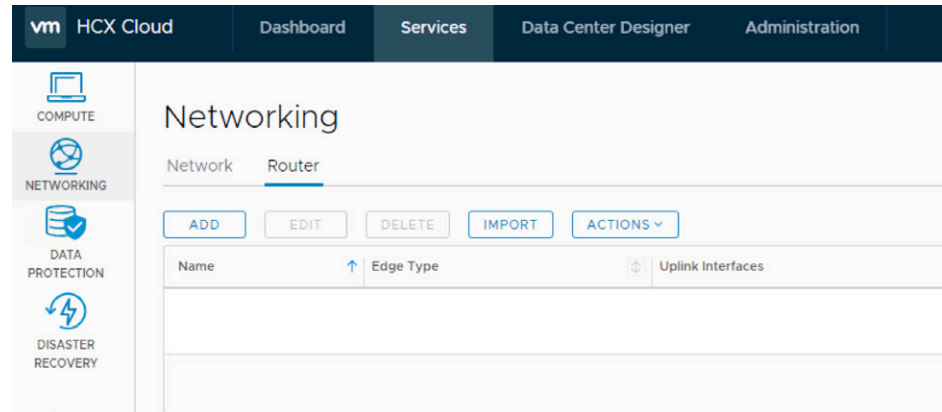
Back

Next

Finish

Cancel

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.

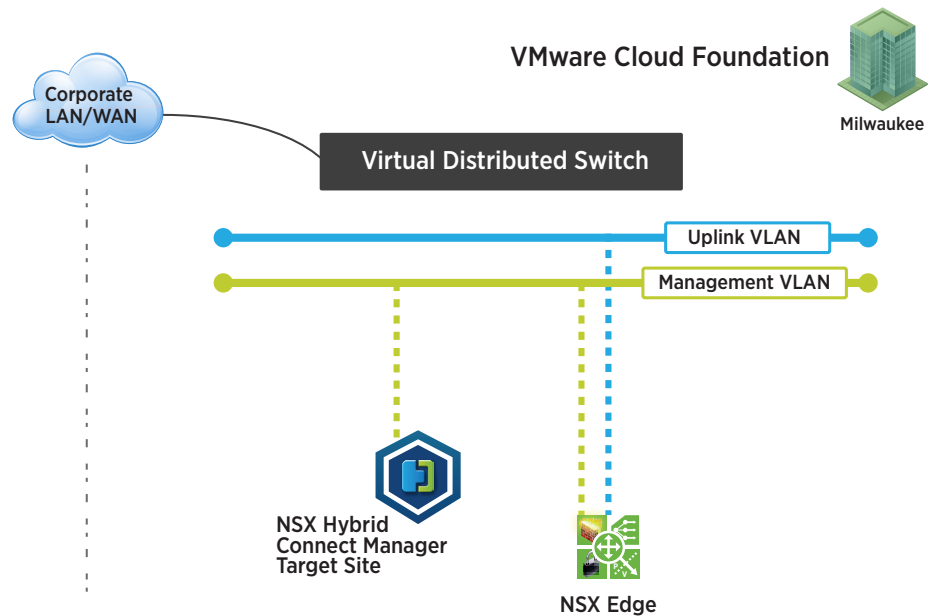
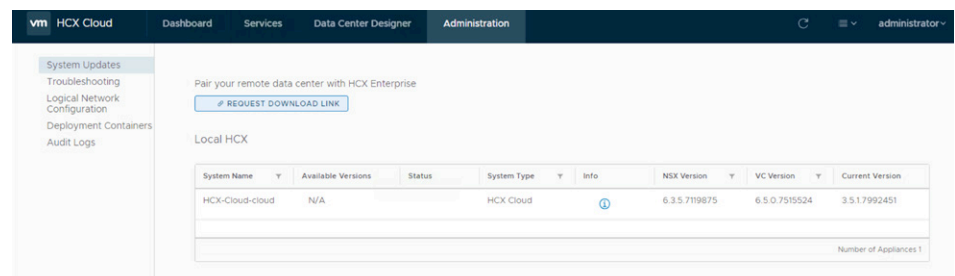


Figure 15. NSX Hybrid Connect Target Site Installation

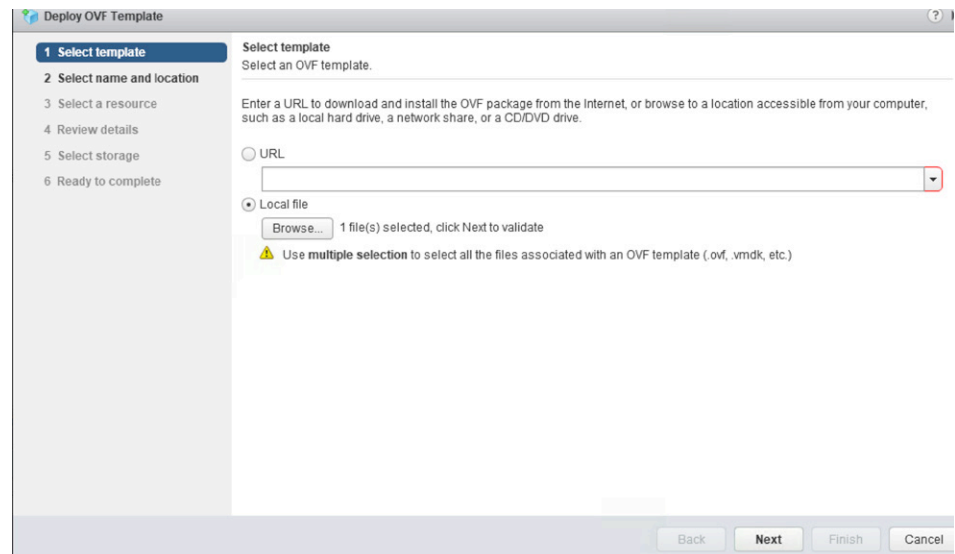
Installation – NSX Hybrid Connect Manager Source (Legacy vSphere Site)

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**.

The screenshot shows the 'Deploy OVF Template' wizard at step 2, 'Select name and location'. The left sidebar shows a progress list with steps 1 through 6, where step 2 is highlighted. The main area has a title 'Select name and location' and a subtitle 'Enter a name for the OVF and select a deployment location.' Below this is a text input field for 'Name' containing 'VMware-HCX-Enterprise-3.5.1-8327309'. There are 'Filter' and 'Browse' buttons. Below them is a subtitle 'Select a datacenter or folder.' and a tree view showing a folder structure: 'vc01.lab.local' > 'Datacenter'. The 'Datacenter' folder is selected. At the bottom right are buttons for 'Back', 'Next', 'Finish', and 'Cancel'.

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

The screenshot shows the 'Deploy OVF Template' wizard at step 3, 'Select a resource'. The left sidebar shows a progress list with steps 1 through 6, where step 3 is highlighted. The main area has a title 'Select a resource' and a subtitle 'Select where to run the deployed template.' Below this are 'Filter' and 'Browse' buttons. Below them is a subtitle 'Select a host or cluster or resource pool or vapp.' and a tree view showing a folder structure: 'Datacenter' > 'Cluster1' > 'SDDC' > '10.0.1.225' > '10.0.1.26'. The '10.0.1.26' resource is selected. At the bottom right are buttons for 'Back', 'Next', 'Finish', and 'Cancel'.

Review details and click **Next**.

Deploy OVF Template

1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Accept license agreements
6 Select storage
7 Select networks
8 Customize template
9 vService bindings
10 Ready to complete

Review details
Verify the template details.

The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

Product	HCX
Version	3.5.1
Vendor	VMware, Inc.
Publisher	VMware, Inc. (Trusted certificate)
Download size	1.7 GB
Size on disk	2.6 GB (thin provisioned) 60.0 GB (thick provisioned)
Description	HCX enables your Enterprise Hybrid Cloud Mobility. Datacenter migrations are complex elongated processes. Moving to a datacenter across the WAN is even more complicated. VMware HCX allow efficient datacenter migration beginning at datacenter setup and design through migrations leveraging VMware technologies such as Cross-Cloud vMotion. Learn about VMware's SD-WAN technologies with high throughput Layer-2 Network Extension, Disaster Recovery, Low/No Downtime Migration and optimized datacenter-to-datacenter or datacenter-to-cloud connectivity. HCX™ offers vSphere users a seamless option for extending their on-premises data center into your Hybrid Cloud. HCX is a single point of administration for Hybrid Cloud workloads that offers hybrid networking and bi-directional workload migration capabilities, simplifying on and off-premises resource integration and management workloads.
Extra configuration	hybridity.vmbuild = 8327309 hybridity.vmversion = 3.5.1 hybridity.vmtune = Manager

Back Next Finish Cancel

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

Deploy OVF Template

1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Accept license agreements
6 Select storage
7 Select networks
8 Customize template
9 vService bindings
10 Ready to complete

Accept license agreements
Read and accept the license agreements associated with this template before continuing.

VMware End User License Agreement
PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY:BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE If You are licensing the Software for evaluation purposes, Your use of the Software is only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.

1. DEFINITIONS.

1.1 "Affiliate" means, with respect to a party, an entity that is directly or indirectly controlled by or is under common control with such party, where "control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the relevant entity (but only as long as such person or entity meets these requirements).

1.2 "Documentation" means that documentation that is generally provided to You by VMware with the Software, as revised by

Accept

Back Next Finish Cancel

Select **storage** location. Click **Next**.

Select storage
Select location to store the files for the deployed template.

Select virtual disk format: **Thick provision lazy zeroed**

VM storage policy: **None**

☐ Show datastores from Storage DRS clusters

Filter

Datastores Datastore Clusters

Name	Status	VM storage policy	Capacity	Free
DataStore1	Normal	VM Encryption P...	1.15 TB	119.65 GB
VMwareNFSVol2	Normal	VM Encryption P...	1.15 TB	118.58 GB

2 Objects Copy

Back Next Finish Cancel

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

Select networks
Select a destination network for each source network.

Source Network	Destination Network
VSMgmt	VM Network

IP Allocation Settings

IP protocol: IPv4 IP allocation: Static - Manual

Back Next Finish Cancel

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

Deploy OVF Template

1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Accept license agreements
6 Select storage
7 Select networks
8 Customize template
9 vService bindings
10 Ready to complete

Customize template
Customize the deployment properties of this software solution.

All properties have valid values [Show next...](#) [Collapse all...](#)

DNS 2 settings

DNS Server list The DNS server list(space separated) for this VM.

Domain Search List The domain Search list(space separated) for this VM.

Network properties 4 settings

Default IPv4 Gateway The default gateway for this VM.

Hostname The hostname for this VM.

Network 1 IPv4 Address The IPv4 Address for this interface. Leave this empty for DHCP base IP assignment.

Network 1 IPv4 Prefix Length The IPv4 prefix Length for this interface.

[Back](#) [Next](#) [Finish](#) [Cancel](#)

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

Deploy OVF Template

1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Accept license agreements
6 Select storage
7 Select networks
8 Customize template
9 vService bindings
10 Ready to complete

Customize template
Customize the deployment properties of this software solution.

All properties have valid values [Show next...](#) [Collapse all...](#)

Passwords 2 settings

CLI "admin" User Password The password for default CLI user for this VM.
Enter password
Confirm password

root Password The password for root user.
Enter password
Confirm password

Services Configuration 2 settings

Enable SSH Enabling SSH service is not recommended for security reasons.
☐

NTP Server List The NTP server list(space separated) for this VM.

[Back](#) [Next](#) [Finish](#) [Cancel](#)

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

The screenshot shows the 'Deploy OVF Template' wizard in the vSphere Client. The left sidebar lists steps 1 through 10, with '10 Ready to complete' selected. The main area is titled 'Ready to complete' and 'Review configuration data.' It displays a table of configuration details:

Name	VMware-HCX-Enterprise-3.5.1-8327309
Source VM name	VMware-HCX-Enterprise-3.5.1-8327309
Download size	1.7 GB
Size on disk	60.0 GB
Datacenter	Datacenter
Resource	Cluster1
Storage mapping	1
Network mapping	1
IP allocation settings	IPv4, Static - Manual
Properties	DNS Server list = Domain Search List = Default IPv4 Gateway = Hostname = Network 1 IPv4 Address = Network 1 IPv4 Prefix Length = Enable SSH = False NTP Server List =

At the bottom right, there are buttons for 'Back', 'Next', 'Finish', and 'Cancel'.

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.

The screenshot shows the NSX Hybrid Connect Manager web UI. The top navigation bar includes 'vm HCX Manager', 'Dashboard', 'Appliance Summary', 'Configuration', and 'Administration'. The main content area is titled 'Activate your HCX instance' and contains the following fields:

- Enter your activation key
- HCX Server: <https://connect.hcx.vmware.com>
- Activation Key: Enter activation key

At the bottom right, there are buttons for 'ACTIVATE LATER' and 'ACTIVATE'. On the left side of the main content area, there is a large graphic with the HCX logo and the text: 'Let's get your HCX system configured. Activate and configure your system.'

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

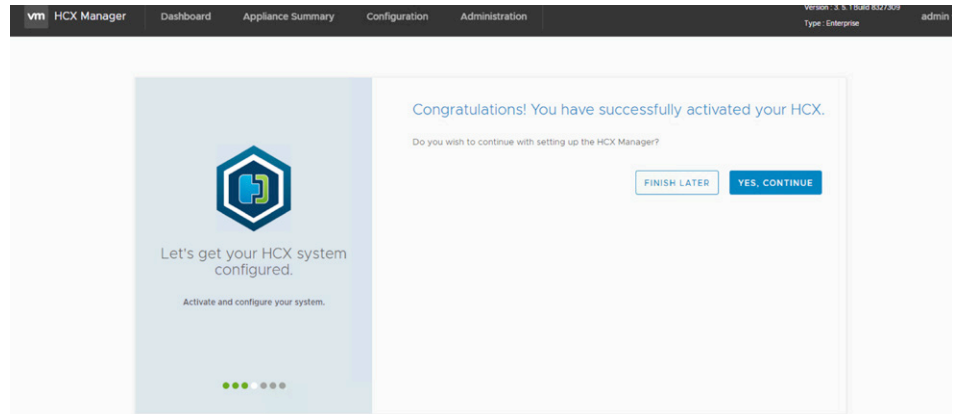
Select the data center location for the NSX Hybrid Connect Manager source site installation. Click **CONTINUE**.

The screenshot shows the NSX Hybrid Connect Manager configuration wizard. The left panel displays the VMware logo and the text "Let's get your HCX system configured. Activate and configure your system." The right panel is titled "Where is your HCX system located?" and includes a sub-label "Location of your datacenter (nearest city)". A text input field contains "Palo Alto, United States of America". Below the text is a world map with a red pin indicating the location. A green "CONTINUE" button is at the bottom right.

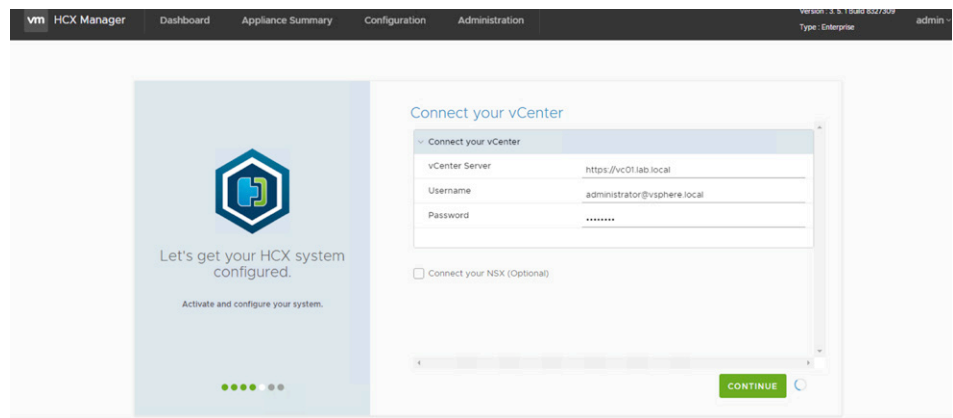
Provide a **System Name** for the NSX Hybrid Connect Manager source site system. Click **CONTINUE**.

The screenshot shows the NSX Hybrid Connect Manager configuration wizard at the "System Name" step. The left panel is identical to the previous step. The right panel is titled "System Name" and has a sub-label "System Name". A text input field contains "HCX-Enterprise-PaloAlto". A green "CONTINUE" button is at the bottom right.

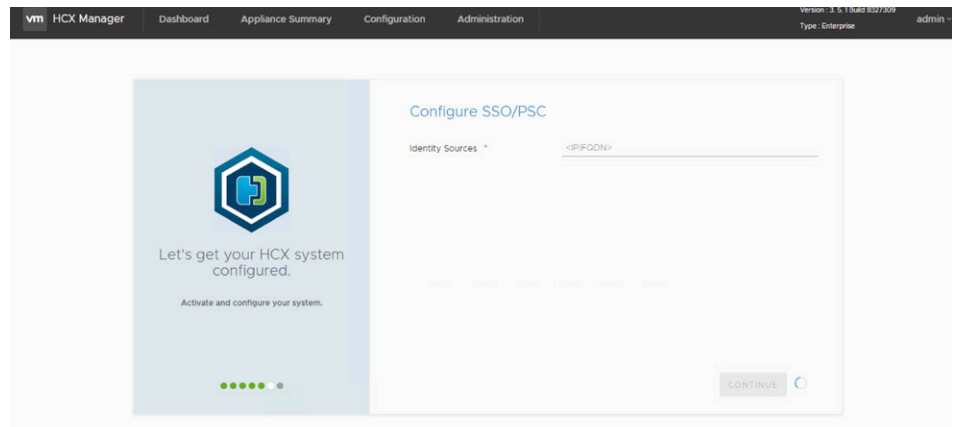
After completing the activation, select **YES, CONTINUE**.



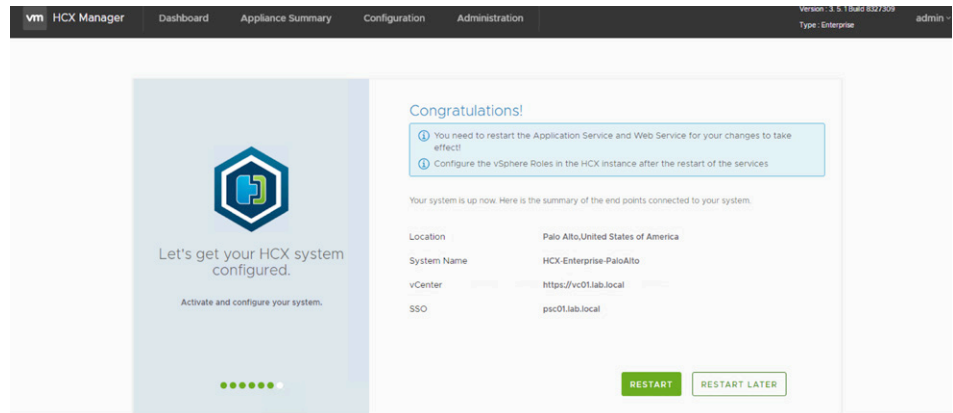
Now connect the NSX Hybrid Connect Manager source site appliance to the legacy vCenter Server system. Enter the web URL for the legacy vCenter Server system and provide the **Username** and **Password**.



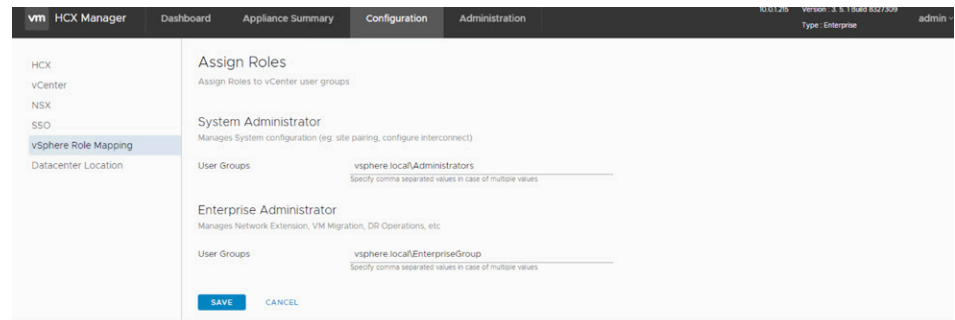
If the Platform Services Controller instance is not internal to your vCenter Server system, direct the NSX Hybrid Connect Manager source site instance to the Platform Services Controller instance in your legacy vCenter Server system.



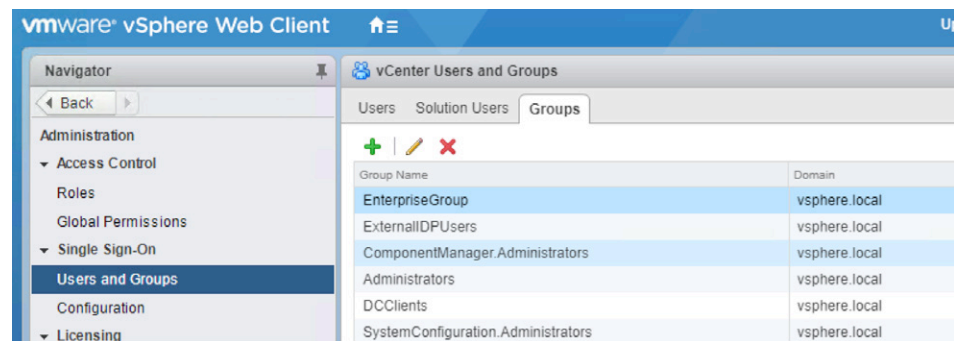
After a restart of NSX Hybrid Connect Manager source site services, the NSX Hybrid Connect Manager source site dashboard will reappear.



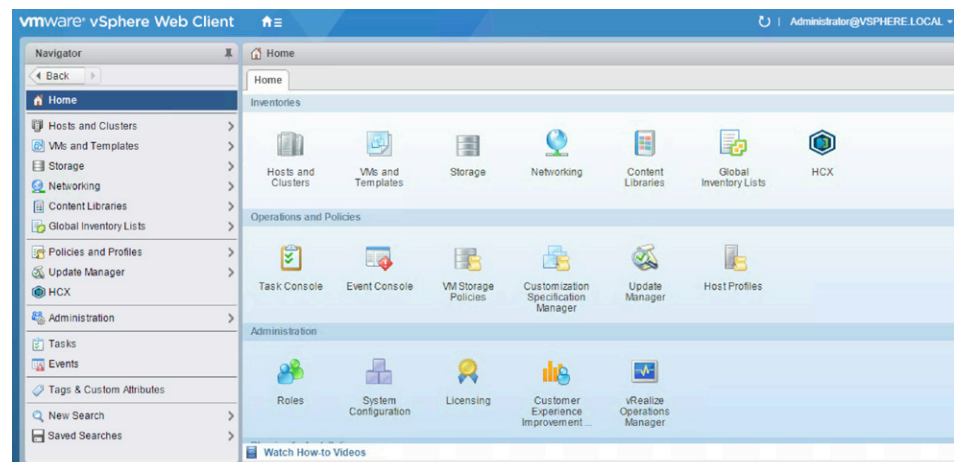
On the NSX Hybrid Connect Manager source site dashboard, configure the **EnterpriseGroup** account.



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.

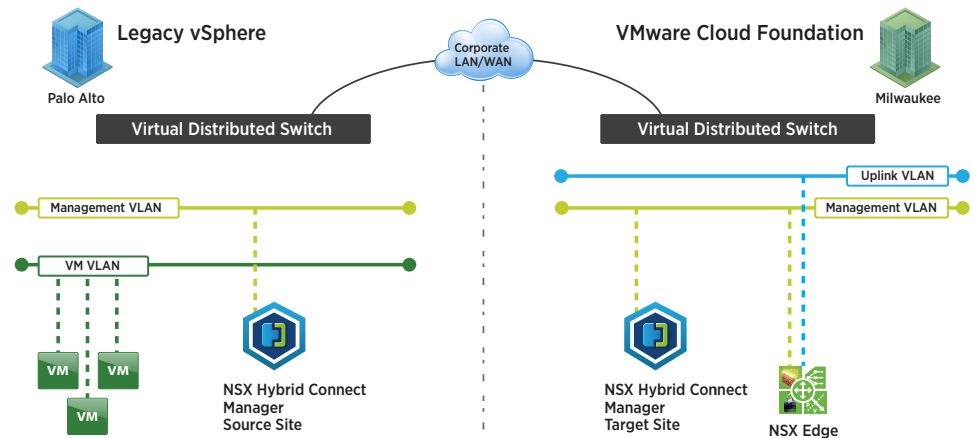
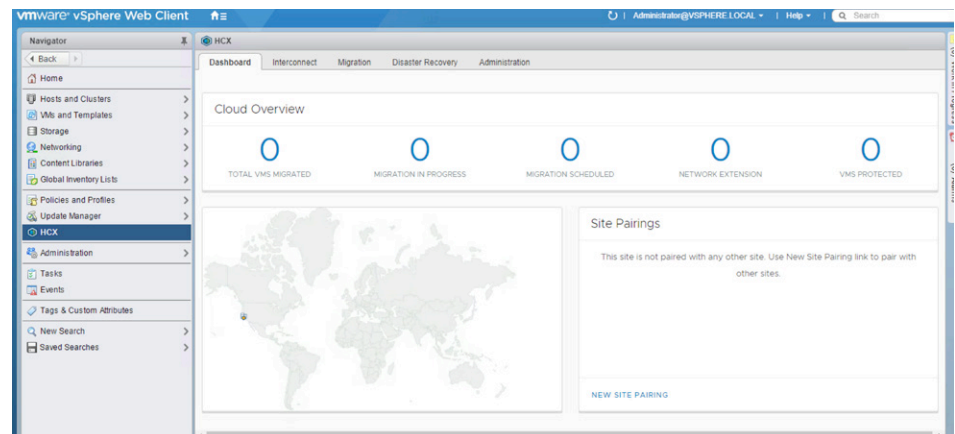


Figure 16. NSX Hybrid Connect Architecture Overview

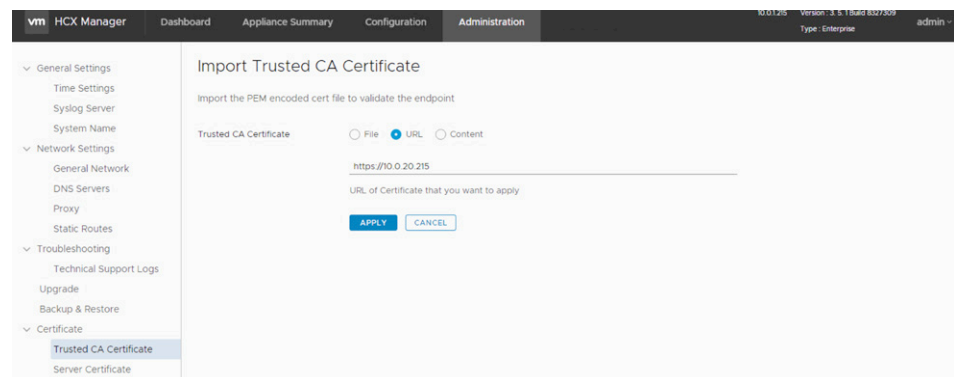
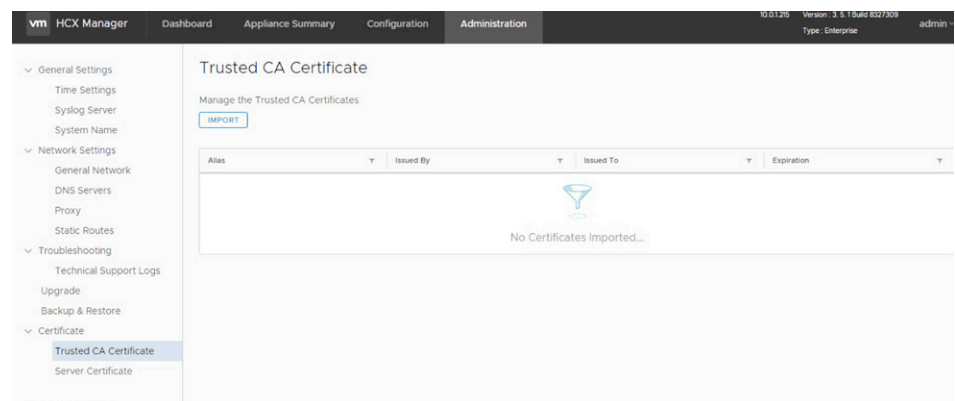
The two NSX Hybrid Connect Manager appliances are installed and connected to a VLAN that enables them to communicate with each other, over the LAN or WAN interface, and with the local vCenter Server environments.

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.



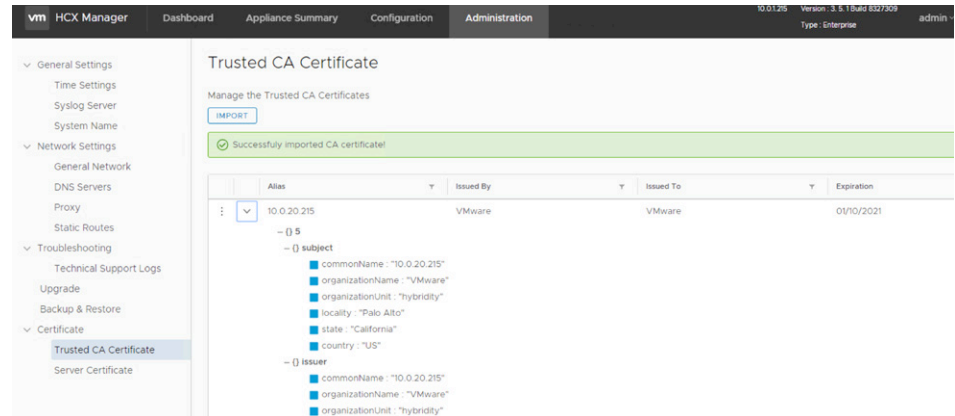
Before enabling the new site pairing link, the NSX Hybrid Connect Manager source site must trust the SSL certificate of the NSX Hybrid Connect Manager target site. Log in to the NSX Hybrid Connect Manager source web UI and import the certificate, located at <https://<Hybrid Connect Manager Source Site>:9443/>.

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**.

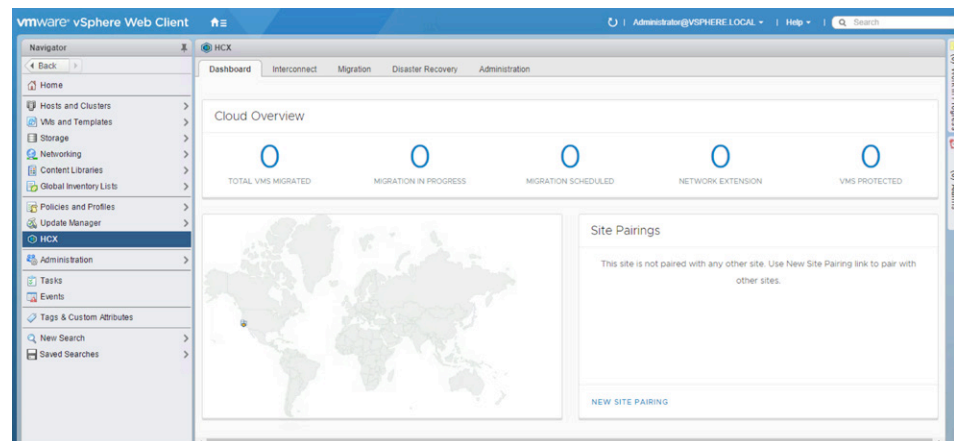


The site pairing process will not work if the common name (CN) in the SSL certificate does not match the name in the URL. In this white paper, we use the IP address in the CN name of the appliance and have updated the SSL certificate with this information.

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**.



Register Site

1 Choose Hybrid Services
2 Ready to complete

Choose Hybrid Services

Remote Site Connection:

No registered connections found.
You may:

- Register Connection
- Reload Connections

☐ HCX Interconnect Service (Not available for this vCenter!)

HCX Interconnect service provides resilient access over the Internet and private lines to the target site while providing strong encryption, traffic engineering and extending the datacenter. This services simplifies secure pairing of sites and management of HCX components

☐ WAN Optimization Service (Not available for this vCenter!)

Improves performance characteristics of the private lines or Internet paths by leveraging WAN Optimization techniques like data de-duplication and line conditioning. This makes performance closer to a LAN environment.

☐ Network Extension Service (Not available for this vCenter!)

High throughput Network Extension service with integrated Proximity Routing which unlocks seamless mobility and simple disaster recovery plans across sites.

Back Next Finish Cancel

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**.

Register Site

1 Choose Hybrid Services
2 Ready to complete

Choose Hybrid Services

Remote Site Connection:

Register new Connection

Site URL:

The URL must be specified using either a FQDN format or an IP address.

User Name:

Password:

Register Cancel

☐ HCX Interconnect Service (Not available for this vCenter!)

HCX Interconnect service provides resilient access over the Internet and private lines to the target site while providing strong encryption, traffic engineering and extending the datacenter. This services simplifies secure pairing of sites and management of HCX components

☐ WAN Optimization Service (Not available for this vCenter!)

Improves performance characteristics of the private lines or Internet paths by leveraging WAN Optimization techniques like data de-duplication and line conditioning. This makes performance closer to a LAN environment.

☐ Network Extension Service (Not available for this vCenter!)

High throughput Network Extension service with integrated Proximity Routing which unlocks seamless mobility and simple disaster recovery plans across sites.

Back Next Finish Cancel

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.

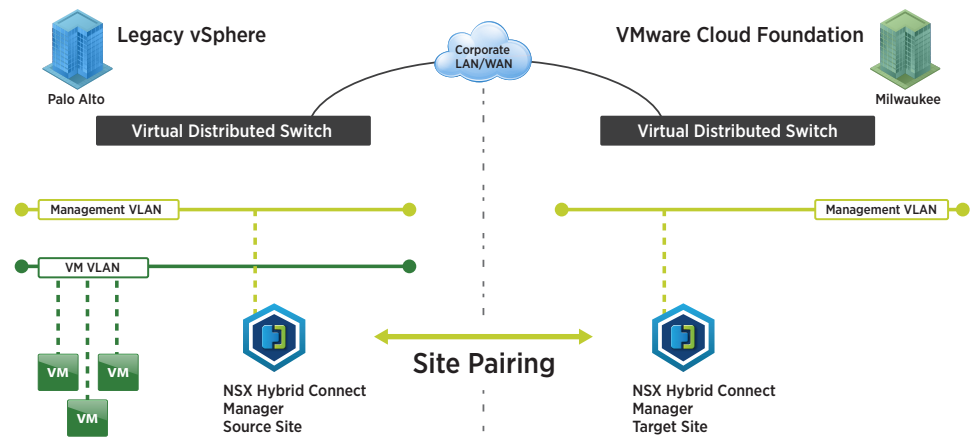


Figure 17. Site Pairing Process Completed

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**.

Register Site

✓ 1 Choose Hybrid Services

2 HCX Interconnect Service

3 WAN Optimization Service

4 Network Extension Service

5 Ready to complete

HCX Interconnect Service

Specify parameters for local Gateway deployment. Remote Gateway will be provisioned automatically.

Placement of local Hybrid Cloud Gateway

Network: DPG-VMGuest

Cluster/Host: Cluster1

Datastore: VMwareNFSVol2

Appliance Name: CGW-LMNZM

IP Assignment

IP Address /PL: 10.0.1.225/24 (see IPvt CIDR blocks)

Default Gateway: 10.0.1.1

DNS: 10.0.1.49

☐ Use static routes

Extended (optional)

VMotion Network: vMotion

Network should be accessible from the Compute resource, where Gateway Appliance will be placed!

IP Address /PL: 172.16.0.100/24 (see IPvt CIDR blocks)

Passwords

admin password: ***** confirm: *****

root password: ***** confirm: *****

Back

Next

Finish

Cancel

vmware®

WHITE PAPER | 82

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

The screenshot shows a 'Register Site' wizard with a sidebar on the left and a main configuration area on the right. The sidebar contains a list of steps: '1 Choose Hybrid Services', '2 HCX Interconnect Service', '3 WAN Optimization Service' (highlighted with a blue bar), '4 Network Extension Service', and '5 Ready to complete'. The main area is titled 'WAN Optimization Service' and contains the instruction 'Specify parameters for WAN Optimization Service.' Below this, there is a 'Bandwidth Limit:' label followed by a text input field containing '10000' and a 'Mb/s' unit label. At the bottom right of the wizard, there are four buttons: 'Back', 'Next' (highlighted with a blue border), 'Finish', and 'Cancel'.

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.

Install HCX Components

- 1 Choose Hybrid Services
- 2 HCX Interconnect Service
- 3 WAN Optimization Service
- 4 Network Extension Service**
- 5 Ready to complete

Network Extension Service
Hybrid Cloud Manager will deploy a L2 Concentrator virtual appliance per Distributed Switch to enable High Throughput Network Extension Service.

Distributed Switch: Uplink MTU:

L2 Concentrator placement:

Compute:

Datastore:

Management Network:

Appliance Name:

IP Address /PL: (see IPv4 CIDR blocks) Uplink MTU:

Default Gateway: VM on extended network can have MTU up to 6550

Passwords

admin password: confirm:

root password: confirm:

+ Add another Distributed Switch

Back Next Finish Cancel

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

Install HCX Components

Ready to complete
Review Virtual Appliances configuration before deployment

1. Destination Cloud: ✓

Cloud: HCX-Cloud-cloud
VC: vcenter-1.sddc.lab.local
URL: https://10.0.20.215
vCenter: vc01.lab.local

2. Hybrid Cloud Gateway: ✓

Core Gateway will be added as a standalone host.

Compute: Cluster1 Datastore: VMwareNFSVol2

Management Network:
Network: DPG-VMkernel Default Gateway: 10.0.1.1
IP Address: 10.0.1.225/24 DNS: 10.0.1.49

vMotion Network:
Network: vMotion
IP Address: 172.16.0.100/24

3. High Performance L2 Concentrator: ✓

Distributed Switch: DSwitch
Uplink MTU: 9000

Back Next Finish Cancel

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.

vmware vSphere Web Client

Updated at 9:58 AM | Administrator@VSPHERE.LOCAL | Help | Search

HCX

Dashboard Interconnect Migration Disaster Recovery Administration

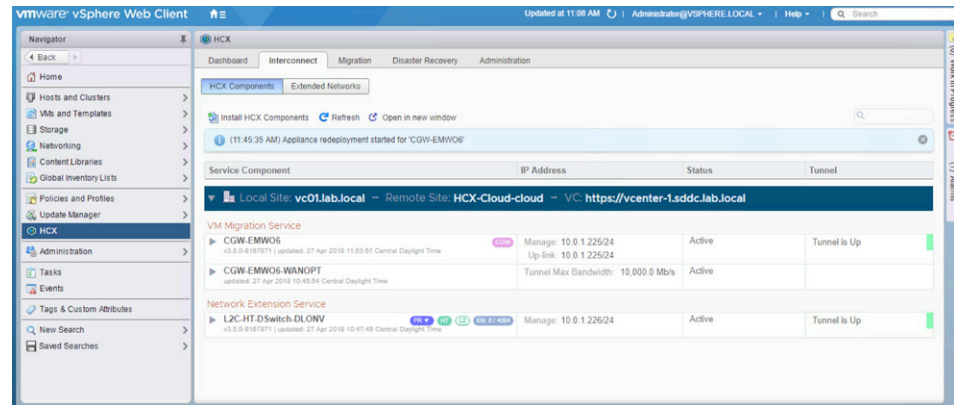
HCX Components Extended Networks

Install HCX Components Refresh Open in new window

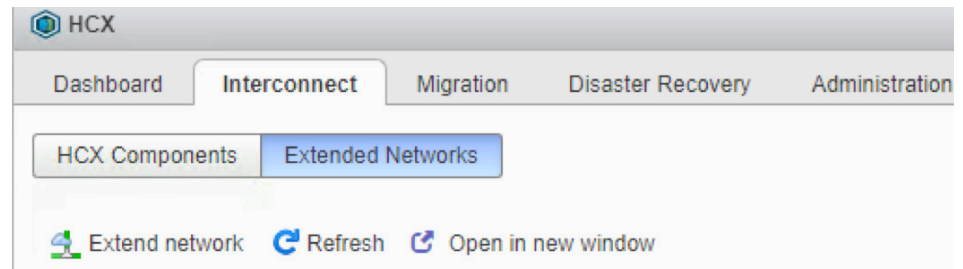
Service Component	IP Address	Status	Tunnel
Local Site: vc01.lab.local ~ Remote Site: HCX-Cloud-cloud ~ VC: https://vcenter-1.sddc.lab.local			
VM Migration Service		Up-Link: NA	Deployment - Queued for Deployment
CGW-EMW06	Managed: 10.0.1.225/24 Up-Link: 10.0.1.225/24	Deployment - Deployment Complete, Reconfiguring Appliance	
Network Extension Service		Up-Link: NA	Deployment - Queued for Deployment, Tunnel is Down

Navigation: Home, Hosts and Clusters, VMs and Templates, Storage, Networking, Content Libraries, Global Inventory Lists, Policies and Profiles, Update Manager, HCX, Administration, Tasks, Events, Tags & Custom Attributes, New Search, Saved Searches

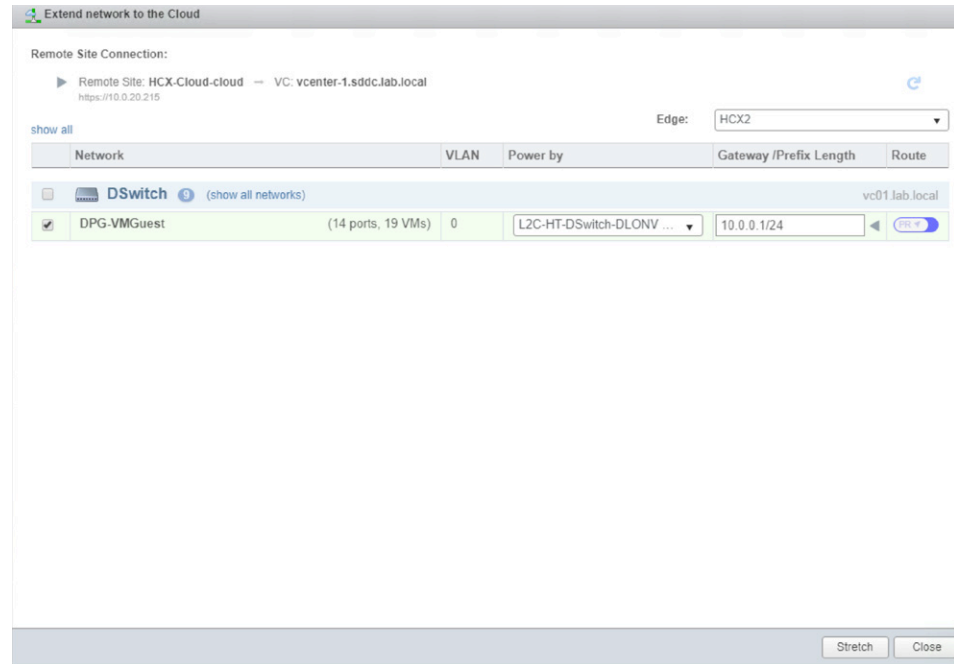
After completion of the automated installation of the NSX Hybrid Connect appliances, log in to the NSX Hybrid Connect **Interconnect** dashboard to verify that the appliances are active and that each hybridity **Tunnel is Up** and greenlit.



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.

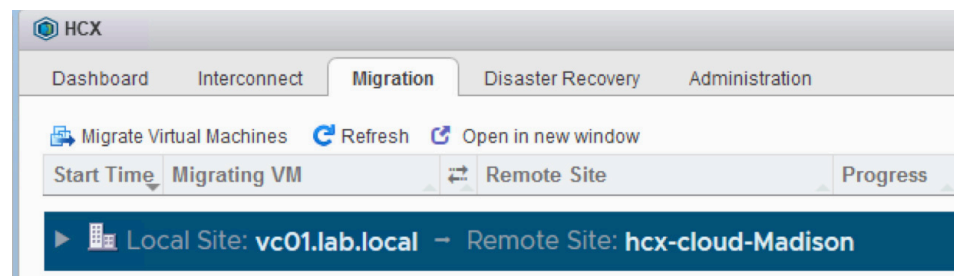
How to Migrate

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.

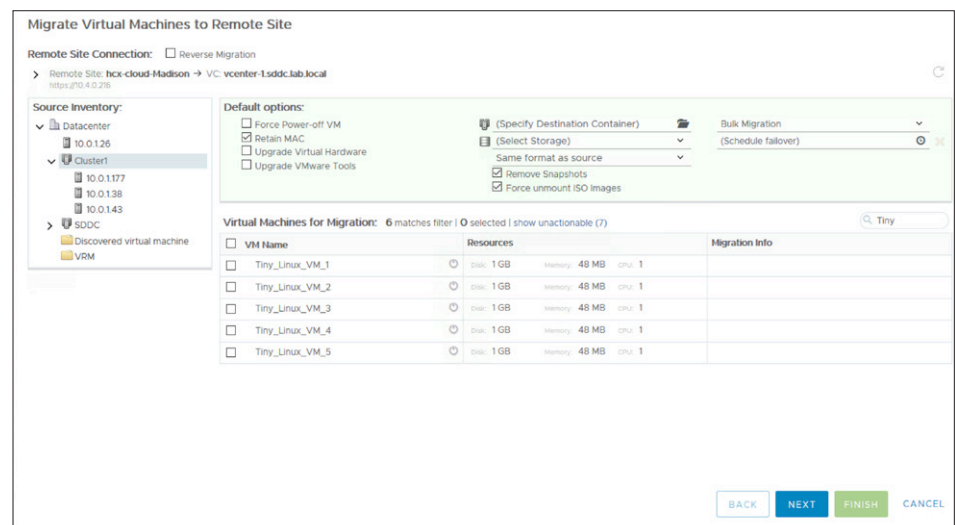


Click **Migration**. Then click **Migrate Virtual Machines**.



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.



Migrate Virtual Machines to Remote Site

Validation is Successful, You can proceed with Migration
(retry validation)

Virtual Machine	Resources	Migration Info
1. Tiny_Linux_VM_1 Provisioning type: Thin Provisioned Storage: vsanDatastore Resourcepool: Compute-ResourcePool Datacenter: vRack-Datacenter Force Power-off VM: No Remove Snapshots: Yes Unmount ISO Images: Yes Retain MAC: No Upgrade Virtual Hardware: No Upgrade VMware Tools: No	Disk: 1 GB Memory: 48 MB CPU: 1 DPG-VMGuest → vRack-DPortGroup-External	Cold
2. Tiny_Linux_VM_2 Provisioning type: Thin Provisioned Storage: vsanDatastore Resourcepool: Compute-ResourcePool Datacenter: vRack-Datacenter Force Power-off VM: No Remove Snapshots: Yes Unmount ISO Images: Yes Retain MAC: No Upgrade Virtual Hardware: No Upgrade VMware Tools: No	Disk: 1 GB Memory: 48 MB CPU: 1 DPG-VMGuest → vRack-DPortGroup-External	Cold
3. Tiny_Linux_VM_3 Provisioning type: Thin Provisioned Storage: vsanDatastore Resourcepool: Compute-ResourcePool Datacenter: vRack-Datacenter Force Power-off VM: No Remove Snapshots: Yes Unmount ISO Images: Yes Retain MAC: No Upgrade Virtual Hardware: No Upgrade VMware Tools: No	Disk: 1 GB Memory: 48 MB CPU: 1 DPG-VMGuest → vRack-DPortGroup-External	Cold

BACK NEXT FINISH CANCEL

You can now monitor the migration progress for each VM.

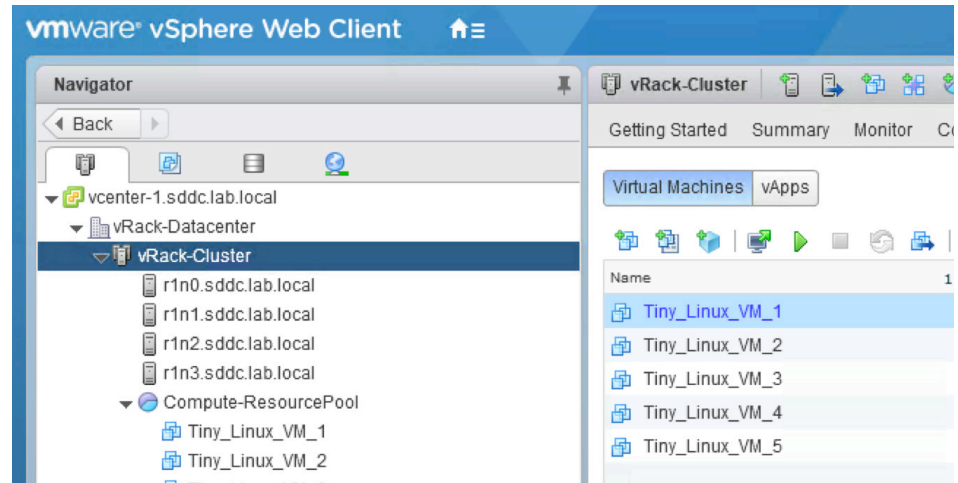
HCX

Dashboard Interconnected Migration Disaster Recovery Administration

Migrate Virtual Machines Refresh Open in new window

Start Time	Migrating VM	Remote Site	Progress	Size	End Time	Status
Local Site: vc01.lab.local - Remote Site: hcx-cloud-Madison						
4:20 PM Centr... Apr 12 Administrator@VSPHERE.LOCAL	Tiny_Linux_VM_5	VC: vcenter-1.sddc.lab.local	waiting...	1GB		Preparing mobility agent at source
4:20 PM Centr... Apr 12 Administrator@VSPHERE.LOCAL	Tiny_Linux_VM_4	VC: vcenter-1.sddc.lab.local	waiting...	1GB		Preparing mobility agent at source
4:20 PM Centr... Apr 12 Administrator@VSPHERE.LOCAL	Tiny_Linux_VM_3	VC: vcenter-1.sddc.lab.local	waiting...	1GB		Waiting for the MA Reconfigure
4:20 PM Centr... Apr 12 Administrator@VSPHERE.LOCAL	Tiny_Linux_VM_2	VC: vcenter-1.sddc.lab.local	19% 194.6MB / 1GB		(copy started at 4:20 PM)	Relocation in progress
4:20 PM Centr... Apr 12 Administrator@VSPHERE.LOCAL	Tiny_Linux_VM_1	VC: vcenter-1.sddc.lab.local	waiting...	1GB		Initiating virtual machine relocation

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



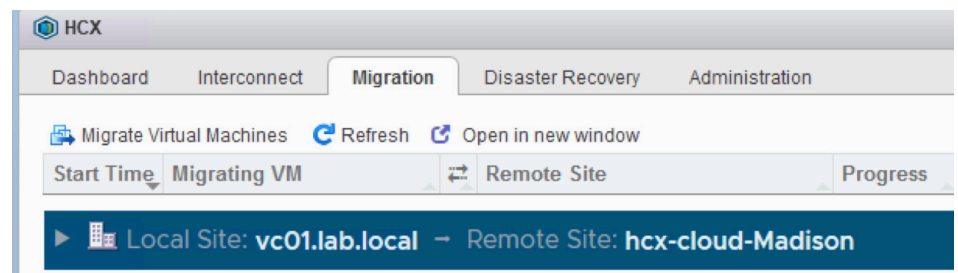
Live Migration

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**.

Migrate to the Cloud

Remote Site Connection: > Remote Site: HCX-Cloud-cloud → VC: vcenter-1.sddc.lab.local
https://10.0.20.215

Default options:

- ☐ Force Power-off VM
- ☐ Retain MAC
- ☐ Upgrade Virtual Hardware
- ☐ Upgrade VMware Tools
- ☒ Compute-ResourcePool
- ☒ vsanDatastore
- ☐ Same format as source
- ☒ Remove Snapshots
- ☒ Force unmount ISO images

Virtual Machines for Migration: 1 selected | hide unselected

VM Name	Resources	Migration info
<input checked="" type="checkbox"/> Tiny_Linux_VM_3	Disk: 1 GB Memory: 48 MB CPU: 1 Compute-ResourcePool vsanDatastore Same format as source	vMotion

DPG-Stretch → VXLAN / L2E_DPG-Stretch-0-b9a7ad29

BACK NEXT FINISH CANCEL

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

Migrate to the Cloud

Validation is Successful, You can proceed with Migration

Migrating 1 virtual machine from vc01lab.local (VC) to vcenter-1.sddc.lab.local (VC)

(retry validation)

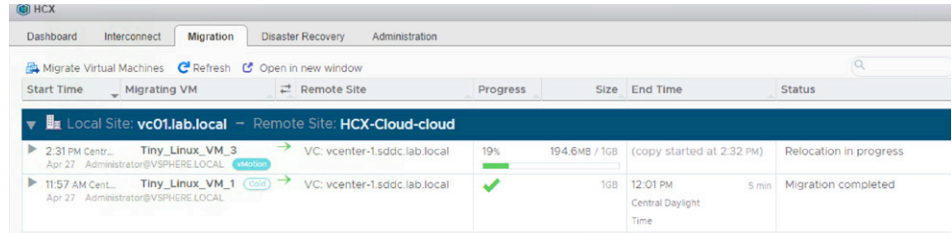
Virtual Machine	Resources	Migration info
1: Tiny_Linux_VM_3	Disk: 1 GB Memory: 48 MB CPU: 1 Compute-ResourcePool vsanDatastore	vMotion

Provisioning type: Same as Source
Storage: vsanDatastore
Resourcepool: Compute-ResourcePool
Datacenter: vRack-Datacenter

DPG-Stretch → L2E_DPG-Stretch-0-b9a7ad29

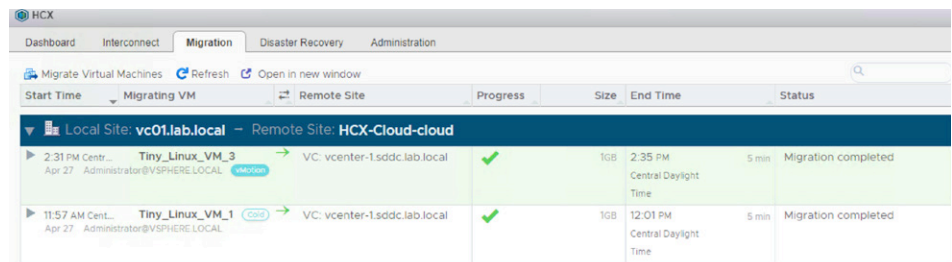
BACK NEXT FINISH CANCEL

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



Start Time	Migrating VM	Remote Site	Progress	Size	End Time	Status
Local Site: vc01.lab.local - Remote Site: HCX-Cloud-cloud						
2:31 PM Centr... Apr 27 Administrator@VSPHERE.LOCAL	Tiny_Linux_VM_3 (Hot)	VC: vcenter-1.sddc.lab.local	19%	194.6MB / 1GB	(copy started at 2:32 PM)	Relocation in progress
11:57 AM Centr... Apr 27 Administrator@VSPHERE.LOCAL	Tiny_Linux_VM_1 (Cold)	VC: vcenter-1.sddc.lab.local	✓	1GB	12:01 PM Central Daylight Time	5 min Migration completed

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



Start Time	Migrating VM	Remote Site	Progress	Size	End Time	Status
Local Site: vc01.lab.local - Remote Site: HCX-Cloud-cloud						
2:31 PM Centr... Apr 27 Administrator@VSPHERE.LOCAL	Tiny_Linux_VM_3 (Hot)	VC: vcenter-1.sddc.lab.local	✓	1GB	2:35 PM Central Daylight Time	5 min Migration completed
11:57 AM Centr... Apr 27 Administrator@VSPHERE.LOCAL	Tiny_Linux_VM_1 (Cold)	VC: vcenter-1.sddc.lab.local	✓	1GB	12:01 PM Central Daylight Time	5 min Migration completed

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](https://twitter.com/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

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: **VMW-vCF-Migration-USLET-101**