NSX-T Data Center Installation Guide

Modified on 29 MAY 2020

VMware NSX-T Data Center 3.0

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

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

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

Contents

NSX-T Data Center Installation Guide 7

1 Overview of NSX-T Data Center 8

Key Concepts 9

Overview of the NSX Manager 12

Configure User Interface Settings 14

2 NSX-T Data Center Installation Workflows 16

NSX-T Data Center Workflow for vSphere 16

NSX-T Data Center Installation Workflow for KVM 17

NSX-T Data Center Configuration Workflow for Bare Metal Server 17

3 Preparing for Installation 19

System Requirements 19

NSX Manager VM and Host Transport Node System Requirements 19

NSX Edge VM System Requirements 22

NSX Edge Bare Metal Requirements 23

Bare Metal Server System Requirements 26

Bare Metal Linux Container Requirements 26

Ports and Protocols 27

4 NSX Manager Installation 28

Modifying the Default Admin Password Expiration 32

5 Installing NSX-T Data Center on vSphere 33

Install NSX Manager and Available Appliances 33

Install NSX Manager on ESXi Using the Command-Line OVF Tool 37

Configure NSX-T Data Center to Display the GRUB Menu at Boot Time 42

Log In to the Newly Created NSX Manager 42

Add a Compute Manager 43

Deploy NSX Manager Nodes to Form a Cluster from UI 45

Configure a Virtual IP (VIP) Address for a Cluster 52

Disable Snapshots on NSX-T Data Center Appliances 53

6 Installing NSX-T Data Center on KVM 55

Set Up KVM 55

Manage Your Guest VMs in the KVM CLI 58

Install NSX Manager on KVM 59

Install Third-Party Packages on a KVM Host 64
Verify Open vSwitch Version on RHEL or CentOS KVM Hosts 66
Verify Open vSwitch Version on SUSE KVM Hosts 67
Verify Open vSwitch Version on Ubuntu KVM Hosts 68
Deploy NSX Manager Nodes to Form a Cluster Using CLI 69

7 Configuring Bare Metal Server to Use NSX-T Data Center 71
Install Third-Party Packages on a Bare Metal Server 71
Create Application Interface for Bare Metal Server Workloads 73
Ansible Server Configuration for Bare Metal Server 74
Secure Workloads on Windows Server 2016 Bare Metal Server 74

8 NSX Manager Cluster Requirements 78
NSX Manager Cluster Requirements for Single, Dual, and Multiple Sites 78

9 Installing NSX Edge 82
NSX Edge Installation Requirements 82
NSX Edge Networking Setup 85
NSX Edge Installation Methods 90
Create an NSX Edge Transport Node 91
Create an NSX Edge Cluster 96
Install an NSX Edge on ESXi Using the vSphere GUI 97
Install NSX Edge on ESXi Using the Command-Line OVF Tool 101
Install NSX Edge via ISO File as a Virtual Appliance 105
Install NSX Edge on Bare Metal 109
Prepare the PXE Server for NSX Edge 109
Install NSX Edge Automatically via ISO File 113
Install NSX Edge Interactively via ISO File 116
Intel QAT Support for IPSec VPN Bulk Cryptography 118
Join NSX Edge with the Management Plane 119
Configure an NSX Edge as a Transport Node 120

10 Transport Zones and Transport Nodes 123
Create Transport Zones 123
Create an IP Pool for Tunnel Endpoint IP Addresses 125
Enhanced Data Path 126
Configuring Profiles 130
Create an Uplink Profile 130
Configuring Network I/O Control Profiles 133
Add an NSX Edge Cluster Profile 143
Add an NSX Edge Bridge Profile 143

Add a Transport Node Profile 144
VMkernel Migration to an N-VDS Switch 149
VMkernel Migration Errors 154
Create a Standalone Host or Bare Metal Server Transport Node 157
Prepare a vSphere Distributed Switch for NSX-T 165
Configure a Managed Host Transport Node 165
Configure an ESXi Host Transport Node with Link Aggregation 171
Verify the Transport Node Status 172
Migrate ESXi VMkernel and Physical Adapters 175
NSX Maintenance Mode 175
Visual Representation of N-VDS 176
Health Check VLAN ID Ranges and MTU Settings 177
View Bidirectional Forwarding Detection Status 181
Manual Installation of NSX-T Data Center Kernel Modules 181
Manually Install NSX-T Data Center Kernel Modules on ESXi Hypervisors 182
Manually Install NSX-T Data Center Software Packages on Ubuntu KVM Hypervisors 185
Manually Install NSX-T Data Center Software Packages on RHEL and CentOS KVM Hypervisors 186
Manually Install NSX-T Data Center Software Packages on SUSE KVM Hypervisors 187
Deploy a Fully Collapsed vSphere Cluster NSX-T 188
VLAN Micro-Segmentation 198

11 Host Profile integration with NSX-T 200
Auto Deploy Stateless Cluster 200
High-Level Tasks to Auto Deploy Stateless Cluster 200
Prerequisites and Supported Versions 201
Create a Custom Image Profile for Stateless Hosts 202
Associate the Custom Image with the Reference and Target Hosts 203
Set Up Network Configuration on the Reference Host 204
Configure the Reference Host as a Transport Node in NSX-T 205
Extract and Verify the Host Profile 207
Verify the Host Profile Association with Stateless Cluster 208
Update Host Customization 209
Trigger Auto Deployment on Target Hosts 210
Troubleshoot Host Profile and Transport Node Profile 219
Stateful Servers 221
Supported NSX-T and ESXi versions 222
Prepare a Target Stateful Cluster 222
VMkernel Migration with Host Profile Applied 224
VMkernel Migration without Host Profile Applied 226

12 Getting Started with NSX Cloud 227

NSX Cloud Architecture and Components 227

Overview of Deploying NSX Cloud 229

Deploy NSX-T Data Center On-Prem Components 229

Install CSM 229

Join CSM with NSX Manager 230

Enable Access to Ports and Protocols 230

(Optional) Configure Proxy Servers 231

(Optional) Set Up vIDM for Cloud Service Manager 232

Add your Public Cloud Account 233

Adding your Microsoft Azure Subscription 233

Adding your AWS Account 239

Deploy the NSX Public Cloud Gateway 243

Deploying PCG in a VNet 245

Deploying PCG in a VPC 248

Link to a Transit VPC or VNet 252

Auto-Configurations after PCG Deployment or Linking 253

(Optional) Install NSX Tools on your Workload VMs 259

Undeploy or Unlink PCG 259

Remove the nsx.network tag in the Public Cloud 260

Disable Quarantine Policy in the NSX Enforced Mode 260

Delete User-created Logical Entities 261

Undeploy or Unlink from CSM 261

Troubleshooting PCG Undeployment 261

13 Getting Started with Federation 262

Federation Requirements 262

Install a Global Manager Appliance 263

Configuring the Global Manager and Local Managers 264

Make the Global Manager Active 264

Add a Location 264

14 Uninstalling NSX-T Data Center from a Host Transport Node 267

Verify Host Network Mappings for Uninstall 267

Uninstall NSX-T Data Center from a vSphere Cluster 269

Uninstall NSX-T Data Center from a Host in a vSphere Cluster 271

Uninstall NSX-T Data Center from a Standalone Host 272

Triggering Uninstallation from the vSphere Web Client 273

15 Troubleshooting Installation Issues 276

Installation Fails Due to Insufficient Space in Bootbank on ESXi Host 276

NSX-T Data Center Installation Guide

The *NSX-T Data Center Installation Guide* describes how to install the VMware NSX-T™ Data Center product. The information includes step-by-step configuration instructions and suggested best practices.

Intended Audience

This information is intended for anyone who wants to install or use NSX-T Data Center. This information is written for experienced system administrators who are familiar with virtual machine technology and network virtualization concepts.

Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to https://www.vmware.com/topics/glossary.

Related Documentation

You can find the VMware NSX® Intelligence™ documentation at https://docs.vmware.com/en/VMware-NSX-Intelligence/index.html. The NSX Intelligence 1.0 content was initially included and released with the NSX-T Data Center 2.5 documentation set.

Overview of NSX-T Data Center 1

In the same way that server virtualization programmatically creates and manages virtual machines, NSX-T Data Center network virtualization programmatically creates and managed software-based virtual networks.

With network virtualization, the functional equivalent of a network hypervisor reproduces the complete set of Layer 2 through Layer 7 networking services (for example, switching, routing, access control, firewalling, QoS) in software. As a result, these services can be programmatically assembled in any arbitrary combination, to produce unique, isolated virtual networks in a matter of seconds.

NSX-T Data Center works by implementing three separate but integrated planes: management, control, and data. These planes are implemented as a set of processes, modules, and agents residing on two types of nodes: NSX Manager and transport nodes.

- Every node hosts a management plane agent.
- NSX Manager nodes host API services and the management plane cluster daemons.
- NSX Controller nodes host the central control plane cluster daemons.
- Transport nodes host local control plane daemons and forwarding engines.

NSX Manager provides a three-node clustering support which merges policy manager, management, and central control services on a cluster of nodes. NSX Manager clustering provides high availability of the user interface and API. The convergence of management and control plane nodes reduces the number of virtual appliances that must be deployed and managed by the NSX-T Data Center administrator.

The NSX Manager appliance is available in three different sizes for different deployment scenarios.

- A small appliance for lab or proof-of-concept deployments.
- A medium appliance for deployments up to 64 hosts and a large appliance for customers who deploy to a large-scale environment.

See NSX Manager VM and Host Transport Node System Requirements and Configuration maximums tool.

This chapter includes the following topics:

- Key Concepts
- Overview of the NSX Manager

Key Concepts

The common NSX-T Data Center concepts that are used in the documentation and user interface.

Compute Manager

A compute manager is an application that manages resources such as hosts and VMs. One example is vCenter Server.

Control Plane

Computes runtime state based on configuration from the management plane. Control plane disseminates topology information reported by the data plane elements, and pushes stateless configuration to forwarding engines.

Data Plane

Performs stateless forwarding or transformation of packets based on tables populated by the control plane. Data plane reports topology information to the control plane and maintains packet level statistics.

External Network

A physical network or VLAN not managed by NSX-T Data Center. You can link your logical network or overlay network to an external network through an NSX Edge. For example, a physical network in a customer data center or a VLAN in a physical environment.

Logical Port Egress

Outbound network traffic leaving the VM or logical network is called egress because traffic is leaving virtual network and entering the data center.

Logical Port Ingress

Inbound network traffic leaving the data center and entering the VM is called ingress traffic.

Logical Router

NSX-T Data Center routing entity.

Logical Router Port

Logical network port to which you can attach a logical switch port or an uplink port to a physical network.

Logical Switch

Entity that provides virtual Layer 2 switching for VM interfaces and Gateway interfaces. A logical switch gives tenant network administrators the logical equivalent of a physical Layer 2 switch, allowing them to connect a set of VMs to a common broadcast domain. A logical switch is a logical entity independent of the physical hypervisor infrastructure and spans many hypervisors, connecting VMs regardless of their physical location.

In a multi-tenant cloud, many logical switches might exist side-by-side on the same hypervisor hardware, with each Layer 2 segment isolated from the others. Logical switches can be connected using logical routers, and logical routers can provide uplink ports connected to the external physical network.

Logical Switch Port

Logical switch attachment point to establish a connection to a virtual machine network interface or a logical router interface. The logical switch port reports applied switching profile, port state, and link status.

Management Plane

Provides single API entry point to the system, persists user configuration, handles user queries, and performs operational tasks on all of the management, control, and data plane nodes in the system. Management plane is also responsible for querying, modifying, and persisting use configuration.

NSX Edge Cluster

Collection of NSX Edge node appliances that have the same settings as protocols involved in high-availability monitoring.

NSX Edge Node

Component with the functional goal is to provide computational power to deliver the IP routing and the IP services functions.

NSX Managed Virtual Distributed Switch or KVM Open vSwitch

The NSX managed virtual distributed switch (N-VDS, previously known as hostswitch)or OVS is used for shared NSX Edge and compute cluster. N-VDS is required for overlay traffic configuration.

An N-VDS has two modes: standard and enhanced datapath. An enhanced datapath N-VDS has the performance capabilities to support NFV (Network Functions Virtualization) workloads.

NSX Manager

Node that hosts the API services, the management plane, and the agent services. NSX Manager is an appliance included in the NSX-T Data Center installation package. You can deploy the appliance in the role of `NSX Manager` or `nsx-cloud-service-manager`. Currently, the appliance only supports one role at a time.

NSX Manager Cluster

A cluster of NSX Managers that can provide high availability.

Open vSwitch (OVS)

Open source software switch that acts as a virtual switch within XenServer, Xen, KVM, and other Linux-based hypervisors.

Overlay Logical Network

Logical network implemented using Layer 2-in-Layer 3 tunneling such that the topology seen by VMs is decoupled from that of the physical network.

Physical Interface (pNIC)

Network interface on a physical server that a hypervisor is installed on.

Segment

Entity that provides virtual Layer 2 switching for VM interfaces and Gateway interfaces. A segment gives tenant network administrators the logical equivalent of a physical Layer 2 switch, allowing them to connect a set of VMs to a common broadcast domain. A segment is a logical entity independent of the physical hypervisor infrastructure and spans many hypervisors, connecting VMs regardless of their physical location. A segment is also known as a logical switch.

In a multi-tenant cloud, many segments might exist side-by-side on the same hypervisor hardware, with each Layer 2 segment isolated from the others. Segments can be connected using gateways, which can provide connectivity to the external physical network.

Tier-0 Gateway or Tier-0 Logical Router

The Tier-0 Gateway in the **Networking** tab interfaces with the physical network and can be realized as an active-active or active-standby cluster. The Tier-0 gateway runs BGP and peers with physical routers. In active-standby mode the gateway can also provide stateful services.

Tier-1 Gateway or Tier-1 Logical Router

The Tier-1 Gateway in the **Networking** tab connects to one Tier-0 gateway for northbound connectivity and one or more overlay networks for southbound connectivity. A Tier-1 gateway can be an active-standby cluster that provides stateful services.

Transport Zone

Collection of transport nodes that defines the maximum span for logical switches. A transport zone represents a set of similarly provisioned hypervisors and the logical switches that connect VMs on those hypervisors. It also has been registered with the NSX-T Data Center management plane and has NSX-T Data Center modules installed. For a hypervisor host or NSX Edge to be part of the NSX-T Data Center overlay, it must be added to the NSX-T Data Center transport zone.

Transport Node

A node capable of participating in an NSX-T Data Center overlay or NSX-T Data Center VLAN networking. For a KVM host, you can preconfigure the N-VDS, or you can have NSX Manager perform the configuration. For an ESXi host, NSX Manager always configures the N-VDS.

Uplink Profile

Defines policies for the links from hypervisor hosts to NSX-T Data Center logical switches or from NSX Edge nodes to top-of-rack switches. The settings defined by uplink profiles might include teaming policies, active/standby links, the transport VLAN ID, and the MTU setting. The transport VLAN set in the uplink profile tags overlay traffic only and the VLAN ID is used by the TEP endpoint.

VM Interface (vNIC)

Network interface on a virtual machine that provides connectivity between the virtual guest operating system and the standard vSwitch or vSphere distributed switch. The vNIC can be attached to a logical port. You can identify a vNIC based on its Unique ID (UUID).

Virtual Tunnel Endpoint

Each hypervisor has a Virtual Tunnel Endpoint (VTEP) responsible for encapsulating the VM traffic inside a VLAN header and routing the packet to a destination VTEP for further processing. Traffic can be routed to another VTEP on a different host or the NSX Edge gateway to access the physical network.

Overview of the NSX Manager

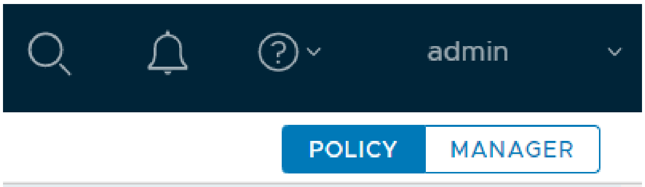
The NSX Manager provides a web-based user interface where you can manage your NSX-T environment. It also hosts the API server that processes API calls.

The NSX Manager interface provides two modes for configuring resources:

- Policy mode
- Manager mode

Accessing Policy Mode and Manager Mode

If present, you can use the **Policy** and **Manager** buttons to switch between the Policy and Manager modes. Switching modes controls which menus items are available to you.



- By default, if your environment contains only objects created through Policy mode, your user interface is in Policy mode and you do not see the **Policy** and **Manager** buttons.
- By default, if your environment contains any objects created through Manager mode, you see the **Policy** and **Manager** buttons in the top-right corner.

These defaults can be changed by modifying the user interface settings. See Configure User Interface Settings for more information.

The same **System** tab is used in the Policy and Manager interfaces. If you modify Edge nodes, Edge clusters, or transport zones, it can take up to 5 minutes for those changes to be visible in Policy mode. You can synchronize immediately using `POST /policy/api/v1/infra/sites/default/enforcement-points/default?action=reload`.

When to Use Policy Mode or Manager Mode

Be consistent about which mode you use. There are a few reasons to use one mode over the other.

- If you are deploying a new NSX-T Data Center environment, using **Policy** mode to create and manage your environment is the best choice in most situations.
    - Some features are not available in Policy mode. If you need these features, use **Manager** mode for all configurations.
- If you plan to use Federation, use **Policy** mode to create all objects. Global Manager supports only Policy mode.
- If you are upgrading from an earlier version of NSX-T Data Center and your configurations were created using the Advanced Networking & Security tab, use **Manager** mode.

  The menu items and configurations that were found under the Advanced Networking & Security tab are available in NSX-T Data Center 3.0 in **Manager** mode.

Important If you decide to use Policy mode, use it to create all objects. Do not use Manager mode to create objects.

Similarly, if you need to use Manager mode, use it to create all objects. Do not use Policy mode to create objects.

Table 1-1. When to Use Policy Mode or Manager Mode

Policy Mode	Manager Mode
Most new deployments should use Policy mode. Federation supports only Policy mode. If you want to use Federation, or might use it in future, use Policy mode.	Deployments which were created using the advanced interface, for example, upgrades from versions before Policy mode was available.
NSX Cloud deployments	Deployments which integrate with other plugins. For example, NSX Container Plug-in, Openstack, and other cloud management platforms.
Networking features available in Policy mode only: ■ DNS Services and DNS Zones ■ VPN ■ Forwarding policies for NSX Cloud	Networking features available in Manager mode only: ■ Forwarding up timer
Security features available in Policy mode only: ■ Endpoint Protection ■ Network Introspection (East-West Service Insertion) ■ Context Profiles ■ L7 applications ■ FQDN ■ New Distributed Firewall and Gateway Firewall Layout ■ Categories ■ Auto service rules ■ Drafts	Security features available in Manager mode only: ■ Bridge Firewall

Names for Objects Created in Policy Mode and Manager Mode

The objects you create have different names depending on which interface was used to create them.

Table 1-2. Object Names

Objects Created Using Policy Mode	Objects Created Using Manager Mode
Segment	Logical switch
Tier-1 gateway	Tier-1 logical router
Tier-0 gateway	Tier-0 logical router
Group	NSGroup, IP Sets, MAC Sets
Security Policy	Firewall section
Gateway firewall	Edge firewall

Policy and Manager APIs

The NSX Manager provides two APIs: Policy and Manager.

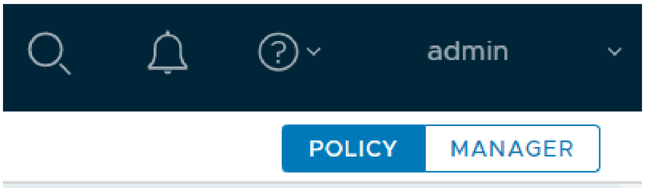
- The Policy API contains URIs that begin with `/policy/api`.
- The Manager API contains URIs that begin with `/api`.

For more information about using the Policy API, see the NSX-T Policy API Getting Started Guide.

Configure User Interface Settings

There are two possible modes in the NSX Manager web interface: Policy and Manager. You can control which mode is default, and if users can switch between them using the user interface mode buttons.

If present, you can use the **Policy** and **Manager** buttons to switch between the Policy and Manager modes. Switching modes controls which menus items are available to you.



- By default, if your environment contains only objects created through Policy mode, your user interface is in Policy mode and you do not see the **Policy** and **Manager** buttons.
- By default, if your environment contains any objects created through Manager mode, you see the **Policy** and **Manager** buttons in the top-right corner.

You can use the User Interface Settings to modify these defaults.

See Overview of the NSX Manager for more information about the modes.

Procedure

1 From your browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.

2 Navigate to **System > User Interface Settings** and click **Edit**.

3 Modify the user interface settings: **Toggle Visibility** and **Default Mode**.

Toggle Visibility	Description
Visible to All Users	If Manager mode objects are present, the mode buttons are visible to all users.
Visible to Users with the Enterprise Admin Role	If Manager mode objects are present, the mode buttons are visible to users with the **Enterprise Admin** role.
Hidden from All Users	Even if Manager mode objects are present, the mode buttons are hidden from all users.

Default Mode can be set to Policy or Manager.

NSX-T Data Center Installation Workflows

2

You can install NSX-T Data Center on vSphere or KVM hosts. You can also configure a bare metal server to use NSX-T Data Center.

To install or configure any of the hypervisors or bare metal, follow the recommended tasks in the workflows.

This chapter includes the following topics:

- NSX-T Data Center Workflow for vSphere
- NSX-T Data Center Installation Workflow for KVM
- NSX-T Data Center Configuration Workflow for Bare Metal Server

NSX-T Data Center Workflow for vSphere

Use the checklist to track your installation progress on a vSphere host.

Follow the recommended order of procedures.

1. Review the NSX Manager installation requirements. See Chapter 4 NSX Manager Installation.
2. Configure the necessary ports and protocols. See Ports and Protocols.
3. Install the NSX Manager. See Install NSX Manager and Available Appliances.
4. Log in to the newly created NSX Manager. See Log In to the Newly Created NSX Manager .
5. Configure a compute manager. See Add a Compute Manager.
6. Deploy additional NSX Manager nodes to form a cluster. See Deploy NSX Manager Nodes to Form a Cluster from UI.
7. Review the NSX Edge installation requirements. See NSX Edge Installation Requirements.
8. Install NSX Edges. See Install an NSX Edge on ESXi Using the vSphere GUI.
9. Create an NSX Edge cluster. See Create an NSX Edge Cluster.
10. Create transport zones. See Create Transport Zones.
11. Create host transport nodes. See Create a Standalone Host or Bare Metal Server Transport Node or Configure a Managed Host Transport Node.

NSX-T Data Center Installation Workflow for KVM

Use the checklist to track your installation progress on a KVM host.

Follow the recommended order of procedures.

1. Prepare your KVM environment. See Set Up KVM.
2. Review the NSX Manager installation requirements. See Chapter 4 NSX Manager Installation.
3. Configure the necessary ports and protocols. See Ports and Protocols.
4. Install the NSX Manager. See Install NSX Manager on KVM.
5. Log in to the newly created NSX Manager. See Log In to the Newly Created NSX Manager .
6. Configure third-party packages on the KVM host. See Install Third-Party Packages on a KVM Host.
7. Deploy additional NSX Manager nodes to form a cluster. See Deploy NSX Manager Nodes to Form a Cluster Using CLI .
8. Review the NSX Edge installation requirements. See NSX Edge Installation Requirements.
9. Install NSX Edges. See Install NSX Edge on Bare Metal .
10. Create an NSX Edge cluster. See Create an NSX Edge Cluster.
11. Create transport zones. See Create Transport Zones.
12. Create host transport nodes. See Create a Standalone Host or Bare Metal Server Transport Node.

    A virtual switch is created on each host. The management plane sends the host certificates to the control plane, and the management plane pushes control plane information to the hosts. Each host connects to the control plane over SSL presenting its certificate. The control plane validates the certificate against the host certificate provided by the management plane. The controllers accept the connection upon successful validation.

Post-Installation

When the hosts are transport nodes, you can create transport zones, logical switches, logical routers, and other network components through the NSX Manager UI or API at any time. When NSX Edges and hosts join the management plane, the NSX-T Data Center logical entities and configuration state are pushed to the NSX Edges and hosts automatically.

For more information, see the *NSX-T Data Center Administration Guide*.

NSX-T Data Center Configuration Workflow for Bare Metal Server

Use the checklist to track your progress when configuring bare metal server to use NSX-T Data Center.

Follow the recommended order of procedures.

1. Review the bare metal requirements. See Bare Metal Server System Requirements.

2 Configure the necessary ports and protocols. See Ports and Protocols.

3 Install the NSX Manager. See Install NSX Manager on KVM.

4 Configure third-party packages on the bare metal server. See Install Third-Party Packages on a Bare Metal Server.

5 Create host transport nodes. See Create a Standalone Host or Bare Metal Server Transport Node.

A virtual switch is created on each host. The management plane sends the host certificates to the control plane, and the management plane pushes control plane information to the hosts. Each host connects to the control plane over SSL presenting its certificate. The control plane validates the certificate against the host certificate provided by the management plane. The controllers accept the connection upon successful validation.

6 Create an application interface for bare metal server workload. See Create Application Interface for Bare Metal Server Workloads.

Preparing for Installation

3

Before installing NSX-T Data Center, make sure your environment is prepared.

This chapter includes the following topics:

- System Requirements
- Ports and Protocols

System Requirements

Before you install NSX-T Data Center, your environment must meet specific hardware and resource requirements.

NSX Manager VM and Host Transport Node System Requirements

Before you install an NSX Manager or other NSX-T Data Center appliances, make sure that your environment meets the supported requirements.

Supported Hypervisors as Host Transport Nodes

Hypervisor	Version	CPU Cores	Memory
vSphere	Supported vSphere version	4	16 GB
CentOS Linux KVM	7.7, 7.6	4	16 GB
Red Hat Enterprise Linux (RHEL) KVM	7.7, 7.6	4	16 GB
SUSE Linux Enterprise Server KVM	12 SP3, 12 SP4	4	16 GB
Ubuntu KVM	16.04, 18.04.2 LTS	4	16 GB

Note To avoid memory errors on a hypervisor host running vSphere ESXi version 7.x.x, ensure that at least 16 GB is available before deploying NSX Manager.

Table 3-1. Supported Hosts for NSX Managers

Support Description	Hypervisor
ESXi	For supported hosts, see the VMware Product Interoperability Matrices.
KVM	RHEL 7.6 and Ubuntu 18.04.2 LTS

For ESXi hosts, NSX-T Data Center supports the Host Profiles and Auto Deploy features on vSphere 6.7 U1 or higher. See *Understanding vSphere Auto Deploy* in the *VMware ESXi Installation and Setup* documentation for more information.

Caution On RHEL and Ubuntu, the `yum update` command might update the kernel version, which must not be greater than 4.14.x, and break the compatibility with NSX-T Data Center. Disable the automatic kernel update when you run `yum update`. Also, after running `yum install`, verify that NSX-T Data Center supports the kernel version.

Hypervisor Host Network Requirements

The NIC card used must be compatible with the ESXi version that is running NSX-T Data Center. For supported NIC card, see the VMware Compatibility Guide.

Tip To quickly identify compatible cards in the Compatibility Guide, apply the following criteria:

- Under **I/O Device Type**, select `Network`.
- Optionally, to use supported GENEVE encapsulation, under **Features**, select the GENEVE options.
- Optionally, to use Enhanced Data Path, select `N-VDS Enhanced Data Path`.

Enhanced Data Path NIC Drivers

Download the supported NIC drivers from the My VMware page.

NIC Card	NIC Driver
Intel 82599	ixgben 1.1.0.26-1OEM.670.0.0.7535516
Intel(R) Ethernet Controller X710 for 10GbE SFP+ Intel(R) Ethernet Controller XL710 for 40GbE QSFP+	i40en 1.2.0.0-1OEM.670.0.0.8169922

NSX Manager VM Resource Requirements

Thin virtual disk size is 3.8 GB and thick virtual disk size is 300 GB.

Appliance Size	Memory	vCPU	Disk Space	VM Hardware Version
NSX Manager Extra Small	8 GB	2	300 GB	10 or later
NSX Manager Small VM	16 GB	4	300 GB	10 or later

Appliance Size	Memory	vCPU	Disk Space	VM Hardware Version
NSX Manager Medium VM	24 GB	6	300 GB	10 or later
NSX Manager Large VM	48 GB	12	300 GB	10 or later

Note NSX Manager provides multiple roles which previously required separate appliances. This includes the policy role, the management plane role and the central control plane role. The central control plane role was previously provide by the NSX Controller appliance.

- You can use the Extra Small VM resource size only for the Cloud Service Manager appliance (CSM). Deploy CSM in the Extra Small VM size or higher, as required. See Overview of Deploying NSX Cloud for more information.
- The NSX Manager Small VM appliance size is suitable for lab and proof-of-concept deployments, and must not be used in production.
- The NSX Manager Medium VM appliance size is suitable for typical production environments. An NSX-T management cluster formed using this appliance size can support up to 64 hypervisors.
- The NSX Manager Large VM appliance size is suitable for large-scale deployments. An NSX-T management cluster formed using this appliance size can support more than 64 hypervisors.

For maximum scale using the NSX Manager Large VM appliance size, go to the VMware Configuration Maximums tool at https://configmax.vmware.com/guest and select NSX-T Data Center from the product list.

Language Support

NSX Manager has been localized into multiple languages: English, German, French, Japanese, Simplified Chinese, Korean, Traditional Chinese, and Spanish.

NSX Manager Browser Support

The following browsers are recommended for working with NSX Manager.

Browser	Windows 10	Mac OS X 10.13, 10.14	Ubuntu 18.04
Google Chrome 80	Yes	Yes	Yes
Mozilla Firefox 72	Yes	Yes	Yes

Browser	Windows 10	Mac OS X 10.13, 10.14	Ubuntu 18.04
Microsoft Edge 80	Yes		
Apple Safari 13		Yes	

Note

- Internet Explorer is not supported.
- Supported Browser minimum resolution is 1280 x 800 px.
- Language support: NSX Manager has been localized into multiple languages: English, German, French, Japanese, Simplified Chinese, Korean, Traditional Chinese, and Spanish. However, because NSX Manager localization utilizes the browser language settings, ensure that your settings match the desired language. There is no language preference setting within the NSX Manager interface itself.

Network Latency Requirements

The maximum network latency between NSX Managers in a NSX Manager cluster is 10ms.

The maximum network latency between NSX Managers and Transport Nodes is 150ms.

Storage Requirements

- The maximum disk access latency is under 10ms.
- It is recommended that NSX Managers be placed on shared storage.
- Storage should be highly available to avoid a storage outage causing all NSX Manager file systems to be placed into read-only mode upon event of a storage failure.

  Please consult documentation for your storage technology on how to best design a highly available storage solution.

NSX Edge VM System Requirements

Before you install NSX Edge, make sure that your environment meets the supported requirements.

Note The following conditions apply to the hosts for the NSX Edge nodes:

- NSX Edge nodes are supported only on ESXi-based hosts with Intel-based and AMD-based chipsets.

  Otherwise, vSphere EVC mode may prevent NSX Edge nodes from starting, showing an error message in the console.
- If vSphere EVC mode is enabled for the host for the NSX Edge VM, the CPU must be Haswell or later generation.
- Only VMXNET3 vNIC is supported for the NSX Edge VM.

NSX Cloud Note If using NSX Cloud, note that the NSX Public Cloud Gateway(PCG) is deployed in a single default size for each supported public cloud. See Deploy the NSX Public Cloud Gateway for details.

NSX Edge VM Resource Requirements

Appliance Size	Memory	vCPU	Disk Space	VM Hardware Version	Notes
NSX Edge Small	4 GB	2	200 GB	11 or later (vSphere 6.0 or later)	The NSX Edge Small VM appliance size is suitable for lab and proof-of-concept deployments.
NSX Edge Medium	8 GB	4	200 GB	11 or later (vSphere 6.0 or later)	The NSX Edge Medium appliance size is suitable for a typical production environments.
NSX Edge Large	32 GB	8	200 GB	11 or later (vSphere 6.0 or later)	The NSX Edge Large appliance size is suitable for environments with load balancing. See Scaling Load Balancer Resources in the *NSX-T Data Center Administration Guide*.
NSX Edge Extra Large	64 GB	16	200 GB	11 or later (vSphere 6.0 or later)	The NSX Edge Extra Large appliance size is suitable for environments with load balancing. See Scaling Load Balancer Resources in the *NSX-T Data Center Administration Guide*.

NSX Edge VM CPU Requirements

For the DPDK support, the underlaying platform needs to meet the following requirements:

- CPU must have AESNI capability.
- CPU must have 1 GB Huge Page support.

Hardware	Type
CPU	■ Intel Xeon E7-xxxx (Westmere-EX and later CPU generation) ■ Intel Xeon 56xx (Westmere-EP) ■ Intel Xeon E5-xxxx (Sandy Bridge and later CPU generation) ■ Intel Xeon Platinum (all generations) ■ Intel Xeon Gold (all generations) ■ Intel Xeon Silver (all generations) ■ Intel Xeon Bronze (all generations)
	■ AMD EPYC™ 7XX1 series (Naples) ■ AMD EPYC™ 3000 Embedded Family and newer ■ AMD EPYC™ 7XX2 series (Rome)

NSX Edge Bare Metal Requirements

Before you configure the NSX Edge bare metal, make sure that your environment meets the supported requirements.

NSX Edge Bare Metal Memory, CPU, and Disk Requirements

Minimum Requirements

Memory	CPU Cores	Disk Space
32 GB	8	200 GB

Recommended Requirements

Memory	CPU Cores	Disk Space
256 GB	24	200 GB

NSX Edge Bare Metal DPDK CPU Requirements

For the DPDK support, the underlaying platform needs to meet the following requirements:

- CPU must have AES-NI capability.
- CPU must have 1 GB Huge Page support.

Hardware	Type
CPU	■ Intel Xeon E7-xxxx (Westmere-EX and later CPU generation) ■ Intel Xeon 56xx (Westmere-EP) ■ Intel Xeon E5-xxxx (Sandy Bridge and later CPU generation) ■ Intel Xeon Platinum (all generations) ■ Intel Xeon Gold (all generations) ■ Intel Xeon Silver (all generations) ■ Intel Xeon Bronze (all generations)
	■ AMD EPYC 7xx1 Series (Naples) ■ AMD EPYC 3000 Embedded Family and newer ■ AMD EPYC 7xx2 Series (Rome)

NSX Edge Bare Metal Hardware Requirements

Verify that the bare metal NSX Edge hardware is listed in this URL https://certification.ubuntu.com/server/models/?release=18.04%20LTS&category=Server. If the hardware is not listed, the storage, video adapter, or motherboard components might not work on the NSX Edge appliance.

NSX Edge Bare Metal NIC Requirements

NIC Type	Description	PCI Device ID	Firmware Version
Mellanox ConnectX-4 EN	PCI_DEVICE_ID_MELLANOX_CONNECTX4	0x1013	12.21.1000 and above
Mellanox ConnectX-4 Lx EN	PCI_DEVICE_ID_MELLANOX_CONNECTX4LX	0x1015	14.21.1000 and above
Mellanox ConnectX-5	PCI_DEVICE_ID_MELLANOX_CONNECTX5	0x1017	16.21.1000 and above

NIC Type	Description	PCI Device ID	Firmware Version
Mellanox ConnectX-5 EX	PCI_DEVICE_ID_MELLANOX_CONNECTX5EX	0x1019	16.21.1000 and above
Intel XXV710	I40E_DEV_ID_25G_B	0x158A	6.0.1
	I40E_DEV_ID_25G_SFP28	0x158B	6.0.1
Intel X520/Intel 82599	IXGBE_DEV_ID_82599_KX4	0x10F7	n/a
	IXGBE_DEV_ID_82599_KX4_MEZZ	0x1514	n/a
	IXGBE_DEV_ID_82599_KR	0x1517	n/a
	IXGBE_DEV_ID_82599_COMBO_BACKPLANE	0x10F8	n/a
	IXGBE_SUBDEV_ID_82599_KX4_KR_MEZZ	0x000C	n/a
	IXGBE_DEV_ID_82599_CX4	0x10F9	n/a
	IXGBE_DEV_ID_82599_SFP	0x10FB	n/a
	IXGBE_SUBDEV_ID_82599_SFP	0x11A9	n/a
	IXGBE_SUBDEV_ID_82599_RNDC	0x1F72	n/a
	IXGBE_SUBDEV_ID_82599_560FLR	0x17D0	n/a
	IXGBE_SUBDEV_ID_82599_ECNA_DP	0x0470	n/a
	IXGBE_DEV_ID_82599_SFP_EM	0x1507	n/a
	IXGBE_DEV_ID_82599_SFP_SF2	0x154D	n/a
	IXGBE_DEV_ID_82599_SFP_SF_QP	0x154A	n/a
	IXGBE_DEV_ID_82599_QSFP_SF_QP	0x1558	n/a
	IXGBE_DEV_ID_82599EN_SFP	0x1557	n/a
	IXGBE_DEV_ID_82599_XAUI_LOM	0x10FC	n/a
	IXGBE_DEV_ID_82599_T3_LOM	0x151C	n/a
Intel X540	IXGBE_DEV_ID_X540T	0x1528	n/a
	IXGBE_DEV_ID_X540T1	0x1560	n/a
Intel X550	IXGBE_DEV_ID_X550T	0x1563	n/a
	IXGBE_DEV_ID_X550T1	0x15D1	n/a
Intel X710	I40E_DEV_ID_SFP_X710	0x1572	6.0.1
	I40E_DEV_ID_KX_C	0x1581	6.0.1
	I40E_DEV_ID_10G_BASE_T	0x1586	6.0.1

NIC Type	Description	PCI Device ID	Firmware Version
Intel XL710	I40E_DEV_ID_KX_B I40E_DEV_ID_QSFP_A I40E_DEV_ID_QSFP_B I40E_DEV_ID_QSFP_C	0x1580 0x1583 0x1584 0x1585	6.0.1 6.0.1 6.0.1 6.0.1
Cisco VIC 1387	Cisco UCS Virtual Interface Card 1387	0x0043	n/a

Note For all the supported NICs listed above, verify that the media adapters and cables you use follow the vendor's supported media types. Any media adapter or cables not supported by the vendor can result in unpredictable behavior, including the inability to boot up due to an unrecognized media adapter. See the NIC vendor documentation for information about supported media adapters and cables.

Bare Metal Server System Requirements

Before you configure the bare metal server, make sure that your server meets the supported requirements.

Important The user performing the installation may require `sudo` command permissions for some of the procedures. See Install Third-Party Packages on a Bare Metal Server.

Bare Metal Server Requirements

Operating System	Version	CPU Cores	Memory
CentOS Linux	7.7 7.6 (kernel: 3.10.0-957)	4	16 GB
Red Hat Enterprise Linux (RHEL)	7.7 7.6 (kernel: 3.10.0-957)	4	16 GB
SUSE Linux Enterprise Server	12 sp3, 12 sp4	4	16 GB
Ubuntu	16.04.2 LTS (kernel: 4.4.0-*) 18.04	4	16 GB
Windows Server	2016	4	16 GB

Note Hosts running Ubuntu 18.04.2 LTS must be upgraded from 16.04 or freshly installed.

Bare Metal Linux Container Requirements

For bare metal Linux container requirements, see the *NSX Container Plug-in for OpenShift - Installation and Administration Guide*.

Ports and Protocols

Ports and protocols allow node-to-node communication paths in NSX-T Data Center, the paths are secured and authenticated, and a storage location for the credentials are used to establish mutual authentication.

Configure the ports and protocols required to be open on both the physical and the host hypervisor firewalls in NSX-T Data Center. Refer to https://ports.vmware.com/home/NSX-T-Data-Center for more details.

By default, all certificates are self-signed certificates. The northbound GUI and API certificates and private keys can be replaced by CA signed certificates.

There are internal daemons that communicate over the loopback or UNIX domain sockets:

- KVM: MPA, OVS
- ESXi: nsx-cfgagent, ESX-DP (in the kernel)

Note To get access to NSX-T Data Center nodes, you must enable SSH on these nodes.

NSX Cloud Note See Enable Access to Ports and Protocols for a list of ports required for deploying NSX Cloud.

NSX Manager Installation

4

NSX Manager provides a graphical user interface (GUI) and REST APIs for creating, configuring, and monitoring NSX-T Data Center components such as logical switches, logical routers, and firewalls.

NSX Manager provides a system view and is the management component of NSX-T Data Center.

For high availability, NSX-T Data Center supports a management cluster of three NSX Managers. For a production environment, deploying a management cluster is recommended. For a proof-of-concept environment, you can deploy a single NSX Manager.

In a vSphere environment, the following functions are supported by NSX Manager:

- vCenter Server can use the vMotion function to live migrate NSX Manager across hosts and clusters.
- vCenter Server can use the Storage vMotion function to live migrate NSX Manager across hosts and clusters.
- vCenter Server can use the Distributed Resource Scheduler function to rebalance NSX Manager across hosts and clusters.
- vCenter Server can use the Anti-affinity function to manage NSX Manager across hosts and clusters.

NSX Manager Deployment, Platform, and Installation Requirements

The following table details the NSX Manager deployment, platform, and installation requirements

Requirements	Description
Supported deployment methods	■ OVA/OVF ■ QCOW2
Supported platforms	See NSX Manager VM and Host Transport Node System Requirements. On ESXi, it is recommended that the NSX Manager appliance be installed on shared storage.
IP address	An NSX Manager must have a static IP address. You cannot change the IP address after installation. Only IPv4 addresses are supported.

Requirements	Description
NSX-T Data Center appliance password	■ At least 12 characters ■ At least one lower-case letter ■ At least one upper-case letter ■ At least one digit ■ At least one special character ■ At least five different characters ■ Default password complexity rules are enforced by the following Linux PAM module arguments: ■ `retry=3`: The maximum number of times a new password can be entered, for this argument at the most 3 times, before returning with an error. ■ `minlen=12`: The minimum acceptable size for the new password. In addition to the number of characters in the new password, credit (of +1 in length) is given for each different kind of character (other, upper, lower and digit). ■ `difok=0`: The minimum number of bytes that must be different in the new password. Indicates similarity between the old and new password. With a value 0 assigned to `difok`, there is no requirement for any byte of the old and new password to be different. An exact match is allowed. ■ `lcredit=1`: The maximum credit for having lower case letters in the new password. If you have less than or 1 lower case letter, each letter will count +1 towards meeting the current `minlen` value. ■ `ucredit=1`: The maximum credit for having upper case letters in the new password. If you have less than or 1 upper case letter each letter will count +1 towards meeting the current `minlen` value. ■ `dcredit=1`: The maximum credit for having digits in the new password. If you have less than or 1 digit, each digit will count +1 towards meeting the current `minlen` value. ■ `ocredit=1`: The maximum credit for having other characters in the new password. If you have less than or 1 other characters, each character will count +1 towards meeting the current minlen value. ■ `enforce_for_root`: The password is set for the root user. **Note** For more details on Linux PAM module to check the password against dictionary words, refer to the man page.
Hostname	When installing NSX Manager, specify a hostname that does not contain invalid characters such as an underscore or special characters such as dot ".". If the hostname contains any invalid character or special characters, after deployment the hostname will be set to **`nsx-manager`**. For more information about hostname restrictions, see https://tools.ietf.org/html/rfc952 and https://tools.ietf.org/html/rfc1123.
VMware Tools	The NSX Manager VM running on ESXi has VMTools installed. Do not remove or upgrade VMTools.

Requirements	Description
System	■ Verify that the system requirements are met. See System Requirements. ■ Verify that the required ports are open. See Ports and Protocols. ■ Verify that a datastore is configured and accessible on the ESXi host. ■ Verify that you have the IP address and gateway, DNS server IP addresses, domain search list, and the NTP server IP address for the NSX Manager to use. ■ If you do not already have one, create the target VM port group network. Place the NSX-T Data Center appliances on a management VM network. If you have multiple management networks, you can add static routes to the other networks from the NSX-T Data Center appliance. ■ Plan your NSX Manager IPv4 IP addressing scheme.
OVF Privileges	Verify that you have adequate privileges to deploy an OVF template on the ESXi host. A management tool that can deploy OVF templates, such as vCenter Server or the vSphere Client. The OVF deployment tool must support configuration options to allow for manual configuration. OVF tool version must be 4.0 or later.
Client Plug-in	The Client Integration Plug-in must be installed.

Note On an NSX Manager fresh install, reboot, or after an `admin` password change when prompted on first login, it might take several minutes for the NSX Manager to start.

NSX Manager Installation Scenarios

Important When you install NSX Manager from an OVA or OVF file, either from vSphere Client or the command line, OVA/OVF property values such as user names and passwords are not validated before the VM is powered on. However, the static IP address field is a mandatory field to install NSX Manager.

- If you specify a user name for the `admin` or `audit` user, the name must be unique. If you specify the same name, it is ignored and the default names (`admin` and `audit`) is used.
- If the password for the `admin` user does not meet the complexity requirements, you must log in to NSX Manager through SSH or at the console as the `admin` user with the password `default`. You are prompted to change the password.
- If the password for the `audit` user does not meet the complexity requirements, the user account is disabled. To enable the account, log in to NSX Manager through SSH or at the console as the `admin` user and run the command `set user audit` to set the `audit` user's password (the current password is an empty string).

- If the password for the `root` or `admin` user does not meet the complexity requirements, you must log in to NSX Manager through SSH or at the console as `root` with password `vmware` and `admin` with password `default`. You are prompted to change the password.

Caution Changes made to the NSX-T Data Center while logged in with the `root` user credentials might cause system failure and potentially impact your network. You can only make changes using the `root` user credentials with the guidance of VMware Support team.

Note The core services on the appliance do not start until a password with sufficient complexity is set.

After you deploy NSX Manager from an OVA file, you cannot change the VM's IP settings by powering off the VM and modifying the OVA settings from vCenter Server.

Configuring NSX Manager for Access by the DNS Server

By default, transport nodes access NSX Managers based on their IP addresses. However, this can be based also on the DNS names of the NSX Managers.

You enable FQDN usage by publishing the FQDNs of the NSX Managers.

Note Enabling FQDN usage (DNS) on NSX Managers is required for multisite Lite and NSX Cloud and deployments. (It is optional for all other deployment types.) See *Multisite Deployment of NSX-T Data Center* in the *NSX-T Data Center Administration Guide* and Chapter 12 Getting Started with NSX Cloud in this guide.

Publishing the FQDNs of the NSX Managers

After installing the NSX-T Data Center core components and CSM, to enable NAT using FQDN, you must set up the forward and reverse lookup entries for the manager nodes on the DNS server.

Important It is highly recommended that you configure both the forward and reverse lookup entries for the NSX Managers' FQDN with a short TTL, for example, 600 seconds.

In addition, you must also enable publishing the NSX Manager FQDNs using the NSX-T API.

Example request: `PUT https://<nsx-mgr>/api/v1/configs/management`

```
{
  "publish_fqdns": true,
  "_revision": 0
}
```

Example response:

```
{
  "publish_fqdns": true,
  "_revision": 1
}
```

See the *NSX-T Data Center API Guide* for details.

Note After publishing the FQDNs, validate access by the transport nodes as described in the next section.

Validating Access via FQDN by Transport Nodes

After publishing the FQDNs of the NSX Managers, verify that the transport nodes are successfully accessing the NSX Managers.

Using SSH, log into a transport node such as a hypervisor or Edge node, and run the `get controllers` CLI command.

Example response:

```
Controller IP    Port  SSL     Status      Is Physical Master   Session State    Controller FQDN
192.168.60.5    1235  enabled  connected  true                 up               nsxmgr.corp.com
```

This chapter includes the following topics:

- Modifying the Default Admin Password Expiration

Modifying the Default Admin Password Expiration

By default, the administrative password for the NSX Manager and NSX Edge appliances expires after 90 days. However, you can reset the expiration period after initial installation and configuration.

If the password expires, you will be unable to log in and manage components. Additionally, any task or API call that requires the administrative password to execute will fail. If your password expires, see Knowledge Base article 70691 NSX-T admin password expired.

Procedure

1 Use a secure program to connect to the NSX CLI console.

2 Reset the expiration period.

   You can set the expiration period for between 1 and 9999 days.

   ```
   nsxcli> set user admin password-expiration <1 - 9999>
   ```

   Note Alternatively, you can use API commands to set the admin password expiration period.

3 (Optional) You can disable password expiry so the apassword never expires.

   ```
   nsxcli> clear user audit password-expiration
   ```

Installing NSX-T Data Center on vSphere

5

You can install the NSX-T Data Center components, NSX Manager and NSX Edge using the UI or CLI.

Make sure that you have the supported vSphere version. See vSphere support.

This chapter includes the following topics:

- Install NSX Manager and Available Appliances
- Configure a Virtual IP (VIP) Address for a Cluster
- Disable Snapshots on NSX-T Data Center Appliances

Install NSX Manager and Available Appliances

You can use the vSphere Client to deploy NSX Manager virtual appliances. The same OVF file can used to deploy three different types of appliances: NSX Manager, NSX Cloud Service Manager for NSX Cloud, and Global Manager for Federation.

Cloud Service Manager is a virtual appliance that uses NSX-T Data Center components and integrates them with your public cloud.

Prerequisites

- Verify that the system requirements are met. See System Requirements.
- Verify that the required ports are open. See Ports and Protocols.
- Verify that a datastore is configured and accessible on the ESXi host.
- Verify that you have the IP address and gateway, DNS server IP addresses, domain search list, and the NTP server IP address for the NSX Manager to use.
- If you do not already have one, create the target VM port group network. Place the NSX-T Data Center appliances on a management VM network.

  If you have multiple management networks, you can add static routes to the other networks from the NSX-T Data Center appliance.
- Plan your NSX Manager IPv4 IP addressing scheme.

Procedure

1 Locate the NSX-T Data Center OVA file on the VMware download portal.

Either copy the download URL or download the OVA file.

2 In the vSphere Client, select the host or host cluster on which to install NSX-T Data Center.

3 Right-click and select **Deploy OVF template** to start the installation wizard.

4 Enter the download OVA URL or navigate to the OVA file, and click **Next**.

5 Enter a name and a location for the NSX Manager VM, and click **Next**.

The name you enter appears in the vSphere and vCenter Server inventory.

6 Select a compute resource for the NSX Manager appliance, and click **Next**.

- To install on a ESXi host managed by vCenter, select a host on which to deploy the NSX Manager appliance.
- To install on a standalone ESXi host, select the host on which to deploy the NSX Manager appliance.

7 Review and verify the OVF template details, and click **Next**.

8 Specify the deployment configuration size, and click **Next**.

The Description panel on the right side of the wizard shows the details of selected configuration.

9 Specify storage for the configuration and disk files.

a Select the virtual disk format.

b Select the VM storage policy.

c Specify the datastore to store the NSX Manager appliance files.

d Click **Next**.

10 Select a destination network for each source network.

11 Select the port group or destination network for the NSX Manager.

12 Configure IP Allocation settings.

a For IP allocation, specify `Static - Manual`.

b For IP protocol, select `IPv4`.

13 Click **Next**.

The following steps are all located in the Customize Template section of the Deploy OVF Template wizard.

14 In the Application section, enter the system root, CLI admin, and audit passwords for the NSX Manager. The `root` and `admin` credentials are mandatory fields.

Your passwords must comply with the password strength restrictions.

- At least 12 characters

- At least one lower-case letter
- At least one upper-case letter
- At least one digit
- At least one special character
- At least five different characters
- Default password complexity rules are enforced by the following Linux PAM module arguments:
  - `retry=3`: The maximum number of times a new password can be entered, for this argument at the most 3 times, before returning with an error.
  - `minlen=12`: The minimum acceptable size for the new password. In addition to the number of characters in the new password, credit (of +1 in length) is given for each different kind of character (other, upper, lower and digit).
  - `difok=0`: The minimum number of bytes that must be different in the new password. Indicates similarity between the old and new password. With a value 0 assigned to `difok`, there is no requirement for any byte of the old and new password to be different. An exact match is allowed.
  - `lcredit=1`: The maximum credit for having lower case letters in the new password. If you have less than or 1 lower case letter, each letter will count +1 towards meeting the current `minlen` value.
  - `ucredit=1`: The maximum credit for having upper case letters in the new password. If you have less than or 1 upper case letter each letter will count +1 towards meeting the current `minlen` value.
  - `dcredit=1`: The maximum credit for having digits in the new password. If you have less than or 1 digit, each digit will count +1 towards meeting the current `minlen` value.
  - `ocredit=1`: The maximum credit for having other characters in the new password. If you have less than or 1 other characters, each character will count +1 towards meeting the current minlen value.
  - `enforce_for_root`: The password is set for the root user.

  Note For more details on Linux PAM module to check the password against dictionary words, refer to the man page.

15 In the Optional parameters section, leave the password fields blank. It is to avoid the risk of compromising passwords set for VMC roles by a user who has access to the vCenter Server. When deploying VMC for NSX-T Data Center, this field is used internally to set passwords for the Cloud Admin and Cloud Audit roles.

16 In the Network Properties section, enter the hostname of the NSX Manager.

Note The host name must be a valid domain name. Ensure that each part of the host name (domain/subdomain) that is separated by dot starts with an alphabet character.

17 Select a **Rolename** for the appliance. The default role is **NSX Manager**.

- To install an NSX Manager appliance, select the **NSX Manager** role.
- To install a Global Manager appliance for a Federation deployment, select the **NSX Global Manager** role.

  See Chapter 13 Getting Started with Federation for details.
- To install a Cloud Service Manager (CSM) appliance for an NSX Cloud deployment, select the **nsx-cloud-service-manager** role.

  See Overview of Deploying NSX Cloud for details.

18 (Required fields) Enter the default gateway, management network IPv4, and management network netmask.

Important If you leave the Management Network IPv4 field blank without entering a static IP address, no IP address is assigned to the NSX Manager during deployment of the appliance. You cannot access the NSX Manager when it powers on. The workaround is to re-deploy the NSX Manager appliance.

19 In the DNS section, enter the DNS Server list and Domain Search list.

20 In the Services Configuration section, enter the NTP Server List.

Optionally, you can enable SSH service and allow root SSH login. (Not recommended.)

21 Verify that all your custom OVF template specification is accurate and click **Finish** to initiate the installation.

The installation might take 7-8 minutes.

22 From the vSphere Client, open NSX Manager VM console to track the boot process.

23 After the NSX Manager boots, log in to the CLI as admin and run the `get interface eth0` command to verify that the IP address was applied as expected.

24 Enter the `get services` command to verify that all the services are running.

25 Verify that your NSX Manager has the required connectivity.

Make sure that you can perform the following tasks.

- Ping your NSX Manager from another machine.
- The NSX Manager can ping its default gateway.
- The NSX Manager can ping the hypervisor hosts that are in the same network as the NSX Manager using the management interface.
- The NSX Manager can ping its DNS server and its NTP server.
- If you enabled SSH, make sure that you can SSH to your NSX Manager.

If connectivity is not established, make sure that the network adapter of the virtual appliance is in the proper network or VLAN.

What to do next

Log in to the NSX Manager from a supported web browser. See Log In to the Newly Created NSX Manager .

Install NSX Manager on ESXi Using the Command-Line OVF Tool

If you prefer to automate or use CLI for the NSX Manager installation, you can use the VMware OVF Tool, which is a command-line utility.

By default, `nsx_isSSHEnabled` and `nsx_allowSSHRootLogin` are both disabled for security reasons. When they are disabled, you cannot SSH or log in to the NSX Manager command line. If you enable `nsx_isSSHEnabled` but not `nsx_allowSSHRootLogin`, you can SSH to NSX Manager but you cannot log in as root.

Prerequisites

- Verify that the system requirements are met. See System Requirements.
- Verify that the required ports are open. See Ports and Protocols.
- Verify that a datastore is configured and accessible on the ESXi host.
- Verify that you have the IP address and gateway, DNS server IP addresses, domain search list, and the NTP server IP address for the NSX Manager to use.
- If you do not already have one, create the target VM port group network. Place the NSX-T Data Center appliances on a management VM network.

  If you have multiple management networks, you can add static routes to the other networks from the NSX-T Data Center appliance.
- Plan your NSX Manager IPv4 IP addressing scheme.

Procedure

1. Run the `ovftool` command with the appropriate parameters.

   The process depends on whether the host is standalone or managed by vCenter Server.

   - For a standalone host:

     Note On a standalone host, if you enter an incorrect role in the `nsx_role` property, then the appliance is deployed in the `NSX Manager` role.

     - Windows example:

       ```
       C:\Program Files\VMware\VMware OVF Tool>ovftool \
       --sourceType=OVA \
       --name=nsx-manager \
       --X:injectOvfEnv \
       --X:logFile=<filepath>\nsxovftool.log \
       --allowExtraConfig \
       --datastore=<datastore name> \
       ```

```
--network=<network name> \
--acceptAllEulas \
--noSSLVerify \
--diskMode=thin \
--powerOn \
--prop:"nsx_role=NSX Manager" \
--prop:"nsx_ip_0=10.168.110.75" \
--prop:"nsx_netmask_0=255.255.255.0" \
--prop:"nsx_gateway_0=10.168.110.1" \
--prop:"nsx_dns1_0=10.168.110.10" \
--prop:"nsx_domain_0=corp.local" \
--prop:"nsx_ntp_0=10.168.110.10" \
--prop:"nsx_isSSHEnabled=<True|False>" \
--prop:"nsx_allowSSHRootLogin=<True|False>" \
--prop:"nsx_passwd_0=<password>" \
--prop:"nsx_cli_passwd_0=<password>" \
--prop:"nsx_cli_audit_passwd_0=<password>" \
--prop:"nsx_hostname=nsx-manager" \
<nsx-unified-appliance-release>.ova \
vi://root:<password>@10.168.110.51
```

Note The above Windows code block uses the backslash (\) to indicate the continuation of the command line. In actual use, omit the backslash and put the entire command in a single line.

Note In the above example, 10.168.110.51 is the IP address of the host machine where NSX Manager is to be deployed.

- Linux example:

```
mgrformfactor="small"
ipAllocationPolicy="fixedPolicy"
mgrdatastore="QNAP-Share-VMs"
mgrnetwork="Management-VLAN-210"

mgrname01="nsx-manager-01"
mgrhostname01="nsx-manager-01"
mgrip01="192.168.210.121"

mgrnetmask="255.255.255.0"
mgrgw="192.168.210.254"
mgrdns="192.168.110.10"
mgrntp="192.168.210.254"
mgrpasswd="<password>"
mgrssh="<True|False>"
mgrroot="<True|False>"
logLevel="trivia"

mgresxhost01="192.168.110.113"

ovftool --noSSLVerify --skipManifestCheck --powerOn \
--deploymentOption=$mgrformfactor \
--diskMode=thin \
--acceptAllEulas \
--allowExtraConfig \
--ipProtocol=IPv4 \
--ipAllocationPolicy=$ipAllocationPolicy \
--datastore=$mgrdatastore \
--network=$mgrnetwork \
--name=$mgrname01 \
--prop:nsx_hostname=$mgrhostname01 \
--prop:nsx_role="NSX Manager" \
--prop:nsx_ip_0=$mgrip01 \
--prop:nsx_netmask_0=$mgrnetmask \
--prop:nsx_gateway_0=$mgrgw \
--prop:nsx_dns1_0=$mgrdns \
--prop:nsx_ntp_0=$mgrntp \
--prop:nsx_passwd_0=$mgrpasswd \
--prop:nsx_cli_passwd_0=$mgrpasswd \
--prop:nsx_cli_audit_passwd_0=$mgrpasswd \
--prop:nsx_isSSHEnabled=$mgrssh \
--prop:nsx_allowSSHRootLogin=$mgrroot \
--X:logFile=nsxt-manager-ovf.log \
--X:logLevel=$logLevel \
/home/<user/nsxt-autodeploy/<nsx-unified-appliance-release>.ova \
vi://root:<password>@$mgresxhost01
```

The result should look something like this:

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://root:<password>@10.168.110.51
Deploying to VI: vi://root:<password>@10.168.110.51
Transfer Completed
Powering on VM: NSX Manager
Task Completed
Completed successfully
```

- For a host managed by vCenter Server:
  - Windows example:

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-manager \
--X:injectOvfEnv \
--X:logFile=ovftool.log \
 --allowExtraConfig \
--datastore=ds1 \
--network="management" \
--acceptAllEulas \
--noSSLVerify \
--diskMode=thin \
--powerOn \
--prop:"nsx_role=NSX Manager" \
--prop:"nsx_ip_0=10.168.110.75" \
--prop:"nsx_netmask_0=255.255.255.0" \
--prop:"nsx_gateway_0=10.168.110.1" \
--prop:"nsx_dns1_0=10.168.110.10" \
--prop:"nsx_domain_0=corp.local" \
--prop:"nsx_ntp_0=10.168.110.10" \
--prop:"nsx_isSSHEnabled=<True|False>" \
--prop:"nsx_allowSSHRootLogin=<True|False>" \
--prop:"nsx_passwd_0=<password>" \
--prop:"nsx_cli_passwd_0=<password>" \
--prop:"nsx_hostname=nsx-manager" \
<nsx-unified-appliance-release>.ova \
vi://administrator@vsphere.local:<password>@10.168.110.24/?ip=10.168.110.51
```

Note The above Windows code block uses the backslash (\) to indicate the continuation of the command line. In actual use, omit the backslash and put the entire command in a single line.

- Linux example:

```
mgrformfactor="small"
ipAllocationPolicy="fixedPolicy"
mgrdatastore="QNAP-Share-VMs"
mgrnetwork="Management-VLAN-210"

mgrname01="nsx-manager-01"
mgrhostname01="nsx-manager-01"
mgrip01="192.168.210.121"

mgrnetmask="255.255.255.0"
mgrgw="192.168.210.254"
mgrdns="192.168.110.10"
mgrntp="192.168.210.254"
mgrpasswd="<password>"
mgrssh="<True|False>"
mgrroot="<True|False>"
logLevel="trivia"

vcadmin="administrator@vsphere.local"
vcpass="<password>"
vcip="192.168.110.151"
mgresxhost01="192.168.110.113"

ovftool --noSSLVerify --skipManifestCheck --powerOn \
--deploymentOption=$mgrformfactor \
--diskMode=thin \
--acceptAllEulas \
--allowExtraConfig \
--ipProtocol=IPv4 \
--ipAllocationPolicy=$ipAllocationPolicy \
--datastore=$mgrdatastore \
--network=$mgrnetwork \
--name=$mgrname01 \
--prop:nsx_hostname=$mgrhostname01 \
--prop:nsx_role="NSX Manager" \
--prop:nsx_ip_0=$mgrip01 \
--prop:nsx_netmask_0=$mgrnetmask \
--prop:nsx_gateway_0=$mgrgw \
--prop:nsx_dns1_0=$mgrdns \
--prop:nsx_ntp_0=$mgrntp \
--prop:nsx_passwd_0=$mgrpasswd \
--prop:nsx_cli_passwd_0=$mgrpasswd \
--prop:nsx_cli_audit_passwd_0=$mgrpasswd \
--prop:nsx_isSSHEnabled=$mgrssh \
--prop:nsx_allowSSHRootLogin=$mgrroot \
--X:logFile=nsxt-manager-ovf.log \
--X:logLevel=$logLevel \
/home/<user/nsxt-autodeploy/<nsx-unified-appliance-release>.ova \
vi://$vcadmin:$vcpass@$vcip/?ip=$mgresxhost01
```

The result should look something like this:

```

Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://administrator@vsphere.local@10.168.110.24:443/
Deploying to VI: vi://administrator@vsphere.local@10.168.110.24:443/
Transfer Completed
Powering on VM: NSX Manager
Task Completed
Completed successfully
```

2 For an optimal performance, reserve memory for the NSX Manager appliance.

   Set the reservation to ensure that NSX Manager has sufficient memory to run efficiently. See NSX Manager VM and Host Transport Node System Requirements.

3 From the vSphere Client, open NSX Manager VM console to track the boot process.

4 After the NSX Manager boots, log in to the CLI as admin and run the `get interface eth0` command to verify that the IP address was applied as expected.

5 Verify that your NSX Manager has the required connectivity.

   Make sure that you can perform the following tasks.

   - Ping your NSX Manager from another machine.
   - The NSX Manager can ping its default gateway.
   - The NSX Manager can ping the hypervisor hosts that are in the same network as the NSX Manager using the management interface.
   - The NSX Manager can ping its DNS server and its NTP server.
   - If you enabled SSH, make sure that you can SSH to your NSX Manager.

   If connectivity is not established, make sure that the network adapter of the virtual appliance is in the proper network or VLAN.

What to do next

Log in to the NSX Manager from a supported web browser. See Log In to the Newly Created NSX Manager .

Configure NSX-T Data Center to Display the GRUB Menu at Boot Time

Configuring the NSX-T Data Center appliance to display the GRUB menu at boot time is required to reset the root password of the NSX-T Data Center appliance.

Important If the configuration is not performed after deploying the appliance and you forget the root, admin, or audit password, resetting it is not possible.

Procedure

1. Log in to the VM as root.
2. Change the value for the parameter `GRUB_HIDDEN_TIMEOUT` in the `/etc/default/grub` file.

   ```
   GRUB_HIDDEN_TIMEOUT=2
   ```
3. (Optional) Change the GRUB password in the `/etc/grub.d/40_custom` file.

   The default password is `VMware1`.
4. Update the GRUB configuration.

   ```
   update-grub
   ```

Log In to the Newly Created NSX Manager

After you install NSX Manager, you can use the user interface to perform other installation tasks.

After you install NSX Manager, you can join the Customer Experience Improvement Program (CEIP) for NSX-T Data Center. See Customer Experience Improvement Program in the *NSX-T Data Center Administration Guide* for more information about the program, including how to join or leave the program later.

Prerequisites

Verify that NSX Manager is installed. See Install NSX Manager and Available Appliances.

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.

   The EULA appears.
2. Read and accept the EULA terms.
3. Select whether to join the VMware's Customer Experience Improvement Program (CEIP).
4. Click **Save**

Add a Compute Manager

A compute manager, for example, vCenter Server, is an application that manages resources such as hosts and VMs.

NSX-T Data Center polls compute managers to collect cluster information from vCenter Server.

When you add a vCenter Server compute manager, you must provide a vCenter Server user's credentials. You can provide the vCenter Server administrator's credentials, or create a role and a user specifically for NSX-T Data Center and provide this user's credentials. This role must have the following vCenter Server privileges:

`Extension.Register extension`
`Extension.Unregister extension`
`Extension.Update extension`
`Sessions.Message`
`Sessions.Validate session`
`Sessions.View and stop sessions`
`Host.Configuration.Maintenance`
`Host.Configuration.NetworkConfiguration`
`Host.Local Operations.Create virtual machine`
`Host.Local Operations.Delete virtual machine`
`Host.Local Operations.Reconfigure virtual machine`
`Tasks`
`Scheduled task`
`Global.Cancel task`
`Permissions.Reassign role permissions`
`Resource.Assign vApp to resource pool`
`Resource.Assign virtual machine to resource pool`
`Virtual Machine.Configuration`
`Virtual Machine.Guest Operations`
`Virtual Machine.Provisioning`
`Virtual Machine.Inventory`
`Network.Assign network`
`vApp`

For more information about vCenter Server roles and privileges, see the *vSphere Security* document.

Prerequisites

- Verify that you use the supported vSphere version. See Supported vSphere version.
- IPv6 and IPv4 communication with vCenter Server.

- Verify that you use the recommended number of compute managers. See https://configmax.vmware.com/home.

  Note NSX-T Data Center does not support the same vCenter Server to be registered with more than one NSX Manager.

Procedure

1. From your browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Select **System > Fabric > Compute Managers > Add**.
3. Complete the compute manager details.

Option	Description
Name and Description	Type the name to identify the vCenter Server. You can optionally describe any special details such as, the number of clusters in the vCenter Server.
FQDN or IP Address	Type the FQDN or IP address of the vCenter Server.
Type	The default compute manager type is set to vCenter Server.
HTTPS Port of Reverse Proxy	The default port is 443. If you use another port, verify that the port is open on all the NSX Manager appliances. Set the reverse proxy port to register the compute manager in NSX-T.
Username and Password	Type the vCenter Server login credentials.
SHA-256 Thumbprint	Type the vCenter Server SHA-256 thumbprint algorithm value.
Enable Trust	Supported only on vCenter Server 7.0 and later versions. Enable this field to trust compute manager for authentication.

   If you left the thumbprint value blank, you are prompted to accept the server provided thumbprint.

   After you accept the thumbprint, it takes a few seconds for NSX-T Data Center to discover and register the vCenter Server resources.

   Note If the FQDN, IP, or thumbprint of the compute manager changes after registration, edit the computer manager and enter the new values.

4. If the progress icon changes from **In progress** to **Not registered**, perform the following steps to resolve the error.

   a. Select the error message and click **Resolve**. One possible error message is the following:

   ```
   Extension already registered at CM <vCenter Server name> with id <extension ID>
   ```

   b. Enter the vCenter Server credentials and click **Resolve**.

   If an existing registration exists, it will be replaced.

Results

It takes some time to register the compute manager with vCenter Server and for the connection status to appear as UP.

You can click the compute manager's name to view the details, edit the compute manager, or to manage tags that apply to the compute manager.

After the vCenter Server is successfully registered, do not power off and delete the NSX Manager VM without deleting the compute manager first. Otherwise, when you deploy a new NSX Manager, you will not be able to register the same vCenter Server again. You will get the error that the vCenter Server is already registered with another NSX Manager.

Note After a vCenter Server (VC) compute manager is successfully added, it cannot be removed if you successfully performed any of the following actions:

- Transport nodes are prepared using VDS that is dependent on the VC.
- Service VMs deployed on a host or a cluster in the VC using NSX service insertion.
- You use the NSX Manager UI to deploy Edge VMs, NSX Intelligence VM, or NSX Manager nodes on a host or a cluster in the VC.

If you try to perform any of these actions and you encounter an error (for example, installation failed), you can remove the VC if you have not successfully performed any of the actions listed above.

If you have successfully prepared any transport node using VDS that is dependent on the VC or deployed any VM, you can remove the VC after you have done the following:

- Unprepare all transport nodes. If uninstalling a transport node fails, you must force delete the transport node.
- Undeploy all service VMs, any NSX Intelligence VM, all NSX Edge VMs and all NSX Manager nodes. The undeployment must be successful or in a failed state.

This restriction applies to a fresh installation of NSX-T Data Center 3.0 as well as an upgrade.

Deploy NSX Manager Nodes to Form a Cluster from UI

You can deploy multiple NSX Manager nodes to provide high availability and reliability.

After the new nodes are deployed, these nodes connect to the NSX Manager node to form a cluster. Ensure that the number of clustered NSX Manager nodes is three.

Note Deploying multiple NSX Manager nodes using the UI is supported only on ESXi hosts managed by vCenter Server.

All the repository details and the password of the first deployed NSX Manager node are synchronized with the newly deployed nodes in the cluster.

Prerequisites

- Verify that an NSX Manager node is installed. See Install NSX Manager and Available Appliances.

- Verify that compute manager is configured. See Add a Compute Manager.
- Verify that the system requirements are met. See System Requirements.
- Verify that the required ports are open. See Ports and Protocols.
- Verify that a datastore is configured and accessible on the ESXi host.
- Verify that you have the IP address and gateway, DNS server IP addresses, domain search list, and the NTP server IP address for the NSX Manager to use.
- If you do not already have one, create the target VM port group network. Place the NSX-T Data Center appliances on a management VM network.

  If you have multiple management networks, you can add static routes to the other networks from the NSX-T Data Center appliance.

Procedure

1 From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.

2 Select **System > Appliances > Overview > Add NSX Appliance**.

3 Enter the NSX Manager node details.

Option	Description
Host Name or FQDN	Enter a name for the NSX Manager node.
Management IP/Netmask	Enter an IP address to be assigned to the NSX Manager node.
Management Gateway	Enter a gateway IP address to be used by the NSX Manager node.
DNS Servers	Enter DNS server IP addresses to be used by the NSX Manager node.
NTP Server	Enter an NTP server IP address to be used by the NSX Manager node.
Node Size	Select the form factor to deploy the NSX Manager node from the following options: ■ Small (4 vCPU, 16 GB RAM, 300 GB storage) ■ Medium (6 vCPU, 24 GB RAM, 300 GB storage) ■ High (12 vCPU, 48 GB RAM, 300 GB storage)

4 Enter the NSX Manager configuration details.

Option	Description
Compute Manager	Select the vCenter Server to provision compute resources for deploying the NSX Manager node.
Compute Cluster	Select the cluster the node is going to join.
Resource Pool	Select either a resource pool or a host for the node from the drop-down menu.
Host	If you did not select a resource pool, select the host to deploy the NSX Manager VIBs.
Datastore	Select a datastore for the node files from the drop-down menu.

Option	Description
Virtual Disk Format	- For NFS datastores, select a virtual disk format from the available provisioned policies on the underlying datastore. - With hardware acceleration, **Thin Provision**, **Thick Provision Lazy Zeroed**, and **Thick Provision Eager Zeroed** formats are supported. - Without hardware acceleration, only **Thin Provision** format is supported. - For VMFS datastores, **Thin Provision**, **Thick Provision Lazy Zeroed**, and **Thick Provision Eager Zeroed** formats are supported. - For vSAN datastores, you cannot choose a virtual disk format because the format is defined by the VM storage policy. - The actual disk format is determined by the vSAN storage policies. The default virtual disk format for vSAN is Thin Provision. You can change the vSAN storage policies to set a percentage of the virtual disk that must be thick provisioned. By default, the virtual disk for an NSX Manager node is prepared in the **Thin Provision** format. **Note** You can provision each NSX Manager node with a different disk format based on which policies are provisioned on the datastore.
Network	Assign the network from the drop-down menu.

5 Enter the NSX Manager common attribute details.

Option	Description
Enable SSH	Toggle the button to allow an SSH login to the new NSX Manager node.
Enable Root Access	Toggle the button to allow the root access to the new NSX Manager node.

Option	Description
CLI User name and Password Confirmation	Set the CLI password and password confirmation for the new node. Your password must comply with the password strength restrictions. - At least 12 characters - At least one lower-case letter - At least one upper-case letter - At least one digit - At least one special character - At least five different characters - Default password complexity rules are enforced by the following Linux PAM module arguments: - `retry=3`: The maximum number of times a new password can be entered, for this argument at the most 3 times, before returning with an error. - `minlen=12`: The minimum acceptable size for the new password. In addition to the number of characters in the new password, credit (of +1 in length) is given for each different kind of character (other, upper, lower and digit). - `difok=0`: The minimum number of bytes that must be different in the new password. Indicates similarity between the old and new password. With a value 0 assigned to `difok`, there is no requirement for any byte of the old and new password to be different. An exact match is allowed. - `lcredit=1`: The maximum credit for having lower case letters in the new password. If you have less than or 1 lower case letter, each letter will count +1 towards meeting the current `minlen` value. - `ucredit=1`: The maximum credit for having upper case letters in the new password. If you have less than or 1 upper case letter each letter will count +1 towards meeting the current `minlen` value. - `dcredit=1`: The maximum credit for having digits in the new password. If you have less than or 1 digit, each digit will count +1 towards meeting the current `minlen` value. - `ocredit=1`: The maximum credit for having other characters in the new password. If you have less than or 1 other characters, each character will count +1 towards meeting the current minlen value. - `enforce_for_root`: The password is set for the root user. **Note** For more details on Linux PAM module to check the password against dictionary words, refer to the man page. The CLI user name is already set to admin.

Option	Description
Root Password and Password Confirmation	Set the root password and password confirmation for the new node. Your password must comply with the password strength restrictions. ■ At least 12 characters ■ At least one lower-case letter ■ At least one upper-case letter ■ At least one digit ■ At least one special character ■ At least five different characters ■ Default password complexity rules are enforced by the following Linux PAM module arguments: ■ `retry=3`: The maximum number of times a new password can be entered, for this argument at the most 3 times, before returning with an error. ■ `minlen=12`: The minimum acceptable size for the new password. In addition to the number of characters in the new password, credit (of +1 in length) is given for each different kind of character (other, upper, lower and digit). ■ `difok=0`: The minimum number of bytes that must be different in the new password. Indicates similarity between the old and new password. With a value 0 assigned to `difok`, there is no requirement for any byte of the old and new password to be different. An exact match is allowed. ■ `lcredit=1`: The maximum credit for having lower case letters in the new password. If you have less than or 1 lower case letter, each letter will count +1 towards meeting the current `minlen` value. ■ `ucredit=1`: The maximum credit for having upper case letters in the new password. If you have less than or 1 upper case letter each letter will count +1 towards meeting the current `minlen` value. ■ `dcredit=1`: The maximum credit for having digits in the new password. If you have less than or 1 digit, each digit will count +1 towards meeting the current `minlen` value. ■ `ocredit=1`: The maximum credit for having other characters in the new password. If you have less than or 1 other characters, each character will count +1 towards meeting the current minlen value. ■ `enforce_for_root`: The password is set for the root user. **Note** For more details on Linux PAM module to check the password against dictionary words, refer to the man page.
DNS Servers	Enter the DNS server IP address available in the vCenter Server.
NTP Servers	Enter the NTP server IP address.

6 Click **Save**.

7 (Optional) Click **New Node** and configure another node.

Repeat preceding two steps.

8 Click **Finish**.

The new nodes are deployed. You can track the deployment process on the **System > Appliances > Overview** page or the vCenter Server.

9 Wait for 10-15 minutes for the deployment, cluster formation, and repository synchronization to complete.

   All the repository details and the password of the first deployed NSX Manager node are synchronized with the newly deployed nodes in the cluster.

   Note If the master node reboots when the deployment of a new node is in progress, the new node might fail to register with the cluster. It displays the `Failed to Register` message on the new node's thumbnail. To redeploy the node manually on the cluster, delete and redeploy the node.

10 After the NSX Manager boots, log in to the CLI as admin and run the `get interface eth0` command to verify that the IP address was applied as expected.

11 Enter the `get services` command to verify that all the services are running.

   If the services are not running, wait for all the services to start running.

   Note The following services are not running by default: liagent, migration-coordinator, and snmp. You can start them as follows:

   - `start service liagent`
   - `start service migration-coordinator`

     Note Start this service on only one NSX Manager node. See the *NSX-T Data Center Migration Coordinator Guide*.

   - For SNMPv1/SNMPv2:

     ```
     set snmp community <community-string>
     start service snmp
     ```

     The maximum character limit for **`community-string`** is 64.

   - For SNMPv3

     ```
     set snmp v3-users <user_name> auth-password <auth_password> priv-password <priv_password>
     ```

     The maximum character limit for **`user_name`** is 32. Ensure that your passwords meet PAM constraints. If you want to change the default engine id, use the following command:

     ```
     set snmp v3-engine-id <v3-engine-id>

     start service snmp
     ```

     `v3-engine-id` is a hexadecimal string that is 10 to 64 characters long.

     NSX-T Data Center supports SHA1 and AES128 as the authentication and privacy protocols. You can also use API calls to set up SNMPv3. For more information, see the *NSX-T Data Center API Guide*.

12 Log in to the first deployed NSX Manager node and enter the `get cluster status` command to verify that the nodes are successfully added to the cluster.

13 Verify that your NSX Manager has the required connectivity.

   Make sure that you can perform the following tasks.

   - Ping your NSX Manager from another machine.
   - The NSX Manager can ping its default gateway.
   - The NSX Manager can ping the hypervisor hosts that are in the same network as the NSX Manager using the management interface.
   - The NSX Manager can ping its DNS server and its NTP server.
   - If you enabled SSH, make sure that you can SSH to your NSX Manager.

   If connectivity is not established, make sure that the network adapter of the virtual appliance is in the proper network or VLAN.

What to do next

Configure NSX Edge. See Install an NSX Edge on ESXi Using the vSphere GUI.

Deploy NSX Manager Nodes to Form a Cluster Using CLI

Joining the NSX Manager to form a cluster using CLI ensures that all the NSX Manager nodes in cluster can communicate with each other.

Prerequisites

The installation of NSX-T Data Center components must be complete.

Procedure

1 Open an SSH session to the first deployed NSX Manager node.

2 Log in with the administrator credentials.

3 On the NSX Manager node, run the `get certificate api thumbprint` command.

   The command output is a string of numbers that is unique to this NSX Manager.

4 Run the `get cluster config` command to get the first deployed NSX Manager cluster ID.

5 Add a NSX Manager node to the cluster.

   Note You must run the join command on the newly deployed NSX Manager node.

   Provide the followingNSX Manager information:

   - The IP address of the node that you want to join
   - Cluster ID
   - User name

   - Password
   - Certificate thumbprint

   You can use the CLI command or API call.

   - CLI command

     ```
     host> join <NSX-Manager-IP> cluster-id <cluster-id> username <NSX-Manager-username> password
     <NSX-Manager-password> thumbprint <NSX-Manager-thumbprint>
     ```

   - API call `POST https://<nsx-mgr>/api/v1/cluster?action=join_cluster`

   The joining and cluster stabilizing process might 10-15 minutes.

6. Add the third NSX Manager node to the cluster.

   Repeat step 5.

7. Verify the cluster status by running the `get cluster status` command on your hosts.

8. (NSX Manager UI) Select **System > Appliances > Overview** and verify the cluster connectivity.

What to do next

Create a transport zone. See Create a Standalone Host or Bare Metal Server Transport Node.

Configure a Virtual IP (VIP) Address for a Cluster

To provide fault tolerance and high availability to NSX Manager nodes, assign a virtual IP address (VIP) to a member of the NSX-T cluster.

NSX Managers of a cluster become part of an HTTPS group to service API and UI requests. The leader node of the cluster assumes ownership of the set VIP of the cluster to service any API and UI request. Any API and UI request coming in from clients is directed to the leader node.

Note When assigning Virtual IP, all the NSX Manager VMs in the cluster must be configured in the same subnet.

If the leader node that owns VIP becomes unavailable, NSX-T elects a new leader. The new leader owns the VIP. It sends out a gratuitous ARP packet advertising the new VIP to MAC address mapping. After a new leader node is elected, new API and UI requests are sent to the new leader node.

Failover of VIP to a new leader node of the cluster might take a few minutes to become functional. If the VIP fails over to a new leader node because the previous leader node became unavailable, reauthenticate credentials so that API requests are directed to the new leader node.

Note VIP is not designed to serve as a load-balancer and you cannot use it if you enable the vIDM **External Load Balancer Integration** from **System > Users > Configuration**. Do not set up a VIP if you want to use the External Load Balancer from vIDM. See Configure VMware Identity Manager Integration in the *NSX-T Data Center Administration Guide* for more details.

Procedure

1 From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.

2 Go to **System** > **Appliances**.

3 In the Virtual IP field, click **Set Virtual IP**.

4 Enter the VIP for the cluster. Ensure that VIP is part of the same subnet as the other management nodes.

5 Click **Save**.

6 To verify the cluster status and the API leader of the HTTPS group, enter the NSX Manager CLI command `get cluster status verbose` in the NSX Manager console or over SSH.

The following is an example output with the leader marked in bold.

```
Group Type: HTTPS
Group Status: STABLE

Members:
    UUID                                       FQDN                  IP
STATUS
    cdb93642-ccba-fdf4-8819-90bf018cd727       nsx-manager       192.196.197.84
UP
    51a13642-929b-8dfc-3455-109e6cc2a7ae       nsx-manager       192.196.198.156
UP
    d0de3642-d03f-c909-9cca-312fd22e486b       nsx-manager       192.196.198.54
UP

Leaders:
    SERVICE                                    LEADER                                     LEASE
VERSION
    api                                        cdb93642-ccba-fdf4-8819-90bf018cd727       8
```

7 To troubleshoot VIP, verify Reverse Proxy logs at `/var/log/proxy/reverse-proxy.log` and cluster manager logs at `/var/log/cbm/cbm.log` in the NSX Manager CLI.

Results

Any API requests to NSX-T is redirected to the virtual IP address of the cluster, which is owned by the leader node. The leader node then routes the request forward to the other components of the appliance.

Disable Snapshots on NSX-T Data Center Appliances

As VMs, the NSX Manager, NSX Edges and other appliances, such as the Global Manager, may be configured for having their snapshots taken and stored. However, clones and snapshots of NSX-T appliances are not supported and may cause functionality and unknown other issues. For this reason, it is highly recommended that you disable snapshots of NSX-T appliance VMs.

Perform the following procedure on each NSX-T appliance VM.

Procedure

1. Locate the appliance VMs in the vSphere Client.
2. Power down the VM.
3. Right-click the VM and select **Edit Settings**.
4. Click the **VM Options** tab, then expand **Advanced**.
5. In the **Configuration Parameters** field, click **Edit Configuration...**.
6. In the **Configuration Parameters** window, click **Add Configuration Params**.
7. Enter the following:
   - For Name, enter `snapshot.MaxSnapshots`.
   - For Value, enter –`0`.
8. Click **OK** to save the changes.
9. Power the VM back on.

Installing NSX-T Data Center on KVM

6

NSX-T Data Center supports KVM in two ways: as a host transport node and as a host for NSX Manager.

Make sure that you have the supported KVM versions. See NSX Manager VM and Host Transport Node System Requirements.

This chapter includes the following topics:

- Set Up KVM
- Manage Your Guest VMs in the KVM CLI
- Install NSX Manager on KVM
- Install Third-Party Packages on a KVM Host
- Verify Open vSwitch Version on RHEL or CentOS KVM Hosts
- Verify Open vSwitch Version on SUSE KVM Hosts
- Verify Open vSwitch Version on Ubuntu KVM Hosts
- Deploy NSX Manager Nodes to Form a Cluster Using CLI

Set Up KVM

If you plan to use KVM as a transport node or as a host for NSX Manager guest VM, but you do not already have a KVM setup, you can use the procedure described here.

Note The Geneve encapsulation protocol uses UDP port 6081. You must allow this port access in the firewall on the KVM host.

Procedure

1 (Only RHEL) Open the `/etc/yum.conf` file.

2 Search for the line `exclude`.

3 Add the line "`kernel* redhat-release*`" to configure YUM to avoid any unsupported RHEL upgrades.

```
exclude=[existing list] kernel* redhat-release*
```

If you plan to run NSX-T Data Center Container Plug-in, which has specific compatibility requirements, exclude the container-related modules as well.

```
exclude=[existing list] kernel* redhat-release* kubelet-* kubeadm-* kubectl-* docker-*
```

The supported RHEL versions are 7.6, and 7.7.

4 Install KVM and bridge utilities.

Linux Distribution	Commands

Ubuntu	`apt-get install -y qemu-kvm libvirt-bin ubuntu-vm-builder bridge-utils`
	`virtinst virt-manager virt-viewer libguestfs-tools`

RHEL or CentOS Linux	`yum groupinstall "Virtualization Hypervisor"`
	`yum groupinstall "Virtualization Client"`
	`yum groupinstall "Virtualization Platform"`
	`yum groupinstall "Virtualization Tools"`

SUSE Linux Enterprise Server	Start YaSt and select **Virtualization > Install Hypervisor and Tools**. YaSt allows you to automatically enable and configure the network bridge.

5 For NSX manager to automatically install NSX software packages on KVM host, prepare the network configuration of the uplink/data interface.

The KVM host can have multiple network interfaces. For the network interface that you plan to provide as an uplink interface (data interface) for NSX-T purposes, it is important to have network configuration files correctly populated. NSX-T looks at these network configuration files to create NSX-T specific network devices. On Ubuntu, populate `/etc/network/interfaces` file. On RHEL, CentOS, or SUSE, populate the `/etc/sysconfig/network-scripts/ifcfg-$uplinkdevice` file.

In the following examples, interface "ens32" is the uplink device (data interface). Depending on your deployment environment, this interface can use DHCP or static IP settings.

Note Interface names might vary in different environments.

Important For Ubuntu, all network configurations must be specified in `/etc/network/interfaces`. Do not create individual network configuration files such as `/etc/network/ifcfg-eth1`, which can lead to failure of transport node creation.

Linux Distribution	Network Configuration

Ubuntu	Edit `/etc/network/interfaces`:
	`auto eth0`
	`iface eth0 inet manual`
	
	`auto ens32`
	`iface ens32 inet manual`

RHEL or CentOS Linux	Edit `/etc/sysconfig/network-scripts/ifcfg-ens32`:
	`DEVICE="ens32"`
	`  TYPE="Ethernet"`
	`  NAME="ens32"`
	`  UUID="<something>"`
	`  BOOTPROTO="none"`
	`  HWADDR="<something>"`
	`  ONBOOT="yes"`
	`  NM_CONTROLLED="no"`

SUSE Linux Enterprise Server	If a SLES host already exists, verify that data interfaces is already configured on the host.
	If you do not have a pre-configured SLES host, see the reference configuration for the management and data interface.
	Edit /etc/sysconfig/network/ifcfg-ens32:
	`DEVICE="ens32"`
	`NAME="ens32"`
	`UUID="<UUID>"`
	`BOOTPROTO="none"`
	`LLADDR="<HWADDR>"`
	`STARTMODE="yes"`

6 Restart networking service `systemctl restart network` or reboot the Linux server for the networking changes take effect.

7 After the KVM host is configured as a transport node, the bridge interface '`nsx-vtep0.0`' is automatically created by NSX-T.

In Ubuntu, the `/etc/network/interfaces` file has entries such as the following:

```
iface nsx-vtep0.0 inet static
pre-up ip addr flush dev nsx-vtep0.0
address <IP_pool_address>
netmask <subnet_mask>
mtu 1600
down ifconfig nsx-vtep0.0 down
up ifconfig nsx-vtep0.0 up
```

In RHEL, the host NSX agent (nsxa) creates a configuration file named `ifcfg-nsx-vtep0.0` that has entries such as the following:

```
DEVICE=nsx-vtep0.0
BOOTPROTO=static
NETMASK=<IP address>
IPADDR=<subnet mask>
MTU=1600
ONBOOT=yes
USERCTL=no
NM_CONTROLLED=no
```

In SUSE,

```
DEVICE=nsx-vtep0.0
BOOTPROTO=static
NETMASK=255.255.255.0
IPADDR=192.168.13.119
MACADDR=ae:9d:b7:ca:20:4a
MTU=1600
USERCTL=no
STARTMODE=auto
```

Manage Your Guest VMs in the KVM CLI

NSX Manager can be installed as KVM VMs. In addition, KVM can be used as the hypervisor for NSX-T Data Center transport nodes.

KVM guest VM management is beyond the scope of this guide. However, here are some simple KVM CLI commands to get you started.

To manage your guest VMs in the KVM CLI, use the `virsh` commands. Following are some common `virsh` commands. Refer to the KVM documentation for additional information.

```

# List running
virsh list

# List all
virsh list --all

# Control instances
virsh start <instance>
virsh shutdown <instance>
virsh destroy <instance>
virsh undefine <instance>
virsh suspend <instance>
virsh resume <instance>

# Access an instance's CLI
virsh console <instance>
```

In the Linux CLI, the `ifconfig` command shows the vnetX interface, which represents the interface created for the guest VM. If you add additional guest VMs, additional vnetX interfaces are added.

```
ifconfig
...

vnet0     Link encap:Ethernet  HWaddr fe:54:00:b0:a0:6d
          inet6 addr: fe80::fc54:ff:feb0:a06d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13183 errors:0 dropped:0 overruns:0 frame:0
          TX packets:181524 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:4984832 (4.9 MB)  TX bytes:29498709 (29.4 MB)
```

Install NSX Manager on KVM

Install NSX Manager on a KVM host running on a bare metal server. Do not install NSX Manager on a KVM host running as a virtual appliance on another host (nested environment).

The QCOW2 installation procedure uses guestfish, a Linux command-line tool to write virtual machine settings into the QCOW2 file.

Prerequisites

- KVM set up. See Set Up KVM.
- Privileges to deploy a QCOW2 image on the KVM host.
- Verify that the password in the guestinfo adheres to the password complexity requirements so that you can log in after installation. See Chapter 4 NSX Manager Installation.
- Familiarize yourself with the NSX Manager resource requirements. See NSX Manager VM and Host Transport Node System Requirements.
- If you plan to install Ubuntu OS, it is recommened to install Ubuntu version 18.04 before installing NSX Manager on the KVM host.

Important

- If you are deploying an NSX Manager on a KVM v18.04 for a production environment, ensure that the KVM host is not running as a virtual machine on an ESXi host. However, if you want to deploy an NSX Manager in a nested KVM environment for purposes of proof-of-concept, deploy the NSX Manager in the QEMU user space, by using `virt-type qemu`.
- Do not deploy NSX Manager on a single disk. If you install NSX Manager on a single disk, some startup services might fail to come up.

Procedure

1 Download NSX Manager QCOW2 images (for primary and secondary disk) from the **nsx-unified-appliance > exports > kvm** folder.

2 Make three copies of the images to the KVM machine that is going to run the NSX Manager using SCP or sync.

3 (Ubuntu only) Add the currently logged in user as a libvirtd user:

```
adduser $USER libvirtd
```

4 In the same directory where you saved the QCOW2 image, create three files (name: guestinfo.xml) for the primary disk image and populate it with the NSX Manager VM's properties. You do not need to create any files for the secondary disk image.

Property	Description
■ **nsx_cli_passwd_0** ■ **nsx_cli_audit_passwd_0** ■ **nsx_passwd_0**	Your passwords must comply with the password strength restrictions. ■ At least 12 characters ■ At least one lower-case letter ■ At least one upper-case letter ■ At least one digit ■ At least one special character ■ At least five different characters ■ Default password complexity rules are enforced by the following Linux PAM module arguments: ■ `retry=3`: The maximum number of times a new password can be entered, for this argument at the most 3 times, before returning with an error. ■ `minlen=12`: The minimum acceptable size for the new password. In addition to the number of characters in the new password, credit (of +1 in length) is given for each different kind of character (other, upper, lower and digit). ■ `difok=0`: The minimum number of bytes that must be different in the new password. Indicates similarity between the old and new password. With a value 0 assigned to `difok`, there is no requirement for any byte of the old and new password to be different. An exact match is allowed. ■ `lcredit=1`: The maximum credit for having lower case letters in the new password. If you have less than or 1 lower case letter, each letter will count +1 towards meeting the current `minlen` value. ■ `ucredit=1`: The maximum credit for having upper case letters in the new password. If you have less than or 1 upper case letter each letter will count +1 towards meeting the current `minlen` value. ■ `dcredit=1`: The maximum credit for having digits in the new password. If you have less than or 1 digit, each digit will count +1 towards meeting the current `minlen` value. ■ `ocredit=1`: The maximum credit for having other characters in the new password. If you have less than or 1 other characters, each character will count +1 towards meeting the current minlen value. ■ `enforce_for_root`: The password is set for the root user. **Note** For more details on Linux PAM module to check the password against dictionary words, refer to the man page.
nsx_hostname	Enter the host name for the NSX Manager. The host name must be a valid domain name. Ensure that each part of the host name (domain/subdomain) that is separated by dot must start with an alphabet character.
nsx_role	■ *nsx-manager*: Select this role to install the NSX Manager appliance. ■ *nsx-cloud-service-manager*: Select this role to install the Cloud Service Manager appliance for NSX Cloud. See Overview of Deploying NSX Cloud for details. ■ *nsx-global-manager*: Select this role to install the Global Manager appliance for Federation. See Chapter 13 Getting Started with Federation for details.

Property	Description
nsx_isSSHEnabled	You can enable or disable this property. If enabled, you can log in to the NSX Manager using SSH.
nsx_allowSSHRootLogin	You can enable or disable this property. If enabled, you can log in to the NSX Manager using SSH as the root user. To be able to use this property, `nsx_isSSHEnabled` must be enabled.
■ **nsx_dns1_0** ■ **nsx_ntp_0** ■ **nsx_domain_0** ■ **nsx_gateway_0** ■ **nsx_netmask_0** ■ **nsx_ip_0**	Enter IP addresses for the default gateway, management network IPv4, management network netmask, DNS, and NTP IP address.

For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<Environment
     xmlns="http://schemas.dmtf.org/ovf/environment/1"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xmlns:oe="http://schemas.dmtf.org/ovf/environment/1">
   <PropertySection>
    <Property oe:key="nsx_cli_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_cli_audit_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_hostname" oe:value="nsx-manager1"/>
    <Property oe:key="nsx_role" oe:value="nsx-manager"/>
    <Property oe:key="nsx_isSSHEnabled" oe:value="True"/>
    <Property oe:key="nsx_allowSSHRootLogin" oe:value="True"/>
    <Property oe:key="nsx_dns1_0" oe:value="10.168.110.10"/>
    <Property oe:key="nsx_ntp_0" oe:value="10.168.110.10"/>
    <Property oe:key="nsx_domain_0" oe:value="corp.local"/>
    <Property oe:key="nsx_gateway_0" oe:value="10.168.110.83"/>
    <Property oe:key="nsx_netmask_0" oe:value="255.255.252.0"/>
    <Property oe:key="nsx_ip_0" oe:value="10.168.110.19"/>
   </PropertySection>
</Environment>
```

Note In the example, `nsx_isSSHEnabled` and `nsx_allowSSHRootLogin` are both enabled. When they are disabled, you cannot SSH or log in to the NSX Manager command line. If you enable `nsx_isSSHEnabled` but not `nsx_allowSSHRootLogin`, you can SSH to NSX Manager but you cannot log in as root.

5. Use guestfish to write the `guestinfo.xml` file into the QCOW2 image.

   Note After the `guestinfo` information is written into a QCOW2 image, the information cannot be overwritten.

   ```
   sudo guestfish --rw -i -a nsx-unified-appliance-<BuildNumber>.qcow2 upload guestinfo /config/
   guestinfo
   ```

6. Deploy the QCOW2 image with the `virt-install` command.

   The vCPU and RAM values are suitable for a large VM. The network name and portgroup name are specific to your environment. The model must be `virtio`.

   (On RHEL hosts)

   ```
   sudo virt-install \
   --import \
   --ram 48000 \
   --vcpus 12 \
   --name <manager-name> \
   --disk path=<manager-qcow2-file-path>,bus=virtio,cache=none \
   --disk path=<secondary-qcow2-file-path>,bus=virtio,cache=none \
   --network [bridge=<bridge-name> or network=<network-name>],
     portgroup=<portgroup-name>,model=virtio \
   --noautoconsole              \
   --cpu mode=host-passthrough

   Starting install...
   Domain installation still in progress. Waiting for installation to complete.
   ```

   (On Ubuntu hosts)

   ```
   sudo virt-install \
   --import \
   --ram 48000 \
   --vcpus 12 \
   --name <manager-name> \
   --disk path=<manager-qcow2-file-path>,bus=virtio,cache=none \
   --disk path=<secondary-qcow2-file-path>,bus=virtio,cache=none \
   --network [bridge=<bridge-name> or network=<network-name>],
     portgroup=<portgroup-name>,model=virtio \
   --noautoconsole              \
   --cpu mode=host-passthrough,cache.mode=passthrough

   Starting install...
   Domain installation still in progress. Waiting for installation to complete.
   ```

7. Verify that the NSX Manager is deployed.

   ```
   virsh list --all

   Id    Name             State
   ---------------------------------
   18    nsx-manager1     running
   ```

8. Open the NSX Manager console and log in.

   ```
   virsh console 18
   Connected to domain nsx-manager1
   Escape character is ^]

   nsx-manager1 login: admin
   Password:
   ```

9. After the NSX Manager boots, log in to the CLI as admin and run the `get interface eth0` command to verify that the IP address was applied as expected.

10. Run `get services` to verify that the services are running.

11. Verify that your NSX Manager has the required connectivity.

    Make sure that you can perform the following tasks.

    - Ping your NSX Manager from another machine.
    - The NSX Manager can ping its default gateway.
    - The NSX Manager can ping the hypervisor hosts that are in the same network as the NSX Manager using the management interface.
    - The NSX Manager can ping its DNS server and its NTP server.
    - If you enabled SSH, make sure that you can SSH to your NSX Manager.

    If connectivity is not established, make sure that the network adapter of the virtual appliance is in the proper network or VLAN.

12. Exit the KVM console.

    `control-]`

13. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.

What to do next

Log in to the NSX Manager. See Log In to the Newly Created NSX Manager .

Install Third-Party Packages on a KVM Host

To prepare a KVM host to be a fabric node, you must install some third-party packages.

Prerequisites

- (RHEL and CentOS Linux) Before you install the third-party packages, run the following commands to install the virtualization packages.

  ```
  yum groupinstall “Virtualization Hypervisor”
  yum groupinstall “Virtualization Client”
  yum groupinstall "Virtualization Platform"
  yum groupinstall "Virtualization Tools"
  ```

  If you are not able to install the packages, you can manually install them by running `yum install glibc.i686 nspr` command on a new installation.

- (Ubuntu) Before you install the third-party packages, run the following commands to install the virtualization packages.

  ```
  apt install -y \
  qemu-kvm \
  libvirt-bin \
  virtinst \
  virt-manager \
  virt-viewer \
  ubuntu-vm-builder \
  bridge-utils
  ```

- (SUSE Linux Enterprise Server) Before you install the third-party packages, run the following commands to install the virtualization packages.

  ```
  libcap-progs
  ```

Procedure

- On Ubuntu 18.04.2 LTS, run `apt-get install <package_name>` to install the following third-party packages manually.

  ```
  traceroute
  python-mako
  python-simplejson
  python-unittest2
  python-yaml
  python-netaddr
  python-netifaces
  dkms
  libc6-dev
  libelf-dev
  ```

- On RHEL and CentOS Linux, run `yum install <package_name>` to install the third-party packages manually.

  If you manually prepare the host that is already registered to RHEL or CentOS, you do not need to install third-party packages on the host.

RHEL 7.7, 7.6	CentOS Linux 7.7, 7.6

`wget`
`PyYAML`
`libunwind`
`python-gevent`
`python-mako`
`python-netaddr`
`python-netifaces`
`redhat-lsb-core`
`tcpdump`
	`wget`
	`PyYAML`
	`libunwind`
	`python-gevent`
	`python-mako`
	`python-netaddr`
	`python-netifaces`
	`redhat-lsb-core`
	`tcpdump`

- On SUSE, run `zypper install <package_name>` to install the third-party packages manually.

SUSE Linux Enterprise Server 12.0

`python-simplejson`
`python-PyYAML`
`python-netaddr`
`python-netifaces`
`lsb-release`
`libcap-progs`

Verify Open vSwitch Version on RHEL or CentOS KVM Hosts

Skip this topic if there are no OVS packages on the RHEL or CentOS host. If OVS packages already exist on a RHEL or CentOS host, you must either remove the existing OVS packages and install the NSX-T supported OVS packages or upgrade the existing OVS packages to NSX-T supported ones.

The supported Open vSwitch version is 2.12.1.xxxxxx.

Procedure

1 Verify the current version of the Open vSwitch installed on the host.

```
ovs-vswitchd --version
```

Important If the existing Open vSwitch packages run the latest or an earlier version, you must replace the existing Open vSwitch packages with the supported version.

2 Verify if there are existing Open vSwitch packages on the host.

```
rpm -qa | grep openvswitch
```

3 Navigate to the Open vSwitch packages required by NSX-T Data Center.

a Log in to the host as an administrator.

b Download and copy the nsx-lcp file into the /tmp directory.

c Untar the package.

```
tar -zxvf nsx-lcp-<release>-rhel77_x86_64.tar.gz
```

d Navigate to the package directory.

```
cd nsx-lcp-rhel77_x86_64/
```

4 Verify the Open vSwitch packages in the `nsx-lcp` bundle.

```
ls | grep openvswitch
```

5 Delete the Open vSwitch packages.

```
rpm -e <package1> <package2> <package3>...
```

6 If the Open vSwitch packages are successfully deleted on the host, proceed to the NSX Manager UI to prepare the KVM host as a transport node. If the Open vSwitch packages cannot be deleted, then proceed to the next step.

7 If packages cannot be deleted, upgrade the existing Open vSwitch package version with the supported one.

```
rpm -Uv --replacepkgs --oldpackage *openvswitch*.rpm
```

Verify Open vSwitch Version on SUSE KVM Hosts

Skip this topic if there are no OVS packages on the SUSE host. If OVS packages exist on a SUSE host, you must either remove the existing OVS packages and install the NSX-T supported OVS packages or upgrade the existing OVS packages to NSX-T supported ones.

The supported Open vSwitch version is 2.12.1.xxxxxx.

Procedure

1 Verify the current version of the Open vSwitch installed on the host.

```
ovs-vswitchd --version
```

Important If the existing Open vSwitch packages run the latest or an earlier version, you must replace the existing Open vSwitch packages with the supported version.

2 Verify if there are existing Open vSwitch packages on the host.

```
rpm -qa | grep openvswitch
```

3 Navigate to the Open vSwitch packages required by NSX-T Data Center.

a Log in to the host as an administrator.

b Download and copy the nsx-lcp file into the /tmp directory.

   c Untar the package.

   ```
   nsx-lcp-3.0.0.0.0.14335404-linux64-sles12sp3.tar.gz
   ```

   d Navigate to the package directory.

   ```
   nsx-lcp-linux64-sles12sp3/
   ```

4 Verify the Open vSwitch packages in the `nsx-lcp` bundle.

   ```
   ls | grep openvswitch
   ```

5 Delete the Open vSwitch packages.

   ```
   rpm -e <package1> <package2> <package3>...
   ```

6 If the Open vSwitch packages are successfully deleted on the host, proceed to the NSX Manager UI to prepare the KVM host as a transport node. If the Open vSwitch packages cannot be deleted, then proceed to the next step.

7 If packages cannot be deleted, upgrade the existing Open vSwitch package version with the supported one.

   ```
   rpm -Uv --replacepkgs --oldpackage *openvswitch*.rpm
   ```

Verify Open vSwitch Version on Ubuntu KVM Hosts

Skip this topic if there are no OVS packages on the Ubuntu host. If OVS packages already exist on the Ubuntu host, you must either remove the existing OVS packages and install the NSX-T supported OVS packages or upgrade the existing OVS packages to NSX-T supported ones.

The supported Open vSwitch version is 2.12.1.xxxxxx.

Procedure

1 Verify the current version of the Open vSwitch installed on the host.

   ```
   ovs-vswitchd --version
   ```

   Important If the existing Open vSwitch packages run the latest or an earlier version, you must replace the existing Open vSwitch packages with the supported version.

2 Verify if there are existing Open vSwitch packages on the host.

   ```
   dpkg -l | grep openvswitch
   ```

3 Navigate to the Open vSwitch packages required by NSX-T Data Center.

   a Log in to the host as an administrator.

   b Download and copy the nsx-lcp file into the /tmp directory.

   c Untar the package.

   `tar -zxvf nsx-lcp-<release>-ubuntu-xenial_amd64.tar.gz` OR

   `tar -zxvf nsx-lcp-<version>-linux64-bionic_amd64.tar.gz`

   d Navigate to the package directory.

   `cd nsx-lcp-xenial_amd64` OR

   `cd nsx-lcp-bionic_amd64`

4. Verify the Open vSwitch packages in the `nsx-lcp` bundle.

   ```
   ls | grep openvswitch
   ```

5. Delete the Open vSwitch packages.

   ```
   dpkg --purge <package1> <package2> <package3>….
   ```

6. If the Open vSwitch packages are successfully deleted on the host, proceed to the NSX Manager UI to prepare the KVM host as a transport node. If the Open vSwitch packages cannot be deleted, then proceed to the next step.

7. If packages cannot be deleted, upgrade the existing Open vSwitch package version with the supported one.

   ```
   dpkg -iRB *openvswitch*.deb
   ```

Deploy NSX Manager Nodes to Form a Cluster Using CLI

Joining the NSX Manager to form a cluster using CLI ensures that all the NSX Manager nodes in cluster can communicate with each other.

Prerequisites

The installation of NSX-T Data Center components must be complete.

Procedure

1. Open an SSH session to the first deployed NSX Manager node.

2. Log in with the administrator credentials.

3. On the NSX Manager node, run the `get certificate api thumbprint` command.

   The command output is a string of numbers that is unique to this NSX Manager.

4. Run the `get cluster config` command to get the first deployed NSX Manager cluster ID.

5. Add a NSX Manager node to the cluster.

   Note You must run the join command on the newly deployed NSX Manager node.

   Provide the followingNSX Manager information:

   - The IP address of the node that you want to join

   - Cluster ID
   - User name
   - Password
   - Certificate thumbprint

   You can use the CLI command or API call.

   - CLI command

     ```
     host> join <NSX-Manager-IP> cluster-id <cluster-id> username <NSX-Manager-username> password
     <NSX-Manager-password> thumbprint <NSX-Manager-thumbprint>
     ```

   - API call `POST https://<nsx-mgr>/api/v1/cluster?action=join_cluster`

   The joining and cluster stabilizing process might 10-15 minutes.

6. Add the third NSX Manager node to the cluster.

   Repeat step 5.

7. Verify the cluster status by running the `get cluster status` command on your hosts.
8. (NSX Manager UI) Select **System > Appliances > Overview** and verify the cluster connectivity.

What to do next

Create a transport zone. See Create a Standalone Host or Bare Metal Server Transport Node.

Configuring Bare Metal Server to Use NSX-T Data Center

7

To use NSX-T Data Center on a bare metal (BM) server, you must install supported third-party packages.

Bare Metal Concepts:

- Application - represents the actual application running on the bare metal server, such as a web server or a data base server.
- Application Interface - represents the network interface card (NIC) which the application uses for sending and receiving traffic. One application interface per bare metal server is supported.
- Management Interface - represents the NIC which manages the bare metal server.
- VIF - the peer of the application interface which is attached to the logical switch. This is similar to a VM vNIC.

NSX-T Data Center supports the bare metal server in two ways: as a host transport node and as a host for NSX Manager.

Make sure that you have the supported bare metal server versions. See Bare Metal Server System Requirements.

Note If your NSX Edges are in VM form factor and you intend to use the NSX DHCP service (deployed on VLAN-based logical switch), you must set the forged transmits option to Accept on the bare metal hosts on which the NSX Edges are deployed. See Forged Transmits in the vSphere product documentation.

This chapter includes the following topics:

- Install Third-Party Packages on a Bare Metal Server
- Create Application Interface for Bare Metal Server Workloads
- Ansible Server Configuration for Bare Metal Server
- Secure Workloads on Windows Server 2016 Bare Metal Server

Install Third-Party Packages on a Bare Metal Server

To prepare a bare metal server to be a fabric node, you must install some third-party packages.

Prerequisites

- Verify that the user performing the installation has administrative permission to do the following actions, some of which may require `sudo` permissions:
  - Download and untar the bundle.
  - Run `dpkg` or `rpm` commands for installing/uninstalling NSX components.
  - Execute `nsxcli` command for executing join management plane commands.
- Verify that the virtualization packages are installed.
  - Redhat or CentOS - `yum install libvirt-libs`
  - Ubuntu - `apt-get install libvirt0`
  - SUSE - `zypper install libvirt-libs`

Procedure

◆ On Ubuntu, run `apt-get install <package_name>` to install the third-party packages.

Ubuntu 18.04.2	Ubuntu 16.04
traceroute python-mako python-netaddr python-simplejson python-unittest2 python-yaml python-openssl dkms libvirt0 libelf-dev python-netifaces	libunwind8 libgflags2v5 libgoogle-perftools4 traceroute python-mako python-simplejson python-unittest2 python-yaml python-netaddr python-openssl libboost-filesystem1.58.0 libboost-chrono1.58.0 libgoogle-glog0v5 dkms libboost-date-time1.58.0 python-protobuf python-gevent libsnappy1v5 libleveldb1v5 libboost-program-options1.58.0 libboost-thread1.58.0 libboost-iostreams1.58.0 libvirt0 libelf-dev python-netifaces

- On RHEL or CentOS, run `yum install` to install the third-party packages.

RHEL 7.7, 7.6, and 7.5	CentOS 7.7, 7.6, and 7.5

`tcpdump`
`boost-filesystem`
`PyYAML`
`boost-iostreams`
`boost-chrono`
`python-mako`
`python-netaddr`
`python-six`
`gperftools-libs`
`libunwind`
`libelf-dev`
`snappy`
`boost-date-time`
`c-ares`
`redhat-lsb-core`
`wget`
`net-tools`
`yum-utils`
`lsof`
`python-gevent`
`libev`
`python-greenlet`
`libvirt-libs`
`python-netifaces`
	`tcpdump`
	`boost-filesystem`
	`PyYAML`
	`boost-iostreams`
	`boost-chrono`
	`python-mako`
	`python-netaddr`
	`python-six`
	`gperftools-libs`
	`libunwind`
	`libelf-dev`
	`snappy`
	`boost-date-time`
	`c-ares`
	`redhat-lsb-core`
	`wget`
	`net-tools`
	`yum-utils`
	`lsof`
	`python-gevent`
	`libev`
	`python-greenlet`
	`libvirt-libs`
	`python-netifaces`

- On SUSE, run `zypper install <package_name>` to install the third-party packages manually.

```
net-tools
tcpdump
python-simplejson
python-netaddr
python-PyYAML
python-six
libunwind
wget
lsof
libcap-progs
libvirt-libs
python-netifaces
```

Create Application Interface for Bare Metal Server Workloads

You must configure NSX-T Data Center install Linux third-party packages before you create or migrate an application interface for bare metal server workloads.

NSX-T Data Center does not support Linux OS interface bonding. You must use Open vSwitch (OVS) bonding for Bare Metal Server Transport Nodes. See Knowledge Base article 67835 Bare Metal Server supports OVS bonding for Transport Node configuration in NSX-T.

Procedure

1. Install the required third-party packages.

   See Install Third-Party Packages on a Bare Metal Server.

2. Configure the TCP and UDP ports.

   See https://ports.vmware.com/home/NSX-T-Data-Center.

3. Add a bare metal server to the NSX-T Data Center fabric and create a transport node.

   See Create a Standalone Host or Bare Metal Server Transport Node.

4. Use the Ansible playbook to create an application interface.

   See https://github.com/vmware/bare-metal-server-integration-with-nsxt.

Ansible Server Configuration for Bare Metal Server

When virtual interfaces (VIFs) are being configured, unique IDs of the VIFs have to be configured to be used as the segment port.

Ansible support modes are a set of automated scripts that set up the application interface for bare metal servers.

- Static Mode - Application interface IP Address is configured manually.
- DHCP Mode - Application interface IP Address is configured dynamically.
- Migrate Mode - This mode supports management and application sharing the same IP address. Also called underlay mode or VLAN-0.

For all Linux or Windows VM and physical machines:

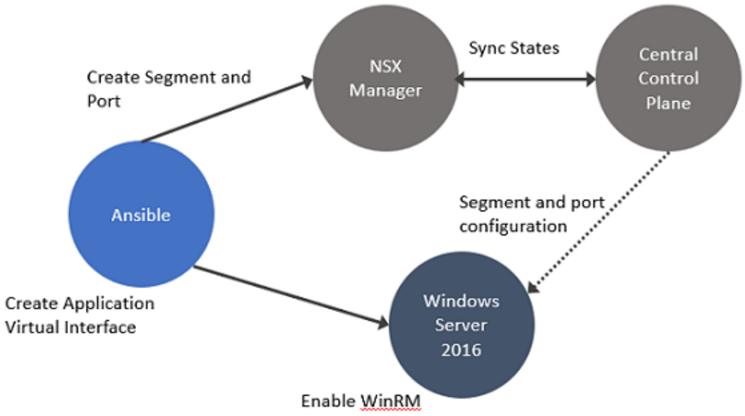
1. Install Ansible based on the operating system: –https://docs.ansible.com/ansible/latest/installation_guide/intro_installation.html
2. Run the command `ansible-version`, and check that Ansible is version is 2.4.3 or later.
3. Download and extract the Bare Metal integration with NSX-T Data Centerfrom Github: –https://github.com/vmware/bare-metal-server-integration-with-nsxt

For Windows Bare Metal Servers only:

1. Install pip for pywinrm.
2. Install pywinrm, and run `pip install pywinrm`.

Secure Workloads on Windows Server 2016 Bare Metal Server

Use Ansible to configure an application VIF on Windows Server 2016 and integrate it with NSX-T. The NSX-T agent installed on the servers provides connectivity and security to the bare metal workloads.



In this procedure, establish connectivity between the workloads and NSX Manager. Then, configure DFW rules to secure ingress and egress traffic running between virtual or physical and Windows Server 2016 bare metal workloads.

Procedure

1 Enable Windows Remote Management (WinRM) on Windows Server 2016 to allow the Windows server to interoperate with third-party software and hardware. To enable the WinRM service with a self-signed certificate.

   a Run `PS$ wget -o ConfigureWinRMService.ps1` https://github.com/vmware/bare-metal-server-integration-with-nsxt/blob/master/bms-ansible-nsx/windows/ConfigureWinRMService.ps1.

   b Run `PS$ powershell.exe -ExecutionPolicy ByPass -File ConfigureWinRMService.ps1`.

2 Configure WinRM to use HTTPS. The default port used for HTTPS is 5986.

   a Run Powershell as an administrator.

   b Run `winrm quickconfig`.

   c Run `winrm set winrm/config/service/auth @{Basic="true"}`.

   d Run `winrm set winrm/config/service @{AllowUnencrypted="true"}`.

   e Run `winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="win16-colib-001";CertificateThumbprint="cd 65 61 d8 b2 25 a7 ca 99 f8 1f a5 0c 55 8b f1 38 0d 06 26"}`.

   f Verify configuration of WinRM. Run `winrm e winrm/config/listener`.

3 Using Ansible, create an application interface for the Windows server.

   See https://github.com/vmware/bare-metal-server-integration-with-nsxt.

4 Using Ansible, create a segment and segment ports on NSX Manager over the WinRM channel.

   The application virtual interface, NSX Manager, and Windows Remote Management are synchronized with the segment and ports created for the application virtual interface.

5 In Windows, customize OVSIM driver for the Windows server to create two new network adapters - application virtual interfaces and virtual tunnel endpoint (VTEP) for overlay-backed workload.

```
$:> Get-NetAdapter
```

`vEthernet1-VTEP`: Used for overlay-backed VTEP interface. Not needed for a VLAN-backed workload.

`vEthernet1-VIF1`: Used for virtual interface or application interface of the bare metal Windows server.

6 To verify network adapters, go to the Windows server and run `Get-NetAdapter`.

7 Add the bare metal server as a standalone transport node. In the NSX Manager, go to **System** → **Fabric** → **Nodes** → **Host Transport Nodes**.

8 In the **Managed by** drop-down menu, select **Standalone Hosts** and click **+ Add**.

9 During transport node creation, ensure the following conditions are met:

- In the **Uplink** field, map an uplink to an available IP address on the Windows server. Run `Get-NetAdapter` on the Windows Server to know which ethernet address to configure as uplinks for the bare metal transport node.
- On an overlay-backed workload, select among IP Pool, Static IP, or DHCP as the mode for assigning a VTEP address to the host.
- On a VLAN-backed workload, there is not IP assignment required for the host.

The NSX Manager automatically installs required NSX-T VIBs and NSX-T agent on the bare metal server. For more details, see Create a Standalone Host or Bare Metal Server Transport Node.

10 Alternatively, you can manually prepare the bare metal server as a transport node or follow the interactive mode to prepare the server as a transport node.

a Download and install the NSX-T LCP Windows bundle using the `wget` command.

b To silently install NSX-T, run `\\install_helper.ps1 -operation install -setupFile VMware-NSX-<version>_baremetal-server_setup.exe -installPath <path>`.

c To interactively install NSX-T, double click the `setup.exe` file and follow the wizard to complete installation.

d Run the `nsxcli` command to join the Windows Server to the NSX Manager.

e Configure the host as a transport node either from the NSX Manager UI or REST APIs. For more details, see Create a Standalone Host or Bare Metal Server Transport Node.

11 Verify whether OVS bridges are created on the Windows server. The OVS bridge connects the application virtual interface to the nsx switch on the transport node.

```
ovs-vsctl show
```

The output must show the bridges created from `nsxswitch` and `nsx managed` host component. The `nsxswitch` bridge is for the transport node that was created. The `nsx managed` bridge is created for the application virtual interface on the Windows host. These bridge entries indicate that communication channel is established between the nsx switch and Windows remote listener.

12 Using the Ansible client, configure a static IP address for the overlay or VLAN-backed segment.

    Run `vi win_hosts`

13 Launch Ansible playbook for the service to configure Windows bare metal server.

    Run `ansible-playbook -i win_hosts win_static_config.yml`

14 On the overlay-backed transport node, verify:

    - The static IP address is reflected as the IP address of the overlay segment to which the Windows Server workload is connected.
    - The GENEVE tunnels are created between the nsx switch and the nsx managed host component on the Windows host.

    Note Likewise, on a VLAN-backed transport node, verify that the static IP address is reflected as the IP address of the VLAN segment to which the Windows Server workload is connected.

15 Verify connectivity between the application, Windows bare metal server, and NSX Manager .

16 Add and publish L2 or L3 DFW rules for the overlay or VLAN-backed bare metal workload.

17 Verify ingress and egress traffic between virtual or physical workloads and bare metal workloads is flowing as per the DFW rules published.

NSX Manager Cluster Requirements

8

The following subsections describe the NSX Manager cluster requirements and provides recommendations for specific site deployments. They also describe how you can use vSphere HA (High Availability) with NSX-T Data Center to enable quick recovery if the host running the NSX Manager node fails.

This chapter includes the following topics:

- NSX Manager Cluster Requirements for Single, Dual, and Multiple Sites

NSX Manager Cluster Requirements for Single, Dual, and Multiple Sites

Your NSX Manager cluster configuration will vary depending on whether your deployment is for single, dual, or multiple sites.

You can use vSphere HA with NSX-T Data Center to enable quick recovery if the host running the NSX Manager node fails.

Note See *Creating and Using vSphere HA Clusters* in the vSphere product documentation.

Cluster Requirements

- In a production environment, the NSX Manager cluster must have three members to avoid an outage to the management and control planes.

  Each cluster member should be placed on a unique hypervisor host with three physical hypervisor hosts in total. This is required to avoid a single physical hypervisor host failure impacting the NSX control plane. It is recommended you apply anti-affinity rules to ensure that all three cluster members are running on different hosts.

  The normal production operating state is a three-node NSX Manager cluster. However, you can add additional, temporary NSX Manager nodes to allow for IP address changes.

  Important As of NSX-T Data Center 2.4, the NSX Manager contains the NSX Central Control Plane process. This service is critical for the operation of NSX. If there is a complete loss of NSX Managers, or if the cluster is reduced from three NSX Managers to one NSX Manager, you will not be able to make topology changes to your environment, and vMotion of machines depending on NSX will fail.

- For lab and proof-of-concept deployments where there are no production workloads, you can run a single NSX Manager to save resources. NSX Manager nodes can be deployed on either ESXi or KVM. However, mixed deployments of managers on both ESXi and KVM are not supported.

Single Site Requirements and Recommendations

The following recommendations apply to single site NSX-T Data Center deployments.

- It is recommended that you place your NSX Managers on different hosts to avoid a single host failure impacting multiple managers.
- Maximum latency between NSX Managers is 10ms.
- You can place NSX Managers in different vSphere clusters or in a common vSphere cluster.
- It is recommended that you place NSX Managers in different management subnets or a shared management subnet. When using vSphere HA it is recommended to use a shared management subnet soNSX Managers that are recovered by vSphere can preserve their IP address.
- It is recommended that you place NSX Managers on shared storage also. For vSphere HA, please review the requirements for that solution.

You can also use vSphere HA with NSX-T to provide recovery of a lost NSX Manager when the host where the NSX Manager is running fails.

Scenario example:

- A vSphere cluster in which all three NSX Managers are deployed.
- The vSphere cluster consists of four or more hosts:
  - Host-01 with nsxmgr-01 deployed
  - Host-02 with nsxmgr-02 deployed
  - Host-03 with nsxmgr-03 deployed
  - Host-04 with no NSX Manager deployed
- vSphere HA is configured to recover any lost NSX Manager (e.g., nsxmgr-01) from any host (e.g., Host-01) to Host-04.

Thus, upon the loss of any hosts where a NSX Manager is running, vSphere recovers the lost NSX Manager on Host-04.

Dual Site Requirements and Recommendations

The following recommendations apply to dual site (Site A/Site B) NSX-T Data Center deployments.

- It is not recommended to deploy NSX Managers in a dual-site scenario without vSphere HA. In this scenario, one site requires the deployment of twoNSX Managers and the loss of that site will impact the operation of NSX-T Data Center.

- Deployment of NSX Managers in a dual site scenario with vSphere HA can be done with the following considerations:
  - A single stretched vSphere cluster contains all the hosts for NSX Managers.
  - All three NSX Managers are deployed to a common management subnet/VLAN to allow IP address preservation upon recovery of a lost NSX Managers.
  - For latency between sites, see the storage product requirements.

Scenario example:

- A vSphere cluster in which all three NSX Managers are deployed.
- The vSphere cluster consists of six or more hosts, with three hosts in Site A and three hosts in Site B.
- The three NSX Managers are deployed to distinct hosts with additional hosts for placement of recovered NSX Managers:

  Site A:

  - Host-01 with nsxmgr-01 deployed
  - Host-02 with nsxmgr-02 deployed
  - Host-03 with nsxmgr-03 deployed

  Site B:

  - Host-04 with no NSX Manager deployed
  - Host-05 with no NSX Manager deployed
  - Host-06 with no NSX Manager deployed
- vSphere HA is configured to recover any lost NSX Manager (e.g., nsxmgr-01) from any host (e.g., Host-01) in Site A to one of the hosts in Site B.

Thus, upon failure of Site A, vSphere HA will recover all NSX Managers to hosts in site B.

Important You must you properly configure anti-affinity rules to prevent NSX Managers from being recovered to the same common host.

Multiple (Three or More) Site Requirements and Recommendations

The following recommendations apply to multiple-site (Site A/Site B/Site C) NSX-T Data Center deployments.

In a scenario with three or more sites, you can deploy NSX Managers with or without vSphere HA.

If you deploy without vSphere HA:

- It is recommended that you use separate management subnets or VLANs per site.
- Maximum latency between NSX Managers is 10ms.

Scenario example (three sites):

- Three separate vSphere clusters, one per site.
- At least one host per site running NSX Manager:
  - Host-01 with nsxmgr-01 deployed
  - Host-02 with nsxmgr-02 deployed
  - Host-03 with nsxmgr-03 deployed

Failure scenarios:

- Single site failure: Two remaining NSX Managers in other sites continue to operate. NSX-T Data Center is in a degraded state but still operational. It is recommended you manually deploy a third NSX Manager to replace the lost cluster member.
- Two site failure: Loss of quorum and therefore impact to NSX-T Data Center operations.

Recovery of NSX Managers may take as long as 20 minutes depending on environmental conditions such as CPU speed, disk performance, and other deployment factors.

Installing NSX Edge

9

Install NSX Edge on ESXi using the NSX-T UI, the vSphere web client, or the command-line OVF tool.

This chapter includes the following topics:

- NSX Edge Installation Requirements
- NSX Edge Networking Setup
- NSX Edge Installation Methods
- Create an NSX Edge Transport Node
- Create an NSX Edge Cluster
- Install an NSX Edge on ESXi Using the vSphere GUI
- Install NSX Edge on Bare Metal
- Join NSX Edge with the Management Plane
- Configure an NSX Edge as a Transport Node

NSX Edge Installation Requirements

The NSX Edge provides routing services and connectivity to network NSX Edges that are external to the NSX-T Data Center deployment. An NSX Edge is required if you want to deploy a tier-0 router or a tier-1 router with stateful services such as network address translation (NAT), VPN, and so on.

Note There can be only one tier-0 router per NSX Edge node. However, multiple tier-1 logical routers can be hosted on one NSX Edge node. NSX Edge VMs of different sizes can be combined in the same cluster; however, it is not recommended.

Table 9-1. NSX Edge Deployment, Platforms, and Installation Requirements

Requirements	Description
Supported deployment methods	■ OVA/OVF ■ ISO with PXE ■ ISO without PXE
Supported platforms	NSX Edge is supported only on ESXi or on bare metal. NSX Edge is not supported on KVM.

Table 9-1. NSX Edge Deployment, Platforms, and Installation Requirements (continued)

Requirements	Description
PXE installation	The Password string must be encrypted with sha-512 algorithm for the root and admin user password.
NSX-T Data Center appliance password	■ At least 12 characters ■ At least one lower-case letter ■ At least one upper-case letter ■ At least one digit ■ At least one special character ■ At least five different characters ■ No dictionary words ■ No palindromes ■ More than four monotonic character sequence is not allowed
Hostname	When installing NSX Edge, specify a hostname that does not contain invalid characters such as an underscore. If the hostname contains any invalid character, after deployment the hostname will be set to `localhost`. For more information about hostname restrictions, see https://tools.ietf.org/html/rfc952 and https://tools.ietf.org/html/rfc1123.
VMware Tools	The NSX Edge VM running on ESXi has VMTools installed. Do not remove or upgrade VMTools.
System	Verify that the system requirements are met. See NSX Edge VM System Requirements.
Ports	Verify that the required ports are open. See Ports and Protocols.
IP Addresses	If you have multiple management networks, you can add static routes to the other networks from the NSX-T Data Center appliance. Plan your NSX Edge IPv4 or IPv6 IP addressing scheme.
OVF Template	■ Verify that you have adequate privileges to deploy an OVF template on the ESXi host. ■ Verify that hostnames do not include underscores. Otherwise, the hostname is set to *localhost*. ■ A management tool that can deploy OVF templates, such as vCenter Server or the vSphere Client. The OVF deployment tool must support configuration options to allow for a manual configuration. ■ The Client Integration Plug-in must be installed.
NTP Server	The same NTP server must be configured on all NSX Edge VMs or Bare Metal Edges in an Edge cluster.

Intel-based Chipsets

NSX Edge nodes are supported on ESXi-based hosts with Intel chipsets. If an unsupported chipset type is used, vSphere EVC mode may prevent Edge nodes from starting, showing an error message in the console. See NSX Edge VM System Requirements.

AMD EPYC

NSX Edge nodes are also supported on AMD-based chipsets. NSX Edge nodes can now be deployed on AMD EPYC series chipsets. See NSX Edge VM System Requirements.

- AMD EPYC 7xx1 Series (Naples)
- AMD EPYC 3000 Embedded Family and newer
- AMD EPYC 7xx2 Series (Rome)

NSX Edge Support of vSphere Business Continuity Features

Starting in NSX-T Data Center 2.5.1, vMotion, DRS, and vSphere HA are supported for NSX Edge nodes.

NSX Edge VM Support on a Host Configured in Enhanced Mode

In a collapsed cluster topology, where the NSX Edge VM, management VM, and host transport nodes are deployed on a single host, if you want to install an NSX Edge VM on a transport node configured in Enhanced mode, ensure that the host version is ESXi 6.7p02.

NSX Edge Installation Scenarios

Important When you install NSX Edge from an OVA or OVF file, either from vSphere Web Client or the command line, OVA/OVF property values such as user names, passwords, or IP addresses are not validated before the VM is powered on.

- If you specify a user name for the `admin` or `audit` user, the name must be unique. If you specify the same name, it is ignored and the default names (`admin` and `audit`) is used.
- If the password for the `admin` user does not meet the complexity requirements, you must log in to NSX Edge through SSH or at the console as the `admin` user with the password `default`. You are prompted to change the password.
- If the password for the `audit` user does not meet the complexity requirements, the user account is disabled. To enable the account, log in to NSX Edge through SSH or at the console as the `admin` user and run the command `set user audit` to set the `audit` user's password (the current password is an empty string).

- If the password for the `root` user does not meet the complexity requirements, you must log in to NSX Edge through SSH or at the console as `root` with the password `vmware`. You are prompted to change the password.

Caution Changes made to the NSX-T Data Center while logged in with the `root` user credentials might cause system failure and potentially impact your network. You can only make changes using the `root` user credentials with the guidance of VMware Support team.

Note The core services on the appliance do not start until a password with sufficient complexity has been set.

After you deploy NSX Edge from an OVA file, you cannot change the VM's IP settings by powering off the VM and modifying the OVA settings from vCenter Server.

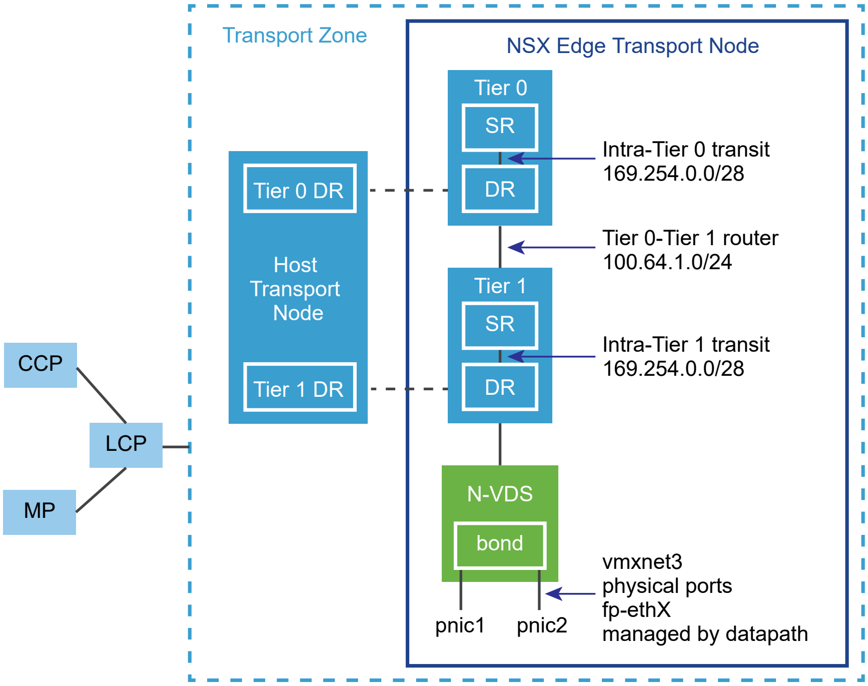
NSX Edge Networking Setup

NSX Edge can be installed using ISO, OVA/OVF, or PXE start. Regardless of the installation method, make sure that the host networking is prepared before you install NSX Edge.

High-Level View of NSX Edge Within a Transport Zone

The high-level view of NSX-T Data Center shows two transport nodes in a transport zone. One transport node is a host. The other is an NSX Edge.

Figure 9-1. High-Level Overview of NSX Edge



When you first deploy an NSX Edge, you can think of it as an empty container. The NSX Edge does not do anything until you create logical routers. The NSX Edge provides the compute backing for tier-0 and tier-1 logical routers. Each logical router contains a services router (SR) and a distributed router (DR). When we say that a router is distributed, we mean that it is replicated on all transport nodes that belong to the same transport zone. In the figure, the host transport node contains the same DRs contained on the tier-0 and tier-1 routers. A services router is required if the logical router is going to be configured to perform services, such as NAT. All tier-0 logical routers have a services router. A tier-1 router can have a services router if needed based on your design considerations.

By default, the links between the SR and the DR use the 169.254.0.0/28 subnet. These intra-router transit links are created automatically when you deploy a tier-0 or tier-1 logical router. You do not need to configure or modify the link configuration unless the 169.254.0.0/28 subnet is already in use in your deployment. On a tier-1 logical router, the SR is present only if you select an NSX Edge cluster when creating the tier-1 logical router.

The default address space assigned for the tier-0-to-tier-1 connections is 100.64.0.0/10. Each tier-0-to-tier-1 peer connection is provided a /31 subnet within the 100.64.0.0/10 address space. This link is created automatically when you create a tier-1 router and connect it to a tier-0 router. You do not need to configure or modify the interfaces on this link unless the 100.64.0.0/10 subnet is already in use in your deployment.

Each NSX-T Data Center deployment has a management plane cluster (MP) and a control plane cluster (CCP). The MP and the CCP push configurations to each transport zone's local control plane (LCP). When a host or NSX Edge joins the management plane, the management plane agent (MPA) establishes connectivity with the host or NSX Edge, and the host or NSX Edge becomes an NSX-T Data Center fabric node. When the fabric node is then added as a transport node, LCP connectivity is established with the host or NSX Edge.

Lastly, the figure shows an example of two physical NICs (pNIC1 and pNIC2) that are bonded to provide high availability. The datapath manages the physical NICs. They can serve as either VLAN uplinks to an external network or as tunnel endpoint links to internal NSX-T Data Center-managed VM networks.

It is a best practice to allocate at least two physical links to each NSX Edge that is deployed as a VM. Optionally, you can overlap the port groups on the same pNIC using different VLAN IDs. The first network link found is used for management. For example, on an NSX Edge VM, the first link found might be vnic1. On a bare-metal installation, the first link found might be eth0 or em0. The remaining links are used for the uplinks and tunnels. For example, one might be for a tunnel endpoint used by NSX-T Data Center-managed VMs. The other might be used for an NSX Edge-to-external TOR uplink.

You can view the physical link information of the NSX Edge, by logging in to the CLI as an administrator and running the `get interfaces` and `get physical-ports` commands. In the API, you can use the `GET fabric/nodes/<edge-node-id>/network/interfaces` API call. Physical links are discussed in more detail in the next section.

Whether you install NSX Edge as a VM appliance or on bare metal, you have multiple options for the network configuration, depending on your deployment.

Transport Zones and N-VDS

To understand NSX Edge networking, you must know something about transport zones and N-VDS. Transport zones control the reach of Layer 2 networks in NSX-T Data Center. N-VDS is a software switch that gets created on a transport node. The purpose of N-VDS is to bind logical router uplinks and downlinks to physical NICs. For each transport zone that an NSX Edge belongs to, a single N-VDS gets installed on the NSX Edge.

There are two types of transport zones:

- Overlay for internal NSX-T Data Center tunneling between transport nodes.
- VLAN for uplinks external to NSX-T Data Center.

An NSX Edge can belong to zero VLAN transport zones or many. For zero VLAN transport zones, the NSX Edge can still have uplinks because the NSX Edge uplinks can use the same N-VDS installed for the overlay transport zone. You might do this if you want each NSX Edge to have only one N-VDS. Another design option is for the NSX Edge to belong to multiple VLAN transport zones, one for each uplink.

The most common design choice is three transport zones: One overlay and two VLAN transport zones for redundant uplinks.

To use the same VLAN ID for a transport network for overlay traffic and other for VLAN traffic, such as a VLAN uplink, configure the ID on two different N-VDS, one for VLAN and the other for overlay.

Virtual-Appliance/VM NSX Edge Networking

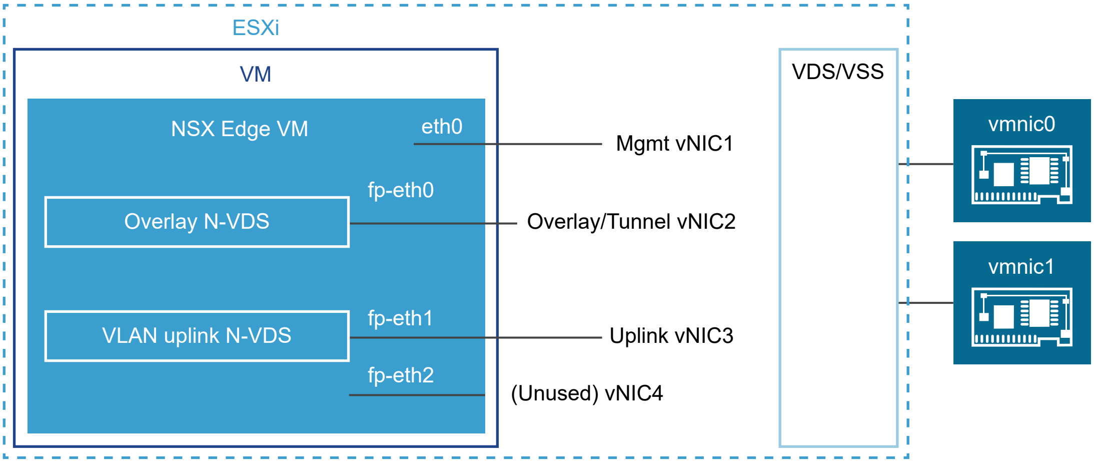
When you install NSX Edge as a virtual appliance or VM, internal interfaces are created, called fp-ethX, where X is 0, 1, 2, and 3. These interfaces are allocated for uplinks to a top-of-rack (ToR) switches and for NSX-T Data Center overlay tunneling.

When you create the NSX Edge transport node, you can select fp-ethX interfaces to associate with the uplinks and the overlay tunnel. You can decide how to use the fp-ethX interfaces.

On the vSphere distributed switch or vSphere Standard switch, you must allocate at least two vmnics to the NSX Edge: One for NSX Edge management and one for uplinks and tunnels.

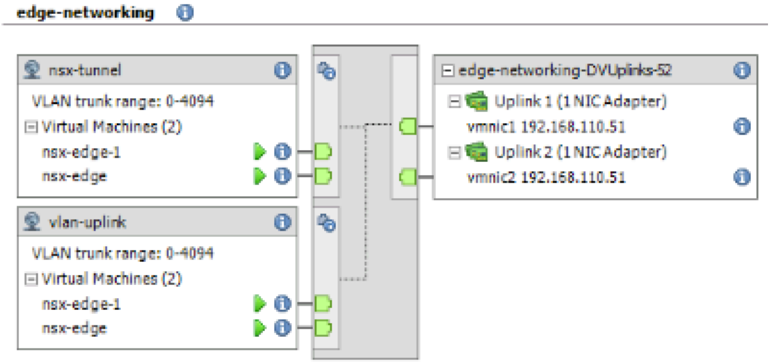
In the following sample physical topology, fp-eth0 is used for the NSX-T Data Center overlay tunnel. fp-eth1 is used for the VLAN uplink. fp-eth2 and fp-eth3 are not used. vNIC1 is assigned to the management network.

Figure 9-2. One Suggested Link Setup for NSX Edge VM Networking



The NSX Edge shown in this example belongs to two transport zones (one overlay and one VLAN) and therefore has two N-VDS, one for tunnel and one for uplink traffic.

This screenshot shows the virtual machine port groups, nsx-tunnel, and vlan-uplink.



edge-networking

nsx-tunnel
VLAN trunk range: 0-4094
⊟ Virtual Machines (2)
nsx-edge-1
nsx-edge

vlan-uplink
VLAN trunk range: 0-4094
⊟ Virtual Machines (2)
nsx-edge-1
nsx-edge

⊟ edge-networking-DVUplinks-52
⊟ Uplink 1 (1 NIC Adapter)
vmnic1 192.168.110.51
⊟ Uplink 2 (1 NIC Adapter)
vmnic2 192.168.110.51

During deployment, you must specify the network names that match the names configured on your VM port groups. For example, to match the VM port groups in the example, your network ovftool settings can be as follows if you were using the ovftool to deploy NSX Edge:

```
--net:"Network 0-Mgmt" --net:"Network 1-nsx-tunnel" --net:"Network 2=vlan-uplink"
```

The example shown here uses the VM port group names Mgmt, nsx-tunnel, and vlan-uplink. You can use any names for your VM port groups.

The tunnel and uplink VM port groups configured for the NSX Edge do not need to be associated with VMkernel ports or given IP addresses. This is because they are used at Layer 2 only. If your deployment uses DHCP to provide an address to the management interface, make sure that only one NIC is assigned to the management network.

Notice that the VLAN and tunnel port groups are configured as trunk ports. This is required. For example, on a standard vSwitch, you configure trunk ports as follows: . **Host > Configuration > Networking > Add Networking > Virtual Machine > VLAN ID All (4095)**.

If you are using an appliance-based or VM NSX Edge, you can use standard vSwitches or vSphere distributed switches.

NSX Edge VM can be installed on an NSX-T Data Center prepared host and configured as a transport node. There are two types of deployment:

- NSX Edge VM can be deployed using VSS/VDS port groups where VSS/VDS consume separate pNIC(s) on the host. Host transport node consumes separate pNIC(s) for N-VDS installed on the host. N-VDS of the host transport node co-exists with a VSS or VDS, both consuming separate pNICs. Host TEP (Tunnel End Point) and NSX Edge TEP can be in the same or different subnets.
- NSX Edge VM can be deployed using VLAN-backed logical switches on the N-VDS of the host transport node. Host TEP and NSX Edge TEP must be in different subnets.

Optionally, you can install multiple NSX Edge appliances/VMs on a single host, and the same management, VLAN, and tunnel endpoint port groups can be used by all installed NSX Edges.

With the underlying physical links up and the VM port groups configured, you can install the NSX Edge.

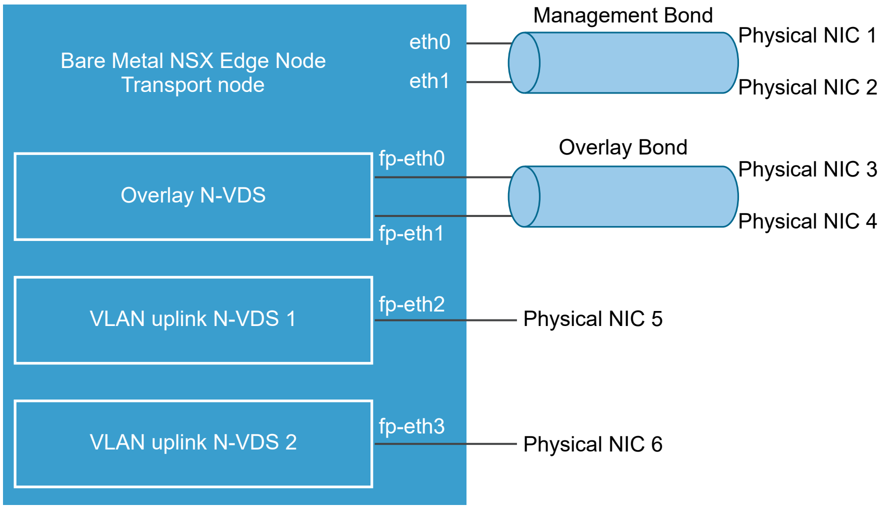
Bare-Metal NSX Edge Networking

The bare-metal NSX Edge contains internal interfaces called fp-ethX, where X is 0, 1, 2, 3, or 4. The number of fp-ethX interfaces created depends on how many physical NICs your bare-metal NSX Edge has. Up to four of these interfaces can be allocated for uplinks to top-of-rack (ToR) switches and NSX-T Data Center overlay tunneling.

When you create the NSX Edge transport node, you can select fp-ethX interfaces to associate with the uplinks and the overlay tunnel.

You can decide how to use the fp-ethX interfaces. In the following sample physical topology, fp-eth0 and fp-eth1 are bonded and used for the NSX-T Data Center overlay tunnel. fp-eth2 and fp-eth3 are used as redundant VLAN uplinks to TORs.

Figure 9-3. One Suggested Link Setup for Bare-Metal NSX Edge Networking



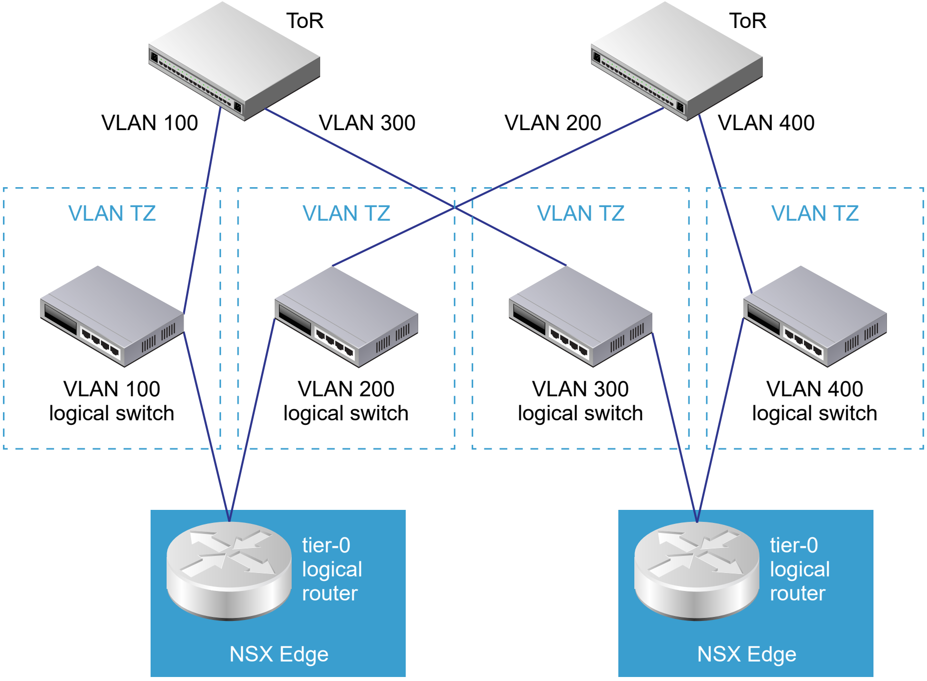
NSX Edge Uplink Redundancy

NSX Edge uplink redundancy allows two VLAN equal-cost multipath (ECMP) uplinks to be used on the NSX Edge-to-external TOR network connection.

When you have two ECMP VLAN uplinks, you must also have two TOR switches for high availability and fully meshed connectivity. Each VLAN logical switch has an associated VLAN ID.

When you add an NSX Edge to a VLAN transport zone, a new N-VDS is installed. For example, if you add an NSX Edge node to four VLAN transport zones, as shown in the figure, four N-VDS get installed on the NSX Edge.

Figure 9-4. One Suggested ECMP VLAN Setup for NSX Edges to TORs



Note For an Edge VM deployed on an ESXi host that has the vSphere Distributed Switch (vDS) and not N-VDS, you must do the following:

- Enable forged transmit for DHCP to work.
- Enable promiscuous mode for the Edge VM to receive unknown unicast packets because MAC learning is disabled by default. This is not necessary for vDS 6.6 or later, which has MAC learning enabled by default.

NSX Edge Installation Methods

Install NSX Edge on an ESXi host using NSX Manager UI (recommended method), vSphere web client, or the vSphere command-line OVF tool.

NSX Edge Installation Methods

Installation Method	Instructions
NSX Manager (recommended method to install an NSX Edge VM appliance only)	■ Ensure NSX Edge network requirements are met. See NSX Edge Installation Requirements. ■ Create an NSX Edge transport node. See Create an NSX Edge Transport Node. ■ Create an NSX Edge cluster. See Create an NSX Edge Cluster.
vSphere web client or vSphere command-line OVF tool	■ Ensure NSX Edge network requirements are met. See NSX Edge Installation Requirements. ■ Choose vSphere web client or vSphere command-line OVF tool to install NSX Edge. ■ (Web Client) Install NSX Edge on ESXi. See Install an NSX Edge on ESXi Using the vSphere GUI. ■ (Command-line OVF tool) Install NSX Edge on ESXi. See Install NSX Manager on ESXi Using the Command-Line OVF Tool. ■ Join NSX Edge with the Management Plane. See Join NSX Edge with the Management Plane. ■ Configure an NSX Edge as a transport node. See Configure an NSX Edge as a Transport Node. ■ Create an NSX Edge cluster. See Create an NSX Edge Cluster.
(Bare Metal Server) ISO (Automated or Interactive mode via ISO file) or as an NSX Edge VM appliance	You can configure automated installation of NSX Edge on a bare metal server or install NSX Edge as a VM appliance using PXE. Note that PXE boot installation procedure is not supported on NSX Manager. ■ Ensure NSX Edge network requirements are met. See NSX Edge Installation Requirements. ■ Prepare PXE server. See Prepare the PXE Server for NSX Edge . Choose from one of the supported installation methods: ■ (Automated installation) Install NSX Edge via ISO File on Bare Metal. See Install NSX Edge Automatically via ISO File. ■ (Automated installation) Install NSX Edge via ISO File as a Virtual Appliance. See Install NSX Edge via ISO File as a Virtual Appliance. ■ (Manual installation) Manually Install NSX Edge via ISO File. See Install NSX Edge Interactively via ISO File . ■ Join NSX Edge with the Management Plane. See Join NSX Edge with the Management Plane. ■ Configure an NSX Edge as a transport node. See Configure an NSX Edge as a Transport Node. ■ Create an NSX Edge cluster. See Create an NSX Edge Cluster.

Create an NSX Edge Transport Node

You can add an NSX Edge VM to the NSX-T Data Center fabric and proceed to configure it as a NSX Edge transport node VM.

An NSX Edge Node is a transport node that runs the local control plane daemons and forwarding engines implementing the NSX-T data plane. It runs an instance of the NSX-T virtual switch called the NSX Virtual Distributed Switch, or N-VDS. The Edge Nodes are service appliances dedicated to running centralized network services that cannot be distributed to the hypervisors. They can be instantiated as a bare metal appliance or in virtual machine form factor. They are grouped in one or several clusters, representing a pool of capacity.

An NSX Edge can belong to one overlay transport zone and multiple VLAN transport zones. An NSX Edge belongs to at least one VLAN transport zone to provide the uplink access.

Note If you plan to create transport nodes from a template VM, make sure that there are no certificates on the host in `/etc/vmware/nsx/`. nsx-proxy does not create a certificate if a certificate already exists.

Prerequisites

- Transport zones must be configured. See Create Transport Zones.
- Verify that compute manager is configured. See Add a Compute Manager.
- An uplink profile must be configured or you can use the default uplink profile for NSX Edge nodes. See Create an Uplink Profile.
- An IP pool must be configured or must be available in the network deployment. See Create an IP Pool for Tunnel Endpoint IP Addresses.

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Select **System > Fabric > Nodes > Edge Transport Nodes > Add Edge VM**.
3. Type a name for the NSX Edge.
4. Type the Host name or FQDN from vCenter Server.
5. Select the form factor for the NSX Edge VM appliance.

6 To customize CPU and memory allocated to an NSX Edge VM appliance, tune the following parameters. However, for maximum performance NSX Edge VM appliance must be assigned 100% of the available resources .

Caution If you customize resources allocated to the NSX Edge VM, turn back the reservation later on to 100% to get maximum performance.

Option	Description
Memory Reservation (%)	Reservation percentage is relative to the pre-defined value in the form factor. 100 indicates 100% of memory is reserved for the NSX Edge VM. If you enter 50, it indicates that 50% of the allocated memory is reserved for the Edge transport node.
CPU Reservation Priority	Select the number of shares to be allocated to an NSX Edge VM relative to other VMs that are contending for shared resources. The following shares are for an NSX Edge VM in Medium form factor: ■ Low - 2000 shares ■ Normal - 4000 shares ■ High - 8000 shares ■ Extra High - 10000 shares
CPU Reservation (MHz)	**Caution** Unless you need fine grained control over CPU reservations, do not use this field. Instead, change CPU reservations from the **CPU Reservation Priority** field. The maximum CPU reservation value must not exceed the number of vCPUs multiplied by the normal CPU operation rate of the physical CPU core. If the MHz value entered exceeds the maximum CPU capacity of the physical CPU cores, the NSX Edge VM might fail to start even though the allocation was accepted. For example, consider a system with two Intel Xeon E5-2630 CPUs. Each CPU contains ten cores running at 2.20 GHz. The maximum CPU allocation for a VM configured with two vCPUs is 2 x 2200 MHz = 4400 MHz. If CPU reservation is specified as 8000 MHz, the reconfiguration of the VM completes successfully. However, the VM fails to power on.

7 In the Credentials window, enter the following details.

- Specify the CLI and the root passwords for the NSX Edge. Your passwords must comply with the password strength restrictions.
  - At least 12 characters
  - At least one lower-case letter
  - At least one upper-case letter
  - At least one digit
  - At least one special character
  - At least five different characters

  - No dictionary words
  - No palindromes
  - More than four monotonic character sequence is not allowed
- To enable SSH for an administrator, toggle the **Allow SSH Login** button.
- To enable SSH for a root user, toggle the **Allow Root SSH Login** button.
- Enter credentials for the Audit role. If you do not enter credentials in the **Audit Credentials** section, the audit role remains disabled.

8 Enter the NSX Edge details.

Option	Description
Compute Manager	Select the compute manager from the drop-down menu. The compute manager is the vCenter Server registered in the Management Plane.
Cluster	Designate the cluster the NSX Edge is going to join from the drop-down menu.
Resource Pool or Host	Assign either a resource pool or a specific host for the NSX Edge from the drop-down menu.
Datastore	Select a datastore for the NSX Edge files from the drop-down menu.

9 Enter the NSX Edge interface details.

Option	Description
IP Assignment	It is the IP address assigned to NSX Edge node which is required to communicate with NSX Manager and NSX Controller. Select **DHCP** or **Static** IP. If you select **Static**, enter the values for: ■ Management IP: Enter IP address of NSX Edge in the CIDR notation. ■ Default gateway: Enter the gateway IP address of NSX Edge.
Management Interface	Select the management network interface from the drop-down menu. This interfaces must either be reachable from NSX Manager or must be in the same management interface as NSX Manager and NSX Controller. The NSX Edge management interface establishes communication with the NSX Manager management interface.
Search Domain Names	Enter domain names in the format 'example.com' or enter an IP address.
DNS Servers	Enter the IP address of the DNS server.
NTP Servers	Enter the IP address of the NTP server.

10 Enter the N-VDS information.

Option	Description
Edge Switch Name	Select a VLAN or Overlay switch from the drop-down menu.
Transport Zone	Select the transport zones that this transport node belongs to. An NSX Edge transport node belongs to at least two transport zones, an overlay for NSX-T Data Center connectivity and a VLAN for uplink connectivity. **Note** NSX Edge Nodes support multiple overlay tunnels (multi-TEP) when the following prerequistes are met: ■ TEP configuration must be done on one N-VDS only. ■ All TEPs must use same transport VLAN for overlay traffic. ■ All TEP IPs must be in same subnet and use same default gateway.
Uplink Profile	Select the uplink profile from the drop-down menu. The available uplinks depend on the configuration in the selected uplink profile.
IP Assignment	IP address is assigned to the NSX Edge switch that is configured. It is used to route packets on an overlay or VLAN network. Select **Use IP Pool** or **Use Static IP List** for the overlay N-VDS. ■ If you select **Use Static IP List**, specify: ■ Static IP List: Enter a list of comma-separated IP addresses to be used by the NSX Edge switch. ■ Gateway: Enter the default gateway IP address, which is used to route packets between NSX Edge transport nodes in an overlay network. ■ Subnet mask: Enter the subnet mask for the configured gateway. ■ If you selected **Use IP Pool** for IP assignment, specify the IP pool name.
DPDK Fastpath Interfaces / Virtual NICs	Select the data path interface name for the uplink interface. **Note** If the uplink profile applied to the Edge node is using a Named Teaming policy, ensure the following condition is met: ■ All uplinks in the Default Teaming policy must be mapped to the physical network interfaces on the Edge VM for traffic to flow through a logical switch that uses the Named Teaming policies.

Note

- LLDP profile is not supported on an NSX Edge VM appliance.
- Uplink interfaces are displayed as **DPDK Fastpath Interfaces** if the NSX Edge is installed using NSX Manager or on a Bare Metal server.
- Uplink interfaces are displayed as **Virtual NICs** if the NSX Edge is installed manually using vCenter Server.

11 View the connection status on the **Transport Nodes** page.

After adding the NSX Edge as a transport node, the connection status changes to Up in 10-12 minutes.

12 (Optional) View the transport node with the `GET https://<nsx-manager>/api/v1/transport-nodes/<transport-node-id>` API call.

13 (Optional) For status information, use the `GET https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/status` API call.

14 If you see inaccurate resource configuration details, such as compute, datastore, or network details that were configured when you installed the NSX Edge node, refresh the configuration details by running the API command.

```
POST api/v1/transport-nodes/<transport-node-id>?
action=refresh_node_configuration&resource_type=EdgeNode
```

NSX Manager displays inaccurate or stale NSX Edge node details if one of these conditions are true:

- On the NSX Edge node, if you change settings such as SSH, NTP, DNS and so from the NSX Edge command line interface.
- If the NSX Edge VM appliance is moved to another host using vCenter, the NSX Manager may have stale values of compute, datastore, and network configuration based on the configuration of the new host.

What to do next

Add the NSX Edge node to an NSX Edge cluster. See Create an NSX Edge Cluster.

Create an NSX Edge Cluster

Having a multi-node cluster of NSX Edges helps ensure that at least one NSX Edge is always available.

In order to create a tier-0 logical router or a tier-1 router with stateful services such as NAT, load balancer, and so on. You must associate it with an NSX Edge cluster. Therefore, even if you have only one NSX Edge, it must still belong to an NSX Edge cluster to be useful.

An NSX Edge transport node can be added to only one NSX Edge cluster.

An NSX Edge cluster can be used to back multiple logical routers.

After creating the NSX Edge cluster, you can later edit it to add additional NSX Edges.

Prerequisites

- Install at least one NSX Edge node.
- Verify that the NSX Edge node is stable, with all services up and running and all groups are stable, before joining the node to the cluster.
- Join the NSX Edges with the management plane.
- Add the NSX Edges as transport nodes.
- Optionally, create an NSX Edge cluster profile for high availability (HA). You can also use the default NSX Edge cluster profile.

Procedure

1 From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.

2 Select **System > Fabric > Nodes > Edge Clusters > Add**.

3 Enter the NSX Edge cluster a name.

4 Select an NSX Edge cluster profile from the drop-down menu.

5 In Member Type drop-down menu, select either `Edge Node` if the virtual machine is deployed on-premises or `Public Cloud Gateway` if the virtual machine is deployed in a public cloud.

6 From the **Available** column, select NSX Edges and click the right-arrow to move them to the **Selected** column.

What to do next

You can now build logical network topologies and configure services. See the *NSX-T Data Center Administration Guide*.

Install an NSX Edge on ESXi Using the vSphere GUI

You can use the vSphere Web Client or vSphere Client to interactively install an NSX Edge on ESXi.

Note Starting in NSX-T Data Center 2.5.1, the NSX Edge VM supports vMotion.

Prerequisites

See NSX Edge network requirements in NSX Edge Installation Requirements.

Procedure

1 Locate the NSX Edge node appliance OVA file on the VMware download portal.

Either copy the download URL or download the OVA file onto your computer.

2 In the vSphere Client, select the host on which to install NSX Edge node appliance.

3 Right-click and select **Deploy OVF template** to start the installation wizard.

4 Enter the download OVA URL or navigate to the saved OVA file, and click **Next**.

5 Enter a name and location for the NSX Edge node VM, and click **Next**.

The name you type appears in the vCenter Server and vSphere inventory.

6 Select a compute resource for the NSX Edge node appliance, and click **Next**.

7 For an optimal performance, reserve memory for the NSX Edge appliance.

Set the reservation to ensure that NSX Edge has sufficient memory to run efficiently. See NSX Edge VM System Requirements.

8 Review and verify the OVF template details, and click **Next**.

9 Select a deployment configuration, **Small**, **Medium**, **Large**, or **XLarge** and click **Next**.

The Description panel on the right side of the wizard shows the details of selected configuration.

10 Select storage for the configuration and disk files, and click **Next**.

   a Select the virtual disk format.

   b Select the VM storage policy.

   c Specify the datastore to store the NSX Edge node appliance files.

11 Select a destination network for each source network.

   a For network 0, select the VDS management portgroup.

   b For networks 1, 2, and 3, select the previously configured VDS trunk portgroups.

12 Configure IP Allocation settings.

   a For IP allocation, specify `Static - Manual`.

   b For IP protocol, select `IPv4`.

13 Click **Next**.

   The following steps are all located in the Customize Template section of the Deploy OVF Template wizard.

14 Enter the NSX Edge node system root, CLI admin, and audit passwords.

   Note In the Customize Template window, ignore the message `All properties have valid values` that is displayed even before you have entered values in any of the fields. This message is displayed because all parameters are optional. The validation passes as you have not entered values in any of the fields.

   When you log in for the first time, you are prompted to change the password. This password change method has strict complexity rules, including the following:

   - At least 12 characters
   - At least one lower-case letter
   - At least one upper-case letter
   - At least one digit
   - At least one special character
   - At least five different characters
   - No dictionary words
   - No palindromes
   - More than four monotonic character sequence is not allowed

   Important The core services on the appliance do not start until a password with sufficient complexity has been set.

15 (Optional) If you have an available NSX Manager and want to register the NSX Edge with the management plane during the OVA deployment, complete the Manager IP, Username, Password, and Thumbprint.

- Manager IP: Enter the NSX Manager node IP address.

  Note Do not register the NSX Edge with the virtual IP (VIP) address of the management plane during the OVA deployment.

- Manager Username: Enter the NSX Manager username.
- Manager Password: Enter the NSX Manager password.
- Manager Thumbprint: Enter the NSX Manager thumbprint.
- Node ID: Leave the field blank. The Node UUID field is only for internal use.

16 (Optional) If you want to deploy the NSX Edge as an autonomous edge in a L2 VPN topology, enable the option. An autonomous edge is not managed by NSX-T Data Center. Do not enable the option if you want to deploy an NSX Edge that provides centralized edge services to host transport nodes in an NSX-T Data Center topology.

Note The fields in the External and HA sections are required only when you are configure an autonomous edge node.

17 Enter the hostname of the NSX Edge node VM.

18 Enter the default gateway, management network IPv4, and management network netmask address.

Skip any VMC network settings.

19 Enter the DNS Server, the Domain Search list, and the NTP Server list.

20 (Optional) Do not enable SSH if you prefer to access NSX Edge using the console. However, if you want root SSH login and CLI login to the NSX Edge command line, enable the SSH option.

By default, SSH access is disabled for security reasons.

21 Verify that all your custom OVA template specification is accurate and click **Finish** to initiate the installation.

The installation might take 7-8 minutes.

22 Open the console of the NSX Edge node VM to track the boot process.

If the console window does not open, make sure that pop-ups are allowed.

23 After the NSX Edge node VM starts, log in to the CLI with admin credentials.

Note After NSX Edge node VM starts, if you do not log in with admin credentials for the first time, the data plane service does not automatically start on the NSX Edge node VM.

24 Run the `get interface eth0` (without VLAN) or `get interface eth0.<vlan_ID>` (with a VLAN) command to verify that the IP address was applied as expected.

```
nsx-edge-1> get interface eth0.100

Interface: eth0.100
  Address: 192.168.110.37/24
  MAC address: 00:50:56:86:62:4d
  MTU: 1500
  Default gateway: 192.168.110.1
  Broadcast address: 192.168.110.255
  ...
```

Note When bringing up NSX Edge VMs on non-NSX managed host, verify that the MTU setting is set to 1600 (instead of 1500) on the physical host switch for the data NIC.

25 Run the `get managers` command to verify that the NSX Edge is registered.

```
- 10.173.161.17  Connected (NSX-RPC)
- 10.173.161.140 Connected (NSX-RPC)
- 10.173.160.204 Connected (NSX-RPC)
```

26 If NSX Edge is not registered with the management plane, see Join NSX Edge with the Management Plane.

27 Verify that the NSX Edge node VM has the required connectivity.

If you enabled SSH, make sure that you can SSH to your NSX Edge node VM and verify the following:

- You can ping your NSX Edge node VM management interface.
- From the NSX Edge node VM, you can ping the node's default gateway.
- From the NSX Edge node VM, you can ping the hypervisor hosts that are either in the same network or a network reachable through routing.
- From the NSX Edge node VM, you can ping the DNS server and NTP server.

28 Troubleshoot connectivity problems.

Note If connectivity is not established, make sure the VM network adapter is in the proper network or VLAN.

By default, the NSX Edge node VM datapath claims all virtual machine NICs except the management NIC (the one that has an IP address and a default route). If you incorrectly assigned a NIC as the management interface, follow these steps to use DHCP to assign management IP address to the correct NIC.

a Log in CLI and type the **`stop service dataplane`** command.

b Type the **`set interface`** ***`interface`*** **`dhcp plane mgmt`** command.

c Place *interface* into the DHCP network and wait for an IP address to be assigned to that *interface*.

d Type the `start service dataplane` command.

The datapath fp-ethX ports used for the VLAN uplink and the tunnel overlay are shown in the **get interfaces** and **get physical-port** commands on the NSX Edge node VM.

What to do next

Configure NSX Edge as a transport node. See Configure an NSX Edge as a Transport Node.

Install NSX Edge on ESXi Using the Command-Line OVF Tool

If you prefer to automate NSX Edge installation, you can use the VMware OVF Tool, which is a command-line utility.

Prerequisites

- Verify that the system requirements are met. See System Requirements.
- Verify that the required ports are open. See Ports and Protocols.
- Verify that a datastore is configured and accessible on the ESXi host.
- Verify that you have the IP address and gateway, DNS server IP addresses, domain search list, and the NTP server IP address for the NSX Manager to use.
- If you do not already have one, create the target VM port group network. Place the NSX-T Data Center appliances on a management VM network.

  If you have multiple management networks, you can add static routes to the other networks from the NSX-T Data Center appliance.
- Plan your NSX Manager IPv4 IP addressing scheme.
- See NSX Edge network requirements in NSX Edge Installation Requirements.
- Verify that you have adequate privileges to deploy an OVF template on the ESXi host.
- Verify that hostnames do not include underscores. Otherwise, the hostname is set to *localhost*.
- OVF Tool version 4.3 or later.
- Know parameters that you can use to deploy a NSX Edge VM and join it to the management plane.

Field Name	OVF Parameter	Field Type
System root password	`nsx_passwd_0`	Required to install. NSX Edge
CLI admin password	`nsx_cli_passwd_0`	Required to install NSX Edge.
CLI audit password	`nsx_cli_audit_passwd_0`	Optional
CLI admin username	`nsx_cli_username`	Optional
CLI audit username	`nsx_cli_audit_username`	Optional
NSX Manager IP	`mpIp`	Required to join NSX Edge VM to NSX Manager.

Field Name	OVF Parameter	Field Type
NSX Manager token	`mpToken`	Required to join NSX Edge VM to NSX Manager. To retrieve token, on the NSX Manager, run `POST https://<nsx-manager>/api/v1/aaa/registration-token`.
NSX Manager thumbprint	`mpThumbprint`	Required to join NSX Edge VM to NSX Manager. To retrieve thumbprint, on the NSX Manager node, run `get certificate api thumbprint`.
Node Id	`mpNodeId`	Only for internal use.
Hostname	`nsx_hostname`	Optional
Default IPv4 gateway	`nsx_gateway_0`	Optional
Management network IP address	`nsx_ip_0`	Optional
Management network netmask	`nsx_netmask_0`	Optional
DNS servers	`nsx_dns1_0`	Optional
Domain Search suffixes	`nsx_domain_0`	Optional
NTP Servers	`nsx_ntp_0`	Optional
Is SSH service enabled	`nsx_isSSHEnabled`	Optional
Is SSH enabled for root login	`nsx_allowSSHRootLogin`	Optional
Is autonomous Edge	is_autonomous_edge	Optional. Valid values: `True`, `False` (default)

Procedure

- For a standalone host, run the `ovftool` command with the appropriate parameters.

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-edge-1
--deploymentOption=medium
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--net:"Network 0=Mgmt"
--net:"Network 1=nsx-tunnel"
--net:"Network 2=vlan-uplink"
--net:"Network 3=vlan-uplink"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.37
```

```
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=True
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-edge
--prop:mpIp=<NSXManager-IP>
--prop:mpToken=<NSXManager-Token>
--prop:mpThumbprint=<NSXManager-Thumbprint>
--prop:is_autonomous_edge=False
<path/url to nsx component ova>
vi://root:<password>@192.168.110.51
```

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://root@192.168.110.24
Deploying to VI: vi://root@192.168.110.24
Transfer Completed
Powering on VM: nsx-edge-1
Task Completed
Completed successfully
```

- For a host managed by vCenter Server, run the `ovftool` command with the appropriate parameters.

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-edge-1
--deploymentOption=medium
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--net:"Network 0=Mgmt"
--net:"Network 1=nsx-tunnel"
--net:"Network 2=vlan-uplink"
--net:"Network 3=vlan-uplink"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.37
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=True
```

```
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-edge
--prop:mpIp=<NSXManager-IP>
--prop:mpToken=<NSXManager-Token>
--prop:mpThumbprint=<NSXManager-Thumbprint>
--prop:is_autonomous_edge=False
<path/url to nsx component ova>
vi://administrator@vsphere.local:<password>@192.168.110.24/?ip=192.168.210.53
```

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://administrator@vsphere.local@192.168.110.24:443/
Deploying to VI: vi://administrator@vsphere.local@192.168.110.24:443/
Transfer Completed
Powering on VM: nsx-edge-1
Task Completed
Completed successfully
```

- For an optimal performance, reserve memory for the NSX Manager appliance.

  Set the reservation to ensure that NSX Manager has sufficient memory to run efficiently. See NSX Manager VM and Host Transport Node System Requirements.

- Open the console of the NSX Edge node VM to track the boot process.

- After the NSX Edge node VM starts, log in to the CLI with admin credentials.

- Run the `get interface eth0` (without VLAN) or `get interface eth0.<vlan_ID>` (with a VLAN) command to verify that the IP address was applied as expected.

```
nsx-edge-1> get interface eth0.100

Interface: eth0.100
  Address: 192.168.110.37/24
  MAC address: 00:50:56:86:62:4d
  MTU: 1500
  Default gateway: 192.168.110.1
  Broadcast address: 192.168.110.255
  ...
```

Note When bringing up NSX Edge VMs on non-NSX managed host, verify that the MTU setting is set to 1600 (instead of 1500) on the physical host switch for the data NIC.

- Verify that the NSX Edge node VM has the required connectivity.

  If you enabled SSH, make sure that you can SSH to your NSX Edge node VM and verify the following:

  - You can ping your NSX Edge node VM management interface.
  - From the NSX Edge node VM, you can ping the node's default gateway.
  - From the NSX Edge node VM, you can ping the hypervisor hosts that are either in the same network or a network reachable through routing.
  - From the NSX Edge node VM, you can ping the DNS server and NTP server.

- Troubleshoot connectivity problems.

  Note If connectivity is not established, make sure the VM network adapter is in the proper network or VLAN.

  By default, the NSX Edge node VM datapath claims all virtual machine NICs except the management NIC (the one that has an IP address and a default route). If you incorrectly assigned a NIC as the management interface, follow these steps to use DHCP to assign management IP address to the correct NIC.

  a Log in CLI and type the `stop service dataplane` command.

  b Type the `set interface` *`interface`* `dhcp plane mgmt` command.

  c Place *interface* into the DHCP network and wait for an IP address to be assigned to that *interface*.

  d Type the `start service dataplane` command.

  The datapath fp-ethX ports used for the VLAN uplink and the tunnel overlay are shown in the **get interfaces** and **get physical-port** commands on the NSX Edge node VM.

What to do next

If you did not join the NSX Edge with the management plane, see Join NSX Edge with the Management Plane.

Install NSX Edge via ISO File as a Virtual Appliance

You can install NSX Edge VMs in a manual fashion using an ISO file.

Important The NSX-T Data Center component virtual machine installations include VMware Tools. Removal or upgrade of VMware Tools is not supported for NSX-T Data Center appliances.

Prerequisites

- See NSX Edge network requirements in NSX Edge Installation Requirements.

Procedure

1 Go to your MyVMware account (myvmware.com) and navigate to **VMware NSX-T Data Center > Downloads**.

2. Locate and download the ISO file for NSX Edge.
3. In the vSphere Client, select the host datastore.
4. Select **Files > Upload Files > Upload a File to a Datastore**, browse to the ISO file, and upload.

   If you are using a self-signed certificate, open the IP address in a browser and accept the certificate and reupload the ISO file.
5. In the vSphere Client inventory, select the host you uploaded the ISO file. or in the vSphere Client,
6. Right-click and select **New Virtual Machine** .
7. Select a compute resource for the NSX Edge appliance.
8. Select a datastore to store the NSX Edge appliance files.
9. Accept the default compatibility for your NSX Edge VM.
10. Select the supported ESXi operating systems for your NSX Edge VM.
11. Configure the virtual hardware.
    - New Hard Disk - `200 GB`
    - New Network - `VM Network`
    - New CD/DVD Drive - `Datastore ISO File`

      You must click **Connect** to bind the NSX Edge ISO file to the VM.
12. Power on the new NSX Edge VM.
13. During ISO boot, open the VM console and choose **Automated installation**.

    There might be a pause of 10 seconds after you press Enter.

    During installation, the installer prompts you to enter a VLAN ID for the management interface. Select **Yes** and enter a VLAN ID to create a VLAN subinterface for the network interface. Select **No** if you do not want to configure VLAN tagging on the packet.

    During power-on, the VM requests a network configuration via DHCP. If DHCP is not available in your environment, the installer prompts you for IP settings.

    By default, the root login password is `vmware`, and the admin login password is `default`.

    When you log in for the first time, you are prompted to change the password. This password change method has strict complexity rules, including the following:
    - At least 12 characters
    - At least one lower-case letter
    - At least one upper-case letter
    - At least one digit
    - At least one special character
    - At least five different characters

- No dictionary words
- No palindromes
- More than four monotonic character sequence is not allowed

Important The core services on the appliance do not start until a password with sufficient complexity has been set.

14. For an optimal performance, reserve memory for the NSX Edge appliance.

    Set the reservation to ensure that NSX Edge has sufficient memory to run efficiently. See NSX Edge VM System Requirements.

15. After the NSX Edge node VM starts, log in to the CLI with admin credentials.

    Note After NSX Edge node VM starts, if you do not log in with admin credentials for the first time, the data plane service does not automatically start on the NSX Edge node VM.

16. There are three ways to configure a management interface.

    Note If the server uses Mellanox NIC cards, do not configure the Edge in In-band management interface.

    - Untagged interface. This interface type creates an out-of-band management interface.

      (DHCP) `set interface eth0 dhcp plane mgmt`

      (Static) `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt`

    - Tagged interface.

      `set interface eth0 vlan <vlan_ID> plane mgmt`

      (DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

      (Static) `set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`

    - In-band interface.

      `set interface mac <mac_address> vlan <vlan_ID> in-band plane mgmt`

      (DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

      (Static) `set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`

17. (Optional) Start SSH service. Run `start service ssh` .

18. Run the `get interface eth0` (without VLAN) or `get interface eth0.<vlan_ID>` (with a VLAN) command to verify that the IP address was applied as expected.

```
nsx-edge-1> get interface eth0.100

Interface: eth0.100
  Address: 192.168.110.37/24
  MAC address: 00:50:56:86:62:4d
```

```
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

Note When bringing up NSX Edge VMs on non-NSX managed host, verify that the MTU setting is set to 1600 (instead of 1500) on the physical host switch for the data NIC.

19. (Tagged interface and In-band interface) Any existing VLAN management interface must be cleared before creating a new one.

    ```
    Clear interface eth0.<vlan_ID>
    ```

    To set a new interface, refer to step 15.

20. Verify that the NSX Edge node VM has the required connectivity.

    If you enabled SSH, make sure that you can SSH to your NSX Edge node VM and verify the following:

    - You can ping your NSX Edge node VM management interface.
    - From the NSX Edge node VM, you can ping the node's default gateway.
    - From the NSX Edge node VM, you can ping the hypervisor hosts that are either in the same network or a network reachable through routing.
    - From the NSX Edge node VM, you can ping the DNS server and NTP server.

21. Troubleshoot connectivity problems.

    Note If connectivity is not established, make sure the VM network adapter is in the proper network or VLAN.

    By default, the NSX Edge node VM datapath claims all virtual machine NICs except the management NIC (the one that has an IP address and a default route). If you incorrectly assigned a NIC as the management interface, follow these steps to use DHCP to assign management IP address to the correct NIC.

    a. Log in CLI and type the **`stop service dataplane`** command.

    b. Type the **`set interface`** ***`interface`*** **`dhcp plane mgmt`** command.

    c. Place *interface* into the DHCP network and wait for an IP address to be assigned to that *interface*.

    d. Type the **`start service dataplane`** command.

       The datapath fp-ethX ports used for the VLAN uplink and the tunnel overlay are shown in the **get interfaces** and **get physical-port** commands on the NSX Edge node VM.

What to do next

If you did not join the NSX Edge with the management plane, see Join NSX Edge with the Management Plane.

Install NSX Edge on Bare Metal

Use PXE server to automate nstallation of NSX Edge on a bare metal server or use ISO file to install NSX Edge as a VM appliance or on a bare metal server.

Note PXE boot installation is not supported for NSX Manager. You also cannot configure networking settings, such as the IP address, gateway, network mask, NTP, and DNS.

Prepare the PXE Server for NSX Edge

PXE is made up of several components: DHCP, HTTP, and TFTP. This procedure demonstrates how to set up a PXE server on Ubuntu.

DHCP dynamically distributes IP settings to NSX-T Data Center components, such as NSX Edge. In a PXE environment, the DHCP server allows NSX Edge to request and receive an IP address automatically.

TFTP is a file-transfer protocol. The TFTP server is always listening for PXE clients on the network. When it detects any network PXE client asking for PXE services, it provides the NSX-T Data Center component ISO file and the installation settings contained in a preseed file.

Prerequisites

- A PXE server must be available in your deployment environment. The PXE server can be set up on any Linux distribution. The PXE server must have two interfaces, one for external communication and another for providing DHCP IP and TFTP services.

  If you have multiple management networks, you can add static routes to the other networks from the NSX-T Data Center appliance.

- Verify that the preseeded configuration file has the parameters net.ifnames=0 and biosdevname=0 set after `--` to persist after reboot.
- See NSX Edge network requirements in NSX Edge Installation Requirements.

Procedure

1 (Optional) Use a kickstart file to set up a new TFTP or DHCP services on an Ubuntu server.

  A kickstart file is a text file that contains CLI commands that you run on the appliance after the first boot.

  Name the kickstart file based on the PXE server it is pointing to. For example:

```
nsxcli.install
```

  The file must be copied to your Web server, for example at `/var/www/html/nsx-edge/nsxcli.install`.

In the kickstart file, you can add CLI commands. For example, to configure the IP address of the management interface:

```
stop dataplane
set interface eth0 <ip-cidr-format> plane mgmt
start dataplane
```

To change the admin user password:

```
set user admin password <new_password> old-password <old-password>
```

If you specify a password in the preseed.cfg file, use the same password in the kickstart file. Otherwise, use the default password, which is "default".

To join the NSX Edge with the management plane:

```
join management-plane <manager-ip> thumbprint <manager-thumbprint> username <manager-username>
password <manager password>
```

2 Create two interfaces, one for management and another for DHCP and TFTP services.

Make sure that the DHCP/TFTP interface is in the same subnet that the NSX Edge resides in.

For example, if the NSX Edge management interfaces are going to be in the 192.168.210.0/24 subnet, place eth1 in that same subnet.

```
# The loopback network interface
auto lo
iface lo inet loopback

# PXE server's management interface
auto eth0
iface eth0 inet static
  address 192.168.110.81
  gateway 192.168.110.1
  netmask 255.255.255.0
  dns-nameservers 192.168.110.10

# PXE server's DHCP/TFTP interface
auto eth1
iface eth1 inet static
  address 192.168.210.82
  gateway 192.168.210.1
  netmask 255.255.255.0
  dns-nameservers 192.168.110.10
```

3 Install DHCP server software.

```
sudo apt-get install isc-dhcp-server -y
```

4. Edit the `/etc/default/isc-dhcp-server` file, and add the interface that provides the DHCP service.

   ```
   INTERFACES="eth1"
   ```

5. (Optional) If you want this DHCP server to be the official DHCP server for the local network, uncomment the **authoritative;** line in the `/etc/dhcp/dhcpd.conf` file.

   ```
   ...
   authoritative;
   ...
   ```

6. In the `/etc/dhcp/dhcpd.conf` file, define the DHCP settings for the PXE network.

   For example:

   ```
   subnet 192.168.210.0 netmask 255.255.255.0 {
      range 192.168.210.90 192.168.210.95;
      option subnet-mask 255.255.255.0;
      option domain-name-servers 192.168.110.10;
      option routers 192.168.210.1;
      option broadcast-address 192.168.210.255;
      default-lease-time 600;
      max-lease-time 7200;
   }
   ```

7. Start the DHCP service.

   ```
   sudo service isc-dhcp-server start
   ```

8. Verify that the DHCP service is running.

   ```
   service --status-all | grep dhcp
   ```

9. Install Apache, TFTP, and other components that are required for PXE booting.

   ```
   sudo apt-get install apache2 tftpd-hpa inetutils-inetd
   ```

10. Verify that TFTP and Apache are running.

    ```
    service --status-all | grep tftpd-hpa
    service --status-all | grep apache2
    ```

11. Add the following lines to the `/etc/default/tftpd-hpa` file.

    ```
    RUN_DAEMON="yes"
    OPTIONS="-l -s /var/lib/tftpboot"
    ```

12. Add the following line to the `/etc/inetd.conf` file.

    ```
    tftp    dgram   udp    wait    root    /usr/sbin/in.tftpd /usr/sbin/in.tftpd -s /var/lib/tftpboot
    ```

13. Restart the TFTP service.

    ```
    sudo /etc/init.d/tftpd-hpa restart
    ```

14. Copy or download the NSX Edge installer ISO file to a temporary folder.

15. Mount the ISO file and copy the install components to the TFTP server and the Apache server.

    ```
    sudo mount -o loop ~/nsx-edge.<build>.iso /mnt
    cd /mnt
    sudo cp -fr install/netboot/* /var/lib/tftpboot/
    sudo mkdir /var/www/html/nsx-edge
    sudo cp -fr /mnt/* /var/www/html/nsx-edge/
    ```

16. (Optional) Edit the `/var/www/html/nsx-edge/preseed.cfg` file to modify the encrypted passwords.

    You can use a Linux tool such as mkpasswd to create a password hash.

    ```
    sudo apt-get install whois
    sudo mkpasswd -m sha-512

    Password:
    $6$SUFGqs[...]FcoHLijOuFD
    ```

    a. Modify the root password, edit `/var/www/html/nsx-edge/preseed.cfg` and search for the following line:

       ```
       d-i passwd/root-password-crypted password $6$tgmLNLMp$9BuAHhN...
       ```

    b. Replace the hash string.

       You do not need to escape any special character such as $, ', ", or \.

    c. Add the `usermod` command to `preseed.cfg` to set the password for root, admin, or both.

       For example, search for the `echo 'VMware NSX Edge'` line and add the following command.

       ```
       usermod --password '\$6\$VS3exId0aKmzW\$U3g0V7BF0DXlmRI.LR0v/VgloxVotEDp00bO2hUF8u/' root; \
       usermod --password '\$6\$VS3exId0aKmzW\$U3g0V7BF0DXlmRI.LR0v/VgloxVotEDp00bO2hUF8u/' admin; \
       ```

       The hash string is an example. You must escape all special characters. The root password in the first `usermod` command replaces the password that is set in `d-i passwd/root-password-crypted password $6$tgm....`

       If you use the `usermod` command to set the password, the user is not prompted to change the password at the first login. Otherwise, the user must change the password at the first login.

17. Add the following lines to the `/var/lib/tftpboot/pxelinux.cfg/default` file.

    Replace 192.168.210.82 with the IP address of your TFTP server.

    ```
    label nsxedge
        kernel ubuntu-installer/amd64/linux
        ipappend 2
    ```

```
    append netcfg/dhcp_timeout=60 auto=true priority=critical vga=normal partman-lvm/
device_remove_lvm=true netcfg/choose_interface=auto debian-installer/allow_unauthenticated=true
preseed/url=http://192.168.210.82/nsx-edge/preseed.cfg mirror/country=manual mirror/http/
hostname=192.168.210.82 nsx-kickstart/url=http://192.168.210.82/nsx-edge/nsxcli.install mirror/
http/directory=/nsx-edge initrd=ubuntu-installer/amd64/initrd.gz mirror/suite=xenial --
```

18 Add the following lines to the `/etc/dhcp/dhcpd.conf` file.

Replace 192.168.210.82 with the IP address of your DHCP server.

```
allow booting;
allow bootp;

next-server 192.168.210.82; #Replace this IP address
filename "pxelinux.0";
```

19 Restart the DHCP service.

```
sudo service isc-dhcp-server restart
```

Note If an error is returned, for example: "stop: Unknown instance: start: Job failed to start", run `sudo /etc/init.d/isc-dhcp-server stop` and then `sudo /etc/init.d/isc-dhcp-server start`. The `sudo /etc/init.d/isc-dhcp-server start` command returns information about the source of the error.

What to do next

Install NSX Edge on bare metal using an ISO file. See Install NSX Edge Automatically via ISO File.

Install NSX Edge Automatically via ISO File

You can install NSX Edge devices in a manual fashion on bare metal using an ISO file. This includes configuring networking settings, such as IP address, gateway, network mask, NTP, and DNS.

Prerequisites

- Verify that the system BIOS mode is set to Legacy BIOS.
- See NSX Edge network requirements in NSX Edge Installation Requirements.

Procedure

1 Go to your MyVMware account (myvmware.com) and navigate to **VMware NSX-T Data Center > Downloads**.

2 Locate and download the ISO file for NSX Edge for Bare Metal.

3 Log in to the out-of-band management interface (for example, Integrated Lights-Out (ILO) on HP servers) of the bare metal.

4 Click **Launch** in the virtual console preview.

5 Select **Virtual Media > Connect Virtual Media**.

   Wait a few seconds for the virtual media to connect.

6 Select **Virtual Media > Map CD/DVD** and browse to the ISO file.

7 Select **Next Boot > Virtual CD/DVD/ISO**.

8 Select **Power > Reset System (warm boot)**.

   The installation duration depends on the bare metal environment.

9 Choose **Automated installation**.

   There might be a pause of 10 seconds after you press Enter.

10 Select the applicable primary network interface.

   During power-on, the installer requests a network configuration via DHCP. If DHCP is not available in your environment, the installer prompts you for IP settings.

   By default, the root login password is **vmware**, and the admin login password is **default**.

11 Open the console of the NSX Edge node VM to track the boot process.

   If the console window does not open, make sure that pop-ups are allowed.

12 After the NSX Edge node VM starts, log in to the CLI with admin credentials.

   Note After NSX Edge node VM starts, if you do not log in with admin credentials for the first time, the data plane service does not automatically start on the NSX Edge node VM.

13 After the reboot, you can log in with either admin or root credentials. The default root password is `vmware`.

14 There are three ways to configure a management interface.

   Note If the server uses Mellanox NIC cards, do not configure the Edge in In-band management interface.

   - Untagged interface. This interface type creates an out-of-band management interface.

     (DHCP) `set interface eth0 dhcp plane mgmt`

     (Static) `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt`

   - Tagged interface.

     `set interface eth0 vlan <vlan_ID> plane mgmt`

     (DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

     (Static) `set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`

   - In-band interface.

     `set interface mac <mac_address> vlan <vlan_ID> in-band plane mgmt`

     (DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

(Static) `set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`

- (Optional) Create a **`bond0`** interface for management HA interface with multiple interfaces.

  You can configure a bond management interface on an NSX Edge using the following CLI command. Use console to clear existing mangement IP before you create a bond and add an interface to it.

  Note Only active-backup mode is allowed on a bond interface. It does not allows you to configure VLAN. So, you need to configure VLAN on an access VLAN that sits closer to the physical switch.

  `set interface bond0 ip x.x.x.x/mask gateway x.x.x.x plane mgmt mode active-backup members eth0, eth1 primary eth0`

15 Run the `get interface eth0` (without VLAN) or `get interface eth0.<vlan_ID>` (with a VLAN) command to verify that the IP address was applied as expected.

```
nsx-edge-1> get interface eth0.100

Interface: eth0.100
  Address: 192.168.110.37/24
  MAC address: 00:50:56:86:62:4d
  MTU: 1500
  Default gateway: 192.168.110.1
  Broadcast address: 192.168.110.255
  ...
```

Note When bringing up NSX Edge VMs on non-NSX managed host, verify that the MTU setting is set to 1600 (instead of 1500) on the physical host switch for the data NIC.

16 (Tagged interface and In-band interface) Any existing VLAN management interface must be cleared before creating a new one.

`clear interface eth0.<vlan_ID>`

To set a new interface, refer to step 13.

17 Set physical NICs to be used by NSX-T Data Center dataplane from the list of available PCI devices.

a `get dataplace device list`

b `set dataplane device list <NIC1>, <NIC2>, <NIC3>`

c `restart service dataplane`

d `get physical-port`

After selecting physical NICs, restart NSX-T Data Center dataplane services for changes to take effect.

Note Claim up to 16 physical NICs.

18 To avoid network configuration errors, verify that the physical NICs selected match the NICs configured in the transport node profiles.

19 Before creating NSX Edge as a transport node, reset the NIC list on dataplane.

```
reset dataplane nic list
```

20 Verify that the NSX Edge node VM has the required connectivity.

If you enabled SSH, make sure that you can SSH to your NSX Edge node VM and verify the following:

- You can ping your NSX Edge node VM management interface.
- From the NSX Edge node VM, you can ping the node's default gateway.
- From the NSX Edge node VM, you can ping the hypervisor hosts that are either in the same network or a network reachable through routing.
- From the NSX Edge node VM, you can ping the DNS server and NTP server.

21 Troubleshoot connectivity problems.

Note If connectivity is not established, make sure the VM network adapter is in the proper network or VLAN.

By default, the NSX Edge node VM datapath claims all virtual machine NICs except the management NIC (the one that has an IP address and a default route). If you incorrectly assigned a NIC as the management interface, follow these steps to use DHCP to assign management IP address to the correct NIC.

a Log in CLI and type the `stop service dataplane` command.

b Type the `set interface` *`interface`* `dhcp plane mgmt` command.

c Place *interface* into the DHCP network and wait for an IP address to be assigned to that *interface*.

d Type the `start service dataplane` command.

The datapath fp-ethX ports used for the VLAN uplink and the tunnel overlay are shown in the **get interfaces** and **get physical-port** commands on the NSX Edge node VM.

What to do next

If you did not join the NSX Edge with the management plane, see Join NSX Edge with the Management Plane.

Install NSX Edge Interactively via ISO File

Install NSX Edge devices on bare metal using an ISO file in the interactive mode.

Prerequisites

- Verify that the system BIOS mode is set to Legacy BIOS.
- See NSX Edge network requirements in NSX Edge Installation Requirements.

Procedure

1. Go to your MyVMware account (myvmware.com) and navigate to **VMware NSX-T Data Center > Downloads**.
2. Locate and download the ISO file for NSX Edge for Bare Metal.
3. Log in to the ILO of the bare metal.
4. Click **Launch** in the virtual console preview.
5. Select **Virtual Media > Connect Virtual Media**.

   Wait a few seconds for the virtual media to connect.
6. Select **Virtual Media > Map CD/DVD** and browse to the ISO file.
7. Select **Next Boot > Virtual CD/DVD/ISO**.
8. Select **Power > Reset System (warm boot)**.

   The installation duration depends on the bare metal environment.
9. Choose **Interactive Install**.

   There might be a pause of 10 seconds after you press Enter.
10. In the Configure the keyboard window, select `Yes` if the installer must auto-detect the keyboard or select `No` if the keyboard must not be detected by the console.
11. Select English US as the language.
12. In the Configure the network window, select the applicable primary network interface.
13. Enter the host name that connects to the selected primary interface and click `Ok`.

    During power-on, the installer requests a network configuration via DHCP. If DHCP is not available in your environment, the installer prompts you for IP settings.

    By default, the root login password is **vmware**, and the admin login password is **default**.
14. In the Configure NSX appliance using kickstart window:
    - Enter the URL of the NSX kickstart config file if you want to automate NSX configuration on the bare metal server.
    - Leave the field blank if you want to manually configure NSX on the bare metal server.
15. In the Partition disks window, choose one of the following options:
    - Select `Yes` if you want to unmount existing partitions so that new partitions can be created on disks.
    - Select `No` if you want to use existing partitions.
16. After the NSX Edge node VM starts, log in to the CLI with admin credentials.

    Note After NSX Edge node VM starts, if you do not log in with admin credentials for the first time, the data plane service does not automatically start on the NSX Edge node VM.

17 Run the `get interface eth0` (without VLAN) or `get interface eth0.<vlan_ID>` (with a VLAN) command to verify that the IP address was applied as expected.

```
nsx-edge-1> get interface eth0.100

Interface: eth0.100
  Address: 192.168.110.37/24
  MAC address: 00:50:56:86:62:4d
  MTU: 1500
  Default gateway: 192.168.110.1
  Broadcast address: 192.168.110.255
  ...
```

Note When bringing up NSX Edge VMs on non-NSX managed host, verify that the MTU setting is set to 1600 (instead of 1500) on the physical host switch for the data NIC.

18 Troubleshoot connectivity problems.

Note If connectivity is not established, make sure the VM network adapter is in the proper network or VLAN.

By default, the NSX Edge node VM datapath claims all virtual machine NICs except the management NIC (the one that has an IP address and a default route). If you incorrectly assigned a NIC as the management interface, follow these steps to use DHCP to assign management IP address to the correct NIC.

a Log in CLI and type the **`stop service dataplane`** command.

b Type the **`set interface`** ***`interface`*** **`dhcp plane mgmt`** command.

c Place *interface* into the DHCP network and wait for an IP address to be assigned to that *interface*.

d Type the **`start service dataplane`** command.

The datapath fp-ethX ports used for the VLAN uplink and the tunnel overlay are shown in the **get interfaces** and **get physical-port** commands on the NSX Edge node VM.

What to do next

If you did not join the NSX Edge with the management plane, see Join NSX Edge with the Management Plane.

Intel QAT Support for IPSec VPN Bulk Cryptography

Beginning with the NSX-T Data Center 3.0 release, support for the Intel QuickAssist Technology (QAT) is provided on bare metal servers. Intel QAT provides the hardware acceleration for various cryptography operations.

The QAT feature is enabled by default if the NSX Edge is deployed on a bare metal server with an Intel QuickAssist PCIe card that is based on the installed C62x chipset (Intel QuickAssist Adapter 8960 or 8970). The single root I/O virtualization (SR-IOV) interface must be enabled in the BIOS firmware.

To check the status of the QAT feature, enter the following command on the NSX Edge bare metal server CLI.

```
get dataplane qat
```

The possible responses you might receive are listed in the following table.

Status of QAT Feature	Definition
`QAT present, enabled, running`	The QAT feature is enabled and running.
`QAT present, enabled, not running`	The QAT feature has been enabled, but the dataplane service must be restarted for the status change to take effect.
`QAT present, disabled, not running`	The QAT feature is disabled.
`QAT present, disabled, running`	The QAT feature has been disabled, but the dataplane service must be restarted for the status change to take effect.
`QAT not present`	The bare metal server on which you ran the CLI command does not have a QAT device installed.
`QAT not supported in VM`	You ran the CLI command on a VM edge.

To disable or enable the use of an installed QAT device, use the following CLI commands. The expected responses are also shown.

```
set dataplane qat disabled
QAT disabled. Please restart service dataplane to take effect.
```

```
set dataplane qat enabled
QAT enabled. Please restart service dataplane to take effect.
```

Important You must enter the `restart service dataplane` command at the CLI prompt for the QAT feature status change to take effect.

Join NSX Edge with the Management Plane

Joining NSX Edges with the management plane ensures that the NSX Manager and NSX Edges can communicate with each other.

Prerequisites

Verify that you have admin privileges to log in to the NSX Edges and NSX Manager appliance.

Procedure

1 Open an SSH session or console session to one of the NSX Manager appliances.

2 Open an SSH session or console session to the NSX Edge node VM.

3 On the NSX Manager appliance, run the `get certificate api thumbprint` command.

The command output is a string of alphanumeric numbers that is unique to this NSX Manager.

For example:

```
NSX-Manager1> get certificate api thumbprint
659442c1435350edbbc0e87ed5a6980d892b9118f851c17a13ec76a8b985f57
```

4. On the NSX Edge node VM, run the **join management-plane** command.

   Provide the following information:

   - Hostname or IP address of the NSX Manager with an optional port number
   - User name of the NSX Manager
   - Certificate thumbprint of the NSX Manager
   - Password of the NSX Manager

   ```
   NSX-Edge1> join management-plane <Manager-IP> thumbprint <Manager-thumbprint> username admin
   ```

   Repeat this command on each NSX Edge node VM.

5. Verify the result by running the `get managers` command on your NSX Edge node VMs.

   ```
   nsx-edge-1> get managers
   - 10.173.161.17  Connected (NSX-RPC)
   - 10.173.161.140 Connected (NSX-RPC)
   - 10.173.160.204 Connected (NSX-RPC)
   ```

6. In the NSX Manager UI, navigate to **System > Fabric > Nodes > Edge Transport Nodes**.

   On the NSX Edge Transport Node page:

   - The **Configuration State** column displays `Configure NSX`. Click `Configure NSX` to begin configuration on the node. If the **NSX Version** column does not display the version number installed on the node, try refreshing the browser window.
   - Before you configure NSX on the NSX Edge node, the **Node Status** and **Tunnel Status** columns display state `Not Available`. The **Transport Zones** and **N-VDS** switches columns display value `0`, indicating there are no transport zones attached or N-VDS switches configured on the NSX Edge node.

What to do next

When installing NSX Edge using NSX Manager see Create an NSX Edge Transport Node.

When installing NSX Edge manually, see Configure an NSX Edge as a Transport Node.

Configure an NSX Edge as a Transport Node

After manually installing NSX Edge on ESXi or Bare Metal, configure an NSX Edge to the NSX-T Data Center fabric as a transport node.

A transport node is a node that is capable of participating in an NSX-T Data Center overlay or NSX-T Data Center VLAN networking. Any node can serve as a transport node if it contains an N-VDS. Such nodes include but are not limited to NSX Edges.

An NSX Edge can belong to one overlay transport zone and multiple VLAN transport zones. If a VM requires access to the outside world, the NSX Edge must belong to the same transport zone that the VM's logical switch belongs to. Generally, the NSX Edge belongs to at least one VLAN transport zone to provide the uplink access.

Prerequisites

- Transport zones must be configured.
- Verify that compute manager is configured. See Add a Compute Manager.
- An uplink profile must be configured or you can use the default uplink profile for bare-metal NSX Edge nodes.
- An IP pool must be configured or must be available in the network deployment.
- At least one unused physical NIC must be available on the host or NSX Edge node.

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Select **System > Fabric > Nodes > Edge Transport Nodes > Edit Edge**.
3. Select the Edge node and click **Edit**.
4. Enter the N-VDS information.

Option	Description
Edge Switch Name	Select a VLAN switch from the drop-down menu.
Transport Zone	Select the transport zones that this transport node belongs to. An NSX Edge transport node belongs to at least two transport zones, an overlay for NSX-T Data Center connectivity and a VLAN for uplink connectivity. **Note** Multiple VTEPs in a transport zone must be configured to the same network segment. If VTEPs in a transport zone are configured to different network segments, BFD sessions cannot be established between the VTEPs.
Uplink Profile	Select the uplink profile from the drop-down menu. The available uplinks depend on the configuration in the selected uplink profile.

Option	Description
IP Assignment	Select **Use IP Pool** or **Use Static IP List** for the overlay N-VDS. These IP addresses are assigned as VTEPs to the NSX Edge transport node. Multiple VTEPs on an NSX Edge must be in the same subnet. ■ If you select **Use Static IP List**, you must specify a list of comma-separated IP addresses, a gateway, and a subnet mask. ■ If you selected **Use IP Pool** for IP assignment, specify the IP pool name.
DPDK Fastpath Interfaces / Virtual NICs	Select the data path interface name for the uplink interface. **Note** To ensure that traffic flows through logical switches configured with named teaming policies, map all uplinks in the default teaming policy to physical network interfaces on the NSX Edge VM.

5 View the connection status on the **Transport Nodes** page.

After adding the NSX Edge as a transport node, the connection status changes to Up in 10-12 minutes.

6 (Optional) View the transport node with the `GET https://<nsx-manager>/api/v1/transport-nodes/<transport-node-id>` API call.

7 (Optional) For status information, use the `GET https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/status` API call.

8 If you see inaccurate resource configuration details, such as compute, datastore, or network details that were configured when you installed NSX Edge node, refresh the configuration details by running the API command.

```
POST api/v1/transport-nodes/<transport-node-id>?
ction=refresh_node_configuration&resource_type=EdgeNode
```

NSX Manager displays inaccurate or stale NSX Edge node details if one of these conditions are true:

- On the NSX Edge node, if you change settings such as SSH, NTP, DNS and so from the NSX Edge command line interface.
- If the NSX Edge VM appliance is moved to another host using vCenter, the NSX Manager may have stale values of compute, datastore, and network configuration based on the configuration of the new host.

What to do next

Add the NSX Edge node to an NSX Edge cluster. See Create an NSX Edge Cluster.

Transport Zones and Transport Nodes

10

Transport zones and transport nodes are important concepts in NSX-T Data Center.

This chapter includes the following topics:

- Create Transport Zones
- Create an IP Pool for Tunnel Endpoint IP Addresses
- Enhanced Data Path
- Configuring Profiles
- Create a Standalone Host or Bare Metal Server Transport Node
- Manual Installation of NSX-T Data Center Kernel Modules
- Deploy a Fully Collapsed vSphere Cluster NSX-T
- VLAN Micro-Segmentation

Create Transport Zones

Transport zones dictate which hosts and, therefore, which VMs can participate in the use of a particular network. A transport zone does this by limiting the hosts that can "see" a logical switch—and, therefore, which VMs can be attached to the logical switch. A transport zone can span one or more host clusters.

An NSX-T Data Center environment can contain one or more transport zones based on your requirements. A host can belong to multiple transport zones. A logical switch can belong to only one transport zone.

NSX-T Data Center does not allow connection of VMs that are in different transport zones in the Layer 2 network. The span of a logical switch is limited to a transport zone, so virtual machines in different transport zones cannot be on the same Layer 2 network.

The overlay transport zone is used by both host transport nodes and NSX Edges. When a host is added to an overlay transport zone, you can configure an N-VDS or a VDS switch on the host. When an NSX Edge transport node is added to an overlay transport zone, you can only configure an N-VDS switch.

The VLAN transport zone is used by the NSX Edge and host transport nodes for its VLAN uplinks. When an NSX Edge is added to a VLAN transport zone, a VLAN N-VDS is installed on the NSX Edge.

Procedure

1 From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.

2 Select **System > Fabric > Transport Zones > Add**.

3 Enter a name for the transport zone and optionally a description.

4 Select a traffic type between **Overlay** and **VLAN**.

5 Enter one or more uplink teaming policy names. These named teaming policies can be used by logical switches attached to the transport zone. If the logical switches do not find a matching named teaming policy, then the default uplink teaming policy is used.

6 After you add the transport zone, go to the **Transport Zones** page and view the newly added transport zone.

7 (Optional) You can also view the new transport zone with the `GET https://<nsx-mgr>/api/v1/transport-zones` API call.

```
{
  "cursor": "00369b661aed-1eaa-4567-9408-ccbcfe50b416tz-vlan",
  "result_count": 2,
  "results": [
    {
      "resource_type": "TransportZone",
      "description": "comp overlay transport zone",
      "id": "efd7f38f-c5da-437d-af03-ac598f82a9ec",
      "display_name": "tz-overlay",
      "host_switch_name": "overlay-hostswitch",
      "transport_type": "OVERLAY",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ],
      "_create_time": 1459547126454,
      "_last_modified_user": "admin",
      "_system_owned": false,
      "_last_modified_time": 1459547126454,
      "_create_user": "admin",
      "_revision": 0,
      "_schema": "/v1/schema/TransportZone"
    },
    {
      "resource_type": "TransportZone",
      "description": "comp vlan transport zone",
      "id": "9b661aed-1eaa-4567-9408-ccbcfe50b416",
      "display_name": "tz-vlan",
      "host_switch_name": "vlan-uplink-hostwitch",
      "transport_type": "VLAN",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ],
      "_create_time": 1459547126505,
      "_last_modified_user": "admin",
      "_system_owned": false,
      "_last_modified_time": 1459547126505,
      "_create_user": "admin",
      "_revision": 0,
      "_schema": "/v1/schema/TransportZone"
    }
  ]
}
```

What to do next

Optionally, create a custom transport-zone profile and bind it to the transport zone. You can create custom transport-zone profiles using the `POST /api/v1/transportzone-profiles` API. There is no UI workflow for creating a transport-zone profile. After the transport-zone profile is created, you can find it to the transport zone with the `PUT /api/v1/transport-zones/<transport-zone-id>` API.

Create a transport node. See Create a Standalone Host or Bare Metal Server Transport Node.

Create an IP Pool for Tunnel Endpoint IP Addresses

You can use an IP pool for the tunnel endpoints. Tunnel endpoints are the source and destination IP addresses used in the external IP header to identify the hypervisor hosts originating and end the NSX-T Data Center encapsulation of overlay frames. You can also use either DHCP or manually configured IP pools for tunnel endpoint IP addresses.

If you are using both ESXi and KVM hosts, one design option might be to use two different subnets for the ESXi tunnel endpoint IP pool (sub_a) and the KVM tunnel endpoint IP Pool (sub_b). In this case, on the KVM hosts a static route to sub_a must be added with a dedicated default gateway.

An example of the resulting routing table on an Ubuntu host where sub_a = 192.168.140.0 and sub_b = 192.168.150.0. (The management subnet, for example, might be 192.168.130.0).

Kernel IP routing table:

```
Destination          Gateway          Genmask          Iface
0.0.0.0              192.168.130.1    0.0.0.0          eth0
192.168.122.0        0.0.0.0          255.255.255.0    virbr0
192.168.130.0        0.0.0.0          255.255.255.0    eth0
192.168.140.0        192.168.150.1    255.255.255.0    nsx-vtep0.0
192.168.150.0        0.0.0.0          255.255.255.0    nsx-vtep0.0
```

The route can be added in at least two different ways. Of these two methods, the route persists after host reboot only if you add the route by editing the interface. Adding a route using the route add command does not persist after a host reboot.

```
route add -net 192.168.140.0 netmask 255.255.255.0 gw 192.168.150.1 dev nsx-vtep0.0
```

In /etc/network/interfaces before "up ifconfig nsx-vtep0.0 up" add this static route:

```
post-up route add -net 192.168.140.0 netmask 255.255.255.0 gw 192.168.150.1
```

Procedure

1 From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.

2 Select **Networking** → **IP Address Pools** → **Add IP Address Pool**.

3 Enter the IP pool details.

Option	Parameter Example
Name and Description	Enter the IP pool and optional description.
IP Ranges	IP allocation ranges 192.168.200.100 - 192.168.200.115
Gateway	192.168.200.1
CIDR	Network address in a CIDR notation 192.168.200.0/24
DNS Servers	Comma-separated list of DNS servers 192.168.66.10
DNS Suffix	corp.local

Results

The IPv4 or IPv6 address pool is listed on the IP pool page.

You can also use the `GET https://<nsx-mgr>/api/v1/pools/ip-pools` API call to view the IP pool list.

What to do next

Create an uplink profile. See Create an Uplink Profile.

Enhanced Data Path

Enhanced data path is a networking stack mode, which when configured provides superior network performance. It is primarily targeted for NFV workloads, which offer performance benefits leverging DPDK capability.

The N-VDS switch can be configured in the enhanced data path mode only on an ESXi host. ENS also supports traffic flowing through Edge VMs.

In the enhanced data path mode, both traffic modes are supported:

- Overlay traffic
- VLAN traffic

Supported VMkernel NICs

With NSX-T Data Center supporting multiple ENS host switches, the maximum number of VMkernel NICs supported per host is 32.

High-Level Process to Configure Enhanced Data Path

As a network administrator, before creating transport zones supporting N-VDS in the enhanced data path mode, you must prepare the network with the supported NIC cards and drivers. To improve network performance, you can enable the Load Balanced Source teaming policy to become NUMA node aware.

The high-level steps are as follows:

1. Use NIC cards that support the enhanced data path.

   See VMware Compatibility Guide to know NIC cards that support enhanced data path.

   On the VMware Compatibility Guide page, under the **IO devices** category, select **ESXi 6.7**, IO device Type as **Network**, and feature as **N-VDS Enhanced Datapath**.

2. Download and install the latest NIC drivers from the My VMware page.

   a. Go to **Drivers & Tools** > **Driver CDs**.

   b. Download NIC drivers:

      ```
      VMware ESXi 6.7 ixgben-ens 1.1.3 NIC Driver for Intel Ethernet Controllers
      82599, x520, x540, x550, and x552 family
      ```

      ```
      VMware ESXi 6.7 i40en-ens 1.1.3 NIC Driver for Intel Ethernet Controllers
      X710, XL710, XXV710, and X722 family
      ```

   c. To use the host as an ENS host, at least one ENS capable NIC must be available on the system. If there are no ENS capable NICs, the management plane will not allow hosts to be added to ENS transport zones.

   d. List the ENS driver.

      ```
      esxcli software vib list | grep -E "i40|ixgben"
      ```

   e. Verify whether the NIC is capable to process ENS datapath traffic.

      ```
      esxcfg-nics -e
      ```

      ```
      Name    Driver   ENS Capable   ENS Driven    MAC Address       Description
      vmnic0  ixgben   True          False         e4:43:4b:7b:d2:e0 Intel(R) Ethernet Controller
      X550
      vmnic1  ixgben   True          False         e4:43:4b:7b:d2:e1 Intel(R) Ethernet Controller
      X550
      vmnic2  ixgben   True          False         e4:43:4b:7b:d2:e2 Intel(R) Ethernet Controller
      ```

```
X550
vmnic3  ixgben   True          False        e4:43:4b:7b:d2:e3 Intel(R) Ethernet Controller
X550
vmnic4  i40en    True          False        3c:fd:fe:7c:47:40 Intel(R) Ethernet Controller
X710/X557-AT 10GBASE-T
vmnic5  i40en    True          False        3c:fd:fe:7c:47:41 Intel(R) Ethernet Controller
X710/X557-AT 10GBASE-T
vmnic6  i40en    True          False        3c:fd:fe:7c:47:42 Intel(R) Ethernet Controller
X710/X557-AT 10GBASE-T
vmnic7  i40en    True          False        3c:fd:fe:7c:47:43 Intel(R) Ethernet Controller
X710/X557-AT 10GBASE-T
```

f Install the ENS driver.

```
esxcli software vib install -v file:///<DriverInstallerURL> --no-sig-check
```

g Alternately, download the driver to the system and install it.

```
wget <DriverInstallerURL>
```

```
esxcli software vib install -v file:///<DriverInstallerURL> --no-sig-check
```

h Reboot the host to load the driver. Proceed to the next step.

i To unload the driver, follow these steps:

```
vmkload_mod -u i40en
```

```
ps | grep vmkdevmgr
```

```
kill -HUP "$(ps | grep vmkdevmgr | awk {'print $1'})"
```

```
ps | grep vmkdevmgr
```

```
kill -HUP <vmkdevmgrProcessID>
```

```
kill -HUP "$(ps | grep vmkdevmgr | awk {'print $1'})"
```

j To uninstall the ENS driver, `esxcli software vib remove --vibname=i40en-ens --force --no-live-install`.

3 Create an uplink policy.

See Create an Uplink Profile.

4 Create a transport zone.

See Create Transport Zones.

Note ENS transport zones configured for overlay traffic: For a Microsoft Windows virtual machine running VMware tools version earlier to version 11.0.0 and vNIC type is `VMXNET3`, ensure MTU is set to 1500. For a Microsoft Windows virtual machine running vSphere 6.7 U1 and VMware tools version 11.0.0 and later, ensure MTU is set to a value less than 8900. For virtual machines running other supported OSes, ensure that the virtual machine MTU is set to a value less than 8900.

5 Create a host transport node. Configure mode in Enhanced Datapath on an N-VDS or VDS switch with logical cores and NUMA nodes.

See Create a Standalone Host or Bare Metal Server Transport Node.

Load Balanced Source Teaming Policy Mode Aware of NUMA

The Load Balanced Source teaming policy mode defined for an enhanced datapath N-VDS becomes aware of NUMA when the following conditions are met:

- The **Latency Sensitivity** on VMs is **High**.
- The network adapter type used is VMXNET3.

If the NUMA node location of either the VM or the physical NIC is not available, then the Load Balanced Source teaming policy does not consider NUMA awareness to align VMs and NICs.

The teaming policy functions without NUMA awareness in the following conditions:

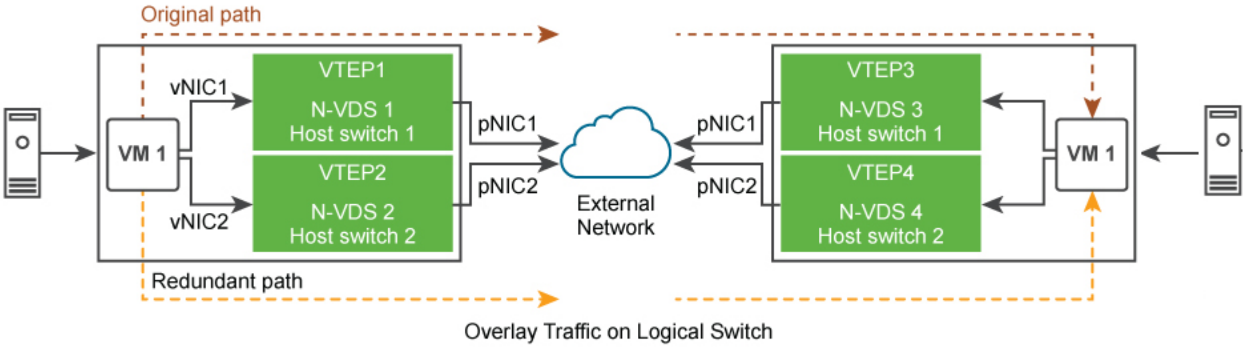
- The LAG uplink is configured with physical links from multiple NUMA nodes.
- The VM has affinity to multiple NUMA nodes.
- The ESXi host failed to define NUMA information for either VM or physical links.

ENS Support for Applications Requiring Traffic Reliability

NFV workloads might use multi-homing and redundancy features provided by Stream Control Transmission Protocol (SCTP) to increase resiliency and reliability to the traffic running on applications. Multi-homing is the ability to support redundant paths from a source VM to a destination VM.

Depending upon the number of physical NICs available to be used as an uplink for an overlay or a VLAN network, those many redundant network paths are available for a VM to send traffic over to the target VM. The redundant paths are used when the pinned pNIC to a logical switch fails. The enhanced data path switch provides redundant network paths between the hosts.

Figure 10-1. Multi-homing and Redundancy of Traffic over ENS



The high-level tasks are:

1 Prepare host as an NSX-T Data Center transport node.

2 Prepare VLAN or Overlay Transport Zone with two N-VDS switches in Enhanced Data Path mode.

3 On N-VDS 1, pin the first physical NIC to the switch.

4 On N-VDS 2, pin the second physical NIC to the switch.

The N-VDS in enhanced data path mode ensures that if pNIC1 becomes unavailable, then traffic from VM 1 is routed through the redundant path - vNIC 1 → tunnel endpoint 2 → pNIC 2 → VM 2.

Configuring Profiles

Profiles allow you to consistently configure identical capabilities for network adapters across multiple hosts or nodes.

Profiles are containers for the properties or capabilities that you want your network adapters to have. Instead of configuring individual properties or capabilities for each network adapter, you can specify the capabilities in the profiles, which you can then apply across multiple hosts or nodes.

Create an Uplink Profile

An uplink is a link from the NSX Edge nodes to the top-of-rack switches or NSX-T Data Center logical switches. A link is from a physical network interface on an NSX Edge node to a switch.

An uplink profile defines policies for the uplinks. The settings defined by uplink profiles can include teaming policies, active and standby links, transport VLAN ID, and MTU setting.

Configuring uplinks for VM appliance-based NSX Edge nodes and Host Transport nodes:

- If the Failover teaming policy is configured for an uplink profile, then you can only configure a single active uplink in the teaming policy. Standby uplinks are not supported and must not be configured in the failover teaming policy. When you install NSX Edge as a virtual appliance or host transport node, use the default uplink profile.
- If the Load Balanced Source teaming policy is configured for an uplink profile, then you can configure multiple active uplinks on the same N-VDS. Each uplink is associated with one physical NIC with a distinct name and IP address. The IP address assigned to an uplink endpoint is configurable using IP Assignment for the N-VDS.

You must use the **Load Balanced Source** teaming policy for traffic load balancing.

Prerequisites

- See NSX Edge network requirements in NSX Edge Installation Requirements.
- Each uplink in the uplink profile must correspond to an up and available physical link on your hypervisor host or on the NSX Edge node.

  For example, your hypervisor host has two physical links that are up: vmnic0 and vmnic1. Suppose vmnic0 is used for management and storage networks, while vmnic1 is unused. This might mean that vmnic1 can be used as an NSX-T Data Center uplink, but vmnic0 cannot. To do link teaming, you must have two unused physical links available, such as vmnic1 and vmnic2.

  For an NSX Edge, tunnel endpoint and VLAN uplinks can use the same physical link. For example, vmnic0/eth0/em0 might be used for your management network and vmnic1/eth1/em1 might be used for your fp-ethX links.

Procedure

1 From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.

2 Select **System > Fabric > Profiles > Uplink Profiles > Add**.

3 Complete the uplink profile details.

Option	Description
Name and Description	Enter an uplink profile name. Add an optional uplink profile description.
LAGs	(Optional) In the LAGs section, click **Add** for Link aggregation groups (LAGs) using Link Aggregation Control Protocol (LACP) for the transport network. **Note** For LACP, multiple LAG is not supported on KVM hosts. The active and standby uplink names you create can be any text to represent physical links. These uplink names are referenced later when you create transport nodes. The transport node UI/API allows you to specify which physical link corresponds to each named uplink. Possible LAG hashing mechanism options: ■ Source MAC address ■ Destination MAC address ■ Source and destination MAC address ■ Source and destination IP address and VLAN ■ Source and destination MAC address, IP address, and TCP/UDP port
Teamings	In the Teaming section, you can either enter a default teaming policy or you can choose to enter a named teaming policy. Click **Add** to add a naming teaming policy. A teaming policy defines how N-VDS uses its uplink for redundancy and traffic load balancing. You can configure a teaming policy in the following modes: ■ **Failover Order**: An active uplink is specified along with an optional list of standby uplinks. If the active uplink fails, the next uplink in the standby list replaces the active uplink. No actual load balancing is performed with this option. ■ **Load Balance Source**: A list of active uplinks is specified, and each interface on the transport node is pinned to one active uplink. This configuration allows use of several active uplinks at the same time. **Note** ■ On KVM hosts: Only Failover Order teaming policy is supported, whereas Load Balance Source and Load Balance Source MAC teaming policies are not supported. ■ On NSX Edge: For default teaming policy, Load Balance Source and Failover Order teaming policies are supported. For named teaming policy, only Failover Order policy is supported. ■ On ESXi hosts: Load Balance Source MAC, Load Balance Source, and Failover Order teaming policies are supported. (ESXi hosts and NSX Edge) You can define the following policies for a transport zone: ■ A Named teaming policy for every VLAN-based logical switch or segment. ■ A Default teaming policy for the entire N-VDS.

Option	Description
	Named teaming policy: A named teaming policy means that for every VLAN-based logical switch or segment, you can define a specific teaming policy mode and uplinks names. This policy type gives you the flexibility to select specific uplinks depending on the traffic steering policy, for example, based on bandwidth requirement. ■ If you define a named teaming policy, N-VDS uses that named teaming policy if it is attached to the VLAN-based transport zone and finally selected for specific VLAN-based logical switch or segment in the host. ■ If you do not define any named teaming policies, N-VDS uses the default teaming policy.

4 Enter a Transport VLAN value. The transport VLAN set in the uplink profile tags overlay traffic only and the VLAN ID is used by the TEP endpoint.

5 Enter the MTU value.

The uplink profile MTU default value is 1600.

The global physical uplink MTU configures the MTU value for all the N-VDS instances in the NSX-T Data Center domain. If the global physical uplink MTU value is not specified, the MTU value is inferred from the uplink profile MTU if configured or the default 1600 is used. The uplink profile MTU value can override the global physical uplink MTU value on a specific host.

The global logical interface MTU configures the MTU value for all the logical router interfaces. If the global logical interface MTU value is not specified, the MTU value is inferred from the tier-0 logical router. The logical router uplink MTU value can override on a specific port the global logical interface MTU value.

Results

In addition to the UI, you can also view the uplink profiles with the API call `GET /api/v1/host-switch-profiles`.

What to do next

Create a transport zone. See Create Transport Zones.

Configuring Network I/O Control Profiles

Use the Network I/O Control (NIOC) profile to allocate the network bandwidth to business-critical applications and to resolve situations where several types of traffic compete for common resources.

NIOC profile introduces a mechanism to reserve bandwidth for the system traffic based on the capacity of the physical adapters on a host. Version 3 of the Network I/O Control feature offers improved network resource reservation and allocation across the entire switch.

Network I/O Control version 3 for NSX-T Data Center supports the resource management of the system traffic related to virtual machines and to infrastructure services, such as vSphere Fault Tolerance. System traffic is strictly associated with an ESXi host.

Note NIOC profiles cannot be applied to NSX Edge transport nodes.

Bandwidth Guarantee to System Traffic

Network I/O Control version 3 provisions bandwidth to the network adapters of virtual machines by using constructs of shares, reservation, and limit. These constructs can be defined in the NSX-T Data Center Manager UI. The bandwidth reservation for virtual machine traffic is also used in the admission control. When you power on a virtual machine, admission control utility verifies that enough bandwidth is available before placing a VM on a host that can provide the resource capacity.

Bandwidth Allocation for System Traffic

You can configure Network I/O Control to allocate a certain amount of bandwidth for traffic generated by vSphere Fault Tolerance, vSphere vMotion, virtual machines, and so on.

- Management Traffic: is traffic for a host management
- Fault Tolerance (FT) traffic: is traffic for failover and recovery.
- NFS Traffic: is traffic related to a file transfer in the network file system.
- vSAN Traffic: is traffic generated by virtual storage area network.
- vMotion Traffic: is traffic for computing resource migration.
- vSphere Replication Traffic: is traffic for replication.
- vSphere Data Protection Backup Traffic: is traffic generated by backup of data.
- Virtual machine Traffic: is traffic generated by virtual machines.
- iSCSI Traffic: is traffic for Internet Small Computer System Interface.

vCenter Server propagates the allocation from the distributed switch to each physical adapter on the hosts that are connected to the switch.

Bandwidth Allocation Parameters for System Traffic

By using several configuration parameters, the Network I/O Control service allocates the bandwidth to traffic from basic vSphere system features. Allocation Parameters for System Traffic.

Allocation Parameters for System Traffic

- Shares: Shares, from 1 to 100, reflect the relative priority of a system traffic type against the other system traffic types that are active on the same physical adapter. The relative shares assigned to a system traffic type and the amount of data transmitted by other system features determine the available bandwidth for that system traffic type.

- Reservation: The minimum bandwidth, in Mbps, that must be guaranteed on a single physical adapter. The total bandwidth reserved among all system traffic types cannot exceed 75 percent of the bandwidth that the physical network adapter with the lowest capacity can provide. Reserved bandwidth that is unused becomes available to other types of system traffic. However, Network I/O Control does not redistribute the capacity that system traffic does not use to virtual machine placement.
- Limit: The maximum bandwidth, in Mbps or Gbps, that a system traffic type can consume on a single physical adapter.

Note You can reserve no more than 75 percent of the bandwidth of a physical network adapter.

For example, if the network adapters connected to an ESXi host are 10 GbE, you can only allocate 7.5 Gbps bandwidth to the various traffic types. You might leave more capacity unreserved. The host can allocate the unreserved bandwidth dynamically according to shares, limits, and use. The host reserves only the bandwidth that is enough for the operation of a system feature.

Configure Network I/O Control and Bandwidth Allocation for System Traffic on an N-VDS

To guarantee the minimum bandwidth to the system traffic running on NSX-T Data Center hosts, enable and configure a network resource management on an N-VDS.

Procedure

1 From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.

2 Select **System > Fabric > Profiles > NIOC Profiles > Add**.

3 Enter the NIOC profile details.

Option	Description
Name and Description	Enter a NIOC profile name. You can optionally enter the profile details such as, the traffic types enabled.
Status	Toggle to enable the bandwidth allocations listed in the traffic resources.
Host Infra Traffic Resource	You can accept the default listed traffic resources. Click **Add** and enter your traffic resource to customize the NIOC profile. (Optional) Select an existing traffic type and click **Delete** to remove the resource from the NIOC profile.

The new NIOC profile is added to the NIOC profiles list.

Configure Network I/O Control and Bandwidth Allocation for System Traffic on an N-VDS Using APIs

You can use NSX-T Data Center APIs to configure the network and bandwidth for applications running on the host.

Procedure

1 Query the host to display both system-defined and user-defined host switch profiles.

2 GET `https://<nsx-mgr>/api/v1/host-switch-profiles?include_system_owned=true`.

The sample response displays the NIOC profile that is applied to the host.

```
{
  "description": "This profile is created for Network I/O Control (NIOC).",
  "extends": {
  "$ref": "BaseHostSwitchProfile"+
  },
  "id": "NiocProfile",
  "module_id": "NiocProfile",
  "polymorphic-type-descriptor": {
  "type-identifier": "NiocProfile"
  },
  "properties": {
  "_create_time": {
  "$ref": "EpochMsTimestamp"+,
  "can_sort": true,
  "description": "Timestamp of resource creation",
  "readonly": true
    },
  "_create_user": {
  "description": "ID of the user who created this resource",
  "readonly": true,
  "type": "string"
    },
  "_last_modified_time": {
  "$ref": "EpochMsTimestamp"+,
  "can_sort": true,
  "description": "Timestamp of last modification",
  "readonly": true
    },

  "_last_modified_user": {
  "description": "ID of the user who last modified this resource",
  "readonly": true,
  "type": "string"
    },

  "_links": {
  "description": "The server will populate this field when returning the resource. Ignored on PUT
and POST.",
  "items": {
  "$ref": "ResourceLink"+
    },

  "readonly": true,
  "title": "References related to this resource",
  "type": "array"
    },
  "_protection": {
  "description": "Protection status is one of the following:
     PROTECTED - the client who retrieved the entity is not allowed to modify it.
     NOT_PROTECTED - the client who retrieved the entity is allowed to modify it
     REQUIRE_OVERRIDE - the client who retrieved the entity is a super user and can modify it,
     but only when providing the request header X-Allow-Overwrite=true.
     UNKNOWN - the _protection field could not be determined for this entity.",
  "readonly": true,
  "title": "Indicates protection status of this resource",
  "type": "string"
    },

  "_revision": {
  "description": "The _revision property describes the current revision of the resource.
    To prevent clients from overwriting each other's changes, PUT operations must include the
             current _revision of the resource,
    which clients should obtain by issuing a GET operation.
                If the _revision provided in a PUT request is missing or stale, the operation
will be rejected.",
  "readonly": true,
  "title": "Generation of this resource config",
  "type": "int"
    },

  "_schema": {
  "readonly": true,
  "title": "Schema for this resource",
  "type": "string"
    },

  "_self": {
  "$ref": "SelfResourceLink"+,
  "readonly": true,
  "title": "Link to this resource"
    },

  "_system_owned": {
  "description": "Indicates system owned resource",
  "readonly": true,
  "type": "boolean"
    },

  "description": {
  "can_sort": true,
  "maxLength": 1024,
  "title": "Description of this resource",
  "type": "string"
    },

  "display_name": {
  "can_sort": true,
  "description": "Defaults to ID if not set",
  "maxLength": 255,
  "title": "Identifier to use when displaying entity in logs or GUI",
  "type": "string"
    },
  "enabled": {
  "default": true,
  "description": "The enabled property specifies the status of NIOC feature.

  When enabled is set to true, NIOC feature is turned on and the bandwidth allocations
     specified for the traffic resources are enforced.
  When enabled is set to false, NIOC feature is turned off and no bandwidth allocation is
guaranteed.

  By default, enabled will be set to true.",

  "nsx_feature": "Nioc",
  "required": false,
  "title": "Enabled status of NIOC feature",
  "type": "boolean"
    },

  "host_infra_traffic_res": {
  "description": "host_infra_traffic_res specifies bandwidth allocation for various traffic
resources.",
  "items": {
  "$ref": "ResourceAllocation"+
    },
  "nsx_feature": "Nioc",
  "required": false,
  "title": "Resource allocation associated with NiocProfile",
  "type": "array"
    },

  "id": {
  "can_sort": true,
  "readonly": true,
  "title": "Unique identifier of this resource",
  "type": "string"
    },

  "required_capabilities": {
  "help_summary":
                            "List of capabilities required on the fabric node if this profile is
used.
          The required capabilities is determined by whether specific features are enabled in the
profile.",
  "items": {
  "type": "string"
    },
  "readonly": true,
  "required": false,
  "type": "array"
    },

  "resource_type": {
  "$ref": "HostSwitchProfileType"+,
  "required": true
    },
  "tags": {
  "items": {
  "$ref": "Tag"+
      },

  "maxItems": 30,
  "title": "Opaque identifiers meaningful to the API user",
  "type": "array"
    }
  },
  "title": "Profile for Nioc",
  "type": "object"
  }
```

3 If a NIOC profile does not exist, create a NIOC profile.

POST `https://<nsx-mgr>/api/v1/host-switch-profiles`

```
{
  "description": "Specify limit, shares and reservation for all kinds of traffic.
   Values for limit and reservation are expressed in percentage. And for shares,
   the value is expressed as a number between 1-100.\nThe overall reservation among all traffic
types should not exceed 75%.
   Otherwise, the API request will be rejected.",

  "id": "ResourceAllocation",
  "module_id": "NiocProfile",
  "nsx_feature": "Nioc",
  "properties": {
    "limit": {
      "default": -1.0,
      "description": "The limit property specifies the maximum bandwidth allocation for a given
      traffic type and is expressed in percentage. The default value for this
      field is set to -1 which means the traffic is unbounded for the traffic
      type. All other negative values for this property is not supported\nand will be rejected by
the API.",
      "maximum": 100,
      "minimum": -1,
      "required": true,
      "title": "Maximum bandwidth percentage",
      "type": "number"
    },

    "reservation": {
      "default": 0.0,
      "maximum": 75,
      "minimum": 0,
      "required": true,
      "title": "Minimum guaranteed bandwidth percentage",
      "type": "number"
    },

    "shares": {
      "default": 50,
      "maximum": 100,
      "minimum": 1,
      "required": true,
      "title": "Shares",
      "type": "int"
    },

    "traffic_type": {
      "$ref": "HostInfraTrafficType"+,
      "required": true,
      "title": "Resource allocation traffic type"
    }

  },

  "title": "Resource allocation information for a host infrastructure traffic type",
  "type": "object"
```

4 Update the transport node configuration with the NIOC profile ID of the newly created NIOC profile.

PUT `https://<nsx-mgr>/api/v1/transport-nodes/<TN-id>`

```
{
    "resource_type": "TransportNode",
    "description": "Updated NSX configured Test Transport Node",
    "id": "77816de2-39c3-436c-b891-54d31f580961",
    "display_name": "NSX Configured TN",
    "host_switch_spec": {
      "resource_type": "StandardHostSwitchSpec",
      "host_switches": [
        {
        "host_switch_profile_ids": [
          {
            "value": "e331116d-f59e-4004-8cfd-c577aefe563a",
            "key": "UplinkHostSwitchProfile"
          },
        {
       "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
       "key": "LldpHostSwitchProfile"
        }
       {
        "value": "b0185099-8003-4678-b86f-edd47ca2c9ad",
        "key": "NiocProfile"
       }
        ],
       "host_switch_name": "nsxvswitch",
       "pnics": [
      {
       "device_name": "vmnic1",
       "uplink_name": "uplink1"
      }
      ],
      "ip_assignment_spec": {
      "resource_type": "StaticIpPoolSpec",
      "ip_pool_id": "ecddcdde-4dc5-4026-ad4f-8857995d4c92"
      }
```

```
     }
    ]
  },
   "transport_zone_endpoints": [
    {
    "transport_zone_id": "e14c6b8a-9edd-489f-b624-f9ef12afbd8f",
    "transport_zone_profile_ids": [
      {
        "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
        "resource_type": "BfdHealthMonitoringProfile"
      }
    ]
    }
  ],

   "host_switches": [
    {
      "host_switch_profile_ids": [
        {
        "value": "e331116d-f59e-4004-8cfd-c577aefe563a",
        "key": "UplinkHostSwitchProfile"
       },
        {
        "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
        "key": "LldpHostSwitchProfile"
        }
      ],

      "host_switch_name": "nsxvswitch",
      "pnics": [
      {
        "device_name": "vmnic1",
        "uplink_name": "uplink1"
        }
      ],
      "static_ip_pool_id": "ecddcdde-4dc5-4026-ad4f-8857995d4c92"
    }
  ],
  "node_id": "41a4eebd-d6b9-11e6-b722-875041b9955d",
  "_revision": 0
}
```

5 Verify that the NIOC profile parameters are updated in the `com.vmware.common.respools.cfg` file.

# [root@ host:] `net-dvs -l`

```

         switch 1d 73 f5 58 99 7a 46 6a-9c cc d0 93 17 bb 2a 48 (vswitch)
max ports: 2560
global properties:

com.vmware.common.opaqueDvs = true ,     propType = CONFIG
com.vmware.nsx.kcp.enable = true ,     propType = CONFIG
com.vmware.common.alias = nsxvswitch ,     propType = CONFIG
com.vmware.common.uplinkPorts: uplink1   propType = CONFIG
```

```
   com.vmware.common.portset.mtu = 1600, propType = CONFIG
   com.vmware.etherswitch.cdp = LLDP, listen  propType = CONFIG
   com.vmware.common.respools.version = version3,   propType = CONFIG
   com.vmware.common.respools.cfg:
   netsched.pools.persist.ft:0:50:-1:255
   netsched.pools.persist.hbr:0:50:-1:255
   netsched.pools.persist.vmotion:0:50:-1:255
   netsched.pools.persist.vm:0:100:-1:255
   netsched.pools.persist.iscsi:0:50:-1:255
   netsched.pools.persist.nfs:0:50:-1:255
   netsched.pools.persist.mgmt:0:50:-1:255
   netsched.pools.persist.vdp:0:50:-1:255
   netsched.pools.persist.vsan:0:50:-1:255
   propType = CONFIG
```

6 Verify NIOC profiles in the host kernel.

   # [root@ host:] `/get /net/portsets/DvsPortset-1/ports/50335755/niocVnicInfo`

```
Vnic NIOC Info
                    {
      Uplink reserved on:vmnic4
      Reservation in Mbps:200
      Shares:50
      Limit in Mbps:4294967295
      World ID:1001400726
      vNIC Index:0
      Respool Tag:0
      NIOC Version:3
      Active Uplink Bit Map:15
      Parent Respool ID:netsched.pools.persist.vm
     }
```

7 Verify the NIOC profile information.

   # [root@ host:] `/get /net/portsets/DvsPortset-1/uplinks/vmnic4/niocInfo`

```
Uplink NIOC Info
            {
    Uplink device:vmnic4
    Link Capacity in Mbps:750
    vm respool reservation:275
    link status:1
    NetSched Ready:1
    Infrastructure reservation:0
    Total VM reservation:200
    Total vnics on this uplink:1
    NIOC Version:3
    Uplink index in BitMap:0
   }
```

Results

NIOC profile is configured with a pre-defined bandwidth allocation for applications running on NSX-T Data Center hosts.

Add an NSX Edge Cluster Profile

The NSX Edge cluster profile defines the policies for the NSX Edge transport node.

Prerequisites

Verify that the NSX Edge cluster is available.

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Select **System > Fabric > Profiles > Edge Cluster Profiles > Add**.
3. Enter the NSX Edge cluster profile details.

Option	Description
Name and Description	Enter a NSX Edge cluster profile name. You can optionally enter the profile details such as, the Bidirectional Forwarding Detection (BFD) setting.
BFD Probe Interval	Accept the default setting. BFD is detection protocol used to identify the forwarding path failures. You can set the interval timing for BFD to detect a forwarding path failure.
BFD Allowed Hops	Accept the default setting. You can set the number of multihop BFD sessions allowed for the profile.
BFD Declare Dead Multiple	Accept the default setting. You can set the number of number of times the BFD packet is not received before the session is flagged as down.
Stand By Relocation Threshold	Accept the default setting.

Add an NSX Edge Bridge Profile

The NSX Edge bridge profile defines the policies for the ESXi bridge cluster.

A bridge cluster is a collection of ESXi host transport nodes.

Prerequisites

- Verify that the NSX Edge cluster is available.
- Verify that the ESXi bridge cluster is available.

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Select **Networking** → **Segments** → **Edge Bridge Profiles** → **Add Edge Bridge Profile**.
3. Enter the NSX Edge cluster profile details.

Option	Description
Name and Description	Enter a NSX Edge bridge cluster profile name. You can optionally enter the profile details such as, the primary and backup node details.
Edge Cluster	Select the NSX Edge cluster that you can to use.
Primary Node	Designate the preferred NSX Edge node from the cluster.
Backup Node	Designate the back up NSX Edge node if the primary node fails.
Failover Mode	Select either **Preemptive** or **Non-Preemptive** mode. The default HA mode is preemptive, which can slowdown traffic when the preferred NSX Edge node goes back online. The non-preemptive mode does not cause any traffic slowdown.

Add a Transport Node Profile

A transport node profile is a template to define configuration that is applied to a cluster. It is not applied to prepare standalone hosts. Prepare vCenter Server cluster hosts as transport nodes by applying a transport node profile. Transport node profiles define transport zones, member hosts, N-VDS switch configuration including uplink profile, IP assignment, mapping of physical NICs to uplink virtual interfaces and so on.

Note Transport node profiles are only applicable to hosts. It cannot be applied to NSX Edge transport nodes.

Transport node creation begins when a transport node profile is applied to a vCenter Server cluster. NSX Manager prepares the hosts in the cluster and installs the NSX-T Data Center components on all the hosts. Transport nodes for the hosts are created based on the configuration specified in the transport node profile.

On a cluster prepared with a transport node profile, these outcomes are true:

- When you move an unprepared host into a cluster applied with a transport node profile, NSX-T Data Center automatically prepares the host as a transport node using the transport node profile.
- When you move a transport node from the cluster to an unprepared cluster or directly as a standalone host under the data center, first the transport node configuration applied to the node is removed and then NSX-T Data Center VIBs are removed from the host. See Triggering Uninstallation from the vSphere Web Client.

To delete a transport node profile, you must first detach the profile from the associated cluster. The existing transport nodes are not affected. New hosts added to the cluster are no longer automatically converted into transport nodes.

Points to note when you create a Transport Node Profile:

- You can add a maximum of four N-VDS or VDS switches for each configuration: enhanced N-VDS or VDS created for VLAN transport zone, standard N-VDS or VDS created for overlay transport zone, enhanced N-VDS or VDS created for overlay transport zone.
- There is no limit on the number of standard N-VDS switches created for VLAN transport zone.
- In a single host cluster topology running multiple standard overlay N-VDS switches and edge VM on the same host, NSX-T Data Center provides traffic isolation such that traffic going through the first N-VDS is isolated from traffic going through the second N-VDS and so on. The physical NICs on each N-VDS must be mapped to the edge VM on the host to allow the north-south traffic connectivity with the external world. Packets moving out of a VM on the first transport zone must be routed through an external router or an external VM to the VM on the second transport zone.
- Each N-VDS switch name must be unique. NSX-T Data Center does not allow use of duplicate switch names.
- Each transport zone ID associated with each N-VDS or VDS host in a transport node configuraiton or transport node profile configuration must be unique.

Prerequisites

- Verify that the hosts are part of a vCenter Server cluster.
- vCenter Server must have at least one cluster.
- Verify that a transport zone is configured. See Create Transport Zones.
- Verify that a cluster is available. See Deploy NSX Manager Nodes to Form a Cluster from UI.
- Verify that an IP pool is configured, or DHCP must be available in the network deployment. See Create an IP Pool for Tunnel Endpoint IP Addresses.
- Verify that a compute manager is configured. See Add a Compute Manager.

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Select **System > Fabric > Profiles > Transport Node Profiles > Add**.
3. Enter a name to identify the transport node profile.

   You can optionally add the description about the transport node profile.
4. In the **Add Transport Node Profile** panel, expand **New Node Switch**.
5. In the Type field, select between **N-VDS** and **VDS** as the host switch type to prepare the transport node.

6 In the **Mode** field, depending upon the workload requirements, select the appropriate mode:

- **Standard** mode that applies to all the supported hosts. It is used for regular workloads.
- **Enhanced Datapath** is a networking stack mode that applies to only transport nodes of ESXi host version 6.7 and later type that can belong in a transport zone. It is used for telecom workloads that require relatively higher throughput and performance.

7 Select the available transport zones and click the **>** button to include the transport zones in the transport node profile.

Note You can add multiple transport zones.

8 Select **N-VDS** as the host switch type and enter the switch details. Skip to the next step to select **VDS** as the host switch.

Option	Description
Name	Enter a name for the N-VDS switch.
Transport Zones	Shows the transport zones that are realized by the associated host switches. You cannot add a transport zone if it is not realized by any N-VDS in the transport node profile.
NIOC Profile	Select the NIOC profile from the drop-down menu. The bandwidth allocations specified in the profile for the traffic resources are enforced.
Uplink Profile	Select an existing uplink profile from the drop-down menu or create a custom uplink profile. You can also use the default uplink profile.
LLDP Profile	By default, NSX-T only receives LLDP packets from a LLDP neighbor. However, NSX-T can be set to send LLDP packets to and receive LLDP packets from a LLDP neighbor.
IP Assignment	Select **Use DHCP**, **Use IP Pool**, or **Use Static IP List** to assign an IP address to virtual tunnel endpoints (VTEPs) of the transport node. If you select **Use Static IP List**, you must specify a list of comma-separated IP addresses, a gateway, and a subnet mask. All the VTEPs of the transport node must be in the same subnet otherwise bidirectional flow (BFD) session is not established.
IP Pool	If you selected **Use IP Pool** for an IP assignment, specify the IP pool name.

Option	Description
Physical NICs	Add physical NICs to the transport node. You can use the default uplink or assign an existing uplink from the drop-down menu. Click **Add PNIC** to configure additional physical NICs to the transport node. **Note** Migration of the physical NICs that you add in this field depends on how you configure **PNIC only Migration**, **Network Mappings for Install**, and **Network Mappings for Uninstall**. ■ To migrate a used physical NIC (for example, by a vSphere Standard Switch or a vSphere Distributed Switch) without an associated VMkernel mapping, ensure that **PNIC only Migration** is enabled. Otherwise, the transport node state remains in **partial success**, and the fabric node LCP connectivity fails to establish. ■ To migrate a used physical NIC with an associated VMkernel network mapping, disable **PNIC only Migration** and configure the VMkernel network mapping. ■ To migrate a free physical NIC, enable **PNIC only Migration**.
PNIC only Migration	Before setting this field, consider the following points: ■ Know whether the physical NIC defined is a used NIC or a free NIC. ■ Determine whether VMkernel interfaces of a host need to be migrated along with physical NICs. Set the field: ■ Enable **PNIC only Migration** if you only want to migrate physical NICs from a VSS or DVS switch to an N-VDS switch. ■ Disable **PNIC only Migration** if you want to migrate a used physical NIC and its associated VMkernel interface mapping. A free or available physical NIC is attached to the N-VDS switch when a VMkernel interface migration mapping is specified. On a host with multiple host switches: ■ If all host switches are to migrate only PNICs, then you can migrate the PNICs in a single operation. ■ If some hosts switches are to migrate VMkernel interfaces and the remaining host switches are to migrate only PNICs: 1 In the first operation, migrate only PNICs. 2 In the second operation, migrate VMkernel interfaces. Ensure that **PNIC only Migration** is disabled. Both PNIC only migration and VMkernel interface migration are not supported at the same time across multiple hosts. **Note** To migrate a management network NIC, configure its associated VMkernel network mapping and keep **PNIC only Migration** disabled. If you only migrate the management NIC, the host loses connectivity. For more information, see VMkernel Migration to an N-VDS Switch.

Option	Description
Network Mappings for Install	To migrate VMkernels to N-VDS switch during installation, map VMkernels to an existing logical switch. The NSX Manager migrates the VMkernel to the mapped logical switch on N-VDS. **Caution** Ensure that the management NIC and management VMkernel interface are migrated to a logical switch that is connected to the same VLAN that the management NIC was connected to before migration. If vmnic<*n*> and VMkernel<*n*> are migrated to a different VLAN, then connectivity to the host is lost. **Caution** For pinned physical NICs, ensure that the host switch mapping of physical NIC to a VMkernel interface matches the configuration specified in the transport node profile. As part of the validation procedure, NSX-T Data Center verifies the mapping and if the validation passes migration of VMkernel interfaces to an N-VDS switch is successful. It is also mandatory to configure the network mapping for uninstallation because NSX-T Data Center does not store the mapping configuration of the host switch after migrating the VMkernel interfaces to the N-VDS switch. If the mapping is not configured, connectivity to services, such as vSAN, can be lost after migrating back to the VSS or VDS switch. For more information, see VMkernel Migration to an N-VDS Switch.
Network Mappings for Uninstall	To revert the migration of VMkernels attached to an N-VDS switch during uninstallation, map VMkernels to port groups on VSS or DVS, so that NSX Manager knows which port group the VMkernel must be migrated back to on the VSS or DVS. For a DVS switch, ensure that the port group is of the type `Ephemeral`. To revert the migration of VMkernels attached to a NSX-T port group created on a vSphere Distributed Switch (VDS) during uninstallation, map VMkernels to port groups on VSS or DVS, so that NSX Manager knows which port group the VMkernel must be migrated back to on the VSS or DVS. For a DVS switch, ensure that the port group is of the type `Ephemeral`. **Caution** For pinned physical NICs, ensure that the transport node profile mapping of physical NIC to VMkernel interface matches the configuration specified in the host switch. It is mandatory to configure the network mapping for uninstallation because NSX-T Data Center does not store the mapping configuration of the host switch after migrating the VMkernel interfaces to the N-VDS switch. If the mapping is not configured, connectivity to services, such as vSAN, can be lost after migrating back to the VSS or VDS switch. For more information, see VMkernel Migration to an N-VDS Switch.

9 Select **VDS** as the host switch type and enter the switch details.

Option	Description
Name	(Hosts managed by a vSphere cluster) Select the vCenter Server that manages the host switch. Select the VDS that is created in vCenter Server.
Transport Zones	Shows the transport zones that are realized by the associated host switches. You cannot add a transport zone if it is not realized by any host switch.

Option	Description
Uplink Profile	Select an existing uplink profile from the drop-down menu or create a custom uplink profile. **Note** Ensure MTU value entered in the NSX-T Data Center uplink profile and VDS switch is set to at least 1600. If the MTU value in vCenter Server for the VDS switch is lower than the MTU value entered in the uplink profile, then NSX-T Data Center displays an error asking you to enter an appropriate MTU value in the vCenter Server. You can also use the default uplink profile. **Note** Link Aggregation Groups defined in an uplink profile cannot be mapped to VDS uplinks.
IP Assignment	Select **Use DHCP**, **Use IP Pool**, or **Use Static IP List** to assign an IP address to virtual tunnel endpoints (VTEPs) of the transport node. If you select **Use Static IP List**, you must specify a list of comma-separated IP addresses, a gateway, and a subnet mask. All the VTEPs of the transport node must be in the same subnet otherwise bidirectional flow (BFD) session is not established.
IP Pool	If you selected **Use IP Pool** for an IP assignment, specify the IP pool name.
Teaming Policy Switch Mapping	Map the uplinks defined in the NSX-T uplink profile with the VDS switch uplinks. Alternatively, NSX-T uplinks can also be mapped to LAGs configured on the VDS switch. To configure or view the VDS switch uplinks, go to vCenter Server → *vSphere Distributed Switch*. Click **Actions** → **Settings** → **Edit Settings**.

Note For a VDS switch, Uplinks/LAGs, NIOC profile, LLDP profile can be defined only in vSphere ESXi host. These configurations are not available in NSX Manager. In addition, in NSX Manager, you cannot configure networking mapping for install and uninstall if the host switch is a VDS switch. To manage VMkernel adapters on a VDS switch, go to vCenter Server to attach VMkernel adapters to Distributed Virtual port groups or NSX port groups.

10 If you have selected multiple transport zones, click **ADD SWITCH** again to configure the switch for the other transport zones.

11 Click **Finish** to complete the configuration.

What to do next

Apply the transport node profile to an existing vSphere cluster. See Configure a Managed Host Transport Node.

VMkernel Migration to an N-VDS Switch

To migrate VMkernel interfaces from a VSS or DVS switch to an N-VDS switch at a cluster-level, configure the transport node profile with network-mapping details required for migration (map VMkernel interfaces to logical switches). Similarly, to migrate VMkernel interfaces on a host node, configure the transport node configuration. To revert migrate VMkernel interfaces back to a VSS or DVS switch, configure uninstall network-mapping (map logical ports to VMkernel interface) in the transport node profile to be realized during uninstallation.

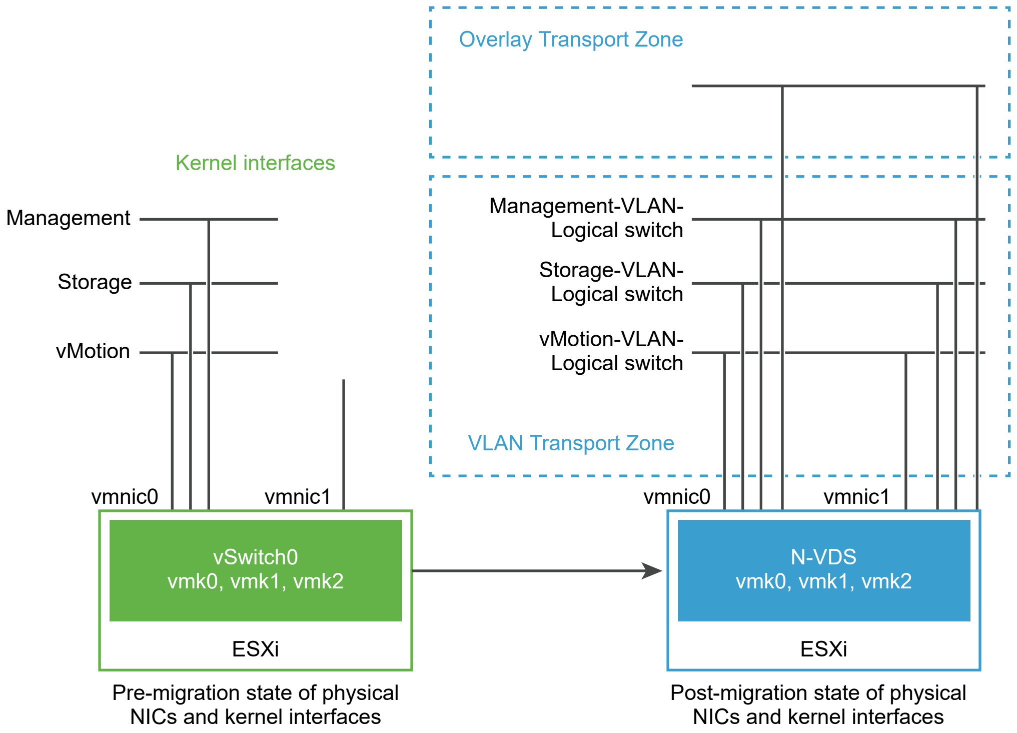
During migration physical NICs currently in use are migrated to an N-VDS switch, while available or free physical NICs are attached to the N-VDS switch after migration.

Note Transport node profiles are applied to all member hosts of a cluster. But if you want to limit migration of VMkernel interfaces on specific hosts, you can directly configure the host. After migration, N-VDS handles traffic on the VLAN and overlay network for those interfaces attached to the N-VDS switch.

Important Configurations done to individual hosts are marked with the `Overridden` flag. Any further updates to the transport node profile are not applied to these overridden hosts. These hosts remain in overridden state until NSX-T Data Center is uninstalled.

In the following figure, if a host has only two physical NICs, you might want to assign both those NICs to the N-VDS for redundancy and their associated VMkernel interfaces so that the interfaces do not lose connectivity with the host.

Figure 10-2. Pre and Post Migration of Network Interfaces to an N-VDS


Overlay Transport Zone
Kernel interfaces
Management
Storage
vMotion
Management-VLAN-Logical switch
Storage-VLAN-Logical switch
vMotion-VLAN-Logical switch
VLAN Transport Zone
vmnic0
vmnic1
vmnic0
vmnic1
vSwitch0
vmk0, vmk1, vmk2
ESXi
N-VDS
vmk0, vmk1, vmk2
ESXi
Pre-migration state of physical NICs and kernel interfaces
Post-migration state of physical NICs and kernel interfaces

Before migration, the ESXi host has two uplinks derived from the two physical ports - vmnic0 and vmnic1. Here, vmnic0 is configured to be in an active state, attached to a VSS, whereas vmnic1 is unused. In addition, there are three VMkernel interfaces: vmk0, vmk1, and vmk2.

You can migrate VMkernel interfaces by using the NSX-T Data Center Manager UI or NSX-T Data Center APIs. See *NSX-T Data Center API Guide*.

Post migration, the vmnic0, vmnic1, and their VMkernel interfaces are migrated to the N-VDS switch. Both vmnic0 and vmnic1 are connected over VLAN and overlay transport zones.

Considerations for VMkernel Migration

- PNIC and VMkernel migration: Before you migrate pinned physical NICs and associated VMkernel interfaces to an N-VDS switch, make a note of the network-mapping (physical NICs to port group mapping) on the host switch.
- PNIC only migration: If you plan to only migrate PNICs, ensure that the management physical NIC connected to the management VMkernel interface is not migrated. It results in loss of connectivity with the host. For more details, see the **PNIC only Migration** field in Add a Transport Node Profile.
- Revert migration: Before you plan to revert migrate VMkernel interfaces to the VSS or DVS host switch for pinned physical NICs, ensure that you make a note of the network-mapping (physical NIC to port group mapping) on the host switch. It is mandatory to configure the transport node profile with the host switch mapping in the **Network Mapping for Uninstallation** field. Without this mapping, NSX-T Data Center does not know which port groups must the VMkernel interfaces be migrated back to. This situation can lead to loss of connectivity to the vSAN network.
- vCenter Server registration before migration: If you plan to migrate a VMkernel or PNIC connected to a DVS switch, ensure that a vCenter Server is registered with the NSX Manager.
- Match VLAN ID: After migration, the management NIC and management VMkernel interface must be on the same VLAN the management NIC was connected to before migration. If vmnic0 and vmk0 are connected to the management network and migrated to a different VLAN, then connectivity to the host is lost.
- Migration to VSS switch: Cannot migrate back two VMkernel interfaces to the same port group of a VSS witch.
- vMotion: Perform vMotion to move VM workloads to another host before VMkernel and/or PNIC migration. If migration fails, then workload VMs are not impacted.
- vSAN: If the vSAN traffic is running on the host, place the host in maintenance mode through vCenter Server and move VMs out of the host using vMotion functionality before VMkernel and/or PNIC migration.
- Migration: If a VMkernel is already connected to a target switch, it can still be selected to be migrated into the same switch. This property makes the VMK and/or PNIC migration operation idempotent. It helps when you want to migrate only PNICs into a target switch. As migration always requires at least one VMkernel and a PNIC, you select a VMkernel that is already migrated to a target switch when you migrate only PNICs into a target switch. If no VMkernel needs to be migrated, create a temp VMkernel through a vCenter Server in either the source switch or target switch. Then migrate it together with the PNICs, and delete the temp VMkernel through vCenter Server after the migration is finished.
- MAC sharing: If a VMkernel interface and a PNIC share the same MAC and they are in the same switch, they must be migrated together to the same target switch if they will be both used after migration. Always keep vmk0 and vmnic0 in the same switch.

Check the MACs used by all VMKs and PNICs in the host by running the following commands:

```
esxcfg-vmknic -l
```

```
esxcfg-nics -l
```

- VIF logical ports created after migration: After you migrate VMkernel from a VSS or DVS switch to an N-VDS switch, a logical switch port of the type VIF is created on the NSX Manager. You must not create distributed firewall rules on these VIF logical switch ports.

Migrate VMkernel Interfaces to an N-VDS Switch

The high-level workflow to migrate VMkernel Interfaces to an N-VDS switch:

1. Create a logical switch if needed.
2. Power off VMs on the host from which VMkernel interfaces and PNICs are migrated to an N-VDS switch.
3. Configure a transport node profile with a network mapping that is used to migrate the VMkernel interfaces during the creation of transport nodes. Network mapping means mapping a VMkernel interface to a logical switch.

   For more details, see Add a Transport Node Profile.
4. Verify that the network adapter mappings in vCenter Server reflect a new association of the VMkernel switch with an N-VDS switch. In case of pinned physical NICs, verify the mapping in NSX-T Data Center reflects any VMkernels pinned to a physical NIC in the vCenter Server.
5. In NSX Manager, go to **Networking** → **Segments**. On the **Segments** page, verify that the VMkernel interface is attached to the segment through a newly created logical port.
6. Go to **System** > **Nodes** > **Host Transport Node**. For each transport node, verify the status on the **Node Status** column is Success to confirm that the transport node configuration is successfully validated.
7. On the **Host Transport Node** page, verify the status on the **Configuration State** is Success to confirm that the host is successfully realized with the specified configuration.

After you migrate VMkernel interfaces and PNICs from a VDS to a N-VDS switch using NSX-T UI or transport node API, vCenter Server displays warnings for the VDS. If the host need be connected to the VDS, remove the host out of the VDS. The vCenter Server no longer displays any warning for VDS.

For details on errors that might encounter during migration, see VMkernel Migration Errors

Revert Migration of VMkernel Interfaces to a VSS or DVS Switch

The high-level workflow to revert migration of VMkernel Interfaces from an N-VDS switch to a VSS or DVS switch during NSX-T Data Center uninstallation:

1. On the ESXi host, power off VMs connected to the logical ports that hosts the VMkernel interface after migration.

2 Configure the transport node profile with network mapping that is used to migrate the VMkernel interfaces during the uninstallation process. Network mapping during uninstallation maps the VMkernel interfaces to a port group on VSS or DVS switch on the ESXi host.

   Note Reverting migration of a VMkernel to a port group on a DVS switch, ensure that the port group type is set to `Ephemeral`.

   For more details, see Add a Transport Node Profile.

3 Verify the network adapter mappings in vCenter Server reflect a new association of the VMkernel switch with a port group of VSS or DVS switch.

4 In NSX Manager, go to **Networking** → **Segments**. On the **Segments** page, verify that the segment containing VMkernel interfaces are deleted.

For details on errors that you might encounter during migration, see VMkernel Migration Errors

Update Host Switch Mapping

Important

- Stateful hosts: Add and Update operations are supported. To update an existing mapping, you can add a new VMkernel interface entry to the network-mapping configuration. If you update the network mapping configuration of a VMkernel interface that is already migrated to the N-VDS switch, the updated network mapping is not realized on the host.
- Stateless hosts: Add, Update, and Remove operations are supported. Any changes you make to the network-mapping configuration is realized after the host reboots.

  To update the VMkernel interfaces to a new logical switch, you can edit the transport node profile to apply the network mappings at a cluster level. If you only want the updates to be applied to a single host, configure the transport node using host-level APIs.

Note After you update the transport node configuration for an individual host, then any new updates applied through the transport node profile are not applied to that host. That host state turns to `overriden`.

1 To update all hosts in a cluster, edit the **Network Mapping during Installation** field to update the VMkernel mapping to logical switches.

   For more details, see Add a Transport Node Profile.

2 Save the changes. Changes made to a transport node profile is automatically applied to all the member hosts of the cluster, except on hosts that are marked with the `overridden` state.

3 Similarly, to update an individual host, edit the VMkernel mapping in the transport node configuration.

Note If you update the **Network Mapping during Installation** field with a new VMkernel mapping, then the same VMkernel interface must be added to the **Network Mapping during uninstallation** field.

For details on errors that you might encounter during migration, see VMkernel Migration Errors

Migrate VMkernel Interfaces on a Stateless Cluster

1 Prepare and configure a host as a reference host using transport node APIs.

2 Extract the host profile from the reference host.

3 In the vCenter Server, apply the host profile to the stateless cluster.

4 In NSX-T Data Center, apply the transport node profile to the stateless cluster.

5 Reboot each host of the cluster.

The cluster hosts might take several minutes to realize the updated states.

Migration Failure Scenarios

- If migration fails for some reason, the host attempts to migrate the physical NICs and VMkernel interfaces three times.
- If the migration still continues to fail, the host performs a rollback to the earlier configuration by retaining VMkernel connectivity with the management physical NIC, vmnic0.
- In case the rollback also fails such that the VMkernel configured to the management physical NIC was lost, you must reset the host.

Unsupported Migration Scenarios

The following scenarios are not supported:

- VMkernel interfaces from two different VSS or DVS switches are migrated at the same time.
- On stateful hosts, network mapping is updated to map VMkernel interface to another logical switch. For example, before migration the VMkernel is mapped to Logical Switch 1, and the VMkernel interface is mapped to Logical Switch 2.

VMkernel Migration Errors

You can encounter errors when migrating VMkernel interfaces and physical NICs from a VSS or DVS switch to an N-VDS switch or revert migrating interfaces to a VSS or DVS host switch.

Table 10-1. VMkernel Migration Errors

Error Code	Problem	Cause	Resolution
8224	Unable to find the host switch specified by the transport node configuration.	The host switch ID cannot be found.	■ Ensure that the transport zone is created with the host switch name and then create the transport node. ■ Ensure that a valid host switch is used in the transport node configuration.
8225	VMkernel migration is in progress.	Migration is in progress.	Wait for the migration to complete before performing another action.
8226	VMkernel migration is only supported on a ESXi host.	Migration is only valid for ESXi hosts.	Ensure that the host is a ESXi host before you initiate migration.

Table 10-1. VMkernel Migration Errors (continued)

Error Code	Problem	Cause	Resolution
8227	VMkernel interface is not appended with the host switch name.	On a host with multiple host switches, NSX-T Data Center cannot identify association of each VMkernel interface with its host switch.	If the host has multiple N-VDS host switches, ensure the VMkernel interface is appended with the host switch name of the N-VDS the host is connected to. For example, the network mapping for uninstallation of a host with N-VDS host switch name nsxvswitch1 and VMkernel1 and another N-VDS host switch name nsxvswitch2 and VMkernel2 must be defined as follows: `device_name: VMkernel1@nsxvswitch1`, `destination_network: DPortGroup`.
8228	Host switch used in the `device_name` field not found on the host.	Incorrect host switch name.	Enter the correct host switch name.
8229	Transport node did not specify the transport zone of the logical switch.	Transport zone not added.	Add the transport zone to the transport node configuration.
8230	No physical NIC on the host switch.	There must be at least one physical NIC on the host switch.	Specify at least one physical NIC to an uplink profile and the VMkernel network mapping configuration to a logical switch.
8231	Host switch name does not match.	If the host switch name used in `vmk1@host_switch` does not match the host switch name used by the destination logical switch of the interface.	Ensure that the host switch name specified in the network mapping configuration matches the name used by the logical switch of the interface.
8232	Logical switch not realized on the host.	Realization of logical switch on the host was unsuccessful.	Synchronize the host with the NSX Manager.
8233	Unexpected logical switch in the network interface mapping.	The network interface mapping for installation and uninstallation lists both logical switches and port groups.	Network mapping for installation must only contain logical switches as destination targets. Similarly, network mapping for uninstallation must only contain port groups as destination targets.
8294	Logical switch does not exist in the network interface mapping.	Logical switches not specified.	Ensure that logical switches are specified in the network interface mapping configuration.
8296	Host switch mismatch.	The network interface mapping for uninstallation is configured with the incorrect host switch name.	Ensure that the host switch name used in the mapping configuration matches the name entered on the host switch where the VMkernel interfaces reside on.

Table 10-1. VMkernel Migration Errors (continued)

Error Code	Problem	Cause	Resolution
8297	Duplicate VMkernel.	Duplicate VMkernels are specified for migration.	Ensure that no duplicate VMkernel interfaces are specified in the installation or uninstallation mapping configuration.
8298	Mismatch of number of VMkernel interfaces and destinations.	Incorrect configuration.	Ensure that each VMkernel interface has a corresponding destination specified in the configuration.
8299	Cannot delete transport node as the VMkernel interface is using ports on N-VDS.	VMkernel interfaces are using ports from the N-VDS switch.	Revert the migration of all VMkernel interfaces from the N-VDS switch to a VSS/DVS switch. Then attempt to delete the transport node.
9412	VMkernel cannot be migrated from one N-VDS to another N-VDS.	Unsupported action.	Revert the migration of the VMkernel interface to a VSS or DVS switch. Then, you can migrate the VMkernel interface to another N-VDS switch.
9413	VMkernel interfaces cannot be migrated to a different logical switch.	On stateful hosts, a VMkernel connected to a logical switch cannot be migrated to another logical switch.	Revert the migration of the VMkernel from the logical switch to a VSS/DVS switch. Then, migrate the VMkernel to another logical switch on the N-VDS.
9414	Duplicate VMkernel interfaces.	Duplicate VMkernel interfaces mapped in the installation and uninstallation mapping configuration.	Ensure that each VMkernel interface is unique in the installation and uninstallation mappings.
9415	Powered on VMs on the host.	With powered on VMs, migration does not proceed.	Power off the VMs on the host before you initiate migration of VMkernel interfaces.
9416	VMkernel cannot be found on the host.	Did not specify a VMkernel that exists on the host in the network mapping configuration.	Specify a VMkernel that exists in the network mapping configuration.
9417	Port group not found.	Did not specify a port group that exists on the host in the network mapping configuration.	Specify a port group that exists in the network mapping configuration.
9419	Logical switch not found during migration.	Did not find the logical switch defined in the network interface mapping configuration.	Specify a logical switch that exists in the network interface mapping configuration.
9420	Logical port not found during migration.	During migration, NSX-T Data Center does not find the ports created on the logical switch.	Ensure that no logical ports are deleted from the logical switch for migration to be successful.
9421	Host information missing to validate the migration process.	Unable to retrieve host information from inventory.	Retry the migration process.

Table 10-1. VMkernel Migration Errors (continued)

Error Code	Problem	Cause	Resolution
9423	Pinned physical NICs to a VMkernel interface are not migrated to the correct host switch.	A pinned physical NIC was found in the environment but the VMkernel and physical NIC are not being migrated to the same host switch.	A physical NIC pinned with VMkernel interface must have a transport node configuration that maps the physical NIC with the VMkernel on the same host switch.
600	Object not found.	The specified transport zone used by the logical switch does not exist. The logical switch found in the VMK mapping destination cannot be found.	■ Specify a transport zone which exists in the environment. ■ Create the desired logical switch or use an existing VLAN logical switch.
8310	The logical switch type is incorrect.	The logical switch type is Overlay.	Create a VLAN logical switch.
9424	Cannot migrate if both PNIC only Migration and Network Mapping for install or uninstall settings are configured at the same time.	Migration progresses only when one of these settings is configured.	Ensure that either the PNIC only Migration or Network Mapping for install or uninstall setting is configured.

Create a Standalone Host or Bare Metal Server Transport Node

You must first add your ESXi host, KVM host, or bare metal server to the NSX-T Data Center fabric and then configure the transport node.

For a host or bare metal server to be part of the NSX-T Data Center overlay, it must first be added to the NSX-T Data Center fabric.

A transport node is a node that participates in an NSX-T Data Center overlay or NSX-T Data Center VLAN networking.

For a KVM host or bare metal server, you can preconfigure the N-VDS, or you can have NSX Manager perform the configuration. For a ESXi host, NSX Manager always configures the N-VDS.

Note If you plan to create transport nodes from a template VM, make sure that there are no certificates on the host in `/etc/vmware/nsx/`. nsx-proxy does not create a certificate if a certificate exists.

Bare metal server supports an overlay and VLAN transport zone. You can use the management interface to manage the bare metal server. The application interface allows you to access the applications on the bare metal server.

Single physical NICs provide an IP address for both the management and application IP interfaces.

Dual physical NICs provide a physical NIC and a unique IP address for the management interface. Dual physical NICs also provide a physical NIC, and a unique IP address for the application interface.

Multiple physical NICs in a bonded configuration provide dual physical NICs, and a unique IP address for both the management interface and the application insterface.

You can add a maximum of four N-VDS switches for each configuration:

- standard N-VDS created for VLAN transport zone
- enhanced N-VDS created for VLAN transport zone
- standard N-VDS created for overlay transport zone
- enhanced N-VDS created for overlay transport zone

In a single host cluster topology running multiple standard overlay N-VDS switches and edge VM on the same host, NSX-T Data Center provides traffic isolation such that traffic going through the first N-VDS is isolated from traffic going through the second N-VDS. The physical NICs on each N-VDS must be mapped to the edge VM on the host to allow the north-south traffic connectivity with the external world. Packets moving out of a VM on the first transport zone must be routed through an external router, or an external VM to the VM on the second transport zone.

Prerequisites

- The host must be joined with the management plane, and connectivity must be Up.
- A transport zone must be configured.
- An uplink profile must be configured, or you can use the default uplink profile.
- An IP pool must be configured, or DHCP must be available in the network deployment.
- At least one unused physical NIC must be available on the host node.
- Hostname
- Management IP address
- User name
- Password
- (Optional) (KVM) SHA-256 SSL thumbprint
- (Optional) (ESXi) SHA-256 SSL thumbprint
- Verify that the required third-party packages are installed.
  - See Install Third-Party Packages on a KVM Host.
  - See Install Third-Party Packages on a Bare Metal Server.

Procedure

1 (Optional) Retrieve the hypervisor thumbprint so that you can provide it when adding the host to the fabric.

a Gather the hypervisor thumbprint information.

Use a Linux shell.

```
# echo -n | openssl s_client -connect <esxi-ip-address>:443 2>/dev/null | openssl x509 -noout
-fingerprint -sha256
```

Use the ESXi CLI in the host.

```
[root@host:~] openssl x509 -in /etc/vmware/ssl/rui.crt -fingerprint -sha256 -noout
SHA256
Fingerprint=49:73:F9:A6:0B:EA:51:2A:15:57:90:DE:C0:89:CA:7F:46:8E:30:15:CA:4D:5C:95:28:0A:9E:A
2:4E:3C:C4:F4
```

b Retrieve the SHA-256 thumbprint from a KVM hypervisor, run the command in the KVM host.

```
# awk '{print $2}' /etc/ssh/ssh_host_rsa_key.pub | base64 -d | sha256sum -b | sed 's/ .*$//'
| xxd -r -p | base64
```

2 Select **System > Fabric > Nodes > Host Transport Nodes**.

3 From the Managed by field, select **Standalone Hosts** and click **+ Add**.

4 Enter the standalone host or bare metal server details to add to the fabric.

Option	Description
Name and Description	Enter the name to identify the standalone host or bare metal server. You can optionally add the description of the operating system used for the host or bare metal server.
IP Addresses	Enter the host or bare metal server IP address.
Operating System	Select the operating system from the drop-down menu. Depending on your host or bare metal server, you can select any of the supported operating systems. See System Requirements. **Important** Among the different flavors of Linux supported, you must know the distinction between a bare metal server running a Linux distribution versus using a Linux distribution as a hypervisor host. For example, selecting Ubuntu Server as the operating system means setting up a bare metal server running a Linux server, whereas selcting Ubuntu KVM means the Linux hypervisior deployed is Ubuntu.
Username and Password	Enter the host user name and password.
SHA-256 Thumbprint	Enter the host thumbprint value for authentication. If you leave the thumbprint value empty, you are prompted to accept the server provided value. It takes a few seconds for NSX-T Data Center to discover and authenticate the host.

5 (Required) For a KVM host or bare metal server, select the N-VDS type.

Option	Description
NSX Created	NSX Manager creates the N-VDS. This option is selected by default.
Preconfigured	The N-VDS is already configured.

For an ESXi host, the N-VDS type is always set to **NSX Created**.

6 If you select the N-VDS switch to operate in **Standard (All hosts)** mode, enter value to the following fields. You can configure multiple N-VDS switches on a single host.

Option	Description
Name	Enter a name for the N-VDS host switch.
Transport Zone	From the drop-down menu, select a transport zone that this transport node.
NIOC Profile	From the drop-down menu, select an NIOC profile for the ESXi host or create a custom NIOC profile. You can also select the default NIOC profile.
Uplink Profile	Select an existing uplink profile from the drop-down menu or create a custom uplink profile. You can also use the default uplink profile.
LLDP Profile	By default, NSX-T only receives LLDP packets from a LLDP neighbor. However, NSX-T can be set to send LLDP packets to and receive LLDP packets from a LLDP neighbor.
IP Assignment	Select **Use DHCP**, **Use IP Pool**, or **Use Static IP List**. If you select **Use Static IP List**, you must specify a list of comma-separated IP addresses, a gateway, and a subnet mask.
IP Pool	If you selected **Use IP Pool** for IP assignment, specify the IP pool name.
Teaming Policy Switch Mapping	Add physical NICs to the transport node. You can use the default uplink or assign an existing uplink from the drop-down menu.

Option	Description
PNIC only Migration	Before setting this field, consider the following points: ■ Know whether the physical NIC defined is a used NIC or a free NIC. ■ Determine whether VMkernel interfaces of a host need to be migrated along with physical NICs. Set the field: ■ Enable **PNIC only Migration** if you only want to migrate physical NICs from a VSS or DVS switch to an N-VDS switch. ■ Disable **PNIC only Migration** if you want to migrate a used physical NIC and its associated VMkernel interface mapping. A free or available physical NIC is attached to the N-VDS switch when a VMkernel interface migration mapping is specified. On a host with multiple host switches: ■ If all host switches are to migrate only PNICs, then you can migrate the PNICs in a single operation. ■ If some hosts switches are to migrate VMkernel interfaces and the remaining host switches are to migrate only PNICs: 1 In the first operation, migrate only PNICs. 2 In the second operation, migrate VMkernel interfaces. Ensure that **PNIC only Migration** is disabled. Both PNIC only migration and VMkernel interface migration are not supported at the same time across multiple hosts. **Note** To migrate a management network NIC, configure its associated VMkernel network mapping and keep **PNIC only Migration** disabled. If you only migrate the management NIC, the host loses connectivity. For more information, see VMkernel Migration to an N-VDS Switch.

Option	Description
Network Mappings for Install	To migrate VMkernels to N-VDS switch during installation, map VMkernels to an existing logical switch. The NSX Manager migrates the VMkernel to the mapped logical switch on N-VDS. **Caution** Ensure that the management NIC and management VMkernel interface are migrated to a logical switch that is connected to the same VLAN that the management NIC was connected to before migration. If vmnic<*n*> and VMkernel<*n*> are migrated to a different VLAN, then connectivity to the host is lost. **Caution** For pinned physical NICs, ensure that the host switch mapping of physical NIC to a VMkernel interface matches the configuration specified in the transport node profile. As part of the validation procedure, NSX-T Data Center checks the mapping and if the validation passes migration of VMkernel interfaces to an N-VDS switch is successful. At the same time it is mandatory to configure the network mapping for uninstallation because NSX-T Data Center does not store the mapping configuration of the host switch after migrating the VMkernel interfaces to the N-VDS switch. If the mapping is not configured, connectivity to services, such as vSAN, can be lost after migrating back to the VSS or VDS switch. For more information, see VMkernel Migration to an N-VDS Switch.
Network Mappings for Uninstall	To revert the migration of VMkernels during uninstallation, map VMkernels to port groups on VSS or DVS, so that NSX Manager knows which port group the VMkernel must be migrated back to on the VSS or DVS. For a DVS switch, ensure the port group is of the type `Ephemeral`. To revert the migration of VMkernels attached to a NSX-T port group created on a vSphere Distributed Virtual Switch 7.0 during uninstallation, map VMkernels to port groups on VSS or DVS, so that NSX Manager knows which port group the VMkernel must be migrated back to on the VSS or DVS. For a DVS switch, ensure that the port group is of the type `Ephemeral`. **Caution** For pinned physical NICs, ensure that the transport node profile mapping of physical NIC to VMkernel interface matches the configuration specified in the host switch. It is mandatory to configure the network mapping for uninstallation because NSX-T Data Center does not store the mapping configuration of the host switch after migrating the VMkernel interfaces to the N-VDS switch. If the mapping is not configured, connectivity to services, such as vSAN, can be lost after migrating back to the VSS or VDS switch. For more information, see VMkernel Migration to an N-VDS Switch.

7 If you select the N-VDS switch to operate in **Performance** mode, enter values to the following additional fields. You can configure multiple N-VDS switches on a single host.

Option	Description
(CPU Config) **NUMA Node Index**	In the NUMA Node Index drop-down menu, select the NUMA node that you want to assign to an N-VDS switch. The first NUMA node present on the node is represented with the value 0. You can find out the number for NUMA nodes on your host by running the `esxcli hardware memory get` command. **Note** If you want to change the number of NUMA nodes that have affinity with an N-VDS switch, you can update the NUMA Node Index value.
(CPU Config) **LCores per NUMA Nodes**	In the Lcore per NUMA node drop-down menu, select the number of logical cores that must be used by enhanced datapath. You can find out the maximum number of logical cores that can be created on the NUMA node by running the `esxcli network ens maxLcores get` command. **Note** If you exhaust the available NUMA nodes and logical cores, any new switch added to the transport node cannot be enabled for ENS traffic.

8 For a preconfigured N-VDS, provide the following details.

Option	Description
N-VDS External ID	Must be the same as the N-VDS name of the transport zone that this node belongs to.
VTEP	Virtual tunnel endpoint name.

9 View the connection status on the **Host Transport Nodes** page. During the configuration process, each transport node displays the percentage of progress of the installation process. If installation fails at any stage, you can restart the process by clicking the **Resolve** link that is available against the failed stage of the process.

After adding the host or bare metal server as a transport node, the connection to NSX Manager state displays as `UP` only after the host is successfully created as a transport node.

10 Alternatively, view the connection status using CLI commands.

- For ESXi, enter the `esxcli network ip connection list | grep 1234` command.

```
# esxcli network ip connection list | grep 1234
tcp   0   0  192.168.210.53:20514  192.168.110.34:1234   ESTABLISHED  1000144459  newreno
nsx-cfgagent
```

- For KVM, enter the command `netstat -anp --tcp | grep 1234`.

```
user@host:~$ netstat -anp --tcp | grep 1234
tcp  0   0 192.168.210.54:57794  192.168.110.34:1234   ESTABLISHED -
```

- For Windows, from a command prompt enter `netstat | find "1234"`

- For Windows, from a command prompt enter `netstat | find "1235"`

11 Verify that the NSX-T Data Center modules are installed on your host or bare metal server.

As a result of adding a host or bare metal server to the NSX-T Data Center fabric, a collection of NSX-T Data Center modules are installed on the host or bare metal server.

The modules on different hosts are packaged as follows:

- KVM on RHEL, CentOS, or SUSE - RPMs.
- KVM on Ubuntu - DEBs
- On ESXi, enter the command `esxcli software vib list | grep nsx`.

  The date is the day you performed the installation.
- On RHEL or CentOS, enter the command `yum list installed` or `rpm -qa`.
- On Ubuntu, enter the command `dpkg --get-selections`.
- On SUSE, enter the command `rpm -qa | grep nsx`.
- On Windows, open Task Manager. Or, from the command line enter `tasklist /V | grep nsx findstr “nsx ovs`

12 (Optional) Change the polling intervals of certain processes, if you have 500 hypervisors or more.

The NSX Manager might experience high CPU use and performance problems if there are more than 500 hypervisors.

a Use the NSX-T Data Center CLI command `copy file` or the API `POST /api/v1/node/file-store/<file-name>?action=copy_to_remote_file` to copy the `aggsvc_change_intervals.py` script to a host.

b Run the script, which is located in the NSX-T Data Center file store.

```
python aggsvc_change_intervals.py -m '<NSX ManagerIPAddress>' -u 'admin' -p '<password>' -i
900
```

c (Optional) Change the polling intervals back to their default values.

```
python aggsvc_change_intervals.py -m '<NSX ManagerIPAddress>' -u 'admin' -p '<password>' -r
```

Results

Note For an NSX-T Data Center created N-VDS, after the transport node is created, if you want to change the configuration, such as IP assignment to the tunnel endpoint, you must do it through the NSX Manager GUI and not through the CLI on the host.

What to do next

Migrate network interfaces from a vSphere Standard Switch to an N-VDS switch. See VMkernel Migration to an N-VDS Switch.

Prepare a vSphere Distributed Switch for NSX-T

Before you configure an NSX-T transport node using vSphere Distributed Switch (VDS) as a host switch, ensure that the VDS created on a vCenter Server 7.0 or a later version is configured to manage NSX-T traffic.

High-level tasks to configure a cluster or a standalone managed host using a VDS switch.

Important To create a VDS switch supporting NSX-T networking, the following conditions must be met:

- vCenter Server 7.0 or a later version
- ESXi 7.0 or a later version

Prerequisites

- Verify that ESXi hosts have the required number of physical NICs to meet networking requirements. For example, if you plan to configure teaming policies and remote span port mirroring, ensure that a free physical NIC is available to avoid uplink conflicts.

Procedure

1. In a vCenter Server, create a VDS. For more information about creating a VDS, see the *vSphere Networking* documentation.
   - Set the MTU value for the VDS to at least `1600`.
   - Connect the switch to hosts that you want to prepare for NSX-T networking.
   - Assign physical NICs to uplinks on the VDS.
2. In NSX-T, add an uplink profile that defines a teaming policy mapping NSX-T uplinks with VDS uplinks.
3. In NSX-T, prepare an ESXi host using VDS as the host switch.

   At the end of the configuration, the host is prepared as NSX-T transport node with VDS as the host switch.

What to do next

Configure the host as a transport node. See Configure a Managed Host Transport Node.

Configure a Managed Host Transport Node

If you have a vCenter Server, you can automate the installation and creation of transport nodes on all the NSX-T Data Center hosts instead of configuring manually.

This task is only to prepare individual ESXi nodes as transport nodes. If you want to prepare a cluster so that all hosts in that cluster are prepared as transport nodes, apply the cluster with transport node profile. See Add a Transport Node Profile.

Prerequisites

- Verify that all hosts in the vCenter Server are powered on.
- Verify that the system requirements are met. See System Requirements.
- Verify that a transport zone is available. See Create Transport Zones.
- Verify that a transport node profile is configured. See Add a Transport Node Profile.
- (Host in lockdown mode) If your exception list for vSphere lockdown mode includes expired user accounts, NSX-T Data Center installation on vSphere fails. Ensure that you delete all expired user accounts before you begin installation. For more information on accounts with access privileges in lockdown mode, see *Specifying Accounts with Access Privileges in Lockdown Mode* in the *vSphere Security Guide*.
- With VMware vSphere® vSphere Lifecycle Manager enabled on a cluster, these limitations apply:
  - You cannot prepare an individual host that is part of the cluster as a transport node. Even though a standalone prepared host can be included in the cluster, you must avoid moving such a transport node to the cluster. Because, when an administrator remediates the host, NSX-T VIBs are removed from the transport node. See *vSphereLifecycle Manager Guide*.
  - You cannot apply transport node profile to the cluster to prepare cluster hosts as transport nodes.

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Select **System > Fabric > Nodes > Host Transport Nodes**.
3. From the Managed By drop-down menu, select an existing vCenter Server.

   The page lists the available vSphere clusters and/or ESXi hosts from the selected vCenter Server. You may need to expand a cluster to view the ESXi hosts.
4. Select a single host from the list and click **Configure NSX**.

   The Configure NSX dialog box opens.

   a. Verify the host name in the Host Details panel. Optionally, you can add a description.

   b. Click **Next** to move to the **Configure NSX** panel.

   c. Select the available transport zones and click the **>** button to include the transport zones in the transport node profile.
5. Verify the host name in the Host Details panel, and click **Next**.

   Optionally, you can add a description.
6. In the **Configure NSX** panel, expand **New Node Switch**.
7. In the **Type** field, select between **N-VDS** and **VDS** as the host switch type to prepare the transport node.

8 In the **Mode** field, depending upon the workload requirements, select the appropriate mode:

- **Standard** mode that applies to all the supported hosts. It is used for regular workloads.
- **Enhanced Datapath** is a networking stack mode that applies to only transport nodes of ESXi host version 6.7 and later type that can belong in a transport zone. It is used for telecom workloads that require relatively higher throughput and performance.

9 Select **N-VDS** as the host switch type and enter the switch details. Skip to the next step to select **VDS** as the host switch.

Option	Description
Name	Enter a name for the N-VDS switch.
Transport Zones	Shows the transport zones that are realized by the associated host switches. You cannot add a transport zone if it is not realized by any N-VDS in the transport node profile.
NIOC Profile	Select the NIOC profile from the drop-down menu. The bandwidth allocations specified in the profile for the traffic resources are enforced.
Uplink Profile	Select an existing uplink profile from the drop-down menu or create a custom uplink profile. You can also use the default uplink profile.
LLDP Profile	By default, NSX-T only receives LLDP packets from a LLDP neighbor. However, NSX-T can be set to send LLDP packets to and receive LLDP packets from a LLDP neighbor.
IP Assignment	Select **Use DHCP**, **Use IP Pool**, or **Use Static IP List** to assign an IP address to virtual tunnel endpoints (VTEPs) of the transport node. If you select **Use Static IP List**, you must specify a list of comma-separated IP addresses, a gateway, and a subnet mask. All the VTEPs of the transport node must be in the same subnet otherwise bidirectional flow (BFD) session is not established.
IP Pool	If you selected **Use IP Pool** for an IP assignment, specify the IP pool name.
Physical NICs	Add physical NICs to the transport node. You can use the default uplink or assign an existing uplink from the drop-down menu. Click **Add PNIC** to configure additional physical NICs to the transport node. **Note** Migration of the physical NICs that you add in this field depends on how you configure **PNIC only Migration**, **Network Mappings for Install**, and **Network Mappings for Uninstall**. ■ To migrate a used physical NIC (for example, by a vSphere Standard Switch or a vSphere Distributed Switch) without an associated VMkernel mapping, ensure that **PNIC only Migration** is enabled. Otherwise, the transport node state remains in **partial success**, and the fabric node LCP connectivity fails to establish. ■ To migrate a used physical NIC with an associated VMkernel network mapping, disable **PNIC only Migration** and configure the VMkernel network mapping. ■ To migrate a free physical NIC, enable **PNIC only Migration**.

Option	Description
PNIC only Migration	Before setting this field, consider the following points: ■ Know whether the physical NIC defined is a used NIC or a free NIC. ■ Determine whether VMkernel interfaces of a host need to be migrated along with physical NICs. Set the field: ■ Enable **PNIC only Migration** if you only want to migrate physical NICs from a VSS or DVS switch to an N-VDS switch. ■ Disable **PNIC only Migration** if you want to migrate a used physical NIC and its associated VMkernel interface mapping. A free or available physical NIC is attached to the N-VDS switch when a VMkernel interface migration mapping is specified. On a host with multiple host switches: ■ If all host switches are to migrate only PNICs, then you can migrate the PNICs in a single operation. ■ If some hosts switches are to migrate VMkernel interfaces and the remaining host switches are to migrate only PNICs: 1 In the first operation, migrate only PNICs. 2 In the second operation, migrate VMkernel interfaces. Ensure that **PNIC only Migration** is disabled. Both PNIC only migration and VMkernel interface migration are not supported at the same time across multiple hosts. **Note** To migrate a management network NIC, configure its associated VMkernel network mapping and keep **PNIC only Migration** disabled. If you only migrate the management NIC, the host loses connectivity. For more information, see VMkernel Migration to an N-VDS Switch.

Option	Description
Network Mappings for Install	To migrate VMkernels to N-VDS switch during installation, map VMkernels to an existing logical switch. The NSX Manager migrates the VMkernel to the mapped logical switch on N-VDS. **Caution** Ensure that the management NIC and management VMkernel interface are migrated to a logical switch that is connected to the same VLAN that the management NIC was connected to before migration. If vmnic<*n*> and VMkernel<*n*> are migrated to a different VLAN, then connectivity to the host is lost. **Caution** For pinned physical NICs, ensure that the host switch mapping of physical NIC to a VMkernel interface matches the configuration specified in the transport node profile. As part of the validation procedure, NSX-T Data Center verifies the mapping and if the validation passes migration of VMkernel interfaces to an N-VDS switch is successful. It is also mandatory to configure the network mapping for uninstallation because NSX-T Data Center does not store the mapping configuration of the host switch after migrating the VMkernel interfaces to the N-VDS switch. If the mapping is not configured, connectivity to services, such as vSAN, can be lost after migrating back to the VSS or VDS switch. For more information, see VMkernel Migration to an N-VDS Switch.
Network Mappings for Uninstall	To revert the migration of VMkernels attached to an N-VDS switch during uninstallation, map VMkernels to port groups on VSS or DVS, so that NSX Manager knows which port group the VMkernel must be migrated back to on the VSS or DVS. For a DVS switch, ensure that the port group is of the type `Ephemeral`. To revert the migration of VMkernels attached to a NSX-T port group created on a vSphere Distributed Switch (VDS) during uninstallation, map VMkernels to port groups on VSS or DVS, so that NSX Manager knows which port group the VMkernel must be migrated back to on the VSS or DVS. For a DVS switch, ensure that the port group is of the type `Ephemeral`. **Caution** For pinned physical NICs, ensure that the transport node profile mapping of physical NIC to VMkernel interface matches the configuration specified in the host switch. It is mandatory to configure the network mapping for uninstallation because NSX-T Data Center does not store the mapping configuration of the host switch after migrating the VMkernel interfaces to the N-VDS switch. If the mapping is not configured, connectivity to services, such as vSAN, can be lost after migrating back to the VSS or VDS switch. For more information, see VMkernel Migration to an N-VDS Switch.

10 Select **VDS** as the host switch type and enter the switch details.

Option	Description
Name	(Hosts managed by a vSphere cluster) Select the vCenter Server that manages the host switch. Select the VDS that is created in vCenter Server.
Transport Zones	Shows the transport zones that are realized by the associated host switches. You cannot add a transport zone if it is not realized by any host switch.

Option	Description
Uplink Profile	Select an existing uplink profile from the drop-down menu or create a custom uplink profile. **Note** Ensure MTU value entered in the NSX-T Data Center uplink profile and VDS switch is set to at least 1600. If the MTU value in vCenter Server for the VDS switch is lower than the MTU value entered in the uplink profile, then NSX-T Data Center displays an error asking you to enter an appropriate MTU value in the vCenter Server. You can also use the default uplink profile. **Note** Link Aggregation Groups defined in an uplink profile cannot be mapped to VDS uplinks.
IP Assignment	Select **Use DHCP**, **Use IP Pool**, or **Use Static IP List** to assign an IP address to virtual tunnel endpoints (VTEPs) of the transport node. If you select **Use Static IP List**, you must specify a list of comma-separated IP addresses, a gateway, and a subnet mask. All the VTEPs of the transport node must be in the same subnet otherwise bidirectional flow (BFD) session is not established.
IP Pool	If you selected **Use IP Pool** for an IP assignment, specify the IP pool name.
Teaming Policy Switch Mapping	Map the uplinks defined in the NSX-T uplink profile with the VDS switch uplinks. Alternatively, NSX-T uplinks can also be mapped to LAGs configured on the VDS switch. To configure or view the VDS switch uplinks, go to vCenter Server → *vSphere Distributed Switch*. Click **Actions** → **Settings** → **Edit Settings**.

Note For a VDS switch, Uplinks/LAGs, NIOC profile, LLDP profile can be defined only in vSphere ESXi host. These configurations are not available in NSX Manager. In addition, in NSX Manager, you cannot configure networking mapping for install and uninstall if the host switch is a VDS switch. To manage VMkernel adapters on a VDS switch, go to vCenter Server to attach VMkernel adapters to Distributed Virtual port groups or NSX port groups.

11 If you have selected multiple transport zones, click **ADD SWITCH** again to configure the switch for the other transport zones.

12 Click **Finish** to complete the configuration.

13 (Optional) View the ESXi connection status.

```
# esxcli network ip connection list | grep 1235
tcp   0   0  192.168.210.53:20514  192.168.110.34:1234   ESTABLISHED  1000144459  newreno  nsx-
proxy
```

14 From the Host Transport Node page, verify that the NSX Manager connectivity status of hosts in the cluster is Up and NSX-T Data Center configuration state is Success. During the configuration process, each transport node displays the percentage of progress of the installation process. If installation fails at any stage, you can restart the process by clicking the **Resolve** link that is available against the failed stage of the process.

   You can also see that the transport zone is applied to the hosts in the cluster.

   Note If you again configure a host that is part of a cluster that is already prepared by a transport node profile, the configuration state of a node is in `Configuration Mismatch` state.

15 (Optional) Remove an NSX-T Data Center VIBs on the host.

   a Select one or more hosts and click **Actions > Remove NSX**.

   The uninstallation takes up to three minutes. Uninstallation of NSX-T Data Center removes the transport node configuration on hosts and the host is detached from the transport zone(s) and N-VDS switch. Similar to the installation process, you can follow the percentage of the uninstallation process completed on each transport node. If uninstallation fails at any stage, you can restart the process by clicking the **Resolve** link that is available against the failed stage of the process.

16 (Optional) Remove a transport node from the transport zone.

   a Select a single transport node and click **Actions > Remove from Transport Zone**.

What to do next

When the hosts are transport nodes, you can create transport zones, logical switches, logical routers, and other network components through the NSX Manager UI or API at any time. When NSX Edge nodes and hosts join the management plane, the NSX-T Data Center logical entities and configuration state are pushed to the NSX Edge nodes and hosts automatically. You can create transport zones, logical switches, logical routers, and other network components through the NSX Manager UI or API at any time. When the hosts are transport nodes, these entities gets realized on the host.

Create a logical switch and assign logical ports. See the Advanced Switching section in the *NSX-T Data Center Administration Guide*.

Configure an ESXi Host Transport Node with Link Aggregation

This procedure describes how to create an uplink profile that has a link aggregation group configured, and how to configure an ESXi host transport node to use that uplink profile.

Prerequisites

- Familiarize yourself with the steps to create an uplink profile. See Create an Uplink Profile.
- Familiarize yourself with the steps to create a host transport node. See Create a Standalone Host or Bare Metal Server Transport Node.

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Select **System > Fabric > Profiles > Uplink Profiles > Add**.
3. Enter a name and optionally a description.

   For example, you enter the name `uplink-profile1`.
4. Under **LAGs**, click **Add** to add a link aggregation group.

   For example, you add an LAG called `lag1` with 2 uplinks.
5. Under **Teamings**, select **Default Teaming**.
6. In the **Active Uplinks** field, enter the name of the LAG that you added in the step 4. In this example, the name is `lag1`.
7. Enter a value for the **Transport VLAN** and **MTU**.
8. Click **Add** at the bottom of the dialog box.
9. Under **Teamings**, click **Add** to add an entry for link aggregation.
10. Select **Fabric > Nodes > Host Transport Nodes > Add**.
11. In the **Host Details** tab, enter IP address, OS name, admin credentials, and SHA-256 thumbprint of the host.
12. In the **N-VDS** tab, select the uplink profile `uplink-profile1` that was created in step 3.
13. In the **Physical NICs** field, the physical NICs and uplinks dropdown list reflects the new NICs and uplink profile. Specifically, the uplinks `lag1-0` and `lag1-1`, corresponding to the LAG `lag1` that was created in step 4 are displayed. Select a physical NIC for `lag1-0` and a physical NIC for `lag1-1`.
14. Enter information for the other fields.

Verify the Transport Node Status

Make sure that the transport node creation process is working correctly.

After creating a host transport node, the N-VDS gets installed on the host.

Procedure

1. Log in to the NSX-T Data Center.
2. Navigate to the Transport Node page and view the N-VDS status.

3 Alternatively, view the N-VDS on ESXi with the `esxcli network ip interface list` command.

On ESXi, the command output should include a vmk interface (for example, vmk10) with a VDS name that matches the name you used when you configured the transport zone and the transport node.

```
# esxcli network ip interface list
...

vmk10
   Name: vmk10
   MAC Address: 00:50:56:64:63:4c
   Enabled: true
   Portset: DvsPortset-1
   Portgroup: N/A
   Netstack Instance: vxlan
   VDS Name: overlay-hostswitch
   VDS UUID: 18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2
   VDS Port: 10
   VDS Connection: 10
   Opaque Network ID: N/A
   Opaque Network Type: N/A
   External ID: N/A
   MTU: 1600
   TSO MSS: 65535
   Port ID: 67108895

 ...
```

If you are using the vSphere Client, you can view the installed N-VDS in the UI by selecting host **Configuration > Network Adapters**.

The KVM command to verify the N-VDS installation is `ovs-vsctl show`. Note that on KVM, the N-VDS name is nsx-switch.0. It does not match the name in the transport node configuration. This is by design.

```
# ovs-vsctl show
...
    Bridge "nsx-switch.0"
        Port "nsx-uplink.0"
            Interface "em2"
        Port "nsx-vtep0.0"
            tag: 0
            Interface "nsx-vtep0.0"
                type: internal
        Port "nsx-switch.0"
            Interface "nsx-switch.0"
                type: internal
    ovs_version: "2.4.1.3340774"
```

4 Check the transport node's assigned tunnel endpoint address.

The vmk10 interface receives an IP address from the NSX-T Data Center IP pool or DHCP, as shown here:

```
# esxcli network ip interface ipv4 get
Name   IPv4 Address    IPv4 Netmask   IPv4 Broadcast   Address Type  DHCP DNS
-----  --------------  -------------  ---------------  ------------  --------
vmk0   192.168.210.53  255.255.255.0  192.168.210.255  STATIC           false
vmk1   10.20.20.53     255.255.255.0  10.20.20.255     STATIC           false
vmk10  192.168.250.3   255.255.255.0  192.168.250.255  STATIC           false
```

In KVM, you can verify the tunnel endpoint and IP allocation with the `ifconfig` command.

```
# ifconfig
...
nsx-vtep0.0 Link encap:Ethernet  HWaddr ba:30:ae:aa:26:53
          inet addr:192.168.250.4  Bcast:192.168.250.255  Mask:255.255.255.0
         ...
```

5 Check the API for transport node state information.

Use the `GET https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state` API call. For example:

```
{
  "state": "success",
  "host_switch_states": [
    {
      "endpoints": [
        {
          "default_gateway": "192.168.250.1",
          "device_name": "vmk10",
          "ip": "192.168.250.104",
          "subnet_mask": "255.255.255.0",
          "label": 69633
        }
      ],
      "transport_zone_ids": [
        "efd7f38f-c5da-437d-af03-ac598f82a9ec"
      ],
      "host_switch_name": "overlay-hostswitch",
      "host_switch_id": "18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2"
    }
  ],
  "transport_node_id": "2d030569-5769-4a13-8918-0c309c63fdb9"
}
```

Migrate ESXi VMkernel and Physical Adapters

After preparing a host as a transport node, you can make changes to the current migration configuration of VMkernel adapters and physical adapters.

Prerequisites

- Ensure that the host has at least one free physical adapter.
- Ensure that VMkernel adapters and port groups exist on the host.

Procedure

1 From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.

2 Go to **System** > **Fabric** > **Host Transport Nodes**.

3 Select a transport node and click **Actions** > **Migrate ESX VMkernel and Physical Adapters**.

4 In the Migrate ESX VMkernel and Physical Adapters, enter the following details.

Field	Description
Direction	Make a selection: ■ **Migrate to Logical Switches**: To migrate VMkernel adapters from a VSS or VDS switch to an N-VDS switch in NSX-T Data Center. ■ **Migrate to Port Groups**: To migrate VMkernel adapters from an N-VDS switch to a VSS or VDS switch.
Select Switch	Select the switch from which you want to migrate the VMkernel adapters and physical adapters. You can select from the available switches.
Select VMkernel Adapters to Migrate	Click **Add** to enter the VMkernel adapter name and select destination as a logical switch or port group depending on where you want to migrate to.
Edit Physical Adapters in N-VDS	Click **Add** to enter the physical adapter name and map it to an uplink on the host switch.

5 Click **Save** to begin migration of VMkernel adapters and physical adapters.

Results

The updated VMkernel adapters and physical adapters are migrated to the N-VDS switch or revert migrated to the VSS or VDS switch in the ESXi host.

NSX Maintenance Mode

If you want to avoid vMotion of VMs to a transport node that is not functional, place that transport node in NSX Maintenance Mode.

To put a transport node in NSX Maintenance Mode, select the node, click Actions → NSX Maintenance Mode.

When you put a host in NSX Maintenance Mode, the transport node cannot participate in networking. Also, VMs running on other transport nodes that have N-VDS or vSphere Distributed Switch as the host switch cannot be vMotioned to this transport node. In addition, logical network cannot be configured on ESXi or KVM hosts.

Scenarios to put the transport node in NSX Maintenance Mode:

- A transport node is not functional.
- If a host has hardware or software issues that are unrelated to NSX-T, but you want to retain the node and its configurations in NSX-T, place the host in NSX Maintenance Mode.
- A transport node is automatically put in NSX Maintenance Mode when an upgrade on that transport node fails.

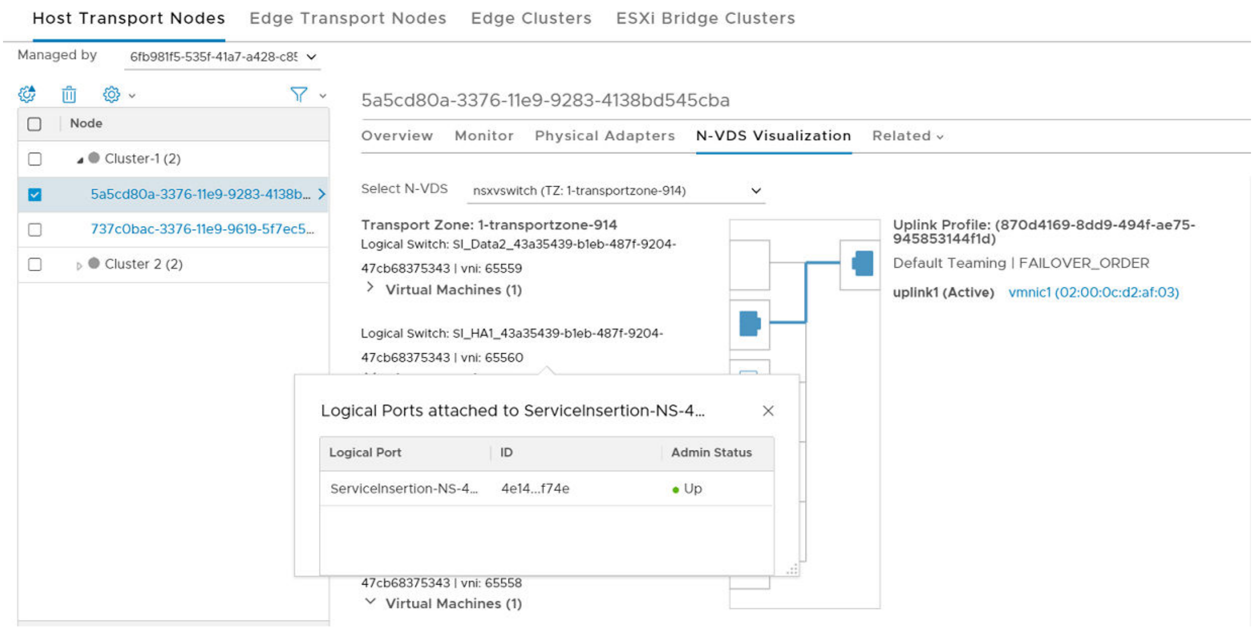
Any transport node put in the NSX Maintenance Mode is not upgraded.

Visual Representation of N-VDS

You get a granular view of N-VDS at an individual host level. NSX-T Data Center provides a visual representation of the connectivity status between the uplink of the N-VDS and VMs associated to a transport zone. The objects represented visually include the teaming policy - uplink and physical NIC that provide connectivity to VMs. The other set of objects represented visually are VMs, associated logical ports and switches, and status of VMs. The visual representation makes it easier to manage N-VDS.

Note Only ESXi hosts support visualization of N-VDS object.

Figure 10-3. N-VDS Visualization



Managed by 6fb981f5-535f-41a7-a428-c8ᵋ

- □ Cluster-1 (2)
- ☑ 5a5cd80a-3376-11e9-9283-4138b...
- □ 737c0bac-3376-11e9-9619-5f7ec5...
- □ Cluster 2 (2)

5a5cd80a-3376-11e9-9283-4138bd545cba

Select N-VDS nsxvswitch (TZ: 1-transportzone-914)

Transport Zone: 1-transportzone-914

Logical Switch: SI_Data2_43a35439-b1eb-487f-9204-47cb68375343 | vni: 65559

Virtual Machines (1)

Logical Switch: SI_HA1_43a35439-b1eb-487f-9204-47cb68375343 | vni: 65560

47cb68375343 | vni: 65558

Virtual Machines (1)

Uplink Profile: (870d4169-8dd9-494f-ae75-945853144f1d)

Default Teaming | FAILOVER_ORDER

uplink1 (Active) vmnic1 (02:00:0c:d2:af:03)

Logical Ports attached to ServiceInsertion-NS-4...

Logical Port	ID	Admin Status
ServiceInsertion-NS-4...	4e14...f74e	● Up

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Select **System > Fabric > Nodes > Host Transport Nodes**.
3. From the Managed by field, select **Standalone Host** or a *compute manager*.
4. Select the host.
5. Click the **N-VDS Visualization** tab.
6. Select an N-VDS.

   NSX-T visually represents uplink profiles connected to VMs, logical ports associated to VMs, logical switches connected to a transport zone.
7. To view uplink profiles connected to a VM and the logical port to which a VM is connected, select a VM.

   NSX-T visually represents the connectivity between a VM and an uplink profile.
8. To view which VMs are connected to an uplink profile, select the uplink profile.
9. To view logical ports associated to a VM, expand the logical switch, click the VM.

   The logical port details are displayed in a separate dialog box.

   Note The admin status of a logical port is displayed on the dialog box. If the operational status is down it is not displayed on the dialog box.

Health Check VLAN ID Ranges and MTU Settings

Run health check APIs to verify compatibility between VLAN ID ranges you specified and the MTU settings on a transport node with the corresponding settings on a physical switch.

VLAN or MTU configuration mismatch is a common configuration error that can lead to connectivity outage.

Note

- Health check results are only indicators of possible network configuration errors. For example, health check run on hosts from different L2 domains results in untrunked VLAN IDs. This result cannot be considered as a configuration error as hosts must be in the same L2 domain for the health check tool to give correct results.
- Only 50 health check operations can be in progress at any given time.
- After a health check finishes, NSX-T Data Center preserves that result on the system only for 24 hours.

In a health check operation, the NSX-T Data Center opsAgent sends probe packets from a transport node to another node to verify compatibility between VLAN ID range you specified and the MTU value on the transport node with corresponding settings on the physical switch.

As the number of VLAN ID ranges to be verified increases, the waiting time increases.

Number of VLANs	Waiting Time (secs)
[3073,4095]	150
[1025, 3072]	120
[513, 1024]	80
[128, 512]	60
[64, 127]	30
[1, 63]	20

Prerequisites

- At least two uplinks configured on N-VDS for VLAN and MTU check to work.
- Transport nodes on the same L2 domain.
- Health check supported on ESX hosts running v6.7U2 or later.

Procedure

1 Create a manual health check.

`POST https://<NSXManager_IP>/api/v1/manual-health-checks`

```
Example Request:
POST https://<nsx-mgr>/api/v1/manual-health-checks
{
  "resource_type": "ManualHealthCheck",
  "display_name": "Manual HealthCheck 002",
  "transport_zone_id": "7754341c-8f3c-443f-9c1a-2d635d5b0d1c",
  "vlans":{
    "vlan_ranges":[{
      "start": 0,
      "end": 6
    },]
  },
}
Example Response:
{
    "operation_status": "FINISHED",
    "transport_zone_id": "7754341c-8f3c-443f-9c1a-2d635d5b0d1c",
    "vlans": {
        "vlan_ranges": [
            {
                "start": 0,
                "end": 6
            }
        ]
    },
    "result": {
        "vlan_mtu_status": "UNTRUNKED",
        "results_per_transport_node": [
            {
                "transport_node_id": "dfcabffa-8839-11e9-b30e-6f45344d8a04",
                "result_on_host_switch": {
                    "host_switch_name": "nsxvswitch",
                    "results_per_uplink": [
                        {
                            "uplink_name": "uplink1",
                            "vlan_and_mtu_allowed": [
                                {
                                    "start": 0,
                                    "end": 0
                                }
                            ],
                            "mtu_disallowed": [],
                            "vlan_disallowed": [
                                {
                                    "start": 1,
                                    "end": 6
                                }
                            ]
                        }
                    ]
                }
            },
            {
                "transport_node_id": "a300ea62-8839-11e9-a94e-31732bb71949",
                "result_on_host_switch": {
                    "host_switch_name": "nsxvswitch",
                    "results_per_uplink": [
                        {
                            "uplink_name": "uplink1",
                            "vlan_and_mtu_allowed": [
                                {
                                    "start": 0,
                                    "end": 0
                                }
                            ],
                            "mtu_disallowed": [],
                            "vlan_disallowed": [
                                {
                                    "start": 1,
                                    "end": 6
                                }
                            ]
                        }
                    ]
                }
            }
        ]
    },
    "resource_type": "ManualHealthCheck",
    "id": "8a56ed9e-a31b-479e-987b-2dbfbde07c38",
    "display_name": "mc1",
    "_create_user": "admin",
    "_create_time": 1560149933059,
    "_last_modified_user": "system",
    "_last_modified_time": 1560149971220,
    "_system_owned": false,
    "_protection": "NOT_PROTECTED",
    "_revision": 0
}
```

A new health check object is created with id `8a56ed9e-a31b-479e-987b-2dbfbde07c38`.

2. To get a list of all manual health check operations initiated, make the API call.

   `GET https://<NSXManager_IP>/api/v1/manual-health-checks`

3. To delete a manual health check, make the API call.

   `DELETE https://<NSXManager_IP>/api/v1/manual-health-checks/<Health-check-ID>`

4. To get a single health check initiated manually, make the API call.

   `GET https://<NSXManager_IP>/api/v1/manual-health-checks/< Health-check-ID>`

Results

The API response section contains the health check results. The NSX Ops agent waits for an acknowledgement packet from the destination transport node to retrieve VLAN ID ranges supported on the physical switch.

- Untrunked: Lists the VLAN ID ranges that are not compatible with a physical switch. The VLAN ID ranges that are compatible with the physical switch are also listed.
- Trunked: Lists the VLAN ID ranges that are compatible with a physical switch.
- Unknown: There is no valid result for some or all uplinks because of infrastructure issues or unsupported platform types such as KVM and Edge.

Parameters in the API response section:

- vlan_and_mtu_allowed: Lists the VLAN ID ranges that are compatible.
- mtu_disallowed: Lists the VLAN ID ranges for which the MTU value is not compatible with a physical switch.
- vlan_disallowed: Lists the VLAN ID ranges that are not compatible with a physical switch.

What to do next

- In an overlay-based transport zone, update both VLAN ID and MTU config in the uplink profile on N-VDS. Likewise, update VLAN or MTU on the physical switch.
- In a vlan-based transport zone, update MTU config in the uplink profile. And, update VLAN config on logical switches of that transport zone. Likewise update VLAN or MTU on the physical switch.

View Bidirectional Forwarding Detection Status

View BFD status between transport nodes. Each transport node detects connectivity status with another remote transport node through a tunnel status that displays the BFD status among other details related to the node.

Both Host Transport nodes (standalone and hosts registered to a vCenter) and Edge nodes display the tunnel status. BFD packets support both GENEVE and STT encapsulation. GENEVE is the default encapsulation.

Procedure

1 From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.

2 Navigate to **System > Fabric > Nodes > Host Transport Nodes**.

3 On the Tunnel column, click the tunnel number that is displayed.

The Monitor page displays the status of tunnel, BFD diagnostic code, remote node UUID, encapsulation on BFD packets, and tunnel name.

The tunnel BFD diagnostic code indicates the reason for the change in the session state.

Code	Description
0	No Diagnostic
1	Control Detection Time Expired
2	Echo Function Failed
3	Neighbor Signaled Session Down
4	Forwarding Plane Reset
5	Path Down
6	Concatenated Path Down
7	Administratively Down
8	Reverse Concatenated Path Down

Results

If the BFD status is down, use the diagnostic code to establish connectivity between transport nodes.

Manual Installation of NSX-T Data Center Kernel Modules

As an alternative to using the NSX-T Data Center **Fabric > Nodes > Hosts > Add** UI or the `POST /api/v1/fabric/nodes` API, you can install NSX-T Data Center kernel modules manually from the hypervisor command line.

Note You cannot manually install of NSX-T Data Center kernel modules on a bare metal server.

Manually Install NSX-T Data Center Kernel Modules on ESXi Hypervisors

To prepare hosts to participate in NSX-T Data Center, you must install NSX-T Data Center kernel modules on ESXi hosts. This allows you to build the NSX-T Data Center control-plane and management-plane fabric. NSX-T Data Center kernel modules packaged in VIB files run within the hypervisor kernel and provide services such as distributed routing, distributed firewall, and bridging capabilities.

You can download the NSX-T Data Center VIBs manually and make them part of the host image. The download paths can change for each release of NSX-T Data Center. Always check the NSX-T Data Center downloads page to get the appropriate VIBs.

Procedure

1 Log in to the host as root or as a user with administrative privileges

2 Navigate to the /tmp directory.

```
[root@host:~]: cd /tmp
```

3 Download and copy the nsx-lcp file into the /tmp directory.

4 Run the install command.

```
[root@host:/tmp]: esxcli software vib install -d /tmp/nsx-lcp-<release>.zip
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: VMware_bootbank_nsx-aggservice_<release>, VMware_bootbank_nsx-da_<release>, 
VMware_bootbank_nsx-esx-datapath_<release>, VMware_bootbank_nsx-exporter_<release>, 
VMware_bootbank_nsx-host_<release>, VMware_bootbank_nsx-lldp_<release>, VMware_bootbank_nsx-
mpa_<release>, VMware_bootbank_nsx-cfgagent_<release>, VMware_bootbank_nsx-python-
protobuf_<release>, VMware_bootbank_nsx-sfhc_<release>, VMware_bootbank_nsxa_<release>, 
VMware_bootbank_nsxcli_<release>
   VIBs Removed:
   VIBs Skipped:
```

Depending on what was already installed on the host, some VIBs might be installed, some might be removed, and some might be skipped. A reboot is not required unless the command output says `Reboot Required: true`.

Results

As a result of adding an ESXi host to the NSX-T Data Center fabric, the following VIBs get installed on the host.

nsx-adf

(Automated Diagnostics Framework) Collects and analyzes performance data to produce both local (at host) and central (across datacenter) diagnoses of performance issues.

nsx-aggservice

Provides host-side libraries for NSX-T Data Center aggregation service. NSX-T Data Center aggregation service is a service that runs in the management-plane nodes and fetches runtime state from NSX-T Data Center components.

nsx-cfgagent

Provides communication between the central control plane and hypervisors. Receives logical networking state from the central control plane and programs this state in the data plane.

nsx-cli-libs

Provides the NSX-T Data Center CLI on hypervisor hosts.

nsx-common-libs

Provide some utilities classes such as AES, SHA-1, UUID, bitmap, and others.

nsx-context-mux

Provides NSX Guest Introspection relay functionality. Allows VMware Tools guest agents to relay guest context to inhouse and registered third-party partner appliances.

nsx-esx-datapath

Provides NSX-T Data Center data plane packet processing functionality.

nsx-exporter

Provides host agents that report runtime state to the aggregation service running in the management plane.

nsx-host

Provides metadata for the VIB bundle that is installed on the host.

nsx-metrics-libs

Provides metric utility classes for collecting daemon metrics.

nsx-mpa

Provides communication between NSX Manager and hypervisor hosts.

nsx-nestdb-libs

NestDB is a database that stores NSX configurations related to the host (desired/runtime state, etc).

nsx-opsagent

Communicates operations agent executions (transport node realization, Link Layer Discovery Protocol - LLDP,traceflow, packet capture, etc.) with the management plane.

nsx-platform-client

Provides a common CLI execution agent, for centralized CLI and audit log collecting.

nsx-profiling-libs

Provides the functionality of profiling based on gpeftool which used for daemon process profiling.

nsx-proxy

Provides the only northbound contact point agent, which talks to the central control plane and management plane.

nsx-python-gevent

Contains Python Gevent.

nsx-python-greenlet

Contains Python Greenlet library (third party libraries).

nsx-python-logging

Contains the Python logs.

nsx-python-protobuf

Provides Python bindings for protocol buffers.

nsx-rpc-libs

This library provides nsx-rpc functionality.

nsx-sfhc

Service fabric host component (SFHC). Provides a host agent for managing the lifecycle of the hypervisor as a fabric host in the management plane's inventory. This provides a channel for operations such as NSX-T Data Center upgrade and uninstall and monitoring of NSX-T Data Center modules on hypervisors.

nsx-shared-libs

Contains the shared NSX libraries.

nsx-upm-libs

Provides unified profile management functionality for flattening client-side configuration and avoiding duplicate data transmission.

nsx-vdpi

Provides Deep Packet Inspection capabilities for NSX-T Data Center Distributed Firewall.

nsx-vsipfwlib

Provides distributed firewall functionality.

nsxcli

Provides the NSX-T Data Center CLI on hypervisor hosts.

To verify, you can run the **esxcli software vib list | grep nsx** or **esxcli software vib list | grep <yyyy-mm-dd>** command on the ESXi host, where the date is the day that you performed the installation.

What to do next

Add the host to the NSX-T Data Center management plane. See Deploy NSX Manager Nodes to Form a Cluster Using CLI .

Manually Install NSX-T Data Center Software Packages on Ubuntu KVM Hypervisors

To prepare hosts to participate in NSX-T Data Center, you can manually install NSX-T Data Center kernel modules on Ubuntu KVM hosts. This allows you to build the NSX-T Data Center control-plane and management-plane fabric. NSX-T Data Center kernel modules packaged in DEB files run within the hypervisor kernel and provide services such as distributed routing, distributed firewall, and bridging capabilities.

You can download the NSX-T Data Center DEBs manually and make them part of the host image. Be aware that download paths can change for each release of NSX-T Data Center. Always check the NSX-T Data Center downloads page to get the appropriate DEBs.

Prerequisites

- Verify that the required third-party packages are installed. See Install Third-Party Packages on a KVM Host.

Procedure

1 Log in to the host as a user with administrative privileges.

2 (Optional) Navigate to the /tmp directory.

```
cd /tmp
```

3 Download and copy the nsx-lcp file into the /tmp directory.

4 Untar the package.

```
tar -xvf nsx-lcp-<release>-ubuntu-trusty_amd64.tar.gz
```

5 Navigate to the package directory.

```
cd nsx-lcp-trusty_amd64/
```

6 Install the packages.

```
sudo dpkg -i *.deb
```

7 Reload the OVS kernel module.

```
/etc/init.d/openvswitch-switch force-reload-kmod
```

If the hypervisor uses DHCP on OVS interfaces, restart the network interface on which DHCP is configured. You can manually stop the old dhclient process on the network interface and restart a new dhclient process on that interface.

8 To verify, you can run the `dpkg -l | egrep 'nsx|openvswitch'` command.

The installed packages in the output must match the packages in the `nsx-lcp-trusty_amd64` directory.

Any errors are most likely caused by incomplete dependencies. The `apt-get install -f` command can attempt to resolve dependencies and re-run the NSX-T Data Center installation.

What to do next

Add the host to the NSX-T Data Center management plane. See Deploy NSX Manager Nodes to Form a Cluster Using CLI .

Manually Install NSX-T Data Center Software Packages on RHEL and CentOS KVM Hypervisors

To prepare hosts to participate in NSX-T Data Center, you can manually install NSX-T Data Center kernel modules on RHEL or CentOS KVM hosts.

This allows you to build the NSX-T Data Center control-plane and management-plane fabric. NSX-T Data Center kernel modules packaged in RPM files run within the hypervisor kernel and provide services such as distributed routing, distributed firewall, and bridging capabilities.

You can download the NSX-T Data Center RPMs manually and make them part of the host image. Be aware that download paths can change for each release of NSX-T Data Center. Always check the NSX-T Data Center downloads page to get the appropriate RPMs.

Prerequisites

Ability to reach a RHEL or CentOS repository.

Procedure

1 Log in to the host as an administrator.

2 Download and copy the nsx-lcp file into the /tmp directory.

3 Untar the package.

```
tar -zxvf nsx-lcp-<release>-rhel7.4_x86_64.tar.gz
```

4 Navigate to the package directory.

```
cd nsx-lcp-rhel74_x86_64/
```

5 Install the packages.

```
sudo yum install *.rpm
```

When you run the yum install command, any NSX-T Data Center dependencies are resolved, assuming the RHEL or CentOS hosts can reach their respective repositories.

6 Reload the OVS kernel module.

```
/usr/share/openvswitch/scripts/ovs-systemd-reload force-reload-kmod
```

If the hypervisor uses DHCP on OVS interfaces, restart the network interface on which DHCP is configured. You can manually stop the old dhclient process on the network interface and restart a new dhclient process on that interface.

7 To verify, you can run the `rpm -qa | egrep 'nsx|openvswitch'` command.

The installed packages in the output must match the packages in the nsx-rhel74 or nsx-centos74 directory.

What to do next

Add the host to the NSX-T Data Center management plane. See Deploy NSX Manager Nodes to Form a Cluster Using CLI .

Manually Install NSX-T Data Center Software Packages on SUSE KVM Hypervisors

To prepare hosts to participate in NSX-T Data Center, you can manually install NSX-T Data Center kernel modules on SUSE KVM hosts.

This allows you to build the NSX-T Data Center control-plane and management-plane fabric. NSX-T Data Center kernel modules packaged in RPM files run within the hypervisor kernel and provide services such as distributed routing, distributed firewall, and bridging capabilities.

You can download the NSX-T Data Center RPMs manually and make them part of the host image. Be aware that download paths can change for each release of NSX-T Data Center. Always check the NSX-T Data Center downloads page to get the appropriate RPMs.

Prerequisites

Ability to reach a SUSE repository.

Procedure

1 Log in to the host as an administrator.

2 Download and copy the nsx-lcp file into the /tmp directory.

3 Untar the package.

```
tar -zxvf nsx-lcp-3.0.0.0.0.14335404-linux64-sles12sp3.tar.gz
```

4 Navigate to the package directory.

```
cd nsx-lcp-linux64-sles12sp3
```

5 Install the packages.

```
sudo zypper --no-gpg-checks  install -y *.rpm
```

When you run the zypper install command, any NSX-T Data Center dependencies are resolved, assuming the SUSE hosts can reach their respective repositories.

6 Reload the OVS kernel module.

```
/usr/share/openvswitch/scripts/ovs-systemd-reload force-reload-kmod
```

If the hypervisor uses DHCP on OVS interfaces, restart the network interface on which DHCP is configured. You can manually stop the old dhclient process on the network interface and restart a new dhclient process on that interface.

7 To verify, you can run the `zypper packages --installed-only | grep System | egrep 'openvswitch|nsx'` command.

The installed packages in the output must match the packages in the `nsx-lcp-linux64-sles12sp3` directory.

What to do next

Add the host to the NSX-T Data Center management plane. See Deploy NSX Manager Nodes to Form a Cluster Using CLI .

Deploy a Fully Collapsed vSphere Cluster NSX-T

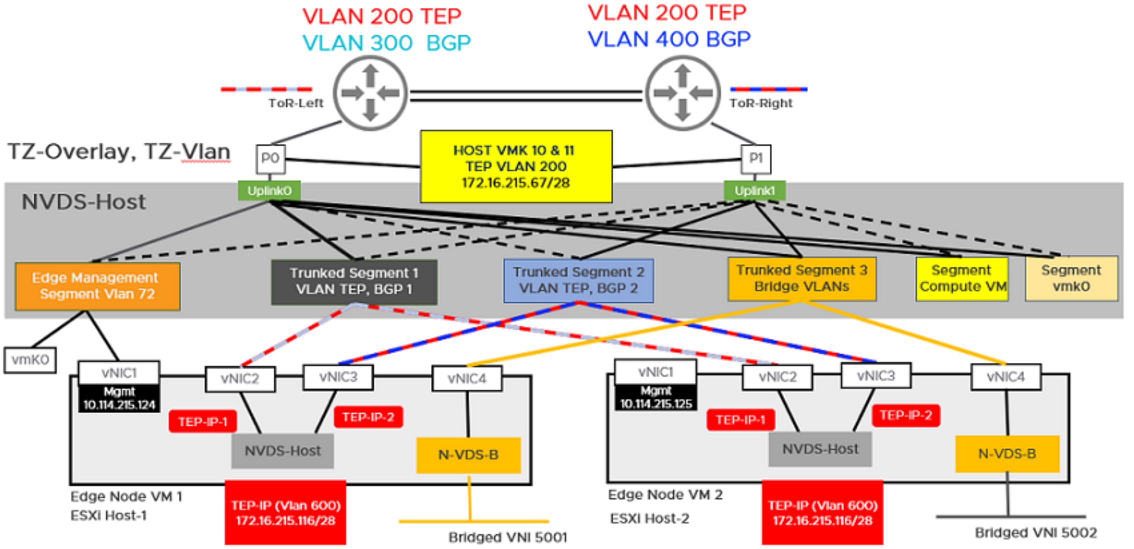
You can configure NSX Manager, host transport nodes, and NSX Edge VMs on a single cluster. Each host in the cluster provides two physical NICs that are configured for NSX-T.

Important Deploy the fully collapsed single vSphere cluster topology starting with NSX-T 2.4.2 or 2.5 release.

The topology referenced in this procedure uses:

- vSAN configured with the hosts in the cluster.
- A minimum of two physical NICs per host.
- vMotion and Management VMkernel interfaces.

Figure 10-4. Topology: Single N-VDS Switch Managing Host Communication with NSX Edge and Guest VMs

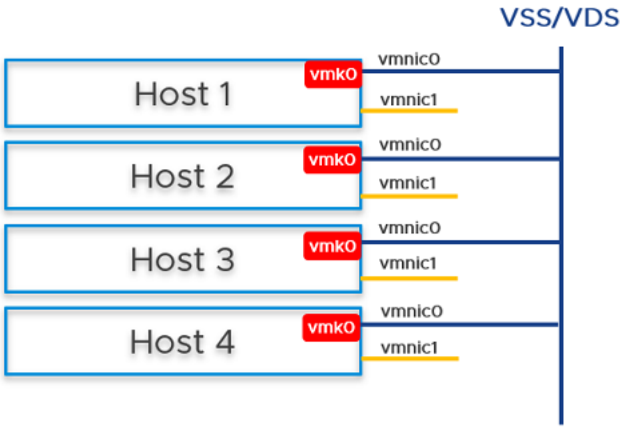


Prerequisites

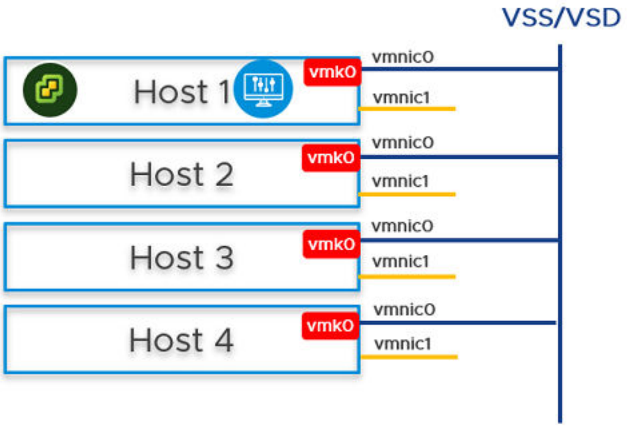
- All the hosts must be part of a vSphere cluster.
- Each host has two physical NICs enabled.
- Register all hosts to a vCenter Server.
- Verify on the vCenter Server that shared storage is available to be used by the hosts.
- Host TEP IP and NSX Edge TEP IP must be in a different VLAN. North-South traffic from Host workloads is encapsulated in GENEVE and sent to an NSX Edge node with Source IP as Host TEP and destination IP as NSX Edge TEP. Since these TEPs must sit in different VLAN or subnets, this traffic must be routed through Top-of-rack (TOR) switches. Transport VLAN used for Host is VLAN 200 and transport VLAN used for NSX Edge is VLAN 600.

Procedure

1 Prepare four ESXi hosts with vmnic0 on vSS or vDS, vmnic1 is free.



2 On Host 1, install vCenter Server, configure a vSS/vDS port group, and install NSX Manager on the port group created on the host.



3 Prepare ESXi hosts 1, 2, 3 and 4 to be transport nodes.

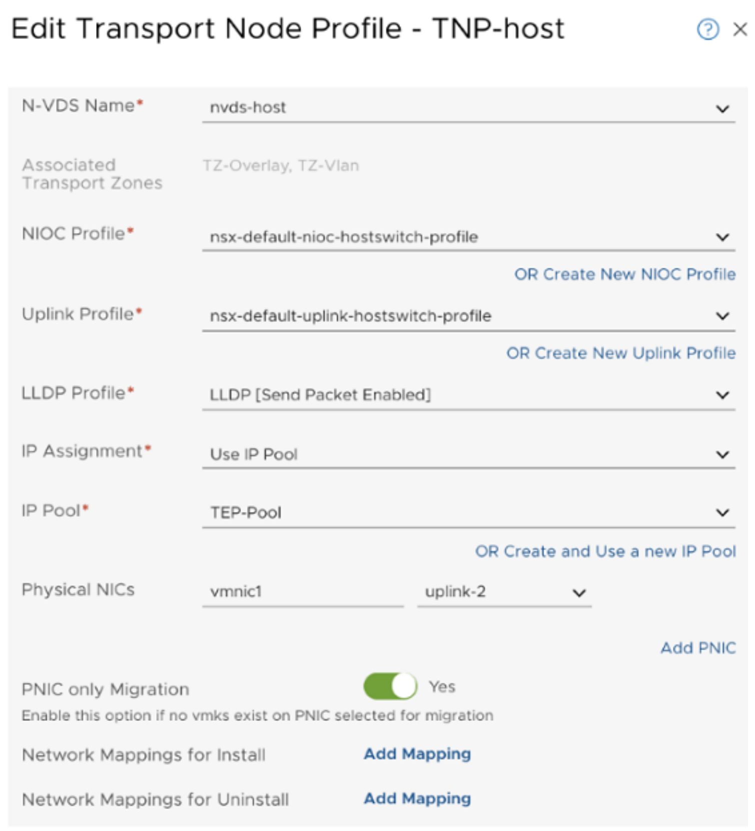
a Create VLAN transport zone and overlay transport zone with a named teaming policy. See Create Transport Zones.

b Create an IP pool or DHCP for tunnel endpoint IP addresses for the hosts. See Create an IP Pool for Tunnel Endpoint IP Addresses.

c Create an IP pool or DHCP for tunnel endpoint IP addresses for the Edge node. See Create an IP Pool for Tunnel Endpoint IP Addresses.

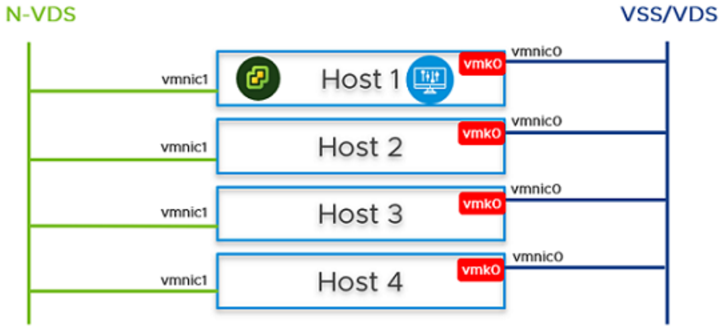
d Create an uplink profile with a named teaming policy. See Create an Uplink Profile.

e Configure hosts as transport nodes by applying a transport node profile. In this step, the transport node profile only migrates vmnic1 (unused physical NIC) to the N-VDS switch. After the transport node profile is applied to the cluster hosts, the N-VDS switch is created and vmnic1 is connected to the N-VDS switch. See Add a Transport Node Profile.



Edit Transport Node Profile - TNP-host

N-VDS Name*	nvds-host
Associated Transport Zones	TZ-Overlay, TZ-Vlan
NIOC Profile*	nsx-default-nioc-hostswitch-profile OR Create New NIOC Profile
Uplink Profile*	nsx-default-uplink-hostswitch-profile OR Create New Uplink Profile
LLDP Profile*	LLDP [Send Packet Enabled]
IP Assignment*	Use IP Pool
IP Pool*	TEP-Pool OR Create and Use a new IP Pool
Physical NICs	vmnic1 uplink-2 Add PNIC
PNIC only Migration Enable this option if no vmks exist on PNIC selected for migration	Yes
Network Mappings for Install	Add Mapping
Network Mappings for Uninstall	Add Mapping

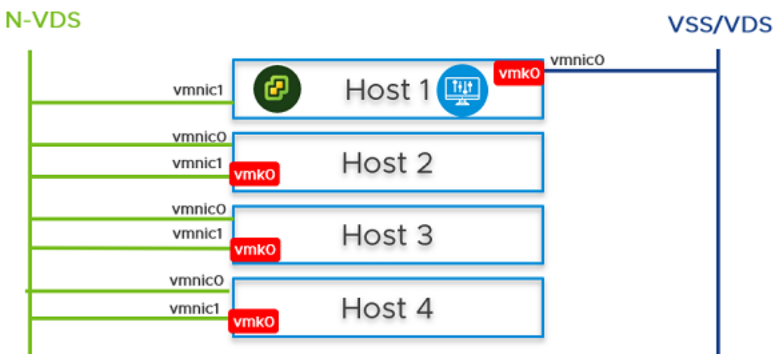


vmnic1 on all hosts are added to the N-VDS switch. So, out of the two physical NICs, one is migrated to the N-VDS switch. The vmnic0 interface is still connected to the vSS or vDS switch, which ensures connectivity to the host is available.

4 In the NSX Manager UI, create VLAN-backed segments for NSX Manager, vCenter Server, and NSX Edge. Ensure to select the correct teaming policy for each of the VLAN-backed segments. Do not use VLAN trunk logical switch as the target. When creating the target segments in NSX Manager UI, in the **Enter List of VLANs** field, enter only one VLAN value.

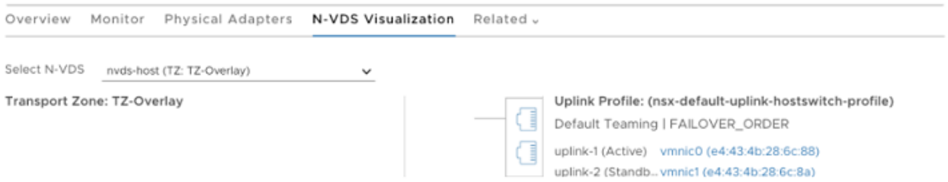
5 On Host 2, Host 3, and Host 4, you must migrate the vmk0 adapter and vmnic0 together from VSS/VDS to N-VDS switch. Update the NSX-T configuration on each host. While migrating ensure

- vmk0 is mapped to **Edge Management Segment** .
- vmnic0 is mapped to an active uplink, **uplink-1** .



6 In the vCenter Server, go to Host 2, Host 3, and Host 4, and verify that vmk0 adapter is connected to vmnic0 physical NIC on the N-VDS and must be reachable.

7 In the NSX Manager UI, go to Host 2, Host 3, and Host 4, and verify both pNICs are on the N-VDSswitch.



Select N-VDS nvds-host (TZ: TZ-Overlay)

Transport Zone: TZ-Overlay

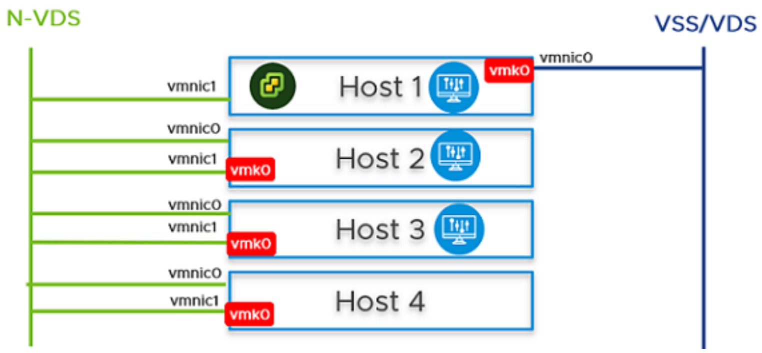
Uplink Profile: (nsx-default-uplink-hostswitch-profile)

Default Teaming | FAILOVER_ORDER

uplink-1 (Active) vmnic0 (e4:43:4b:28:6c:88)

uplink-2 (Standb... vmnic1 (e4:43:4b:28:6c:8a)

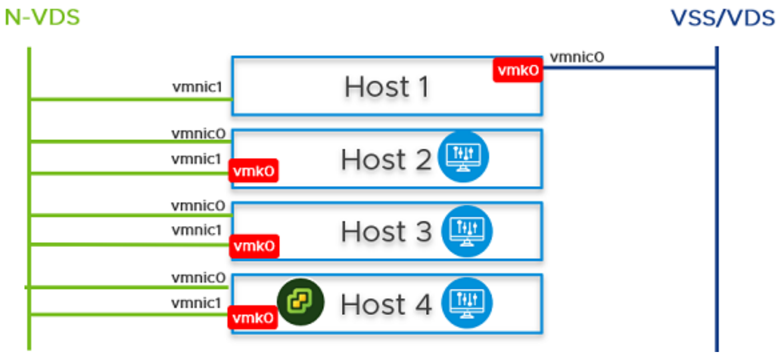
8 On Host 2 and Host 3, from the NSX Manager UI, install NSX Manager and attach NSX Manager to the segment. Wait for approximately 10 minutes for the cluster to form and verify that the cluster has formed.



9 Power off the first NSX Manager node. Wait for approximately 10 minutes.

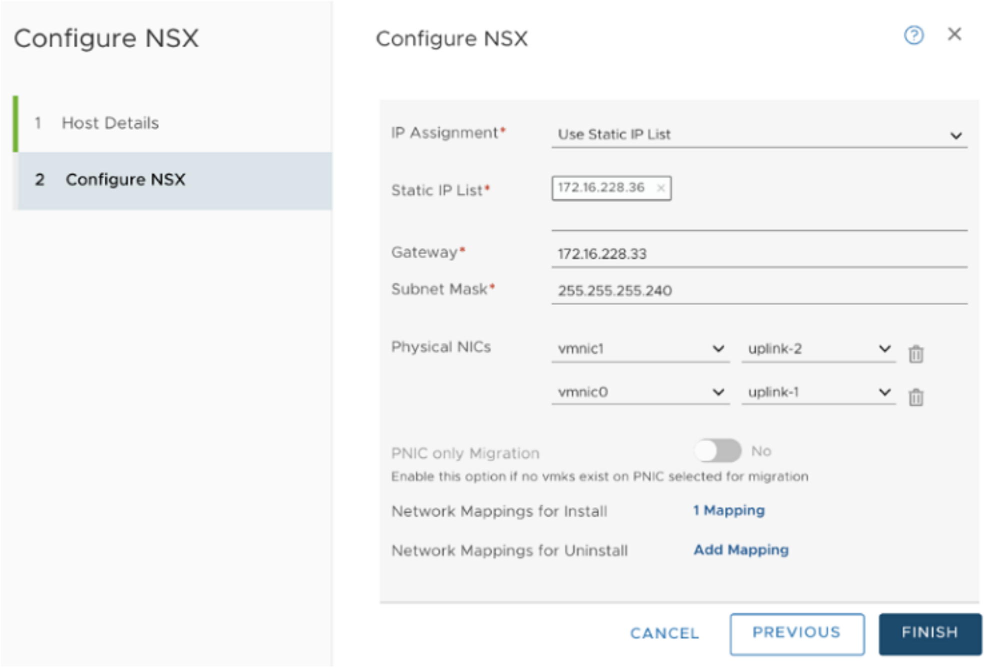
10 Reattach the NSX Manager and vCenter Server to the previously created logical switch. On host 4, power on the NSX Manager. Wait for approximately 10 minutes to verify that the cluster is in a stable state. With the first NSX Manager powered off, perform cold vMotion to migrate the NSX Manager and vCenter Server from host 1 to host 4.

For vMotion limitations, see https://kb.vmware.com/s/article/56991.



11 From the NSX Manager UI, go to Host 1, migrate vmk0 and vmnic0 together from VSS to N-VDS switch.

12 In the **Network Mapping for Install** field, ensure that the vmk0 adapter is mapped to the **Edge Management Segment** on the N-VDS switch.



Configure NSX

1 Host Details

2 Configure NSX

Configure NSX

IP Assignment* Use Static IP List

Static IP List* 172.16.228.36

Gateway* 172.16.228.33

Subnet Mask* 255.255.255.240

Physical NICs vmnic1 uplink-2

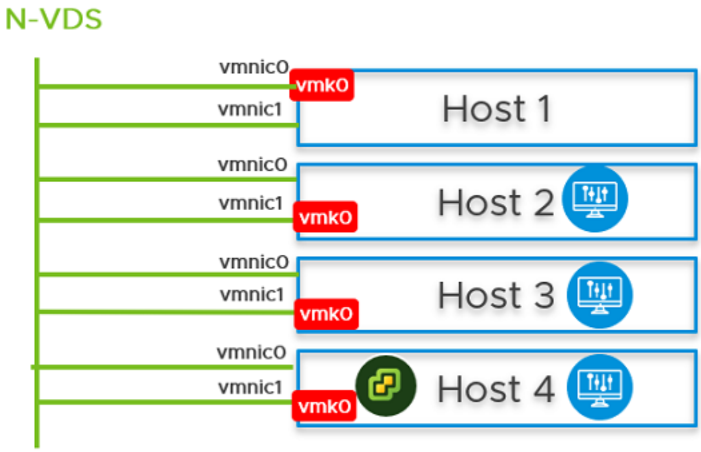
vmnic0 uplink-1

PNIC only Migration No

Enable this option if no vmks exist on PNIC selected for migration

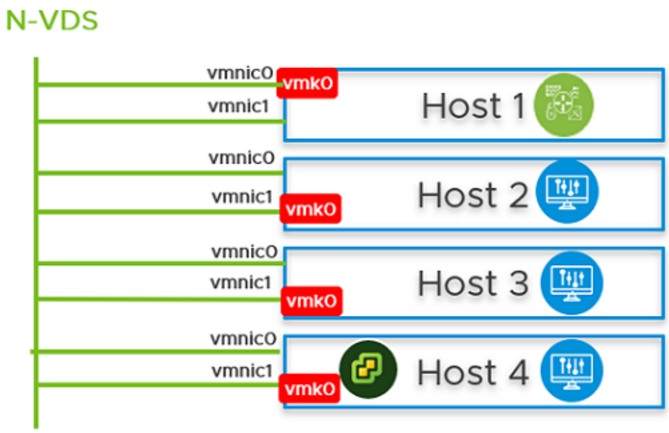
Network Mappings for Install 1 Mapping

Network Mappings for Uninstall Add Mapping



13 On Host 1, install the NSX Edge VM from the NSX Manager UI.

See Create an NSX Edge Transport Node.



14 Join the NSX Edge VM with the management plane.

See Join NSX Edge with the Management Plane.

15 To establish the north-south traffic connectivity, configure NSX Edge VM with an external router.

16 Verify that north-south traffic connectivity between the NSX Edge VM and the external router.

17 If there is a power failure scenario where the whole cluster is rebooted, the NSX-T management component might not come up and communicate with N-VDS. To avoid this scenario, perform the following steps:

Caution Any API command that is incorrectly run results in a loss of connectivity with the NSX Manager.

Note In a single cluster configuration, management components are hosted on an N-VDS switch as VMs. The N-VDS port to which the management component connects to by default is initialized as a blocked port due to security considerations. If there is a power failure requiring all the four hosts to reboot, the management VM port will be initialized in a blocked state. To avoid circular dependencies, it is recommended to create a port on N-VDS in the unblocked state. An unblocked port ensures that when the cluster is rebooted, the NSX-T management component can communicate with N-VDS to resume normal function.

At the end of the subtask, the migration command takes the :

- UUID of the host node where the NSX Manager resides.
- UUID of the NSX Manager VM and migrates it to the static logical port which is in an unblocked state.

If all the hosts are powered-off or powered-on or if an NSX Manager VM moves to another host, then after the NSX Manager comes back up it gets attached to the unblocked port, so preventing loss of connectivity with the management component of NSX-T.

a In the NSX Manager UI, go to **Manager Mode > Networking > Logical Switches** tab (3.0 and later releases). Search for the **Segment Compute VM** segment. Select the **Overview** tab, find and copy the UUID. The UUID used in this example is, *c3fd8e1b-5b89-478e-abb5-d55603f04452*.

b Create a JSON payload for each NSX Manager.

- In the JSON payload, create logical ports with initialization status in `UNBLOCKED_VLAN` state by replacing the value for `logical_switch_id` with the UUID of the previously created **Edge Management Segment**.
- In the payload for each NSX Manager, the `attachment_type_id` and `display_name` values will be different.

Important Repeat this step to create a total of four JSON files - three for NSX Managers and one for vCenter Server Appliance (VCSA).

```
port1.json
{
"admin_state": "UP",
"attachment": {
"attachment_type": "VIF",
"id": "nsxmgr-port-147"
},
"display_name": "NSX Manager Node 147 Port",
"init_state": "UNBLOCKED_VLAN",
"logical_switch_id": "c3fd8e1b-5b89-478e-abb5-d55603f04452"
}
```

Where,

- `admin_state`: This is state of the port. It must UP.
- `attachment_type`: Must be set to VIF. All VMs are connected to NSX-T switch ports using a VIF ID.
- `id`: This is the VIF ID. It must be unique for each NSX Manager. If you have three NSX Managers, there will be three payloads, and each one of them must have a different VIF ID. To generate a unique UUID, log into the root shell of the NSX Manager and run `/usr/bin/uuidgen` to generate a unique UUID.
- `display_name`: It must be unique to help NSX admin identify it from other NSX Manager display names.
- `init_state`: With the value set to `UNBLOCKED_VLAN`, NSX unblocks the port for NSX Manager, even if the NSX Manager is not available.
- `logical_switch_id`: This is the logical switch ID of the **Edge Management Segment**.

c If there are three NSX Managers deployed, you need to create three payloads, one for each logical port of a NSX Manager. For example, port1.json, port2.json, port3.json.

Run the following commands to create payloads.

```
curl -X POST -k -u '<username>:<password>' -H 'Content-Type:application/json' -d
@port1.json https://nsxmgr/api/v1/logical-ports
```

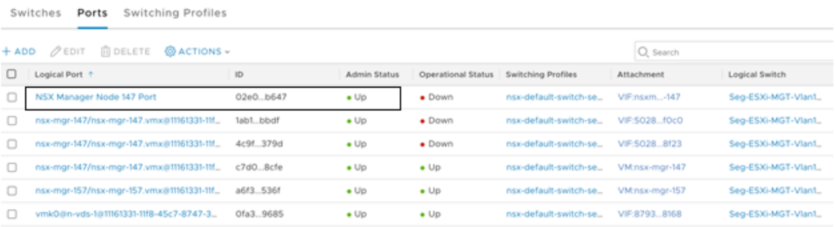
```
curl -X POST -k -u '<username>:<password>' -H 'Content-Type:application/json' -d
@port2.json https://nsxmgr/api/v1/logical-ports
```

```
curl -X POST -k -u '<username>:<password>' -H 'Content-Type:application/json' -d
@port3.json https://nsxmgr/api/v1/logical-ports
```

An example of API execution to create a logical port.

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -X POST -k -u
'<username>:<password>' -H 'Content-Type:application/json' -d @port1.json https://
localhost/api/v1/logical-ports
{
  "logical_switch_id" : "c3fd8e1b-5b89-478e-abb5-d55603f04452",
  "attachment" : {
    "attachment_type" : "VIF",
    "id" : "nsxmgr-port-147"
  },
  "admin_state" : "UP",
  "address_bindings" : [ ],
  "switching_profile_ids" : [ {
    "key" : "SwitchSecuritySwitchingProfile",
    "value" : "fbc4fb17-83d9-4b53-a286-ccdf04301888"
  }, {
    "key" : "SpoofGuardSwitchingProfile",
    "value" : "fad98876-d7ff-11e4-b9d6-1681e6b88ec1"
  }, {
    "key" : "IpDiscoverySwitchingProfile",
    "value" : "0c403bc9-7773-4680-a5cc-847ed0f9f52e"
  }, {
    "key" : "MacManagementSwitchingProfile",
    "value" : "1e7101c8-cfef-415a-9c8c-ce3d8dd078fb"
  }, {
    "key" : "PortMirroringSwitchingProfile",
    "value" : "93b4b7e8-f116-415d-a50c-3364611b5d09"
  }, {
    "key" : "QosSwitchingProfile",
    "value" : "f313290b-eba8-4262-bd93-fab5026e9495"
  } ],
  "init_state" : "UNBLOCKED_VLAN",
  "ignore_address_bindings" : [ ],
  "resource_type" : "LogicalPort",
  "id" : "02e0d76f-83fa-4839-a525-855b47ecb647",
  "display_name" : "NSX Manager Node 147 Port",
  "_create_user" : "admin",
  "_create_time" : 1574716624192,
  "_last_modified_user" : "admin",
  "_last_modified_time" : 1574716624192,
  "_system_owned" : false,
  "_protection" : "NOT_PROTECTED",
  "_revision" : 0
```

d Verify that the logical port is created.



□	Logical Port ↑	ID	Admin Status	Operational Status	Switching Profiles	Attachment	Logical Switch
□	NSX Manager Node 147 Port	02e0...b647	● Up	● Down	nsx-default-switch-se...	VIF:nsxm...-147	Seg-ESXi-MGT-Vlan1...
□	nsx-mgr-147/nsx-mgr-147.vmx@11161331-11f...	1ab1...bbdf	● Up	● Down	nsx-default-switch-se...	VIF:5028...f0c0	Seg-ESXi-MGT-Vlan1...
□	nsx-mgr-147/nsx-mgr-147.vmx@11161331-11f...	4c9f...379d	● Up	● Down	nsx-default-switch-se...	VIF:5028...8f23	Seg-ESXi-MGT-Vlan1...
□	nsx-mgr-147/nsx-mgr-147.vmx@11161331-11f...	c7d0...8cfe	● Up	● Up	nsx-default-switch-se...	VM:nsx-mgr-147	Seg-ESXi-MGT-Vlan1...
□	nsx-mgr-157/nsx-mgr-157.vmx@11161331-11f...	a6f3...536f	● Up	● Up	nsx-default-switch-se...	VM:nsx-mgr-157	Seg-ESXi-MGT-Vlan1...
□	vmk0@n-vds-1@11161331-11f8-45c7-8747-3...	0fa3...9685	● Up	● Up	nsx-default-switch-se...	VIF:8793...8168	Seg-ESXi-MGT-Vlan1...

e Find out the VM instance ID for each of the NSX Manager. You can retrieve the instance ID from the **Inventory** → **Virtual Machines**, select the NSX Manager VM, select the **Overview** tab and copy the instance ID. Alternatively, search the instance ID from the managed object browser (MOB) of vCenter Server. Add `:4000` to the ID to get the VNIC hardware index of an NSX Manager VM.

For example, if the instance UUID of the VM is `503c9e2b-0abf-a91c-319c-1d2487245c08`, then its vnic index is `503c9e2b-0abf-a91c-319c-1d2487245c08:4000`. The three NSX Manager vnic indices are:

```
mgr1 vnic: 503c9e2b-0abf-a91c-319c-1d2487245c08:4000

mgr2 vnic: 503c76d4-3f7f-ed5e-2878-cffc24df5a88:4000

mgr3 vnic: 503cafd5-692e-d054-6463-230662590758:4000
```

f Find out the transport node ID that hosts NSX Managers. If you have three NSX Manager , each hosted on a different transport node, note down the tranport node IDs. For example, the three transport node IDs are:

```
tn1: 12d19875-90ed-4c78-a6bb-a3b1dfe0d5ea

tn2: 4b6e182e-0ee3-403f-926a-fb7c8408a9b7

tn3: d7cec2c9-b776-4829-beea-1258d8b8d59b
```

g Retrieve the transport node configuration that is to be used as payloads when migrating the NSX Manager to the newly created port.

For example,

```
curl -k -u '<user>:<password>' https://nsxmgr/api/v1/transport-nodes/
12d19875-90ed-4c78-a6bb-a3b1dfe0d5ea > tn1.json

curl -k -u '<user>:<password>' https://nsxmgr/api/v1/transport-nodes/
4b6e182e-0ee3-403f-926a-fb7c8408a9b7 > tn2.json

curl -k -u '<user>:<password>' https://nsxmgr/api/v1/transport-nodes/d7cec2c9-
b776-4829-beea-1258d8b8d59b > tn3.json
```

h Migrate the NSX Manager from the previous port to the newly created unblocked logical port on the **Edge Management Segment**. The `VIF-ID` value is the attachment ID of the port created previously for the NSX Manager.

The following parameters are needed to migrate NSX Manager:

- Transport node ID
- Transport node configuration
- NSX Manager VNIC hardware index
- NSX Manager VIF ID

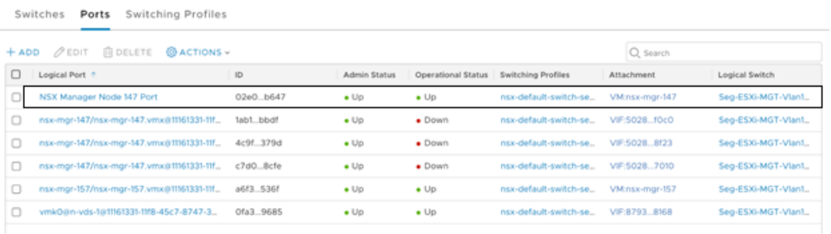
The API command to migrate NSX Manager to the newly created unblocked port is:

```
/api/v1/transport-nodes/<TN-ID>?vnic=<VNIC-ID>&vif=<VIF-ID>
```

For example,

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -k -X PUT -u 'admin:VMware1!
VMware1!' -H 'Content-Type:application/json' -d @mgr.json 'https://
localhost/api/v1/transport-nodes/11161331-11f8-45c7-8747-34e7218b687f?
vnic=5028d756-d36f-719e-3db5-7ae24aa1d6f3:4000&vif=nsxmgr-port-147'
```

i Ensure that the statically created logical port is `Up`.



□	Logical Port ↑	ID	Admin Status	Operational Status	Switching Profiles	Attachment	Logical Switch
□	NSX Manager Node 147 Port	02e0...b647	● Up	● Up	nsx-default-switch-se...	VM:nsx-mgr-147	Seg-ESXi-MGT-Vlan1...
□	nsx-mgr-147/nsx-mgr-147.vmx@11161331-11f...	1ab1...bbdf	● Up	● Down	nsx-default-switch-se...	VIF:5028...f0c0	Seg-ESXi-MGT-Vlan1...
□	nsx-mgr-147/nsx-mgr-147.vmx@11161331-11f...	4c9f...379d	● Up	● Down	nsx-default-switch-se...	VIF:5028...8f23	Seg-ESXi-MGT-Vlan1...
□	nsx-mgr-147/nsx-mgr-147.vmx@11161331-11f...	c7d0...8cfe	● Up	● Down	nsx-default-switch-se...	VIF:5028...7010	Seg-ESXi-MGT-Vlan1...
□	nsx-mgr-157/nsx-mgr-157.vmx@11161331-11f...	a6f3...536f	● Up	● Up	nsx-default-switch-se...	VM:nsx-mgr-157	Seg-ESXi-MGT-Vlan1...
□	vmk0@n-vds-1@11161331-11f8-45c7-8747-3...	0fa3...9685	● Up	● Up	nsx-default-switch-se...	VIF:8793...8168	Seg-ESXi-MGT-Vlan1...

j Repeat the preceding steps on every NSX Manager in the cluster.

VLAN Micro-Segmentation

VLAN micro-segmentation walks you through selecting clusters, assigning uplinks, and migrating VMkernal (VMK) ports.

The simplified VLAN micro-segmentation workflow includes:

- A transport node profile is created and assigned to the selected cluster. The profile name can be edited after deployment.
- Users select the uplink to physical NICs (pNICs) mapping for each cluster. Both vSphere 7, and the NSX-T Virtual Distributed Switch (N-VDS) are supported.

- Optional - NSX-T migrates selected VMkernal (VMK) ports to the N-VDS that is automatically created. The user specifies a VLAN segment for each of the VMK interfaces. Power off all virtual machines before migration.
- For ESXi hosts that are version 6.7 and earlier, NVDS is created and the uplink to physical NICs mapping is displayed.
- If you have both version 7.0 ESXi hosts and version 7.0 VDS, the uplink mapping is displayed. These uplinks are then mapped onto the VDS.
- VMkernal migration is not supported with VDS.

Before going through the wizard for VLAN backed micro-segmentation, you must have a compute manager.

1 Navigate to **System > Get Started**. To prepare clusters for micro-segmentation using VLAN, click **Get Started - Prepare Clusters for VLAN Micro-segmentation**.

2 Select the cluster you want to prepare from the list of available clusters. Only clusters which do not have a transport node profile applied are listed. Expand each cluster to view the hosts it contains. No stand-alone hosts are listed.

3 To filter the cluster by cluster name, host IP address, host name, or host version, click the filter icon on the right of the screen.

4 Click **Next**.

5 Select the physical NICs (pNICs) that are assigned as uplinks for the N-VDS, or VDS on each cluster. pNICs that are common across the cluster are listed. Both vSphere 7 and VDS are supported.

6 Click **Next**.

7 (Optional) To configure the interfaces for VMkernal migration, where virtual NICs are migrated to VLAN segments, click **Select**. Power off all virtual machines before migration.

8 (Optional) Select an existing segment, or create a segment by entering a segment name and the VLAN ID.

9 (Optional) Click **Apply**. The segment is automatically mapped to the VMkernal.

10 Click **Finish**.

Host Profile integration with NSX-T

11

Integrate host profiles extracted from an ESXi host with NSX-T to deploy ESXi and NSX-T VIBs on stateful and stateless servers.

This chapter includes the following topics:

- Auto Deploy Stateless Cluster
- Stateful Servers

Auto Deploy Stateless Cluster

Stateless hosts do not persist configuration, so they need an auto-deploy server to provide the required start files when hosts power on.

This section helps you to set up a stateless cluster using vSphere Auto Deploy and NSX-T Transport Node Profile to reprovision a host with a new image profile that contains a different version of ESXi and NSX-T. Hosts that are set up for vSphere Auto Deploy use an auto-deploy server and vSphere host profiles to customize hosts. These hosts can also be set up for NSX-T Transport Node Profile to configure NSX-T on the hosts.

So, a stateless host can be set up for vSphere Auto Deploy and NSX-T Transport Node Profile to reprovision a host with a custom ESXi and NSX-T version.

High-Level Tasks to Auto Deploy Stateless Cluster

High-level tasks to auto deploy a stateless cluster.

The high-level tasks to set up an auto deploy stateless cluster are:

1 Prerequisites and Supported Versions. See Prerequisites and Supported Versions.

2 (Reference host) Create a Custom Image Profile. See Create a Custom Image Profile for Stateless Hosts.

3 (Reference and Target hosts) Associate the Custom Image Profile. See Associate the Custom Image with the Reference and Target Hosts.

4 (Reference host) Set up Network Configuration in ESXi. See Set Up Network Configuration on the Reference Host.

5 (Reference host) Configure as a Transport Node in NSX. See Configure the Reference Host as a Transport Node in NSX-T.

6 (Reference host) Extract and Verify Host Profile. See Extract and Verify the Host Profile.

7 (Reference and Target hosts) Verify the Host Profile Association with Stateless Cluster. See Verify the Host Profile Association with Stateless Cluster.

8 (Reference host) Update Host Customization. See Update Host Customization.

9 (Target hosts) Trigger Auto Deployment. See Trigger Auto Deployment on Target Hosts.

   a Before applying Transport Node Profile. See Reboot Hosts Before Applying TNP.

   b Apply Transport Node Profile. See Apply TNP on Stateless Cluster.

   c After applying Transport Node Profile. See Reboot Hosts After Applying TNP.

10 Troubleshoot Host Profile and Transport Node Profile. See Troubleshoot Host Profile and Transport Node Profile.

Prerequisites and Supported Versions

Prerequisites and supported ESXi and NSX-T versions.

Supported Workflows

- With Image Profile and HostProfile

Prerequisites

- Only homogeneous clusters (all hosts within a cluster must be either stateless or stateful) are supported.
- Image builder service must be enabled.
- Auto deploy service must be enabled.

Supported NSX and ESXi Versions

Supported EXSi Version	ESXi 67ep6	ESXi 67u2	ESXi 67u3	ESXi 67ep7	ESXi 7.0.0.1
NSX-T Data Center 2.4	Yes	Yes	No	No	No
NSX-T Data Center 2.4.1	Yes	Yes	No	No	No
NSX-T Data Center 2.4.2	Yes	Yes	No	No	No
NSX-T Data Center 2.4.3	Yes	Yes	No	No	No
NSX-T Data Center 2.5	Yes	Yes	Yes	Yes	No
NSX-T Data Center 2.5.1	Yes	Yes	Yes	Yes	No
NSX-T Data Center3.0	Yes	Yes	Yes	Yes	Yes

Create a Custom Image Profile for Stateless Hosts

In your data center, identify a host to be prepared as the reference host.

The first time the reference host starts up, ESXi associates the default rule with the reference host. In this procedure, we are adding a custom image profile (ESXi and NSX VIBs) and associate the reference host with the new custom image. An image profile with the NSX-T image significantly reduces the installation time. The same custom image is associated with the target hosts in the stateless cluster.

Note Alternatively, you can add only an ESXi image profile to the reference and target stateless cluster. The NSX-T VIBs are downloaded when you apply the transport node profile on the stateless cluster. See Add a Software Depot.

Prerequisites

Ensure that the auto-deploy service and image builder service are enabled. See Using vSphere Auto Deploy to Reprovision Hosts.

Procedure

1 To import NSX-T packages, create a software depot.

2 Download the `nsx-lcp` packages.

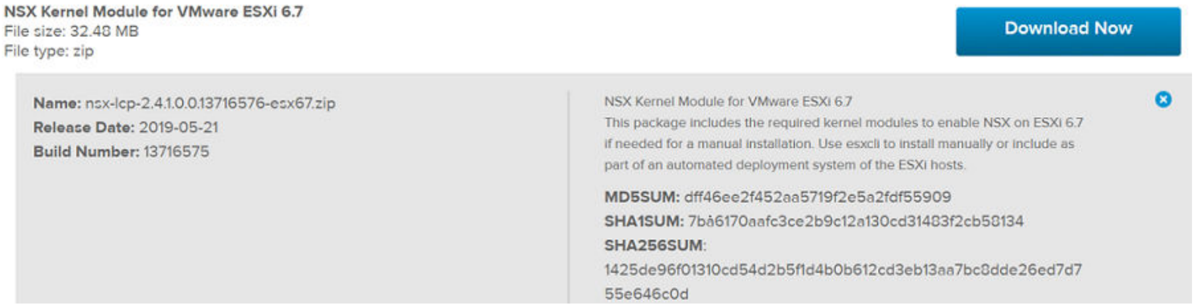
   a Log in to `https://my.vmware.com`.

   b On the Download VMware NSX-T Data Center page, select the NSX-T version.

   c In the Product Downloads page, search NSX-T Kernel Modules for a specific VMware ESXi version.

   d Click **Download Now** to begin downloading the `nsx-lcp` package.

   e Import `nsx-lcp` packages into the software depot.



NSX Kernel Module for VMware ESXi 6.7
File size: 32.48 MB
File type: zip

Name: nsx-lcp-2.4.1.0.0.13716576-esx67.zip
Release Date: 2019-05-21
Build Number: 13716575

NSX Kernel Module for VMware ESXi 6.7
This package includes the required kernel modules to enable NSX on ESXi 6.7 if needed for a manual installation. Use esxcli to install manually or include as part of an automated deployment system of the ESXi hosts.

MD5SUM: dff46ee2f452aa5719f2e5a2fdf55909
SHA1SUM: 7bà6170aafc3ce2b9c12a130cd31483f2cb58134
SHA256SUM:
1425de96f01310cd54d2b5f1d4b0b612cd3eb13aa7bc8dde26ed7d7
55e646c0d

3 Create another software depot to import ESXi packages.

   The vSphere Web Client displays two depots created on the reference host.

4 Create a custom software depot to clone previously imported ESXi image and `nsx-lcp` packages.

   a Select the ESXi Image profile from the ESXi software depot created in the earlier step.

   b Click **Clone**.

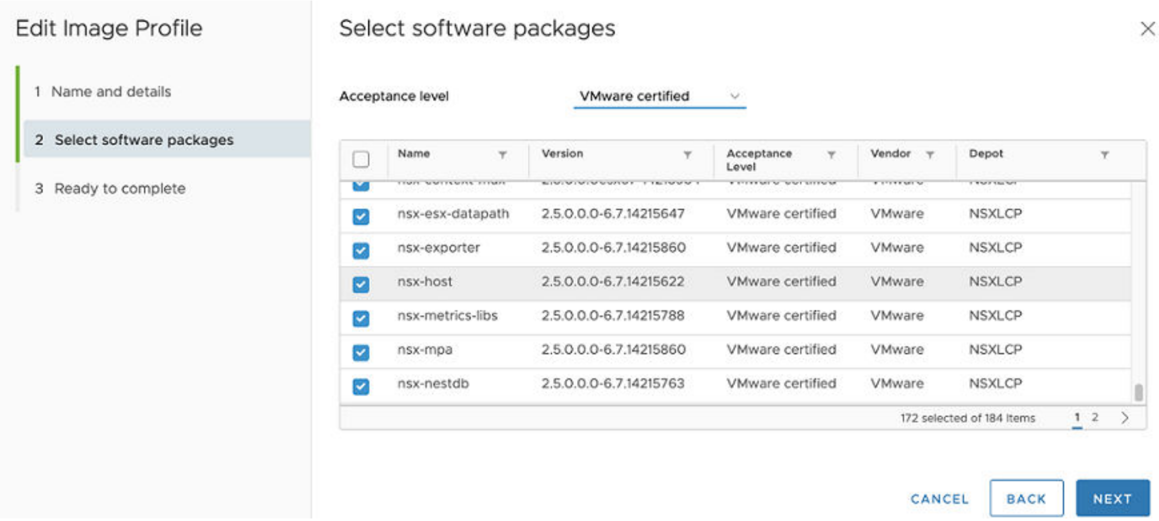
c In the Clone Image Profile wizard, enter a name for the custom image to be created.

d Select the custom software depot where the cloned image (ESXi) must be available.

e In the Select software packages window, select the Acceptance level to **VMware Certified**. The ESXi VIBs are preselected.

f Identify and select the NSX-T packages manually from the list of packages and click **Next**.

g In the Ready to complete screen, verify the details and click **Finish** to create the cloned image containing ESXi and NSX-T packages into the custom software depot.



Edit Image Profile

1 Name and details

2 Select software packages

3 Ready to complete

Select software packages

Acceptance level: VMware certified

☐	Name	Version	Acceptance Level	Vendor	Depot
☑	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
☑	nsx-esx-datapath	2.5.0.0.0-6.7.14215647	VMware certified	VMware	NSXLCP
☑	nsx-exporter	2.5.0.0.0-6.7.14215860	VMware certified	VMware	NSXLCP
☑	nsx-host	2.5.0.0.0-6.7.14215622	VMware certified	VMware	NSXLCP
☑	nsx-metrics-libs	2.5.0.0.0-6.7.14215788	VMware certified	VMware	NSXLCP
☑	nsx-mpa	2.5.0.0.0-6.7.14215860	VMware certified	VMware	NSXLCP
☑	nsx-nestdb	2.5.0.0.0-6.7.14215763	VMware certified	VMware	NSXLCP

172 selected of 184 Items

What to do next

Associate the custom image with the reference and target hosts. See Associate the Custom Image with the Reference and Target Hosts.

Associate the Custom Image with the Reference and Target Hosts

To start the reference host and target hosts with the new custom image containing ESXi and NSX packages, associate the custom image profile.

At this point in the procedure, the custom image is only being associated to the reference and target hosts but NSX installation does not happen.

Important Perform this custom image association procedure on both reference and target hosts.

Prerequisites

Procedure

1 On the ESXi host, navigate to **Menu** > **Auto Deploy** > **Deployed Hosts**.

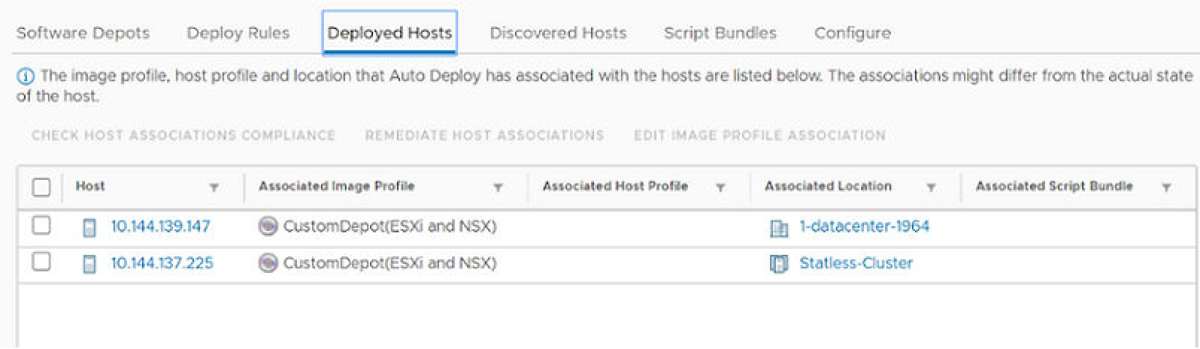
2 To associate the custom image profile with a host, select the custom image.

3 Click **Edit Image Profile Association**.

4 In the Edit Image Profile Association wizard, click **Browse** and select the custom depot and select the custom image profile.

5 Enable **Skip image profile signature check**.

6 Click **Ok**.


Software Depots
Deploy Rules
Deployed Hosts
Discovered Hosts
Script Bundles
Configure
CHECK HOST ASSOCIATIONS COMPLIANCE
REMEDIATE HOST ASSOCIATIONS
EDIT IMAGE PROFILE ASSOCIATION

ⓘ The image profile, host profile and location that Auto Deploy has associated with the hosts are listed below. The associations might differ from the actual state of the host.

□	Host	Associated Image Profile	Associated Host Profile	Associated Location	Associated Script Bundle
□	10.144.139.147	CustomDepot(ESXi and NSX)		1-datacenter-1964	
□	10.144.137.225	CustomDepot(ESXi and NSX)		Statless-Cluster	

Results

What to do next

Set up Network Configuration on the Reference Host. See Set Up Network Configuration on the Reference Host.

Set Up Network Configuration on the Reference Host

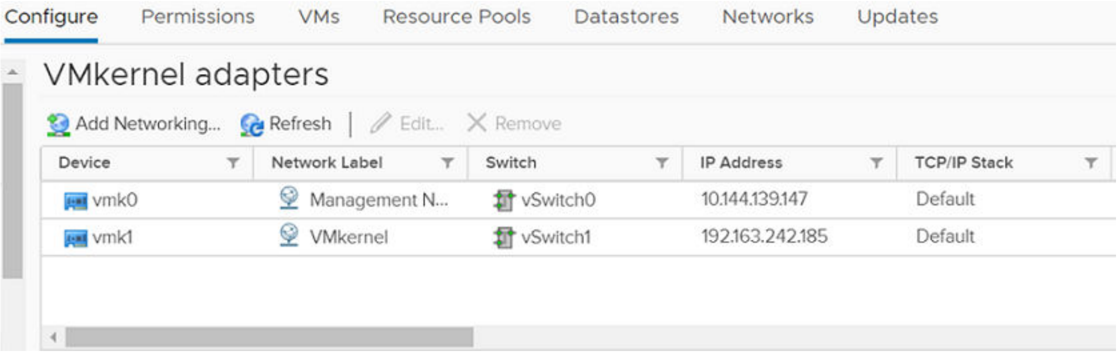
On the reference host, a standard switch with a VMkernel adapter is created to set up the network configuration on ESXi.

This network configuration is captured in the host profile which is extracted from the reference host. During a stateless deployment, the host profile replicates this network configuration setting on each target host.

Procedure

1 On the ESXi host, configure a vSphere Standard Switch (VSS) or Distributed Virtual switch (DVS) by adding a VMkernel adapter.

2 Verify that the newly added VSS/DVS switch is displayed in the VMkernel adapters page.



Device	Network Label	Switch	IP Address	TCP/IP Stack
vmk0	Management N...	vSwitch0	10.144.139.147	Default
vmk1	VMkernel	vSwitch1	192.163.242.185	Default

What to do next

Configure the Reference Host as a Transport Node in NSX-T. See Configure the Reference Host as a Transport Node in NSX-T.

Configure the Reference Host as a Transport Node in NSX-T

After the reference host is associated with the custom image profile and configured with a VSS switch, set up the reference host as a transport node in NSX-T.

Procedure

1 From a browser, log in to NSX-T at https://<NSXManager_IPaddress>.

2 To locate the reference host, navigate to **System** -> **Nodes** -> **Host Transport Node**.

3 Create a VLAN transport zone to define the span of the virtual network. The span is defined by attaching N-VDS switches to the transport zone. Based on this attachment, N-VDS can access segments defined within the transport zone. See Create a Transport Zone.

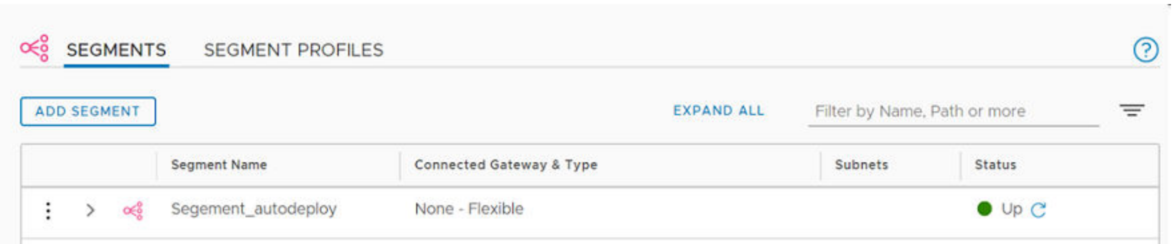
4 Create a VLAN segment on the transport zone. The created segment is displayed as a logical switch.

   a Navigate to **Networking** -> **Segments**.

   b Select the transport zone to attach the segment.

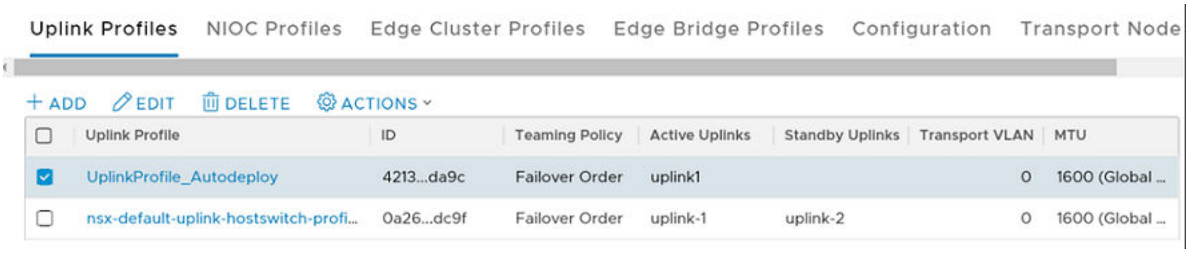
   c Enter VLAN ID.

   d Click **Save**.



Segment Name	Connected Gateway & Type	Subnets	Status
Segement_autodeploy	None - Flexible		● Up

5 Create an uplink profile for the reference host that defines how an N-VDS or VDS switch connects to the physical network. See, Create an Uplink Profile.



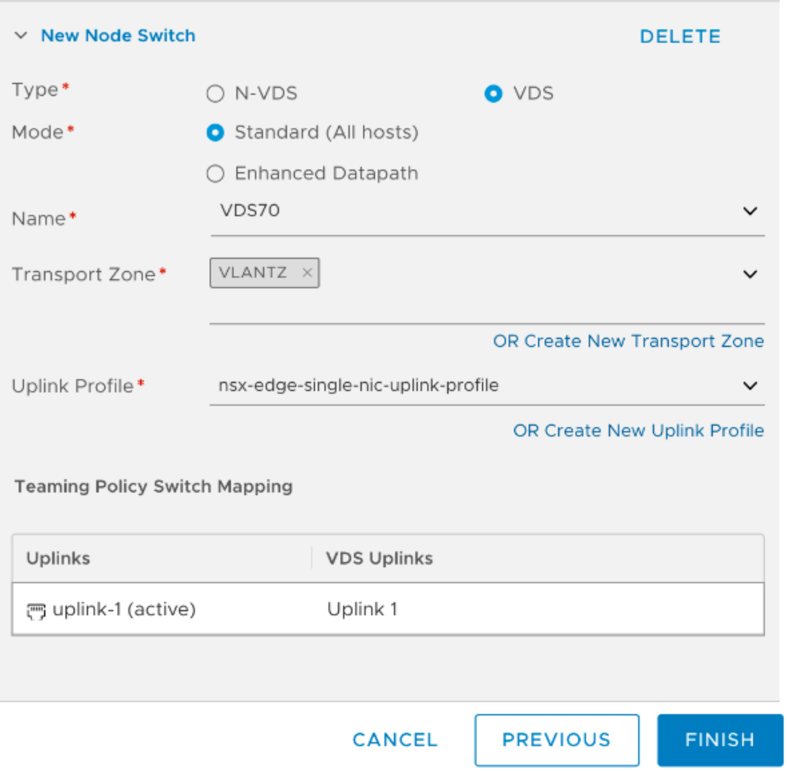
□	Uplink Profile	ID	Teaming Policy	Active Uplinks	Standby Uplinks	Transport VLAN	MTU
☑	UplinkProfile_Autodeploy	4213...da9c	Failover Order	uplink1		0	1600 (Global ...
□	nsx-default-uplink-hostswitch-profi...	0a26...dc9f	Failover Order	uplink-1	uplink-2	0	1600 (Global ...

6 Configure the reference host as a transport node. See Configure a Managed Host Transport Node.

   a In the Host Transport Node page, select the reference host.

   b (On a N-VDS switch) Click Configure NSX and select the previously created transport zone, N-VDS, uplink profile.

c (On a VDS switch) Click Configure NSX and select the previously created transport zone, VDS, uplink profile.



New Node Switch

DELETE

Type* ○ N-VDS ● VDS

Mode* ● Standard (All hosts) ○ Enhanced Datapath

Name* VDS70

Transport Zone* VLANTZ ×

OR Create New Transport Zone

Uplink Profile* nsx-edge-single-nic-uplink-profile

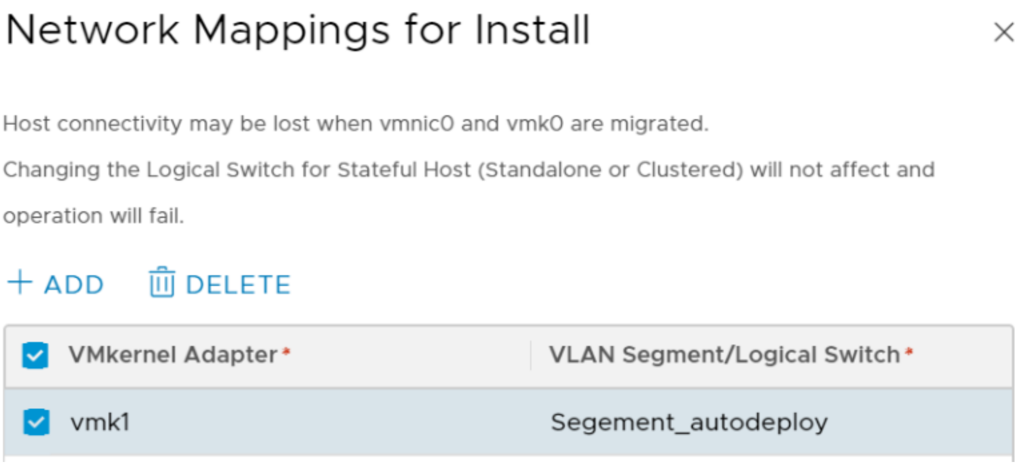
OR Create New Uplink Profile

Teaming Policy Switch Mapping

Uplinks	VDS Uplinks
uplink-1 (active)	Uplink 1

7 In the Network Mappings to Install section, click **Add Mapping** to add the VMkernel to Segment/ Logical switch mapping.

Note On a VDS switch, VMkernel adapter migration is not supported.



Network Mappings for Install

Host connectivity may be lost when vmnic0 and vmk0 are migrated.

Changing the Logical Switch for Stateful Host (Standalone or Clustered) will not affect and operation will fail.

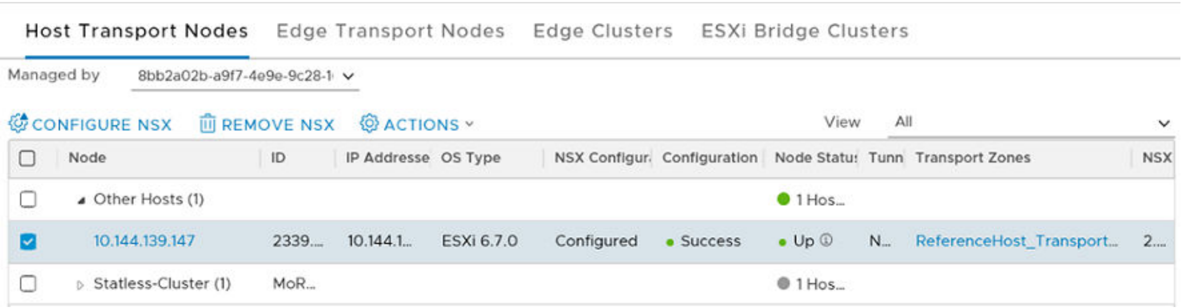
☑ VMkernel Adapter*	VLAN Segment/Logical Switch*
☑ vmk1	Segement_autodeploy

8 Click **Finish** to begin installation of NSX-T on the reference host.

(On a VDS switch) After installation, configuration status of the reference host is displayed as `Success`. In the vCenter Server, the VDS switch is displayed as NSX switch.

(On an N-VDS switch) During installation, VMkernel adapters and physical NICs are migrated from a VSS or DVS switch to an N-VDS switch. After installation, configuration status of the reference host is displayed as `Success`.

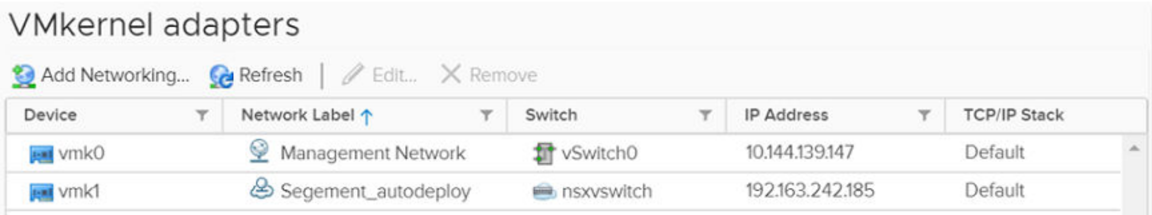
Note The reference host is listed under Other Hosts.



☐	Node	ID	IP Addresse	OS Type	NSX Configur	Configuration	Node Statu	Tunn	Transport Zones	NSX
☐	Other Hosts (1)						● 1 Hos...			
☑	10.144.139.147	2339....	10.144.1...	ESXi 6.7.0	Configured	● Success	● Up ⓘ	N...	ReferenceHost_Transport...	2....
☐	Statless-Cluster (1)	MoR...					● 1 Hos...			

9 In vCenter Server, verify that the PNICs and VMkernels adapters on the VSS switch are migrated and connected to the N-VDS switch.

Note On a VDS switch, VMkernel adapter and physical NIC migration is not supported. Attaching a VMkernel adapter to an NSX Distributed Virtual port group is not supported.



Device	Network Label ↑	Switch	IP Address	TCP/IP Stack
vmk0	Management Network	vSwitch0	10.144.139.147	Default
vmk1	Segement_autodeploy	nsxvswitch	192.163.242.185	Default

What to do next

Extract and Verify the Host Profile. See Extract and Verify the Host Profile.

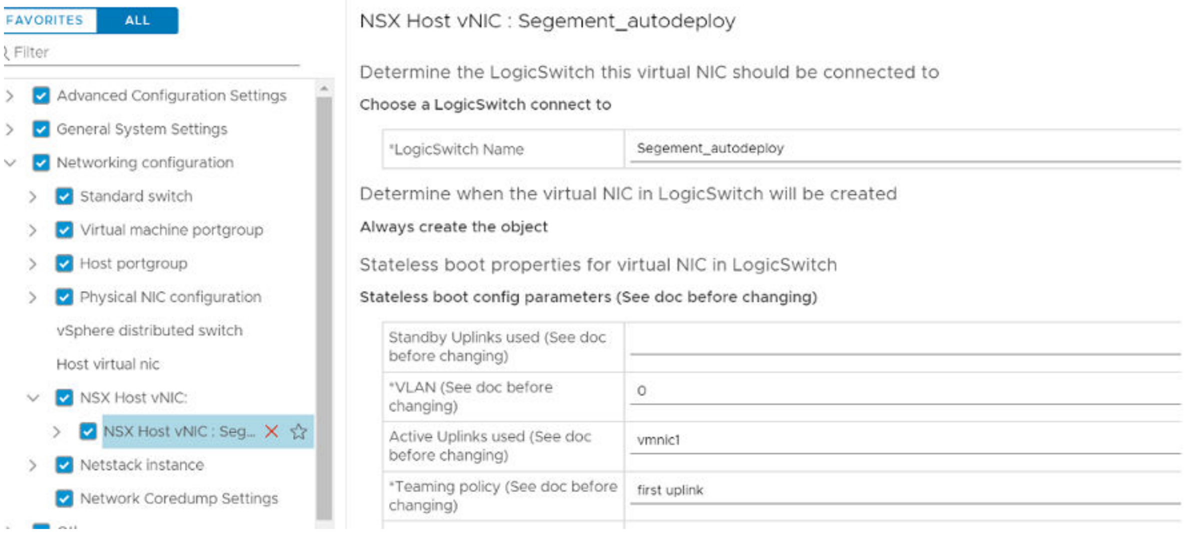
Extract and Verify the Host Profile

After you extract the host profile from the reference host, verify the NSX-T configuration extracted in the host profile. It consists of ESXi and NSX-T configuration that is applied to target hosts.

Procedure

1 To extract the host profile, Extract and Configure Host Profile from the Reference Host.

2 Verify the NSX configuration in the extracted host profile.



NSX Host vNIC : Segement_autodeploy

Determine the LogicSwitch this virtual NIC should be connected to

Choose a LogicSwitch connect to

*LogicSwitch Name	Segement_autodeploy

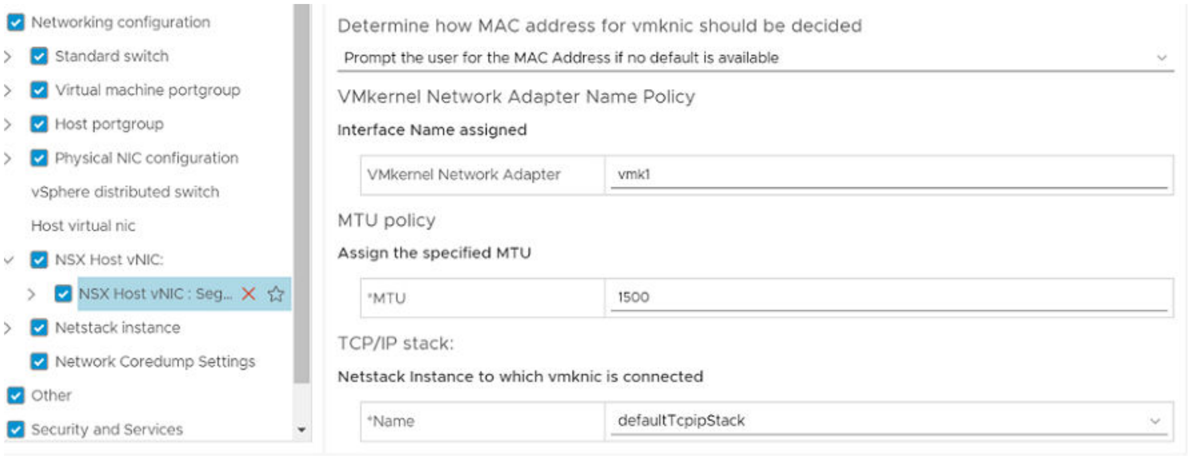
Determine when the virtual NIC in LogicSwitch will be created

Always create the object

Stateless boot properties for virtual NIC in LogicSwitch

Stateless boot config parameters (See doc before changing)

Standby Uplinks used (See doc before changing)	
*VLAN (See doc before changing)	0
Active Uplinks used (See doc before changing)	vmnic1
*Teaming policy (See doc before changing)	first uplink



Determine how MAC address for vmknic should be decided

Prompt the user for the MAC Address if no default is available

VMkernel Network Adapter Name Policy

Interface Name assigned

VMkernel Network Adapter	vmk1

MTU policy

Assign the specified MTU

*MTU	1500

TCP/IP stack:

Netstack Instance to which vmknic is connected

*Name	defaultTcpipStack

Results

The host profile contains configuration related to ESXi and NSX as the host was prepared for both environments.

What to do next

Verify the Host Profile Association with Stateless Cluster. See Verify the Host Profile Association with Stateless Cluster.

Verify the Host Profile Association with Stateless Cluster

To prepare the target stateless cluster with ESXi and NSX configuration, associate the host profile extracted from the reference host to the target stateless cluster.

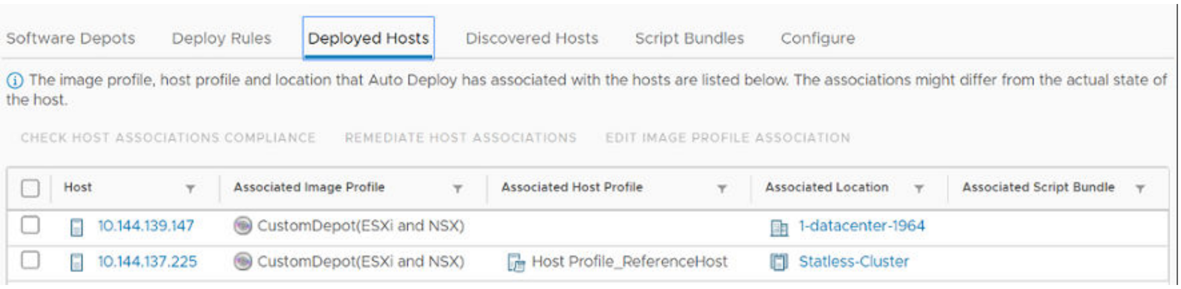
Without the host profile associated to the stateless cluster, new nodes joining the cluster cannot be auto deployed with ESXi and NSX VIBs.

Procedure

1 Attach or Detach Host Profile to Stateless Cluster. See Attach or Detach Entities from a Host Profile.

2 In the Deployed Hosts tab, verify that the existing stateless host is associated with the correct image and associated with the host profile.

3 If the host profile association is missing, select the target host and click Remediate Host Associations to force update the image and host profile to the target host.


Software Depots
Deploy Rules
Deployed Hosts
Discovered Hosts
Script Bundles
Configure
CHECK HOST ASSOCIATIONS COMPLIANCE
REMEDIATE HOST ASSOCIATIONS
EDIT IMAGE PROFILE ASSOCIATION

ⓘ The image profile, host profile and location that Auto Deploy has associated with the hosts are listed below. The associations might differ from the actual state of the host.

□	Host	Associated Image Profile	Associated Host Profile	Associated Location	Associated Script Bundle
□	10.144.139.147	CustomDepot(ESXi and NSX)		1-datacenter-1964	
□	10.144.137.225	CustomDepot(ESXi and NSX)	Host Profile_ReferenceHost	Statless-Cluster	

What to do next

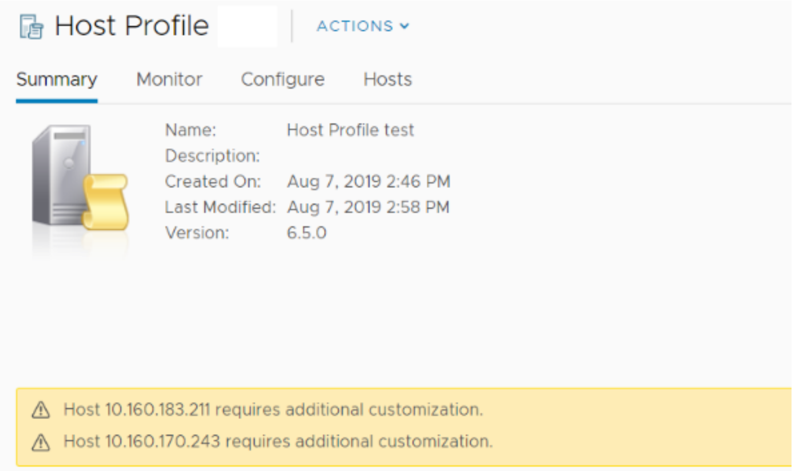
Update Host Customization. See Update Host Customization.

Update Host Customization

After the attaching the host profile to the target cluster, additional custom entries might be required on the host to successfully auto deploy the ESXi and NSX-T packages on it.

Procedure

1 After attaching the host profile to the target cluster, if the hosts are not updated with custom values, the system displays the following message.

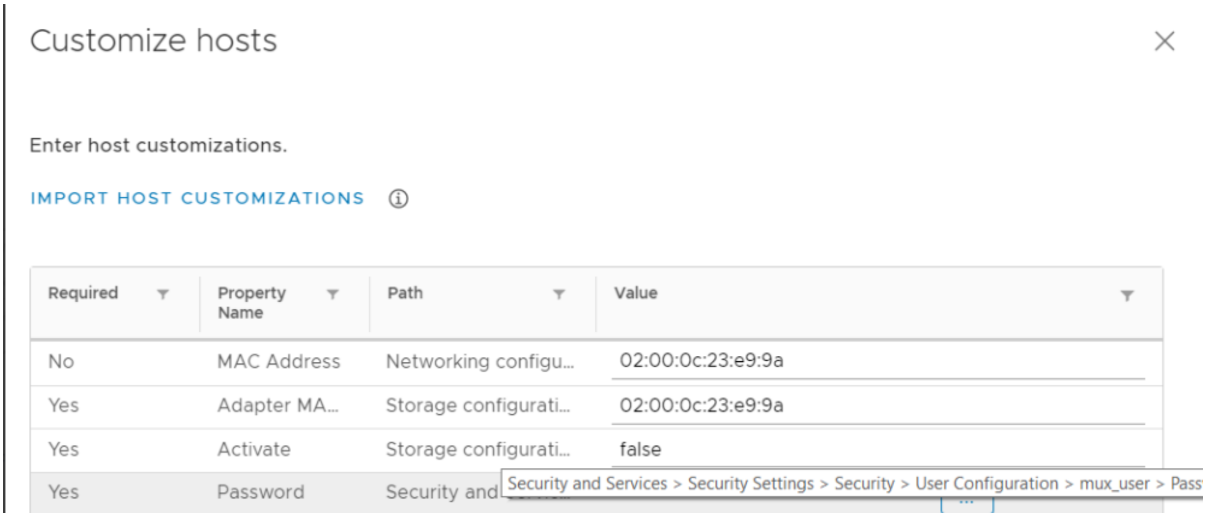


Name: Host Profile test
Description:
Created On: Aug 7, 2019 2:46 PM
Last Modified: Aug 7, 2019 2:58 PM
Version: 6.5.0

⚠ Host 10.160.183.211 requires additional customization.
⚠ Host 10.160.170.243 requires additional customization.

2 To update host customizations, navigate to the host profile, click **Actions** -> **Edit Host Customizations**.

3 For ESXi versions 67ep6, 67ep7, 67u2, enter the MUX user password.



Customize hosts

Enter host customizations.

Required	Property Name	Path	Value
No	MAC Address	Networking configu...	02:00:0c:23:e9:9a
Yes	Adapter MA...	Storage configurati...	02:00:0c:23:e9:9a
Yes	Activate	Storage configurati...	false
Yes	Password	Security and	...

Security and Services > Security Settings > Security > User Configuration > mux_user > Pass

4 Verify that all the required fields are updated with appropriate values.

What to do next

Trigger Auto Deployment on Target Hosts. See Trigger Auto Deployment on Target Hosts.

Trigger Auto Deployment on Target Hosts

When a new node is added to the cluster, it needs to be manually rebooted for the ESXi and NSX-T VIBs to be configured.

Note Only applies to stateless hosts.

There are two ways to prepare hosts to trigger auto-deployment of ESXi and NSX-T VIBs to be configured.

- Reboot hosts before applying TNP to the stateless cluster.
- Reboot hosts after applying TNP to the stateless cluster.

If you want to migrate VMkernel adapters when installing NSX-T on the hosts, see:

- Scenarios When the Stateless Host Is in the Target Cluster
- Scenarios When the Stateless Host Is Outside of the Target Cluster

What to do next

Reboot hosts before applying TNP to the stateless cluster. See Reboot Hosts Before Applying TNP.

Reboot Hosts Before Applying TNP

Only applies to stateless hosts. In this scenario, the transport node profile is not applied to the stateless cluster, which means that NSX-T is not installed and configured on the target host.

Procedure

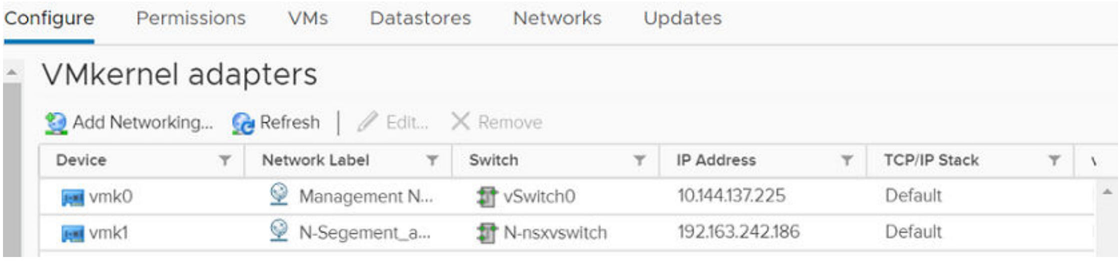
1 Reboot hosts.

The target host starts with the ESXi image. After starting, the target host remains in maintenance mode until the TNP profile is applied to the target host and NSX-T installation is complete. Profiles are applied on hosts in the following order:

Profiles are applied on hosts in the following order.

- Image profile is applied to the host.
- Host profile configuration is applied to the host.
- NSX-T configuration is applied to the host.

2 On the ESXi host, the VMkernel adapter is attached to a temporary segment named <N-LogicalSegment> because the host is not yet a transport node. After NSX-T is installed the temporary switch is replaced with the actual N-VDS switch and logical segment.



Device	Network Label	Switch	IP Address	TCP/IP Stack
vmk0	Management N...	vSwitch0	10.144.137.225	Default
vmk1	N-Segement_a...	N-nsxvswitch	192.163.242.186	Default

ESXi VIBs are applied to all the rebooted hosts. A temporary NSX switch in an ESXi host. When TNP is applied to the hosts, the temporary switch is replaced by the actual NSX-T switch.

What to do next

Apply TNP to the stateless cluster. See Apply TNP on Stateless Cluster.

Apply TNP on Stateless Cluster

NSX-T configuration and installation only happens on the target hosts when TNP is applied to the cluster.

Procedure

1 Note down the settings extracted in the Host Profile from the reference host. The corresponding entities in the TNP profile must have the same value. For example, the N-VDS name used in the Host Profile and TNP must be the same.

For more information on extracted host profile settings, see Extract and Verify the Host Profile.

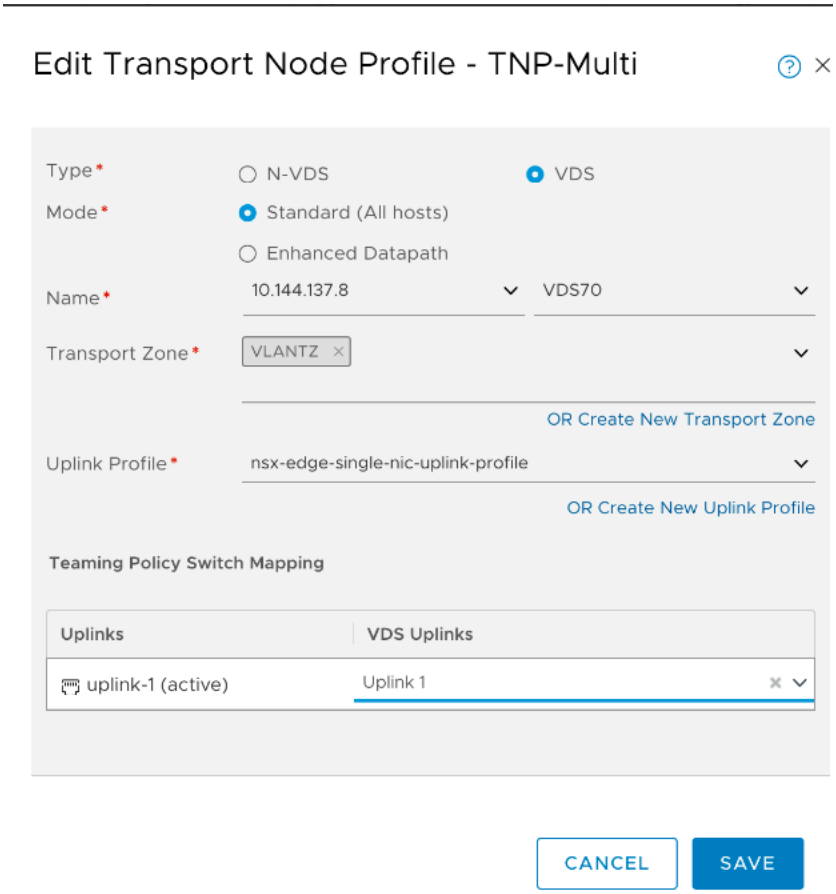
2 Add a TNP. See Add a Transport Node Profile.

3 Add a TNP by entering all required field. See Add a Transport Node Profile.

Ensure that values of the following parameters are the same on both the new TNP profile and the existing Host Profile.

Note On a VDS switch, migration of VMkernel adapters and physical NIC migration is not supported.

- Transport Zone: Ensure transport zone referenced in Host Profile and TNP is the same.
- N-VDS Name: Ensure N-VDS name referenced in Host Profile and TNP is the same.
- Uplink Profile: Ensure uplink profile referenced in Host Profile and TNP is the same.
- Teaming Policy:
  - (On a VDS switch) In vCenter Server, when creating VDS uplinks, verify the NIC used in the Host Profile and map that physical NIC to the VDS uplink. In NSX-T, you map NSX-T uplinks to VDS uplinks. So, verify the configuration on the VDS switch in vCenter Server.
  - (On an N-VDS switch) When mapping a physical NIC to an uplink profile, first verify the NIC used in the Host Profile and map that physical NIC to the uplink profile.
- Network mapping for install: When mapping network during installation, first verify the VMkernel to logical switch mapping on the Host Profile and add the same mapping in TNP.
- Network mapping for uninstall: When mapping network during uninstallation, first verify the VMkernel to VSS/DVS switch mapping on the Host Profile and add the same mapping in TNP.



Edit Transport Node Profile - TNP-Multi

Type* ○ N-VDS ● VDS

Mode* ● Standard (All hosts) ○ Enhanced Datapath

Name* 10.144.137.8 VDS70

Transport Zone* VLANTZ

Uplink Profile* nsx-edge-single-nic-uplink-profile

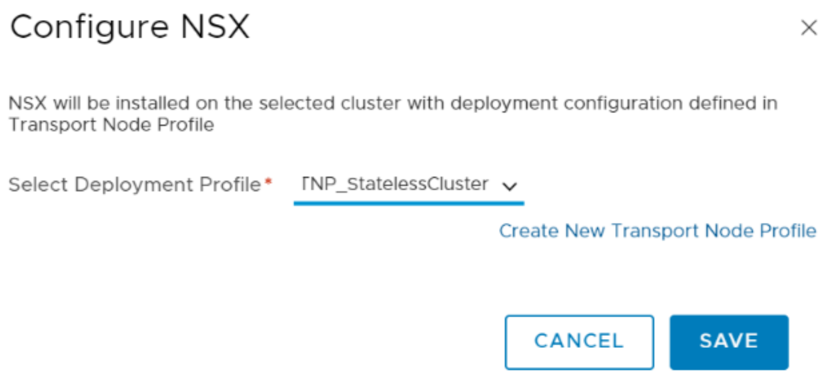
Teaming Policy Switch Mapping

Uplinks	VDS Uplinks
uplink-1 (active)	Uplink 1

After applying TNP on target nodes, if the TNP configuration does not match Host Profile configuration, the node might not come up because of compliance errors.

4 Verify that the TNP profile is successfully created.

5 Apply TNP profile to the target cluster and click **Save**.



Configure NSX

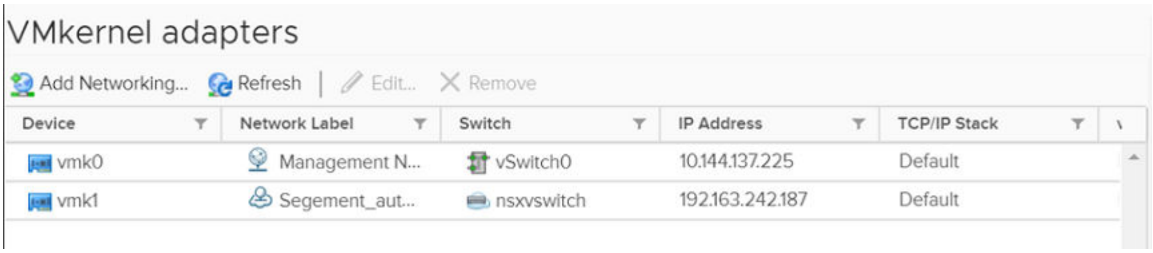
NSX will be installed on the selected cluster with deployment configuration defined in Transport Node Profile

Select Deployment Profile* ΓNP_StatelessCluster

6 Verify that the TNP profile is successfully applied to the target cluster. It means that NSX is successfully configured on all nodes of the cluster.

7 In vSphere, verify that the physical NICs or VMkernel adapters are attached to the N-VDS switch.

Note On a VDS switch, VMkernel adapter migration is not supported.



Device	Network Label	Switch	IP Address	TCP/IP Stack
vmk0	Management N...	vSwitch0	10.144.137.225	Default
vmk1	Segement_aut...	nsxvswitch	192.163.242.187	Default

8 In NSX, verify that the ESXi host is configured successfully as a transport node.

What to do next

Alternatively, you can reboot a target host after applying TNP to the cluster. See Reboot Hosts After Applying TNP.

Reboot Hosts After Applying TNP

Only applies to stateless hosts. When a new node is added to the cluster, manually reboot the node for the ESXi and NSX-T packages to be configured on it.

Procedure

1 Apply TNP to the stateless cluster that is already prepared with host profile. See Create and Apply TNP on Stateless Cluster.

2 Reboot hosts.

After applying TNP profile to the stateless cluster, when you reboot any new node joining the cluster that node is automatically configured with NSX-T on the host.

What to do next

Ensure that you reboot any new node joining the cluster to automatically deploy and configure ESXi and NSX-T on the rebooted node.

To troubleshoot issues related to host profile and transport node profile when configuring auto-deployment, see Troubleshoot Host Profile and Transport Node Profile.

Scenarios When the Stateless Host Is in the Target Cluster

This section discusses use cases when a stateless host exists in the target cluster.

Important On a stateless target host:

- (On an N-VDS switch) Migration of vmk0 adapter from VSS/DVS to N-VDS is not supported on NSX-T 2.4 and NSX-T 2.4.1.
- (On an N-VDS switch) Migration of vmk0 adapter from VSS/DVS to N-VDS is supported on NSX-T 2.5.
- (On a VDS switch) Migration of VMkernel adapters is not supported.

Target Host	Reference Host Configuration	Steps To Auto Deploy Target Hosts
Target host has vmk0 adapter configured.	The host profile extracted from the reference host has vmk0 configured on an N-VDS switch. In NSX-T, TNP has only vmk0 migration mapping configured.	1 Attach the host profile to the target host. The vmk0 adapter is attached to a vSwitch. 2 Update host customizations, if required. 3 Reboot the host. The host profile is applied to the host. vmk0 is attached to a temporary switch. 4 Apply TNP. The vmk0 adapter migrates to N-VDS. The target host is successfully deployed with ESXi and NSX-T VIBs.
Target host has vmk0 adapter configured.	The host profile extracted from the reference host has vmk0 on vSwitch and vmk1 is on an N-VDS switch. In NSX-T, TNP has only vmk1 migration mapping configured.	1 Attach the host profile to the target host. The vmk0 adapter is attached to a vSwitch, but vmk1 is not realized on any switch. 2 Update host customizations, if required. 3 Reboot the host. vmk0 is attached to a vSwitch and vmk1 is attached to a temporary NSX switch. 4 Apply TNP. The vmk1 adapter migrates to N-VDS. 5 (optional) If the host remains non-compliant with the host profile, reboot the host to make the host compliant. The target host is successfully deployed with ESXi and NSX-T VIBs.

Target Host	Reference Host Configuration	Steps To Auto Deploy Target Hosts
Target host has vmk0 adapter configured.	The host profile extracted from the reference host has vmk0 is configured on a vSwitch and vmk1 is configured on an N-VDS switch. In NSX-T, TNP has vmk0 and vmk1 migration mappings configured.	1 Attach the host profile to the target host. The vmk0 adapter is attached to a vSwitch, but vmk1 is not realized on any switch. 2 Update host customizations, if required. 3 Reboot the host. The vmk0 adapter is attached to a vSwitch and vmk1 is attached to a temporary NSX switch. 4 Apply TNP. 5 (optional) If the host remains non-compliant with the host profile, reboot the host to make the host compliant. The target host is successfully deployed with ESXi and NSX-T VIBs.
Target host has vmk0 and vmk1 adapters configured.	The host profile extracted from the reference host has vmk0 on vSwitch and vmk1 configured on an N-VDS switch. In NSX-T, TNP has a vmk1 migration mapping configured.	1 Attach the host profile to the target host. The vmk0 and vmk1 adapters are attached to a vSwitch. 2 Update host customizations, if required. 3 Reboot the host. 4 Apply TNP. The vmk0 adapter is attached to a vSwitch and vmk1 is attached to an N-VDS switch. 5 (optional) If the host remains non-compliant with the host profile, reboot the host to make the host compliant. The target host is successfully deployed with ESXi and NSX-T VIBs.
Target host has vmk0 and vmk1 adapters configured.	The host profile extracted from the reference host has vmk0 and vmk1 configured on an N-VDS switch. In NSX-T, TNP has vmk0 and vmk1 migration mappings configured.	1 Attach the host profile to the target host. The vmk0 and vmk1 adapters are attached to a vSwitch. 2 Update host customizations, if required. 3 Reboot the host. 4 Apply TNP. The vmk0 and vmk1 are migrated to an N-VDS switch. The target host is successfully deployed with ESXi and NSX-T VIBs.

Scenarios When the Stateless Host Is Outside of the Target Cluster

This section discusses use cases when a stateless host exists outside of the target cluster.

Important On stateless hosts:

- (On an N-VDS switch) Migration of vmk0 adapter from VSS/DVS to N-VDS is not supported on NSX-T 2.4 and NSX-T 2.4.1.
- (On an N-VDS switch) Migration of vmk0 adapter from VSS/DVS to N-VDS is supported on NSX-T 2.5.
- (On a VDS switch) Migration of VMkernel adapters is not supported.

.

Target Host State	Reference Host Configuration	Steps To Auto Deploy Target Hosts
Host is in powered-off state (first-time start). It is later added to the cluster. The default auto-deploy rule is configured for the target cluster and associated with the host profile. The TNP is applied on the cluster.	The host profile extracted from the reference host has VMkernel adapter 0 (vmk0) on vSwitch and VMkernel adapter 1 (vmk1) configured on an N-VDS switch. In NSX-T, TNP has only vmk1 migration mapping configured.	1 Power on the host. After the host is powered on. ■ The host gets added to cluster. ■ The host profile is applied on the target host. ■ The vmk0 adapter is on vSwitch and vmk1 adapter is on a temporary switch. ■ TNP is triggered. ■ After TNP is applied to cluster, the vmk0 adapter is on vSwitch and vmk1 is migrated to the N-VDS switch. 2 (Optional) If the host remains non-compliant with the host profile, reboot the host to make the host compliant. The host is successfully deployed with ESXi and NSX-T VIBs.
Host is in powered-off state (first-time start). It is later added to the cluster. The default auto-deploy rule is configured for the target cluster and associated to the host profile. The TNP is applied on the cluster.	The host profile extracted from the reference host has VMkernel adapter 0 (vmk0) and VMkernel adapter 1 (vmk1) configured on an N-VDS switch. In NSX-T, TNP has vmk0 and vmk1 migration configured.	1 Power on the host. After the host is powered on. ■ The host gets added to cluster. ■ The host profile is applied on the target host. ■ The vmk0 and vmk1 adapters are on a temporary switch. ■ TNP is triggered. ■ After TNP is applied to cluster, the vmk0 and vmk1 are migrated to the N-VDS switch. The host is successfully deployed with ESXi and NSX-T VIBs.

Target Host State	Reference Host Configuration	Steps To Auto Deploy Target Hosts
Host is in powered-on state. It is later added to the cluster. The default auto-deploy rule is configured for the target cluster and associated to the host profile. Target host only has a vmk0 adapter configured on it.	The host profile extracted from the reference host has VMkernel adapter 0 (vmk0) on vSwitch and VMkernel adapter 1 (vmk1) configured on an N-VDS switch. In NSX-T, TNP has a vmk1 migration mapping configured.	1 Move the host to be part of the cluster. 2 Reboot the host. After the host is rebooted the host profile is applied on the target host. ■ The vmk0 adapter is attached to a vSwitch, whereas the vmk1 adapter is attached to a temporary NSX switch. ■ TNP is triggered. ■ vmk1 is migrated to the N-VDS switch. 3 (Optional) If the host remains non-compliant with the host profile, reboot the host to make the host compliant. The host is successfully deployed with ESXi and NSX-T VIBs.
Host is in powered-on state. It is later added to the cluster. The default auto-deploy rule is configured for the target cluster and associated to the host profile. Target host only has a vmk0 adapter configured on it.	The host profile extracted from the reference host has VMkernel adapter 0 (vmk0) and VMkernel adapter 1 (vmk1) configured on N-VDS. In NSX-T, TNP has vmk0 and vmk1 migration configured.	1 Move the host to be part of the cluster. 2 Reboot the host. After the rebooting the host, the host profile is applied to the target host. ■ The vmk0 and vmk1 adapters are attached to a temporary NSX switch. ■ TNP is triggered. ■ vmk0 and vmk1 are attached to an N-VDS switch. The host is successfully deployed with ESXi and NSX-T VIBs.

Target Host State	Reference Host Configuration	Steps To Auto Deploy Target Hosts
Host is in powered-on state. It is later added to the cluster. The default auto-deploy rule is configured for the target cluster and associated to the host profile. Target host has vmk0 and vmk1 network mapping configured.	The host profile extracted from the reference host has VMkernel adapter 0 (vmk0) on vSwitch and VMkernel adapter 1 (vmk1) configured on an N-VDS switch. In NSX-T, TNP has a vmk1 migration configured.	1 Move the host to be part of the cluster. 2 Reboot the host. After the host is rebooted the host profile is applied on the target host. ■ The vmk0 adapter is attached to a vSwitch, whereas the vmk1 adapter is attached to a temporary NSX switch. ■ TNP is triggered. ■ vmk1 is migrated to the N-VDS switch. 3 (Optional) If the host remains non-compliant with the host profile, reboot the host to make the host compliant. The host is successfully deployed with ESXi and NSX-T VIBs.
Host is in powered-on state. It is later added to the cluster. The default auto-deploy rule is configured for the target cluster and associated to the host profile. Host has vmk0 and vmk1 network mapping configured.	In the reference host, the host profile has VMkernel adapter 0 (vmk0) and VMkernel adapter 1 (vmk1) configured on an N-VDS switch. In NSX-T, TNP has vmk0 and vmk1 migration configured.	1 Move the host to be part of the cluster. 2 Reboot the host. After the host is rebooted the host profile is applied on the target host. ■ The vmk0 and vmk1 adapters are attached to a temporary NSX switch. ■ TNP is triggered. ■ The vmk0 and vmk1 adapters are migrated to the N-VDS switch. The host is successfully deployed with ESXi and NSX-T VIBs.

Troubleshoot Host Profile and Transport Node Profile

Troubleshoot issues with host profiles and TNPs when they are used to auto deploy stateless clusters.

Scenario	Description
When multiple VMkernel adapters enabled to support Management, vMotion and other traffic are migrated to the same logical switch, VMkernel adapters get migrated to logical switch after reboot. But the service on one VMkernel adapter is enabled on a different adapter.	For example, before migration, vmk0 is enabled to support Management traffic and vmk1 is enabled for vMotion traffic. After host reboot, vmk0 supports vMotion traffic and vmk1 supports Management traffic. This results in non-compliant error after reboot. Workaround: None. There is no impact as both VMkernel adapters are on the same logical switch.
Host preparation progress is stuck at 60% while the node status displays `UP`.	Issue: When a TNP is applied on a cluster, NSX-T is successfully installed on the host and node status displays `UP`, but GUI still shows 60% progress. Workaround: Reapply the TNP or TN configuration without any change in the config. This will fix the status to 100% on the GUI.

Scenario	Description
Even though VMkernel migration is successful there was a validation error on the TN before host switches are removed.	Issue: When you migrate vmk0 the management interface from vSwitch to a logical switch, NSX-T is successfully installed on the host. VMkernel migration is successful, but TN status shows Partial Success with error. `Validation before host switches removal failed: [error: No management vmk will have PNIC after ['vmk1'] in ['9a bb eb c1 04 81 40 e2-bc 3f 3e aa bd 14 62 1e'] lose all PNICs.]; LogicalSwitch full-sync: LogicalSwitch full-sync realization query skipped.` Workaround: None. Ignore the error message as VMkernel migration is successful.
Reapplying a TNP where the Network Mapping for Install lists vmk0 results in host losing connectivity.	Issue: When a TNP configuration consists of vmk0 in the Networking Mapping for Install, the hosts loses connectivity. Workaround: Instead of reapplying the TNP, reboot the host with necessary configurations in TNP.
Cannot apply the host profile because MUX user password policy and password were not reset.	Issue: Only on hosts running versions earlier than vSphere 6.7 U3. Host remediation and host profile application on hosts might fail unless the **`mux_user`** password is reset. Workaround: Under Policies & Profiles, edit the host profile to modify the mux_user password policy and reset the **`mux_user`** password.
Host Profile is not portable.	Issue: None of the vCenter servers can use the host profile containing NSX-T configuration. Workaround: None.
Auto Deploy Rule Engine	Issue: Host profile cannot be used in auto deploy rules to deploy new clusters. If new clusters are deployed, the hosts get deployed with basic networking and remain in maintenance mode. Workaround: Prepare each cluster from NSX-T GUI. See Apply TNP on Stateless Cluster.
Check compliance errors.	Issue: Host profile remediation cannot fix the compliance errors related to the NSX-T configuration. ■ Physical NICs configured on Host Profile and TNP are different. ■ Mapping between vNIC to LS mapping. Host Profile finds a mismatch in the logical switch to vNIC mapping with the TNP profile. ■ VMkernel connected to N-VDS mismatch on Host Profile and TNP. ■ Opaque switch mismatch on Host Profile and TNP. Workaround: Ensure the NSX-T configuration matches on Host Profile and TNP. Reboot the host to realize the configuration changes. The host comes up.
Remediation	Issue: If there are any NSX-T specific compliance errors, host profile remediation on that cluster is blocked. Incorrect configuration: ■ Mapping between vNIC to LS mapping ■ Mapping of physical NICs Workaround: Ensure that the NSX-T configuration matches on Host Profile and TNP. Reboot the host to realize the configuration changes. The host comes up.

Scenario	Description
Attach	Issue: In a cluster configured with NSX-T, host profile cannot be attached at the host-level. Workaround: None.
Detach	Issue: Detaching and attaching a new host profile in a cluster configured with NSX-T does not remove the NSX-T configuration. Even though the cluster is compliant with newly attach the host profile, it still has the NSX-T configuration from a previous profile. Workaround: None.
Update	Issue: If the user has changed NSX-T configuration in the cluster, then extract a new host profile. Update the host profile manually for all the settings that were lost. Workaround: None.
Host-level transport node configuration	Issue: After anportsport node was auto-deployed, it acts as individual entity. Any update to that transport node might not match with the TNP. Workaround: Update the cluster. Any update in a standalone transport node cannot persist its migration specification. The migration might fail to post the reboot.
PeerDNS configuration is not supported on the VMkernel adapter selected for migration to the NVDS switch.	Issue: If a VMkernel adapter selected for migration to NVDS is peer-DNS enabled, then host profile application fails. Workaround: Edit the extracted host profile by disabling peer-DNS setting on the VMkernel adapter that must be migrated to an NVDS switch. Alternatively, ensure that you do not migrate peer-DNS enabled VMkernel adapters to an NVDS switch.
DHCP address of the VMkernel NIC address not retained	Issue: If the reference host is stateful, then any stateless hosts using profile extracted from the stateful reference host cannot retain their VMkernel management MAC address derived from PXE started MAC. It results in DHCP addressing issues. Workaround: Edit extracted host profile of stateful host and modify the '**Determine how MAC address for vmknic should be decided**' to '**Use the MAC address from which the system was PXE started**'.
Host Profile application failure in vCenter can lead to NSX configuration errors on the host.	Issue: If host profile application fails in vCenter, NSX configuration might also fail. Workaround: In vCenter, verify that host profile was successfully applied. Fix the errors and try again.
LAGS are not supported on stateless ESXi hosts.	Issue: The uplink profile configured as LAGs in NSX is not supported in a stateless ESXi host managed by a vCenter Server or in NSX. Workaround: None.

Stateful Servers

Integrate host profiles of an ESXi host with NSX-T on stateful servers.

A stateful host is a host that retains all configurations and the installed VIBs even after it is rebooted. While an auto-deploy server is needed for stateless hosts because the boot up files required to bring up a stateless hosts are stored on the auto-deploy server, a stateful host does not need a similar infrastructure. Because the boot up files required to bring up a stateful host is stored on its hard drive.

In this procedure, the reference host is outside of the stateful cluster and the target hosts in the cluster. A target host can be within a cluster or a standalone host outside of the cluster. Prepare a cluster by applying host profile and transport node profile (TN profile) , so that any new target hosts joining the cluster is automatically prepared with NSX-T VIBs. Configure the target host as a transport node. Similarly, for a standalone host, apply the host profile and configure NSX-T to install NSX-T VIBs and when NSX-T configuration is complete, it becomes a transport node.

Note NSX-T VIBs are installed from TN profile and ESXi host configurations are applied by the Host Profiles.

During the configuration of a target host into a transport node, VMkernel adapters and vmnics or physical network interfaces that are attached to the VSS or VDS switch can be migrated and get connected to the NSX-T virtual distributed switch, N-VDS switch.

Supported NSX-T and ESXi versions

Supported NSX-T and ESXi versions on stateful servers.

Version Name	67ep6	67U2	67U3	67ep7	67U2C	6.5U3	6.5p03	7.0.0.1
NSX-T 2.4	Yes	No	No	No	No	No	Yes	No
NSX-T 2.4.1	Yes	Yes	No	No	No	No	Yes	No
NSX-T 2.4.2	Yes	Yes	No	No	No	No	Yes	No
NSX-T 2.4.3	Yes	Yes	No	No	No	No	Yes	No
NSX-T 2.5	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
NSX-T 2.5.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
NSX-T 3.0	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Prepare a Target Stateful Cluster

Prepare a target stateful cluster so that any new host joining the cluster is automatically deployed with ESXi and NSX-T VIBs.

You can select a host either within the cluster or outside of the cluster to be the reference host. You need to create a reference host because the host profile from the reference host is extracted and applied to a target host. Both N-VDS and VDS switch types support migration of VMkernel adapters.

In this procedure, as an example the instructions are to migrate vmk0 (management traffic) and vmk1 (vMotion traffic) to an N-VDS switch.

Prerequisites

Procedure

1 On the Reference host, deploy a supported ESXi build.

   a In vSphere, add vmk1 adapter. vmk0 is already present to serve management traffic.

2 Configure the reference node as a transport node.

   a Using vSphere Web Client, before migrating vmk0 and vmk1, ensure a logical switch is created in NSX-T.

   b (Optional) Using NSX-T Manager UI, configure NSX such that after installation of NSX-T, vmk1 adapter mapped to a logical switch is migrated to the N-VDS switch.

   c (Optional) Using NSX-T Manager UI, configure NSX-T such that after installation of NSX-T, vmk0 adapter mapped to a logical switch is migrated to the N-VDS switch.

   Note vmk0 and vmk1 can be on different VSS or DVS switches.

   d Using vSphere Web Client, ensure that vmk0 and vmk1 are connected to a logical switch on N-VDS switch.

3 Extract the host profile from the reference host.

4 In your environment, there might be a number of vmkernel adapter that need to be migrated to the N-VDS switch. However, before migrating vmk adapters from VSS/DVS to an N-VDS switch, ensure that the configuration parameters on the target host match those on the reference host.

5 On a target host that is a standalone host:

   a Attach the host profile to the target host.

   b Manually configure NSX-T on the host. When configuring the host as a transport node because the host profile on the ESXi, ensure the following conditions are met.

   c Host must belong to the same transport zone.

   d vmk1 adapter must be connected to the same logical switch that is used by the reference host.

   e Target host must use the same IP pool that is used by the reference host.

   f Uplink profile, LLDP, NIOC, network mapping for install, N-VDS configured on the target host must be the same as configured on the reference host.

   g Manually add VMkernel adapter, vmk1 and vmnic1 so that it is migrated from the VSS/DVS switch to the N-VDS switch. See vmk1 migration scenarios.

   h Manually add management adapter, vmk0 and or vmnic0.

6 On a target host that is part of a cluster:

   a Attach the host profile to the stateful target cluster.

   b Create and apply the TN profile on the cluster.

   c To configure vmk1 and vmnic1 to be migrated, see vmk1 migration scenarios.

d To configure vmk0 and vmnic0 to be migrated, see vmk0 migration scenarios.

e To apply TN profile on the cluster.

What to do next

Scenarios when VMkernel adapters are migrated with and without host profiles applied to NSX-T.

VMkernel Migration with Host Profile Applied

Migration of VMkernel adapters is supported on transport nodes using an N-VDS or VDS host switch. In the scenario illustrated in this section, VMkernel-1 (vmk1) adapter is migrated to an N-VDS switch on a host where host profile is applied. The vmk1 adapter supports infrastructure traffic for vMotion, Fault Tolerance, and other infrastructure services.

Scenario	Error	Workaround
vmk1 migration on a standalone target host by applying reference host profile.	The target host is not configured as a transport node. As the target host does not know about any NSX-T objects, host profile application fails. Remediation of host profile on the target host fails. `Error: Received SOAP response fault : generate HostConfigTask Spec..`	1 Before applying the reference host profile to migrate vmk1 to the logical switch on the target host, configure the target host as a transport node, which installs NSX-T VIBs, creates an N-VDS switch and migrates vmk1 adapter from the VSS switch to N-VDS switch. When configuring the host as a transport node because the host profile on the ESXi, ensure the following conditions are met: ■ Host must belong to the same transport zone. ■ vmk1 adapter must be connected to the same logical switch that is used by the reference host. ■ Target host must use the same IP pool that is used by the reference host. ■ Uplink profile, LLDP, NIOC, network mapping for install, N-VDS configured on the target host must be the same as configured on the reference host. Host profile remediation is successful when the target host is configured with the same logical switch name that is present in the host profile.
vmk1 migration on target hosts in a stateful cluster.	Before applying the host profile to the target host, if you prepare the cluster by applying TN profile configured with vmk1 mapped to the logical switch, then vmk1 migration fails. `Error: vmk1 missing on the host.`	1 Apply the reference host profile to the target host that joined the cluster. 2 Remediate the host profile on the target host to create vmk1 adapter on the target host. 3 Re-apply the TN profile to the cluster to migrate vmk1 to the target cluster.

Scenario	Error	Workaround
vmk0 and vmk1 migration on a standalone host.	When configuring NSX-T on the standalone host, if the Network Mapping for Install field does not specify vmk0 or vmk1 mappings, then migration fails.	When configuring NSX-T on the target host, ensure that the Network Mapping for Install field is specified with vmk0 and vmk1 mapped to the same logical switch on the N-VDS.
vmk0 and vmk1 migration on a cluster host.	When applying TN profile to a cluster, if the Network Mapping for Install field does not specify vmk0 or vmk1 mappings, then migration fails.	Apply TN profile to the cluster. When configuring TN profile to the cluster, ensure that Network Mapping for Install field is specified with vmk0 and vmk1 mapped to a logical switch on the N-VDS.

VMkernel Migration without Host Profile Applied

Migration of VMkernel adapters is supported on transport nodes using an N-VDS or VDS host switch. In the scenario illustrated in this section, the VMkernel 0 (vmk0) adapter is migrated to an N-VDS or a VDS switch on a host where host profile is not applied. The vmk0 adapter supports management traffic for NSX-T.

You do not need to apply a host profile to the target host as vmk0 already exists on it. vmk0 adapter supports management traffic on an ESXi host.

Scenario	Procedure	Result
vmk0 migration on a standalone host.	When configuring NSX-T on the target host, ensure that the **Network Mapping for Install** field is specified with vmk0 mapped to a logical switch on the N-VDS.	vmk0 is migrated to the logical switch on the target host.
vmk0 migration on a cluster host.	Apply TN profile to the cluster. When configuring TN profile on the cluster, ensure that the **Network Mapping for Install** field is specified with vmk0 mapped to a logical switch on the N-VDS.	vmk0 is migrated to the logical switch on the target host.

Getting Started with NSX Cloud

12

NSX Cloud provides a single pane of glass for managing your public cloud networks.

NSX Cloud is agnostic of provider-specific networking that does not require hypervisor access in a public cloud.

It offers several benefits:

- You can develop and test applications using the same network and security profiles used in the production environment.
- Developers can manage their applications until they are ready for deployment.
- With disaster recovery, you can recover from an unplanned outage or a security threat to your public cloud.
- If you migrate your workloads between public clouds, NSX Cloud ensures that similar security policies are applied to workload VMs regardless of their new location.

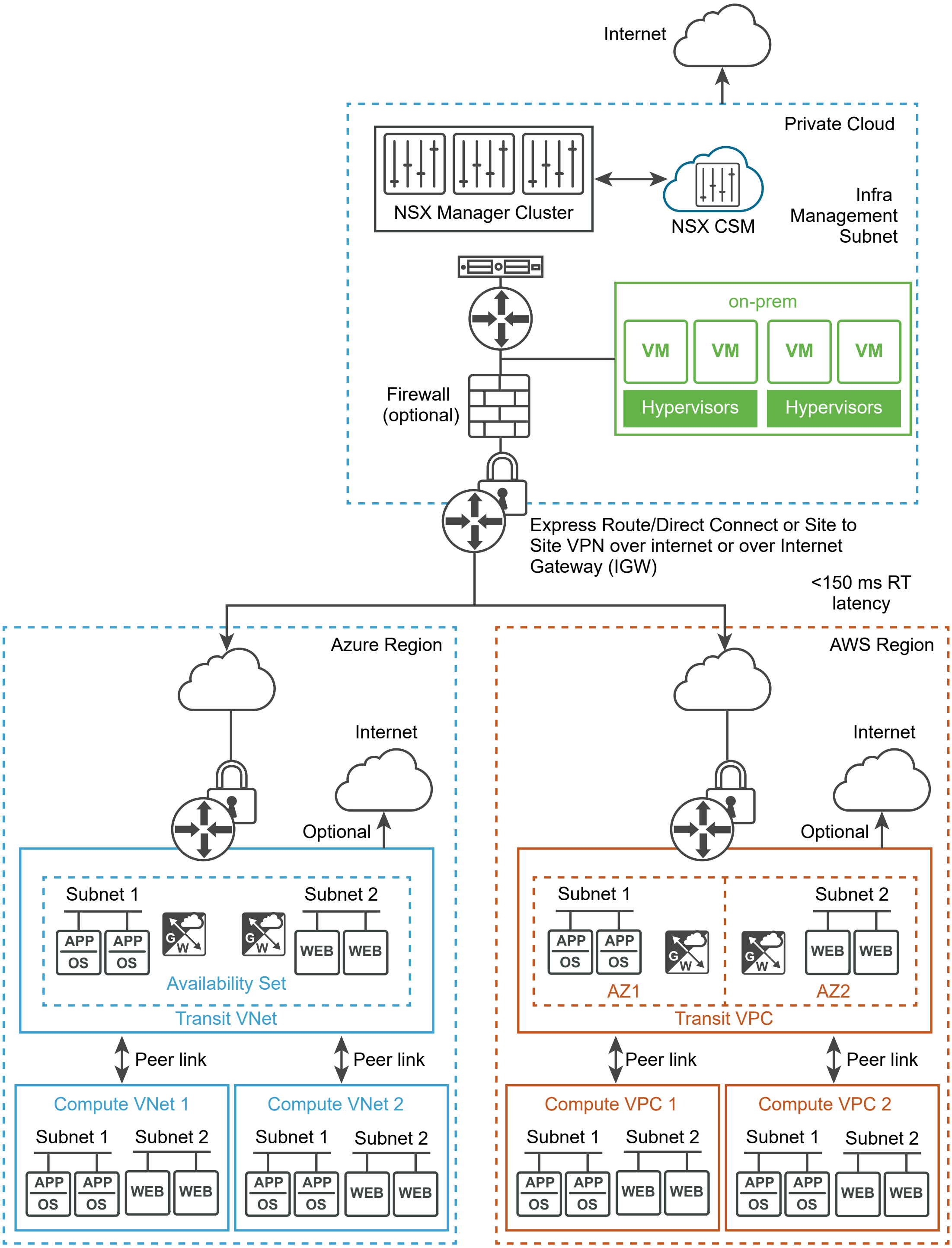
This chapter includes the following topics:

- NSX Cloud Architecture and Components
- Overview of Deploying NSX Cloud
- Deploy NSX-T Data Center On-Prem Components
- Add your Public Cloud Account
- Deploy the NSX Public Cloud Gateway
- (Optional) Install NSX Tools on your Workload VMs
- Undeploy or Unlink PCG

NSX Cloud Architecture and Components

NSX Cloud integrates the NSX-T Data Center core components with your public cloud to provide network and security across your implementations.

Figure 12-1. NSX Cloud Architecture



Core Components

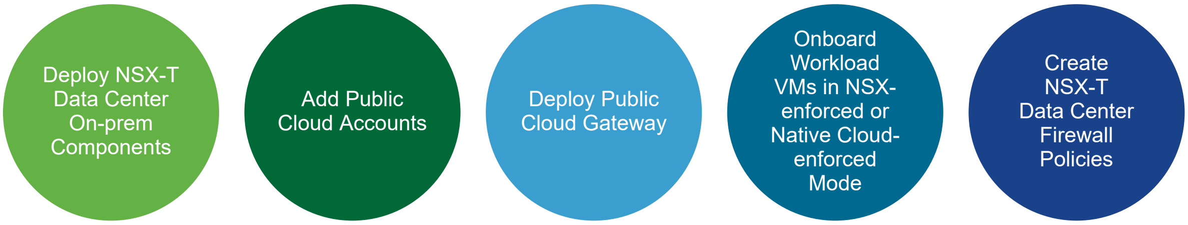
The core NSX Cloud components are:

- **NSX Manager** for the management plane with policy-based routing, role-based access control (RBAC), control plane and runtime states defined.

- **Cloud Service Manager (CSM)** for integration with NSX Manager to provide public cloud-specific information to the management plane.
- **Public Cloud Gateway (PCG)** for connectivity to the NSX management and control planes, NSX Edge gateway services, and for API-based communications with the public cloud entities.
- **NSX Tools** functionality that provides NSX-managed datapath for workload VMs.

Overview of Deploying NSX Cloud

Refer to this overview to understand the overall process of installing and configuring NSX Cloud components to enable NSX-T Data Center to manage your public cloud workload VMs.


Deploy NSX-T Data Center On-prem Components
Add Public Cloud Accounts
Deploy Public Cloud Gateway
Onboard Workload VMs in NSX-enforced or Native Cloud-enforced Mode
Create NSX-T Data Center Firewall Policies

Note While planning your deployment, ensure that the on-prem NSX-T Data Center appliances have good connectivity with the PCG deployed in the public cloud and Transit VPCs/VNets are be in the same region as the Compute VPCs/VNets.

Table 12-1. Workflow for deploying NSX Cloud

Task	Instructions
□ Install CSM and connect with NSX Manager.	See Deploy NSX-T Data Center On-Prem Components.
□ Add one or more of your public cloud accounts in CSM.	See Add your Public Cloud Account.
□ Deploy PCG in your Transit VPCs or VNets and link to your Compute VPCs or VNets.	See Deploy the NSX Public Cloud Gateway .
What to do next?	Follow instructions at Using NSX Cloud in the *NSX-T Data Center Administration Guide*.

Deploy NSX-T Data Center On-Prem Components

You must have already installed NSX Manager to proceed with installing CSM.

Install CSM

The Cloud Service Manager (CSM) is a core component of NSX Cloud.

After installing NSX Manager, install CSM by following the same steps as for installing NSX Manager and selecting **nsx-cloud-service-manager** as the VM role. See Install NSX Manager and Available Appliances for instructions.

You can deploy CSM in the Extra Small VM size or higher, as required. See NSX Manager VM and Host Transport Node System Requirements for details.

Join CSM with NSX Manager

You must connect the CSM appliance with NSX Manager to allow these components to communicate with each other.

Prerequisites

- NSX Manager must be installed and you must have the username and password for the admin account to log in to NSX Manager
- CSM must be installed and you must have the Enterprise Administrator role assigned in CSM.

Procedure

1 From a browser, log in to CSM.

2 When prompted in the setup wizard, click **Begin Setup**.

3 Enter the following details in the NSX Manager Credentials screen:

Option	Description
NSX Manager Host Name	Enter the fully qualified domain name (FQDN) of the NSX Manager, if available. You may also enter the IP address of NSX Manager.
Admin Credentials	Enter an Enterprise Administrator username and password for NSX Manager.
Manager Thumbprint	Optionally, enter the NSX Manager's thumbrpint value. If you leave this field blank, the system identifies the thumbprint and displays it in the next screen.

4 (Optional) If you did not provide a thumbprint value for NSX Manager, or if the value was incorrect, the **Verify Thumbprint** screen appears. Select the checkbox to accept the thumbprint discovered by the system.

5 Click **Connect**.

Note If you missed this setting in the setup wizard or if you want to change the associated NSX Manager, log in to CSM, click **System > Settings**, and click **Configure** on the panel titled **Associated NSX Node**.

CSM verifies the NSX Manager thumbprint and establishes connection.

6 (Optional) Set up the Proxy server. See instructions in (Optional) Configure Proxy Servers.

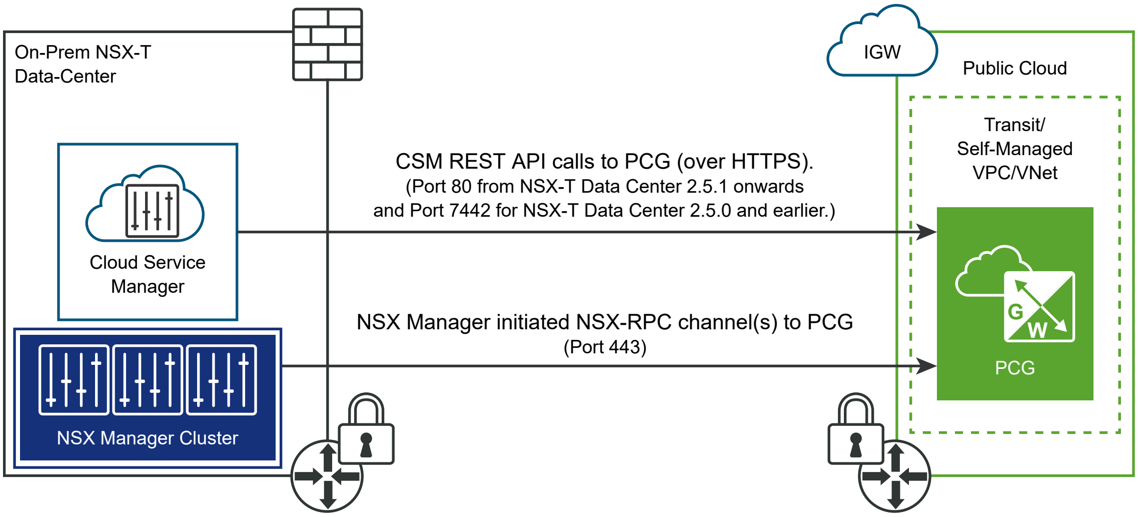
Enable Access to Ports and Protocols

No inbound ports are required to be open in your on-prem deployment of NSX-T Data Center to enable public cloud connectivity.

The following outbound ports are required:

Table 12-2. Ports and Protocols Required for Public Cloud Connectivity with NSX-T Data Center

From	To	Port	Protocol	Required for:
CSM	PCG	80 **Note** If you are using NSX-T Data Center version 2.5.0, you need to open the non-standard port 7442 instead, and ensure your firewall allows SSL traffic over it.	TCP	CSM configuration, such as upgrade workflow, over HTTPS.
NSX Manager	PCG	443	TCP	NSX RPC channel(s).
CSM	NSX Manager	443	TCP	CSM to access NSX Manager. See Ports and Protocols for details on the on-prem deployment.


On-Prem NSX-T Data-Center
Cloud Service Manager
NSX Manager Cluster
IGW
Public Cloud
Transit/ Self-Managed VPC/VNet
CSM REST API calls to PCG (over HTTPS).
(Port 80 from NSX-T Data Center 2.5.1 onwards and Port 7442 for NSX-T Data Center 2.5.0 and earlier.)
NSX Manager initiated NSX-RPC channel(s) to PCG
(Port 443)
G
W
PCG

(Optional) Configure Proxy Servers

If you want to route and monitor all internet-bound HTTP/HTTPS traffic through a reliable HTTP Proxy, you can configure up to five proxy servers in CSM.

All public cloud communication from PCG and CSM is routed through the selected proxy server.

Proxy settings for PCG are independent of proxy settings for CSM. You can choose to have none or a different proxy server for PCG.

You can choose the following levels of authentication:

- Credentials-based authentication.

- Certificate-based authentication for HTTPS interception.
- No authentication.

Procedure

1 Click **System > Settings**. Then click **Configure** on the panel titled **Proxy Servers**.

Note You can also provide these details when using the CSM Setup Wizard that is available when you first install CSM.

2 In the Configure Proxy Servers screen, enter the following details:

Option	Description
Default	Use this radio button to indicate the default proxy server.
Profile Name	Provide a proxy server profile name. This is mandatory.
Proxy Server	Enter the proxy server's IP address. This is mandatory.
Port	Enter the proxy server's port. This is mandatory.
Authentication	Optional. If you want to set up additional authentication, select this check box and provide valid username and password.
Username	This is required if you select the Authentication checkbox.
Password	This is required if you select the Authentication checkbox.
Certificate	Optional. If you want to provide an authentication certificate for HTTPS interception, select this checkbox and copy-paste the certificate in the text box that appears.
No Proxy	Select this option if you do not want to use any of the proxy servers configured.

(Optional) Set Up vIDM for Cloud Service Manager

If you use VMware Identity Manager, you can set it up to access CSM from within NSX Manager.

Procedure

1 Configure vIDM for NSX Manager and CSM. See instructions at Configure VMware Identity Manager Integration in the *NSX-T Data Center Administration Guide*.

2 Assign the same role to the vIDM user for NSX Manager and CSM, for example, **Enterprise Admin** role assigned to the user named `vIDM_admin`. You must log in to NSX Manager and CSM each and assign the same role to the same username. See Add a Role Assignment or Principal Identity in the *NSX-T Data Center Administration Guide* for detailed instructions.

3 Log in to NSX Manager. You are redirected to the vIDM login.

4 Enter the vIDM user's credentials. Once you log in, you can switch between NSX Manager and CSM by clicking the Applications icon.

Add your Public Cloud Account

To add your public cloud inventory, you need to connect your public cloud account with the on-prem deployment of NSX-T Data Center and create roles in your public cloud to allow access to NSX Cloud.

These steps are in no specific order and can be completed independently.

Note

- Connect VPCs/VNets with on-prem using suitable methods, such as Direct Connect for AWS or Express Route for Microsoft Azure or site-to-site VPN with any VPN endpoint on-premises and PCG acting as the VPN endpoint in your public cloud.
- If you choose to have a Transit/Compute topology, make sure there are peering connections established between the Transit and Compute VPCs/VNets. You can have a single PCG manage multiple compute VPCs/VNets. You may also choose to have a flat compute VPC/VNet architecture with a PCG pair installed in each VPC/VNet. See Deploy the NSX Public Cloud Gateway for details on PCG deployment options.

Adding your Microsoft Azure Subscription

For NSX Cloud to operate in your subscription, create a Service Principal to grant the required permissions, and roles for CSM and PCG based on the Microsoft Azure feature for managing identities for Azure Resources.

Overview:

- NSX Cloud provides a PowerShell script to generate the Service Principal and roles that use the managed identity feature of Microsoft Azure to manage authentication while keeping your Microsoft Azure credentials secure. You can also include multiple subscriptions under one Service Principal using this script.
- You have the option of reusing the Service Principal for all your subscriptions, or to create new Service Principals as required. There is an additional script if you want to create separate Service Principals for additional subscriptions.
- For multiple subscriptions, whether you are using a single Service Principal for all, or multiple Service Principals, you must update the JSON files for the CSM and PCG roles to add each additional subscription name under the section *AssignableScopes*.
- If you already have an NSX Cloud Service Principal in your VNet, you can update it by running the scripts again and leaving out the Service Principal name from the parameters.
- The Service Principal name must be unique for your Microsoft Azure Active Directory. You may use the same Service Principal in different subscriptions under the same Active Directory domain, or different Service Principals per subscription. But you cannot create two Service Principals with the same name.
- You must either be the owner of or have permissions to create and assign roles in all the Microsoft Azure subscriptions.

- The following scenarios are supported:
  - **Scenario 1:** You have a single Microsoft Azure Subscription that you want to enable with NSX Cloud.
  - **Scenario 2:** You have multiple Microsoft Azure Subscriptions under the same Microsoft Azure Directory, that you want to enable with NSX Cloud, but want to use one NSX Cloud Service Principal across all your subscriptions.
  - **Scenario 3:** You have multiple Microsoft Azure Subscriptions under the same Microsoft Azure Directory, that you want to enable with NSX Cloud, but want to use different NSX Cloud Service Principal names for different subscriptions.

Here is an outline of the process:

1. Use the NSX Cloud PowerShell script to:
   - Create a Service Principal account for NSX Cloud.
   - Create a role for CSM.
   - Create a role for PCG.
2. (Optional) Create Service Principals for other subscriptions you want to link.
3. Add the Microsoft Azure subscription in CSM.

   Note If using multiple subscriptions, whether using the same or different Service Principals, you must add each subscription separately in CSM.

Generate the Service Principal and Roles

NSX Cloud provides PowerShell scripts that help you generate the required service principal and roles for one or multiple subscriptions.

Prerequisites

- You must have PowerShell 5.0+ with the AzureRM Module installed.
- You must either be the owner of or have permissions to create and assign roles in all the Microsoft Azure subscriptions.

Note The response time from Microsoft Azure can cause the script to fail when you run it the first time. If the script fails, try running it again.

Procedure

1. On a Windows desktop or server, download the ZIP file named `CreateNSXCloudCredentials.zip` from the NSX-T Data Center **Download page > Drivers & Tools > NSX Cloud Scripts > Microsoft Azure**.

2 Extract the following contents of the ZIP file in your Windows system:

Script/File	Description
CreateNSXRoles.ps1	The PowerShell script to generate the NSX Cloud Service Principal and managed identity roles for CSM and PCG. This script takes the following parameters: ■ `-subscriptionId <the Transit_VNet's_Azure_subscription_ID>` ■ (optional) `-servicePrincipalName <Service_Principal_Name>` ■ (optional) `-useOneServicePrincipal`
AddServicePrincipal.ps1	An optional script required if you want to add multiple subscriptions and assign different Service Principals to each subscription. See **Scenario 3** in the following steps. This script takes the following parameters: ■ `-computeSubscriptionId <the_Compute_VNet's_Azure_subscription_ID>` ■ `-transitSubscriptionId <the Transit_VNet's_Azure_Subscription_ID>` ■ `-csmRoleName <CSM_Role_Name>` ■ `-servicePrincipalName <Service_Principal_Name>`
nsx_csm_role.json	A JSON template for the CSM role name and permissions. This file is required as an input to the PowerShell script and must be in the same folder as the script.
nsx_pcg_role.json	A JSON template for the PCG role name and permissions. This file is required as an input to the PowerShell script and must be in the same folder as the script. **Note** The default PCG (Gateway) Role Name is `nsx-pcg-role`. You need to provide this value when adding your subscription in CSM.

3 **Scenario 1:** You have a single Microsoft Azure Subscription that you want to enable with NSX Cloud.

a From a PowerShell instance, go to the directory where you downloaded the Microsoft Azure scripts and JSON files.

b Run the script named CreateNSXRoles.ps1 with the parameter -SubscriptionId, as follows:

```
.\CreateNSXRoles.ps1 -subscriptionId <the_single_Azure_subscription_ID>
```

Note If you want to override the default Service Principal name of `nsx-service-admin`, you can also use the parameter `-servicePrincipalName`. The Service Principal name must be unique in your Microsoft Azure Active Directory.

4 **Scenario 2:** You have multiple Microsoft Azure Subscriptions under the same Microsoft Azure Directory, that you want to enable with NSX Cloud, but want to use one NSX Cloud Service Principal across all your subscriptions.

   a From a PowerShell instance, go to the directory where you downloaded the Microsoft Azure scripts and JSON files.

   b Edit each of the JSON files to add a list of other subscription IDs under the section titled *"AssignableScopes"*, for example:

```
"AssignableScopes": [

"/subscriptions/aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",

"/subscriptions/aaaaaaaa-bbbb-cccc-dddd-ffffffffffff",

"/subscriptions/aaaaaaaa-bbbb-cccc-dddd-000000000000"
```

Note You must use the format shown in the example to add subscription IDs: `"/subscriptions/<Subscription_ID>"`

   c Run the script named `CreateNSXRoles.ps1` with the parameters `-subscriptionID` and `-useOneServicePrincipal`:

```
.\CreateNSXRoles.ps1 -subscriptionId <the_Transit_VNet's_Azure_subscription_ID> -
useOneServicePrincipal
```

Note Omit the Service Principal name here if you want to use the default name: `nsx-service-admin`. If that Service Principal name already exists in your Microsoft Azure Active Directory, running this script without a Service Principal name updates that Service Principal.

5 **Scenario 3:** You have multiple Microsoft Azure Subscriptions under the same Microsoft Azure Directory, that you want to enable with NSX Cloud, but want to use different NSX Cloud Service Principal names for different subscriptions.

   a From a PowerShell instance, go to the directory where you downloaded the Microsoft Azure scripts and JSON files.

   b Follow steps **b** and **c** from the second scenario to add multiple subscriptions to the *AssignableScopes* section in each of the JSON files.

c Run the script named `CreateNSXRoles.ps1` with the parameters -subscriptionID:

```
.\CreateNSXRoles.ps1 -subscriptionId <One of the subscription_IDs>
```

Note Omit the Service Principal name here if you want to use the default name: `nsx-service-admin`. If that Service Principal name exists in your Microsoft Azure Active Directory, running this script without a Service Principal name updates that Service Principal.

d Run the script named `AddServicePrincipal.ps1` with the following parameters:

Parameter	Value
`-computeSubscriptionId`	The Compute_VNet's Azure Subscription ID
`-transitSubscriptionId`	The Transit VNet's Azure Subscription ID
`-csmRoleName`	Get this value from the file `nsx_csm_role.JSON`
`-servicePrincipalName`	New Service Principal name

```
./AddServicePrincipal.ps1 -computeSubscriptionId <the_Compute_VNet's_Azure_subscription_ID>
 -transitSubscriptionId <the_Tranist_VNet's_Azure_Subscription_ID>
-csmRoleName <CSM_Role_Name>
-servicePrincipalName <new_Service_Principal_Name>”
```

6 Look for a file in the same directory where you ran the PowerShell script. It is named like: `NSXCloud_ServicePrincipal_<your_subscription_ID>_<NSX_Cloud_Service_Principal_name>`. This file contains the information required to add your Microsoft Azure subscription in CSM.

- Client ID
- Client Key
- Tenant ID
- Subscription ID

Results

The following constructs are created:

- an Azure AD application for NSX Cloud.
- an Azure Resource Manager Service Principal for the NSX Cloud application.
- a role for CSM attached to the Service Principal account.
- a role for PCG to enable it to work on your public cloud inventory.

- a file named like `NSXCloud_ServicePrincipal_<your_subscription_ID>_<NSX_Cloud_Service_Principal_name>` is created in the same directory where you ran the PowerShell script. This file contains the information required to add your Microsoft Azure subscription in CSM.

Note Refer to the JSON files that are used to create the CSM and PCG roles for a list of permissions available to them after the roles are created.

What to do next

Add your Microsoft Azure Subscription in CSM

Note When enabling NSX Cloud for multiple subscriptions, you must add each separate subscription to CSM individually, for example, if you have five total subscriptions you must add five Microsoft Azure accounts in CSM with all other values the same but different subscription IDs.

Add your Microsoft Azure Subscription in CSM

Once you have the details of the NSX Cloud Service Principal and the CSM and PCG roles, you are ready to add your Microsoft Azure subscription in CSM.

Prerequisites

- You must have the Enterprise Administrator role in NSX-T Data Center.
- You must have the output of the PowerShell script with details of the NSX Cloud Service Principal.
- You must have the value of the PCG role you provided when running the PowerShell script to create the roles and the Service Principal. The default value is `nsx-pcg-role`.

Procedure

1. Log in to CSM using an account with the Enterprise Administrator role.
2. Go to **CSM > Clouds > Azure**.
3. Click **+Add** and enter the following details:

Option	Description
Name	Provide a suitable name to identify this account in CSM. You may have multiple Microsoft Azure subscriptions that are associated with the same Microsoft Azure tenant ID. Name your account account and you can name them appropriately in CSM, for example, Azure-DevOps-Account, Azure-Finance-Account, etc.
Client ID	Copy paste this value from the output of the PowerShell script.
Key	Copy paste this value from the output of the PowerShell script.
Subscription ID	Copy paste this value from the output of the PowerShell script.
Tenant ID	Copy paste this value from the output of the PowerShell script.

Option	Description
Gateway Role Name	The default value is `nsx-pcg-role`. This value is available from the *nsx_pcg_role.json* file if you changed the default.
Cloud Tags	By default this option is enabled and allows your Microsoft Azure tags to be visible in NSX Manager

4 Click **Save**.

   CSM adds the account and you can see it in the **Accounts** section within three minutes.

5 Whitelist all the VMs in the VNet where you want VMs managed. This is not required, but highly recommended for brownfield deployments because of Quarantine Policy impact when changed from disabled to enabled.

What to do next

Deploy PCG in a VNet

Adding your AWS Account

You might have one or more AWS accounts with VPCs and workload VMs that you want to bring under NSX-T Data Center management.

Overview:

- NSX Cloud provides a shell script that you can run from the AWS CLI of your AWS account to create the IAM profile and role, and create a trust relationship for Transit and Compute VPCs .
- The following scenarios are supported:
  - **Scenario 1:** You want to use a single AWS account with NSX Cloud.
  - **Scenario 2:** You want to use multiple sub-accounts in AWS that are managed by a master AWS account.
  - **Scenario 3:** You want to use multiple AWS accounts with NSX Cloud, designating one account where you will install the PCG, that is a Transit VPC, and other accounts that will link to this PCG, that is, Compute VPCs. See Deploy the NSX Public Cloud Gateway for details on PCG deployment options.

Here is an outline of the process:

1 Use the NSX Cloud shell script to do the following. This step requires AWS CLI configured with the account you want to add.
   - Create an IAM profile.
   - Create a role for PCG.
   - (Optional) Create a trust relationship between the AWS account hosting the Transit VPC and the AWS account hosting the Compute VPC.

2 Add the AWS account in CSM.

Generate the IAM Profile and PCG Role

NSX Cloud provides a SHELL script to help set up one or more of your AWS accounts by generating an IAM profile and a role for PCG attached to the profile that provides necessary permissions to your AWS account.

If you plan to host a Transit VPC linked to multiple Compute VPCs in two different AWS accounts, you can use the script to create a trust relationship between these accounts.

Note The PCG (Gateway) role name is `nsx_pcg_service` by default. If you want a different value for the Gateway Role Name, you can change it in the script, but make a note of this value because it is required for adding the AWS account in CSM.

Prerequisites

You must have the following installed and configured on your Linux or compatible system before you run the script:

- AWS CLI configured for the account and the default region.
- `jq` (a JSON parser).
- `openssl` (network security requirement).

Note If using AWS GovCloud (US) accounts, ensure that your AWS CLI is configured for the GovCloud (US) account and the default region is specified in the AWS CLI configuration file.

Procedure

- On a Linux or compatible desktop or server, download the SHELL script named `nsx_csm_iam_script.sh` from the NSX-T Data Center **Download page > Drivers & Tools > NSX Cloud Scripts > AWS**.
- **Scenario 1:** You want to use a single AWS account with NSX Cloud.

  a Run the script, for example:

  ```
  bash nsx_csm_iam_script.sh
  ```

  b Enter `yes` when prompted with the question `Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no]`

  c Enter a name for the IAM user when asked `What do you want to name the IAM User?`

  Note The IAM user name must be unique in your AWS account.

  d Enter `no` when asked `Do you want to add trust relationship for any Transit VPC account? [yes/no]`

When the script runs successfully, the IAM profile and a role for PCG is created in your AWS account. The values are saved in the output file named `aws_details.txt` in the same directory where you ran the script. Next, follow instructions at Add your AWS Account in CSM and then Deploy PCG in a VPC to finish the process of setting up a Transit or Self-Managed VPC.

- **Scenario 2:** You want to use multiple sub-accounts in AWS that are managed by one master AWS account.

  a Run the script from your AWS master account.

  ```
  bash nsx_csm_iam_script.sh
  ```

  b Enter `yes` when prompted with the question `Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no]`

  c Enter a name for the IAM user when asked `What do you want to name the IAM User?`

  Note The IAM user name must be unique in your AWS account.

  d Enter `no` when asked `Do you want to add trust relationship for any Transit VPC account? [yes/no]`

  Note With a master AWS account, if your Transit VPC has permission to view Compute VPCs in the sub-accounts, you do not need to establish a trust relationship with your sub-accounts. If not, follow the steps for **Scenario 3** to set up multiple accounts.

  When the script runs successfully, the IAM profile and a role for PCG is created in your AWS master account. The values are saved in the output file in the same directory where you ran the script. The filename is `aws_details.txt`. Next, follow instructions at Add your AWS Account in CSM and then Deploy PCG in a VPC to finish the process of setting up a Transit or Self-Managed VPC.

- **Scenario 3:** You want to use multiple AWS accounts with NSX Cloud, designating one account for Transit VPC and other accounts for Compute VPCs. See Deploy the NSX Public Cloud Gateway for details on PCG deployment options.

  a Make a note of the 12-digit AWS account number where you want to host the Transit VPC.

  b Set up the Transit VPC in the AWS account by following steps `a` through `d` for *Scenario 1* and finish the process of adding the account in CSM.

  c Download and run the NSX Cloud script from a Linux or compatible system in your other AWS account where you want to host the Compute VPCs. Alternatively, you can use AWS profiles with different account credentials to use the same system to run the script again for your other AWS account.

d The script poses the question: `Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no]`. Use the following guidance for the appropriate response:

This AWS account was already added to CSM.	Enter **no** in response to `Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no]`
This account has not been added to CSM before.	Enter **yes** in response to `Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no]`

e (Optional) If you answered **yes** to creating an IAM user for CSM and PCG in the previous question, enter a name for the IAM user when asked `What do you want to name the IAM User?`. The IAM user name must be unique in your AWS account.

f Enter **yes** when asked `Do you want to add trust relationship for any Transit VPC account? [yes/no]`

g Enter or copy-paste the 12-digit AWS account number that you noted in step 1 when asked `What is the Transit VPC account number?`

An IAM Trust Relationship is established between the two AWS accounts and an ExternalID is generated by the script.

When the script runs successfully, the IAM profile and a role for PCG is created in your AWS master account. The values are saved in the output file in the same directory where you ran the script. The filename is *aws_details.txt*. Next, follow instructions at Add your AWS Account in CSM and then Link to a Transit VPC or VNet to finish the process of linking to a Transit VPC.

Add your AWS Account in CSM

Add your AWS account using values generated by the script.

Procedure

1 Log in to CSM using the Enterprise Administrator role.

2 Go to **CSM > Clouds > AWS**.

3 Click **+Add** and enter the following details using the output file aws_details.txt generated from the NSX Cloud script:

Option	Description
Name	Enter a descriptive name for this AWS Account
Access Key	Enter your account's Access Key
Secret Key	Enter your account's Secret Key
Discover Cloud Tags	By default this option is enabled and allows your AWS tags to be visible in NSX Manager
Gateway Role Name	The default value is `nsx_pcg_service`. You can find this value in the output of the script in the file *aws_details.txt*.

The AWS account gets added in CSM.

In the VPCs tab of CSM, you can view all the VPCs in your AWS account.

In the Instances tab of CSM, you can view the EC2 Instances in this VPC.

4 Whitelist all the VMs in the VPC where you want VMs managed. This is not required, but highly recommended for brownfield deployments because of Quarantine Policy impact when changed from disabled to enabled.

What to do next

Deploy PCG in a VPC

Deploy the NSX Public Cloud Gateway

The NSX Public Cloud Gateway (PCG) provides north-south connectivity between the public cloud and the on-prem management components of NSX-T Data Center.

Familiarize yourself with the following terminology explaining the PCG's architecture and deployment modes for workload VM-management.

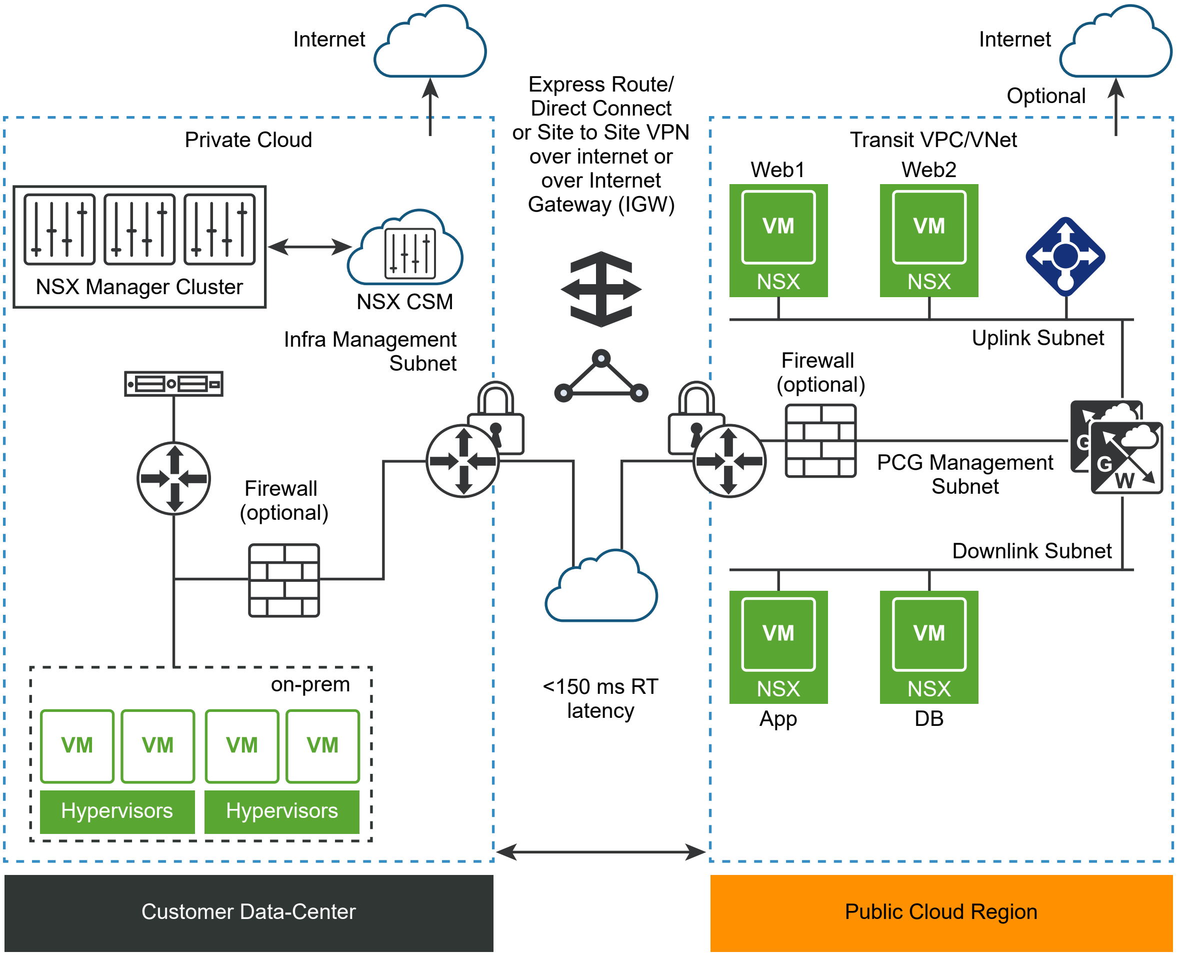
Note The PCG is deployed in a single default size for each supported public cloud:

Public Cloud	PCG instance type
AWS	c5.xlarge **Note** Some regions may not support this instance type. Refer to AWS documentation for details.
Microsoft Azure	Standard DS3 v.2

Architecure

The PCG can either be a standalone gateway appliance or shared between your public cloud VPCs or VNets to achieve a hub and spoke topology.

Figure 12-2. NSX Public Cloud Gateway Architecture



Modes of Deployment

Self-managed VPC/VNet: When you deploy the PCG in a VPC or VNet, it qualifies the VPC or VNet as *self-managed*, that is, you can bring VMs hosted in this VPC or VNet under NSX management.

Transit VPC/VNet: A self-mananged VPC/VNet becomes a *Transit* VPC/VNet when you link Compute VPCs/VNets to it.

Compute VPC/VNet: VPCs/VNets that do not have the PCG deployed on them but link to a Transit VPC/VNet are called *Compute* VPCs/VNets.

Subnets Required in your VPC/VNet to deploy PCG

The PCG utilizes the following subnets that you set up in your VPC/VNet. See Connect Microsoft Azure with On-prem NSX-T Data Center or Connect AWS with On-prem NSX-T Data Center .

- **Management subnet**: This subnet is used for management traffic between on-prem NSX-T Data Center and PCG. The recommended range is /28.
- **Uplink subnet**: This subnet is used for north-south internet traffic. The recommended range is /24.

- **Downlink subnet**: This subnet encompasses the workload VM's IP address range, and should be sized accordingly. Bear in mind that you may need to incorporate additional interfaces on the workload VMs for debugging.

PCG deployment aligns with your network addressing plan with FQDNs for the NSX-T Data Center components and a DNS server that can resolve these FQDNs.

Note It is not recommended to use IP addresses for connecting the public cloud with NSX-T Data Center using PCG, but if you choose that option, do not change your IP addresses.

Modes of VM-Management

NSX Enforced Mode: In this mode, workload VMs are brought under NSX management by using NSX Tools that have to be installed on each such workload VM after the tag "nsx.network=default" is applied to them in AWS or Microsoft Azure.

Native Cloud Enforced Mode:In this mode, your workload VMs can be brought under NSX management without the use of NSX Tools.

Quarantine Policy

Quarantine Policy: This is NSX Cloud's threat detection feature that works with your public cloud security groups.

- In the NSX Enforced Mode you can enable or disable Quarantine Policy. It is recommended to have the Quarantine Policy disabled and all your VMs whitelisted when onboarding workload VMs.
- In the Native Cloud Enforced Mode Quarantine Policy is always enabled and cannot be disabled.

Possible Design Options

Regardless of the mode you deploy the PCG in, you can link a Compute VPC/VNet to it in either mode.

Table 12-3. Possible Design Options with PCG Deployment Modes

PCG Deployment Mode in Transit VPC/VNet	Possible Modes when linking a Compute VPCs/VNets to this Transit VPC/VNet
NSX Enforced Mode	■ NSX Enforced Mode ■ Native Cloud Enforced Mode
Native Cloud Enforced Mode	■ NSX Enforced Mode ■ Native Cloud Enforced Mode

Note Once a mode is selected for a Transit or Compute VPC/VNet, you cannot change the mode. If you want to switch modes, you must undeploy the PCG and redeploy it in the desired mode.

Deploying PCG in a VNet

Ensure the VNet is connected with your on-prem NSX-T Data Center before deploying PCG.

Connect Microsoft Azure with On-prem NSX-T Data Center

A connection must be established between your Microsoft Azure network and your on-prem NSX-T Data Center appliances.

Note You must have already installed and connected NSX Manager with CSM in your on-prem deployment.

Overview

- Connect your Microsoft Azure subscription with on-prem NSX-T Data Center.
- Configure your VNets with the necessary CIDR blocks and subnets required by NSX Cloud.
- Synchronize time on the CSM appliance with the Microsoft Azure Storage server or NTP.

Connect your Microsoft Azure subscription with on-prem NSX-T Data Center

Every public cloud provides options to connect with an on-premises deployment. You can choose any of the available connectivity options that suit your requirements. Refer to Microsoft Azure Reference documentation for details.

Note You must review and implement the applicable security considerations and best practices by Microsoft Azure, for example, all privileged user accounts accessing the Microsoft Azure portal or API should have Multi Factor Authentication (MFA) enabled. MFA ensures only a legitimate user can access the portal and reduces the likelihood of access even if credentials are stolen or leaked. For more information and recommendations, refer to Microsoft Azure Security Center Documentation.

Configure your VNet

In Microsoft Azure, create routable CIDR blocks and set up the required subnets.

- One management subnet with a recommended range of at least /28, to handle:
  - control traffic to on-prem appliances
  - API traffic to cloud-provider API endpoints
- One downlink subnet with a recommended range of /24, for the workload VMs.
- One, or two for HA, uplink subnets with a recommended range of /24, for routing of north-south traffic leaving from or entering the VNet.

See Deploy the NSX Public Cloud Gateway for details on how these subnets are used.

Deploy PCG in a VNet

Follow these instructions to deploy PCG in your Microsoft Azure VNet.

The VNet in which you deploy a PCG can act as a Transit VNet to which other VNets can connect (known as Compute VNets). This VNet can also manage VMs and act as a self-managed VNet.

Follow these instructions to deploy a PCG. If you want to link to an existing Transit VNet, see Link to a Transit VPC or VNet .

Prerequisites

- Your public cloud accounts must be already added into CSM.
- The VNet on which you are deploying PCG must have the required subnets appropriately adjusted for High Availability: *uplink*, *downlink*, and *management*.

Procedure

1. Log in to CSM using an account with the Enterprise Administrator role.
2. Click **Clouds > Azure** and go to the **VNets** tab.
3. Click a VNet where you want to deploy the PCG.
4. Click **Deploy Gateways**. The **Deploy Gateway** wizard opens.
5. For General Properties, use the following guidelines:

Option	Description
SSH Public Key	Provide an SSH public key that can be validated while deploying PCG. This is required for each PCG deployment.
Quarantine Policy on the Associated VNet	You can only change the Quarantine Policy setting if you choose to manage workload VMs using NSX Tools (NSX Enforced Mode). Quarantine Policy is always enabled in the Native Cloud Enforced Mode. Leave this in the default **disabled** mode when you first deploy PCG. You can change this value after onboarding VMs. See **Manage Quarantine Policy** in the *NSX-T Data Center Administration Guide* for details.
Manage with NSX Tools	Leave in the default disabled state to onboard workload VMs in the Native Cloud Enforced Mode. If you want to install NSX Tools on your workload VMs to use the NSX Enforced Mode, enable this option.
Auto-install NSX Tools	This is only available when you enable Manage with NSX Tools. If selected, NSX Tools are auto-installed on all workload VMs in the Transit/Self-managed/linked Compute VNet if the tag `nsx.network=default` is applied to them.
Local Storage Account	When you add a Microsoft Azure subscription to CSM, a list of your Microsoft Azure Storage Accounts is available to CSM. Select the Storage Account from the drop-down menu. When proceeding with deploying PCG, CSM copies the publicly available VHD of the PCG into this Storage Account of the selected region. **Note** If the VHD image has been copied to this storage account in the region already for a previous PCG deployment, then the image is used from this location for subsequent deployments to reduce the overall deployment time.
VHD URL	If you want to use a different PCG image that is not available from the public VMware repository, you can enter the URL of the PCG's VHD here. The VHD must be present in the same account and region where this VNet is created. **Note** The VHD must be in the correct URL format. We recommend that you use the **Click to copy** option in Microsoft Azure.

Option	Description
Proxy Server	Select a proxy server to use for internet-bound traffic from this PCG. The proxy servers are configured in CSM. You can select the same proxy server as CSM if one, or select a different proxy server from CSM, or select **No Proxy Server**. See (Optional) Configure Proxy Servers for details on how to configure proxy servers in CSM.
Advanced	The advanced DNS settings provide flexibility in selecting DNS servers for resolving NSX-T Data Center management components.
Obtain via Public Cloud Provider's DHCP	Select this option if you want to use Microsoft Azure DNS settings. This is the default DNS setting if you do not pick either of the options to override it.
Override Public Cloud Provider's DNS Server	Select this option if you want to manually provide the IP address of one or more DNS servers to resolve NSX-T Data Center appliances as well as the workload VMs in this VNet.
Use Public Cloud Provider's DNS server only for NSX-T Data Center Appliances	Select this option if you want to use the Microsoft Azure DNS server for resolving the NSX-T Data Center management components. With this setting, you can use two DNS servers: one for PCG that resolves NSX-T Data Center appliances; the other for the VNet that resolves your workload VMs in this VNet.

6 Click **Next**.

7 For **Subnets**, use the following guidelines:

Option	Description
Enable HA for NSX Cloud Gateway	Select this option to enable High Availability.
Subnets	Select this option to enable High Availability.
Public IP on Mgmt NIC	Select **Allocate New IP address** to provide a public IP address to the management NIC. You can manually provide the public IP address if you want to reuse a free public IP address.
Public IP on Uplink NIC	Select **Allocate New IP address** to provide a public IP address to the uplink NIC. You can manually provide the public IP address if you want to reuse a free public IP address.

What to do next

Follow instructions at Using NSX Cloud in the *NSX-T Data Center Administration Guide*.

Deploying PCG in a VPC

Ensure the VPC is connected with your on-prem NSX-T Data Center before deploying PCG.

Connect AWS with On-prem NSX-T Data Center

A connection must be established between your Amazon Web Services (AWS) network and your on-prem NSX-T Data Center appliances.

Note You must have already installed and connected NSX Manager with CSM in your on-prem deployment.

Overview

- Connect your AWS account with on-prem NSX Manager appliances using any of the available options that best suit your requirements.
- Configure your VPC with subnets and other requirements for NSX Cloud.

Connect your AWS account with your on-prem NSX-T Data Center deployment

Every public cloud provides options to connect with an on-premises deployment. You can choose any of the available connectivity options that suit your requirements. Refer to AWS Reference Documentation for details.

Note You must review and implement the applicable security considerations and best practices by AWS; refer to AWS Security Best Practices for details.

Configure your VPC

You need the following configurations:

- six subnets for supporting PCG with High Availability
- an Internet gateway (IGW)
- a private and a public route table
- subnet association with route tables
- DNS resolution and DNS hostnames enabled

Follow these guidelines to configure your VPC:

1 Assuming your VPC uses a /16 network, for each gateway that needs to be deployed, set up three subnets.

   Important If using High Availability, set up three additional subnets in a different Availability Zone.

   - **Management subnet**: This subnet is used for management traffic between on-prem NSX-T Data Center and PCG. The recommended range is /28.
   - **Uplink subnet**: This subnet is used for north-south internet traffic. The recommended range is /24.
   - **Downlink subnet**: This subnet encompasses the workload VM's IP address range, and should be sized accordingly. Bear in mind that you may need to incorporate additional interfaces on the workload VMs for debugging purposes.

   Note Label the subnets appropriately, for example, `management-subnet`, `uplink-subnet`, `downlink-subnet`,because you will need to select the subnets when deploying PCG on this VPC.

   See Deploy the NSX Public Cloud Gateway for details.

2 Ensure you have an Internet gateway (IGW) that is attached to this VPC.

3 Ensure the routing table for the VPC has the **Destination** set to `0.0.0.0/0` and the **Target** is the IGW attached to the VPC.

4 Ensure you have DNS resolution and DNS hostnames enabled for this VPC.

Deploy PCG in a VPC

Follow these instructions to deploy PCG in your AWS VPC.

The VPC in which you deploy a PCG can act as a Transit VPC to which other VPCs can connect (known as Compute VPCs). This VPC can also manage VMs and act as a self-managed VPC.

Follow these instructions to deploy a PCG. If you want to link to an existing Transit VPC, see Link to a Transit VPC or VNet .

Prerequisites

- Your public cloud accounts must be already added into CSM.
- The VPC on which you are deploying PCG must have the required subnets appropriately adjusted for High Availability: *uplink*, *downlink*, and *management*.
- The configuration for your VPC's network ACL must include an ALLOW inbound rule.

Procedure

1 Log in to CSM using an account with the Enterprise Administrator role.

2 Click **Clouds > AWS > `<AWS_account_name>`** and go to the **VPCs** tab.

3 In the **VPCs** tab, select an AWS region name, for example, `us-west`. The AWS region must be the same where you created the compute VPC.

4 Select a VPC configured for NSX Cloud.

5 Click Deploy Gateways.

6 Complete the general gateway details:

Option	Description
PEM File	Select one of your PEM files from the drop-down menu. This file must be in the same region where NSX Cloud was deployed and where you created your compute VPC. This uniquely identifies your AWS account.
Quarantine Policy on the Associated VPC	You can only change the Quarantine Policy setting if you choose to manage workload VMs using NSX Tools (NSX Enforced Mode). Quarantine Policy is always enabled in the Native Cloud Enforced Mode Leave this in the default **disabled** mode when you first deploy PCG. You can change this value after onboarding VMs. See **Manage Quarantine Policy** in the *NSX-T Data Center Administration Guide* for details.
Manage with NSX Tools	Leave in the default disabled state to onboard workload VMs in the Native Cloud Enforced Mode. If you want to install NSX Tools on your workload VMs to use the NSX Enforced Mode, enable this option.

Option	Description
Proxy Server	Select a proxy server to use for internet-bound traffic from this PCG. The proxy servers are configured in CSM. You can select the same proxy server as CSM if one, or select a different proxy server from CSM, or select **No Proxy Server**. See (Optional) Configure Proxy Servers for details on how to configure proxy servers in CSM.
Advanced	The advanced settings provide extra options if required.
Override AMI ID	Use this advanced feature to provide a different AMI ID for the PCG from the one that is available in your AWS account.
Obtain via Public Cloud Provider's DHCP	Select this option if you want to use AWS settings. This is the default DNS setting if you do not pick either of the options to override it.
Override Public Cloud Provider's DNS Server	Select this option if you want to manually provide the IP address of one or more DNS servers to resolve NSX-T Data Center appliances as well as the workload VMs in this VPC.
Use Public Cloud Provider's DNS server only for NSX-T Data Center Appliances	Select this option if you want to use the AWS DNS server for resolving the NSX-T Data Center management components. With this setting, you can use two DNS servers: one for PCG that resolves NSX-T Data Center appliances; the other for the VPC that resolves your workload VMs in this VPC.

7 Click Next.

8 Complete the Subnet details.

Option	Description
Enable HA for Public Cloud Gateway	The recommended setting is Enable, that sets up a High Availability Active/Standby pair to avoid an unscheduled downtime.
Primary gateway settings	Select an Availability Zone such as `us-west-1a`, from the drop-down menu as the primary gateway for HA. Assign the uplink, downlink, and management subnets from the drop-down menu.
Secondary gateway settings	Select another Availability Zone such as `us-west-1b`, from the drop-down menu as the secondary gateway for HA. The secondary gateway is used when the primary gateway fails. Assign the uplink, downlink, and management subnets from the drop-down menu.
Public IP on Mgmt NIC	Select **Allocate New IP address** to provide a public IP address to the management NIC. You can manually provide the public IP address if you want to reuse a free public IP address.
Public IP on Uplink NIC	Select **Allocate New IP address** to provide a public IP address to the uplink NIC. You can manually provide the public IP address if you want to reuse a free public IP address.

Click Deploy.

9 Monitor the status of the primary (and secondary, if you selected it) PCG deployment. This process can take 10-12 minutes.

10 Click Finish when PCG is successfully deployed.

What to do next

Follow instructions at Using NSX Cloud in the *NSX-T Data Center Administration Guide*.

Link to a Transit VPC or VNet

You can link one or more compute VPCs or VNets to a Transit VPC or VNet.

Prerequisites

- Verify that you have a Transit VPC or VNet with a PCG.
- Verify that the VPC/VNet you want to link is connected to the Transit VPC or VNet through VPN or peering.
- Verify that the Compute VPC/VNet is in the same region as the Transit VPC/VNet.

Note In route-based IPSec VPN configuration, you must specify the IP address for the virtual tunnel interface (VTI) port. This IP must be in a different subnet than workload VMs. This prevents workload VM inbound traffic from being directed to the VTI port, from which it will be dropped.

Note In the public cloud, a default limit exists for the number of inbound/outbound rules per security group and NSX Cloud creates default security groups. This affects how many Compute VPCs/VNets can be linked to a Transit VPC/VNet. Assuming 1 CIDR block per VPC/VNet, NSX Cloud supports 10 Compute VPCs/VNets per Transit VPC/VNet. If you have more than 1 CIDR in any Compute VPC/VNet, the number of supported Compute VPCs/VNets per Transit VPC/VNet reduces. You can adjust the default limits by reaching out to your public cloud provider.

Procedure

1 Log in to CSM using an account with the Enterprise Administrator role.

2 Click **Clouds > AWS / Azure > <`public cloud_account_name`>** and go to the **VPCs / VNets** tab.

3 In the **VPCs** or **VNets** tab, select a region name where you are hosting one or more compute VPCs or VNets.

4 Select a compute VPC/VNet configured for NSX Cloud.

5 Click **LINK TO TRANSIT VPC** or **LINK TO TRANSIT VNET**

6 Complete the options in the **Link Transit VPC or VNet** window:

Option	Description
Transit VPC or VNet	Select a Transit VPC or VNet from the dropdown menu. The Transit VPC or VNet you select must be already linked with this VPC by way of VPN or peering. **Note** If connecting to a Transit VNet, you must have a DNS forwarder configured in that VNet and the tag `nsx.dnsserver=<IP address of the DNS forwarder>` applied to the Transit VNet. See Microsoft Azure documentation for information on setting up the DNS forwarder.
Default Quarantine Policy	Leave this in the default **disabled** mode when you first deploy PCG. You can change this value after onboarding VMs. See **Manage Quarantine Policy** in the *NSX-T Data Center Administration Guide* for details.
Manage with NSX Tools	Leave in the default disabled state to onboard workload VMs in the Native Cloud Enforced Mode. If you want to install NSX Tools on your workload VMs to use the NSX Enforced Mode, enable this option.
Auto-install NSX Tools	This is only available when you choose to manage with NSX Tools and only for Microsoft Azure VNets. If selected, NSX Tools are auto-installed on all workload VMs in the Transit/Self-managed/linked Compute VNet if the tag `nsx.network=default` is applied to them.

What to do next

Follow instructions at Using NSX Cloud in the *NSX-T Data Center Administration Guide*.

Auto-Configurations after PCG Deployment or Linking

The deployment of PCG in a Transit VPC/VNet and linking a compute VPC/VNet to it triggers necessary configurations in NSX-T Data Center and the public cloud.

Auto-created NSX-T Logical Entities

A set of logical entities are auto-created in NSX Manager.

Log in to NSX Manager to view the auto-created logical entities.

Important Do not delete any of these auto-created entities except if you are manually undeploying PCG. See Troubleshooting PCG Undeployment for details.

System Entities

You can see the following entities under the **System** tab:

Table 12-4. Auto-Created System Entities

Logical System Entity	How many are created?	Nomenclature	Scope
Transport Zones	Two Transport Zones are created for each Transit VPC/VNet	■ TZ-<VPC/VNet-ID>-OVERLAY ■ TZ-<VPC/VNet-ID>-VLAN	Scope: Global
Edge Transport Nodes	One Edge Transport Node is created for each deployed PCG, two if deployed in high availability mode.	■ PublicCloudGatewayTN-<VPC/VNET-ID> ■ PublicCloudGatewayTN-<VPC/VNET-ID>-preferred	Scope: Global
Edge Cluster	One Edge Cluster is created per deployed PCG, whether one or in a high availability pair.	PCG-cluster-<VPC/VNet-ID>	Scope: Global

Inventory Entities

The following entities are available under the **Inventory** tab:

Table 12-5. Groups

Groups	Scope
Two Groups named: ■ `cloud-default-route` ■ `cloud-metadata services`	Scope: Shared across all PCGs
One Group created at the Transit VPC/VNet level as a parent Group for individual segments created at the Compute VPC/VNet level. `cloud-<Transit VPC/VNet ID>-all-segments`	Scope: shared across all Compute VPCs/VNets

Table 12-5. Groups (continued)

Groups	Scope
Two Groups for each Compute VPC/VNet: - Network CIDR Group for all CIDRs of the Compute VPC/VNet: `cloud-<Compute VPC/VNet ID>-cidr` - Local Segment Group for all managed segments within the Compute VPC/VNet:`cloud-<Compute VPC/VNet ID>-local-segments`	Scope: shared across all Compute VPC/VNets
The following Groups are created for the currently supported public cloud services: - `aws-dynamo-db-service-endpoint` - `aws-elb-service-endpoint` - `aws-rds-service-endpoint` - `aws-s3-service-endpoint` - `azure-cosmos-db-service-endpoint` - `azure-load-balancer-service-endpoint` - `azure-sql-service-endpoint` - `azure-storage-service-endpoint`	Scope: Shared across all PCGs

Note For PCGs deployed or linked to in the Native Cloud Enforced Mode, all the workload VMs in the VPC/VNet become available under Virtual Machines in NSX Manager.

Security Entities

The following entities are available under the **Security** tab:

Table 12-6. Auto-Created Security Entities

Logical Security Entity	How many are created?	Nomenclature	Scope
Distributed Firewall (East-West)	Two per Transit VPC/VNet: - Stateless - Stateful	- cloud-stateless-<VPC/VNet ID> - cloud-stateful-<VPC/VNet ID>	- Stateful rule to allow traffic within local managed segments - Stateful rule to reject traffic from unmanaged VMs
Gateway Firewall (North-South)	One per Transit VPC/VNet	cloud-<Transit VPC/VNet ID>	

Networking Entities

The following entities are created at different stages of onboarding and can be found under the **Networking** tab:

Figure 12-3. Auto-created NSX-T Data Center Networking Entities After PCG is Deployed

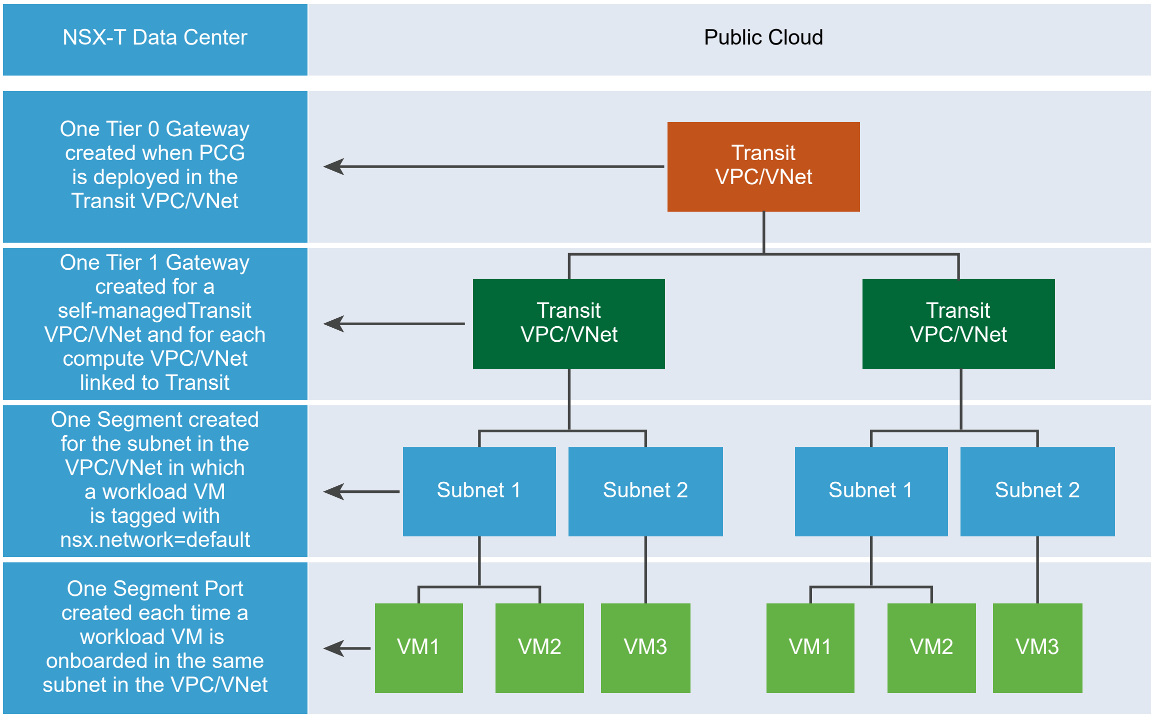

NSX-T Data Center
Public Cloud
One Tier 0 Gateway created when PCG is deployed in the Transit VPC/VNet
Transit VPC/VNet
One Tier 1 Gateway created for a self-managedTransit VPC/VNet and for each compute VPC/VNet linked to Transit
Transit VPC/VNet
Transit VPC/VNet
One Segment created for the subnet in the VPC/VNet in which a workload VM is tagged with nsx.network=default
Subnet 1
Subnet 2
Subnet 1
Subnet 2
One Segment Port created each time a workload VM is onboarded in the same subnet in the VPC/VNet
VM1
VM2
VM3
VM1
VM2
VM3

Table 12-7. Auto-Created Networking Entities

Onboarding Task	Logical Entities Created in NSX-T Data Center
PCG deployed on Transit VPC/VNet	■ Tier-0 Gateway ■ Infra Segment (Default VLAN switch) ■ Tier-1 router
Compute VPC or VNet linked to the Transit VPC/VNet	■ Tier-1 router
A workload VM with the NSX agent installed on it is tagged with the "nsx.network:default" key:value in a subnet of a compute or self-managed VPC/VNet	■ A Segment is created for this specific subnet of the compute or self-managed VPC or VNet ■ Hybrid ports are created for each tagged workload VM that has the NSX agent installed on it
More workload VMs are tagged in the same subnet of the Compute or self-managed VPC/VNet	■ Hybrid ports are created for each tagged workload VM that has the NSX agent installed on it

Forwarding Policies

The following three forwarding rules are set up for a Compute VPC/VNet, including Self-managed Transit VPC/VNet:

- Access any CIDR of the same Compute VPC over the public cloud's network (underlay)
- Route traffic pertaining to public cloud metadata services over the public cloud's network (underlay)
- Route everything not in the Compute VPC/VNet's CIDR block, or a known service, through the NSX-T Data Center network (overlay)

Auto-created Public Cloud Configurations

In your public clouds, some configurations are set up automatically after you deploy PCG.

Some auto configurations are common to all public clouds and both NSX management modes. Other configurations are specific to either the public cloud or the NSX management mode.

Specific to AWS

The following are specific to AWS:

- In the AWS VPC, a new Type A Record Set gets added with the name `nsx-gw.vmware.local` into a private hosted zone in Amazon Route 53. The IP address mapped to this record matches the Management IP address of the PCG which is assigned by AWS using DHCP and will differ for each VPC. This DNS entry in the private hosted zone in Amazon Route 53 is used by NSX Cloud to resolve the PCG's IP address.

  Note When you use custom DNS domain names defined in a private hosted zone in Amazon Route 53, the **DNS Resolution** and **DNS Hostnames** attributes must be set to **Yes** for your VPC settings in AWS.

- A secondary IP for the uplink interface for PCG is created. An AWS Elastic IP is associated with this secondary IP address. This configuration is for SNAT.

Specific to Microsoft Azure

The following are specific to Microsoft Azure:

- A common Resource Group is created per region, per subscription. It is named like: `nsx-default-<region-name>-rg`, for example: `nsx-default-westus-rg`. All VNets in this region share this Resource Group. This Resource Group and all the NSX-created security groups named like default-<vnet-ID>-sg are not deleted from the Microsoft Azure region after you off-board a VNet in this region from NSX Cloud.

Common to both modes and all public clouds

The following are created in all public clouds and for both NSX-management modes: NSX Enforced Mode and Native Cloud Enforced Mode:

- The **gw** security groups are applied to the respective PCG interfaces in VPCs or VNets.

Table 12-8. Public Cloud Security Groups created by NSX Cloud for PCG interfaces

Security Group name	Description
gw-mgmt-sg	Gateway Management Security Group
gw-uplink-sg	Gateway Uplink Security Group
gw-vtep-sg	Gateway Downlink Security Group

Specific to Native Cloud Enforced Mode

The following security groups are created when the PCG is deployed in the Native Cloud Enforced Mode.

After workload VMs are matched with groups and corresponding security policies in NSX Manager, security groups named like `nsx–<GUID>` are created in the public cloud for each matching security policy.

Note In AWS, Security Groups are created. In Microsoft Azure, Application Security Groups are created corresponding to Groups in NSX Manager and Network Security Groups are created corresponding to Security Policies in NSX Manager.

Security Group name	Available in Microsoft Azure?	Available in AWS?	Description
default-vnet-<vnet-id>-sg	Yes	No	NSX Cloud-created security group in the common Microsoft Azure Resource Group for assigning to VMs that are not matched with a security policy in NSX-T Data Center.
default	No	Yes	An existing security group in AWS used by NSX Cloud for assigning to VMs that are not matched with a security policy in NSX-T Data Center.
vm-overlay-sg	Yes	Yes	VM overlay security group (this is not used in the current release)

Specific to NSX Enforced Mode

The following security groups are created for workload VMs when you deploy PCG in the NSX Enforced Mode.

Table 12-9. Public Cloud Security Groups created by NSX Cloud for Workload VMs in the NSX Enforced Mode

Security Group name	Available in Microsoft Azure?	Available in AWS?	Description
default-vnet-<vnet-id>-sg	Yes	No	NSX Cloud-created security group in Microsoft Azure for threat-detection workflows in the NSX Enforced Mode
default	No	Yes	An existing security group in AWS used by NSX Cloud for threat-detection workflows in the NSX Enforced Mode
vm-underlay-sg	Yes	Yes	VM underlay security group
vm-overlay-sg	Yes	Yes	VM overlay security group (this is not used in the current release)

(Optional) Install NSX Tools on your Workload VMs

If you are using the NSX Enforced Mode, proceed to installing NSX Tools in your workload VMs.

See instructions and further details at Onboarding VMs in the NSX Enforced Mode in the *NSX-T Data Center Administration Guide*.

Undeploy or Unlink PCG

You can undeploy or unlink PCG after you have removed some NSX Cloud configurations.

In the NSX Enforced Mode

- Remove the `nsx.network=default` tag from NSX-managed workload VMs.
- Disable the Quarantine Policy if it is enabled.
- Delete all user-created logical entities associated with the PCG.

In the Native Cloud Enforced Mode

- Delete all user-created logical entities associated with the PCG.

Follow the steps relevant to the NSX management mode your PCG is deployed in.

Procedure

1 Remove the nsx.network tag in the Public Cloud

Before you can undeploy PCG, all VMs must be unmanaged.

2 Disable Quarantine Policy in the NSX Enforced Mode

If using the NSX Enforced Mode you must disable Quarantine Policy if previously enabled. .

3 Delete User-created Logical Entities

   All user-created logical entities associated with the PCG must be deleted.

4 **Undeploy or Unlink** from CSM

   Follow these instructions to undeploy or unlink PCG after completing the prerequisites.

5 Troubleshooting PCG Undeployment

   If PCG undeployment fails, you have to manually delete all the NSX Cloud-created entities in NSX Manager as well as in the public cloud.

Remove the nsx.network tag in the Public Cloud

Before you can undeploy PCG, all VMs must be unmanaged.

Note This is only applicable in the NSX Enforced Mode.

Go to the VPC or VNet in your public cloud and remove the `nsx.network=default` tag from the managed VMs.

Disable Quarantine Policy in the NSX Enforced Mode

If using the NSX Enforced Mode you must disable Quarantine Policy if previously enabled. .

This step is only applicable to the NSX Enforced Mode.

With Quarantine Policy enabled, your VMs are assigned security groups in your public cloud that are defined by NSX Cloud.

When you undeploy PCG, you must disable Quarantine Policy. Follow these steps: :

1 Go to the VPC or VNet in CSM.

2 From **Actions > Edit Configurations** >, turn off the setting for **Default Quarantine** .

3 All VMs that are unmanaged or quarantined in this VPC or VNet will be assigned to the `default` security group in AWS and the `default-vnet-<vnet-id>-sg` security group in Microsoft Azure.

4 If there are managed VMs while disabling Quarantine Policy, they retain their NSX Cloud-assigned security groups. The first time you remove the `nsx.network=default` tag from such VMs to take them out from NSX management, they are also assigned to the `default` security group in AWS and the `default-vnet-<vnet-id>-sg` security group in Microsoft Azure.

   Note The common Resource Group created in Microsoft Azure, that is named like: `nsx-default-<region-name>-rg`, for example: `nsx-default-westus-rg`, is not removed when you undeploy PCG. This Resource Group and all the NSX-created security groups named like `default-<vnet-ID>-sg` are not deleted from the Microsoft Azure region. You can remove the NSX Cloud-specific security group any time after the VNet is off-boarded.

See Auto-Configurations after PCG Deployment or Linking for a list of NSX Cloud security groups.

Delete User-created Logical Entities

All user-created logical entities associated with the PCG must be deleted.

Identify entities which are associated with the PCG and delete them.

Note Do not delete the auto-created logical entities. These are deleted automatically after you click **Undeploy** or **Unlink from Transit VPC/VNet** from CSM. See Auto-Configurations after PCG Deployment or Linking for details.

Undeploy or Unlink from CSM

Follow these instructions to undeploy or unlink PCG after completing the prerequisites.

1 Log in to CSM and go to your public cloud:

   - If using AWS, go to **Clouds > AWS > VPCs**. Click on the VPC on which one or a pair of PCGs is deployed and running.
   - If using Microsoft Azure, go to **Clouds > Azure > VNets**. Click on the VNet on which one or a pair of PCGs is deployed and running.

2 Click **Undeploy** or **Unlink from Transit VPC/VNet**.

The default entities created by NSX Cloud are removed automatically when the PCG is undeployed or unlinked.

Troubleshooting PCG Undeployment

If PCG undeployment fails, you have to manually delete all the NSX Cloud-created entities in NSX Manager as well as in the public cloud.

- In your public cloud:
  - Terminate all PCGs in the Transit VPC/VNet.
  - Move all your workload VMs to a security group not created by NSX Cloud.
  - Delete the NSX Cloud-created security groups in the public cloud as listed here: Auto-created Public Cloud Configurations .
  - For Microsoft Azure, also delete the NSX Cloud-created Resource Group named like `nsx-gw-<vnet ID>-rg`.
- Resync your public cloud inventory in CSM.
- Delete the auto-created entities with the VPC/VNet ID in NSX Manager as listed here: Auto-created NSX-T Logical Entities.

  Note Do not delete the global entities that are auto-created. Only delete the ones that have the VPC/VNet ID in their name.

Getting Started with Federation 13

To get started with Federation, you install a Global Manager appliance, configure the appliance as active, and add locations.

Task	Details
Check the requirements for Federation.	See Federation Requirements.
Install a Global Manager appliance.	See Install a Global Manager Appliance.
Make the Global Manager cluster active.	See Make the Global Manager Active.
Add Locations to the active Global Manager.	See Add a Location .

For further configuration tasks, such as preparing Edge clusters for stretched networking, and creating objects from the Global Manager, see *Federation* in the *NSX-T Data Center Administration Guide*.

Procedure

1 Federation Requirements

To support Federation, your environment must meet the following requirements.

2 Install a Global Manager Appliance

To use Federation, you must install a Global Manager appliance.

3 Configuring the Global Manager and Local Managers

A Federation environment contains a Global Manager and up to three Local Manager clusters.

Federation Requirements

To support Federation, your environment must meet the following requirements.

- There must be a latency of 150 ms or less between locations with the Federation environment.
- The Global Manager and all Local Managers must have NSX-T Data Center 3.0 installed.
- The required ports must be open to allow communication between the Global Manager and Local Managers. See VMware Ports and Protocols at https://ports.vmware.com/home/NSX-T-Data-Center.
- There must be connectivity without NAT between the following:
  - Global Manager and Local Manager.
  - Local Manager and remote Local Manager.

  - Edge node RTEP and remote Edge node RTEP.
- Global Manager supports only Policy Mode. Federation does not support Manager Mode. See Overview of the NSX Manager for more information.

A Federation environment has the following configuration maximums:

- For most configurations, the Local Manager cluster has the same configuration maximums as an NSX Manager cluster. Go to VMware Configuration Maximums tool and select NSX-T Data Center.

  Select the Federation category for NSX-T Data Center in the VMware Configuration Maximums tool for exceptions and other Federation-specific values.
- For a given location, the following configurations contribute to the configuration maximum:
  - Objects that were created on the Local Manager.
  - Objects that were created on the Global Manager and include the location in its span.

  You can view the capacity and usage on each Local Manager. See *View the Usage and Capacity of Categories of Objects* in the *NSX-T Data Center Administration Guide*.

Install a Global Manager Appliance

To use Federation, you must install a Global Manager appliance.

Installing a Global Manager appliance is similar to installing an NSX Manager appliance. The only difference is that when you deploy the appliance, you select *NSX Global Manager* for the **Rolename**.

Important Do not configure the Global Manager node to publish its FQDN. You can restore a Global Manager only from an IP address and not from an FQDN.

Prerequisites

- Verify that your environment meets the requirements for NSX Manager installation. See NSX Manager VM and Host Transport Node System Requirements.
- Decide which location will contain the Global Manager.
- Verify that you are installing the Global Manager appliance with NSX-T Data Center 3.0.

Procedure

1 Install a Global Manager.

  - If you are installing Global Manager on vSphere, follow these instructions: Install NSX Manager and Available Appliances.
    - Select *Small* for the deployment configuration size. Select *NSX Global Manager* for the **Rolename**.
    - Select *Small* for the appliance size.

    Install only one appliance, do not install a cluster.

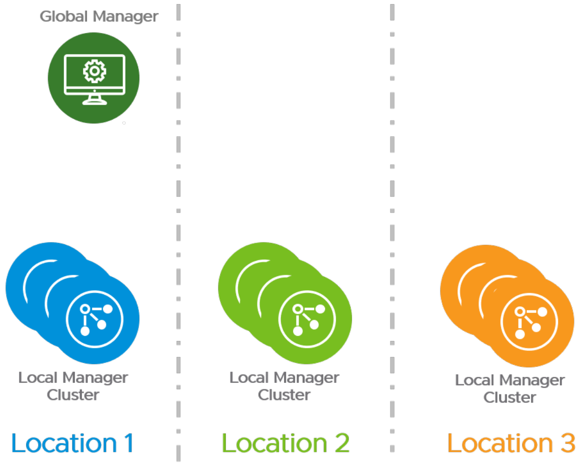
- If you are installing Global Manager on KVM, follow these instructions: Install NSX Manager on KVM.
  - Select *Small* for the deployment configuration size. Select *NSX Global Manager* for the **Rolename**.
  - Select *Small* for the appliance size.

  Install only one appliance, do not install a cluster.

2 Disable snapshots for the Global Manager appliance. See Disable Snapshots on NSX-T Data Center Appliances.

Configuring the Global Manager and Local Managers

A Federation environment contains a Global Manager and up to three Local Manager clusters.



Make the Global Manager Active

After you have deployed a Global Manager appliance, you can make the Global Manager active.

Procedure

1 Log in to the Global Manager appliance at https://global-manager-ip-or-fqdn/.

2 Select **System > Location Manager**. In the **Global Manager** tile, click **Make Active**. Provide a descriptive name for the active Global Manager and click **Save**.

Add a Location

After you add a location to Global Manager, you can create objects from Global Manager that span that location.

You can add up to three locations to a Global Manager.

After you add a location to the Global Manager, the NSX Manager is called a Local Manager.

Prerequisites

- Verify that you have an NSX-T Data Center environment installed in the location you want to add.

  You can add a new NSX-T Data Center environment or an NSX-T Data Center environment with an existing configuration.

- The NSX-T Data Center environment in the new location must have three NSX Manager nodes deployed and a cluster VIP or an external load balancer configured. See Configure a Virtual IP (VIP) Address for a Cluster.

  For a proof-of-concept environment, you can add a location that has only one NSX Manager node, but you must still configure a cluster VIP or an external load balancer.

- Verify that the latency between the Global Manager and the location is 150 ms or less.
- Verify that the environment you are adding has NSX-T Data Center 3.0 installed.

Procedure

1 Log in to the Global Manager at https://global-manager-ip-or-fqdn/.

2 Select **System > Location Manager** and click **Add On-Prem Location**.

3 In the **Add New Location** dialog box, enter the Location details.

Option	Description
Location Name	Provide a name for the location.
FQDN/IP	Enter the FQDN or IP address of the NSX Manager cluster VIP or external load balancer. Do not enter an individual NSX Manager FQDN or IP.
Username and Password	Provide the admin user's credentials for the NSX Manager at the location.

Option	Description

SHA-256 Thumbprint	There are two ways you can get the cluster SHA-256 thumbprint:
	■ If the NSX Manager cluster has a cluster VIP configured, you can log into any NSX Manager node in the cluster and run this command:
	`get certificate cluster thumbprint`
	The result is the cluster VIP certificate:
	`bfae1a0a...`
	■ If the NSX Manager cluster has an external load balancer configured, you can get the thumbprint using the `openssl` command. Log into a system that has OpenSSL installed, such as a Linux server, and run this command:
	`echo -n | openssl s_client -connect` *`cluster-fqdn-or-ip`*`:443 2>/dev/null | openssl x509 -noout -fingerprint -sha256`
	The result is the cluster VIP certificate:
	`SHA256 Fingerprint=BF:AE:1A:0A...`
	For *cluster-fqdn-or-ip*, use the same FQDN or IP that you provided earlier in the **FQDN/IP** text box.
	The thumbprint is accepted with or without colons. Omit the text before the thumbprint: `SHA256 Fingerprint=`.

Check Compatibility	Click **Check Compatibility** to ensure that the location can be added. This checks that the NSX-T Data Center version is compatible.

4 Click **Save**.

The location is added to the Global Manager. Information about all locations is displayed on the **System > Location Manager** page.

Uninstalling NSX-T Data Center from a Host Transport Node 14

The steps to uninstall NSX-T Data Center from a host transport node vary depending on the host type and how it is configured.

- Verify Host Network Mappings for Uninstall

  Before you uninstall NSX-T Data Center from an ESXi host, verify that you have appropriate network mappings for uninstall configured. The mappings are required if the ESXi host has VMkernel interfaces connected to N-VDS.

- Uninstall NSX-T Data Center from a vSphere Cluster

  If you have installed NSX-T Data Center on a vSphere Cluster using transport node profiles, you can follow these instructions to uninstall NSX-T Data Center from all hosts in the cluster.

- Uninstall NSX-T Data Center from a Host in a vSphere Cluster

  You can uninstall NSX-T Data Center from a single host that is managed by vCenter Server. The other hosts in the cluster are not affected.

- Uninstall NSX-T Data Center from a Standalone Host

  You can uninstall NSX-T Data Center from a standalone host. Standalone hosts can be ESXi or KVM.

- Triggering Uninstallation from the vSphere Web Client

  In the vSphere Web Client. if you move a host from a cluster prepared with a transport node profile to either another cluster, outside of the cluster as a standalone host, or outside of the data center, then NSX-T Data Center is uninstalled on the host that is moved. Such an uninstallation is not triggered when a host that is individually prepared with a transport node configuration is moved.

Verify Host Network Mappings for Uninstall

Before you uninstall NSX-T Data Center from an ESXi host, verify that you have appropriate network mappings for uninstall configured. The mappings are required if the ESXi host has VMkernel interfaces connected to N-VDS.

The uninstall mapping determines where the interfaces are connected after the uninstall. There are uninstall mappings for physical interfaces (vmnicX) and VMkernel interfaces (vmkX). When you uninstall, VMkernel interfaces are moved from their current connections to the port groups specified in the uninstall mapping. If a physical interface is included in the uninstall mapping, the physical interface is connected to the appropriate vSphere Distributed Switch or vSphere Standard Switch based on the destination port group of the VMkernel interfaces.

Caution Uninstalling NSX-T Data Center from an ESXi host is disruptive if the physical interfaces or VMkernel interfaces are connected to N-VDS. If the host or cluster is participating in other applications such as vSAN, those applications might be affected by the uninstall.

There are two places that you can configure network mappings for uninstall.

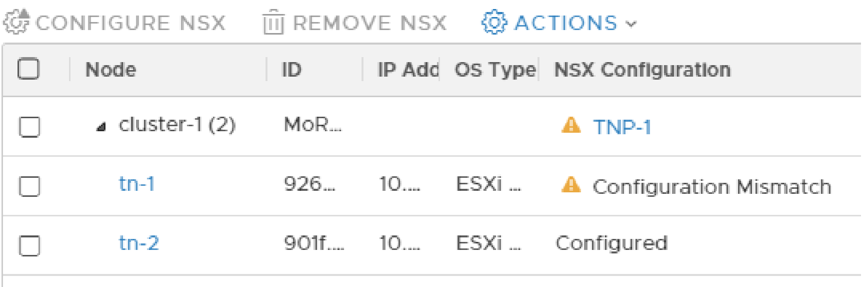
- In the transport node configuration, which applies to that host.
- In a transport node profile configuration, which can then be applied to a cluster.

  Note You must have a compute manager configured to apply a transport node profile to a cluster.

If a compute manager is configured, a host can have both a transport node configuration and a transport node profile configuration. The most recently applied configuration is active. Verify that the network mappings for uninstall are correctly configured on the active configuration.

Transport node configuration on a node cannot be overriden if underlying segments or VMs are connected to that transport node. For example, consider a two ESXi host cluster, where host-1 is configured as transport-node-1, but host-2 is unprepared. Segments and VMs are connected to transport-node-1. After preparing host-1 as a transport node (associated to transport-zone-1), if you apply a transport node profile to that cluster (associated to transport-zone-2), then NSX-T does not override the transport node configuration with the transport node profile configuration. To successfully override configuration on host-1, power off the VMs and disconnect the segment before applying the transport node profile to associate host-1 to transport-zone-2 and disassociate it from transport-zone-1.

In this example, the cluster cluster-1 has transport node profile TNP-1 applied to it. The host tn-1 is displaying `Configuration Mismatch`. This mismatch message indicates that a different configuration has been applied to tn-1 after the transport node profile was applied. Transport node tn-2 uses the network mappings from the transport node profile, and transport node tn-1 uses its own configuration.



☐	Node	ID	IP Add	OS Type	NSX Configuration
☐	cluster-1 (2)	MoR...			⚠ TNP-1
☐	tn-1	926...	10....	ESXi ...	⚠ Configuration Mismatch
☐	tn-2	901f....	10....	ESXi ...	Configured

Prerequisites

- Verify that you have appropriate port groups configured to use in the uninstall mapping. You must use vSphere Distributed Switch ephemeral port groups or vSphere Standard Switch port groups.
- Configure a compute manager if you want to use a vSphere Distributed Switch port group in the uninstall mappings for a standalone ESXi host. See Add a Compute Manager. If there is no compute manager configured, you must use a vSphere Standard Switch port group.

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Select **System > Fabric > Nodes > Host Transport Nodes**.
3. For each host (on N-VDS Switch) you want to uninstall, verify that the network mapping for uninstall includes a port group for each VMkernel interface that is on N-VDS. Add any missing mappings.

   Important

   - The port group in the network mapping for uninstall must be a vSphere Distributed Switch ephemeral port group or a vSphere Standard Switch port group.

   a. To view VMkernel interfaces, log in vCenter Server, select the host, and click **Configure > VMkernel Adapters**.

   b. If the transport node configuration is the active configuration, select the host and click **Edit** (for standalone hosts) or **Configure NSX** (for managed hosts). Click **Next**, then click **Network Mappings for Uninstall**. View the mappings in the **VMKNic Mappings** and **Physical NIC Mappings** tabs.

   c. If the transport node profile is the active configuration, click the name of the transport node profile for the cluster in the **NSX Configuration** column and click **Edit**. On the **Host Switch** tab, click **Network Mappings for Uninstall**. View the mappings in the **VMKNic Mappings** and **Physical NIC Mappings** tabs.
4. For each host (on a VDS Switch) you want to uninstall:

   a. As the NSX Manager UI does not allow you to configure network mapping for install or uninstall when the host switch is vSphere Distributed Switch, ensure that you migrate back any VMkernel adapters connected to NSX port groups to either a Distributed Virtual port group or a VSS port group from vCenter Server. Uninstallation fails if there are any VMkernel adapters attached to an NSX port groups on VDS.

Uninstall NSX-T Data Center from a vSphere Cluster

If you have installed NSX-T Data Center on a vSphere Cluster using transport node profiles, you can follow these instructions to uninstall NSX-T Data Center from all hosts in the cluster.

For more information on transport node profiles, see Add a Transport Node Profile.

Caution Uninstalling NSX-T Data Center from an ESXi host is disruptive if the physical interfaces or VMkernel interfaces are connected to N-VDS. If the host or cluster is participating in other applications such as vSAN, those applications might be affected by the uninstall.

If you have not used a transport node profile to install NSX-T Data Center, or if you want to remove NSX-T Data Center from a subset of the hosts in the cluster, see Uninstall NSX-T Data Center from a Host in a vSphere Cluster.

Note Removing a host from a cluster does not uninstall NSX-T Data Center. Follow these instructions to uninstall NSX-T Data Center from a host in a cluster: Uninstall NSX-T Data Center from a Host in a vSphere Cluster.

Prerequisites

- Verify that the hosts you want to uninstall have network uninstall mappings configured. See Verify Host Network Mappings for Uninstall.
- Verify that the hosts you want to uninstall are in maintenance mode in vSphere.

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Select **System > Fabric > Nodes > Host Transport Nodes**.
3. From the **Managed by** drop-down menu, select the vCenter Server.
4. Select the cluster you want to uninstall, and click **Remove NSX**.
5. Verify that the NSX-T Data Center software is removed from the host.
   a. Log into the host's command-line interface as root.
   b. Run this command to check for NSX-T Data Center VIBs

      ```
      esxcli software vib list | grep -E 'nsx|vsipfwlib'
      ```

      If the NSX-T Data Center software is successfully removed, no VIBs are listed. If any NSX VIBs remain on the host, contact VMware Support.

Uninstall NSX-T Data Center from a Host in a vSphere Cluster

You can uninstall NSX-T Data Center from a single host that is managed by vCenter Server. The other hosts in the cluster are not affected.

Caution Uninstalling NSX-T Data Center from an ESXi host is disruptive if the physical interfaces or VMkernel interfaces are connected to N-VDS. If the host or cluster is participating in other applications such as vSAN, those applications might be affected by the uninstall.

Prerequisites

- Verify that the hosts you want to uninstall have network uninstall mappings configured. See Verify Host Network Mappings for Uninstall.
- Verify that the hosts you want to uninstall are in maintenance mode in vSphere.

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Select **System > Fabric > Nodes > Host Transport Nodes**.
3. From the **Managed by** drop-down menu, select the vCenter Server.
4. If the cluster has a transport node profile applied, select the cluster, and click **Actions > Detach TN Profile**.

   If the cluster has a transport node profile applied, the **NSX Configuration** column for the cluster displays the profile name.
5. Select the host and click **Remove NSX**.
6. Verify that the NSX-T Data Center software is removed from the host.

   a. Log into the host's command-line interface as root.

   b. Run this command to check for NSX-T Data Center VIBs

   ```
   esxcli software vib list | grep –E 'nsx|vsipfwlib'
   ```

   If the NSX-T Data Center software is successfully removed, no VIBs are listed. If any NSX VIBs remain on the host, contact VMware Support.
7. If the cluster had a Transport Node Profile applied, and you want to reapply it, select the cluster, click **Configure NSX**, and select the profile from the **Select Deployment Profile** drop-down menu.

Uninstall NSX-T Data Center from a Standalone Host

You can uninstall NSX-T Data Center from a standalone host. Standalone hosts can be ESXi or KVM.

Caution Uninstalling NSX-T Data Center from an ESXi host is disruptive if the physical interfaces or VMkernel interfaces are connected to N-VDS. If the host or cluster is participating in other applications such as vSAN, those applications might be affected by the uninstall.

Prerequisites

If you are uninstalling NSX-T Data Center from a standalone ESXi host, verify the following settings:

- Verify that the hosts you want to uninstall have network uninstall mappings configured. See Verify Host Network Mappings for Uninstall.
- Verify that the hosts you want to uninstall are in maintenance mode in vSphere.

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Select **System > Fabric > Nodes > Host Transport Nodes**.
3. From the **Managed by** drop-down menu, select **None: Standalone Hosts**.
4. Select the host and click **Delete**. In the confirmation dialog box that is displayed, make sure **Uninstall NSX Components** is selected, and **Force Delete** is deselected. Click **Delete**.

   The NSX-T Data Center software is removed from the host. It might take up to 5 minutes for all NSX-T Data Center software to be removed.
5. If the uninstall fails, select the host and click **Delete** again. In the confirmation dialog box, deselect **Uninstall NSX Components** and select **Force Delete**.

   The host transport node is deleted from the management plane, but the host might still have NSX-T Data Center software installed.

6 Verify that the NSX-T Data Center software is removed from the host.

   a Log into the host's command-line interface as root.

   b Run the appropriate command to check for NSX-T Data Center software packages.

Table 14-1. Package List Commands

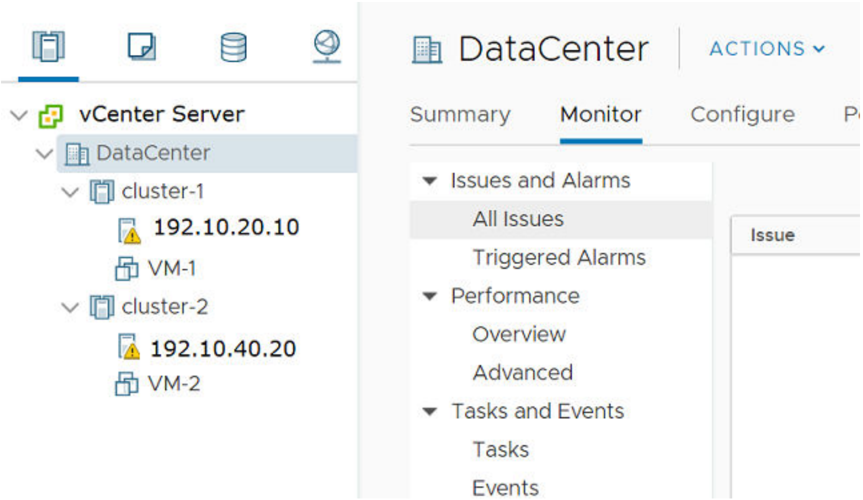
<table>
<tr><th>Host Operating System</th><th>Command</th></tr>
<tr><td>ESXi</td><td><code>esxcli software vib list | grep -E 'nsx|vsipfwlib'</code></td></tr>
<tr><td>Red Hat Enterprise Linux and CentOS Linux</td><td><code>rpm -qa | grep -E 'nsx|vsipfwlib'</code></td></tr>
<tr><td>Ubuntu</td><td><code>dpkg -l | grep -E 'nsx|vsipfwlib'</code></td></tr>
<tr><td>SUSE Linux Enterprise Server</td><td><code>zypper packages --installed-only | grep -E 'nsx|vsipfwlib'</code></td></tr>
</table>

If the NSX-T Data Center software is successfully removed, no packages are listed. If any NSX software packages remain on the host, contact VMware Support.

Triggering Uninstallation from the vSphere Web Client

In the vSphere Web Client. if you move a host from a cluster prepared with a transport node profile to either another cluster, outside of the cluster as a standalone host, or outside of the data center, then NSX-T Data Center is uninstalled on the host that is moved. Such an uninstallation is not triggered when a host that is individually prepared with a transport node configuration is moved.

NSX-T Data Center Uninstallation Scenarios from the vSphere Web Client



Action	Steps/Description	Result
In the vCenter Server, move an ESXi host in cluster-1 (prepared by applying transport node profile) to the data center as a standalone host (not to another cluster).	1 From the vSphere Web Client, log in to the vCenter Server. 2 Move the host in maintenance mode. 3 Move the host from cluster-1 that is prepared with a transport node profile out of the cluster as a standalone managed host. NSX-T Data Center triggers uninstallation of the configuration and NSX-T VIBs. 4 During uninstallation, the transport node is deleted, NSX-T Data Center VIBs are uninstalled. 5 In the NSX-T Data Center UI, the uninstalled host is displayed under **Other Hosts** on the same vCenter Server.	The host is turned into a standalone managed host, which is displayed under 'Other Hosts'. NSX-T Data Center is uninstalled on the host. If the host is under Configuration Mismatch state, then the host remains in that state after it is moved.
In the vCenter Server, move a prepared host from cluster-1 with transport node profile-1 to cluster-2 with transport node profile-2.	1 From the vSphere Web Client, log in to the vCenter Server. 2 Move the host in maintenance mode. 3 As cluster-1 is prepared with transport node profile-1, when a host from cluster-1 is moved to cluster-2, then transport node profile-2 is applied to the host. Only the new transport node profile-2 configuration is applied to the host, whereas NSX-T Data Center VIBs are not uninstalled from the host. 4 If the NSX-T Data Center host is in a failed configuration state, then it is not configured after it moves to cluster-2. The host remains in the failed state.	The host is moved from cluster-1 to cluster-2. A successfully configured host is applied with transport node profile-2. If the host is in the failed state, ensure that the host is successfully configured in NSX-T Data Center.
In the vCenter Server, move a host that is in the Configuration Mismatch state (NSX-T Data Center state) from cluster-1 with transport node profile-1 to cluster-2 with transport node profile-2.	1 From the vSphere Web Client, log in to the vCenter Server. 2 Move the host in maintenance mode. 3 As the host is in the Configuration Mismatch state, even though it is moved to cluster-2, transport node profile-2 is not applied to it.	The host remains in Configuration Mismatch state.
In the vCenter Server, move a host from cluster-1 with transport node profile-1 to cluster-3 not applied with any transport node profile.	1 From the vSphere Web Client, log in to the vCenter Server. 2 Move the host in maintenance mode. 3 Move the host from cluster-1 to cluster-3.	If the NSX-T Data Center host is successfully configured, then NSX-T Data Center uninstallation begins on the host. If the NSX-T Data Center host is in the failed configuration state, then after it moves to cluster-3 the node remains in the failed state.

Action	Steps/Description	Result
In the vCenter Server, delete a host that is in the Configuration Mismatch state (NSX-T Data Center state) because the host has two different configurations applied to it - transport node configuration and transport node profile configurations.	1 From the vSphere Web Client, log in to the vCenter Server. 2 Move the host in maintenance mode. 3 Remove the host from the vCenter Server inventory.	Uninstallation of NSX-T Data Center does not begin because the node configuration was in the Configuration Mismatch state. To ensure that uninstallation begins, ensure that the transport node is configured with a single configuration, either at the host-level or at the cluster-level. After uninstallation, go to the NSX Manager UI and verify that the managed host is moved out of the cluster to become a standalone unmanaged host.
In the vCenter Server, move a prepared host from cluster-1 with transport node profile-1 applied to: ■ Another cluster without any transport node profile applied ■ Data center ■ Outside of the data center	1 From the vSphere Web Client, log in to the vCenter Server. 2 Move the host in maintenance mode. 3 Perform one of the actions: ■ Move the host to another cluster without any transport node profile applied. ■ Move the host as a standalone host in the data center. ■ Move the host to outside of the data center	NSX-T is uninstalled from the host.

Troubleshooting Installation Issues

15

A list of issues related to NSX-T Data Center installation and configuration

Issue	Solution
vCenter Server and/or ESXi hosts are showing opaque networks after removing NSX-T from host or cluster	https://ikb.vmware.com/s/article/75234
Installation Fails Due to Insufficient Space in Bootbank on ESXi Host	https://kb.vmware.com/s/article/74864

This chapter includes the following topics:

- Installation Fails Due to Insufficient Space in Bootbank on ESXi Host

Installation Fails Due to Insufficient Space in Bootbank on ESXi Host

NSX-T Data Center installation might fail if there is insufficient space in the bootbank or in the alt-bootbank on an ESXi host.

Problem

On the ESXi host, you might see a similar log (`esxupdate.log`) message:

```
20**-**-**T13:37:50Z esxupdate: 5557508: BootBankInstaller.pyc:
ERROR: The pending transaction requires 245 MB free space,
however the maximum supported size is 239 MB.^@
```

Cause

Unused VIBs on the ESXi host can be relatively large in size. These unused VIBs can result in insufficient space in the bootbank or in the alt-bootbank when installing the required VIBs.

Solution

- Uninstall the VIBs that are no longer required and free up additional disk space.

For more information on deleting the unused VIBs, see the VMware knowledge base article at https://kb.vmware.com/s/article/74864.