NSX-T Data Center Installation Guide

Modified on 9 SEPT 2024
VMware NSX-T Data Center 3.2

vmware by Broadcom

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

https://docs.vmware.com/

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

Copyright © 2017-2024 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to https://www.broadcom.com. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Contents

NSX-T Data Center Installation Guide 9

1 Overview of NSX-T Data Center 10
- Key Concepts 11
- NSX Manager 14
  - Configure the User Interface Settings 17

2 NSX-T Data Center Installation Workflows 19
- NSX-T Data Center Workflow for vSphere 19
- NSX-T Data Center Installation Workflow for KVM 20
- NSX-T Data Center Configuration Workflow for Bare Metal Server 20

3 Preparing for Installation 22
- System Requirements 22
  - NSX Manager VM and Host Transport Node System Requirements 22
  - NSX Edge VM System Requirements 26
  - NSX Edge Bare Metal Requirements 28
  - Bare Metal Server System Requirements 32
  - Bare Metal Linux Container Requirements 33
- Ports and Protocols 33

4 NSX Manager Installation 34
- Modifying the Default Admin Password Expiration 38

5 NSX Manager Cluster Requirements 40
- Cluster Requirements for an Individual Site 41
- Cluster Requirements for Multiple Sites 42

6 Installing and Configuring NSX-T using vCenter Server Plugin 44
- Install NSX Manager from vSphere Client 44
- Configure NSX-T for Virtual Networking from vSphere Client 48
- Configuring NSX-T for Security from vSphere Client 53
  - Prepare Clusters for NSX-T Security 54
  - Add vCenter Server and NSX Manager to Distributed Firewall Exclusion List 55
  - Create Groups 56
  - Define and Publish Communication Strategies for Groups 58

7 Installing NSX Manager Cluster on vSphere 61

Install NSX Manager and Available Appliances 61
Install NSX Manager on ESXi Using the Command-Line OVF Tool 65
Configure an Appliance to Display the GRUB Menu at Boot Time 72
Log In to the Newly Created NSX Manager 73
Add a Compute Manager 73
Deploy NSX Manager Nodes to Form a Cluster from the UI 77
Configure a Virtual IP Address for a Cluster 85
Configuring an External Load Balancer 87
Disable Snapshots on an NSX Appliance 90

8 Installing NSX Manager Cluster on KVM 91
Set Up KVM 91
Manage Your Guest VMs in the KVM CLI 94
Deploy an NSX Manager Cluster on KVM 95
Install NSX Manager on KVM 95
Form an NSX Manager Cluster Using the CLI 101

9 Transport Zones and Profiles 104
Create Transport Zones 104
Create an IP Pool for Tunnel Endpoint IP Addresses 106
Enhanced Data Path 108
Configuring Profiles 111
Create an Uplink Profile 111
Configuring Network I/O Control Profiles 115
Add an NSX Edge Cluster Profile 124
Add an NSX Edge Bridge Profile 125
VMkernel Migration to an N-VDS Switch 126
VMkernel Migration Errors 132

10 Host Transport Nodes 136
Manual Installation of NSX-T Data Center Kernel Modules 136
Manually Install NSX-T Data Center Kernel Modules on ESXi Hypervisors 136
Manually Install NSX-T Data Center Software Packages on Ubuntu KVM Hypervisors 140
Manually Install NSX-T Data Center Software Packages on RHEL and CentOS Linux KVM Hypervisors 141
Manually Install NSX-T Data Center Software Packages on SUSE KVM Hypervisors 142
Install Third-Party Packages on a KVM Host 143
Verify Open vSwitch Version on RHEL or CentOS Linux KVM Hosts 145
Verify Open vSwitch Version on SUSE KVM Hosts 146
Verify Open vSwitch Version on Ubuntu KVM Hosts 147
Preparing Physical Servers as NSX-T Data Center Transport Nodes 148
Install Third-Party Packages on a Physical Server 149

Configure a Physical Server as a Transport Node from GUI 151
Ansible Server Configuration for Physical Server 158
Create Application Interface for Physical Server Workloads 159
Secure Workloads on Windows Server 2016/2019 Bare Metal Servers 159
Prepare Standalone Hosts as Transport Nodes 161
Preparing ESXi and KVM Hosts as Transport Nodes 169
Transport Node Profiles 169
Sub-TNPs and Sub-clusters 170
Prepare a vSphere Distributed Switch for NSX-T 172
Add a Transport Node Profile 173
Prepare ESXi Cluster Hosts as Transport Nodes 178
Change Sub-cluster 185
Detach Cluster TNP 185
Migrate VMkernels and Physical NICs to a vSphere Distributed Switch 186
Configure an ESXi Host Transport Node with Link Aggregation 188
Prepare Clusters for Networking and Security Using Quick Start Wizard 190
Prepare Clusters for Networking and Security 190
Install Distributed Security for vSphere Distributed Switch 192
Deploy a Fully Collapsed vSphere Cluster NSX-T on Hosts Running N-VDS Switches 193
Multiple NSX Managers Managing a Single vCenter Server 203
Troubleshoot Multi-NSX Issues 206
Cannot Enable Multiple NSX-T on Single vCenter Server 206
Override NSX-T Ownership Constraints 207
Preparing Standalone Host Cluster Results in Failure 209
Traffic Performance Issues Related to NSX Edge VMs in Multiple NSX-T Data Center Environment 209
Managing Transport Nodes 211
Switch Visualization 211
NSX Maintenance Mode 211
Migrate ESXi VMkernel and Physical Adapters 212
Health Check VLAN ID Ranges and MTU Settings 213
View Bidirectional Forwarding Detection Status 217
Verify the Transport Node Status 218

11 Installing NSX Edge 221
NSX Edge Installation Requirements 221
NSX Edge Networking Setup 224
NSX Edge Installation Methods 231
Create an NSX Edge Transport Node 232
Create an NSX Edge Cluster 238
Install an NSX Edge on ESXi Using the vSphere GUI 239
Install NSX Edge on ESXi Using the Command-Line OVF Tool 243

Install NSX Edge via ISO File as a Virtual Appliance 248
Install NSX Edge on Bare Metal 251
Prepare a PXE Server for NSX Edge 253
Install NSX Edge Automatically via ISO File 257
Install NSX Edge Interactively via ISO File 261
Intel QAT Support for IPSec VPN Bulk Cryptography 263
Join NSX Edge with the Management Plane 264
Configure an NSX Edge as a Transport Node 266
Remove NSX Edge Nodes from an Edge Cluster 268

12 vSphere Lifecycle Manager with NSX-T 271
Prepare an NSX-T Cluster with vSphere Lifecycle Manager 272
Enable vSphere Lifecycle Manager on an NSX-T Cluster 274
NSX-T with vSphere Lifecycle Manager Scenarios 277
vSphere Lifecycle Manager Failed to Prepare a Host for NSX-T Networking 278
vSphere Lifecycle Manager Failed to Prepare NSX-T Cluster 279
Delete a NSX-T Depot on vCenter Server 280

13 Host Profile integration with NSX-T 281
Auto Deploy Stateless Cluster 281
High-Level Tasks to Auto Deploy Stateless Cluster 281
Prerequisites and Supported Versions 282
Create a Custom Image Profile for Stateless Hosts 283
Associate the Custom Image with the Reference and Target Hosts 284
Set Up Network Configuration on the Reference Host 285
Configure the Reference Host as a Transport Node in NSX-T 286
Extract and Verify the Host Profile 289
Verify the Host Profile Association with Stateless Cluster 291
Update Host Customization 291
Trigger Auto Deployment on Target Hosts 292
Troubleshoot Host Profile and Transport Node Profile 301
Stateful Servers 304
Supported NSX-T and ESXi versions 304
Prepare a Target Stateful Cluster 305
VMkernel Migration with Host Profile Applied 306
VMkernel Migration without Host Profile Applied 308

14 Getting Started with NSX Federation 309
NSX Federation Key Concepts 309
NSX Federation Requirements 310
Configuring the Global Manager and Local Managers 311

Install the Active and Standby Global Manager 312
Make the Global Manager Active and Add Standby Global Manager 314
Add a Location 315
Remove a Location 321

15 Install NSX Advanced Load Balancer Appliance Cluster 323
Troubleshooting NSX Advanced Load Balancer Controller Issues 326
NSX Advanced Load Balancer does not register with NSX Manager 326
The Second NSX Advanced Load Balancer Controller Remains in Queued State 326
NSX Advanced Load Balancer Controller Password Change Caused Cluster Failure 327
Unable to Delete NSX Advanced Load Balancer Controller 327
NSX Advanced Load Balancer Cluster HA Status is Compromised 328
Credential Mismatch After Changing NSX Advanced Load Balancer Controller Password 328
Deployment of NSX Advanced Load Balancer Controller Failed 329
Cluster Unstable After Two Controllers Are Down 330

16 Getting Started with NSX Cloud 331
NSX Cloud Architecture and Components 332
Overview of Deploying NSX Cloud 333
Deploy NSX-T Data Center On-Prem Components 333
Install CSM 333
Join CSM with NSX Manager 334
Specify CSM IPs for Access by PCG 335
(Optional) Configure Proxy Servers 335
(Optional) Set Up vIDM for Cloud Service Manager 336
Connect your Public Cloud with On-prem NSX-T Data Center 337
Deploy NSX Cloud Components in Microsoft Azure using the NSX Cloud Marketplace Image 339
Deploy NSX Cloud Components in Microsoft Azure using Terraform scripts 341
Deploy NSX Cloud Components in Microsoft Azure without using Terraform scripts 346
Add your Public Cloud Account 350
Adding your Microsoft Azure Subscription 351
Adding your AWS Account 357
Managing Regions in CSM 361
NSX Public Cloud Gateway: Architecture and Modes of Deployment 362
Deploy PCG or Link to a PCG 366
Deploy PCG in a VNet 366
Deploy PCG in a VPC 369
Link to a Transit VPC or VNet 372
Auto-Configurations after PCG Deployment or Linking 373
Auto-created NSX-T Data Center Logical Entities 373

Auto-created Public Cloud Configurations 377
Integrate Horizon Cloud Service with NSX Cloud 379
Auto-Created Entities After Horizon Cloud Integration 382
(Optional) Install NSX Tools on your Workload VMs 385
Un-deploy NSX Cloud 385
Undeploy or Unlink PCG 386

17 Uninstalling NSX-T Data Center from a Host Transport Node 389
Verify Host Network Mappings for Uninstall 390
Migrate Out VMkernels and Physical NICs from a vSphere Distributed Switch 391
Uninstall NSX-T Data Center from a vSphere Cluster 394
Uninstall NSX-T Data Center from a Managed Host in a vSphere Cluster 397
Uninstall NSX-T Data Center from a Standalone ESXi Host 401
Uninstall NSX-T Data Center from a Physical Host 403
Triggering Uninstallation from the vSphere Web Client 405
Uninstall NSX-T Data Center from a Physical Server 407
Uninstall NSX-T from a vSphere Lifecycle Manager cluster through NSX Manager 408

18 Troubleshooting Installation Issues 410
Installation Fails Due to Insufficient Space in Bootbank on ESXi Host 410
Host Fails to Install as Transport Node 411
NSX Agent Times Out Communicating with NSX Manager 411
Troubleshooting Installation 412
Node Status of KVM Transport Node is Degraded 416

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 manages 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 supports a cluster with three node, 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.
- 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.

Read the following topics next:

- Key Concepts
- 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 a Tier-0 Gateway, Tier-1 Gateway or L2 bridge.

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 entering the VM is called ingress traffic.

Gateway

NSX-T Data Center routing entity that provide connectivity between different L2 networks. Configuring a gateway through NSX Manager instantiates a gateway on each hypervisor.

Gateway Port

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

Segment Port

Logical switch attachment point to establish a connection to a virtual machine network interface, container, physical appliances or a gateway interface. The segment 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 user configuration.

NSX Edge Cluster

Is a collection of NSX Edge node appliances that have the same settings and provide high availability if one of the NSX Edge node fails.

NSX Edge Node

Edge nodes are service appliances with pools of capacity, dedicated to running network and security services that cannot be distributed to the hypervisors.

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.

vSphere Distributed Switch (VDS)

Starting in vSphere 7.0, NSX-T Data Center supports VDS switches. You can create segments on VDS switches.

NSX Manager

Node that hosts the API services, the management plane, the control 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.

Opaque Network

An opaque network is a network created and managed by a separate entity outside of vSphere. For example, logical networks that are created and managed by N-VDS switch running on NSX-T Data Center appear in vCenter Server as opaque networks of the type `nsx.LogicalSwitch`. You can choose an opaque network as the backing for a VM network adapter. To manage an opaque network, use the management tools associated with the opaque network, such as NSX Manager or the NSX-T Data Center API management tools.

Overlay Logical Network

Logical network implemented using GENEVE encapsulation protocol as mentioned in https://www.rfc-editor.org/rfc/rfc8926.txt. 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

Previously known as logical switch. It is an 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.

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

A Tier-0 Gateway provides north-south connectivity and connects to the physical routers. It can be configured as an active-active or active-standby cluster. The Tier-0 Gateway runs BGP and peers with physical routers.

Tier-1 Gateway

A Tier-1 Gateway connects to one Tier-0 Gateway for northbound connectivity to the subnetworks attached to it. It connects to one or more overlay networks for southbound connectivity to its subnetworks. A Tier-1 Gateway can be configured as an active-standby cluster.

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 fabric node is prepared as a transport node so that it becomes 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, you can configure the host on a N-VDS or a VDS switch.

Uplink Profile

Defines policies for the links from transport nodes to NSX-T Data Center segments or from NSX Edge nodes to top-of-rack switches. The settings defined by uplink profiles might include teaming policies, 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 NSX-T segment. The vNIC can be attached to a logical port. You can identify a vNIC based on its Unique ID (UUID).

Tunnel Endpoint

Each transport node has a Tunnel Endpoint (TEP) responsible for encapsulating the overlay VM traffic inside a VLAN header and routing the packet to a destination TEP for further processing. TEPs are the source and destination IP addresses used in the external IP header to identify the ESXi hosts that originate and end the NSX-T encapsulation of overlay frames. Traffic can be routed to another TEP on a different host or the NSX Edge gateway to access the physical network. TEPs create a GENEVE tunnel between the source and destination endpoints.

NSX Manager

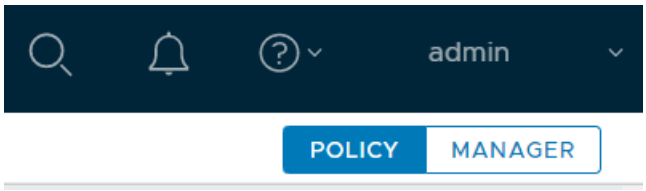
The NSX Manager provides a web-based user interface where you can manage your NSX-T Data Center environment. It also hosts the API server that processes API calls.

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 the 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 NSX 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. NSX Federation supports only Policy mode. If you want to use NSX 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	

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 Policy API: Getting Started Guide.

Security

NSX Manager has the following security features:

- NSX Manager has a built-in user account called **admin**, which has access rights to all resources, but does not have rights to the operating system to install software. NSX-T upgrade files are the only files allowed for installation. You can change the username and role permissions for **admin**, but you cannot delete **admin**.
- NSX Manager supports session timeout and automatic user logout. NSX Manager does not support session lock. Initiating a session lock can be a function of the workstation operating system being used to access NSX Manager. Upon session termination or user logout, users are redirected to the login page.
- Authentication mechanisms implemented on NSX-T follow security best practices and are resistant to replay attacks. The secure practices are deployed systematically. For example, sessions IDs and tokens on NSX Manager for each session are unique and expire after the user logs out or after a period of inactivity. Also, every session has a time record and the session communications are encrypted to prevent session hijacking.

You can view and change the session timeout value with the following CLI commands:

- The command `get service http` displays a list of values including session timeout.
- To change the session timeout value, run the following commands:

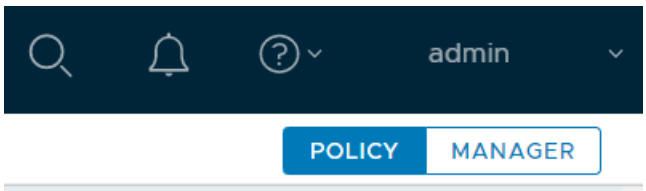
```
set service http session-timeout <timeout-value-in-seconds>
restart service ui-service
```

Configure the User Interface Settings

You can configure how your users view the NSX-T Data Center user interface. These settings are valid for NSX Manager, and in NSX Federation for Global Managers and Local Managers.

Prior to NSX-T Data Center 3.2, users could access two possible modes in the user interface: Policy and Manager. You can control which mode is default, and whether users can switch between them using the user interface mode buttons. The Policy mode is the default. New users of release 4.0 will not see the **Manager** button.

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 NSX Manager for more information about the modes.

Procedure

1 With admin privileges, log in to NSX Manager.

2 Navigate to **System > General System Settings**.

3 Select **User Interface** and click **Edit** in the User Interface Mode Toggle pane.

4 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. This displays Policy mode UI only, even if Manager mode objects are present.
Default Mode	Can be set to Policy or Manager, if available.

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.

Read the following topics next:

- 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 the 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 Prepare ESXi Cluster Hosts as Transport Nodes.

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 Form an NSX Manager Cluster Using the 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 Prepare Standalone Hosts as Transport Nodes.

   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 and Available Appliances.

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

5 Create host transport nodes.

   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 Physical Server Workloads.

Preparing for Installation 3

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

Read the following topics next:

- System Requirements
- Ports and Protocols

System Requirements

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

Before you configure Gateway Firewall features, make sure that the NSX Edge form factor supports the features. See *Supported Gateway Firewall Features on NSX Edge* topic in the *NSX-T Data Center Administration Guide*.

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 for Host Transport Nodes

Hypervisor	Version	CPU Cores	Memory
vSphere	Supported vSphere version	4	16 GB
CentOS Linux KVM	7.9, 8.4	4	16 GB
Red Hat Enterprise Linux (RHEL) KVM	7.9, 8.2, 8.4	4	16 GB
SUSE Linux Enterprise Server KVM	12 SP4	4	16 GB
Ubuntu KVM	18.04.2 LTS, 20.04 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 7.7 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 EP6 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 4.19.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. To find the supported driver for the NIC card vendor, see Firmware Versions of Supported Drivers.

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
Cisco VIC 1400 series	nenic_ens

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	Shares	Reservations	Disk Space	VM Hardware Version
NSX Manager Extra Small (NSX-T Data Center 3.0 onwards)	8 GB	2	81920, Normal	8192 MB	300 GB	10 or later
NSX Manager Small VM (NSX-T Data Center 2.5.1 onwards)	16 GB	4	163840, Normal	16384 MB	300 GB	10 or later
NSX Manager Medium VM	24 GB	6	245760, Normal	24576 MB	300 GB	10 or later
NSX Manager Large VM	48 GB	12	491520, Normal	49152 MB	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 the autoselected appliance size during deployment and is suitable for typical production environments. An NSX-T management cluster formed using this appliance size can support up to 128 hypervisors. Starting with NSX-T 3.1, a single NSX Manager cluster is supported.
- 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 128 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
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 disk access latency is under 10ms.
- It is recommended that NSX Managers be placed on shared storage.
- Storage must 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 NSX Public Cloud Gateway: Architecture and Modes of Deployment 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)	Proof-of-concept deployments only. **Note** L7 rules for firewall, load balancing and so on are not realized on a Tier-1 gateway if you deploy a small sized NSX Edge VM.
NSX Edge Medium	8 GB	4	200 GB	11 or later (vSphere 6.0 or later)	Suggested for L2 through L4 features and when the total throughput requirement is less than 2 Gbps: ■ NAT ■ Routing ■ L4 firewall ■ L4 load balancer

Appliance Size	Memory	vCPU	Disk Space	VM Hardware Version	Notes
NSX Edge Large	32 GB	8	200 GB	11 or later (vSphere 6.0 or later)	Suggested for L2 through L4 features and when the total throughput requirement is between 2 ~ 10 Gbps. ■ NAT ■ Routing ■ L4 Firewall ■ L4 Load Balancer ■ L7 Load Balancer (for example, when SSL offload is required) ■ TLS Inspection See Scaling Load Balancer Resources in the *NSX-T Data Center Administration Guide*. For more information about what the different load balance sizes and NSX Edge form factors can support, see https://configmax.vmware.com.
NSX Edge Extra Large	64 GB	16	200 GB	11 or later (vSphere 6.0 or later)	Suggested for features that have a higher total throughput requirement than the NSX Edge Large form factor: ■ L7 load balancer ■ VPN ■ TLS Inspection ■ L7 Access Profile (URL filtering) ■ IDS/IPS ■ Malware prevention (Adavanced Threat Protection) See Scaling Load Balancer Resources in the *NSX-T Data Center Administration Guide*. For more information about what the different load balance sizes and NSX Edge form factors can support, see https://configmax.vmware.com.

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 Series processors

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.
- NSX Edge Bare Metal supports up to 64 cores for the entire system. This means that a server with a single socket, the CPU can have up to 64 cores. On a server with 2 sockets, each socket cannot have more than 32 cores.

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 Series processors

NSX Edge Bare Metal Hardware Requirements

If you are running NSX Edge Bare Metal version 3.2 to any version prior to 3.2.3, 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 you are running NSX Edge Bare Metal version 3.2.3, verify that the Bare Metal NSX Edge hardware is listed in this URL https://certification.ubuntu.com/server/models/?release=20.04%20LTS&category=Server.

If the hardware is not listed, the storage, video adapter, or motherboard components might not work on the NSX Edge appliance.

Note Starting with NSX-T 3.2, NSX Edge Bare Metal supports both UEFI and legacy BIOS modes. However, in NSX-T 3.1 and previous releases, NSX Edge Bare Metal only supports legacy BIOS mode.

NSX Edge Bare Metal NIC Requirements

NIC Type	Description	Vendor ID	PCI Device ID	Firmware Version
Mellanox ConnectX-4 EN	PCI_DEVICE_ID_MELLANOX_CONNECTX4	15b3	0x1013	12.21.1000 and above
Mellanox ConnectX-4 Lx EN	PCI_DEVICE_ID_MELLANOX_CONNECTX4LX	15b3	0x1015	14.21.1000 and above
Mellanox ConnectX-5	PCI_DEVICE_ID_MELLANOX_CONNECTX5	15b3	0x1017	16.21.1000 and above
Mellanox ConnectX-5 EX	PCI_DEVICE_ID_MELLANOX_CONNECTX5EX	15b3	0x1019	16.21.1000 and above
Intel X520/Intel 82599	IXGBE_DEV_ID_82599_KX4	8086	0x10F7	n/a
	IXGBE_DEV_ID_82599_KX4_MEZZ	8086	0x1514	n/a
	IXGBE_DEV_ID_82599_KR	8086	0x1517	n/a

NIC Type	Description	Vendor ID	PCI Device ID	Firmware Version
	IXGBE_DEV_ID_82599_COMBO_BACKPLANE	8086	0x10F8	n/a
	IXGBE_SUBDEV_ID_82599_KX4_KR_MEZZ	8086	0x000C	n/a
	IXGBE_DEV_ID_82599_CX4	8086	0x10F9	n/a
	IXGBE_DEV_ID_82599_SFP	8086	0x10FB	n/a
	IXGBE_SUBDEV_ID_82599_SFP	8086	0x11A9	n/a
	IXGBE_SUBDEV_ID_82599_RNDC	8086	0x1F72	n/a
	IXGBE_SUBDEV_ID_82599_560FLR	8086	0x17D0	n/a
	IXGBE_SUBDEV_ID_82599_ECNA_DP	8086	0x0470	n/a
	IXGBE_DEV_ID_82599_SFP_EM	8086	0x1507	n/a
	IXGBE_DEV_ID_82599_SFP_SF2	8086	0x154D	n/a
	IXGBE_DEV_ID_82599_SFP_SF_QP	8086	0x154A	n/a
	IXGBE_DEV_ID_82599_QSFP_SF_QP	8086	0x1558	n/a
	IXGBE_DEV_ID_82599EN_SFP	8086	0x1557	n/a
	IXGBE_DEV_ID_82599_XAUI_LOM	8086	0x10FC	n/a
	IXGBE_DEV_ID_82599_T3_LOM	8086	0x151C	n/a
Intel X540	IXGBE_DEV_ID_X540T	8086	0x1528	n/a
	IXGBE_DEV_ID_X540T1	8086	0x1560	n/a
Intel X550	IXGBE_DEV_ID_X550T	8086	0x1563	n/a
	IXGBE_DEV_ID_X550T1	8086	0x15D1	n/a
Intel X710	I40E_DEV_ID_SFP_X710	8086	0x1572	6.80 and later versions (8.x versions are not supported)
	I40E_DEV_ID_KX_C	8086	0x1581	6.80 and later versions (8.x versions are not supported)

NIC Type	Description	Vendor ID	PCI Device ID	Firmware Version
	I40E_DEV_ID_10G_BASE_T	8086	0x1586	6.80 and later versions (8.x versions are not supported)
	I40E_DEV_ID_10G_BASE_T4	8086	0x1589	6.80 and later versions (8.x versions are not supported)
Intel XL710	I40E_DEV_ID_KX_B	8086	0x1580	6.80 and later versions (8.x versions are not supported)
	I40E_DEV_ID_QSFP_A	8086	0x1583	6.80 and later versions (8.x versions are not supported)
	I40E_DEV_ID_QSFP_B	8086	0x1584	6.80 and later versions (8.x versions are not supported)
	I40E_DEV_ID_QSFP_C	8086	0x1585	6.80 and later versions (8.x versions are not supported)
	I40E_DEV_ID_20G_KR2	8086	0x1587	6.80 and later versions (8.x versions are not supported)
	I40E_DEV_ID_20G_KR2_A	8086	0x1588	6.80 and later versions (8.x versions are not supported)
Intel XXV710	I40E_DEV_ID_25G_B	8086	0x158A	6.80 and later versions (8.x versions are not supported)
	I40E_DEV_ID_25G_SFP28	8086	0x158B	6.80 and later versions (8.x versions are not supported)
Cisco VIC 1300 series	Cisco UCS Virtual Interface Card 1300	1137	0x0043	n/a
Cisco VIC 1400 series	Cisco UCS Virtual Interface Card 1400	1137	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 Physical Server.

Bare Metal Server Requirements

Operating System	Version	CPU Cores	Memory
CentOS Linux	7.6 (kernel: 3.10.0-957) 7.7 7.8 7.9 8.0 8.3	4	16 GB
Red Hat Enterprise Linux (RHEL)	7.6 (kernel: 3.10.0-957) 7.7 7.8 7.9 8.0 8.3	4	16 GB
Oracle Linux	7.6 (kernel: 3.10.0-957) 7.7 7.8 7.9	4	16 GB
SUSE Linux Enterprise Server	12 SP3 12 SP4 12 SP5 ((starting in NSX-T Data Center 3.2.1)	4	16 GB
Ubuntu	16.04.2 LTS (kernel: 4.4.0-*) 18.04	4	16 GB
Windows Server	2016 (minor version 14393.2248 and later) 2019	4	16 GB

- Ensure MTU is set to 1600 for Jumbo frame support by NIC or OS drivers.
- Hosts running Ubuntu 18.04.2 LTS must be upgraded from 16.04 or freshly installed.

Physical NICS

For physical servers running Linux: There is no restriction on the physical NIC other than being supported by the operating system.

For physical servers running Windows on Segment-VLAN with MTU at 1500, there is also no restrictions on the physical NIC other than being supported by the operating system.

For physical servers running Windows on Segment-Overlay or with Segment-VLAN with large MTU (> 1500), validate its associated driver support jumbo packet. To verify whether jumbo packet is supported, run the following command:

```
$ (Get-NetAdapterAdvancedProperty -Name "<Ethernet>").DisplayName -Contains "Jumbo Packet"
```

Where, `<Ethernet>` must be replaced with the real adapter name of each physical NIC."

Table 3-2. Virtual NICs

NIC Type	Description	PCI BUS ID	Firmware Version
e1000e	Intel(R) 82574L Gigabit Network	0000:1b:00	12.15.22.6 and later version
vmxnet3	vmxnet3 Ethernet Adapter	0000:0b:00	1.9.2.0 and later version

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 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. Starting with NSX-T Data Center 3.1, a single NSX Manager cluster deployment is supported.

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 file system of an 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 can 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.
	For example, avoid simple and systematic passwords such as `VMware123!123` or `VMware12345`. Passwords that meet complexity standards are not simple and systematic but are a combination of letters, alpahabets, special characters, and numbers, such as `VMware123!45`, `VMware 1!2345` or `VMware@1az23x`.

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 or FQDN list for the NSX Manager or Cloud Service 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.
Certificates	If you plan to configure internal VIP on a NSX Manager cluster, you can apply a different certificate to each NSX Manager node of the cluster. See Configure a Virtual IP Address for a Cluster. If you plan to configure an external load balancer, ensure only a single certificate is applied to all NSX Manager cluster nodes. See Configuring an External Load Balancer.

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 as a standalone host, 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. When you install NSX Manager as a managed host in vCenter Server, OVA/OVF property values such as user names and passwords are validated before the VM is powered on.

- If you specify a user name for any local user, the name must be unique. If you specify the same name, it is ignored and the default names (for example, **admin** and **audit**) are used.
- 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.

- If the password for other local users (for example, **audit**) 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 local_user_name** to set the local user's password (the current password is an empty string). You can also reset passwords in the UI using System > User Management > Local Users.

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 deployments. (It is optional for all other deployment types.) See *Multisite Deployment of NSX Data Center* in the *NSX-T Data Center Administration Guide*.

Publishing the FQDNs of the NSX Managers

After installing the NSX-T Data Center core components, 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 Data Center 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
```

Read the following topics next:

- 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 password never expires.

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

NSX Manager Cluster Requirements

5

The following subsections describe cluster requirements for NSX appliances and provides recommendations for specific site deployments.

Cluster Requirements

- In a production environment, the NSX Manager (Local Manager in an NSX Federation environment) or Global 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 cluster of the NSX Manager (Local Manager in an NSX Federation environment) or Global Manager. However, you can add additional, temporary nodes to allow for IP address changes.

  Important NSX Manager cluster requires a quorum to be operational. This means at least two out of three of its members must be up and running. If a quorum is lost, NSX management and control planes do not work. This results in no access to the NSX Manager's UI and API for configuration updates using the management plane as well as no access to add or vMotion VMs on NSX segments. The dynamic routing on Tier-0 remains operational.

- For lab and proof-of-concept deployments where there are no production workloads, you can run a single NSX Manager or Global Manager to save resources. NSX Manager or Global Manager nodes can be deployed on either ESXi or KVM. However, mixed deployments of managers on both ESXi and KVM are not supported.
- If you deploy a single NSX Manager or Global Manager in a production environment, you can also enable vSphere HA on the host cluster for the manager nodes to get automatic recovery of the manager VM in case of ESXi failure. For more information on vSphere HA, see the *vSphere Availability* guide in the vSphere Documentation Center.

- If one of the NSX Manager node goes down, the three node NSX Manager cluster provides redundancy. However, if one of the NSX Manager node loses its disk, it goes into read only state. It might still continue to participate in the cluster if its network connectivity is Up. This case can result in the management plane and control plane to become unvailable. To resolve the issue, power off the impacted NSX Manager.

Recovery with vSphere HA

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

Read the following topics next:

- Cluster Requirements for an Individual Site
- Cluster Requirements for Multiple Sites

Cluster Requirements for an Individual Site

Each NSX appliance cluster – Global Manager, Local Manager or NSX Manager – must contain three VMs.

Those three VMs can be physically all deployed in the same data center or in different data centers, as long as latency between VMs in the cluster is below 10ms.

Single Site Requirements and Recommendations

The following recommendations apply to single site NSX-T Data Center deployments and cover cluster recommendations for Global Manager, Local Manager and NSX Manager appliances:

- It is recommended that you place your NSX appliances on different hosts to avoid a single host failure impacting multiple managers.
- Maximum latency between NSX appliances is 10ms.
- You can place NSX appliances in different vSphere clusters or in a common vSphere cluster.
- It is recommended that you place NSX appliances in different management subnets or a shared management subnet. When using vSphere HA it is recommended to use a shared management subnet so NSX appliances that are recovered by vSphere can preserve their IP address.
- It is recommended that you place NSX appliances 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 appliance when the host where the NSX appliance 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.

Cluster Requirements for Multiple Sites

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

Dual Site Requirements and Recommendations

Note Starting from NSX-T Data Center v3.0.2 onwards, VMware Site Recovery Manager (SRM) is supported.

- Do not deploy NSX Managers in a dual-site scenario without vSphere HA or VMware SRM. In this scenario, one site requires the deployment of two NSX 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 or VMware SRM 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 or VMware SRM 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 or VMware SRM will recover all NSX Managers to hosts in site B.

Important You must 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

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

If you deploy without vSphere HA or VMware SRM:

- 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 and Configuring NSX-T using vCenter Server Plugin

6

As a VI admin, you can install NSX Manager and NSX-T for virtual networking or security-only use case by installing and configuring the NSX-T plugin in vCenter Server.

There are two workflows - Virtual Networking and Security Only - allowed from the NSX page on the vSphere Client. The Virtual Networking deployment workflow includes both networking and security use cases. In contrast, if you choose to configure Security Only type of deployment, then you cannot configure virtual networking on the selected cluster hosts.

Note You must not enable **Multi NSX** on the vCenter Server on which you plan to install and configure the NSX-T plugin. It might result in unexpected results when using the NSX-T plugin from the vCenter Server.

Supported Browser Resolution

The minimum supported browser resolution is 1280 x 800 px.

Read the following topics next:

- Install NSX Manager from vSphere Client
- Configure NSX-T for Virtual Networking from vSphere Client
- Configuring NSX-T for Security from vSphere Client

Install NSX Manager from vSphere Client

As a VI admin working in the vSphere environment, you can completely install NSX Manager appliance from the vSphere Client. You do not need to perform any installation operations from the NSX Manager UI. After NSX Manager is installed, NSX appears as a plug-in in vCenter Server that is ready to install NSX-T for Virtual Networking or Security-only use cases.

Important In NSX-T Data Center 3.2, only a single NSX Manager cluster is supported.

Prerequisites

- Ensure that ESXi host version is compatible with vCenter Server version v7.0.3.
- Ensure that vCenter Server version is v7.0.3 or later.

- To provision a thick disk, ensure the disk size on host has at least 300GB free space.
- Configure a vSphere Distributed Switch (VDS) switch on hosts. Only VDS 6.6 or later is supported.
- Ensure vCenter Server points to an FQDN address and the DNS server must be able to resolve the address.

Procedure

1 From a browser, log in with admin privileges to an vCenter Server at https://<vcenter-server-ip-address>.

2 On the vSphere Client UI, select **vSphere Client** menu and click **NSX**.

3 On the screen, click **Install NSX**.

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

Important If you enter a URL to download the OVF file, ensure the URL points to a secure HTTPS server. For example, https://<OVF-URL>. There is a separate OVF file available for NSX Manager deployed from vSphere Client. You must select a OVF file name using the following convention: `nsx-embedded-unified-appliance-<releaseversion.buildversion>.ovf`. Do not use the `nsx-unified-appliance-<releaseversion.buildversion>.ova` file.

5 To verify the thumbprint of the SSL certificate of the HTTPS server, click **Yes**.

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

The selected location also indicates the vCenter Server where the NSX Manager is deployed and which vCenter Server is managed by the NSX instance.

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

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

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

9 Select a form factor to deploy the NSX appliance. You must deploy the NSX Manager in either **Medium** or **Large** form factor. If you select any other form factor, then installation fails and NSX appliance is not registered to vCenter Server.

10 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**.

11 Select a destination network for each source network.

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

13 Configure IP Allocation settings.

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

b For IP protocol, select **`IPv4`** or **`IPv6`**.

Note You can ignore the IP Allocation settings. You can select either IPv4 or IPv6. It would not impact ingress or egress network traffic of NSX Manager.

14 Click **Next**.

15 In the Application section, enter the **System GRUB Root User Password**, **System GRUB menu timeout**, **System Root Password**, **CLI 'admin' User Password**, **CLI 'audit' User Password**, **CLI 'admin' username**, and **CLI 'audit' username**. Only the root password and admin password fields are mandatory.

- 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.

For example, avoid simple and systematic passwords such as `VMware123!123` or `VMware12345`. Passwords that meet complexity standards are not simple and systematic but are a combination of letters, alpahabets, special characters, and numbers, such as `VMware123!45`, `VMware 1!2345` or `VMware@1az23x`.

Important If the password you set does not meet the password complexity requirements, installation of the NSX Manager fails. If installation fails, you need to redeploy the NSX Manager again.

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. Also, NSX-T Data Center accepts only latin alphabets that do not have an accent mark, as in í, ó, ú, ý.

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

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

19 In the Services Configuration section, enter the NTP Server IP or FQDN list.

Optionally, you can enable SSH service and allow root SSH login. But, it is not recommended to allow root access to SSH service.

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

See the installation progress in the **Recent Tasks** tab.

21 On the NSX page, you can either click **Start NSX Onboarding** to load the plugin or skip the onboarding workflow and access the NSX Manager UI from the vSphere Client.

What to do next

Apply NSX license.

1 Click **Go To NSX Getting Started**.

2 In the **NSX License Key** section, enter the NSX license key and click **Apply**.

After you successfully apply the NSX license, configure NSX-T for Virtual Networking or Security use case on the vSphere platform. See Configure NSX-T for Virtual Networking from vSphere Client.

Configure NSX-T for Virtual Networking from vSphere Client

As a VI administrator working in the vSphere environment, you can configure NSX-T for virtual networking. The workflow involves configuring logical segments to establish connectivity between hosts even in different subnets, configuring NSX Edge nodes, Tier-0 gateways, Tier-1 gateways and segments. Finally, workload VMs connected to these segments can pass north-south and east-west traffic.

Prerequisites

- Ensure that ESXi hosts are compatible with vCenter Server version v7.0.3 or later.
- Ensure that vCenter Server version is v7.0.3 or later.
- Configure a vSphere Distributed Switch (VDS) switch on hosts. Only VDS 6.6 or later is supported.
- On a vSphere Lifecycle Manager enabled cluster, edit the vCenter Server from the NSX Manager UI to:
  - Create a service account and enable trust between NSX-T and vCenter Server. See Add a Compute Manager.

Procedure

1. From a browser, log in with admin privileges to an vCenter Server at https://<vcenter-server-ip-address>.
2. On the vSphere Client UI, select **vSphere Client** menu and click **NSX**.
3. On the **Welcome to NSX** screen, on the **Virtual Networking** card, click **Getting Started**.
4. In the **Host Cluster Preparation** tab, perform the following tasks.
5. Expand the **Host Cluster** section, select the clusters that you want to prepare for virtual networking and click **Next**.

   Note Any cluster with an incompatible ESXi host is not allowed for host preparation.

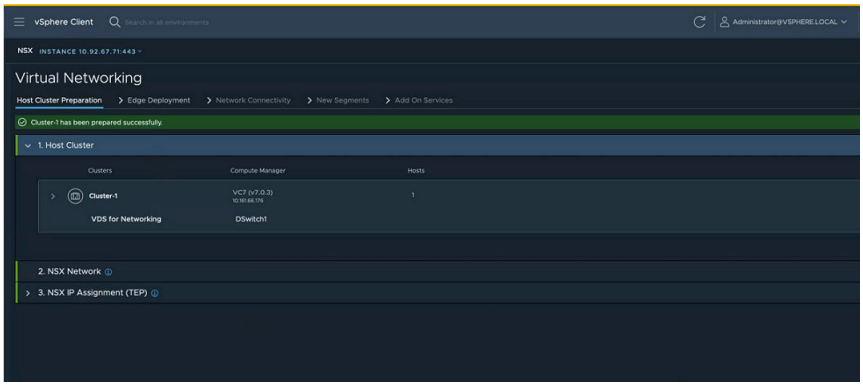
6. Expand the **Transport VLAN** section, enter a VLAN ID that will tag the overlay traffic and click **Next**.
7. Expand the **NSX IP Assignment (TEP)** section, and enter IP details:

Field	Description
IP Assignment	Select the mode of IP assignment, from between static and DHCP. If you select IP pool, enter a name for the pool, IP range, subnet along with prefix (subnet/prefix) and default gateway.

8. Click **Prepare Cluster** to begin installation of NSX-T.

   Cluster preparation begins. View installation progress at each host.

Alternatively, you can also verify the progress in NSX Manager UI. NSX-T creates a new transport node profile using the configuration that you defined in the installation section. The switch is set to VDS. The transport node profile is applied to the cluster to prepare hosts of the cluster as transport nodes.



9 In the **Edge Deployment** tab, expand the **Management Network for Edge Connectivity** and enter the following details:

Field	Description
Management VDS	Select a vSphere Distributed Switch for management traffic on NSX Edge nodes.
Management Network	Select a network for management traffic of NSX Edge nodes.
Management Gateway	Select the gateway to route management traffic. Enter a static IP address.

10 Click **Next**.

11 In the **Edge Deployment** tab, expand the **Edge Node 1** and enter the following details

Field	Description
Name	Enter a name for the Edge node.
Fully Qualified Domain Name	Enter a Fully Qualified Domain Name that resolves to the IP address of the NSX Edge node.
Management IP address	Enter an IP address for management traffic of the NSX Edge node.
External Network Connectivity	Select a distributed port group to be used as a data path interface. This distributed port group manages the ingress and egress traffic of workload VMs that are processed by the NSX Edge node. **Note** Even though there are three data path interfaces on an NSX Edge node, this workflow uses only one interface for a distributed port group.
Edge Node Settings	Select **Apply same settings for all Edges** if you want to replicate the settings across all NSX Edge nodes.
Password	Enter a password that conforms to the required password complexity. Confirm the same password on the next field.

Field	Description
Virtual Machine Size	Select a form factor to deploy the Edge node.
Storage Location	Select the datastore as storage location for installation and configuration files and data generated by the Edge node.

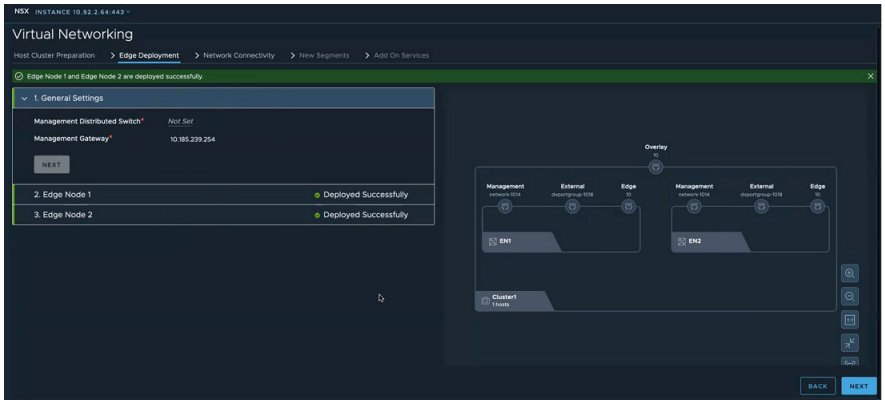
12 On the **Edge Deployment** tab, verify that the visualization is updated with management network, external network and other details related to NSX Edge node.

13 Enter details for **Edge Node 2**.

14 Click **Deploy Edge**.

15 On the confirmation window, click **Deploy**.

16 Observe the topology created based on the configuration details entered on the **Edge Deployment** tab. After NSX Edge nodes are realized, the dotted line turns to a solid line, indicating NSX Edge node is realized.



17 Click **Next** to configure network connectivity.

18 In the **Network Connectivity** tab, expand the **Physical Router** section and enter the following details:

Field	Description

Do you want to peer with a physical router now?	After deploying the NSX Edge node, it can establish a peer connection with a physical router.
	■ Select **Yes** if you want to set up Border Gateway Protocol (BGP) or static routing to your physical router.
	  ■ **BGP Local AS**: Enter the local autonomous system number for use in BGP.
	■ Select **No** if you do not want to set up BGP or static routing to your router. However, you will need to set up NAT to connect to workloads to external networks.
	  ■ In the **Physical Routing IP address** field, enter a static IP address.

How many physical routers do you want to peer with?	Based on your selection, enter the following details for one or two physical routers:
	If you want to allow other routers to peer with your router, then enter the following details:
	For each peer router, enter these details:
	■ BGP Local AS: Enter the local autonomous system number used by the BGP neighbor.
	■ BGP Neighbors:
	  ■ **IP Address**: Enter the IP address of the physical router, which is the BGP neighbor.
	  ■ **Remote AS**: Remote autonomous system number used by BGP neighbors.

19 Click **Next**.

20 In the **Network Connectivity** tab, expand the **NSX Gateway** section and enter the following details:

Field	Description
Gateway Name Prefix	Enter a prefix for the gateway. Every object, such as Tier-0, Tier-1 gateways, that are created for the gateway is prefixed with this value. You can search for objects with a specific prefix to get a list of objects related to a particular gateway.
Uplink VLAN for Router 1	Enter the VLAN ID to tag VLAN traffic going from NSX Edge node to physical router 1.
Uplink VLAN for Router 2	Enter the VLAN ID to tag VLAN traffic going from NSX Edge node to physical router 2.

21 Click **Next**.

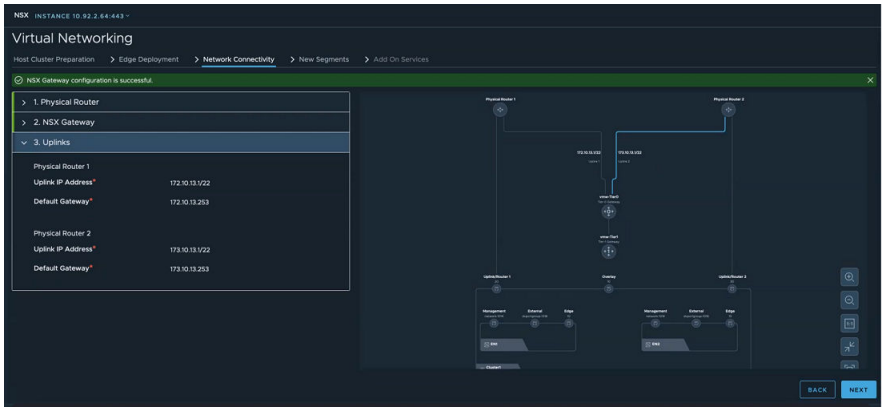
22 In the **Network Connectivity** tab, expand the **Uplinks** section and enter the following details:

Field	Description
IP Address for Uplink 1	Enter the IP address for uplink from NSX gateway or Tier-0 gateway to physical router 1.
IP Address for Uplink 2	Enter the IP address for uplink from NSX gateway or Tier-0 gateway to physical router 2.
Physical Router 1	Enter subnet mask and default gateway for physical router 1.
Physical Router 2	Enter subnet mask and default gateway for physical router 2.

23 Verify the visualization created based on the network details you entered.

24 Click **Create Gateways**.

25 On the confirmation window, click **Create Gateways**.



The NSX Gateway is successfully created.

26 In the **New Segments** tab, create a segment where workloads VMs will be running. For example, create a segment for a web group. Enter the following details:

Field	Description
Name	Enter the name of the segment.
Subnet/Prefix Length	Enter the subnet network for the segment.
Default Gateway	Enter the default gateway that segments should forward traffic to.

27 To create additional segments, click **Add Segment** and enter the required details.

28 Click **Create Segment**.

29 After segments are created, add them to NSX distributed virtual port group.

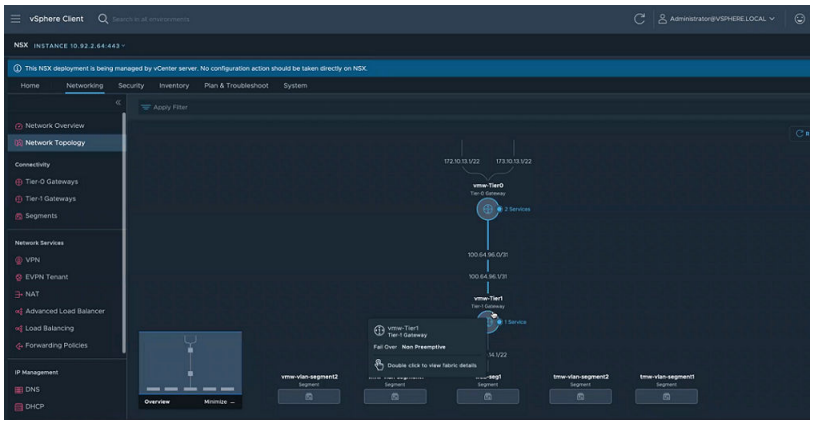
30 Click **Next**.

31 (Optional) In the **Add-on Services** tab, enter Network Address Translation (NAT) details. On the **NAT Only** window, enter the following details:

Field	Description
Name	Enter a name for NAT service.
Source	Select a segment so that IP addresses of local hosts connected to this segment are translated and protected and a single translated IP address is presented to an external network.
Translated	The IP address that is presented to external network thus protecting local hosts from exposing their IP addresses to an external network.

32 Click **Next**.

33 View the created topology created in NSX-T.



Results

NSX-T is configured for virtual networking.

Example:

What to do next

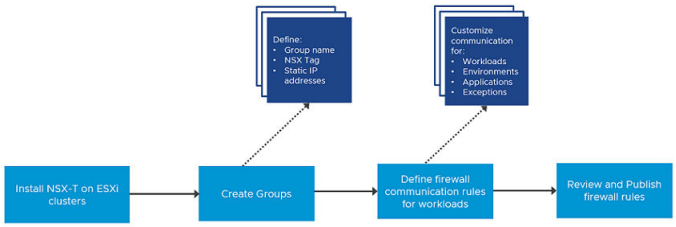
1 From a browser log in to NSX Manager with https://<NSX Manager-IP-Address>/.

2 After logging in to NSX Manager, verify networking configuration is successfully created in NSX-T.

Configuring NSX-T for Security from vSphere Client

As a VI admin working in the vSphere environment, you can use the simplified workflow to prepare ESXi clusters for NSX-T security.

Use the vSphere Client to prepare ESXi clusters for NSX-T security. On such clusters, you can enable micro-segmentation, URL filtering and distributed IDS on application workloads. These clusters are not prepared for NSX-T virtual networking.



High-level tasks:

- Prepare Host Cluster.
- Create Firewall Rules
  - Create Groups for infrastructure services (Active Directory, DNS, and so on), environment groups (production or testing), and application groups (web, database, application).
  - Define communication strategy. Some of the actions you can take are:
    - Define communication between any workload and infrastrcture services.
    - Define communication so that no environment can talk to each other.
    - Limit communication to a specific port or protocol.
    - Specifiy source workloads.
    - Set up exeptions after setting up communication strategies for workloads.
  - Define Action for Default Firewall Rule (to process traffic that does not match firewall rules defined in Communication section).
  - Review and publish firewall rules.

Prepare Clusters for NSX-T Security

Select a host cluster to prepare it for NSX-T security.

The Getting Started section gives you the option to select between **Security Only** or **Virtual Networking**. When you choose to enable clusters only for security, the wizard asks you to define security rules and uses those rules to automatically configure NSX-T security on the distributed virtual port groups of the selected clusters.

Prerequisites

- Ensure that ESXi hosts are compatible with vCenter Server version v7.0.3 or later.
- Ensure that vCenter Server version is v7.0.3 or later.
- Configure a vSphere Distributed Switch (VDS) switch on hosts. Only VDS 6.6 or later is supported.
- On a vSphere Lifecycle Manager enabled cluster, edit the vCenter Server from the NSX Manager UI to:
  - Create a service account and enable trust between NSX-T and vCenter Server. See Add a Compute Manager.

Procedure

1 From a browser, log in with admin privileges to a vCenter Server at https://<vcenter-server-ip-address>.

2 On the vSphere Client UI, select the vSphere Client menu and click **NSX**.

3 On the Welcome to NSX screen, on the **Security Only** card, click **Getting Started**.

4 On the **Host Cluster Preparation** section, select the clusters that you want to prepare for security only and click **Install NSX**.

5 On the Install Security pop-up window, confirm you want to process by clicking **Install**.

Note Any cluster with an incompatible ESXi host is not allowed for host preparation.

6 Click **Next** to define firewall rules.

Results

NSX-T is installed on the host cluster.

What to do next

To avoid any loss of connectiviy, add vCenter Server and NSX Manager to the DFW Exclusion list.

Add vCenter Server and NSX Manager to Distributed Firewall Exclusion List

To ensure connectivity to vCenter Server or NSX Manager VMs, add these VMs to the DFW firewall exclusion list in NSX-T.

After adding the vCenter Server and NSX Manager VMs to the DFW exclusion list, even when you configure the default firewall policy to **`Drop`** from the NSX-T plugin in vCenter Server, you will not lose connectivity to these VMs. Perform the following procedure from the NSX Manager UI.

Procedure

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

2 Go to **Inventory** → **Tags**.

3 Create a new tag, for example, *NSX-VM-Tag* and add both vCenter Server and NSX Manager VMs to it.

4 Create a new group, for example, *NSX-VM-Group*.

5 In the Compute Members field, click **Set**.

6 In the Set Members window, in the Membership Criteria page, click Add Criterion.

7 In Criterion 1 row, match the Virtual Machine tag equal to *NSX-VM-Tag*.

8 Ensure both vCenter Server and NSX Manager VMs are added to the *NSX-VM-Group* group.

9 Click **Apply**.

System VMs - vCenter Server and NSX Manager VMs - are added to DFW exclude list through the *NSX-VM-Group* group. You will not lose connectivity to vCenter Server and NSX Manager VMs even if the Firewall policy is set to **`Drop`**.

What to do next

Start the NSX-T plugin in vCenter Server and create firewall rules that can be applied to workloads running on hosts. See Create Groups.

Create Groups

As part of firewall creation, define infrastructure group that run selected services, such as DHCP, define environment groups, such as production, testing, or so on, comprising of selected group members and define application groups with selected group members.

Prerequisites

- Install NSX-T on the host cluster.

Procedure

1 In the **Create Firewalls Rules** tab, select **Create Groups**.

2 In the **Create Groups** page, expand **Create Infrastructure Groups**.

3 Click **Add Group**.

4 From the **Infrastructure Service** drop-down menu, select a service, such as Active Directory. In the next step, you assign this service to a group comprising of members that form the infrastructure group. You can create an infrastructure service only once in a workflow. It cannot be edited once you create it.

5 To define an infrastructure group, click **[Define Group]**.

An infrastructure can be a combination of VMs, IP address range, or distributed virtual port groups.

a (Optional) In the **Group Name** field, modify the default group name.

b (Optional) In the **NSX Tag** field, modify the default tag name. The defined tag is applied to all VMs and distributed virtual port groups selected for the group. You can edit the default tag name.

c Expand the **Select VMs to add NSX Tag** section and select VMs that must be part of the infrastructure group.

d Expand the **IP Address** section and enter an IP address, IP addresses in CIDR format, or an IP range. Both IPv4 and IPv6 formats are supported.

e Expand the **Select DVPGs to add NSX Tag** section and select the distributed virtual port groups that must be part of the infrastructure group.

f Click **Save**.

The wizard automatically creates the group and applies the NSX tag on all the selected members of the group. For example, if the defined group includes one VM, one distributed virtual port group, and 1 IP address, and DHCP is the selected infrastructure service, then wizard tags all group members with the defined tag.

6 Click **Next**.

7 In the **Create Groups** page, expand **Create Environment Group**.

8 Click **Add Group**.

9 From the **Environment** drop-down menu, select the environment for the group. For example, an environment can be a production, testing, partner or a custom environment that you want to define in your topology.

10 To define an environment group, click **[Define Group]**.

a (Optional) In the **Group Name** field, modify the default group name.

b (Optional) In the **NSX Tag** field, modify the default NSX tag name. This tag name is applied to all VMs and distributed virtual port group selected for the environment group.

c Expand the **Select VMs to add NSX Tag** section and select VMs that must be part of the environment group.

d Expand the **IP Address** section and enter an IP address, IP addresses in CIDR format, or an IP range. Both IPv4 and IPv6 formats are supported.

e Expand the **Select DVPGs to add NSX Tag** section and select the distributed virtual port groups that must be part of the environment group.

f Click **Save**.

11 Click **Next**.

12 In the **Create Groups** page, expand **Create Application Group**.

13 Click **Add Group**.

14 From the **Application Group Name** drop-down menu, select the type of application group you want to create.

15 To define an application group, click **[Define Group]**.

a (Optional) In the **Group Name** field, modify the default group name for the application group.

b (Optional) In the **NSX Tag** field, modify the default tag name. This tag name is applied to all VMs and distributed virtual port group selected for the application group, enter a NSX tag.

c Expand the **Select VMs to add NSX Tag** section and select VMs that must be part of the application group.

d Expand the **IP Address** section and enter an IP address, IP addresses in CIDR format, or an IP range. Both IPv4 and IPv6 formats are supported.

e Expand the **Select DVPGs to add NSX Tag** section and select the distributed virtual port groups that must be part of the application group.

f Click **Save**.

16 Click **Next**.

Results

You created infrastructure groups, environment groups and application groups.

What to do next

After creating groups, define firewall rules that govern communication among workloads and these different groups.

Define and Publish Communication Strategies for Groups

After creating groups, define firewall rules to govern communication between groups, define exceptions and ports or protocols for communication.

Prerequisites

- Install NSX-T on the host cluster.
- Create Infrastructure groups, Environment groups, and Application groups.

Procedure

1 Expand the **Access to infrastructure services** section and define specific workloads that can access shared infrastructure services.

Field	Description
Source	In the Source column, select the workloads that can access the target infrastructure service.
Target	Is the defined infrastructure service that is accessed by source workloads.
(NSX-T3.2.2) Service Entry	Click the Edit icon to add or edit service entries. In the Service Entry window, select a service type and properties for the service type. **Note** In NSX-T 3.2.1 and previous versions, the field name was **L4**.

2 Click **Next**.

3 Expand the **Define communication between environments (Optional)** section and define communication between groups.

Field	Description
Source	Expand the section to define which source environment must communicate with a target environment. (NSX-T 3.2.2): For each source group listed, select a communication method: **Unprotected**, **Allowed** or **Blocked**. **Note** To allow all communication between all source groups and the target group, select **Allow All Communication**. (NSX-T 3.2.1 and previous versions): To allow communication between a Development environment and a Production environment, click the red dotted line between Development and Production. The enabled state is displayed when a green line is established between groups.
Environment	Is the target environment selected by the system.
(NSX-T3.2.2) Service Entry	Select the service type, ports and properties over which the workloads in source and target environments communicate with each other. Click **Apply**. **Note** In NSX-T 3.2.1 and previous versions, the field name was **L4**.

4 Click **Next**.

5 Expand the **Define communication strategies for applications (Optional)** section and define communication for application groups.

Field	Description
Source	Select an application group for which you can select communication rules to manage incoming or outgoing traffic.
Strategy	Select a firewall strategy to apply to an application group. Supported firewall rules are: ■ Allow all external traffic. ■ Deny incoming and allow outgoing traffic. ■ Allow incoming and deny outgoing traffic. ■ Deny all external traffic. **Note** If you want to apply one firewall rule to all application groups, click **Select Strategy**, select the rule and click **Apply**.
Exception	Based on how you want to configure firewall rule, you might want to add exceptions. By default, no exceptions are added. To add an exception, click the **No Exceptions** link. Edit these fields to add exceptions: ■ Source: Select the source. ■ Service Entry: Select the service, port and properties. ■ L7 App ID: Select the App ID. ■ FQDN: Select FQDN of the application. .Click **Apply**.

6 Click **Next**.

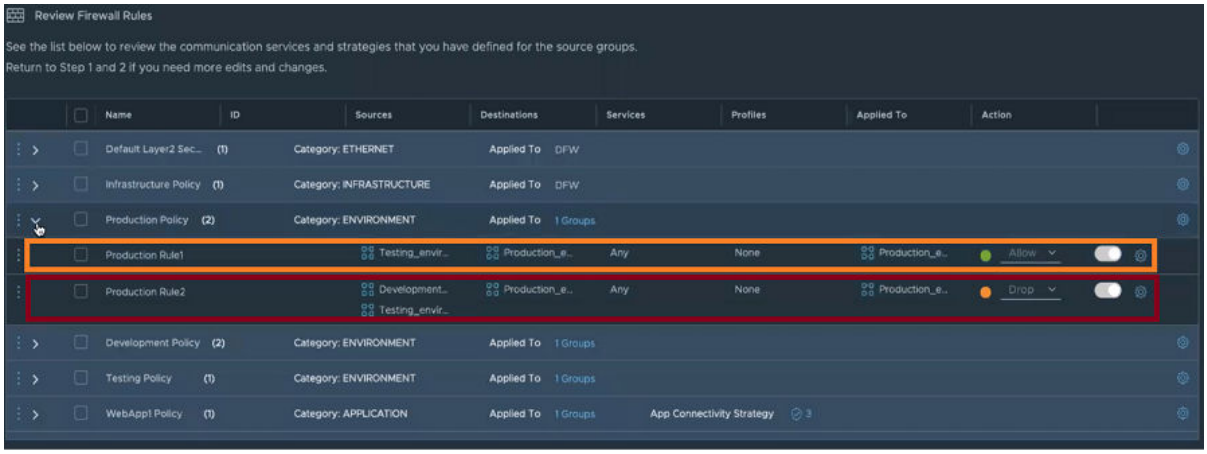
7 Expand the **Define Action for Default Firewall Rules (Optional)** section and define an action that is applied to traffic that does not match the defined criteria.

8 In the Default rule action, select from one of the following:

- **Allow**: Is the default rule set. Allows all traffic that does not match the defined criteria.
- **Drop** or **Reject**: To enforce firewall rules insider your network, you might choose to drop traffic that does not match the defined criteria.

9 Click **Next**.

10 In the Review and Publish page, review the communication strategies and firewall rules that you applied to the groups.



In the screenshot, Production Rule 1 is a user-defined rule and Production Rule 2 is system-defined default rule, where the default action is set to **Drop**.

11 Click **Publish Policies**.

Results

The wizard ends and firewall policies you defined are applied to the groups. The NSX UI is available in vCenter Server.

What to do next

To verify the firewall rules published from vSphere Client are realized on NSX Manager UI.

1 In the NSX Manager UI, go to **Inventory** → **Groups**.

2 On the Groups page, verify whether the workload groups you defined in vSphere Client are realized in NSX Manager.

3 Go to **Security** → **Distributed Firewall** page.

4 On the Distributed Firewall page, verify whether the firewall rules you applied in vSphere Client are realized in NSX Manager.

Installing NSX Manager Cluster on vSphere

7

Install the NSX-T Data Center component, NSX Manager, which is the management plane to manage NSX-T Data Center workfloads and NSX Edge using the UI or CLI.

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

Read the following topics next:

- Install NSX Manager and Available Appliances
- Configure a Virtual IP Address for a Cluster
- Configuring an External Load Balancer
- Disable Snapshots on an NSX Appliance

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 NSX 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 or FQDN list for the NSX Manager or Cloud Service 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`** or **`IPv6`**.

Note You can ignore the IP Allocation settings. You can select either IPv4 or IPv6. It would not impact ingress or egress network traffic of NSX Manager.

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.

For example, avoid simple and systematic passwords such as `VMware123!123` or `VMware12345`. Passwords that meet complexity standards are not simple and systematic but are a combination of letters, alpahabets, special characters, and numbers, such as `VMware123!45`, `VMware 1!2345` or `VMware@1az23x`.

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 Operator 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. Also, NSX-T Data Center accepts only latin alphabets that do not have an accent mark, as in í, ó, ú, ý.

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 NSX Federation deployment, select the **NSX Global Manager** role.

  See Chapter 14 Getting Started with NSX 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.

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

20 In the Services Configuration section, enter the NTP Server IP or FQDN list.

Optionally, you can enable SSH service and allow root SSH login. But, it is not recommended to allow root access to SSH service.

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 the VM console to track the boot process of the node.

23 After the node 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 default services are running.

The following services are not required by default and do not start automatically.

- `liagent`
- `migration-coordinator`: This service is used only when running migration coordinator. See the *NSX-T Data Center Migration Guide* before starting this service.
- `snmp`: For information on starting SNMP see *Simple Network Management Protocol* in the *NSX-T Data Center Administration Guide*.
- `nsx-message-bus`: This service is not used in NSX-T Data Center 3.0.

25 Verify that your NSX Manager, Cloud Service Manager or Global Manager node has the required connectivity.

Make sure that you can perform the following tasks.

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

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

- You can download the latest OVF tool from the Customer Connect Portal.
- 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 or FQDN list for the NSX Manager or Cloud Service 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 \
--name=<nsxmanager>
--X:injectOvfEnv
--X:logFile=ovftool.log
--sourceType=OVA
--vmFolder='Folder-in-VC'
--allowExtraConfig
--datastore=<datastore>
--net:"<network-name-of-OVF>=<network-name>"
--acceptAllEulas
--skipManifestCheck
--noSSLVerify
--diskMode=thin
--quiet
--hideEula
--powerOn
--prop:nsx_ip_0=10.196.176.81
--prop:nsx_netmask_0=255.255.252.0
--prop:nsx_gateway_0=10.196.179.253
--prop:nsx_dns1_0=10.142.7.1
--prop:nsx_domain_0=eng.vmware.com
--prop:nsx_ntp_0=10.128.243.14
--prop:nsx_isSSHEnabled=True
--prop:"nsx_passwd_0=<password>"
--prop:"nsx_cli_passwd_0=<password-cli>"
--prop:"nsx_cli_audit_passwd_0=<password-cli-audit>"
--prop:nsx_hostname=<hostname>
```

```
--prop:mgrhostname01="nsx-manager-02@vmware.com"
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_role="NSX Manager"
--X:logFile=/root/ovftool/<ovf-folder>.log
--X:logLevel=trivia
--ipProtocol=IPv4
--ipAllocationPolicy="fixedPolicy"
<nsx-unified-applicance>.ova
'vi://admin@vsphere.local:password@vc-or-ip.eng.vmware.com/<datacenter>/host/
Install/10.196.6.78/'
```

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.

Note In the above example, --deploymentOption is set to the default size Medium. To know the other supported sizes, see NSX Manager VM and Host Transport Node System Requirements.

- 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
--name=<nsxmanager>
--X:injectOvfEnv
--X:logFile=ovftool.log
--sourceType=OVA
--vmFolder='Folder-in-VC'
--allowExtraConfig
--datastore=<datastore>
```

```
--net:"<network-name-of-OVF>=<network-name>"
--acceptAllEulas
--skipManifestCheck
--noSSLVerify
--diskMode=thin
--quiet
--hideEula
--powerOn
--prop:nsx_ip_0=10.196.176.81
--prop:nsx_netmask_0=255.255.252.0
--prop:nsx_gateway_0=10.196.179.253
--prop:nsx_dns1_0=10.142.7.1
--prop:nsx_domain_0=eng.vmware.com
--prop:nsx_ntp_0=10.128.243.14
--prop:nsx_isSSHEnabled=True
--prop:"nsx_passwd_0=<password>"
--prop:"nsx_cli_passwd_0=<password-cli>"
--prop:"nsx_cli_audit_passwd_0=<password-cli-audit>"
--prop:nsx_hostname=<hostname>
--prop:mgrhostname01="nsx-manager-02@vmware.com"
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_role="NSX Manager"
--X:logFile=/root/ovftool/<ovf-folder>.log
--X:logLevel=trivia
--ipProtocol=IPv4
--ipAllocationPolicy="fixedPolicy"
<nsx-unified-applicance>.ova
'vi://admin@vsphere.local:password@vc-or-ip.eng.vmware.com/<datacenter>/host/
Install/10.196.6.78/'
```

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>@<esxi-IP-address>
Deploying to VI: vi://root:<password>@<esxi-IP-address>
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=<nsxmanager>
--X:injectOvfEnv
--X:logFile=ovftool.log
--sourceType=OVA
--vmFolder='Folder-in-VC'
--allowExtraConfig
```

```
--datastore=<datastore>
--net:"<network-name-of-OVF>=<network-name>"
--acceptAllEulas
--skipManifestCheck
--noSSLVerify
--diskMode=thin
--quiet
--hideEula
--powerOn
--prop:nsx_ip_0=10.196.176.81
--prop:nsx_netmask_0=255.255.252.0
--prop:nsx_gateway_0=10.196.179.253
--prop:nsx_dns1_0=10.142.7.1
--prop:nsx_domain_0=eng.vmware.com
--prop:nsx_ntp_0=10.128.243.14
--prop:nsx_isSSHEnabled=True
--prop:"nsx_passwd_0=<password>"
--prop:"nsx_cli_passwd_0=<password-cli>"
--prop:"nsx_cli_audit_passwd_0=<password-cli-audit>"
--prop:nsx_hostname=<hostname>
--prop:mgrhostname01="nsx-manager-02@vmware.com"
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_role="NSX Manager"
--X:logFile=/root/ovftool/<ovf-folder>.log
--X:logLevel=trivia
--ipProtocol=IPv4
--ipAllocationPolicy="fixedPolicy" <nsx-unified-applicance>.ova
'vi://admin@vsphere.local:password@vc-or-ip.eng.vmware.com/<datacenter>/host/
Install/10.196.6.78/'
```

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, --deploymentOption is set to the default size Medium. To know the other supported sizes, see NSX Manager VM and Host Transport Node System Requirements.

- 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
--name=<nsxmanager>
--X:injectOvfEnv
--X:logFile=ovftool.log
--sourceType=OVA
--vmFolder='Folder-in-VC'
--allowExtraConfig
--datastore=<datastore>
--net:"<network-name-of-OVF>=<network-name>"
--acceptAllEulas
--skipManifestCheck
--noSSLVerify
--diskMode=thin
--quiet
--hideEula
--powerOn
--prop:nsx_ip_0=10.196.176.81
--prop:nsx_netmask_0=255.255.252.0
--prop:nsx_gateway_0=10.196.179.253
--prop:nsx_dns1_0=10.142.7.1
--prop:nsx_domain_0=eng.vmware.com
--prop:nsx_ntp_0=10.128.243.14
--prop:nsx_isSSHEnabled=True
--prop:"nsx_passwd_0=<password>"
--prop:"nsx_cli_passwd_0=<password-cli>"
--prop:"nsx_cli_audit_passwd_0=<password-cli-audit>"
--prop:nsx_hostname=<hostname>
--prop:mgrhostname01="nsx-manager-02@vmware.com"
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_role="NSX Manager"
--X:logFile=/root/ovftool/<ovf-folder>.log
--X:logLevel=trivia
--ipProtocol=IPv4
--ipAllocationPolicy="fixedPolicy" <nsx-unified-applicance>.ova
'vi://admin@vsphere.local:password@vc-or-ip.eng.vmware.com/<datacenter>/host/
Install/10.196.6.78/'
```

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@<esxi-IP-address:port>/
Deploying to VI: vi://administrator@vsphere.local@<esxi-IP-address:port>/
```

```
Transfer Completed
Powering on VM: NSX Manager
Task Completed
Completed successfully
```

2 You can also run the OVF tool in Probe mode to view contents of a source. OVA and OVF packages can be probed among a list of other supported source types. You can use the information returned by the Probe mode to configure deployments.

   `$> \ovftool --allowExtraConfig <OVA path or URL>`

   Where, `--allowExtraConfig` is the supported appliance type for Cloud Service Manager (CSM).

3 For an optimal performance, reserve memory for the 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.

4 From the vSphere Client, open the VM console to track the boot process of the node.

5 After the node 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.

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

   The following services are not required by default and do not start automatically.

   - `liagent`
   - `migration-coordinator`: This service is used only when running migration coordinator. See the *NSX-T Data Center Migration Guide* before starting this service.
   - `snmp`: For information on starting SNMP see *Simple Network Management Protocol* in the *NSX-T Data Center Administration Guide*.
   - `nsx-message-bus`: This service is not used in NSX-T Data Center 3.0.

7 After deployment, verify that the NSX ManagerNSX Manager UI comes up by accessing the following URL, `https://nsx-manager-ip` or `https://nsx-manager-fqdn`.

8 Verify that your NSX Manager, Cloud Service Manager or Global Manager node has the required connectivity.

   Make sure that you can perform the following tasks.

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

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 .

  Note NSX Manager nodes that are removed from the cluster should be powered off or deleted. Do not reuse the same NSX Manager again in your environment.

- If deploying second and third NSX Manager nodes as OVA/OVF, join the manager nodes to first deployed manager node to create NSX Manager Cluster. see Form an NSX Manager Cluster Using the CLI .

Configure an Appliance to Display the GRUB Menu at Boot Time

You must configure an NSX-T Data Center appliance to display the GRUB menu at boot time if you want to reset the root password of the appliance.

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

Procedure

1. Log in to the VM as root.
2. In the `/etc/default/grub` file, set the GRUB_TIMEOUT_STYLE to **`menu`** or **`countdown`**.
   - If this option set to **`menu`**, then GRUB will display the menu and then wait for the timeout set by `GRUB_TIMEOUT` to expire before booting the default entry. Pressing a key interrupts the timeout.
   - If this option is set to **`countdown`**, then before displaying the menu, GRUB will wait for the timeout set by `GRUB_TIMEOUT` to expire. If ESC or F4 are pressed, or SHIFT is held down during that time, it will display the menu and wait for input. It will show a one-line indication of the remaining time.
3. In the `/etc/default/grub` file, change the value for the parameter `GRUB_TIMEOUT`.

   ```
   GRUB_TIMEOUT=4
   ```

4. (Optional) Generate a new password by running the following command:

   ```
   grub-mkpasswd-pbkdf2
   ```

5. (Optional) In the `/etc/grub.d/40_custom` file, replace the existing GRUB password.

   The default password is **`NSX@VM!WaR10`**.

6. 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.

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.
- IPv4 communication with vCenter Server.
- Verify that you use the recommended number of compute managers. See https://configmax.vmware.com/home.
- Provide credentials of a vCenter Server user. You can provide the credentials of vCenter Server administrator, or create a role and a user specifically for NSX-T Data Center and provide this user's credentials. Add global permissions to the newly created user and role and select **Propogate to Children**.

  Create an admin role with 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

To use the NSX-T Data Center license for the vSphere Distributed Switch 7.0 feature, the vCenter Server user must either be an administrator, or the user must have *Global.Licenses* privileges and be a member of the *LicenseService.Administrators* group.

- Before you create a service account for the compute manager, add these additional vCenter Server privileges to the admin user role:

Service Account Management.Administer
Permissions.Modify permission
Permissions.Modify role
VMware vSphere Lifecycle Manager.ESXi Health Perspectives.Read
VMware vSphere Lifecycle Manager.Lifecycle Manager: General Privileges.Read
VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Privileges.Read
VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Privileges.Write
VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Remediation Privileges.Write
VMware vSphere Lifecycle Manager.Lifecycle Manager: Settings Privileges.Read

`VMware vSphere Lifecycle Manager.Lifecycle Manager: Settings Privileges.Write`
`VMware vSphere Lifecycle Manager.Lifecycle Manager: General Privileges.Write`

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 Compute Manager**.
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.
Type	The default compute manager type is set to vCenter Server.
Multi NSX	Starting with NSX-T Data Center 3.2.2, you can register the same vCenter Server with multiple NSX Managers. Enable this field if you want to allow multiple NSX-T Data Center instances to manage a single vCenter Server. This functionality is supported from vCenter Server 7.0 or later versions. **Note** Cannot be enabled on a Workload Control Plane (WCP) cluster or vSphere Lifecycle Manager (vLCM) cluster. See Multiple NSX Managers Managing a Single vCenter Server.
FQDN or IP Address	Type the FQDN or IP address of the 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 Data Center.
Username and Password	Type the vCenter Server login credentials.
SHA-256 Thumbprint	Type the vCenter Server SHA-256 thumbprint algorithm value.
Create Service Account	Enable this field for features such as vSphere Lifecycle Manager that need to authenticate with NSX-T Data Center APIs. Log in with the administrator@vsphere.local credential to register a compute manager. After registration, the compute manager creates a service account. **Note** Service account creation is not supported on a global NSX Manager. If service account creation fails, the compute manager's registration status is set to `Registered with errors`. The compute manager is successfully registered. However, vSphere Lifecycle Manager cannot be enabled on NSX-T Data Center clusters. If a vCenter Server admin deletes the service account after it was successfully created, vSphere Lifecycle Manager tries to authenticate the NSX-T Data Center APIs and the compute manager's registration status is set to `Registered with errors`.

Option	Description
Enable Trust	Enable this field to establish trust between NSX-T Data Center and compute manager, so that services running in vCenter Server can establish trusted communication with NSX-T Data Center. For example, for vSphere Lifecycle Manager to be enabled on NSX-T Data Center clusters, you must enable this field. Supported only on vCenter Server 7.0 and later versions.
Access Level	Enable one of the options based on your requirement: ■ Full Access to NSX: Is selected by default. This access level gives the compute manager complete access to NSX-T Data Center. Full access ensures vSphere for Kubernetes and vSphere Lifecycle Manager can communicate with NSX-T Data Center. The vCenter Server user's role must be set to an Enterprise Admin. ■ Limited Access to NSX: This access level ensures vSphere Lifecycle Manager can communicate with NSX-T Data Center. The vCenter Server user's role must be set to Limited vSphere Admin.

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.
- If an NSX Manager cluster consists of nodes deployed from the VC (manual method) and nodes deployed from the NSX Manager UI, and you had to undeploy the manually deployed nodes, then you cannot remove the VC. To successfully remove the VC, ensure that you re-deploy an NSX Manager node from the VC.

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

Deploy NSX Manager Nodes to Form a Cluster from the UI

Forming an NSX Manager or Global Manager cluster provides high availability and reliability. Deploying nodes using the UI is supported only on ESXi hosts managed by vCenter Server.

For other environments, see Form an NSX Manager Cluster Using the CLI .

When you deploy a new node from the UI, the node connects to the first deployed node to form a cluster. All the repository details and the password of the first deployed node are synchronized with the newly deployed node. The first node is known as the orchestrator node because it contains the original copy of the VIBs and installation files required to prepare hosts of the cluster. The orchestrator node also help identify the node on which the Upgrade-Coordinator is running. When new nodes are added to the cluster, NSX-T Data Center uses the repository IP to synchronize the repository of VIBs and installation files on the new nodes of the cluster.

To create an NSX Manager cluster, deploy two additional nodes to form a cluster of three nodes total.

To create a Global Manager cluster, deploy two additional nodes to form a cluster of three nodes total. However, if your Global Manager has NSX-T Data Center 3.0.0 installed, deploy only one node, and do not form a cluster. See Install the Active and Standby Global Manager .

Prerequisites

- Verify that an NSX Manager or Global 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 or FQDN list for the NSX Manager or Cloud Service 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 the NSX Manager or Global Manager at https://<manager-ip-address>.
2. Deploy an appliance.
   - From NSX Manager, select **System > Appliances > Add NSX Appliance**.
   - From Global Manager, select **System > Global Manager Appliances > Add NSX Appliance**.
3. Enter the appliance information details.

Option	Description
Host Name or FQDN	Enter a name for the node.
Management IP/Netmask	Enter an IP address to be assigned to the node.
Management Gateway	Enter a gateway IP address to be used by the node.
DNS Servers	Enter DNS server IP addresses to be used by the node.

Option	Description
NTP Server	Enter an NTP server IP address to be used by the node.
Node Size	Select the form factor to deploy the node from the following options: ■ Small (4 vCPU, 16 GB RAM, 300 GB storage) ■ Medium (6 vCPU, 24 GB RAM, 300 GB storage) ■ Large (12 vCPU, 48 GB RAM, 300 GB storage) For Global Manager select size: ■ **Medium** GM appliance for deployments up to four locations and 128 hypervisors across all locations ■ **Large** GM appliance for deployments with higher scale Do not use **Small** GM appliance for scale deployment.

4 Enter the configuration details.

Option	Description
Compute Manager	Select the vCenter Server to provision compute resources for deploying the 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 a host for the node.
Datastore	Select a datastore for the node files from the drop-down menu.

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 select a virtual disk format because the VM storage policy defines the format.
	  ■ The vSAN storage policies determine the disk format. 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 or Global Manager node is prepared in the **Thin Provision** format.
	Note You can provision each node with a different disk format based on which policies are provisioned on the datastore.

Network	Click **Select Network** to select the management network for the node.

5 Enter the access and credentials details.

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

Option	Description

System Root Credentials	Set the root password and confirm the password 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.
	For example, avoid simple and systematic passwords such as `VMware123!123` or `VMware12345`. Passwords that meet complexity standards are not simple and systematic but are a combination of letters, alpahabets, special characters, and numbers, such as `VMware123!45`, `VMware 1!2345` or `VMware@1az23x`.

Admin CLI Credentials and Audit CLI Credentials	Select the **Same as root password** check box to use the same password that you configured for root, or deselect the check box and set a different password.

6 Click **Install Appliance**.

The new node is deployed. You can track the deployment process in the **System > Appliances** page for NSX Manager, the **System > Global Manager Appliances** for Global Manager, or the vCenter Server for either. Do not add additional nodes until the installation is finished and the cluster is stable.

7 Wait for the deployment, cluster formation, and repository synchronization to finish.

The joining and cluster stabilizing process might take from 10 to 15 minutes. Run `get cluster status` to view the status. Verify that the status for every cluster service group is `UP` before making any other cluster changes.

Note

- If the first 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.
- If a node deployment fails, you cannot reuse the same IP address to deploy another node until the failed node is deleted.

8 After the node 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.

9 Verify that your NSX Manager, Cloud Service Manager or Global Manager node has the required connectivity.

Make sure that you can perform the following tasks.

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

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

10 If your cluster has only two nodes, add another appliance.

- From NSX Manager, select **System > Appliances > Add NSX Appliance** and repeat the configuration steps.
- From Global Manager, select **System > Global Manager Appliances > Add NSX Appliance** and repeat the configuration steps.

11 If the orchestrator node goes down or is unreachable and the repository is not replicated to the remaining nodes in the cluster, host preparation will fail. To successfully prepare nodes of the cluster, manually deploy the first node to seed the repository.

What to do next

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

Form an NSX Manager Cluster Using the CLI

Forming an NSX Manager or Global Manager cluster provides high availability and reliability. You can use the `join` command to create a cluster.

Prerequisites

- To create an NSX Manager cluster, deploy three nodes to create the cluster.
- To create a Global Manager cluster, deploy three nodes to create the cluster. However, if your Global Manager has NSX-T Data Center 3.0.0 installed, deploy only one node, and do not form a cluster. See Install the Active and Standby Global Manager .

Procedure

1 Open an SSH or console session to the first deployed NSX Manager or Global Manager node and log in with the administrator credentials.

2 On the first deployed node, run the following commands.

   a Run the `get certificate api thumbprint` command.

   The command output is a string that is unique to this node.

   b Run the `get cluster config` command to get the cluster ID of the first deployed node.

```
mgr-first> get cluster config
Cluster Id: 7b50abb9-0402-4ed5-afec-363587c3c705
Cluster Configuration Version: 0
Number of nodes in the cluster: 1

...
```

3 Open an SSH or console session to the new node and log in with the administrator credentials.

4 On the new node that is joining the cluster, run the `join` command.

   Provide the following information about the first deployed node in the `join` command:

   - IP address
   - Cluster ID
   - User name
   - Password

- Certificate thumbprint

```
mgr-new> join <Manager-IP> cluster-id <cluster-id> username <Manager-username> password
<Manager-password> thumbprint <Manager-thumbprint>
```

The joining and cluster stabilizing process might take from 10 to 15 minutes. Run `get cluster status` to view the status. Verify that the status for every cluster service group is `UP` before making any other cluster changes.

5 Add the third node to the cluster.

Repeat step 4 on the third node.

6 Verify the cluster status on the web interface.

- On NSX Manager, log in to the NSX Manager web interface and select **System > Appliances**.
- On Global Manager, log in to the Global Manager web interface and select **System > Global Manager Appliances**.

Results

Verify the result by running the `get managers` command on your hosts.

```
host> get managers
- 192.168.110.47   Connected
```

Based on the NSX-T Data Center version, navigate to the NSX Manager UI and

verify that the host's MPA connectivity is **Up**.

- (NSX-T Data Center 3.2.2 or later) **System > Fabric > Hosts** and select the **Cluster** tab.
- (NSX-T Data Center 3.2.1 or earlier) **System > Fabric > Nodes > Host Transport Nodes**

  and from the **Managed by** dropdown menu, select a vCenter Server.

You can also view the fabric host's state with the **GET https://<nsx-mgr>/api/v1/fabric/nodes/<fabric-node-id>/state** API call:

```
{
  "details": [],
  "state": "success"
}
```

The management plane sends the host certificates to the control plane, and the control plane pushes control plane information to the hosts.

You should see NSX Controller addresses in `/etc/vmware/nsx/controller-info.xml` on each ESXi host or access the CLI using `get controllers`.

```
[root@host:~] cat /etc/vmware/nsx/controller-info.xml
<?xml version="1.0" encoding="utf-8"?>
<config>
  <connectionList>
    <connection id="0">
        <server>10.143.1.47</server>
        <port>1234</port>
        <sslEnabled>true</sslEnabled>
        <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
    <connection id="1">
        <server>10.143.1.45</server>
        <port>1234</port>
        <sslEnabled>true</sslEnabled>
        <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
    <connection id="2">
        <server>10.143.1.46</server>
        <port>1234</port>
        <sslEnabled>true</sslEnabled>
        <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
  </connectionList>
</config>
```

The host connection to NSX-T Data Centers is initiated and sits in "CLOSE_WAIT" status until the host is promoted to a transport node. You can see this with the **esxcli network ip connection list | grep 1234** command.

```
# esxcli network ip connection list | grep 1234
tcp  0 0  192.168.210.53:45823  192.168.110.34:1234  CLOSE_WAIT  37256  newreno  netcpa
```

For KVM, the command is `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   CLOSE_WAIT -
```

What to do next

Create a transport zone. See Prepare Standalone Hosts as Transport Nodes.

Configure a Virtual IP 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 Manager nodes 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.

Important If you reset the cluster VIP, then vIDM configurations that are using the VIP is cleared. You will need to reconfigure vIDM configuration with the new VIP.

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 Verify that the VIP is working correctly.

From a browser, log in to the NSX Manager using the virtual IP address assigned to the cluster at https://<vip-address>.

Results

Any API requests to NSX-T are 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.

Configuring an External Load Balancer

You can configure an external load balancer to distribute traffic to the NSX Managers in a manager cluster.

An NSX Manager cluster does not require an external load balancer. The NSX Manager virtual IP (VIP) provides resiliency in the event of a Manager node failure but has the following limitations:

- VIP does not perform load balancing across the NSX Managers.
- VIP requires all the NSX Managers to be in the same subnet.
- VIP recovery takes about 1 - 3 minutes in the event of a Manager node failure.

An external load balancer can provide the following benefits:

- Load balance across the NSX Managers.
- The NSX Managers can be in different subnets.
- Fast recovery time in the event of a Manager node failure.

An external load balancer will not work with the NSX Manager VIP. Do not configure an NSX Manager VIP if you use an external load balancer.

Authentication Methods When Accessing NSX Manager

The following authentication methods are supported by NSX Manager. For more information about the authentication methods, see the *NSX-T Data Center API Guide*.

- HTTP Basic Authentication
- Session-Based Authentication
- Authentication using an X.509 certificate and a Principal Identity

- Authentication in VMware Cloud on AWS (VMC)

The session-based authentication method (used when you access NSX Manager from a browser) requires source-IP persistence (all requests from the client must go to the same NSX Manager). The other methods do not require source-IP persistence (requests from the client can go to different NSX Managers).

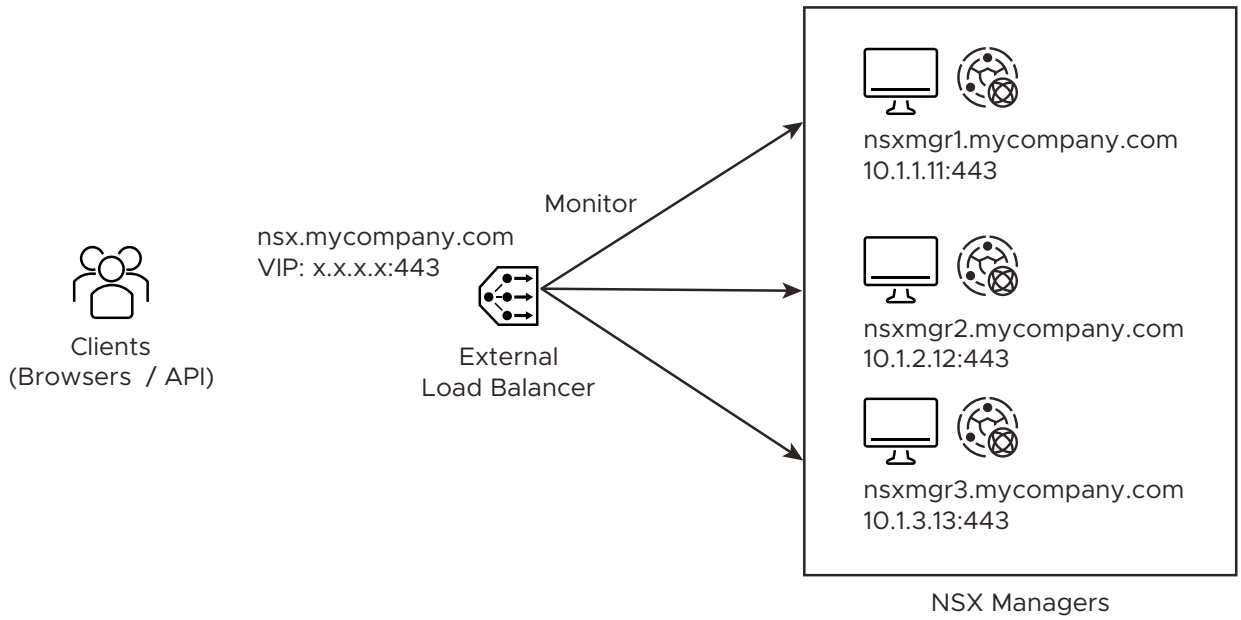
Recommendations

- Create a single VIP on the load balancer with source-IP persistence configured to handle all the authentication methods.
- If you have applications or scripts that might generate a lot of requests to NSX Manager, create a second VIP without source-IP persistence for these applications or scripts. Use the first VIP for browser access to NSX Manager only.

The VIP must have the following configurations:

- Type: Layer4-TCP
- Port: 443
- Pool: NSX Manager Pool
- Persistence: Source-IP persistence for the first VIP. None for the second VIP (if present).

Example of an external load balancer configuration:



NSX Manager's Certificate

The clients access NSX Manager using a FQDN name (for example, nsx.mycompany.com). This FQDN is resolved to the load balancer's VIP. To avoid any certificate mismatch, each NSX Manager must have a certificate that is valid for the VIP's FQDN name. Therefore, you must configure each NSX Manager with a SAN certificate that is valid for its own name (for example, nsxmgr1.mycompany.com) and the VIP's FQDN.

Monitoring the Health of NSX Managers

The load balancer can check that each NSX Manager is running with the following API:

```
GET /api/v1/reverse-proxy/node/health
```

The request headers are:

- Header1
  - Name: Authorization
  - Value: Basic <Base64 Value>

  Note: <Base64 Value> is Username:Password encoded in Base64. You can use https://www.base64encode.net to do the encoding. For example, Header1 might be `Authorization: Basic YWRtaW46Vk13YXJlMSFWTXdhcmUxIQ==` for `admin:VMware1!VMware1!`.
- Header2
  - Name: Content-Type
  - Value: application/json
- Header3
  - Name: Accept
  - Value: application/json

A response indicating that the NSX Manager is running will be:

```
"healthy" : true
```

Note that the format of the response is `"healthy"<space>:<space>true`.

If you change the password of the user that you specify in Header1, you must update Header1 accordingly.

Disable Snapshots on an NSX Appliance

Clones and snapshots of NSX appliances, such as NSX Manager, NSX Edge and Global Manager, are not supported. Follow the procedure below to disable snapshots.

Note Starting with NSX-T Data Center 3.0.1, snapshots are automatically disabled when an NSX appliance is deployed from the NSX Manager GUI. However, if you deploy an NSX appliance manually, for example, using an OVA file, follow the procedure below to disable snapshots.

Procedure

1. Locate the appliance VM 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`**.

   Note NSX-T Data Center does not support taking snapshots of NSX Manager. However, if you still want to take snapshots, enter a value other than zero in the **`snapshot.MaxSnapshots`** to take those many snapshots.
8. Click **OK** to save the changes.
9. Power the VM back on.

Installing NSX Manager Cluster on KVM

8

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.

Read the following topics next:

- Set Up KVM
- Manage Your Guest VMs in the KVM CLI
- Deploy an NSX Manager Cluster on KVM

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 7.7 and 8.2.

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
```

8 Configure the syslog rotation policy as time-based instead of size-based policy. With a size-based syslog rotation policy, the log files generated might be of very large sizes.

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)
```

Deploy an NSX Manager Cluster on KVM

To deploy an NSX Manager cluster, you install three NSX Manager nodes, and then use the `join` command to create the cluster.

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.

The same QCOW2 file can be used to deploy three different types of appliances: NSX Manager, NSX Cloud Service Manager for NSX Cloud, and Global Manager for NSX Federation.

Prerequisites

- Verify that KVM is set up. See Set Up KVM.
- Verify that you have 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 recommended 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 My VMware: https://www.vmware.com/go/download-nsx-t.

   Select the version to download and click **Go to Downloads**. Download the QCOW2 files.

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. For example, avoid simple and systematic passwords such as `VMware123!123` or `VMware12345`. Passwords that meet complexity standards are not simple and systematic but are a combination of letters, alpahabets, special characters, and numbers, such as `VMware123!45`, `VMware 1!2345` or `VMware@1az23x`.
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.

Property	Description
nsx_role	■ To install an NSX Manager appliance, select the **NSX Manager** role. ■ To install a Global Manager appliance for a NSX Federation deployment, select the **NSX Global Manager** role. See Chapter 14 Getting Started with NSX 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.
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 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. For details on other appliance sizes, see NSX Manager VM and Host Transport Node System Requirements. 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 node 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 Enter the `get services` command to verify that all default services are running.

The following services are not required by default and do not start automatically.

- `liagent`
- `migration-coordinator`: This service is used only when running migration coordinator. See the *NSX-T Data Center Migration Guide* before starting this service.
- `snmp`: For information on starting SNMP see *Simple Network Management Protocol* in the *NSX-T Data Center Administration Guide*.
- `nsx-message-bus`: This service is not used in NSX-T Data Center 3.0.

11 Verify that your NSX Manager, Cloud Service Manager or Global Manager node has the required connectivity.

Make sure that you can perform the following tasks.

- Ping your node from another machine.
- The node can ping its default gateway.
- The node can ping the hypervisor hosts that are in the same network using the management interface.
- The node can ping its DNS server and its NTP Server IP or FQDN list.

- If you enabled SSH, make sure that you can SSH to your node.

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 .

Form an NSX Manager Cluster Using the CLI

Forming an NSX Manager or Global Manager cluster provides high availability and reliability. You can use the `join` command to create a cluster.

Prerequisites

- To create an NSX Manager cluster, deploy three nodes to create the cluster.
- To create a Global Manager cluster, deploy three nodes to create the cluster. However, if your Global Manager has NSX-T Data Center 3.0.0 installed, deploy only one node, and do not form a cluster. See Install the Active and Standby Global Manager .

Procedure

1 Open an SSH or console session to the first deployed NSX Manager or Global Manager node and log in with the administrator credentials.

2 On the first deployed node, run the following commands.

a Run the `get certificate api thumbprint` command.

The command output is a string that is unique to this node.

b Run the `get cluster config` command to get the cluster ID of the first deployed node.

```
mgr-first> get cluster config
Cluster Id: 7b50abb9-0402-4ed5-afec-363587c3c705
Cluster Configuration Version: 0
Number of nodes in the cluster: 1

...
```

3 Open an SSH or console session to the new node and log in with the administrator credentials.

4 On the new node that is joining the cluster, run the `join` command.

   Provide the following information about the first deployed node in the `join` command:

   - IP address
   - Cluster ID
   - User name
   - Password
   - Certificate thumbprint

   ```
   mgr-new> join <Manager-IP> cluster-id <cluster-id> username <Manager-username> password
   <Manager-password> thumbprint <Manager-thumbprint>
   ```

   The joining and cluster stabilizing process might take from 10 to 15 minutes. Run `get cluster status` to view the status. Verify that the status for every cluster service group is `UP` before making any other cluster changes.

5 Add the third node to the cluster.

   Repeat step 4 on the third node.

6 Verify the cluster status on the web interface.

   - On NSX Manager, log in to the NSX Manager web interface and select **System > Appliances**.
   - On Global Manager, log in to the Global Manager web interface and select **System > Global Manager Appliances**.

Results

Verify the result by running the `get managers` command on your hosts.

```
host> get managers
- 192.168.110.47   Connected
```

Based on the NSX-T Data Center version, navigate to the NSX Manager UI and

verify that the host's MPA connectivity is **Up**.

- (NSX-T Data Center 3.2.2 or later) **System > Fabric > Hosts** and select the **Cluster** tab.
- (NSX-T Data Center 3.2.1 or earlier) **System > Fabric > Nodes > Host Transport Nodes**

  and from the **Managed by** dropdown menu, select a vCenter Server.

You can also view the fabric host's state with the **GET https://<nsx-mgr>/api/v1/fabric/nodes/<fabric-node-id>/state** API call:

```
{
  "details": [],
```

```
  "state": "success"
}
```

The management plane sends the host certificates to the control plane, and the control plane pushes control plane information to the hosts.

You should see NSX Controller addresses in `/etc/vmware/nsx/controller-info.xml` on each ESXi host or access the CLI using `get controllers`.

```
[root@host:~] cat /etc/vmware/nsx/controller-info.xml
<?xml version="1.0" encoding="utf-8"?>
<config>
  <connectionList>
    <connection id="0">
        <server>10.143.1.47</server>
        <port>1234</port>
        <sslEnabled>true</sslEnabled>
        <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
    <connection id="1">
        <server>10.143.1.45</server>
        <port>1234</port>
        <sslEnabled>true</sslEnabled>
        <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
    <connection id="2">
        <server>10.143.1.46</server>
        <port>1234</port>
        <sslEnabled>true</sslEnabled>
        <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
  </connectionList>
</config>
```

The host connection to NSX-T Data Centers is initiated and sits in "CLOSE_WAIT" status until the host is promoted to a transport node. You can see this with the **esxcli network ip connection list | grep 1234** command.

```
# esxcli network ip connection list | grep 1234
tcp  0 0  192.168.210.53:45823  192.168.110.34:1234  CLOSE_WAIT  37256  newreno  netcpa
```

For KVM, the command is `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   CLOSE_WAIT -
```

What to do next

Create a transport zone. See Prepare Standalone Hosts as Transport Nodes.

Transport Zones and Profiles

9

Transport zones and profiles are building blocks to prepare hosts for NSX-T Data Center networking.

Read the following topics next:

- Create Transport Zones
- Create an IP Pool for Tunnel Endpoint IP Addresses
- Enhanced Data Path
- Configuring Profiles

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 segment—and, therefore, which VMs can be attached to the segment. A transport zone can span one or more host clusters. Also, a transport node can be associated to multiple tranzport zones.

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 segment 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 segment is limited to a transport zone.

The overlay and VLAN transport zone is used by both host transport nodes and NSX Edge nodes. When a host is added to an overlay transport zone, you can configure an N-VDS or a VDS switch on the host. You can only configure a N-VDS switch on NSX Edge transport nodes.

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.

Note vMotion is not supported between two segments or logical switches on different VLAN transport zones.

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 Zone**.

3 Enter a name for the transport zone and optionally a description.

4 Select a traffic type between **Overlay** and **VLAN**.

5 Enter names of Named Teaming Policy. If you defined named teaming policies, ensure that you enter the exact named teaming policy name. These named teaming policies can be used by segments attached to the transport zone. If the segments 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 Prepare Standalone Hosts as Transport Nodes.

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 Prepare Standalone Hosts as Transport Nodes.

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:

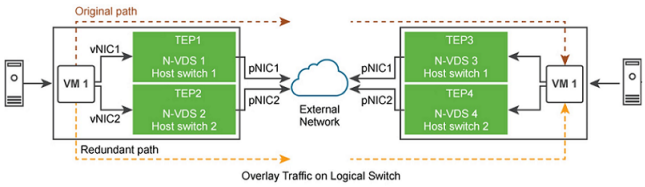
- The LAG uplink is configured with physical links from multiple NUMA nodes.
- The VM has affinity to multiple NUMA nodes.
- The ESXi host failed to define NUMA information for either VM or physical links.

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 9-1. 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 Bare Metal NSX Edge 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. If the teaming policy uses more than one uplink (active/standby list), you cannot use the same uplinks in the same or a different uplink profile for a given NSX Edge transport node.

- If the Load Balanced Source teaming policy is configured for an uplink profile, then you can either configure uplinks associated to different physical NICs or configure an uplink mapped to a LAG that has two physical NICs on the same N-VDS. The IP address assigned to an uplink endpoint is configurable using IP Assignment for the N-VDS. The number of LAGs that you can actually use depends on the capabilities of the underlying physical environment and the topology of the virtual network. For example, if the physical switch supports up to four ports in an LACP port channel, you can connect up to four physical NICs per host to a LAG.

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 Profile**.

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** You can only configure one LAG on a KVM host. During configuration, you map NSX-T Data Center to a Linux Bond that can have many physical NICs as supported by the underlying Linux OS. In this case, NSX-T Data Center is not doing the LAG but sees the LAG interface as a single interface for the OVS. 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** Supported LAG hashing mechanisms on hosts types: ■ NSX Edge nodes: **Source and destination MAC address, IP address, and TCP/UDP port**. ■ KVM hosts: **Source MAC address**. ■ ESXi hosts with N-VDS in Enhanced Networking Stack (ENS) mode: **Source MAC address**, **Destination MAC address**, and **Source and destination MAC address**. ■ ESXi hosts with N-VDS in Standard mode: **Source MAC address**, **Destination MAC address**, **Source and destination MAC address**, and **Source and destination IP address and VLAN**. ■ ESXi hosts with vSphere Distributed Switch (v 7.0 and later that supports NSX-T Data Center): LACP is not configured in NSX-T Data Center. You need to configure it in vCenter Server.
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**: Select 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. If the teaming policy uses more than one uplink (active/standby list), you cannot use the same uplinks in the same or a different uplink profile for a given NSX Edge transport node. For example, in Uplink-Profile-1 you use Uplink-3 as an active uplink and Uplink-4 as a standby link, you cannot use these two uplinks in the same

Option	Description
	or a different uplink profile on the NSX Edge transport node. However, in Uplink-Profile-1 if you use Uplink-3 as an active uplink but don't use any uplink as a standby uplink, you can use Uplink-3 in another teaming policy. ■ **Load Balance Source**: Select a list of active uplinks. When you configure a transport node, you can pin each interface of the transport node to one active uplink. This configuration allows use of several active uplinks at the same time. ■ **Load Balance Source MAC Address**: Select an uplink based on a hash of the source Ethernet. **Note** ■ On hypervisor hosts: ■ KVM hosts: Only Failover Order teaming policy is supported, whereas Load Balance Source and Load Balance Source MAC teaming policies are not supported. ■ ESXi hosts: Load Balance Source MAC, Load Balance Source, and Failover Order teaming policies are 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. **Important** To manage VLAN traffic, if you configure a default teaming policy in Load Balance Source mode, then on failure of the first uplink, traffic will not fail over to the second uplink interface. (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. 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 1700.

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 1700 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. 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 vMotion, virtual machines, and so on.

- Management Traffic: is traffic for a host management

- 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 percentage of uplink bandwidth 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 Profile**.

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:] `vsish`

`/ > 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:] `vsish`

`/ > 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 Profile**.

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 specifies the primary NSX Edge node that will be the preferred node for the active bridge and backup node that will be preferred for the backup bridge.

At the time of the creation of the Bridge Profile, no Bridge is instantiated yet. The Bridge Profile is just a template for the creation of one or several Bridge pairs. Once a Bridge Profile is created, you can attach a segment to it. By doing so, an active Bridge instance is created on the primary Edge, while a standby Bridge is provisioned on the backup Edge. NSX-T Data Center creates a Bridge Endpoint object, which represents this pair of Bridges. The attachment of the segment to the Bridge Endpoint is represented by a dedicated logical port.

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. In the preemptive mode, the Bridge on the primary Edge will always become the active bridge forwarding traffic between overlay and VLAN as soon as it is available. In the non-preemptive mode, the Bridge on the primary Edge will remain standby if it becomes available when the Bridge on the backup Edge is already active.

4 After you create a Bridge Profile, associate it to a segment.

5 Select **Networking > Segments > NSX > Add Segment**.

6 Enter the required details and click **Save**.

7 Edit the segment to which you want to add the Bridge Profile.

8 In the Additional Settings section, in the Edge Bridges field, select **Set**.

9 Click **Add Edge Bridge**.

10 Select the Edge Bridge Profile.

11 Select the Transport Zone where the bridged traffic is sent to the N-VDS selected by the transport zone.

12 Select the VLAN ID for the VLAN traffic as well as the physical port you select on the NSX Edge for sending or receiving this VLAN traffic.

13 Select the teaming policy to decide how N-VDS balances traffic across its uplinks.

14 Click **Add**.

15 Click **Save**.

Results

The newly created NSX Edge Bridge Profile is associated to a segment to balance VLAN traffic.

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.

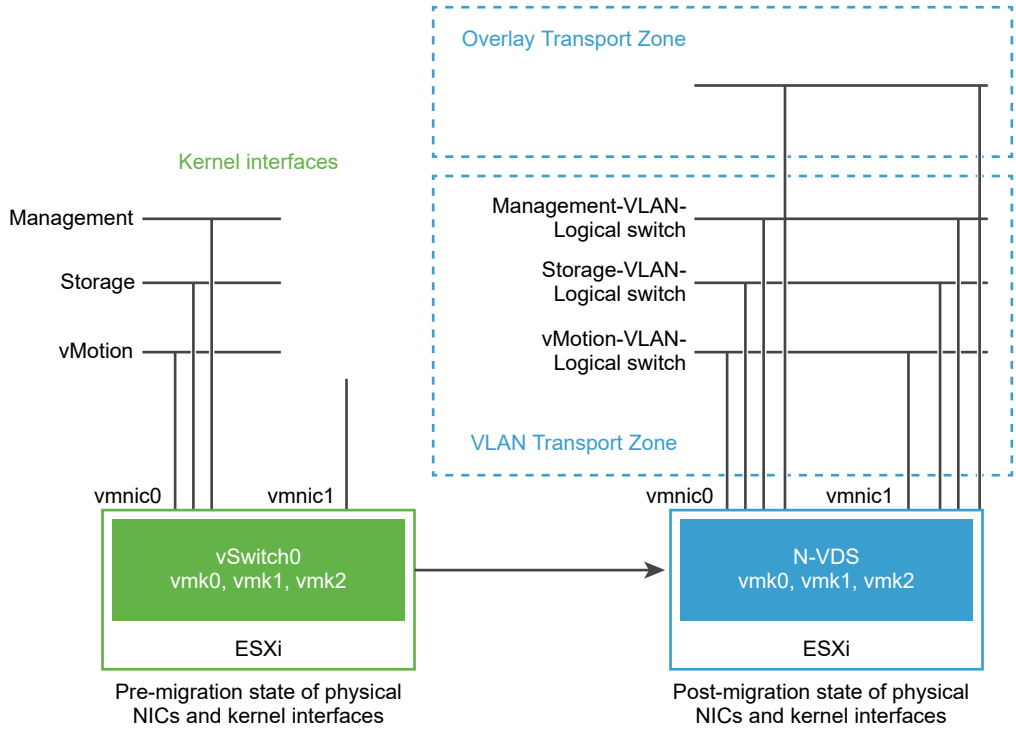
During migration physical NICs currently in use are migrated to an N-VDS switch, while available or free physical NICs are attached to the N-VDS switch after migration.

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 9-2. Pre and Post Migration of Network Interfaces to an N-VDS



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 Based on the NSX-T Data Center version, select one of the following:

  (NSX-T Data Center 3.2.2 or later) **System > Fabric > Hosts** and select the **Cluster** tab.

  (NSX-T Data Center 3.2.1 or earlier) **System > Fabric > Nodes > Host Transport Nodes**

7 For each transport node, verify the status on the **Node Status** column is Success to confirm that the transport node configuration is successfully validated.

8 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 9-1. 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 9-1. 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.

Table 9-1. VMkernel Migration Errors (continued)

Error Code	Problem	Cause	Resolution
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.
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.

Table 9-1. VMkernel Migration Errors (continued)

Error Code	Problem	Cause	Resolution
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.
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.

Host Transport Nodes

10

You can prepare ESXi, KVM hosts and physical servers as NSX-T Data Center transport nodes. Before you prepare KVM or physical servers for NSX-T Data Center networking, ensure the required third-party packages are installed on hosts.

Read the following topics next:

- Manual Installation of NSX-T Data Center Kernel Modules
- Install Third-Party Packages on a KVM Host
- Preparing Physical Servers as NSX-T Data Center Transport Nodes
- Prepare Standalone Hosts as Transport Nodes
- Preparing ESXi and KVM Hosts as Transport Nodes
- Configure an ESXi Host Transport Node with Link Aggregation
- Prepare Clusters for Networking and Security Using Quick Start Wizard
- Deploy a Fully Collapsed vSphere Cluster NSX-T on Hosts Running N-VDS Switches
- Multiple NSX Managers Managing a Single vCenter Server
- Troubleshoot Multi-NSX Issues
- Managing Transport Nodes

Manual Installation of NSX-T Data Center Kernel Modules

As an alternative to using the NSX-T Data Center 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: The update completed successfully, but the system needs to be rebooted for the
changes to be effective.
   Reboot Required: true
   VIBs Installed: VMware_bootbank_nsx-adf_<release>, VMware_bootbank_nsx-
aggservice_<release>, VMware_bootbank_nsx-cli-libs_<release>, VMware_bootbank_nsx-
common-libs_<release>, VMware_bootbank_nsx-context-mux_<release>, VMware_bootbank_nsx-
esx-datapath_<release>, VMware_bootbank_nsx-exporter_<release>, VMware_bootbank_nsx-
host_<release>, VMware_bootbank_nsx-metrics-libs_<release>, VMware_bootbank_nsx-
mpa_<release>, VMware_bootbank_nsx-nestdb-libs_<release>, VMware_bootbank_nsx-
nestdb_<release>, VMware_bootbank_nsx-netcpa_<release>, VMware_bootbank_nsx-
netopa_<release>, VMware_bootbank_nsx-opsagent_<release>, VMware_bootbank_nsx-platform-
client_<release>, VMware_bootbank_nsx-profiling-libs_<release>, VMware_bootbank_nsx-
proxy_<release>, VMware_bootbank_nsx-python-gevent_<release>, VMware_bootbank_nsx-python-
greenlet_<release>, VMware_bootbank_nsx-python-logging_<release>, VMware_bootbank_nsx-
python-protobuf_<release>, VMware_bootbank_nsx-rpc-libs_<release>, VMware_bootbank_nsx-
sfhc_<release>, VMware_bootbank_nsx-shared-libs_<release>, VMware_bootbank_nsx-upm-
libs_<release>, VMware_bootbank_nsx-vdpi_<release>, VMware_bootbank_nsxcli_<release>,
VMware_bootbank_vsipfwlib_<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

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-netcpa

Provides communication required by the different components.

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.

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 -E 'nsx|vsip'** 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 Form an NSX Manager Cluster Using the 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 Form an NSX Manager Cluster Using the CLI .

Manually Install NSX-T Data Center Software Packages on RHEL and CentOS Linux 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 Linux.

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 Linux 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 Linux 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, run the `rpm -qa | egrep 'nsx|openvswitch'` command.

The installed packages in the output must match the packages in the nsx-rhel74, nsx-centos74, or nsxdirectory.

What to do next

Add the host to the NSX-T Data Center management plane. See Form an NSX Manager Cluster Using the 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 Form an NSX Manager Cluster Using the CLI .

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
python3
dkms
libc6-dev
libelf-dev
ifupdown
python3-netifaces
```

- On Ubuntu 20.04.2 LTS, run `apt-get install <package_name>` to install the following third-party packages manually.

```
traceroute
python3-mako
python3-simplejson
python3-unittest2
python3-yaml
python3-netaddr
python3-openssl
python3
dkms
libc6-dev
libelf-dev
ifupdown
python3-netifaces
```

- 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, RHEL 7.9 and CentOS 7.7	RHEL 8.2 and CentOS 8.2
wget PyYAML python-mako python-netaddr python3 redhat-lsb-core tcpdump python-netifaces	wget python36 python3-pyyaml python3-mako python3-netaddr python3-pyOpenSSL redhat-lsb-core tcpdump network-scripts python3-netifaces libbpf

- 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 python3 lsb-release libcap-progs

Verify Open vSwitch Version on RHEL or CentOS Linux KVM Hosts

Skip this topic if there are no OVS packages on the RHEL or CentOS Linux host. If OVS packages already exist on a RHEL or CentOS Linux host, you must either remove the existing OVS

packages and install the NSX-T Data Center supported OVS packages or upgrade the existing OVS packages to NSX-T Data Center supported ones.

The supported Open vSwitch version is 2.13.1.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 2.13.1.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 Data Center supported OVS packages or upgrade the existing OVS packages to NSX-T Data Center supported ones.

The supported Open vSwitch version is 2.13.1.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
```

Preparing Physical Servers as NSX-T Data Center Transport Nodes

To use NSX-T Data Center on a physical server (also known as Bare Metal server), you must install supported third-party packages.

Physical Server Concepts:

- Application - represents the actual application running on the physical server 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 physical server server is supported.
- Management Interface - represents the NIC which manages the physical server 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 physical server server in two ways: as a host transport node and as a host for NSX Manager.

Make sure that you have the supported physical server 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 physical server hosts on which the NSX Edges are deployed. See seciton on Forged Transmits in the *vSphere product documentation*.

Install Third-Party Packages on a Physical Server

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

Prerequisites

- SELinux should be disabled for all Linux physical hosts.
- 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, CentOS or Oracle Linux- `yum install libvirt-libs`
  - Ubuntu - `apt-get install libvirt0`
  - Oracle Linux - `rpm-qa | grep xxx`
  - 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 8.3 and 8.0, and CentOS 8.3 and 8.0, run `yum install` to install the third-party packages.

RHEL 8.3 and 8.0	CentOS 8.3 and 8.0
tcpdump boost-filesystem python3-pyyaml boost-iostreams boost-chrono python3-mako python3-netaddr python3-six snappy boost-date-time c-ares redhat-lsb-core wget net-tools yum-utils lsof libvirt-libs python3-gevent libev python3-greenlet python3 libbpf python3-netifaces network-scripts	tcpdump boost-filesystem python3-pyyaml boost-iostreams boost-chrono python3-mako python3-netaddr python3-six snappy boost-date-time c-ares redhat-lsb-core wget net-tools yum-utils lsof libvirt-libs python3-gevent libev python3-greenlet python3 libbpf python3-netifaces network-scripts

- On RHEL, CentOS, and Oracle Linux run `yum install` to install the third-party packages.

RHEL 7.9, 7.8, 7.7, and 7.6	CentOS 7.9, 7.8, 7.7, and 7.6	Oracle Linux 7.9, 7.8, 7.7, and 7.6
tcpdump boost-filesystem PyYAML boost-iostreams boost-chrono python-mako python-netaddr python-six gperftools-libs libunwind elfutils-libelf-devel snappy boost-date-time c-ares redhat-lsb-core wget net-tools yum-utils lsof python-gevent libev python-greenlet libvirt-libs python-netifaces python3 wget redhat-lsb-core	tcpdump boost-filesystem PyYAML boost-iostreams boost-chrono python-mako python-netaddr python-six gperftools-libs libunwind elfutils-libelf-devel snappy boost-date-time c-ares redhat-lsb-core wget net-tools yum-utils lsof python-gevent libev python-greenlet libvirt-libs python-netifaces python3 wget redhat-lsb-core	tcpdump boost-filesystem PyYAML boost-iostreams boost-chrono python-mako python-netaddr python-six gperftools-libs libunwind snappy boost-date-time c-ares redhat-lsb-core wget net-tools yum-utils lsof libvirt-libs python-netifaces python-greenlet libev python-gevent python3

- On SUSE 12 SP3, 12 SP4, and 12 SP5 (starting in NSX-T Data Center 3.2.1), 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
```

Configure a Physical Server as a Transport Node from GUI

As an admin, you can configure a physical server for NSX-T networking through the NSX Manager GUI.

Alternatively, you can run the Ansible script to achieve the same goal. See Secure Workloads on Windows Server 2016/2019 Bare Metal Servers for configuring Windows physical servers using Ansible. However, it is recommended to use the NSX Manager UI to prepare physical servers for NSX-T networking.

Physical servers supports an overlay and VLAN transport zone. You can use the management interface to manage the physical server server. The application interface allows you to access the applications on the physical server. These NIC configurations are supported on a physical server:

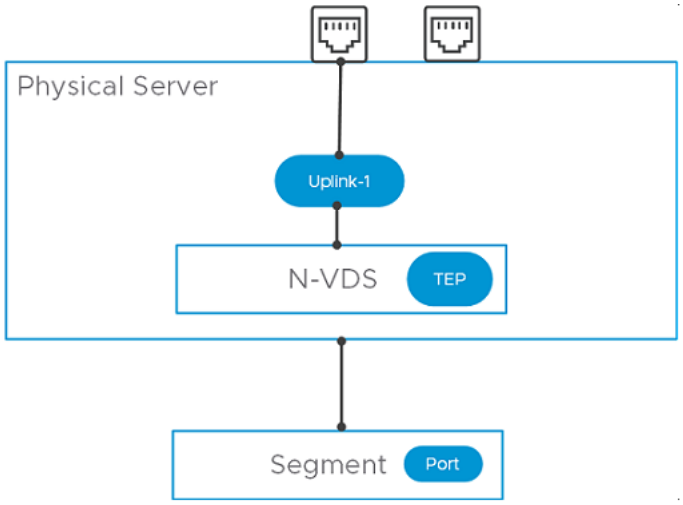
- Single physical NIC cards provide an IP address for both the management and the application IP interfaces.
- Dual physical NIC cards provide a physical NIC and a unique IP address for the management interface. Dual physical NIC cards also provide a physical NIC, and a unique IP address for the application interface.
- Windows servers: Dual physical NIC cards in a bonded configuration provide a unique IP address for both the management interface and the application interface. Such physical NIC bonds are supported through bonds created in the OS. Bond must be configured in the Switch Independent mode. Traffic running on management network is not supported on a bonded teaming interface.
- Linux servers: Bond interface only supports underlay mode (VLAN 0). Supported flavors are CentOS 7.9, CentOS 8.3, RHEL 7.9 and RHEL 8.3. Physical NIC bonds are supported in Active/Active and Active/Standby mode through OVS switch.

Unlike preparation of a standalone or a managed ESXi host that ends when it becomes a transport node, for a physical sever, complete server preparation extends to attaching the application interface of the physical server to an NSX-T segment.

After preparing the host as a transport node, you must complete the following tasks to finish configuring a physical server.

1 Create a segment port on an NSX-T segment.

2 Attach application interface of the physical server to the segment port.



Prerequisites

- 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 physical NIC must be available on the host node.
- Hostname
- Management IP address
- User name
- Password
- A segment (VLAN or Overlay), depending upon your requirement, must be available to attach to the application interface of the physical server.
- Verify that the required third-party packages are installed. Third party packages must be installed on the physical server so that its physical NICs are available during transport node configuration. See Install Third-Party Packages on a Physical Server.
- On Windows physical servers, log in as an administrator to install NSX.
- Starting with NSX Data Center 3.2.1, on Linux physical servers, you can update the `sudoers` file to add custom users with minimal privileges. The custom users allows you to install NSX without root permissions.

  After configuring visudo, run the following command to access the `/etc/sudoers` file.

  $ `sudo visudo`

  RHEL/CentOS/OEL/SLES:

  ```
  tester ALL=(ALL) /usr/bin/rpm, /usr/bin/nsxcli, /usr/bin/systemctl restart openvswitch
  ```

  Ubuntu:

  ```
  tester ALL=(ALL) /bin/ls, /usr/bin/sudo, /usr/bin/dpkg, /bin/nsxcli
  ```

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 → Nodes → Host Transport Node**.
3. On the **Host Transport Node** page, click **+ Add Host Node**.
4. On the **Host Details** window, enter the following details.

Option	Description
Name and Description	Enter the name to identify the physical server. You can optionally add the description of the operating system used for the host or physical server server.
IP Addresses	Enter the host or physical server server IP address.

Option	Description
Operating System	Select an operating system that mentions physical server. For example, if the operating system on the physical server is CentOS, select CentOS Physical Server. NSX-T identifies bare metal servers as physical servers. Depending on your physical 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 physical server 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 physical server 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	This is an optional step. 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 Click **Next**.

6 On the **Prepare Host** window, enter the following details. You can only configure a single N-VDS switch for a single physical server.

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.
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.

Option	Description
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.
Uplinks-Physical NICs Mapping	To map an uplink in NSX-T with a physical NIC or a bonded interface, enter the name of the physical NIC or bonded interface as configured on the physical server. For example, if **`teaming1`** is the name of the interface you configured on the Windows server, then enter **`teaming1`** in the **Physical NICs** field. **Important** ■ You cannot map one uplink to a physical NIC and another uplink to a bonded interface. ■ If you are using a bonded interface, both NICs must be configured to function at the same packet transfer speed. On Windows servers, you can configure teaming interfaces (bonded interfaces). The supported load balancing algorithms for teaming interfaces on Windows servers are: ■ TransportNodes load balancing algorithm ■ MacAddresses load balancing algorithm ■ IPAddresses load balancing algorithm In the teaming interface configuration, set **Teaming Mode** to **Switch Independent** mode. For more details, see Windows documentation. On Linux servers, you can configure a bonded interface by updating the `network-scripts` files. For more information, see Linux documentation.

7 Click **Next**.

8 As the host is configured, the physical server progress is displayed.

9 On the **Configure NSX** window, verify status of host preparation. Based on whether you want to proceed with further configuration, these choices are available:

	Description
Click Select Segment	If the physical server preparation was successful, click **Select Segment**. In the next part of the procedure, you select a segment to attach the physical server's application interface through the NSX agent. Proceed to the next step.
Click Continue Later	If you click **Continue Later** button, then preparation ends without the application interface configured. You can later attach the segment port to the application interface. Go to **Networking** → **Segments**. Configure application interface for the BMS.
Preparation Failed	If preparation failed, go to the Host Transport Node page (**System** → **Fabric** → **Nodes** → **Host Transport Node**). Identify the physical server, check if the Configuration State is in **Failed** state. Click **Resolve** to retry host preparation.

10 If you proceed to select a segment for the physical server, perform the following steps:

a From the list of segments connected to the transport zone you configured for the physical server, select the one to configure for the server.

b Click the vertical ellipses and click **Edit** to customize segment properties.

Note Only properties related to a segment can be edited. Admin can modify: Segment Name, Connected Gateway, Subnet, Uplink Teaming Policy, IP Address Pool.

11 To add a new segment port on an NSX-T segment, got to the Select Segment window, click Add Segment Port. The segment port page is auto-populated.

Option	Description
Name	Enter the Segment Port name.
ID	The virtual interface UUID is auto-populated.
Type	`Static` is auto-populated as the node is of the type, physical server.
Context ID	Transport node UUID is auto-populated.

Note Alternatively, you can also run the API command, `https://<NSX-Manager-IP-address>/PATCH /policy/api/v1/infra/segments/<segment-id>/ports/<port-id>`.

Where, `<port-id>` is the virtual interface UUID, which is displayed on NSX Manager.

12 To attach application interface of physical server to a segment port, go to the **Set Segment Port** window, expand the **Attach Application Interface** section and enter these details:

Note The **Attach Application Interface** section is only applicable for physical servers.

Option	Description
Name	You can change the system-generated application interface name. On a Linux physical server, run `ovs-vsctl show` to verify the application interface name.
Context ID	To enable the application interface configuration, enter the host node ID.
Assign Existing IP	Use an existing IP so that it can be used for migration of the application interface.
Assign New IP	Used when configuring an overlay network. Select an IP assignment method on the segment - IP pool, DHCP, or Static. When you assign a new IP address for the application interface, complete the configuration by providing the **IP address**, **Routing Table** and **Default Gateway** details.

13 Click **Save**.

14 View the summary of the network configuration represented by topology diagram.

15 On the **Host Transport Node** page, select the physical server, and click **Switch Visualization** for the server. It must represent the network you configured on the physical server.

Results

The physical server is configured for NSX-T networking.

Attach Segment Port to Application Interface of Physical Server

When configuring a physical server as a transport node, if you did not attach a segment port to application interface of the server, complete the task to ensure NSX-T is configured on the physical server.

Make changes to the segment or segment port properties in the following scenarios:

- If the application interface of the physical server was not attached to an NSX-T segment, revisit the physical server transport node to complete the configuration.
- If you want to change segment port parameters, such as assigning a different IP address to the application interface and so on to application interface of the physical server.

Prerequisites

- Ensure the physical server is prepared as an NSX-T transport node. See Prepare ESXi 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. If you did not configure the application interface of physical server, on the **Host Transport Node** page the node status is Success. The node indicates by showing a warning icon that segment port is not attached to application interface of physical server.
3. To configure the segment with the application interface, select the physical server, click **Actions → Manage Segment**.

   The **Manage Segment** window displays the segment that is already attached to the application interface of the physical server.
4. For the selected segment, click **Edit Segment Port**, configure the **Application Interface** section and click **Save**. The segment port status displays as **Success**, if everything is functional.
5. To add a new port on the segment, on the **Manage Segment** window, click **Add Segment Port** and add the required details.

   Alternatively, if a port already exists, click **Edit Segment** to proceed with configuration.

Option	Description
Context ID	To enable the application interface configuration, enter the host node ID.
Assign Existing IP	Use an existing IP so that it can be used for migration of the application interface.

Option	Description
Assign New IP	Used when configuring an overlay network. Select an IP assignment method on the segment - IP pool, DHCP, or Static. When you assign a new IP address for the application interface, complete the configuration by providing the **IP address**, **Routing Table** and **Default Gateway** details.
IP Address	Enter IP address for the application interface of the physical server.
Routing table	Enter routing table details.
Default Gateway	Enter the IP address of the gateway.

6 On the **Host Transport Node** page, select the physical server, and click **Switch Visualization** for the server. It must represent the network you configured on the physical server.

Results

A new segment port is attached to application interface of the physical server.

Ansible Server Configuration for Physical Server

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

It is recommended to configure segment ports for application interface of physical server through UI. See Configure a Physical Server as a Transport Node from GUI.

Ansible support modes are a set of automated scripts that set up the application interface for physical 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 servers:

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 physical server integration with NSX-T Data Centerfrom Github: –https://github.com/vmware/bare-metal-server-integration-with-nsxt

For Windows physical servers only:

1 Install pip for pywinrm.

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

Create Application Interface for Physical Server Workloads

Before you create or migrate an application interface for physical server workloads, you must configure NSX-T Data Center and install Linux third-party packages.

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

Procedure

1 Install the required third-party packages.

See Install Third-Party Packages on a Physical Server.

2 Configure the TCP and UDP ports.

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

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

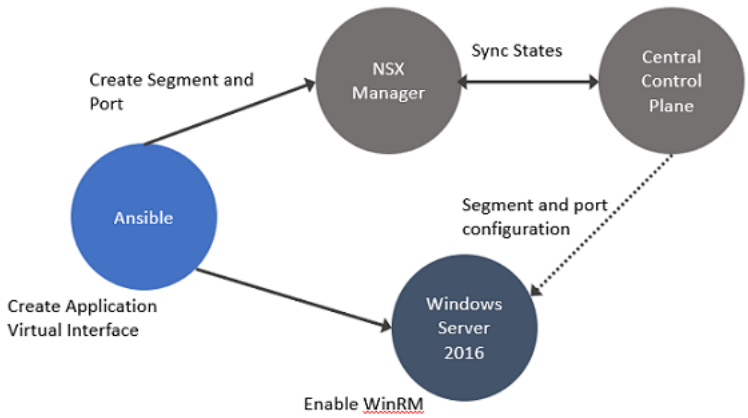
See Configure a Physical Server as a Transport Node from GUI.

4 Use the Ansible playbook to create an application interface.

See Ansible Server Configuration for Physical Server.

Secure Workloads on Windows Server 2016/2019 Bare Metal Servers

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 or 2019 bare metal workloads.

Prerequisites

- Configure your own proxy settings on the physical server.

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://raw.githubusercontent.com/vmware/bare-metal-server-integration-with-nsxt/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="[output of the 2nd command]"}'`.

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

3 Add the bare metal server as a standalone transport node. See Configure a Physical Server as a Transport Node from GUI.

4 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.

5 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.

6 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.

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

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

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

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

Prepare Standalone Hosts as Transport Nodes

You must first add your ESXi host, KVM host to the NSX-T Data Center fabric and then configure the transport node.

For a host 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, 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.

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.
- The reverse proxy service on all nodes of the NSX Manager cluster must be `Up` and running.

  To verify, run `get service http`. If the service is down, restart the service by running `restart service http` on each NSX Manager node. If the service is still down, contact VMware support.
- 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.

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:A2:4E: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 (NSX-T Data Center 3.2.1 and previous versions) Select **System** → **Fabric** → **Nodes** > **Host Transport Nodes**.

3 (NSX-T Data Center 3.2.1 and previous versions) From the **Managed by** dropdown field, select **Standalone Hosts** and click **+ Add Host Node**.

4 (NSX-T Data Center 3.2.2) Select **System** → **Fabric** → **Hosts**.

5 (NSX-T Data Center 3.2.2) Select the **Standalone** tab and click **+ Add Host Node**.

6 On the **Host Details** page, enter details for the following fields.

Option	Description
Name	Enter the name to identify the standalone host.
IP Addresses	Enter the host IP address.
Operating System	Select the operating system from the drop-down menu. Depending on your host, you can select any of the supported operating systems. See System Requirements.
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.

Option	Description
Description	(Optional) Add description for the host.
Tags	Add tags and define scope for tags.

7 (Required) For a KVM host, 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, N-VDS type is always set to **NSX Created**.

8 On the **Prepare Host** tab, configure the host switch that is used to prepare the standalone host. You can configure multiple N-VDS switches on a single host.

9 Click **Add Host Switch** and select **NVDS**.

Option	Description
Name	Enter a name for the NVDS host switch.
Mode	Select the mode you want to use the NVDS switch. ■ Standard ■ Enhanced Datapath ■ ENS Interrupt
Transport Zone	From the drop-down menu, select a transport zone that spans across this transport node.
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. Multiple N-VDS host switches on a transport node can belong to the same VLAN segment or VTEP pool, or they can belong to different VLAN segments or VTEP IP pools. Configuring different transport VLAN segments for different N-VDS host switches allows additional traffic isolation in the underlay as well.
NIOC Profile	Select the NIOC profile that will be applied to the host switch.
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.
Teaming Policy Uplink Mapping	Map uplinks to physical NICs. If NSX Manager cannot fetch the physical NICs of the host, manually enter NIC to complete the mapping.

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	Click **Set** and click **Add**. Map VMkernel Adapter or Physical Adapter to VLAN Segments and click **Apply**. ■ From the **VMkernel Adapter** drop-down menu, select VMkernel Adapter. ■ From the **VLAN Segments** drop-down menu, select VLAN Segment. The NSX Manager migrates the VMkernel Adapters to the mapped VLAN Segment on N-VDS. **Caution** Ensure that the management NIC and management VMkernel interface are migrated to a segment 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.
Network Mappings for Uninstall	Click **Set**. 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`. Add VMKNIC to PortGroup mappings and click **Apply**. ■ In the **VMkernel Adapter** field, enter VMkernel Adapter name. ■ In the **PortGroup** field, enter portgroup name of the type Ephemeral. Add Physical NIC to uplink profile mappings and click **Apply**. ■ In the **Physical NICs** field, enter physical NIC name. ■ In the **Uplink** field, enter uplink name. **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.

10 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.
Transport Zone	From the drop-down menu, select a transport zone that spans across this transport node.
VTEP	Virtual tunnel endpoint name for transport nodes to communicate on an overlay network.

11 View the connection status on the **Standalone** 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 as a transport node, the connection to NSX Manager state displays as `UP` only after the host is successfully created as a transport node.

Note After the transport node is created, if you want to change configuration of the N-VDS 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.

12 (Optional) On KVM hosts, if the transport node creation fails because of multiple processes trying to access the `dpkg` command, select the host and click **Retry** to restart creation of transport node.

13 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"`

14 Verify that the NSX-T Data Center modules are installed on your host.

As a result of adding a host to the NSX-T Data Center fabric, a collection of NSX-T Data Center modules are installed on the host.

The modules on different hosts are packaged as follows:

- KVM on RHEL, CentOS, Oracle Linux, 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, CentOS, or Oracle Linux, 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`

15 (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

The standalone host is configured as a transport node.

Important If you move a standalone transport node to a cluster with transport node profile applied to it, NSX-T Data Center gives precedence to the transport node profile applied to the cluster and overrides the configuration of the standalone transport node. If vmnics on the cluster and standalone host are different, connectivity to the standalone transport can be potentially lost.

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.

Preparing ESXi and KVM Hosts as Transport Nodes

After you create transport zones, IP pools, uplink profiles for transport nodes, prepare a host as a transport node. An ESXi, KVM, or bare metal (physical server) can be prepared as a transport node. Only ESXi hosts support both N-VDS and vSphere Distributed Switch (NSX Switch in vCenter Server). KVMs and physical servers only support the N-VDS host switch type.

Transport Node Profiles

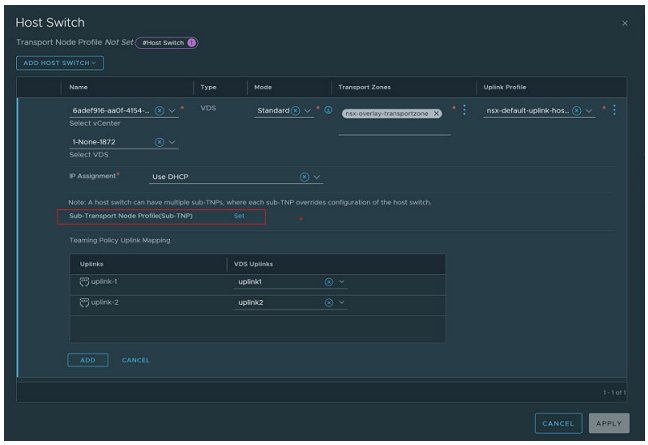
A Transport Node Profile (TNP) is a template to define networking configuration that is applied to a cluster.

Transport Node Profile

Before you create a Transport Node Profile consider these points:

- 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.
- 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.

To create a TNP, you configure Host Switches with transport zones, uplink profiles, mapping uplinks to VDS uplinks (for a VDS switch) and other configurations. TNP can be created on VDS or N-VDS Host Switches.



A stretched cluster is a cluster that extends across multiple TEP subnets. A non-stretched cluster is a cluster that is confined to a single TEP subnet. In a non-stretched cluster, a single TNP is sufficient to be applied to a cluster. However, when a cluster is stretched across multiple subnets or L3 domains, you can create sub-clusters consisting of hosts that need the same configuration.

While a TNP represents the global configuration applied to a Host Switch, a sub-TNP represents the local configuration applied to a sub-cluster. When you apply a sub-TNP to a sub-cluster, all the configuration from sub-TNP takes precedence over the global TNP configuration.

Note A Sub-TNP can only be created for vSphere Distributed Switch (VDS) switches.

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.

Note TNP is not used to prepare standalone hosts.

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.

Sub-TNPs and Sub-clusters

A Sub-TNP is a template to define configuration that is applied to hosts that are part of a Sub-cluster. To accommodate different cluster configurations required for sub-clusters, create sub-TNPs.

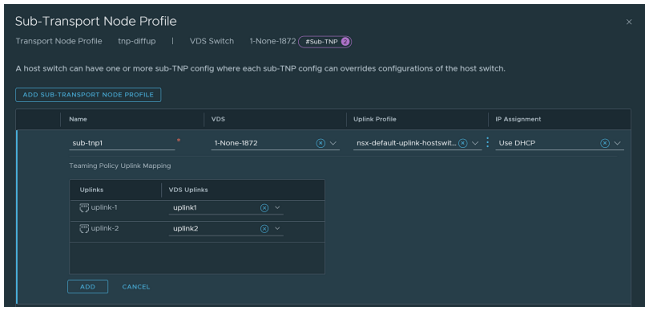
Sub-Transport Node Profile

Starting with NSX-T Data Center 3.2.2, you can configure Sub-TNPs and Sub-clusters.

Note The maximum number of Sub-TNPs under a hostswitch in a TNP is 16.

While a TNP represents the global configuration applied to a Host Switch, a sub-TNP represents the local configuration applied to a sub-cluster. When you apply a sub-TNP to a sub-cluster, the global TNP is overriden on the sub-cluster.

You can only apply a sub-TNP to a VDS switch. A sub-TNP can only override the following fields of a global TNP: VDS Host Switches ID, uplink profiles and IP assignment.



NSX Manager prepares the hosts in sub-clusters where the sub-TNP is applied 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.

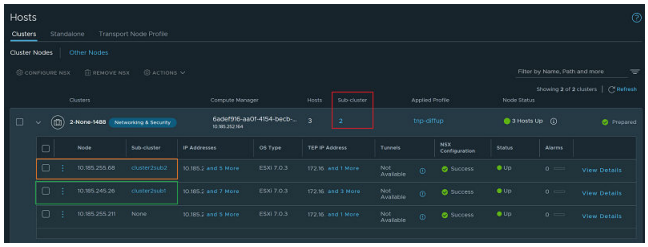
To delete a Sub-TNP, you must first detach the global TNP profile from the associated cluster. The existing transport nodes are not affected. New hosts added to the cluster are no longer automatically converted into transport nodes.

Sub-clusters

Each cluster can have up to 16 sub-clusters.

To manage a cluster that is stretched across different subnets or L3 domains, some hosts will need different configuration, such as a some hosts will need to be in the TEP subnet-1, whereas some other hosts will need to be in TEP subnet-2. So, hosts with similar configuration requirements can be placed in one sub-cluster. And that sub-cluster can be applied with a sub-TNP that provides configuration.

In the following image, the cluster has three hosts: one in each sub-cluster and the last host is not part of any sub-cluster.



Moving Hosts Between Sub-clusters

1 Move host from sub-cluster1 to sub-cluster2.

2 Sub-TNP config of sub-cluster1 is removed from the host.

3 Sub-TNP config of sub-cluster2 is applied to the host.

Limitations of using Sub-clusters

- Sub-clusters can have hosts only from the cluster under which it is created.
- Sub-cluster cannot have hosts which are part of other sub-clusters.

- Maximum number of sub-clusters under a cluster is 16.
- Sub-cluster cannot be deleted if it has some hosts in it. After removing the hosts, sub-cluster can be deleted.
- Minimum supported ESXi version for this feature is 7.0.0.
- Stateless hosts cannot be added to a sub-cluster.

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.
- Ensure that the MTU value of the physical switch port or LACP port is set to 1600.

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**.

     Note On VDS 7.0 or later, the default MTU size is 1500. To prepare a VDS for NSX-T overlay networking, the MTU size of the VDS must be at least 1600. Starting in NSX-T Data Center 3.2.1, if the MTU size of the VDS is below 1600, NSX Manager notifies you that the MTU size will be automatically increased to 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 Prepare ESXi Cluster Hosts as Transport Nodes.

Add a Transport Node Profile

You must create a Transport Node Profile (TNP) and if needed Sub-TNPs before you prepare ESXi clusters as transport nodes. Both VDS and N-VDS Host Switches are supported.

Note Transport node profiles are only applicable to hosts. It cannot be applied to NSX Edge transport nodes.

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 the 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 (NSX-T Data Center 3.2.1 and previous versions) Select **System** → **Fabric** → **Profiles** > **Transport Node Profiles** > **Add Profile**.

3 (NSX-T Data Center 3.2.2) Select **System** → **Fabric** → **Hosts**.

4 (NSX-T Data Center 3.2.2) On the **Hosts** page, select **Transport Node Profile** → **Add Transport Node Profile**.

5 Enter a name to identify the transport node profile.

You can optionally add the description about the transport node profile.

6 The **Applied Clusters** field, is populated with the cluster names that have applied this transport node profile.

7 In the **Host Switch** field, select **Set**.

8 If you select **NVDS** as the host switch type, proceed to enter details for the fields described in this step. Skip to the next step, if you select **VDS** as the host switch type.

Option	Description
Name	Enter a name for the NVDS switch.
Type	Indicates the type of switch that is configured.
Mode	Choose between these options: ■ Standard: Is the standard mode that is available to all supported hypervisors by NSX-T Data Center. ■ ENS Interrupt: Is a variant of the Enhanced Datapath mode. ■ Enhanced Datapath: Is the mode that provides accelerated networking performance. This mode requires nodes to use VMXNET3 vNIC enabled network cards. It is not supported on KVM, NSX Edge nodes and Public Gateways. The supported hypervisor is ESXi. It is recommended to run ESXi v6.7 U2 and later versions.
Transport Zone	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. Multiple N-VDS host switches on a transport node can belong to the same VLAN segment or VTEP pool, or they can belong to different VLAN segments or VTEP IP pools. Configuring different transport VLAN segments for different N-VDS host switches allows additional traffic isolation in the underlay as well.
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 between **Use DHCP** , **Use IP Pool** or **Use Static IP List** to assign an IP address to tunnel endpoints (TEPs) of the transport node. If you selected **Use IP Pool** for an IP assignment, specify the IP pool name and the range of IP addresses that can be used for tunnel endpoints.
Teaming Policy Uplink Mapping	Map uplinks defined in the selected NSX-T uplink profile with physical NICs. The number of uplinks that are presented for mapping depends on the uplink profile configuration. For example, in the upink-1 (active) row, go to the Physical NICs column, click the edit icon, and type in the name of physical NIC to complete mapping it with uplink-1 (active). Likewise, complete mapping for the other uplinks.

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	Click **Set** and click **Add**. Add VMkernel Adapter or Physical Adapter to VLAN Segments mappings and click **Apply**. ■ From the **VMkernel Adapter** drop-down menu, select VMkernel Adapter. ■ From the **VLAN Segments** drop-down menu, select VLAN Segment. The NSX Manager migrates the VMkernel Adapters to the mapped VLAN Segment on N-VDS. **Caution** Ensure that the management NIC and management VMkernel interface are migrated to a segment 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	Click **Set**. 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`. Add VMKNIC to PortGroup mappings and click **Apply**. ■ In the **VMkernel Adapter** field, enter VMkernel Adapter name. ■ In the **PortGroup** field, enter portgroup name of the type Ephemeral. Add Physical NIC to uplink profile mappings and click **Apply**. ■ In the **Physical NICs** field, enter physical NIC name. ■ In the **Uplink** field, enter uplink name. **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.

Option	Description
	For more information, see VMkernel Migration to an N-VDS Switch.

9 Select **VDS** as the host switch type and enter the switch details. You can use the same VDS switch to configure NSX-T Data Center on multiple transport nodes or clusters as long as they are part of that VDS switch in vCenter Server.

Option	Description
vCenter	Select the vCenter Server.
Type	Indicates the switch type that will be configured on the host.
Mode	Choose between these options: ■ Standard: Is the standard mode that is available to all supported hypervisors by NSX-T Data Center. ■ ENS Interrupt: Is a variant of the Enhanced Datapath mode. ■ Enhanced Datapath: Is the mode that provides accelerated networking performance. This mode requires nodes to use VMXNET3 vNIC enabled network cards. It is not supported on KVM, NSX Edge nodes and Public Gateways. The supported hypervisor is ESXi. It is recommended to run ESXi v6.7 U2 and later versions.
VDS	Select a VDS that is created under the selected 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.
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 between **Use DHCP** and **Use IP Pool** to assign an IP address to tunnel endpoints (TEPs) of the transport node. If you selected **Use IP Pool** for an IP assignment, specify the IP pool name and the range of IP addresses that can be used for tunnel endpoints.

Option	Description
Sub-Transport Node Profile (Sub-TNP)	(NSX-T Data Center 3.2.2) Click **Set**. In the Sub-Transport Node Profile window, enter these details and click **Add Sub-Transport Node Profile**: ■ Enter a name for the Sub-TNP. ■ Select a VDS switch for Sub-TNP. ■ Select an uplink profile. ■ Select an IP Assignment: Use DHCP or IP Pool. ■ Map NSX-T uplinks to VDS links. ■ Click **Add**. ■ Click **Apply**.
Teaming Policy Switch Mapping	Before you map uplinks profiles in NSX-T with uplinks in VDS, ensure uplinks are 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**. Map uplinks defined in the selected NSX-T uplink profile with VDS uplinks. The number of NSX-T uplinks that are presented for mapping depends on the uplink profile configuration. For example, in the upink-1 (active) row, go to the Physical NICs column, click the edit icon, and type in the name of VDS uplink to map it with uplink-1 (active). Likewise, complete mapping for the other uplinks.

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 Click **Add** to complete the configuration.

What to do next

Apply the transport node profile to an existing vSphere cluster. See Prepare ESXi Cluster Hosts as Transport Nodes.

Prepare ESXi Cluster Hosts as Transport Nodes

If a cluster of ESXi hosts is registered to a vCenter Server, you can apply transport node profiles on the ESXi cluster to automatically prepare all hosts as NSX-T Data Center transport nodes.

Prerequisites

- Verify that all hosts in the vCenter Server are powered on.
- Verify that the system requirements are met. See System Requirements.
- The reverse proxy service on all nodes of the NSX Manager cluster must be `Up` and running.

To verify, run `get service http`. If the service is down, restart the service by running `restart service http` on each NSX Manager node. If the service is still down, contact VMware support.

- 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*.

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. (NSX-T Data Center 3.2.1 and previous versions) Select **System** → **Fabric** → **Nodes** > **Host Transport Nodes**.
3. (NSX-T Data Center 3.2.1 and previous versions) From the **Managed by** dropdown field, select the vCenter Server.
4. (NSX-T Data Center 3.2.2) Select **System** → **Fabric** → **Hosts** > **Clusters**.
5. (NSX-T Data Center 3.2.2) To set Sub-clusters in the cluster:
   a. In a cluster, go to the **Sub-cluster** field, click **Set**.
   b. In the Sub-cluster window, click **Add Sub-cluster**.
   c. In the Sub-cluster field, enter a name for the Sub-cluster.
   d. In the **Nodes** field, click **Set**.
   e. In the Set Host Nodes window, select the nodes that must be part of the Sub-cluster and click **Apply**.
6. Select a cluster and click **Configure NSX**.
7. In the **NSX Installation** pop-up window, from the **Transport Node Profile** drop-down menu, select the transport node profile to apply to the cluster. If a transport node profile is not created, click **Create New Transport Node Profile** to create a new one. See Add a Transport Node Profile.
8. (NSX-T Data Center 3.2.2) In the **Sub-cluster Nodes** tab, expand each Sub-cluster and assign each Sub-cluster with a Sub-TNP. The Sub-TNPs must have been defined in the TNP applied to the cluster. If no Sub-TNP is assigned to a Sub-cluster, then global TNP will be applied to that Sub-cluster. After applying the TNP, the Sub-TNP configurations will override the TNP configurations for the Sub-cluster.
9. Click **Save** to begin the process of transport node creation of all hosts in the cluster.

10 If you only want to prepare individual hosts as transport nodes, select a host, 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.

11 In the **Prepare Host** page, click **Add Host Switch**.

12 SelectIn the **Configure NSX** panel, expand **New Node Switch**.

13 If you select **NVDS** as the host switch type, proceed to enter details for the fields described in this step. Skip to the next step, if you select **VDS** as the host switch type.

Option	Description
Name	Enter a name for the NVDS switch.
Type	Indicates the type of switch that is configured.
Mode	Choose between these options: ■ Standard: Is the standard mode that is available to all supported hypervisors by NSX-T Data Center. ■ ENS Interrupt: Is a variant of the Enhanced Datapath mode. ■ Enhanced Datapath: Is the mode that provides accelerated networking performance. This mode requires nodes to use VMXNET3 vNIC enabled network cards. It is not supported on KVM, NSX Edge nodes and Public Gateways. The supported hypervisor is ESXi. It is recommended to run ESXi v6.7 U2 and later versions.
Transport Zone	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. Multiple N-VDS host switches on a transport node can belong to the same VLAN segment or VTEP pool, or they can belong to different VLAN segments or VTEP IP pools. Configuring different transport VLAN segments for different N-VDS host switches allows additional traffic isolation in the underlay as well.
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 between **Use DHCP** , **Use IP Pool** or **Use Static IP List** to assign an IP address to tunnel endpoints (TEPs) of the transport node. If you selected **Use IP Pool** for an IP assignment, specify the IP pool name and the range of IP addresses that can be used for tunnel endpoints.

Option	Description
Teaming Policy Uplink Mapping	Map uplinks defined in the selected NSX-T uplink profile with physical NICs. The number of uplinks that are presented for mapping depends on the uplink profile configuration. For example, in the upink-1 (active) row, go to the Physical NICs column, click the edit icon, and type in the name of physical NIC to complete mapping it with uplink-1 (active). Likewise, complete mapping for the other uplinks.
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	Click **Set** and click **Add**. Add VMkernel Adapter or Physical Adapter to VLAN Segments mappings and click **Apply**. ■ From the **VMkernel Adapter** drop-down menu, select VMkernel Adapter. ■ From the **VLAN Segments** drop-down menu, select VLAN Segment. The NSX Manager migrates the VMkernel Adapters to the mapped VLAN Segment on N-VDS. **Caution** Ensure that the management NIC and management VMkernel interface are migrated to a segment 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	Click **Set**. 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`. Add VMKNIC to PortGroup mappings and click **Apply**. ■ In the **VMkernel Adapter** field, enter VMkernel Adapter name. ■ In the **PortGroup** field, enter portgroup name of the type Ephemeral. Add Physical NIC to uplink profile mappings and click **Apply**. ■ In the **Physical NICs** field, enter physical NIC name. ■ In the **Uplink** field, enter uplink name. **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.

Option	Description
	For more information, see VMkernel Migration to an N-VDS Switch.

14 Select **VDS** as the host switch type and enter the switch details.

Option	Description
vCenter	Select the vCenter Server.
Name	Indicates the switch type that will be configured on the host.
Mode	Choose between these options: ■ Standard: Is the standard mode that is available to all supported hypervisors by NSX-T Data Center. ■ ENS Interrupt: Is a variant of the Enhanced Datapath mode. ■ Enhanced Datapath: Is the mode that provides accelerated networking performance. This mode requires nodes to use VMXNET3 vNIC enabled network cards. It is not supported on KVM, NSX Edge nodes and Public Gateways. The supported hypervisor is ESXi. It is recommended to run ESXi v6.7 U2 and later versions.
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.
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.

Option	Description
IP Assignment	Select between **Use DHCP** , **Use IP Pool** or **Use Static IP List** to assign an IP address to tunnel endpoints (TEPs) of the transport node. If you selected **Use IP Pool** for an IP assignment, specify the IP pool name and the range of IP addresses that can be used for tunnel endpoints.
Teaming Policy Switch Mapping	Before you map uplinks profiles in NSX-T with uplinks in VDS, ensure uplinks are 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**. Map uplinks defined in the selected NSX-T uplink profile with VDS uplinks. The number of NSX-T uplinks that are presented for mapping depends on the uplink profile configuration. For example, in the upink-1 (active) row, go to the Physical NICs column, click the edit icon, and type in the name of VDS uplink to complete mapping it with uplink-1 (active). Likewise, complete mapping for the other uplinks.

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.

15 Click **Add** and **Finish** to begin host transport node preparation.

16 (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
```

17 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.

Note If hosts in a cluster are running ESXi v7.0 or later where the host switch is vSphere Distributed Switch, the Host Transport Node page displays TEP addresses of the host in addition to IP addresses. TEP address is the address assigned to the VMkernel NIC of the host, whereas IP address is the management IP address.

18 (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.

19 (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*.

Change Sub-cluster

When you want to apply a different networking configuration to a host in a sub-cluster, such as a different uplink profile, move the host to a different Sub-cluster.

To change Sub-cluster a host belongs to, perform these steps:

Procedure

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

2 Select **System** → **Fabric** → **Hosts**.

3 Select the **Clusters** tab.

4 Select a node and click **Actions** → **Change Sub-cluster**.

5 In the Change Sub-cluster window, select a Sub-cluster that the host must be moved to.

6 Click **Save**.

Detach Cluster TNP

When you want to apply a different cluster TNP, deteach the existing one before applying a new TNP.

To detach cluster TNP, perform these steps:

Procedure

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

2 Select **System** → **Fabric** → **Hosts**.

3 Select the **Clusters** tab.

4 Select a cluster and click **Actions** → **Detach Transport Node Profile**.

NSX detached the existing cluster TNP. At the end of the action, the cluster will not have any TNP applied to it.

Migrate VMkernels and Physical NICs to a vSphere Distributed Switch

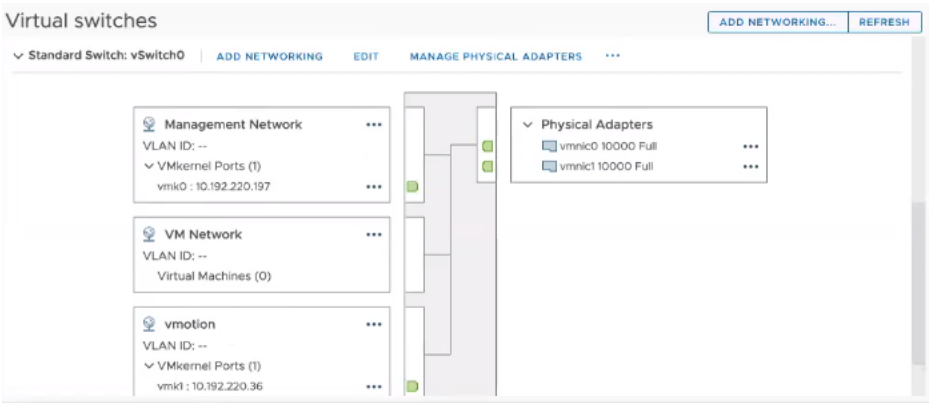
Manually migrate VMkernel adapters from a vSphere Standard Switch or from an N-VDS switch to a vSphere Distributed Switch.

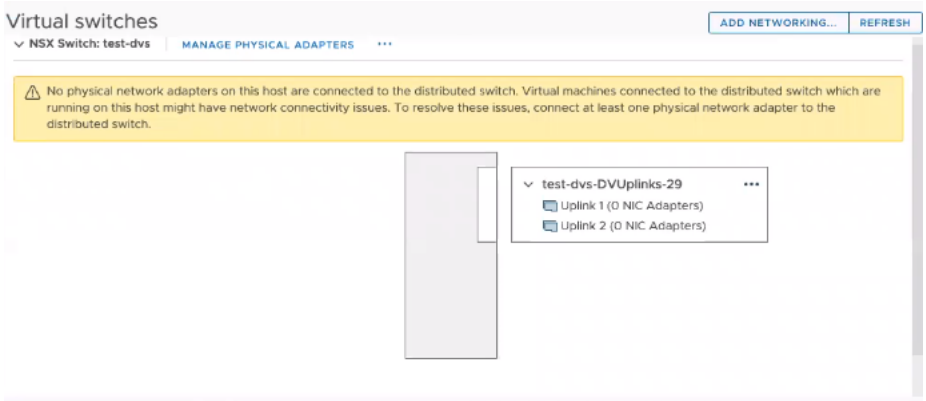
Note Starting with NSX-T Data Center 3.0, transport nodes can be created using vSphere Distributed Switch.

After preparing the transport node with vSphere Distributed Switch host switch type (referred to as an NSX Switch in vCenter Server), manually migrate VMkernel adapters (vmks) and physical NICs (vmnics) to an NSX Switch on the ESXi host.

In the procedure below, consider this switch configuration:

- vmk0, vmk1 are connected to vSwitch0, and vmnic0, vmnic1 are configured as uplink 1 and 2 respectively on the vSwitch0.
- NSX Switch does not have any vmnic or VMkernel adapter configured.





At the end of the procedure, vmnic0, vmnic1 and vmk0, vmk1 are migrated to vSphere Distributed Switch (referred to as an NSX Switch in vCenter Server).

Prerequisites

- ESXi hosts are prepared as transport nodes using vSphere Distributed Switch.

Procedure

1. From a browser, log in with admin privileges to a vCenter Server at https://<vCenterServer-ip-address>.
2. Navigate to **Host** → **Configure** → **Virtual Switches**.
3. View existing vmknics configured on vSwitch0.
4. Make a note of the vmknics to be migrated to the distributed virtual port group of the NSX Switch.
5. Navigate to **Home** → **Networking**, to view all switches configured in the data center.
6. In the Switch page, click **Actions** → **Add and Manage Hosts**.
7. Select **Manage Host Networking**.
8. Click **Next**.
9. In the Select Member Hosts window, select **`hosts`**.
10. Click **Ok**.
11. In the Manage physical adapters window, claim unassigned adapters, as there are available vmnics that can be attached to a switch.
    a. Select an unclaimed uplink and click **Assign uplink**.
    b. Map a vmnic to an uplink on the NSX Switch.
    c. Click **Ok**.

12 In the Manage VMkernel adapters window, assign port groups to NSX Switch.

   a Select a vmk on vSwitch0 and click **Assign port group**.

   b Select a NSX port group to assign a vmk to an NSX segment.

   c Perform steps a and b for the remaining hosts that are managed by the switch.

13 Finish the Add and Manage Hosts wizard.

14 To verify vmk0 and pnics are migrated from vSwitch0 to NSX Switch on the ESXi host, navigate to **Host → Configure → Virtual Switches**. View the updated switch configuration.

15 Alternatively, run the API command, `https://<NSXManager-IP-address>/api/v1/logical-ports`, to verify migration of VMkernel adapters is successful.

Note All vmk0 ports are set to `Unblocked VLAN` state because management traffic and services are managed by vmk0 ports. These vmk0 ports in `Unblocked VLAN` state allows admins to connect to the vmk0 port if hosts lose connectivity.

What to do next

Navigate to NSX Manager. In the Host Transport Node page, verify configuration status changed from `Degraded` to `Success`, as vmnics and vmks are migrated to the NSX Switch, the vSphere Distributed Switch.

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 Prepare Standalone Hosts as Transport Nodes.
- If you plan to configure a VDS switch on the host, configure LAG on the VDS switch.

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 Profile**.

3 Enter a name and optionally a description.

   For example, you enter the name **`uplink-profile1`**.

4 (Only N-VDS) 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, do one of the following:

   a (N-VDS) Enter the name of the LAG that you added in the step 4. In this example, the name is **`lag1`**.

   b (VDS) Enter the name of the LAG that you configured on the VDS switch in vCenter Server.

7 Enter the VLAN ID for **Transport VLAN**.

8 (Only N-VDS) Enter a value for **MTU**. If left blank, NSX-T Data Center sets the value to 1600. This field is not applicable to VDS.

9 Click **Add** at the bottom of the dialog box.

10 (Only N-VDS switches) Under **Teamings**, click **Add** to add an entry for link aggregation.

11 Based on the NSX-T Data Center version, navigate the UI:

   - (NSX-T Data Center 3.2.2 or later) **System > Fabric > Hosts** and select the **Cluster** tab.
   - (NSX-T Data Center 3.2.1 or earlier, 4.0.x) **System > Fabric > Nodes > Host Transport Nodes** and select the vCenter Server that hosts the ESXi host.

12 In the **Host Details** tab, enter IP address, OS name, admin credentials, and SHA-256 thumbprint of the host.

13 During the switch configuration, depending on N-VDS or VDS switch, select the uplink profile **`uplink-profile1`** that was created in step 3.

14 (N-VDS) 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`**.

15 (VDS) In the **Physical NICs** field, the physical NICs and uplinks dropdown list reflects the new NICs and uplink profile. Specifically, the uplink LAG that is configured on the VDS switch is displayed in the uplink profile drop-down list. Select the VDS uplink for LAG.

16 Enter information for the other fields and complete host preparation.

   The ESXi host is prepared as a transport node using the LAG profile.

Prepare Clusters for Networking and Security Using Quick Start Wizard

Using the Quick Start wizard, you can configure ESXi clusters for either Networking and Security or Security Only.

Note If you configure a cluster for Security Only then you cannot configure networking for that cluster.

Prepare Clusters for Networking and Security

Use the Quick Start wizard to prepare ESXi clusters for networking and security using NSX-T recommended host configurations.

The Quick Start wizard gives you two options to prepare ESXi clusters: Networking and Security or Security Only. With either of these options, the wizard helps you finish installation with minimum user input, thus, simplifying the installation process. By default, VLAN networking is the default selection in the wizard.

Based on the type of host, the quick start wizard considers the following default configurations:

- ESXi hosts running 6.7 and earlier versions are prepared on the N-VDS host switch.
- ESXi hosts running 7.0 and later are prepared on the VDS switch. Configure the desired number of uplinks on the VDS switch in vCenter Server and set the MTU to 1600.

Each host switch is assigned an auto-created transport zone and uplink profile.

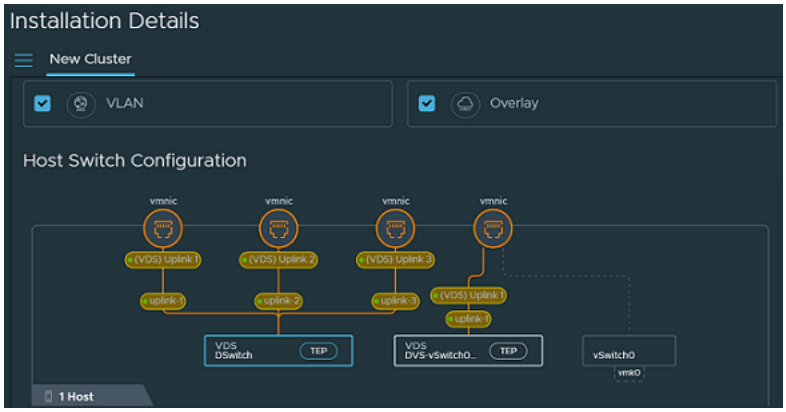
Prerequisites

- As VMkernel adapters are migrated from existing switches to newly created switches, ensure to power off any VMs that are connected to VMkernel adapters.
- Register compute managers with NSX-T.

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Navigate to **System > Quick Start**.
3. On the **Prepare Clusters for Networking and Security** card, click **Get Started**.
4. Select the clusters you want to prepare for NSX-T networking.
5. Click **Install NSX** and then select **Networking and Security**.

6 Depending on your requirement, you can prepare the same cluster for both VLAN and Overlay networking or for one type of networking. With Overlay networking, each host switch is added with a TEP IP address, which is required for overlay networking.



7 View the Host Switch Configuration switch to know the target switches where the physical NICs and VMkernel adapters (if any) will be migrated to.

This is the NSX-T recommended configuration. However, you can customize the settings for the cluster, even though it is an optional step.

Note A dotted line originating from a switch to a physical NIC indicates that it is an existing configuration on the host switch, which will be replaced by a firm line going to the same physical NIC.

8 Even though NSX-T provides recommendations, you can still customize the configuration. To customize a switch, select the switch, and change the recommended configuration.

a **Type**: Switch over the host switch type.

b **Transport Zone**: Select a different transport zone that you want the host to be associated with.

c **Uplink Profile**: If needed, select a different uplink profile in place of the recommended uplink profile.

Note If you configure two VDS switches with the same configuration, the wizard recommends the same uplink profile for both the switches.

d **Uplink to Physical NIC mapping**: On a VDS switch, all uplinks configured on the VDS switch are mapped to the uplinks in NSX-T. On an N-VDS switch, uplinks are mapped to vmnics.

A change to host switch type or uplink to vmnic mapping is reflected in the Host Switch Configuration network representation.

9 Click **Install**.

View the progress of installation on the **Prepare Clusters for Networking and Security** card. If installation on any of the host fails, retry installation by resolving the error.

10 To view successfully prepared hosts, navigate the UI based on the NSX-T Data Center version:

- (NSX-T Data Center 3.2.2 or later) **System > Fabric > Hosts** and select the **Cluster** tab.
- (NSX-T Data Center 3.2.1 or earlier) **System > Fabric > Nodes > Host Transport Nodes** and from the **Managed by** dropdown menu, select a vCenter Server.

Results

The transport nodes are ready for VLAN and Overlay networking.

Install Distributed Security for vSphere Distributed Switch

NSX-T Data Center allows you to install Distributed Security for vSphere Distributed Switch (VDS) without the need to deploy an NSX Virtual Distributed Switch (N-VDS). This ensures that DFW capabilities work on a VM whether it is managed by an NSX host switch or not.

Distributed Security provides security-related functionality to your VDS such as:

- Distributed Firewall (DFW)
- Distributed IDS/IPS
- Identity Firewall
- L7 App ID
- Fully Qualified Domain Name (FQDN) Filtering
- NSX Intelligence
- NSX Malware Prevention
- NSX Guest Introspection

Prerequisites

The following are the requirements for installing Distributed Security for VDS:

- vSphere 6.7 or later.
- The vSphere cluster should have at least one VDS with distributed switch version 6.6 or later configured.
- The vSphere cluster should not have N-VDS deployed.
- A compute manager must be registered in NSX-T. See Add a Compute Manager.

Procedure

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

2 Navigate to **System > Quick Start**.

3 On the **Prepare Clusters for Networking and Security** card, click **Get Started**.

4 Select the clusters that you want to install Distributed Security.

5 Click **Install NSX** and then select **Security Only**.

6 In the dialog box, click **Install**.

Note If the VDS spans across multiple clusters, Distributed Security installs only to the clusters that you selected.

The installation process for Distributed Security starts.

7 To view VDS with Distributed Security installed, navigate the UI based on the NSX-T Data Center version:

- (NSX-T Data Center 3.2.2 or later) **System > Fabric > Hosts** and select the **Cluster** tab.
- (NSX-T Data Center 3.2.1 or earlier) **System > Fabric > Nodes > Host Transport Nodes** and from the Managed by drop-down menu, select a vCenter Server.

Note vSphere clusters prepared for Distributed Security are identified by the **Security** label.

Results

Distributed Security is installed and you can begin using security capabilities such as creating DFW policies and rules for the VDS.

Deploy a Fully Collapsed vSphere Cluster NSX-T on Hosts Running N-VDS Switches

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.

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.
- Starting with NSX-T Data Center 3.1, the TEP of an NSX Edge VM can communicate directly with the TEP of the host on which the NSX Edge VM is running. Before NSX-T 3.1, the NSX Edge VM TEP had to be in a different VLAN than the host TEP.

Note Alternatively, you can deploy the configuration described in this topic by using vSphere Distributed Switches. With vSphere Distributed Switches configured on hosts, the procedure is simple. It does not involve vSphere Distributed Switch to N-VDS migration and NSX Manager deployment on NSX distributed virtual port groups. But, the NSX Edge VM must connect to a VLAN segment to be able to use the same VLAN as the ESXi host TEP.

- Starting with NSX-T Data Center 3.2.2, you can enable multiple NSX Managers to manage a single vCenter Server. See Multiple NSX Managers Managing a Single vCenter Server.

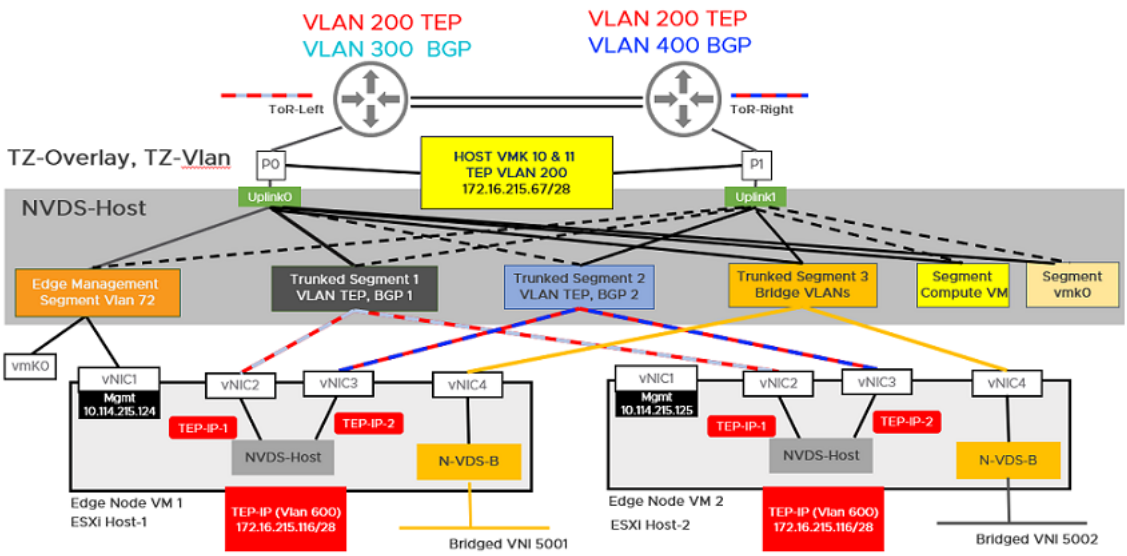
  After you configure a collapsed cluster, if you enable the vCenter Server to work with multiple NSX Managers (multiple NSX Managers are registered to the same vCenter Server), you cannot deploy new NSX Manager nodes to the cluster. The workaround is to create a new cluster and deploy NSX Manager nodes.

  Note 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 has:

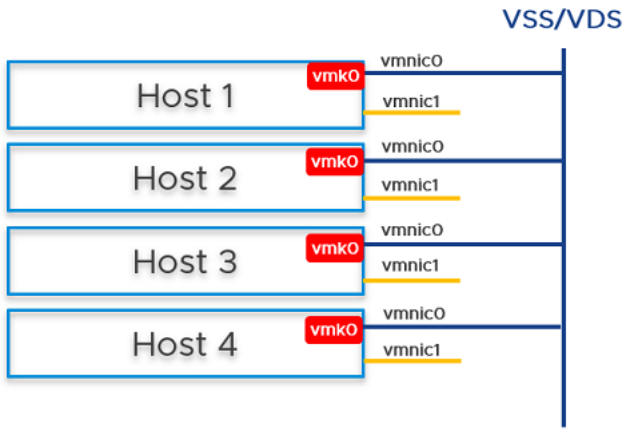
  - vSAN configured with the hosts in the cluster.
  - A minimum of two physical NICs per host.
  - vMotion and Management VMkernel interfaces.

  Figure 10-1. Topology: Single N-VDS Switch Managing Host Communication with NSX Edge and Guest VMs

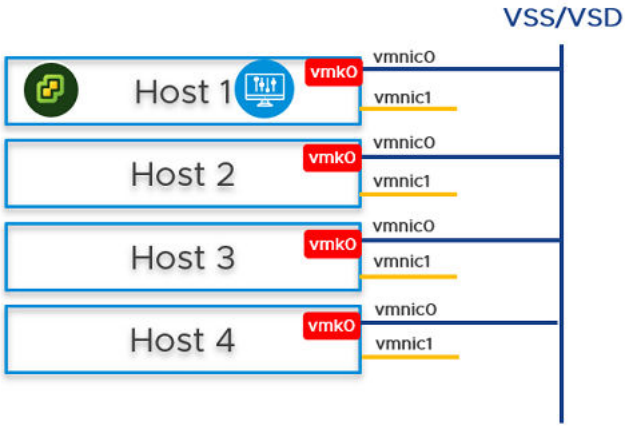


Procedure

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.

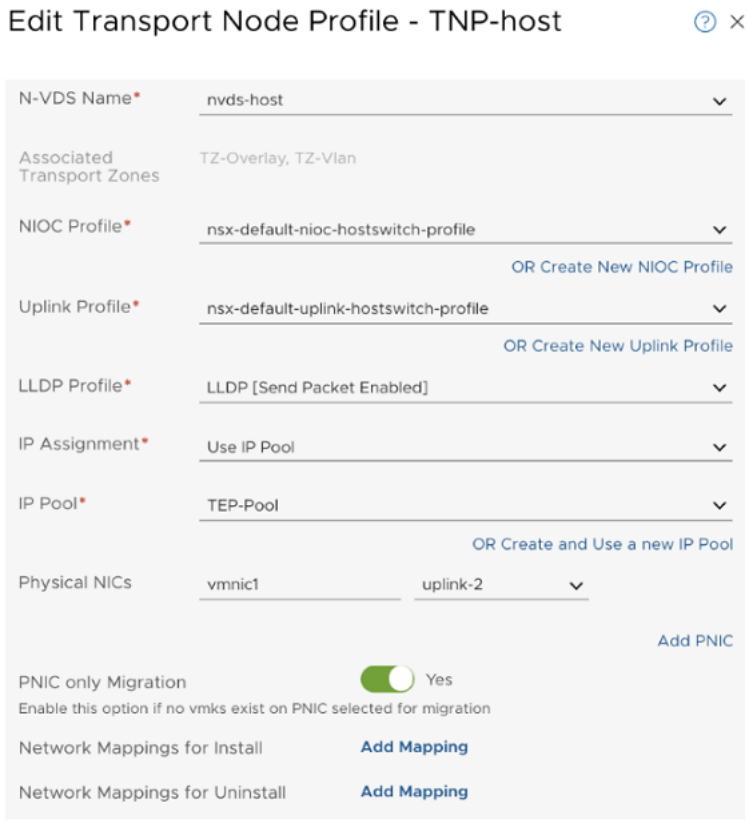
a Create VLAN transport zone and overlay transport zone with a named teaming policy. See Create Transport Zones.

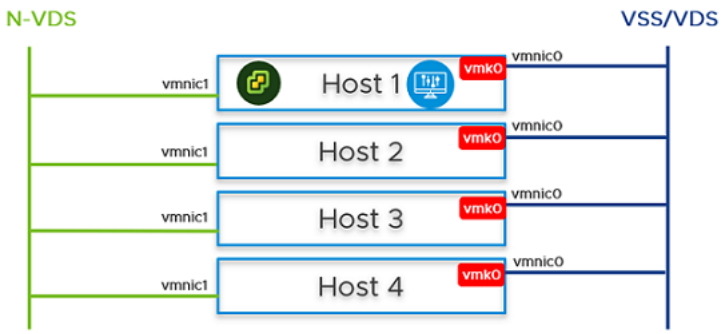
b Create an IP pool or DHCP for tunnel endpoint IP addresses for the hosts. See Create an IP Pool for Tunnel Endpoint IP Addresses.

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.





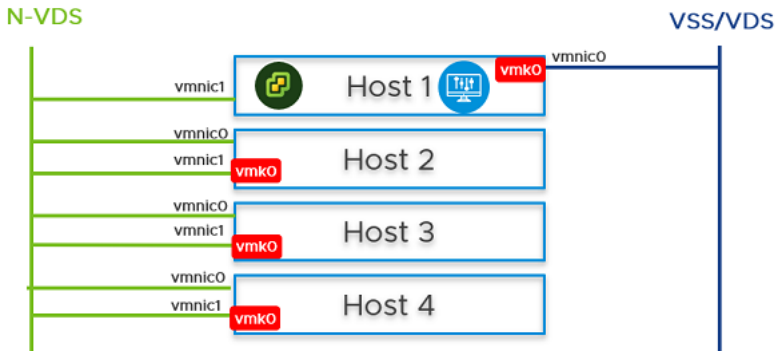
vmnic1 on all hosts are added to the N-VDS switch. So, out of the two physical NICs, one is migrated to the N-VDS switch. The vmnic0 interface is still connected to the vSS or vDS switch, which ensures connectivity to the host is available.

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** .

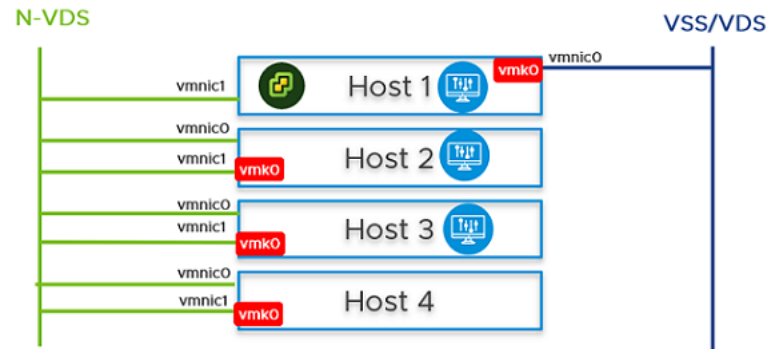
- vmnic0 is mapped to an active uplink, **uplink-1** .



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.

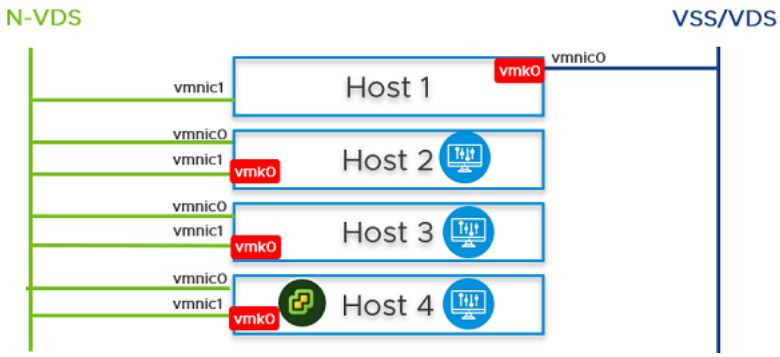
8 On Host 2 and Host 3, from the NSX Manager UI, install NSX Manager and attach NSX Manager to the segment. Wait for approximately 10 minutes for the cluster to form and verify that the cluster has formed.



9 Power off the first NSX Manager node. Wait for approximately 10 minutes.

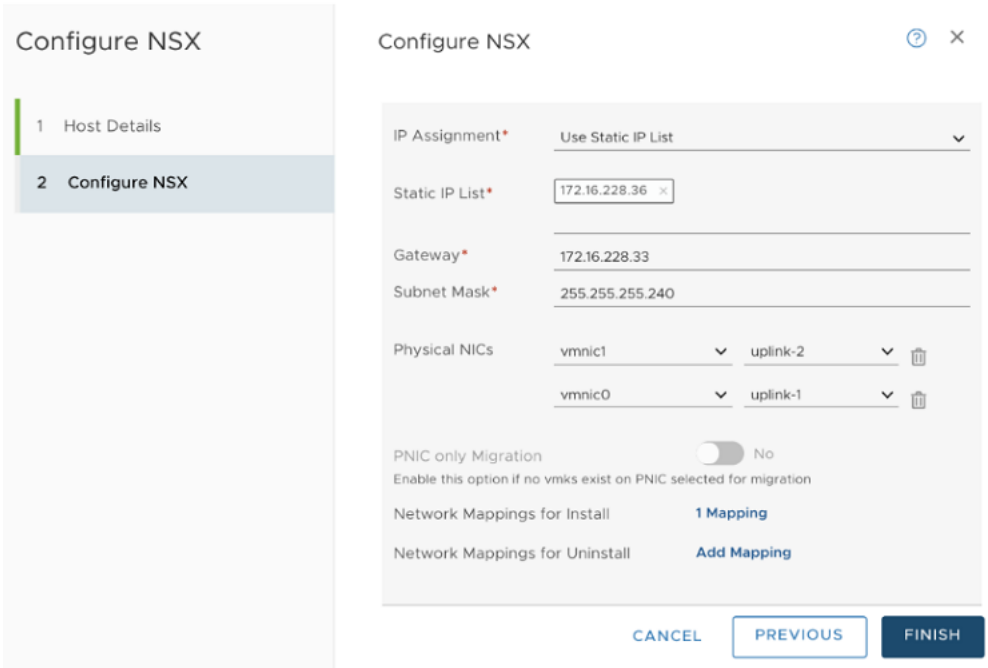
10 Reattach the NSX Manager and vCenter Server to the previously created logical switch. On host 4, power on the NSX Manager. Wait for approximately 10 minutes to verify that the cluster is in a stable state. With the first NSX Manager powered off, perform cold vMotion to migrate the NSX Manager and vCenter Server from host 1 to host 4.

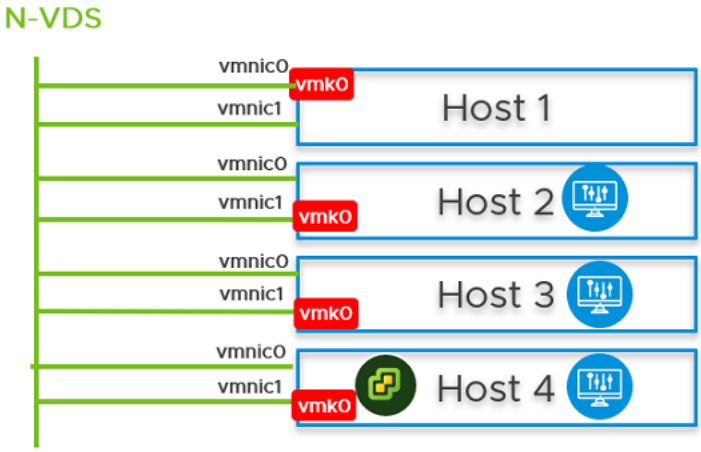
For vMotion limitations, see https://kb.vmware.com/s/article/56991.



11 From the NSX Manager UI, go to Host 1, migrate vmk0 and vmnic0 together from VSS to N-VDS switch.

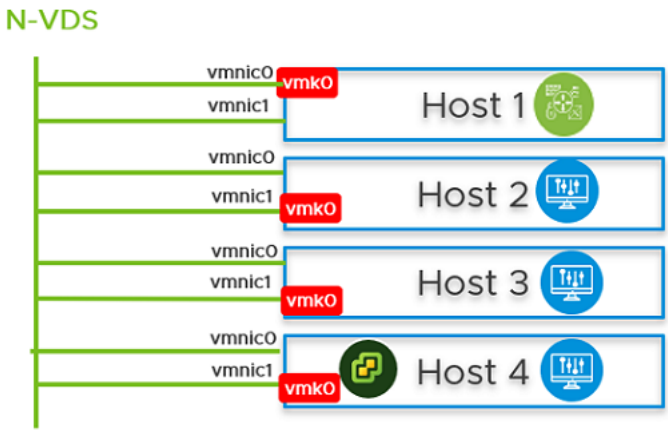
12 In the **Network Mapping for Install** field, ensure that the vmk0 adapter is mapped to the **Edge Management Segment** on the N-VDS switch.





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
```

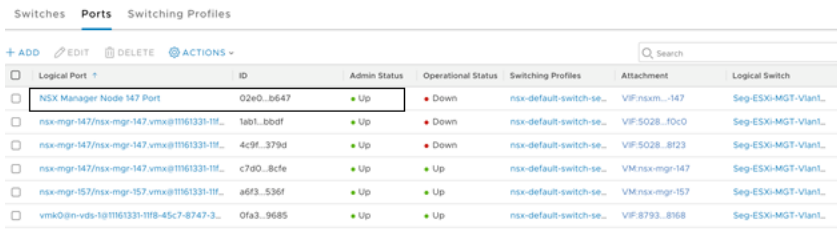
```
curl -X POST -k -u '<username>:<password>' -H 'Content-Type:application/json'
-d @port3.json https://nsxmgr/api/v1/logical-ports
```

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.



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

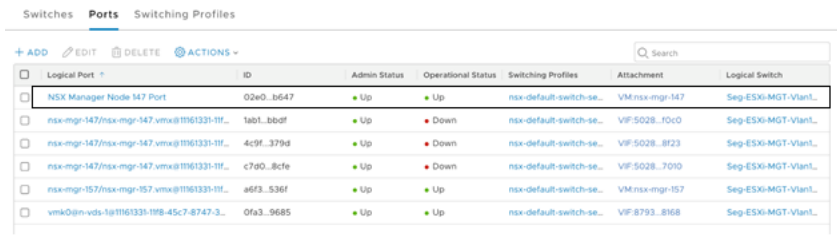
The API command to migrate NSX Manager to the newly created unblocked port is:

```
/api/v1/transport-nodes/<TN-ID>?vnic=<VNIC-
ID>&vnic_migration_dest=<VIF-ID>
```

For example,

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -k -X
PUT -u 'admin:VMware1!VMware1!' -H 'Content-
Type:application/json' -d @<tn1>.json 'https://localhost/api/v1/
transport-nodes/11161331-11f8-45c7-8747-34e7218b687f?vnic=5028d756-
d36f-719e-3db5-7ae24aa1d6f3:4000&vnic_migration_dest=nsxmgr-port-147'
```

i Ensure that the statically created logical port is `Up`.



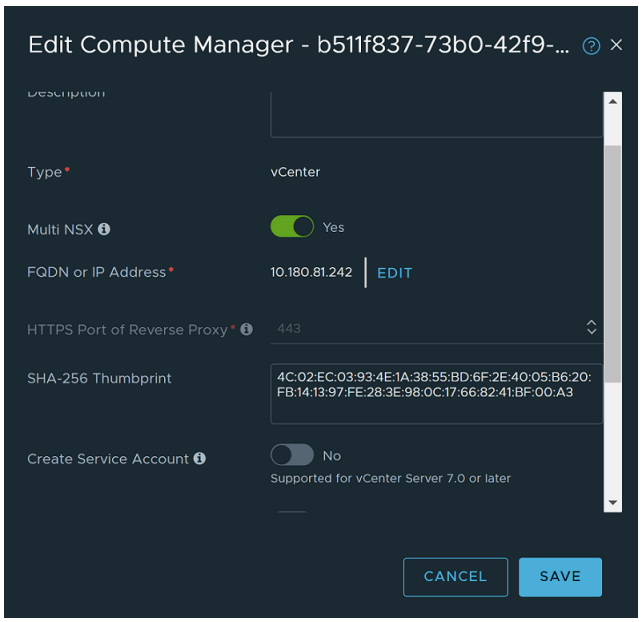
j Repeat the preceding steps on every NSX Manager in the cluster.

Multiple NSX Managers Managing a Single vCenter Server

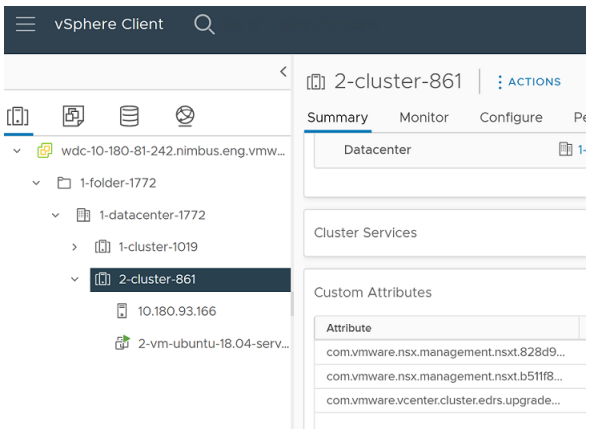
Improve the operational efficiency with multiple NSX Managers managing a single vCenter Server. Admins can manage different clusters in the same vCenter Server by using different NSX Managers.

Starting with NSX-T Data Center 3.2.2, you can enable support of multiple NSX Managers managing a single vCenter Server.

For more details on how the **Multi NSX** flag is enabled in vCenter Server, see Add a Compute Manager.

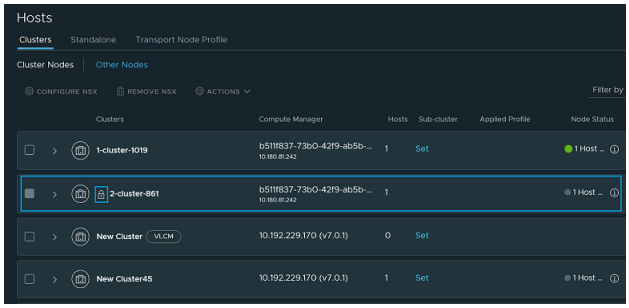


After you prepare a cluster or a host as a transport node, NSX-T appends the cluster, hosts and DVS extensions with a key that indicates these objects are managed by a certain vCenter Server.



NSX-T changes the old extension (`com.vmware.nsx.management.nsxt`) to a custom extension key (`com.vmware.nsx.management.nsxt.<computemanager-id>`), where the `<computemanager-id>` is the vCenter Server ID in NSX-T.

On the **Hosts** → **Clusters** page, NSX-T discovers all clusters managed by the same vCenter Server, where a different NSX Manager can manage its own clusters. If another NSX Manager owns a cluster, you cannot prepare or edit it. These clusters are in read-only mode.



Switching between Single NSX-T Mode to Mulitple NSX-T Mode

When you enable **Multi NSX** flag on the vCenter Server, NSX-T appends its managed objects of NSX-T (cluster, host, Distributed Virtual Switch switch) with the custom extension (`com.vmware.nsx.management.nsxt.<computemanager-id>`).

In Mulitple NSX-T Mode, all NSX Managers registered to the same vCenter Server must have **Multi NSX** flag enabled. You cannot configure **Multi NSX** enabled for NSX Manager-1 and deactivate on NSX Manager-2.

Host Movement Scenarios

Scenario	Action/Result
■ Prepare Cluster-1 using TNP of NSX-T-1. ■ Prepare Cluster-2 using TNP of NSX-T-2. ■ In vCenter Server UI, move one host from Cluster-1 to Cluster-2. ■ On the host that is moved to cluster-2, NSX-T-1 uninstalls NSX-T vibs from the host. NSX Manager-1 removes its ownership from the host. Only after NSX Manager-1 removes its ownership and the Lock icon disappears from the Host Transport Node page does NSX Manager-2 start installation on the host.	■ NSX-T is uninstalled on the host that is moved to Cluster-2. After the host is moved, the host will be prepared by the TNP of NSX-T-2, which is attached to Cluster-2. ■ If there are any uninstallation-related errors, check the **Host** → **Clusters** page. Click **Resolve** to fix issues and proceed.

■ Host-1 is prepared individually as a transport node in any of the following environments where:
  ■ It is not part of a vCenter Server.
  ■ It is part of a vCenter Server but TNP is detached from the cluster.
  ■ It is part of the datacenter in a vCenter Server.
	■ Before moving Host-1 to a NSX-T-managed cluster do the following:
	  ■ Uninstall NSX-T from Host-1 transport node.
	  ■ Add Host-1 to a vCenter Server-managed cluster.
	  ■ TNP is automatically applied to Host-1 and NSX-T is installed.

Limitations of Multiple NSX Managers Managing a Single vCenter Server Setup

- If NSX Manager-1 has stamped its ownership on managed objects (cluster, host, or Distributed Virtual Switch (DVS)), these objects cannot be owned by NSX Manager-2 until the first manager gives up the ownership or ownership is forcefully passed on to another manager. See <xref-topic>.

- Even though you can enable **Multi NSX** on a vCenter Server, where the version is NSX-T 3.2.2, do not register the same vCenter Server with NSX-T 3.2.1 or any previous release.
- Ensure the desired user roles have permissions to update `Global.ManageCustomFields` in vCenter Server. The NSX-T Custom Attribute must not be appended on any of the managed objects. It can lead to disruption of the setup.
- With **Multi NSX** enabled on a vCenter Server, you cannot enable Kubernetes cluster or vLCM cluster to work on the same vCenter Server.
- If you deactivate **Multi NSX** on a vCenter Server, you cannot use the same vCenter Server to register with another NSX-T instance.
- If any custom or legacy vCenter Server extension is not deleted from vCenter Server for reason such as failure of NSX to come up, you will have to manually delete extension from vCenter Server.
- Does not support collapsed cluster environments (where management and workloads are deployed on the same transport node). With Multi NSX flag enabled in a collapsed cluster environment, you cannot deploy new NSX Manager nodes. The workaround is to create a new cluster and deploy NSX Manager nodes.

Troubleshoot Multi-NSX Issues

Troubleshoot issues related to Multi-NSX environments. In a Multi-NSX environment, more than one NSX Manager is registered to a single vCenter Server.

Cannot Enable Multiple NSX-T on Single vCenter Server

If an old NSX-T extension exists in vCenter Server, you cannot enable multiple NSX-T on the vCenter Server as NSX-T is already registered.

Problem

Old extension still exists in vCenter Server.

Cause

You registered NSX-T without enabling **Multi NSX** in vCenter Server and deleted NSX Manager without unregistering the vCenter Server.

Solution

1. Log in to https://<vCenter-Server-IP>/mob/?mob=ExtensionManager.
2. On the ExtensionManager page, go to method "unregisterExtension".
3. Add old extension "`come.vmware.nsx.management.nsxt`" and click **Invoke** method.

Override NSX-T Ownership Constraints

When a transport node profile (TNP) is applied to a cluster if any validations (VMs are running on hosts) fail then Transport Node is not created. After ensuring validations pass, you can reapply cluster configuration using API. However, if you want the node to give up ownership of its managed objects you can call the `override_nsx_ownership` parameter in the API call.

You must only override ownership of managed objects from a NSX-T instance if any one of the following condition is true:

- NSX-T instance is not responding or unusable
- NSX-T is no longer actively managing its objects

Caution If the managed objects affected by this operation are actively used by the NSX-T that owns these objects, then it could corrupt host switch configurations that are pushed down by the NSX-T instance.

Prerequisites

Procedure

- Call the following API to override NSX-T ownership constraints.

  ```
  POST https://<nsx-
  mgr>/api/v1/fabric/discovered-nodes/5c669dc6-47a8-4508-3077-6a48f26c5a4g?
  action=reapply_cluster_config&override_nsx_ownership=true
  ```

  Where, `override_nsx_ownership=true` when set to True overrides NSX-T ownership of managed objects.

  However, it is not recommended to pass this parameter. If you use this parameter it indicates you want to own certain managed objects owned by another NSX instance.

```
{
  "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"
          }
```

```
        ],
        "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"
        },
        "vmknics": [
          {
            "device_name": "vmk1",
            "logical_switch_id": "849e339e-64b7-47cb-9480-33068f70dc5a"
          }
        ]
      }
    ]
  },
  "transport_zone_endpoints": [
    {
      "transport_zone_id": "e14c6b8a-9edd-489f-b624-f9ef12afbd8f",
      "transport_zone_profile_ids": []
    }
  ],
  "node_id": "41a4eebd-d6b9-11e6-b722-875041b9955d",
  "node_deployment_info": {
    "resource_type": "HostNode",
    "id": "41a4eebd-d6b9-11e6-b722-875041b9955d",
    "display_name": "FN1",
    "fqdn": "sc2-rdops-vm03-dhcp-110-133.eng.vmware.com",
    "ip_addresses": [
      "10.192.156.199"
    ],
    "external_id": "a5113680-6a56-4386-9017-adffbe56c99e",
    "discovered_ip_addresses": [],
    "os_type": "ESXI",
    "os_version": "",
    "managed_by_server": "",
    "_create_time": 1538632396987,
    "_last_modified_user": "admin",
    "_protection": "NOT_PROTECTED",
    "_last_modified_time": 1538632396987,
    "_create_user": "admin",
    "_revision": 0
  },
  "_create_time": 1485299990773,
  "_last_modified_user": "admin",
  "_last_modified_time": 1485301913130,
  "_create_user": "admin",
  "_revision": 0
}
```

NSX-T no longer owns managed objects. These objects can be now owned by another NSX-T instance.

Preparing Standalone Host Cluster Results in Failure

Preparing a standlone host cluster for NSX-T 3.2.2 results in failure.

Problem

In this scenario, there are two NSX-T deployments connected to same vCenter Server in NSX-T 3.1.x. The vCenter Server is registered with NSX-T-1 as compute manager and NSX-T-2 is using standalone cluster registered to the same vCenter Server.

You upgrade NSX-T-1 to v3.2.2, then enable multi-NSX flag on the vCenter Server. However, you do not upgrade the NSX-T-2 which remains on 3.1.x. Since NSX-T-1 is enabled with multi-NSX, the NSX Manager UI lists the standalone cluster of NSX-T-2 as an unprepared cluster.

If you try to prepare the standalone NSX-T-2 cluster from NSX-T-1, the standalone host goes into failure state.

Cause

NSX-T-2 hosts go into failure state because it is running NSX-T v3.1.x.

Solution

1. Log in to https://<vCenter-Server-IP>.
2. Migrate all VMs from that host to the other hosts using vCenter Server.
3. Remove NSX from both managers using below API:

   ```
   DELETE https://<NSX Manager-IP>/api/v1/transport-nodes/<transportnode-id>?force=true&unprepare_host=false
   ```

4. Configure NSX-T on the desired NSX Manager.

Traffic Performance Issues Related to NSX Edge VMs in Multiple NSX-T Data Center Environment

In a multiple NSX-T Data Center environment, only the NSX Manager which deployed NSX Edge VM can use it for routing and Inter TEP communication. None of the other NSX Managers registered to the same vCenter Server can use it for routing and Inter TEP communication. The other NSX Manager instances consider the NSX Edge VM as a regular VM. This scenario can cause traffic performance issues on the NSX Edge VM.

Problem

In a multiple NSX-T Data Center scenario, you have the following configuration:

- NSX Manager-1 and NSX Manager-2 are registered to the same vCenter Server (compute manager).
- NSX Manager-1 deployed the NSX Edge VM.

- NSX Manager-2 prepared the ESXi host.
- From vSphere Web Client, you perform vMotion of NSX Edge VM to an ESXi host prepared by NSX Manager-2. NSX Manager-2 did not deploy the NSX Edge VM.
- NSX Manager-1 does not recognize NSX Edge as an inventory VM. So, NSX Manager-1 does not apply any DFW rules on it.

After moving the NSX Edge VM to the new ESXi host:

- NSX Manager-2 categorizes NSX Edge as a regular VM and not as an NSX Edge VM. If there are any DFW rules configured, NSX Manager-2 applies any DFW rules on the NSX Edge VM.

  See a sample output,

```
https://<NSX Manager-2>/api/v1/fabric/virtual-machines
{
            “host_id”: “59ac4c38-56b1-4b82-a131-dd9ad119f53d”,
            “source”: {
                “target_id”: “59ac4c38-56b1-4b82-a131-dd9ad119f53d”,
                “target_display_name”: “10.172.17.133”,
                “target_type”: “HostNode”,
                “is_valid”: true
            },
           …..
            “type”: “REGULAR”,
            “guest_info”: {
                “os_name”: “Ubuntu Linux (64-bit)“,
                “computer_name”: “vm”
            },
            “resource_type”: “VirtualMachine”,
            “display_name”: “mgr2_edge1",
            “_last_sync_time”: 1663802733277
        },
```

Cause

As NSX Manager-2 exclude list does not filter out NSX Edge VM, it is considered as a regular VM and not as a NSX Edge VM. So, DFW rules or any third-party firewall rules configured for workloads are applied to the NSX Edge VM too. This scenario might cause traffic disruption.

Solution

1. Log in to the vCenter Server, https://*vCenter-Server-IP*.
2. As NSX Manager-2 considers the NSX Edge VM as a regular VM, create an NS Group "Edge-VMs-From-Other-Managers" and add the Edge VMs to the NS Group.

3 To identify Edge VMs from NSX Manager-1 that must be added to Exclude lists on NSX Manager-2, follow these steps:

   a Use `display_name` that you get after call the following API, `https://<NSX Manager-1>/api/v1/transport-nodes?node_types=EdgeNode`.

   b Match the name with the `display_name` in API response from NSX Manager-2, `https://<NSX Manager-2>/api/v1/fabric/virtual-machines`.

4 Add NS Group "Edge-VMs-From-Other-Managers" to the DFW Exclusion List and SI Exclusion Lists on NSX Manager-2.

5 Verify and exclude NSX Edge VM from third party firewalls.

6 If Edge VM Id changes, update the NS Group.

7 Before you delete the Edge VM, remove the entry from the Exclude lists.

Note Inter TEP communication on the NSX Edge VM is not supported on NSX Manager-2.

Managing Transport Nodes

After preparing hosts as transport nodes, you can view status of hosts, switch visualization, and other configuration settings related to transport nodes. You can use it to debug issues if the host transport node is in a degraded or failed state.

Switch Visualization

You get a granular view of N-VDS or vSphere Distributed Switch at an individual host level.

Procedure

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

2 Navigate the UI based on the NSX-T Data Center version and select a host:

   - (NSX-T Data Center 3.2.2 or later) **System > Fabric > Hosts** and select the **Cluster** tab.
   - (NSX-T Data Center 3.2.1 or earlier) **System > Fabric > Nodes > Host Transport Nodes**

     and from the Managed by dropdown menu, select **Standalone Hosts** or a vCenter Server.

3 Select the host.

4 Click the **Switch Visualization** tab to view the uplinks configured on the switch and physical NICs that are connected to uplinks.

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.

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. Navigate the UI based on the NSX-T Data Center version and select a host:
   - (NSX-T Data Center 3.2.2 or later) **System > Fabric > Hosts** and select the **Cluster** tab.
   - (NSX-T Data Center 3.2.1 or earlier) **System > Fabric > Nodes > Host Transport Nodes** and from the Managed by dropdown menu, select a vCenter Server.
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.

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 the UI based on the NSX-T Data Center version and select a host:
   - (NSX-T Data Center 3.2.2 or later) **System > Fabric > Hosts** and select the **Cluster** tab.
   - (NSX-T Data Center 3.2.1 or earlier) **System > Fabric > Nodes > Host Transport Nodes** and from the Managed by dropdown menu, select a vCenter Server.
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 troubleshoot the issue.

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"
}
```

Installing NSX Edge

11

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

Read the following topics next:

- 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
- Remove NSX Edge Nodes from an Edge Cluster

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 11-1. 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.
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.

Table 11-1. NSX Edge Deployment, Platforms, and Installation Requirements (continued)

Requirements	Description
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.

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 any of the local users, the name must be unique. If you specify the same name, it is ignored and the default names (for example, **`admin`** or **`audit`**) are used.

- If the password for the **root** or **admin** user does not meet the complexity requirements, you must log in to NSX Edge through SSH or at the console as **root** with password **vmware** and **admin** with password **default**. You are prompted to change the password.
- If the password for other local users (for example, **audit**) 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 local_user_name** to set the local user's password (the current password is an empty string). You can also reset passwords in the UI using System > User Management > Local Users.

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.

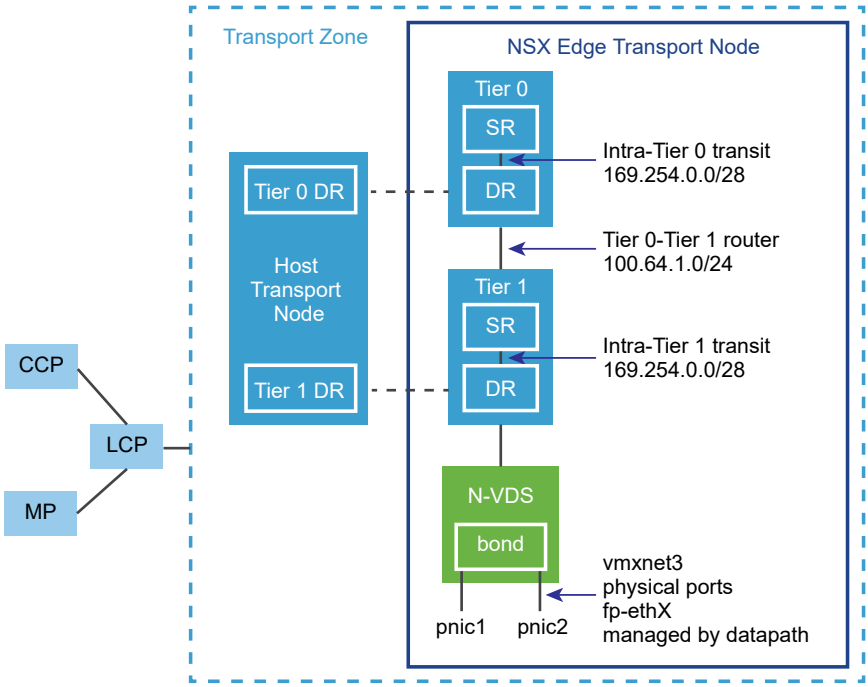
NSX Edge Networking Setup

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 11-1. 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 100.64.0.0/16. Each tier-0-to-tier-1 peer connection is provided a /31 subnet within the 100.64.0.0/16 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 100.64.0.0/16 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 /api/v1/transport-nodes/{transport-node-id}/node/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.

Figure 11-2. NSX Edge Transport Node in VM Form Factor within ESXi

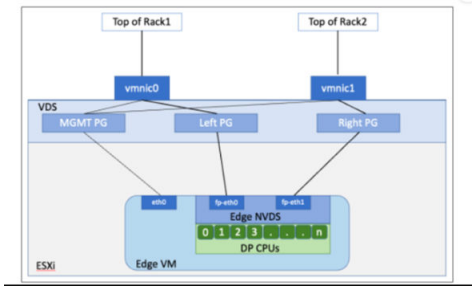
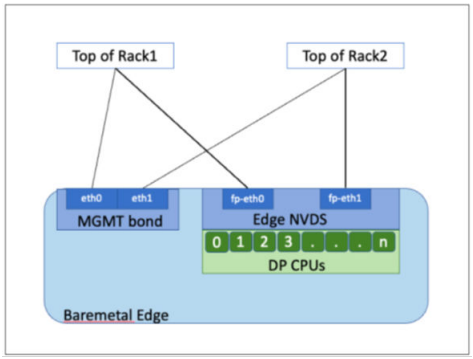


Figure 11-3. Bare Metal Edge Transport Node



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

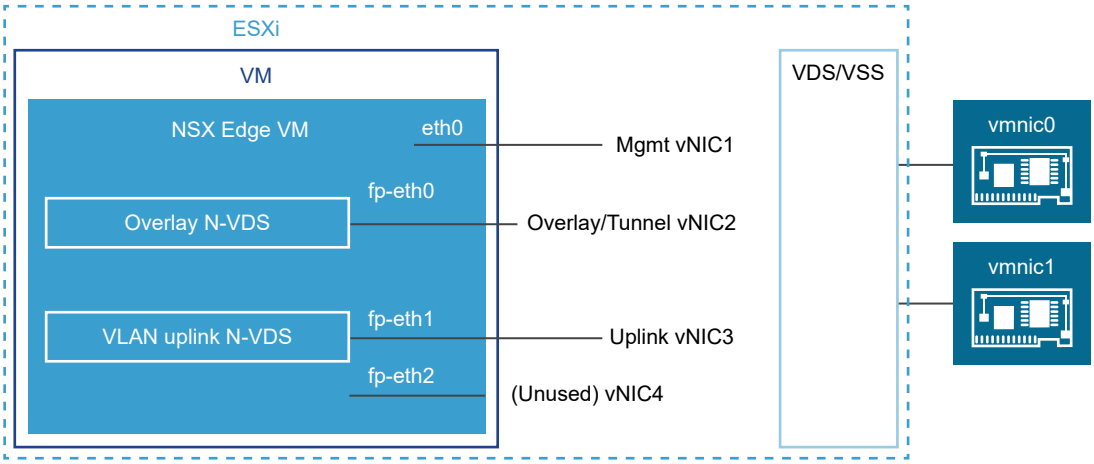
When you install NSX Edge as a virtual appliance or VM, internal interfaces are created, called fp-ethX, where X is 0, 1, 2, and 3. These interfaces are allocated for uplinks to a top-of-rack (ToR) switches and for NSX-T Data Center overlay tunneling.

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.

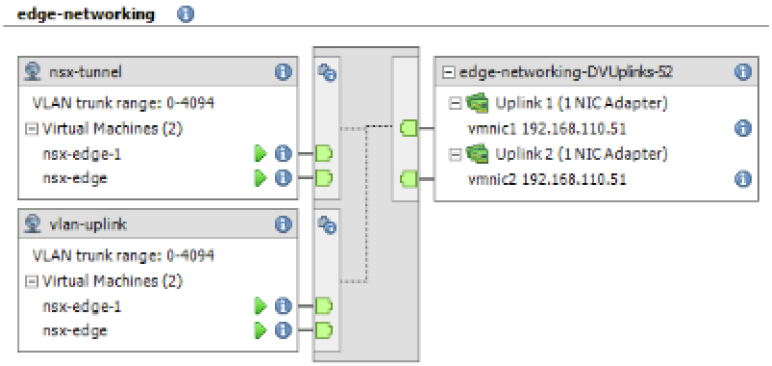
Figure 11-4. One Suggested Link Setup for NSX Edge VM Networking



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.

Figure 11-5. Edge Networking in vSphere



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 can be in the same VLAN or subnet.

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.

Note If NSX Edge VM uplinks (management, fast-path interfaces) will be connecting to VLAN based portgroups then underlying ESXi host does not need to be an NSX transport node. But if NSX Edge VM uplinks will be connecting to NSX VLAN segments (logical switches), then you must configure ESXi hosts hosting the edges as transport nodes.

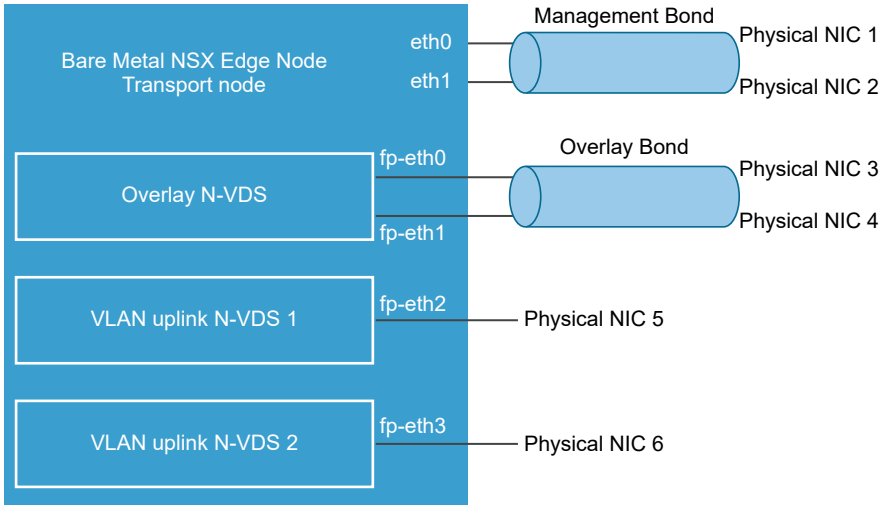
Bare-Metal NSX Edge Networking

The bare-metal NSX Edge contains internal interfaces called fp-ethX, where X is up to 16 interfaces. 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 11-6. One Suggested Link Setup for Bare-Metal NSX Edge Networking



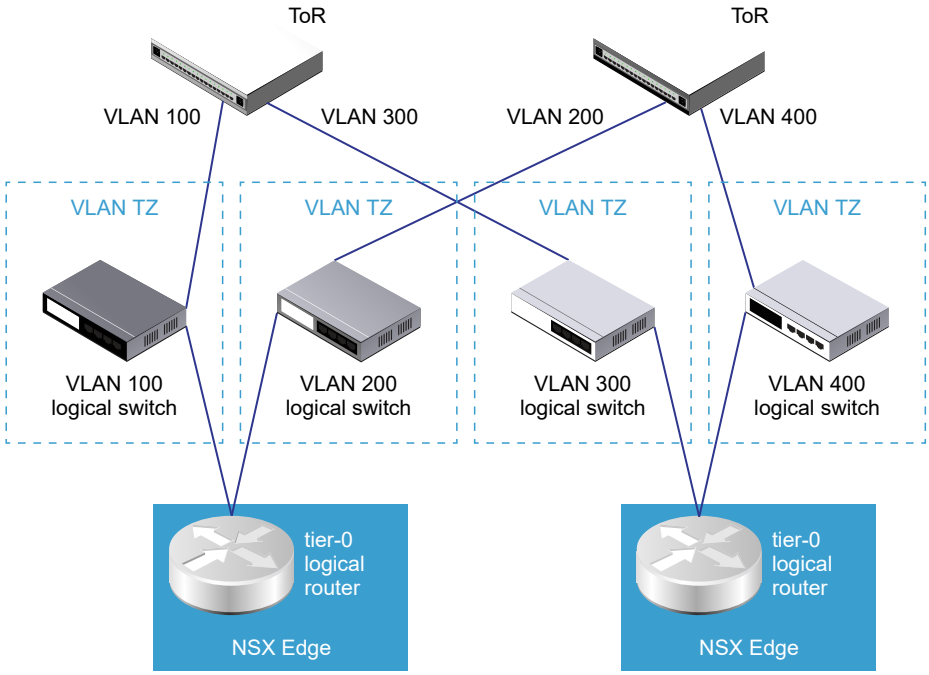
NSX Edge Uplink Redundancy

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 11-7. 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:

- On a vDS switch running version prior (<) to 6.6, enable promiscuous mode for the port connected to NSX Edge VM virtual NIC that provides VLAN connectivity. These settings are needed to support bridging or L2VPN and DHCP functionality for VLAN networks.
- On a vDS switch running version equal to or greater than (>=) 6.6, enable mac learning and disable promiscuous mode. These settings ensure that packets are received at the destination where destination mac address does not match the virtual NIC effective MAC address. These settings also ensure packets are received at destinations that are on an NSX-T Data Center Segment. These settings are needed to support bridging or L2VPN and DHCP functionality for VLAN networks.
- Enable forged transmit on the vDS switch. Forged transmit enables sending packets with source mac address not matching the virtual NIC effective MAC addresses. These settings are needed to support bridging or L2VPN and DHCP functionality for VLAN networks.

NSX Edge Installation Methods

Install NSX Edge on an ESXi host using NSX Manager UI (recommended method), vSphere Web Client (from UI or vSphere command-line OVF tool) or as physical severs.

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 Edge 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.

Physical server (Automated or Interactive mode using ISO file) or NSX Edge VM appliance	Install NSX Edge using ISO file using PXE on physical servers. 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 a PXE Server for NSX Edge . Choose from one of the supported installation methods:
	  ■ (Automated installation) Install NSX Edge using ISO File on physical servers. See Install NSX Edge Automatically via ISO File.
	  ■ (Automated installation) Install NSX Edge using ISO File as a Virtual Appliance. See Install NSX Edge via ISO File as a Virtual Appliance.
	  ■ (Manual installation) Manually Install NSX Edge using 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 Center data plane. It runs an instance of the NSX-T Data Center 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. Each cluster is 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.
- Prepare uplinks. For example, distributed port groups as trunk in vCenter Server or NSX Segments in NSX-T Data Center.
- If the NSX Edge Bare Metal server is running version 6.7u3 or earlier, do not upgrade the NSX Edge `virtualHW.version` to **14** or higher in vCenter Server. By default, the `virtualHW.version` is set to **13**.

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 Node**.
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.

Note After deploying the NSX Edge node, you cannot change the SSH setting for a root user that you set during deployment. For example, you cannot enable SSH for a root user if you disabled it during deployment.

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	From the drop-down menu, select the interface that connects to the NSX Edge management network. This interface 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. The NSX Edge management interface is connected to distributed port groups or segments.
Search Domain Names	Enter domain names in the format 'example.com'.

Option	Description
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	Enter a name for the switch.
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 prerequisites are met: ■ TEP configuration must be done on one N-VDS only. ■ All TEPs must use the same transport VLAN for overlay traffic. ■ All TEP IPs must be in the same subnet and use the 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.

Option	Description

IP Assignment (TEP)	IP address is assigned to the NSX Edge switch that is configured. It is used as the tunnel endpoint of the NSX Edge.
	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.
	  ■ Gateway: Enter the default gateway of the TEP, which is used to route packets another TEP in another network. For eample, ESXi TEP is in 20.20.20.0/24 and NSX Edge TEPs are in 10.10.10.0/24 then we use the default gateway to route packets between these networks.
	  ■ Subnet mask: Enter the subnet mask of the TEP network used on the NSX Edge.
	■ If you selected **Use IP Pool** for IP assignment, specify the IP pool name.

DPDK Fastpath Interfaces / Virtual NICs	Select the data path interface that is either a distributed port group trunk or a segment as the uplink interface. **Note** If the uplink profile applied to the NSX 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 corresponding physical network interfaces on the Edge VM for traffic to flow through a logical switch that uses the Named Teaming policies. Starting with NSX Data Center 3.2.1, you can configure a maximum of four unique data path interfaces as uplinks on an NSX Edge VM. When mapping uplinks to DPDK Fastpath Interfaces, if NSX Edge does not display all the available interfaces (four in total), it means that either the additional interface is not yet added to the NSX Edge VM or the uplink profile has fewer number of uplinks. For NSX Edge VMs upgraded from an earlier version of NSX-T Data Center to 3.2.1 or later, invoke the redeploy API call to redeploy the NSX Edge VM. Invoking the redeploy API ensures the NSX Edge VM deployed recognizes all the available datapath interfaces in NSX Manager UI. Make sure the Uplink profile is correctly configured to use additional datapath NIC. ■ For autodeployed NSX Edges, call the redeploy API. `POST api/v1/transport-nodes/<transport-node-id>?action=redeploy` ■ For manually deployed edges, deploy a new NSX Edge VM. Ensure all the vmx customizations of the old NSX Edge VM are also done for the new NSX Edge VM. Performing vMotion on a NSX Edge VM might result in the NSX Edge VM going into failed state or the additional network adapter cannot be enabled because of memory buffer issues. For troubleshooting memory-related issues when performing a vMotion on a NSX Edge VM, see https://kb.vmware.com/s/article/76387.

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 After an NSX Edge node is migrated to a new host using vCenter Server, you might find NSX Manager UI reporting stale configuration details (Compute, Datastore, Network, SSH, NTP, DNS, Search Domains) of the NSX Edge. To get the latest configuration details of NSX Edge on the new host, run the API command.

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

15 (Optional) You can change the IP address of the NSX Edge node from the command line interface. At the CLI terminal, run `set interface eth0 ip <Gateway_IPaddress> gateway <NSXEdge_IPaddress> plane mgmt`. For example, `set interface eth0 ip 192.168.110.42/24 gateway 192.168.110.1 plane mgmt`.

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 Edge Clusters**.
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 , 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 Manager VM and Host Transport Node 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 node 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 node 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.

  Note An NSX Manager thumbprint is required to join an NSX Edge node to an NSX Manager. To retrieve thumbprint on an NSX Manager node, run `get certificate api 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 node 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 node 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 configure an autonomous NSX Edge node.

17 Enter the hostname of the NSX Edge.

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

Skip any VMC network settings.

19 Enter the DNS Server list, the Domain Search list, and the NTP Server IP or FQDN 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 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 starts, log in to the CLI with admin credentials.

Note After NSX Edge node 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.

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 nodes 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 node 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 has the required connectivity.

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

- You can ping your NSX Edge node management interface.
- From the NSX Edge node, you can ping the node's default gateway.

- From the NSX Edge node, you can ping the hypervisor hosts that are either in the same network or a network reachable through routing.
- From the NSX Edge node, you can ping the DNS server and NTP Server IP or FQDN list.

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 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 to the NSX Edge 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.

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 or FQDN list for the NSX Manager or Cloud Service 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.
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

Field Name	OVF Parameter	Field Type
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 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 to track the boot process.
- After the NSX Edge node 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 nodes 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 has the required connectivity.

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

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

- 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 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 to the NSX Edge 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.

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 manually install NSX Edge 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 https://customerconnect.vmware.com and navigate to **Products and Accounts** → **Products** → **All Products**.
2. Search VMware NSX-T Data Center and select the appropriate product version.
3. Locate and download the ISO file for NSX Edge.
4. In the vSphere Client, select the host datastore.
5. 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.
6. In the vSphere Client inventory, select the host you uploaded the ISO file. or in the vSphere Client,
7. Right-click and select **New Virtual Machine** .
8. Select a compute resource for the NSX Edge appliance.

9 Select a datastore to store the NSX Edge appliance files.

10 Accept the default compatibility for your NSX Edge VM.

11 Select the supported ESXi operating systems for your NSX Edge VM.

12 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.

13 Power on the new NSX Edge VM.

14 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.

15 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 Manager VM and Host Transport Node System Requirements.

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

Note After NSX Edge node 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.

17 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`

18 (Optional) Start SSH service. Run `start service ssh`.

19 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 nodes 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.

20 (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.

21 Verify that the NSX Edge node has the required connectivity.

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

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

22 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 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 to the NSX Edge 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.

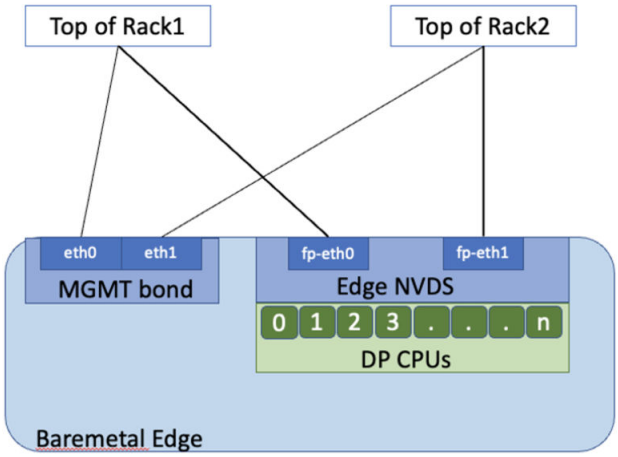
What to do next

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 installation of NSX Edge on a bare metal server or use ISO file to install NSX Edge on a bare metal server.

The NSX Edge bare metal node is a dedicated physical server that runs a special version NSX Edge software. The bare metal NSX Edge node requires a NIC supporting the Data Plane Development Kit (DPDK). VMware maintains a list of the compatibility with various vendor NICs. See the Bare Metal Server System Requirements.



The NSX Edge Bare Metal in the diagram is illustrated with single N-VDS with two datapath interfaces, and two dedicated NICs for management plane high availability.

The NSX Edge nodes in the diagram are illustrated with one NVDS, each with two datapath interfaces. Bare Metal NSX Edge nodes can be configured with more than 2 datapath interfaces depending on the number of NICs available on the server. Bare Metal NSX Edge nodes use pNICs as uplinks that directly connect to the top of rack switches. To provide high availability for bare metal edge management, configure two pNICs on the server as an active/standby Linux bond.

The CPUs on the edge will be assigned as either datapath (DP) CPUs that provide routing and stateful services or services CPUs that provide load balancing and VPN services.

For bare metal edge nodes, all the cores from the first node of a multi-NUMA node server will be assigned to NSX-T Data Center datapath. If the bare metal has only one NUMA node, then 50% of the cores will be assigned for the NSX-T Data Center datapath.

Important VMware does not support the sub-NUMA clustering, which is a server hardware feature, on a Bare Metal NSX Edge is not supported as it may result in a shortage of heap memory.

Bare Metal NSX Edge nodes support a maximum of two NUMA nodes. The sub-NUMA clustering functionality changes the socket of heap memory from two NUMA domains to four NUMA domains. This change limits the size of heap memory allocated to each socket and causes a shortage of heap memory that the datapath requires. You must disabled sub-NUMA functionlity in the BIOS. Any changes made to the BIOS will require a reboot.

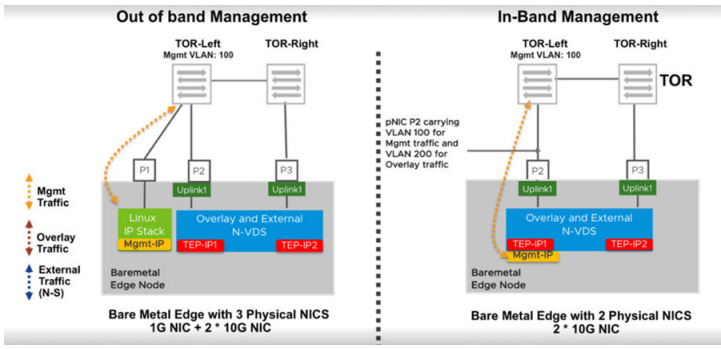
To check if the sub-NUMA functionality is enabled, log in to the bare metal NSX Edge as root and run `lscpu`. The output is captured in the support bundle. If there are more than two sockets per heap, it implies that the sub-NUMA functionality is enabled and it must be disabled.

Note

1 When configuring LACP LAG bonds on Bare Metal NSX Edge nodes, datapath cores (backing NICs) should belong to same NUMA node for load balancing to occur on both devices. If devices forming the bond span multipe NUMA nodes, then bond only uses network device CPU that is local NUMA node (0) to transmit packets. So, not all devices do not get used for balancing traffic that is sent out of the bond device.

   In this case, failover still works: if the device attached to the local NUMA node is down then the bond will send traffic to the other device even though it is not NUMA local.

   Run `get datapath` command to view the NUMA node associated with each datapath interface. To move nics associated with datapath to single NUMA node, physical reconfiguration of the server is required via the BIOS.



When a bare metal Edge node is installed, a dedicated interface is retained for management. This configuration is called out-of-band management. If redundancy is desired, two NICs can be used for management plane high availability. Bare metal Edge also supports in-band management where management traffic can leverage an interface being used for overlay or external (N-S) traffic as in the diagram.

Prerequisites

- Disable sub-NUMA clustering by editing the BIOS settings. NSX-T Data Center does not support sub-NUMA clustering. For more details, refer to the KB article, https://kb.vmware.com/s/article/91790.

Prepare a 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.

  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 service dataplane
set interface eth0 <ip-cidr-format> plane mgmt
start service 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 and configure required settings to set up the PXE server. For more details, see Linux documentation.
4. Install the Apache server and TFTP and other components required to configure the PXE server.
5. Copy or download the NSX Edge installer ISO file to a temporary folder.
6. 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/
```

7 (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, 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.

8 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=bionic netcfg/do_not_use_netplan=true --
```

9 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";
```

10 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 manually install NSX Edge nodes on bare metal using an ISO file. This includes configuring networking settings, such as IP address, gateway, network mask, NTP, and DNS.

Prerequisites

- Both BIOS and UEFI boot modes are supported.
- See NSX Edge network requirements in NSX Edge Installation Requirements.

Procedure

1 Go to https://customerconnect.vmware.com and navigate to **Products and Accounts** → **Products** → **All Products**.

2 Search VMware NSX-T Data Center and select the appropriate product version.

3 Locate and download the ISO file for NSX Edge for Bare Metal.

4 Log in to the out-of-band management interface (for example, Integrated Lights-Out (ILO) on HP servers) of the bare metal.

5 Before you begin installation, select the boot mode for the NSX Edge node.

   a Access the **System Setup** screen and select **System BIOS**.

   b On the **System BIOS Setting** screen, select **Boot Settings**.

   c On the **Boot Settings** screen, set **Boot Mode** to **BIOS** or **UEFI**.

   d Click **Back** and **Finish**.

6 Click **Launch** in the virtual console preview.

7 Select **Virtual Media > Connect Virtual Media**.

Wait a few seconds for the virtual media to connect.

8 Select **Virtual Media > Map CD/DVD** and browse to the ISO file.

9 Select **Next Boot > Virtual CD/DVD/ISO**.

10 Select **Power > Reset System (warm boot)**.

The installation duration depends on the bare metal environment.

11 Choose **Automated installation**.

There might be a pause of 10 seconds after you press Enter.

12 Select the applicable primary network interface. This is for the management network interface.

During power-on, the installer requests a network configuration. Select static IP settings. If the static IP is not avialable, use DHCP.

By default, the root login password is **vmware**, and the admin login password is **default**.

Note During deployment, the installer automatically selects the largest disk to install NSX-T Data Center on the NSX Edge node.

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

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

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

Note After NSX Edge node 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.

15 After the reboot, you can log in with either admin or root credentials. The default root password is **`vmware`**.

16 There are three ways to configure a management interface.

- Untagged interface. This interface type creates an out-of-band management interface.

  (Static) `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt`

  (DHCP) `set interface eth0 dhcp plane mgmt`

- Tagged interface.

  `set interface eth0 vlan <vlan_ID> plane mgmt`

  (Static) `set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`

  (DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

- In-band interface.

  `set interface mac <mac_address> vlan <vlan_ID> in-band plane mgmt`

  (Static) `set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`

  (DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

- Tagged interface and In-band interface.

  Any existing VLAN management interface must be cleared before creating a new one.

  `clear interface eth0.<vlan_ID>`

- (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. You can configure VLANs on a bond0 interface.

  Create a bond interface

  `set interface bond0 ip x.x.x.x/mask gateway x.x.x.x plane mgmt mode active-backup members eth0,eth1 primary eth0`

  Create vlan inteface on bond0

  `set interface bond0 vlan Y plane mgmt`

  Assign IP address to bond0.yyy

  `set interface bond0.yyy ip x.x.x.x/24 gateway z.z.z.z plane mgmt`

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 nodes 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 Set physical NICs to be used by NSX-T Data Center dataplane from the list of available PCI devices.

a `get dataplane device list`

b `reset dataplane device list`

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 Starting in NSX-T Data Center 3.1.2, you can claim up to 16 physical NICs.

Note To configure custom NICs for dataplance, run the `set dataplane device list <NIC1>, <NIC2>, <NIC3>` command.

19 To avoid network configuration errors, verify that the physical NICs selected match the NICs configured in the uplink profiles.

20 Verify that the NSX Edge node has the required connectivity.

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

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

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 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 to the NSX Edge 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.

Install NSX Edge Interactively via ISO File

Install NSX Edge devices on bare metal using an ISO file in the interactive mode.

Prerequisites

- Starting in NSX-T Data Center 3.2 both UEFI or Legacy BIOS modes are supported.
- See NSX Edge network requirements in NSX Edge Installation Requirements.

Procedure

1. Go to https://customerconnect.vmware.com and navigate to **Products and Accounts** → **Products** → **All Products**.
2. Search VMware NSX-T Data Center and select the appropriate product version.
3. Locate and download the ISO file for NSX Edge for Bare Metal.
4. Log in to the ILO of the bare metal.
5. Click **Launch** in the virtual console preview.
6. Select **Virtual Media > Connect Virtual Media**.

   Wait a few seconds for the virtual media to connect.
7. Select **Virtual Media > Map CD/DVD** and browse to the ISO file.
8. Select **Next Boot > Virtual CD/DVD/ISO**.
9. Select **Power > Reset System (warm boot)**.

   The installation duration depends on the bare metal environment.

10 Choose **Interactive Install**.

There might be a pause of 10 seconds after you press Enter. Starting with NSX-T Data Center 3.1.0, edit kernel boot aguments. The following steps are not needed if you are on NSX-T Data Center 3.1.1 and later.

a Press TAB to edit kernel boot arguments.

b Change the kernel boot arguments to:

```
/install/vmlinuz FRONTEND_BACKGROUND=original auto=true priority=high preseed/file=/
cdrom/preseed-interactive.cfg nomodeset initrd=/install/initrd.gz fb=false netcfg/
do_not_use_netplan=true -- quiet net.ifnames=0 biosdevname=0
```

c Press **Enter** to begin installation.

11 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.

12 Select English US as the language.

13 In the Configure the network window, select the applicable primary network interface.

14 Enter the host name that connects to the selected primary interface and click **Ok**.

During power-on, the installer requests a network configuration mode. Select static IP address and provide one. If static IP address is not available, select DHCP.

By default, the root login password is **vmware**, and the admin login password is **default**.

15 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.

16 Select a disk size that meets the system requirements.

17 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.

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

Note After NSX Edge node 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.

19 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 nodes 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.

20 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 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 to the NSX Edge 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.

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

To establish communication between NSX Edges and NSX Manager or NSX Manager cluster, join NSX Edges with NSX Manager. You only need to register NSX Edges with one NSX Manager to ensure communication with the management plane.

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. To retrieve the thumbprint of the NSX Manager appliance, at the NSX Manager appliance console, 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 Alternatively, to retrieve the thumbprint of the cluster, at the NSX Manager appliance console, run `get certificate cluster thumbprint`.

The output is a string of alphanumeric numbers that is unique to the cluster.

5 To join the NSX Edge node (VM or Bare Metal) to the NSX Manager appliance, 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.

6 Alternatively, to join the NSX Manager cluster to the NSX Edge node VM, run the **join management-plane** command.

Provide the following information:

- Virtual IP address of the NSX Manager cluster with an optional port number
- User name of the NSX Manager
- Certificate thumbprint of the NSX Manager cluster
- Password of the NSX Manager

```
NSX-Edge1> join  management-plane <Cluster-VIP> username <Manager-username> password
<Manager-password> thumbprint <Cluster-tumbprint>
```

7 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)
```

8 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.
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 To successfully configure firewall rules on the NSX Edge node, enable service core on the transport node.

```
set debug

set dataplane service-core enabled

restart service dataplane
```

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

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

9 After an NSX Edge node is migrated to a new host using vCenter Server, you might find NSX Manager UI reporting stale configuration details (Compute, Datastore, Network, SSH, NTP, DNS, Search Domains) of the NSX Edge. To get the latest configuration details of NSX Edge on the new host, run the API command.

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

What to do next

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

Remove NSX Edge Nodes from an Edge Cluster

Remove NSX Edge nodes with Tier-1 Gateways or Tier-0 Gateway configured with service router (SR), DHCP and metadata proxy.

Before you remove NSX Edge nodes, relocate the gateway configurations to a new standby node:

- To remove Tier-0 gateway configurations on an NSX Edge node, you must manually relocate Tier-0 configurations such as Tier-0 SR, DHCP and metadata proxy configurations to a standby NSX Edge node.
- To remove Tier-1 gateway configurations on an NSX Edge node, do the following in these scenarios:
  - If Tier-1 SR, DHCP and metadata proxy configurations are auto allocated to the NSX Edge node, you can enable the standby relocation functionality to relocate Tier-1 configurations to a new standby NSX Edge node. The procedure describes how to use the standby relocation functionality to relocate the configurations to a new standby node.
  - If Tier-1 SR, DHCP and metadata proxy configurations are manually allocated to the NSX Edge node, you need to manually relocate Tier-1 configurations to a new standby NSX Edge node.

Procedure

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

2 On NSX Edge nodes configured with Tier-0 configurations, manually move configurations to some other NSX Edgenode.

Note The standby relocation functionality does not relocate Tier-0 configurations such as Tier-0 SRs, DHCP and metadata proxy configurations to a standby NSX Edge node.

a Select **Networking** → **Tier-0 Gateways**.

b To edit a Tier-0 Gateway, select the gateway, click vertical ellipses and click **Edit**.

c Navigate to **Interfaces** section and click the **External and Service Interfaces**.

d In the **Set Interfaces** window, edit the interface configured for NSX Edge node.

e Remove the existing NSX Edge node associated with the interface and select a new NSX Edge node that is configured with the same VLAN connectivity required for the interface and click **Save**.

The above procedure deletes Tier-0 SRs, DHCP and metadata proxy on Tier-0 Gateways of the existing NSX Edge and moves them to the new NSX Edge node.

f Delete the NSX Edge node from the edge cluster.

3 On NSX Edge nodes that are auto allocated with Tier-1 SR, DHCP and metadata proxy configurations, follow these steps to trigger the standby relocation functionality to relocate those configurations and remove the NSX Edge node from the NSX Edge cluster:

a (Optional) For faster failover, change the BFD timers for NSX Edge cluster by setting it to **500** ms.

b Apply the new NSX Edge cluster profile to the transport node profile. It ensures faster failover when the NSX Edge node is powered off.

c Select **Networking** → **Tier-1 Gateways**.

d To edit a Tier-1 Gateway, select the gateway, click vertical ellipses and click **Edit**.

e In the Edit view, select the NSX Edge cluster and enable the **Enable Standby Relocation** field.

Important For standby relocation to function successfully, there must be an additional healthy NSX Edge node in the edge cluster. During the process of removing an NSX Edge node, Tier-1, DHCP or metadata proxy configurations are relocated from an existing NSX Edge to a new standby node.

f Select **System** → **Fabric** → **Profiles** → **Edge Cluster Profiles**.

g Select the edge cluster profile and click **Edit**.

h Set **Standby Relocation Threshold (mins)** that is applied to the edge cluster. The default recommended value is 30 mins and the minimum value is 10 mins.

Note Only auto allocated Tier-1 SR, DHCP and metadata proxy configurations are relocated to a standby NSX Edge. If the NSX Edge node to be removed contains any manually allocated configurations, such configurations will not be relocated out from existing NSX Edge node to a stanby node. You need to manually change the allocation for those Tier-1 configurations.

i Power off the NSX Edge without taking down the node into maintenance mode. If the NSX Edge is running any active service, then all such active service configurations will failover to another NSX Edge because of the HA failover trigger when the node is powered off.

j Wait for the duration of standby relocation threshold timeout. After the threshold limit is reached, all Tier-1 service configurations that have standby relocation enabled will be removed from the edge node being powered-off and relocated to some other NSX Edge in the cluster. There can be minor delays in standby relocation to perform the relocation task.

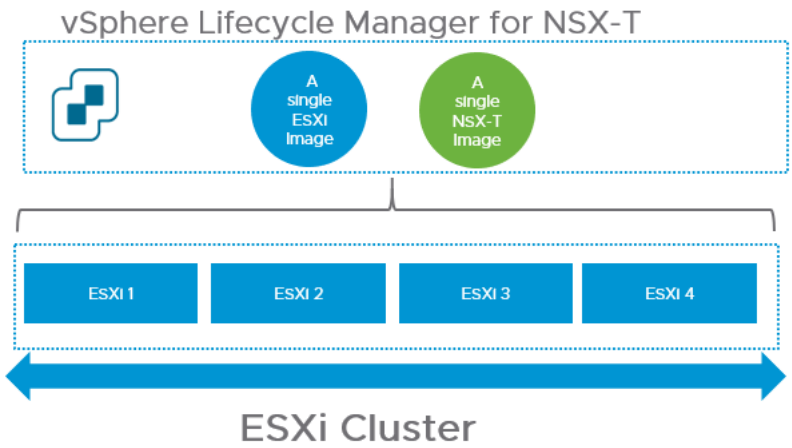
k After Tier-1 configurations are relocated to a standby node, remove the NSX Edge that was powered off from the cluster.

vSphere Lifecycle Manager with NSX-T

12

By enabling VMware vSphere® vSphere Lifecycle Manager on a cluster, you can ensure that all ESXi hosts participating in a cluster are prepared using a single ESXi image and a single NSX-T image. The vSphere Lifecycle Manager functionality minimizes errors and lowers cluster and host maintenance cycles.

Starting from vCenter Server 7.0 U1, ESXi 7.0 U1, and NSX-T 3.1.0 onwards, a vSphere Lifecycle Manager-enabled cluster can manage installation of ESXi and NSX-T VIBs.



vSphere Lifecycle Manager requires two images: one for ESXi and another one for NSX-T. It retrieves the ESXi image from the image directory in vCenter Server. Ensure the ESXi image is uploaded to vCenter Server. vSphere Lifecycle Manager gets the NSX-T image only when a cluster is prepared for NSX-T networking, which is possible from the NSX Manager user interface. The NSX-T image is automatically uploaded to vCenter Server when NSX-T cluster preparation begins. For other clusters in the vCenter Server, vSphere Lifecycle Manager references the already uploaded NSX-T image. vSphere Lifecycle Manager refers to NSX-T as a solution, as it does with other solutions such as HA, DRS and so on.

For more information on the usage of the terminology, such as images and solutions in vSphere Lifecycle Manager, refer to the *Managing Host and Cluster Lifecycle guide* in the VMware vSphere® Documentation center.

The following clusters can be enabled as vSphere Lifecycle Manager clusters:

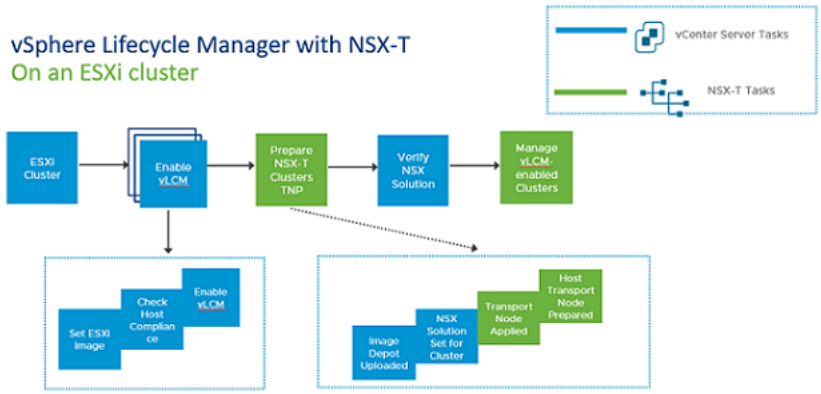
- Clusters with ESXi hosts that are prepared for NSX-T networking using a transport node profile.
- Clusters with ESXi hosts that are not prepared for NSX-T networking.

Read the following topics next:

- Prepare an NSX-T Cluster with vSphere Lifecycle Manager
- Enable vSphere Lifecycle Manager on an NSX-T Cluster
- NSX-T with vSphere Lifecycle Manager Scenarios
- vSphere Lifecycle Manager Failed to Prepare a Host for NSX-T Networking
- vSphere Lifecycle Manager Failed to Prepare NSX-T Cluster
- Delete a NSX-T Depot on vCenter Server

Prepare an NSX-T Cluster with vSphere Lifecycle Manager

You can prepare NSX-T on vSphere Lifecycle Manager-enabled clusters.



For vSphere Lifecycle Manager to get access to the NSX-T image, you must configure the cluster with a transport node profile. When you begin configuring the cluster, NSX-T local control plane bundle (in the format - nsx-lcp-bundle-<*release_version.build_version*>) is uploaded to the image repository in vCenter Server.

During host preparation, vSphere Lifecycle Manager accesses the depot and sets NSX as a solution for that cluster. It applies the NSX solution to the cluster, which begins with the process of remediating hosts. Every host is remediated by vSphere Lifecycle Manager before the NSX switch is configured on the host. vSphere Lifecycle Manager remediation happens when a new ESXi host is added to a vSphere Lifecycle Manager cluster.

vSphere Lifecycle Manager remediates hosts so that the image on each host is the same as the ESXi version set for the cluster. Any drift must be resolved before host preparation can progress in NSX-T. During cluster preparation, if the cluster fails, NSX-T sets the cluster state to Failed. As an admin, you must retrigger host remediation by taking appropriate actions either from the NSX Manager user interface or from the vSphere Client.

Prerequisites

- Ensure all hosts in a cluster are running at least ESXi 7.0 U1 version or higher.
- Ensure Lockdown mode is not enabled on any of the hosts. vSphere Lifecycle Manager might fail to prepare hosts that are enabled to function in Lockdown mode.
- Ensure there is not drift in images between hosts and cluster. Otherwise, you cannot enable vSphere Lifecycle Manager on the cluster. Remediate hosts in vCenter Server to ensure base image matches on host and cluster.
- Ensure vSphere Lifecycle Manager is enabled on the cluster. See VMware vSphere® documentation.
- Register Compute Manager with the following settings:
  - Enable **Trust** and set access level to vSphere Lifecycle Manager. Trust is mandatory to establish communication between NSX-T and vSphere Lifecycle Manager.
  - Enable **Create Service Account**.
- Create a transport node profile using a vSphere Distributed Switch host switch. N-VDS switch is not supported on a vSphere Lifecycle Manager-enabled.

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** → **Nodes** → **Host Transport Nodes**.
3. In the **Managed by** drop-down menu, select the Compute Manager.
4. Select the cluster and click **Configure NSX**.

   Note Identify vSphere Lifecycle Manager-enabled cluster when a cluster is accompanied with vLCM text.

5. Select a transport node profile that uses vSphere Distributed Switch as the host switch.
6. Click **Apply TNP**.

   If this is the first cluster that is enabled for vSphere Lifecycle Manager, NSX-T uploads the NSX LCP bundle to the image repository in vCenter Server. vSphere Lifecycle Manager sets NSX as a solution on the cluster. It sets the desired state to the NSX image uploaded to vCenter Server. Then, vSphere Lifecycle Manager begins installation of NSX VIBs on each host, followed by configuration of NSX switch on each transport node.

As part of host preparation, vSphere Lifecycle Manager remediates the host, registers the host with NSX Manager, configures NSX switch on the host and completes the configuration.

Note Installing NSX-T on a vSphere Lifecycle Manager-enabled cluster might take a little more time than when installing on a non-vSphere Lifecycle Manager-enabled cluster. This difference is due to the additional health checks that are included in this combination of products

7 Troubleshooting issues:

If vSphere Lifecycle Manager could not apply NSX as a solution to the cluster, the NSX-T cluster in NSX Manager goes into Failed state. To remediate the hosts in the cluster, do one of the following:

a Go to the vCenter Server, verify the following conditions are met:

- Hosts are compliant.
- Hosts are not powered off or in maintenance mode.

b Verify cluster status through UI or API. Even if a host in the cluster is in `Failed` state, the cluster status remains in unrealized state.

Run the following API to verify the cluster state, `GET /<NSX-Manager-IP>/api/v1/transport-node-collections/<transport-node-collection-id>`.

c If any one of the host fails, the remaining hosts in the cluster go into `Install Skipped` state. To remediate, read the error message and take any necessary action. Then, click **Resolve** to retry remediation of the host and NSX-T preparation. Note that remediation happens serially, one host at a time.

d If the cluster is still in `Install Failed` state, click **Resolve** for the cluster in UI or run the API to realize the transport node profile on the cluster. Along with remediating the cluster, the following API also tries to prepare those hosts that are in the `Install Skipped` state. It retries remediation on the entire cluster. It tries to prepare the hosts where installation is skipped.

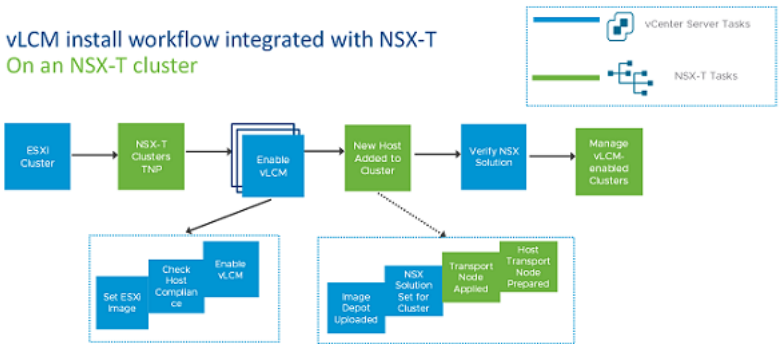
```
POST /api/v1/transport-node-collections/<transport-node-collection-id>?action=retry_profile_realization
```

Results

Sphere Lifecycle Manager prepares all hosts in the cluster as NSX-T transport nodes.

Enable vSphere Lifecycle Manager on an NSX-T Cluster

As you can prepare an NSX-T cluster on a cluster that is already enabled with vSphere Lifecycle Manager, similarly, you can enable vSphere Lifecycle Manager on an existing NSX-T prepared cluster.



Prerequisites

- Ensure all hosts in a cluster are running ESXi 7.0 U1 version.
- Register Compute Manager with the following settings:
  - Enable **Trust** and set access level to vSphere Lifecycle Manager. Trust is mandatory to establish communication between NSX-T and vSphere Lifecycle Manager.
  - Enable **Create Service Account**.
- Prepare the cluster by applying a Transport Node Profile (using VDS as the host switch type) to the cluster.

  Note N-VDS host switch is not supported on a vSphere Lifecycle Manager-enabled cluster.

Procedure

1. From a browser, log in with admin prvileges to a vCenter Server at https://<vccenter-server-ip-address>.
2. Select the cluster on which the vSphere Lifecycle Manager functionality must be enabled.
3. On the Images page, confirm that all hosts are compliant. If any of the host is in non-compliant state, remediate the host to be compliant with the ESXi image set for the cluster.

4 Verify that vSphere Lifecycle Manager sets the solution for the cluster to NSX. To verify that the NSX solution is set on the vSphere Lifecycle Manager cluster, you can do one of the following:

   a In vCenter Server, on the Images page, click **Check Compliance** and check the Components section for an NSX entry.

   b Alternatively, run the API command and verify that component and version are correctly set to NSX.

```
GET https://{server}/api/esx/settings/clusters/{cluster}/software/solutions/
com.vmware.nsxt?vmw-task=true
    components" : [
    {
     "component" : "nsx-lcp-bundle"
    }
    ],
    "version" : "3.1-0"
```

5 When a new host is added to the vSphere Lifecycle Manager-enabled cluster, NSX-T calls vSphere Lifecycle Manager to check host compliance with the ESXi image set for the cluster. If there is no drift in host and cluster image, then transport node profile is applied to the host. NSX-T VIBs on the host. The final part of the installation is followed by registration with NSX Manager and NSX switch configuration.

6 Troubleshooting issues:

   If vSphere Lifecycle Manager could not apply NSX as a solution to the cluster, the NSX-T cluster in NSX Manager goes into **Failed** state. To remediate the hosts in the cluster, do one of the following:

   a Go to the vCenter Server, verify the following conditions are met:

      - Hosts are compliant.
      - Hosts are not powered off or in maintenance mode.

   b Verify cluster status through UI or API. Even if a host in the cluster is in `Failed` state, the cluster status remains in unrealized state.

      Run the following API to verify the cluster state, `GET /<NSX-Manager-IP>/api/v1/transport-node-collections/<transport-node-collection-id>`.

c If any one of the host fails, the remaining hosts in the cluster go into `Install Skipped` state. To remediate, read the error message and take any necessary action. Click **Resolve** to retry remediation of the host and NSX-T preparation. Note that remediation happens serially, one host at a time.

d If the cluster is still in `Failed` state, click **Resolve** for the cluster in UI or run the API to realize the transport node profile on the cluster. Along with remediating the cluster, the following API also tries to prepare those hosts that are in the `Install Skipped` state. It retries remediation on the entire cluster. It tries to prepare the hosts where installation is skipped.

```
POST /api/v1/transport-node-collections/<transport-node-collection-id>?
action=retry_profile_realization
```

Results

vSphere Lifecycle Manager is enabled on a NSX-T cluster.

What to do next

After enabling vSphere Lifecycle Manager on the cluster, you can remediate drifts between hosts in vCenter Server with the image set for the cluster.

NSX-T with vSphere Lifecycle Manager Scenarios

Installation and uninstallation scenarios to consider when you work with vSphere Lifecycle Manager (vLCM) for NSX-T clusters.

Scenario	Result
You try to enable vSphere Lifecycle Manager on a cluster where transport node profile is not applied, but some hosts are individually prepared as host transport nodes.	vSphere Lifecycle Manager cannot be enabled on the cluster because a transport node profile was not applied to the cluster.
You try to enable vSphere Lifecycle Manager on a cluster using a transport node profile configured to apply N-VDS host switch.	vCenter Server checks for cluster eligibility so that the cluster can be converted to a vSphere Lifecycle Manager cluster. As N-VDS host switch type is not supported, apply a transport node profile that is configured to use a VDS host switch.
You move an unprepared host from a non-vSphere Lifecycle Manager cluster to a vSphere Lifecycle Manager cluster.	If the vSphere Lifecycle Manager cluster is prepared with a transport node profile, the unprepared host is prepared as an NSX-T transport node by vSphere Lifecycle Manager. If the vSphere Lifecycle Manager cluster is not prepared with a transport node profile, the host remains in unprepared state.

Scenario	Result
You move a transport node from a vSphere Lifecycle Manager cluster to a non-vSphere Lifecycle Manager cluster that is not prepared for NSX-T.	The NSX-T VIBs are deleted from the host, but the NSX Solution-related data (set by vSphere Lifecycle Manager) is not deleted. Now, if you try to enable vSphere Lifecycle Manager cluster on the cluster, NSX Manager notifies that NSX Solution will be removed from the host. This notfication is misleading because NSX-T VIBs were already removed on the host.
After you perform the **Remove NSX** operation on a Sphere Lifecycle Manager cluster, if vSphere Lifecycle Manager is unable to delete NSX-T from the desired state, all nodes go into `Uninstall Failed` state. Now, you try to remove NSX-T on individual transport nodes.	If you remove NSX-T on each individual transport node, then even though NSX-T VIBs are removed on the host, the cluster continues to have NSX as the desired state in vSphere Lifecycle Manager. This state shows up as drift in host compliance in vCenter Server. So, you must perform **Remove NSX** on the cluster to remove NSX from the vSphere Lifecycle Manager configuration.
vCenter Server is added as a compute manager with **Multi NSX** flag enabled. Apply TNP on another existing vLCM cluster.	NSX-T does not allow preparation of the existing vLCM cluster if it is part of the same vCenter Server.
vCenter Server is added as a compute manager with **Multi NSX** flag enabled. Then try to change the already prepared cluster to a vLCM cluster.	NSX-T does not allow preparation of the existing vLCM cluster.
vCenter Server is added as a compute manager with **Multi NSX** flag enabled. Then try creating a new vLCM cluster.	NSX-T allows preparation of the existing vLCM cluster.
vCenter Server already contains a vLCM cluster and you try to add the vCenter Server as a compute manager with **Multi NSX** flag enabled.	NSX-T fails this operation because the vCenter Server already contains a vLCM cluster.

vSphere Lifecycle Manager Failed to Prepare a Host for NSX-T Networking

vSphere Lifecycle Manager failed to prepare some hosts in the cluster for NSX-T Networking.

Problem

In a cluster containing many hosts, vSphere Lifecycle Manager successfully prepared some hosts, whereas vSphere Lifecycle Manager failed to realize NSX-T on one of the host.

Cause

Hosts can take different states when vSphere Lifecycle Manager triggers installation of NSX-T.

- Cluster goes into `Install Failed` if vSphere Lifecycle Manager fails to remediate the entire cluster.
- If one or more individual hosts fail, failed hosts go into `Install Failed` state. If there are other hosts in the cluster yet to be prepared, those hosts go into `Install Skipped` state. Both cluster and individual hosts display failure states.

Solution

1 On the NSX Manager, go to **System** → **Fabric** → **Nodes** → **Host Transport Node**.

2 From the **Managed by** drop-down menu, select the vCenter Server.

3 Identify the failed cluster to view the error state. Click the error link to open a popup window.

4 If the cluster is in `Install Failed` state, click **Resolve** at the to initiate transport node profile realization on the cluster.

Important With the cluster in `Install Failed` state, first try to resolve the remediation issues at the cluster and then try to remediate individual hosts. If you overlook cluster-level errors and directly try to remediate host-level errors, the UI does not allow you to perform any remediation action at the host-level.

5 If one or more hosts failed but the cluster remediation status is Success, then navigate to the failed host and click **Resolve** to remediate hosts.

6 You can also try to realize the transport node profile on the cluster by executing the following API command, `POST /api/v1/transport-node-collections/{tnc id}?action=retry_profile_realization`.

This API command re-triggers the transport node profile on the cluster.

vSphere Lifecycle Manager Failed to Prepare NSX-T Cluster

vSphere Lifecycle Manager failed to prepare an NSX-T cluster.

Problem

Transport node profile could not be applied to a vSphere Lifecycle Manager cluster, which caused the cluster to go into `Failed` state.

Cause

As vSphere Lifecycle Manager failed to set and apply NSX-T as a solution on the cluster, none of the hosts in the cluster were prepared as transport nodes. View the error state on the cluster in NSX Manager UI.

Solution

1 On the NSX Manager, go to **System** → **Fabric** → **Nodes** → **Host Transport Node**.

2 From the **Managed by** drop-down menu, select the vCenter Server.

3 Identify the failed cluster to view the error state. Click the error link to open a popup window. Click **Resolve** to initiate transport node profile realization on the cluster.

4 Alternatively, run the API command, `POST /api/v1/transport-node-collections/<tnc id>?action=retry_profile_realization`. This command initiates vLCM to realize NSX-T on the cluster.

Delete a NSX-T Depot on vCenter Server

Delete a NSX-T Depot on vCenter Server.

Procedure

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

2 Unregister the compute manager from NSX-T.

When the compute manager s unregistered, NSX-T invokes API to delete the depot in vCenter Server. Depot is deleted from the image depot of vSphere Lifecycle Manager in vCenter Server

3 Troubleshooting:

a If NSX-T is unable to delete the depot after unregistering the compute manager, run the following API.

```
DELETE https://{server}/api/esx/settings/depots/offline/{depot}
```

b Remove the depot entry from the payload.

c To verify that the depot is successfully deleted, run the API command.

```
GET https://{server}/api/esx/settings/depots/offline/{depot}
```

Host Profile integration with NSX-T

13

Integrate host profiles extracted from an ESXi host with NSX-T to deploy ESXi and NSX-T VIBs on stateful and stateless servers.

Read the following topics next:

- 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 ESXi Version	ESXi 67ep6	ESXi 67u2	ESXi 67u3	ESXi 67ep7	ESXi 67ep15	ESXi 7.0
NSX-T Data Center 2.4	Yes	Yes	No	No	No	No
NSX-T Data Center 2.4.1	Yes	Yes	No	No	No	No
NSX-T Data Center 2.4.2	Yes	Yes	No	No	No	No
NSX-T Data Center 2.4.3	Yes	Yes	No	No	No	No
NSX-T Data Center 2.5	Yes	Yes	Yes	Yes	No	No
NSX-T Data Center 2.5.1	Yes	Yes	Yes	Yes	Yes	No
NSX-T Data Center3.0	Yes	Yes	Yes	Yes	Yes	Yes
NSX-T Data Center3.1 and later	Yes	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.

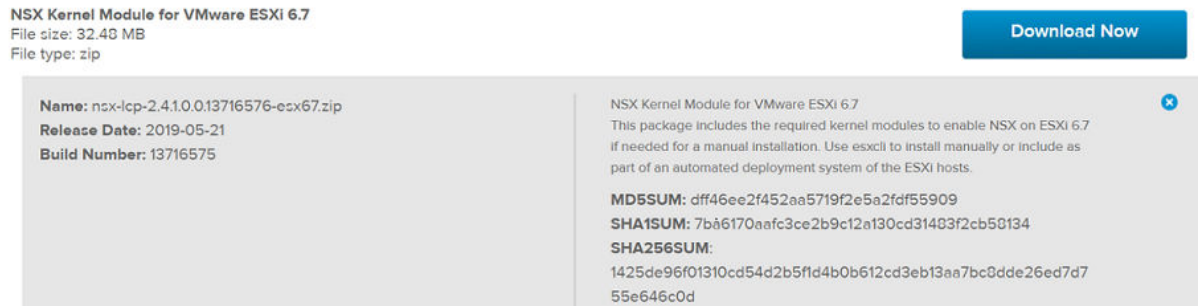
2 Download the `nsx-lcp` packages.

   a Go to https://customerconnect.vmware.com and navigate to **Products and Accounts** → **Products** → **All Products**.

   b In the Product Downloads page, search NSX-T Kernel Modules for a specific VMware ESXi version.

   c Click **Download Now** to begin downloading the `nsx-lcp` package.

   d Import `nsx-lcp` packages into the software depot.



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**.

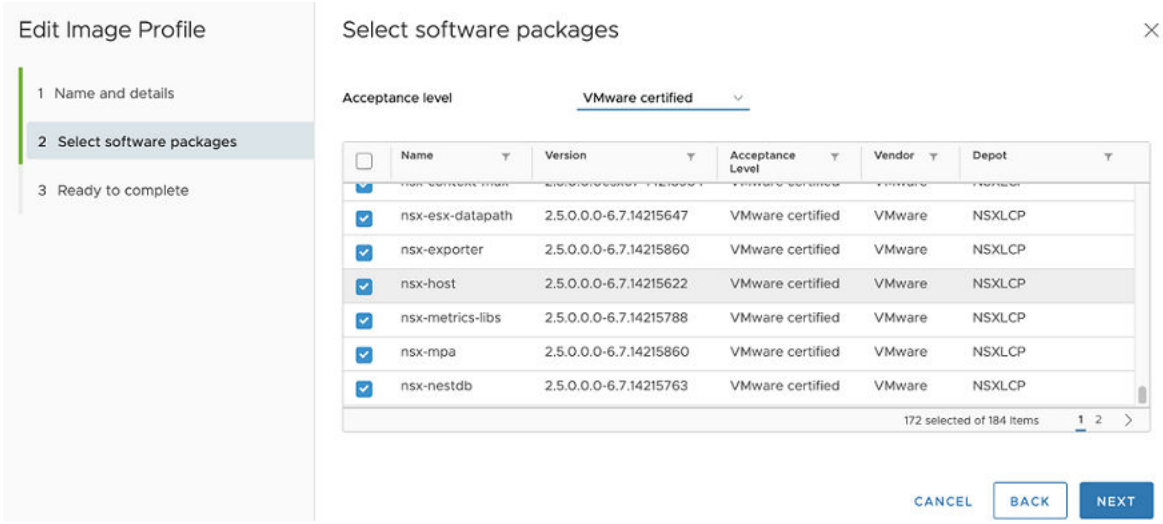
c In the Clone Image Profile wizard, enter a name for the custom image to be created.

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.



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**.

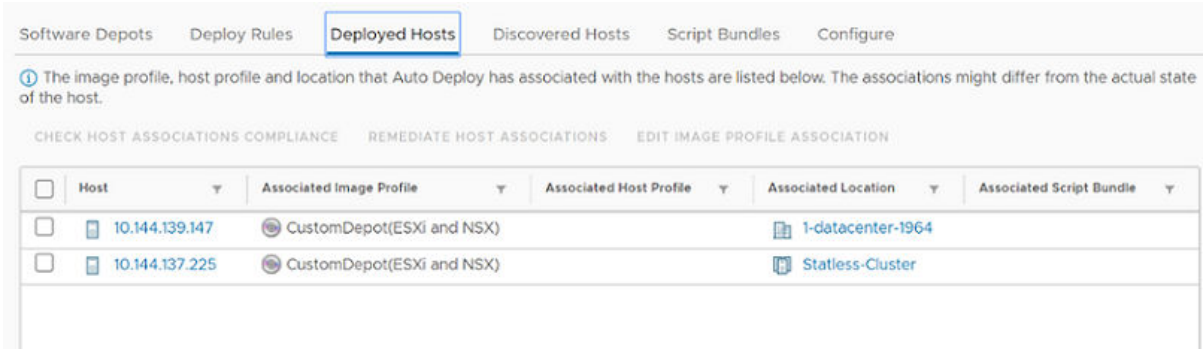
2 To associate the custom image profile with a host, select the custom image.

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**.



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

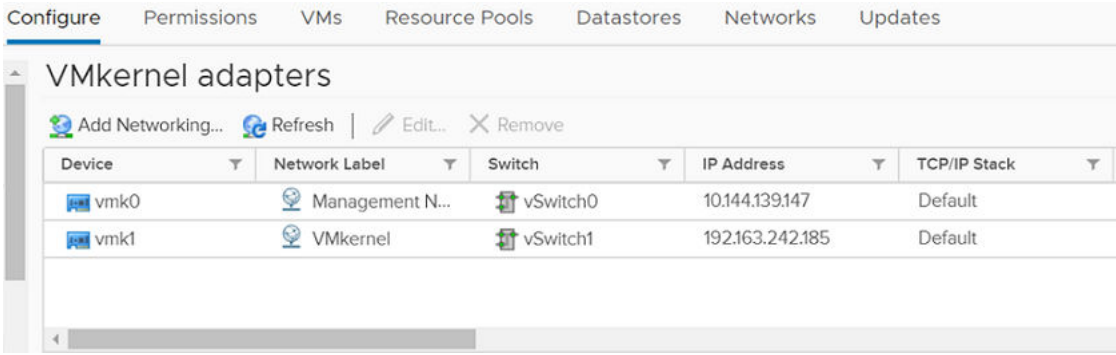
On the reference host, a standard switch with a VMkernel adapter is created to set up the network configuration on ESXi.

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.



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 or DVS switch, deploy the reference host as a NSX-T transport node with NSX-T enabled DVS switch.

Procedure

1 From a browser, log in to NSX-T at https://<NSXManager_IPaddress>.

2 To locate the reference host, navigate the UI based on the NSX-T Data Center version:

- (NSX-T Data Center 3.2.2 or later) **System > Fabric > Hosts** and select the **Cluster** tab.
- (NSX-T Data Center 3.2.1 or earlier) **System > Fabric > Nodes > Host Transport Nodes**

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.

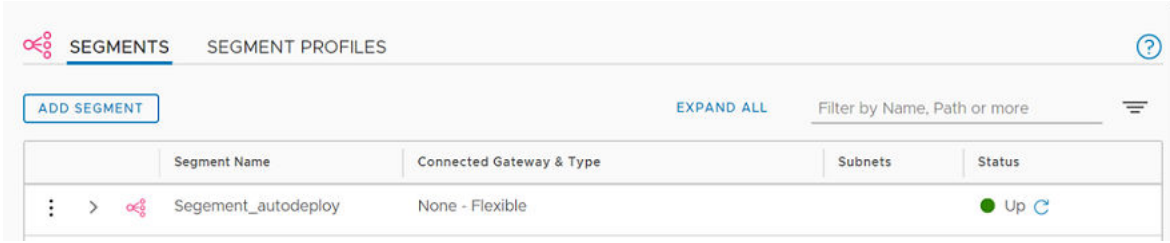
4 Create a VLAN segment on the transport zone. The created segment is displayed as a logical switch.

a Navigate to **Networking** -> **Segments**.

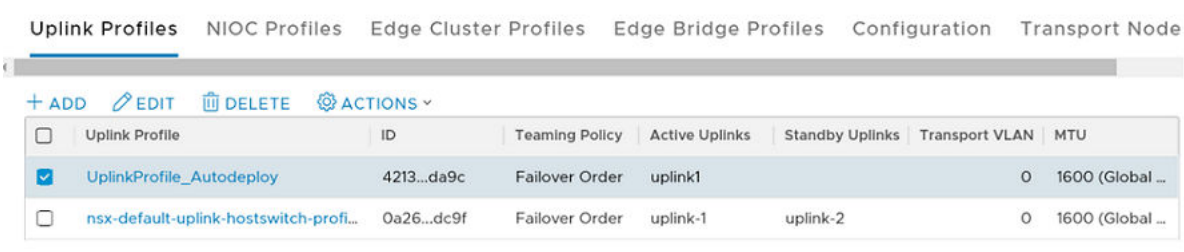
b Select the transport zone to attach the segment.

c Enter VLAN ID.

d Click **Save**.



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.

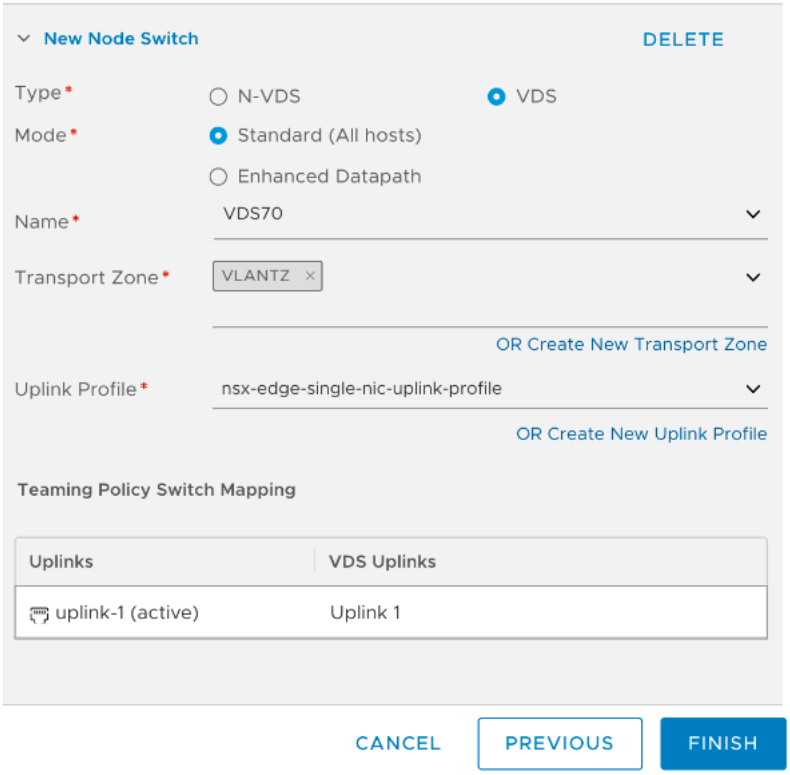


6 Configure the reference host as a transport node. See Configure a Managed Host Transport Node.

a In the Host Transport Node page, select the reference host.

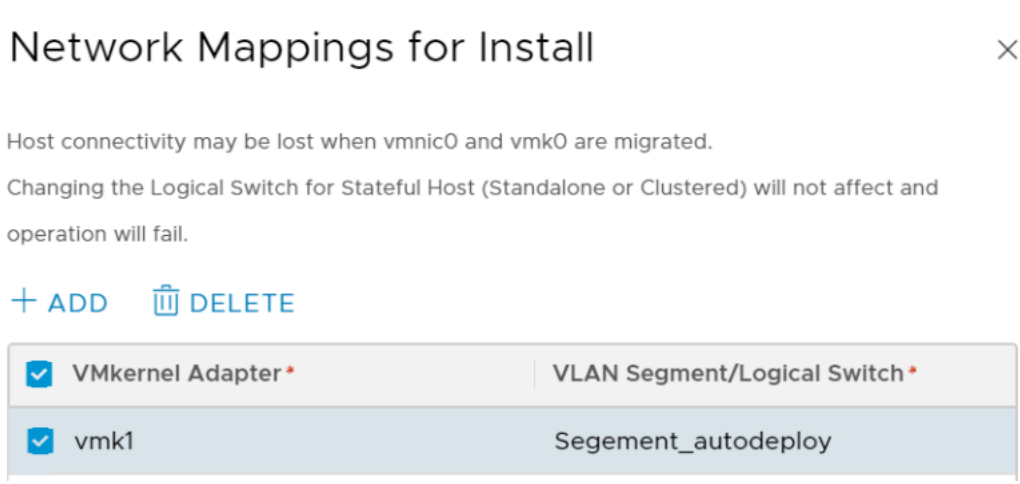
b (On a N-VDS switch) Click Configure NSX and select the previously created transport zone, N-VDS, uplink profile.

c (On a VDS switch) Click Configure NSX and select the previously created transport zone, VDS, uplink profile.



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.

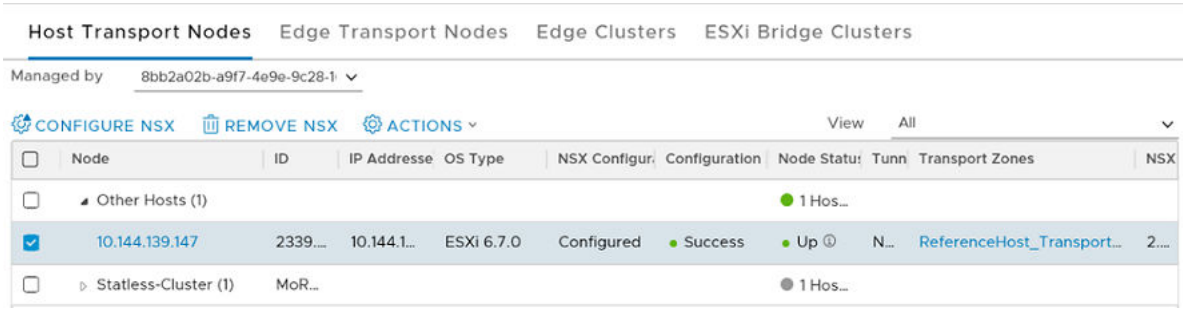


8 Click **Finish** to begin installation of NSX-T on the reference host.

(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.

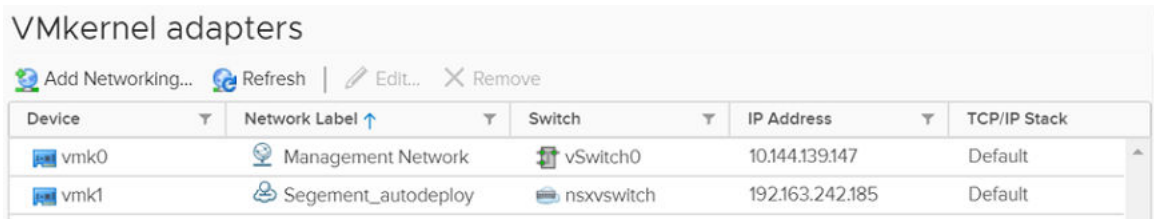
(On an N-VDS switch) During installation, VMkernel adapters and physical NICs are migrated from a VSS or DVS switch to an N-VDS switch. After installation, configuration status of the reference host is displayed as `Success`.

Note The reference host is listed under Other Hosts.



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.



What to do next

Extract and Verify the Host Profile. See Extract and Verify the Host Profile.

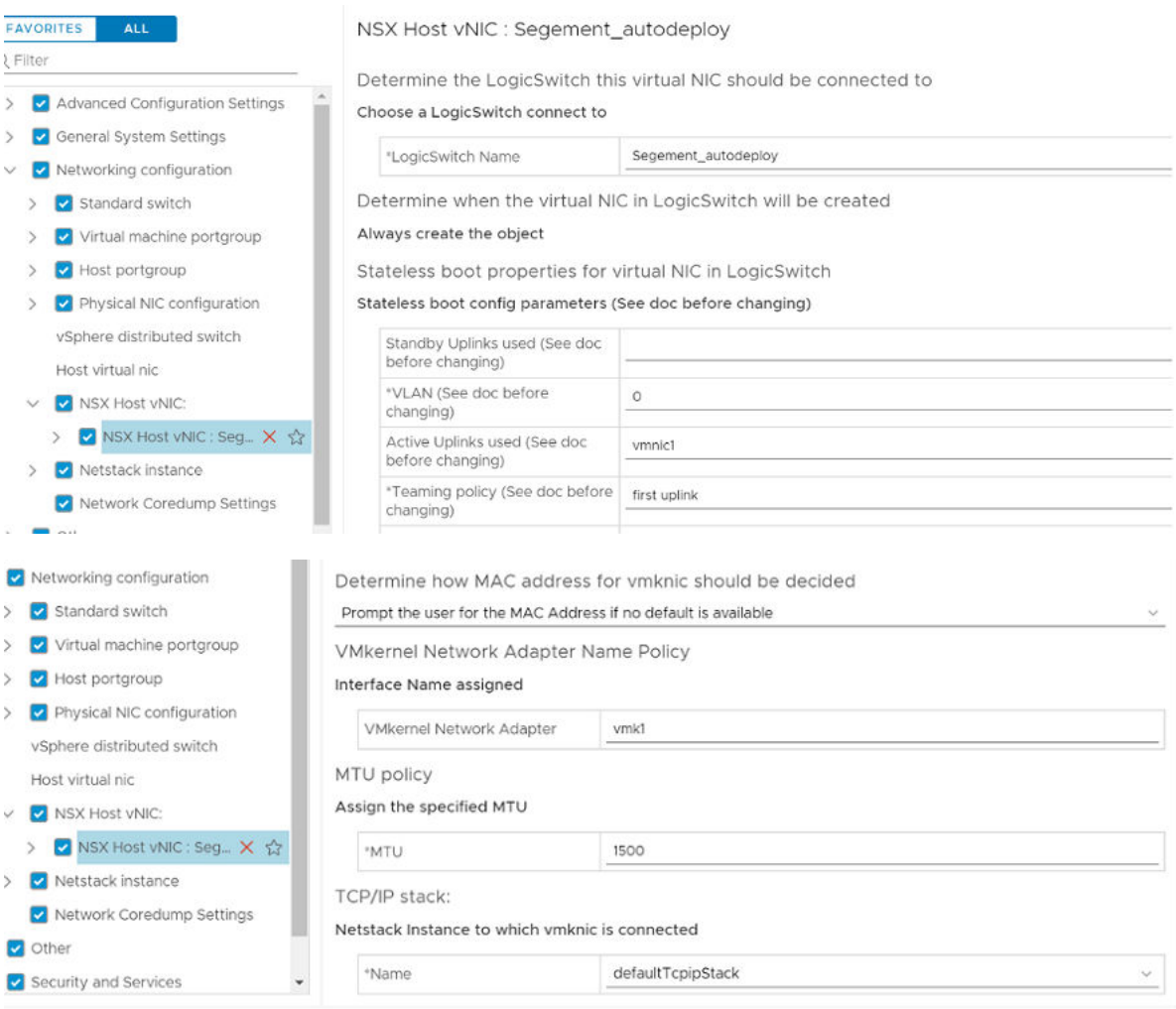
Extract and Verify the Host Profile

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.

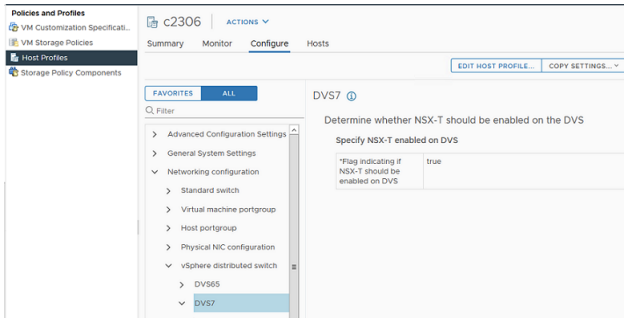
Procedure

1 To extract the host profile, see Extract and Configure Host Profile from the Reference Host.

2 In the extracted host profile verify NSX-T configuration.



3 To verify DVS switch is enabled on NSX-T, select **Policies and Profiles** → **Host Profiles** → **Configure** → **vSphere Distributed Switch**.



4 Select the DVS switch and determine whether NSX-T is enabled on DVS.

What to do next

Verify the host profile association with stateless cluster. See Verify the Host Profile Association with Stateless Cluster.

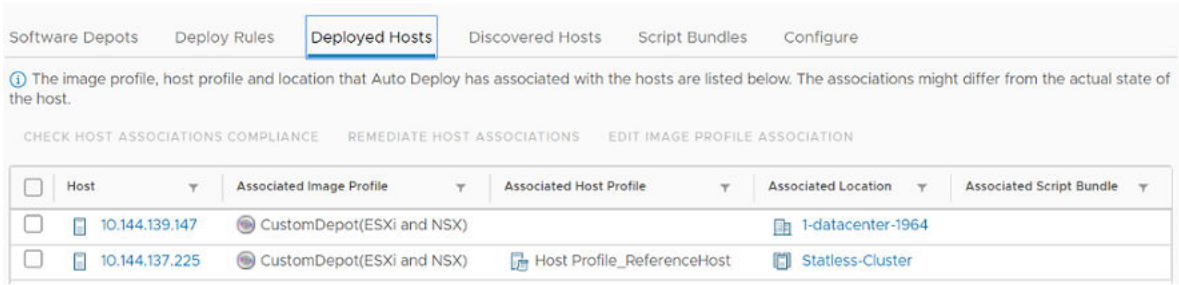
Verify the Host Profile Association with Stateless Cluster

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.



What to do next

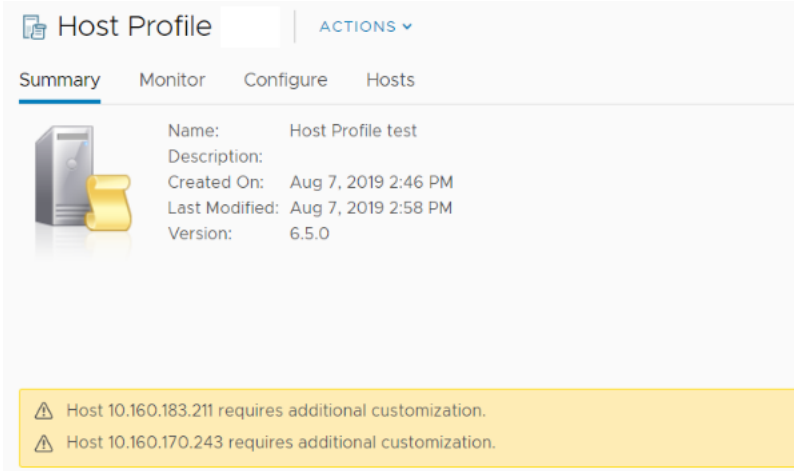
Update Host Customization. See Update Host Customization.

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.

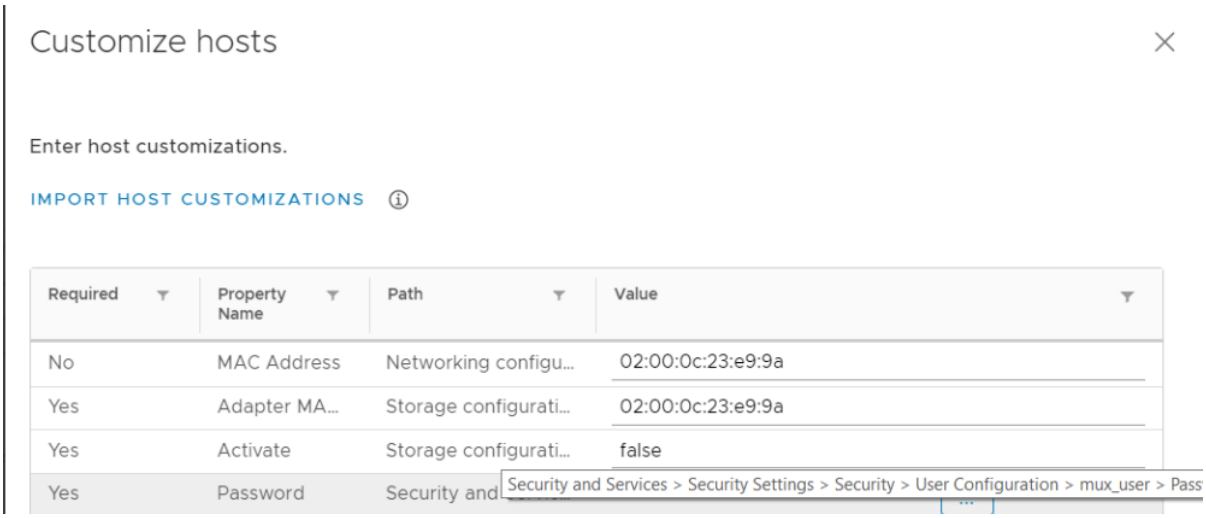
Procedure

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.



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.



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.

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

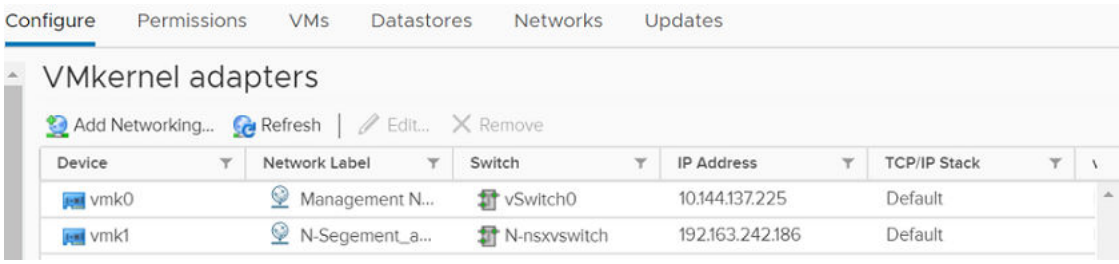
1 Reboot hosts.

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.



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.

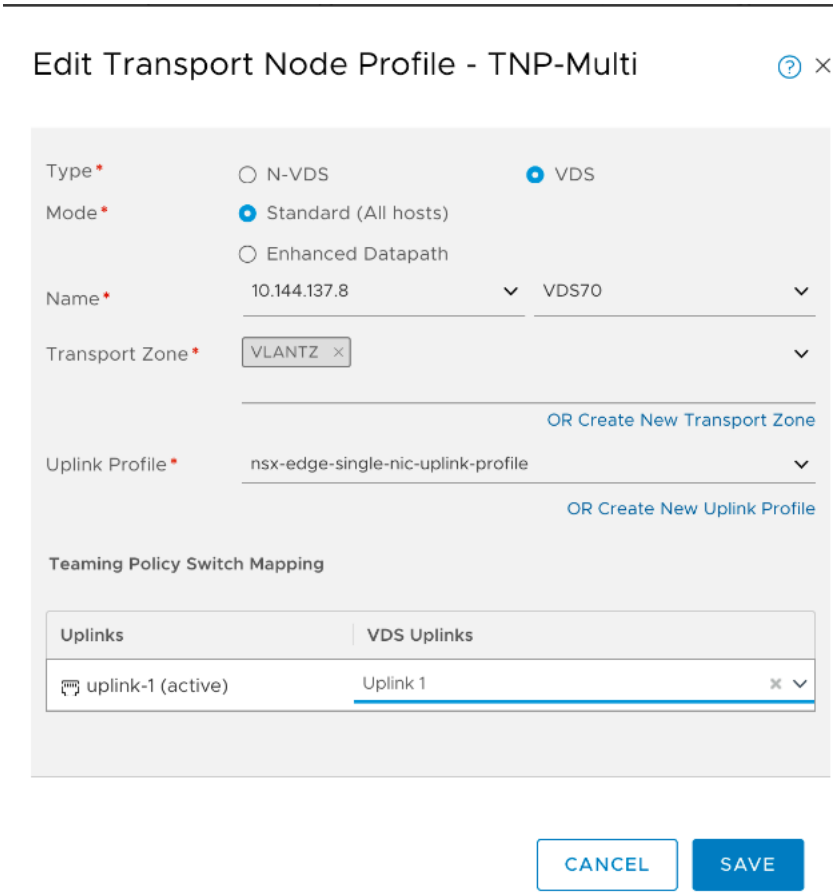
2. Add a TNP. See Add a Transport Node Profile.

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.

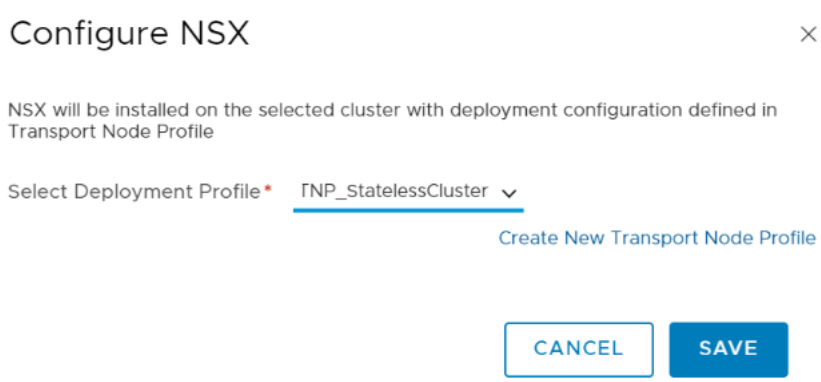
   - Transport Zone: Ensure transport zone referenced in Host Profile and TNP is the same.
   - N-VDS Name: Ensure N-VDS name referenced in Host Profile and TNP is the same.
   - Uplink Profile: Ensure uplink profile referenced in Host Profile and TNP is the same.
   - Teaming Policy:
     - (On a VDS switch) 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.



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.

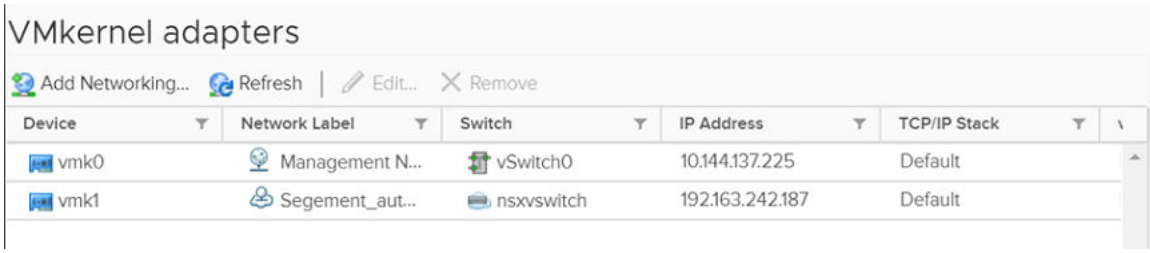
5 Apply TNP profile to the target cluster and click **Save**.



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.



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.

Scenario	Description
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.
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.

Scenario	Description
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.
A stateless host does not boot up with MAC address of PXE NIC when it is applied with a host profile extracted from a stateful host.	Issue: If a stateless host is attached with a host profile extracted from a statelful host, then the VMkernel adapter (vmknic) of the stateless host does not boot up with the MAC address of PXE NIC of the host because a stateful host does not boot up as a PXE-enabled system. Workaround: When you are setting up autodeployment of stateless hosts, ensure that the host profile extracted is from a from a host that boots up as a PXE-enabled system.

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

Version Name	67ep6	67U2	67U3	67ep7	67U2C	6.5U3	6.5p03	7.0.0.1
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 Federation

14

To get started with NSX Federation, you install the Global Manager, configure the Global Manager as active, and add locations.

Task	Details
Check the requirements for Federation.	See NSX Federation Requirements.
Install the Global Manager.	See Install the Active and Standby Global Manager .
Make the Global Manager cluster active.	See Make the Global Manager Active and Add Standby Global Manager.
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 NSX Federation Key Concepts

NSX Federation introduces some new terms and concepts, such as remote tunnel endpoint (RTEP), span, and region.

2 NSX Federation Requirements

To support NSX Federation, your environment must meet various requirements, including round-trip time, software versions, and ports.

3 Configuring the Global Manager and Local Managers

An NSX Federation environment contains an active and a standby Global Manager cluster and one or more Local Manager clusters.

NSX Federation Key Concepts

NSX Federation introduces some new terms and concepts, such as remote tunnel endpoint (RTEP), span, and region.

NSX Federation Systems: Global Manager and Local Manager

An NSX Federation environment includes two types of management systems:

- Global Manager: A system similar to NSX Manager that federates multiple Local Managers.
- Local Manager: An NSX Manager system in charge of network and security services for a location.

NSX Federation Span: Local and Stretched

When you create a networking object from Global Manager, it can span one or more locations.

- Local: The object spans only one location.
- Stretched: The object spans more than one location.

You do not directly configure the span of a segment. A segment has the same span as the gateway it is attached to.

NSX Federation Regions

Security objects have a region. The region can be one of the following:

- Location: Each location automatically creates a region. This region has the span of that location.
- Global: A region that has the span of all available locations.
- Custom Region: You can create regions that include a subset of the available locations.

NSX Federation Tunnel Endpoints

In an NSX Federation environment, there are two types of tunnel endpoints.

- Tunnel End Point (TEP): The IP address of a transport node (Edge node or Host) used for Geneve encapsulation within a location.
- Remote Tunnel End Points (RTEP): The IP address of a transport node (Edge node only) used for Geneve encapsulation across locations.

NSX Federation Requirements

To support NSX Federation, your environment must meet various requirements, including round-trip time, software versions, and ports.

- There must be a maximum round-trip time of 500 ms between the following nodes:
  - Active Global Manager and standby Global Manager.
  - Global Manager and Local Manager.
  - Local Manager and remote Local Manager if you have cross-location security configurations only and 150 ms or less if you have cross-network configurations.

- The Global Manager and Local Manager appliances must all have NSX-T Data Center 3.1.0 or later installed. All appliances in an NSX Federation environment must have the same version 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 nodes:
  - Global Manager and Local Manager.
  - Local Manager and remote Local Manager.
  - Edge node RTEP and remote Edge node RTEP.
- Verify that each location has a default overlay transport zone configured. From each Local Manager, select **System > Fabric > Transport Zones**. Select an overlay transport zone, and click **Actions > Set as Default Transport Zone**.
- Global Manager supports only Policy Mode. NSX Federation does not support Manager Mode. See NSX Manager for more information.

An NSX 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 NSX Federation category for NSX-T Data Center in the VMware Configuration Maximums tool for exceptions and other NSX 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*.

Configuring the Global Manager and Local Managers

An NSX Federation environment contains an active and a standby Global Manager cluster and one or more Local Manager clusters.

Install the Active and Standby Global Manager

To use NSX Federation, you must install the Global Manager.

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 role.

Install a standby Global Manager appliance for high availability and disaster recovery. The standby Global Manager appliance must be installed in a different location with a latency of 500ms or less.

Prerequisites

- Verify that your environment meets the requirements for NSX Manager. See NSX Manager VM and Host Transport Node System Requirements.

- Decide which locations will contain the active and standby Global Manager appliances.
- Verify that you are installing the Global Manager appliance with NSX-T Data Center 3.2.0 or later.

Important All Global Manager and Local Manager appliances in an NSX Federation environment must have the same version of NSX-T Data Center installed.

Procedure

1 Install the first Global Manager appliance.
   - On vSphere: Install NSX Manager and Available Appliances.
     - Select `Medium` or `Large` for the deployment configuration size. Do not use `Small`.
     - Select `NSX Global Manager` for the **Rolename**.
   - On KVM: Install NSX Manager on KVM.
     - Deploy a medium appliance. For example: `virt-install --import --ram 16000--vcpus 6`.
     - Select `NSX Global Manager` for the `nsx_role`.
2 Log in to the NSX Manager appliance.

   See Log In to the Newly Created NSX Manager .
3 (Optional) If you are installing Global Manager on vSphere, configure a compute manager.

   See Add a Compute Manager.

   Note If you are at this step while installing the standby Global Manager, you must configure a separate compute manager. Do not use the same compute manager that you configured for the active Global Manager.
4 Create a Global Manager cluster. See Cluster Requirements for an Individual Site for design recommendations.
   - On vSphere with a compute manager configured: See Deploy NSX Manager Nodes to Form a Cluster from the UI.
   - On vSphere without a compute manager configured: Repeat the NSX Manager install on vSphere steps to install three appliances, then form the cluster. See Form an NSX Manager Cluster Using the CLI .
   - On KVM: Repeat the NSX Manager install on KVM steps to install three appliances, then form the cluster. See Form an NSX Manager Cluster Using the CLI .
5 Configure a VIP for the Global Manager cluster.

   See Configure a Virtual IP Address for a Cluster.
6 In a different location, install a standby Global Manager appliance and form a cluster by repeating these steps.

What to do next

Select the designated Global Manager appliance as active and connect it with the standby Global Manager.

Make the Global Manager Active and Add Standby Global Manager

After you have deployed a Global Manager appliance, you can make the Global Manager active.

Adding a standby Global Manager is optional but recommended for high availability of the Global Manager.

Procedure

1 Log in to the 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**.

3 (Optional) Add a standby Global Manager cluster.

   a Install a new Global Manager appliance in a secondary location and start it. Follow the same instructions as for installing the primary Global Manager, see Install the Active and Standby Global Manager .

   b From the active Global Manager, add this newly installed Global Manager appliance as standby.

   Navigate back to your active Global Manager and click **Add Standby** and provide the following information:

Option	Description
Global Manager Name	Provide a name for the standby Global Manager.
FQDN/IP	Enter the FQDN or IP address of the Global Manager cluster VIP at the secondary location. Do not enter an individual Global Manager FQDN or IP.
Username and Password	Provide the admin user's credentials for the Global Manager at the secondary location.

SHA-256 Thumbprint	Log in to any Global Manager node at the secondary location and run this command:
	`get certificate cluster thumbprint`
	The result is the cluster VIP certificate:
	`bfae1a0a...`
	If the GM-Standby is a single Manager VM, use the same command.

Check Compatibility	Click **Check Compatibility** to ensure that the Global Manager can be added as standby. This checks that the NSX-T Data Center version is compatible.

c Click **Save**.

d Click **Make Standby**.

Add a Location

After you add a location to Global Manager, you can create objects from Global Manager that span that location.

You can find the number of supported locations in the VMware Configuration Maximums tool. Select the appropriate version of NSX-T Data Center, select the NSX Federation category, and click **View Limits**.

Only use the admin account credentials to register the Local Manager with the Global Manager.

After you add a location to the Global Manager, the NSX Manager is called a Local Manager (LM).

Prerequisites

- Verify that the NSX-T Data Center environment you are adding has the latest version of NSX-T Data Center installed.

  This new NSX-T Data Center location can be a new NSX-T Data Center environment or an NSX-T Data Center environment with an existing Network and Security configuration.
- The NSX-T Data Center environment in the new location must have three NSX Manager nodes deployed and a cluster VIP configured. See Configure a Virtual IP 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.
- Verify that the latency between the Global Manager and the location is 500 ms or less for non-stretched networks or 150 ms or less for stretched networks.

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. 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. Do not use any other account to register the Local Manager with the Global Manager.

Option	Description

SHA-256 Thumbprint	Log in to any NSX Manager node in the cluster and run this command:
	`get certificate cluster thumbprint`
	The result is the cluster VIP certificate:
	`bfae1a0a...`

Check Compatibility	Click **Check Compatibility** to ensure that the location can be added. This checks that the NSX-T Data Center version is compatible.

What to do next

If you want to create gateways and segments that span more than one location, you must configure a remote tunnel endpoint (RTEP) on Edge nodes in each location to handle the cross-location traffic. See Configure Edge Nodes for Stretched Networking. After you add a location to your Global Manager, you can import your configurations from that location's Local Manager appliance into the Global Manager. See Importing Configurations from Local Manager.

Importing Configurations from Local Manager

Starting with NSX-T Data Center 3.2.1, after you successfully add a Local Manager location to the Global Manager, you can import all network and security Local Manager configurations to the Global Manager. This feature was temporarily unavailable in NSX-T Data Center 3.2.0 only.

You can only import the entire Local Manager configuration into the Global Manager. There is no support for partial configuration import. You can only import the configurations once.

Local Manager **Configurations supported for importing into** Global Manager

- Context Profiles
- DHCP
- DNS
- Firewall Security Policies
- Gateway Profiles
- Groups
- NAT
- Security Profiles
- Services
- T0 Gateway
- T1 Gateway
- Time-based firewall (import/onboard now supported)

Local Manager **Configurations not supported for importing into** Global Manager

The following features are not supported with NSX Federation. Import of configurations into the Global Manager is blocked if you have any of these configurations in your Local Manager. You must remove unsupported configurations to proceed with importing. After your supported Local Manager configurations are successfully imported into Global Manager, you can add the configurations for any of the unsupported features back into your Local Manager.

- DHCP dynamic binding
- Distributed IDS
- Distributed security for vCenter VDS Port Group only (Global Manager does not see the vCenter VDS port groups to assign them in security groups. However, Global Manager can use dynamic membership in groups based on vCenter VDS port groups tags added by Local Managers.)
- Endpoint protection
- Forwarding policies
- Guest introspection
- Identity firewall
- IDS/IPS
- L2 Bridge
- Load balancer
- Malware prevention
- Metadata proxy
- Multicast
- Network detection and response
- Network introspection
- Routing protocols (OSPF)
- Routing VPN and EVPN
- Service insertion
- T0 VRF
- TLS inspection
- URL filtering

Note If you use a load balancer in the Local Manager, you cannot import the load balancer, but you can still import other configurations if you meet certain conditions as described in the section titled **Importing Configurations if you have a Load Balancer service on the** Local Manager.

Importing Configurations if you have a Load Balancer service on the Local Manager

If your Local Manager has a load balancer service, you can import configurations except the load balancer, if you meet the following conditions:

- The load balancer service must be in one-arm mode on a standalone tier-1 gateway.
- The standalone tier-1 gateway that the one-arm load balancer is attached to:
  - must have only the load balancer service and no other services
  - must not have any downlink segments
  - must not share Gateway Firewall rules with any other tier-0 or tier-1 gateways.
- Groups used in load balancer service must not be used in any firewall rules. If you have groups common to both load balancer and firewall rules, you must either remove the group from the firewall rule or create an identical group to use with the load balancer.

Configurations created by a Principal Identity user in Local Manager

If you have configurations in the Local Manager that are created by the Principal Identity user and the same Principal Identity user is not present in the Global Manager, import is blocked.

You have the following options for importing these entities:

- The system displays a list of Principal Identity usernames that are being used on the Local Managerr to create configurations. Create each of these Principal Identity users in the Global Manager before proceeding to import.
- If you do not want to create Principal Identity usernames in Global Manager, remove all configurations in theLocal Manager that are created using the Principal Identity username. You can then proceed with importing other configurations from the Local Manager.

Prerequisites

- The Local Manager appliance must register with the Global Manager.
- The Local Manager appliance must have a backup that you can restore in case the importing procedure fails.
- You must remove configurations for unsupported features from your Local Manager appliance. You are provided guidance in the NSX-T Data Center UI on how to resolve any importing conflicts.

Procedure

1. Log in to the Global Manager and navigate to **System > Location Manager** .
2. A system message appears for each location that has been successfully added into the Global Manager and has objects that can be imported.
3. Click **Import Now** from the system message. You can also import objects by clicking **Actions > Import** from the location tile.

4 You see a list of objects that can be imported into the Global Manager.

   a If there are naming conflicts, you can provide a prefix or suffix for configurations. The total length of the object including the prefix and suffix must not exceed 256 characters.

      The prefix or suffix gets applied to the following objects being imported:

      - Tier-0 gateway
      - Tier-1 gateway
      - Segments
      - DNS zones
      - DHCP profiles
      - Switching profiles: IPv6, VNI Pool, Gateway QoS, BFD, IPFIX
      - Security profiles: IPFIX, Flood-Protection, DNS Security, Session Timer, Context Profiles
      - L4-L7 services (all services listed under **Inventory > Services**).

      The prefix or suffix does not get applied to the inventory and the firewall objects, that is: groups, firewall policies and firewall rules, and to system-created profiles and services.

   b For other conflicts, follow the guidance provided in the UI.

Results

Global Manager owns any Local Manager objects imported into the Global Manager. These objects appear in the Local Manager with this icon:

. You can only modify these objects from the Global Manager now.

Configure Edge Nodes for Stretched Networking

If you want to create gateways and segments that span more than one location, you must configure1 a remote tunnel endpoint (RTEP) on Edge nodes in each location.

When you configure an RTEP, do it on an Edge cluster basis. All Edge nodes in the cluster must have an RTEP configured. You do not need to configure all Edge clusters with RTEP. RTEPs are required only if the Edge cluster is used to configure a gateway that spans more than one location.

You can configure the TEP and RTEP to use the same physical NIC on the Edge node or use separate physical NICs.

You can also configure RTEPs from each Local Manager. Select **System > Get Started > Configure Remote Tunnel Endpoint**.

You can edit RTEPs on an Edge node. Log into the Local Manager and select **System > Fabric > Nodes > Edge Transport Nodes**. Select an Edge node, and click **Tunnels**. If an RTEP is configured, it is displayed in the **Remote Tunnel Endpoint** section. Click **Edit** to modify the RTEP configuration.

Prerequisites

- Verify that each location participating in the stretched network has at least one Edge cluster.
- Determine which layer 3 networks and VLANs to use for RTEP networks.
  - Intra-location tunnel endpoints (TEP) and inter-location tunnel endpoints (RTEP) must use separate VLANs and layer 3 subnets.
- Verify that all RTEP networks used in a given NSX Federation environment have IP connectivity to each other.
- Verify that external firewalls allow cross-location RTEP tunnels, and BGP sessions between Edges. See VMware Ports and Protocols at https://ports.vmware.com/home/NSX.
- Configure the MTU for RTEP on each Local Manager. The default is 1500. Set the RTEP MTU to be as high as your physical network supports. On each Local Manager, select **System > Fabric > Settings**. Click **Edit** next to **Remote Tunnel Endpoint**.

Procedure

1. From your browser, log in with admin privileges to the active Global Manager at https://<global-manager-ip-address>.
2. Go to **SystemLocal Manager** and click **Networking** from the location you want to configure for stretched networking.
3. Click **Configure** next to the Edge cluster for which you want to set up the RTEP.

   The **Configure Edge Nodes for Stretched Networking** screen opens in the Local Manager with that Edge cluster selected.
4. You can select all Edge Nodes in this cluster or one node at a time. Provide the following details for the RTEP configuration:

Option	Description
Host Switch	Select a host switch from the drop-down menu.
Teaming Policy	Select a teaming policy if you have one configured.
RTEP VLAN	Enter the VLAN ID for the RTEP network. Valid values are between 1 and 4094.
IP Pool for all nodes	Select an IP pool for all nodes in this Edge Cluster. If you want to assign an IP address to an individual node, you can edit the RTEP configuration later.
Inter Location MTU	The default is 1500.

5. Click **Save**.

   You can click each of the Edge nodes that are marked as Configured to see the Edge node configuration details. Select the **Tunnels** tab to view and edit the RTEP configuration.

Remove a Location

Removing a location from the Global Manager removes all objects created from the Global Manager that have a Global scope and are not specific to this location.

Removing a location is disruptive.

All configurations created by the Global Manager that are not specific to this location, such as groups and firewall sections with a Global scope, will be removed from the NSX Manager at this location.

Prerequisites

Before you remove a location, you must delete all objects created from the Global Manager that are specific to this location, such as tier-0 gateway, or firewall policies.

Procedure

1. Log in to the Global Manager at https://global-manager-ip-or-fqdn/.
2. Navigate to **System > Location Manager**.
3. From the location that you want to remove, click **Actions > Remove**.

   You see a message describing the effect of removing a location. If you have not previously removed objects created from the Global Manager that are specific to this location, such as tier-0 gateways or firewall policies, you cannot remove the location. The system automatically removes all other configurations from the NSX Manager at this location, that have a Global scope in your NSX Federation deployment.

Remove a Location When the Global Manager is Unavailable

This procedure is used only if the Global Manager has been deleted **BEFORE** the Local Managers (LM) are aware of its deletion.

This is a possible use case at the completion of a Federation test. In this case, the LM will constantly try to connect to its configured Global Manager (which has been deleted), and share with other Local Managers its stretch GM group members. The API calls will remove the Global Manager constructs on each LM, even when the GM has been deleted.

The below API calls on the Local Manager, will remove the Local Manager, its registration to the Global Manager, and its registration to other Local Managers.

Note The following API calls done on the Local Manager are disruptive.

All configurations created by the Global Manager that are not specific to this location, such as groups and firewall sections with a Global scope, will be removed from the NSX Manager at this location.

Procedure

1. To remove a Global Manager that is active, a Global Manager that is standby, and other Local Managers registrations from the Local Manager use the site manager API (at the Local Manager) `POST https://<LM>/api/v1/sites?action=offboard_local..`
2. To remove Global Manager objects from a Local Manager, run the Local Manager API (at the Local Manager) `POST https://<LM>/policy/api/v1/infra/site?action=offboard`.
3. (Optional) The offboarding progress can be monitored by using the API call `GET https://<LM>/policy/api/v1/infra/site/offboarding-status`.

Results

Install NSX Advanced Load Balancer Appliance Cluster

15

Install three NSX Advanced Load Balancer appliances to form a management cluster. This cluster provides management function to virtual services, profiles, pools and pool groups that you configure for NSX Advanced Load Balancer.

Prerequisites

- Supported Avi controller versions: 20.1.7, 21.1.2 or later versions
- Obtain IP addresses needed to install an appliance:
  - Virtual IP of NSX Advanced Load Balancer appliance cluster
  - Management IP address
  - Management gateway IP address
  - DNS server IP address
- Cluster VIP and all controllers management network must be in same subnet.

Procedure

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

   Note You must log in with enterprise privileges. You cannot install **NSX Advanced Load Balancer** controller nodes with only load balancer privileges.

2. Select **System > Appliances > NSX Advanced Load Balancer**.
3. Before you start deployment, set a virtual IP for the NSX Advanced Load Balancer appliance cluster.
4. Click **Set Virtual IP** and enter the VIP for the cluster. It is mandatory to set a VIP for the cluster.

   Note Verify that the virtual IP address you set is correct. If you set an incorrect cluster virtual IP address, then NSX Manager, API clients and end users cannot access the NSX Advanced Load Balancer controller. The only workaround is to delete all appliances and reconfigure the cluster with correct virtual IP address before proceeding with deployment.

5. Click **Save**.

6 To enter deployment parameters for the first NSX Advanced Load Balancer appliance, click the **Add NSX Advanced Load Balancer** card.

7 In Add Appliance wizard, you can provide a server URL to a remote OVA build.

Field	Action
Remote OVA file	Enter URL of the server where the OVA build is stored.

Note OVA upload can fail if the OVA file version being uploaded is different from the already deployed OVA files. For example, the second or third OVA deployment version is different from the first OVA deployment.

8 Click **Upload**.

9 On the Add Appliance window, configure these fields:

Field	Description
Hostname	Enter a valid hostname for the appliance. To enter a hostname that resolves to a FQDN, contact the DNS owner.
Management IP/Netmask	Enter a static IP address for the management IP address and netmask. For example, 192.168.1.2/22
Management Gateway	Enter a static IP address for the management gateway. The management gateway is used by NSX Advanced Load Balancer controller to communicate with NSX Manager and other NSX-T objects.
DNS Server	Enter the IP address of the DNS server.
NTP Server	Enter the IP address of the NTP server.
Node Size	Select the node size you want to deploy based on the requirements of your network. Supported node sizes are: ■ Small: 8 vCPU, 24 GB RAM, 128 GB storage ■ Medium: 16 vCPU, 32 GB RAM, 256 GB storage ■ Large: 24 vCPU, 48 GB RAM, 512 GB storage

10 Click **Next**.

11 On the Configuration window, configure these fields:

Field	Description
Compute Manager	Select a compute manager that registers the appliance.
Compute Cluster	Select a compute cluster where appliance will be deployed.
Resource Pool	(Optional) Select a resource pool that will be used during appliance deployment.
Host	Select a host where appliance will be deployed. **Note** Select either a host or a resource pool as storage location for deployment.

Field	Description
Datastore	Select a datastore that will be provide storage capacity for appliance.
Virtual Disk Format	By default, the Thin Provision format is selected. However, you can select a format that is feasible in your environment.
Network	Click **Select Network** to select the port group that will provide network connectivity to the appliance.

Note If incorrect compute manager details are provided, deployment fails. As a workaround, you must force delete the deployment and redeploy the appliance by providing the correct compute manager details.

12 Click **Next**.

13 On the Access & Credentials window, enter an admin password that complies with the required complexity.

Important Enter the same password when deploying all the controllers.

14 (Optional) In the **SSH Key** field, enter the private key of the SSH key pair to access controller using SSH key.

15 Click **Install Appliance**.

Do not try to delete the controller when NSX-T is registering the controller.

16 Follow steps 1-14 to deploy the second and third appliance.

Note Cluster formation only happens after the third appliance is deployed.

17 If clustering fails on the deployed controller nodes, the **NSX Advanced Load Balancer** displays an error message. Click **Start Clustering** to retrigger clustering of the deployed controller nodes. If clustering still fails, force delete the controller and reinstall it again.

NSX-T forms a cluster of the deployed controller nodes.

Results

NSX Advanced Load Balancer appliance cluster is deployed and status is `Stable`.

Example:

What to do next

For troubleshooting installation issues related to NSX Advanced Load Balancer appliance cluster, see Troubleshooting NSX Advanced Load Balancer Controller Issues.

After successfully deploying NSX Advanced Load Balancer appliance cluster, configure a NSX-T Cloud Connector in the AVI UI and then configure virtual services that will load balance traffic across servers.

Troubleshooting NSX Advanced Load Balancer Controller Issues

Troubleshoot issues when installing NSX Advanced Load Balancer controller.

NSX Advanced Load Balancer does not register with NSX Manager

Problem

Registration with compute manager failed.

Cause

If the status of deployment is '`VM registration in progress`' and the appliance does not register even after 45 min, registration has failed.

Solution

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

   System > Appliances > NSX Advanced Load Balancer
3. Click **Actions** and click **Delete**.
4. Re-deploy the appliance.

The Second NSX Advanced Load Balancer Controller Remains in Queued State

Problem

After initiating deployment of second controller, its status shows as `Controller VM Deployment Queued`

Cause

The second NSX Advanced Load Balancer controller remains in queued state till the third controller is deployed.

Solution

1. To retrieve controller deployments that are in pending state, run the following API command:

   `https://<NSX-Manager-IP-Address>/api/v1/alb/controller-nodes/deployments?state=PENDING`

   Deployment of the second appliance begins only when you initiate deployment of the third appliance. Till then, the deployment status of the second appliance remains in queued state.

2 To retrieve status of deployments, run the following API command:

```
https://<NSX-Manager-IP-Address>/api/v1/alb/controller-nodes/deployments
```

3 To retrieve controller deployments that are in deployed state, run the following API command:

```
https://<NSX-Manager-IP-Address>/api/v1/alb/controller-nodes/deployments?state=DEPLOYED
```

NSX Advanced Load Balancer Controller Password Change Caused Cluster Failure

Problem

NSX Advanced Load Balancer cluster failed because controller password was changed.

Cause

If you changed password of the leader controller outside of NSX-T, then NSX Advanced Load Balancer cluster goes into failed state. During the password change, if another node was made the leader, then the original leader node loses all its configured objects.

Solution

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

2 Update the password in NSX-T.

3 On the failed controller nodes, click **Start Clustering**.

4 If clustering still fails, delete the controller. Go to

System > Appliances > NSX Advanced Load Balancer

5 Click **Actions** and click **Delete**.

6 Re-deploy the appliance.

Unable to Delete NSX Advanced Load Balancer Controller

Problem

Unable to delete NSX Advanced Load Balancer controller.

Cause

If NSX Advanced Load Balancer objects exist and there is only one node left, NSX-T does not allow you to delete all the deployed NSX Advanced Load Balancer controller nodes. This issue occurred because NSX-T cannot access the node or you manually deleted the node from compute manager.

Solution

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

2 Delete all existing NSX Advanced Load Balancer objects.

3 To delete the controller, go to

System > Appliances > NSX Advanced Load Balancer

4 Click **Actions** and click **Delete** or **Force Delete**.

5 If load balancer objects are present, you cannot the delete the controller node remaining in the cluster. To delete the last controller node, run the following API command.

Note Pass the `inaccessible` flag only if NSX-T cannot access the node and it is the last node in the cluster.

```
/policy/api/v1/alb/controller-nodes/deployments/{{node_id}}?
action=delete&force_delete=true&inaccessible
```

The API command deletes the controller node but the load balancer objects still exist in the system.

NSX Advanced Load Balancer Cluster HA Status is Compromised

Problem

NSX Advanced Load Balancer cluster status shows `Cluster Up HA Compromised`.

Cause

If you deleted one or two of the three NSX Advanced Load Balancer controllers from a stable cluster or if a controller is down, then the cluster status changes from `Cluster UP HA Active (Stable)` to `Cluster Up HA Compromised (Degraded)`.

Solution

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

2 Verify all controllers are Up.

3 If you delete two nodes out of three nodes, SSH to the controller node with admin privileges and run `/opt/avi/scripts/recover_cluster.py`.

4 If the cluster still remains unstable, delete the controller and reinstall again.

Credential Mismatch After Changing NSX Advanced Load Balancer Controller Password

Problem

Credential mismatch after changing NSX Advanced Load Balancer controller password.

Cause

If you change controller password for admin user from outside of NSX-T from the Avi Vantage Platform UI, the new password does not refresh in NSX-T. Any change of password outside of NSX-T is not reflected in NSX Manager. NSX Manager does not reflect the state of the cluster.

Solution

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

2 If you changed the password outside of NSX-T, run the following API to change password.

`PUT https://<NSX-Manager-IPaddress>/api/v1/alb/controller-nodes/deployments/<node_id>`

```
{
"form_factor": "SMALL",
"user_settings": {
"admin_password": "Tilak@123456"
},
"deployment_config": {
"vc_id": "755bd5cb-3700-456c-b74e-25f5140f4a50",
"compute_id": "domain-c201",
"host_id": null,
"storage_id": "datastore-206",
"management_network_id": "network-207",
"hostname": "controller-AA",
"placement_type": "AlbControllerVsphereClusterNodeVmDeploymentConfig",
"disk_provisioning": "THIN",
"dns_servers": [
"8.8.8.8"
]
}
}
```

3 If you changed the password from NSX-T, run the following API to change password, DNS and NTP servers in NSX-T and on the NSX Advanced Load Balancer controller.

PUT https://<NSX-Manager-IPaddress>/api/v1/alb/controller-nodes/deployments/<node-ID>?running_config=true

Deployment of NSX Advanced Load Balancer Controller Failed

Problem

Deployment of NSX Advanced Load Balancer controller failed.

Cause

Deployment might fail because of a number of reasons. Some of the reasons are:

- Deployment of controller failed
- Controller failed to power on
- Controller failed to register with compute manager
- Controller failed to power off
- Controller could not be undeployed
- Connection between NSX and compute manager is broken
- Compute manager registered to controller is deleted
- Controller is deployed with a hostname that already exist in the cluster

Solution

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

   System > Appliances > NSX Advanced Load Balancer
3. Click **Actions** and click **Delete**.

Cluster Unstable After Two Controllers Are Down

Problem

A cluster becomes unstable after two NSX Advanced Load Balancer controllers go down.

Cause

When a three node cluster loses two controllers, the cluster quorum is lost. It becomes unstable.

Solution

1. Open a SSH session and log in to the controller that is up and running.
2. At the terminal, run the `/opt/avi/scripts/recover_cluster.py` script.
3. Verify the VIP of cluster is back up and the cluster status is stable.

Getting Started with NSX Cloud

16

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.

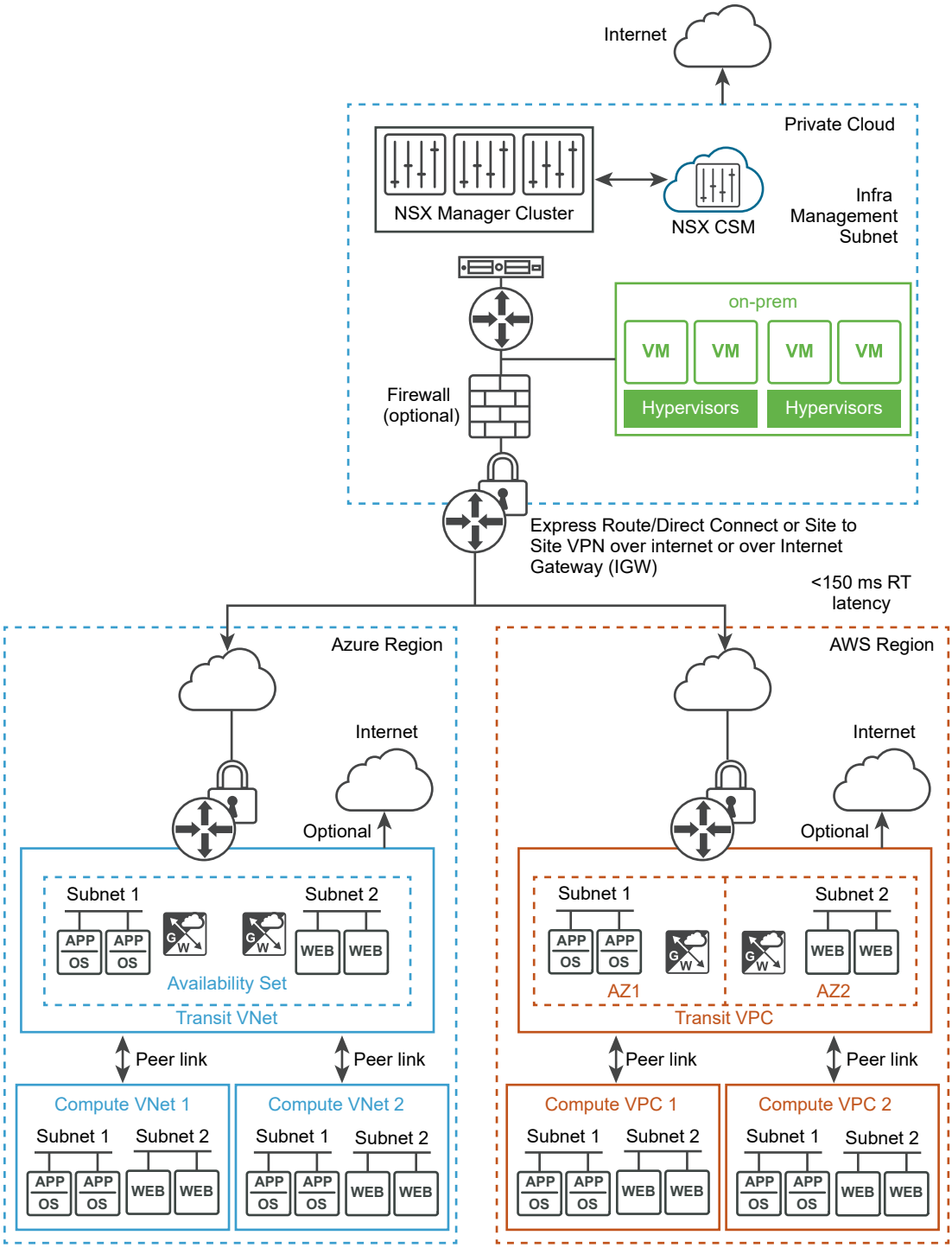
Read the following topics next:

- NSX Cloud Architecture and Components
- Overview of Deploying NSX Cloud
- Deploy NSX-T Data Center On-Prem Components
- Deploy NSX Cloud Components in Microsoft Azure using the NSX Cloud Marketplace Image
- Add your Public Cloud Account
- NSX Public Cloud Gateway: Architecture and Modes of Deployment
- Deploy PCG or Link to a PCG
- Auto-Configurations after PCG Deployment or Linking
- Integrate Horizon Cloud Service with NSX Cloud
- (Optional) Install NSX Tools on your Workload VMs
- Un-deploy NSX Cloud

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 16-1. 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.

Note While planning your deployment, ensure that NSX-T Data Center appliances have good connectivity with the PCG deployed in the public cloud and Transit VPCs/VNets are in the same region as the Compute VPCs/VNets.

Table 16-1. Workflow for deploying NSX Cloud

Task	Instructions
❑ Install CSM and connect with NSX Manager. **Note** Starting in NSX-T Data Center 3.1.1, if you are using Microsoft Azure, you can deploy NSX Cloud components in your Microsoft Azure subscription. See Deploy NSX Cloud Components in Microsoft Azure using the NSX Cloud Marketplace Image.	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 NSX Public Cloud Gateway: Architecture and Modes of Deployment .
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.

Ports and Protocols

For a list of ports and protocols required for inbound and outbound access for CSM, see https://ports.vmware.com/home/NSX-T-Data-Center.

NTP Server Configuration

Many features require that CSM has a valid NTP server entry. You can configure the NTP server at the time of installing CSM or later. Also see *Configuring NTP on Appliances and Transport Nodes* in the *NSX-T Data Center Administration Guide* for other options for configuring NTP.

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.

Specify CSM IPs for Access by PCG

After CSM is deployed, run the following API to use an IP/subnet pool for CSM visible to PCG.

Whenever you run this API, CSM updates `gw-mgmt-sg` associated with the PCG in your public cloud, to append these IP addresses to allow inbound communication on PCG from CSM over these IP addresses or IP address ranges. See Auto-created Public Cloud Configurations for a list of constructs created in the public cloud after PCG is deployed.

```
PUT https://<csm-ip>/api/v1/csm/configs/system-config
```

Example Request Body where **`10.1.1.1/24`** is the IP address of CSM as seen by PCG.

```
{
  "mgmt_ip_config": [
    "10.1.1.1/24",
    "192.168.0.0/24"
  ]
}
```

(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.

Connect your Public Cloud with On-prem NSX-T Data Center

Connect your public cloud account with the on-prem deployment of NSX-T Data Center,

Connect VPCs/VNets with on-prem using suitable methods, such as Direct Connect for AWS or Express Route for Microsoft Azure. You can also use site-to-site VPN with any VPN endpoint on-prem and PCG acting as the VPN endpoint in your public cloud.

To use the Transit/Compute topology, you must have peering connections established between the Transit and Compute VPCs/VNets. You can have a single PCG manage multiple compute VPCs/VNets. You can also have a flat compute VPC/VNet architecture with a PCG pair installed in each VPC/VNet. See NSX Public Cloud Gateway: Architecture and Modes of Deployment for details on PCG deployment options.

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 NSX Public Cloud Gateway: Architecture and Modes of Deployment for details on how these subnets are used.

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 NSX Public Cloud Gateway: Architecture and Modes of Deployment 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.

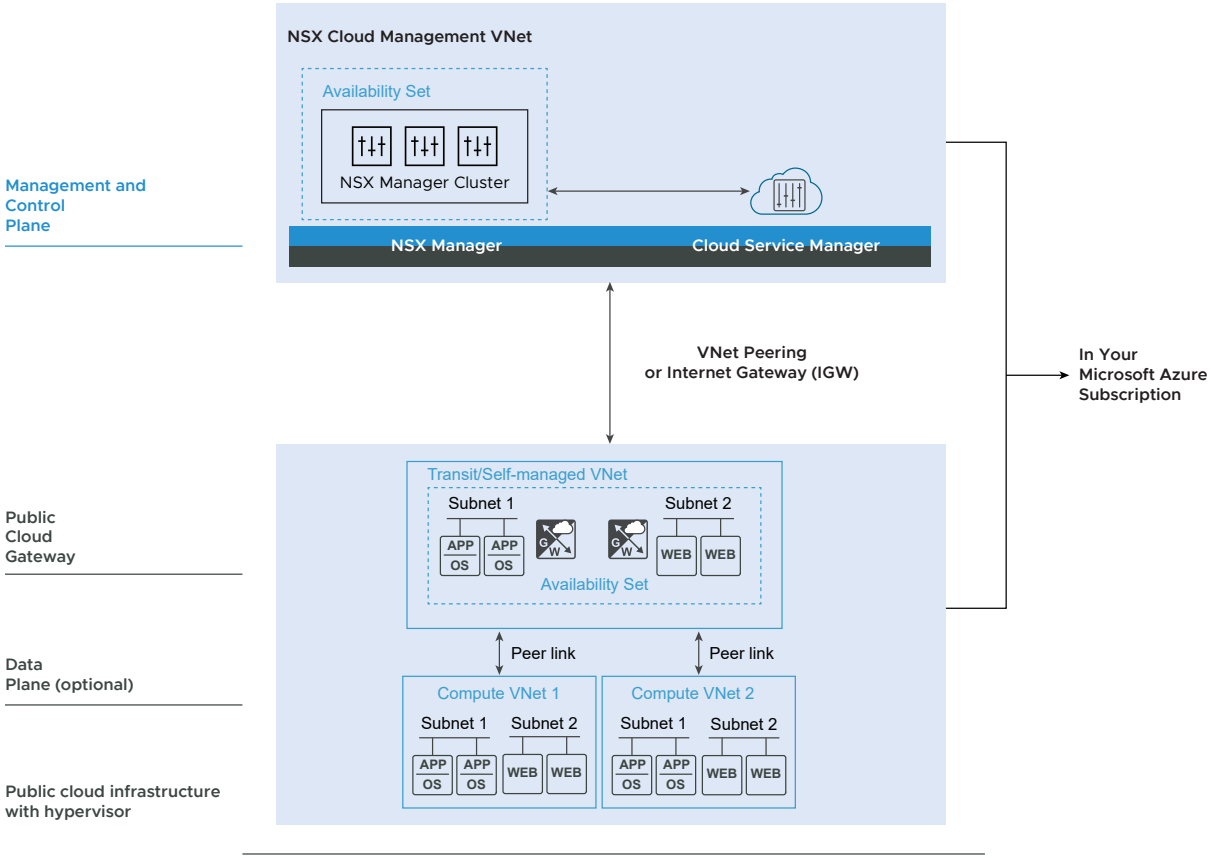
Deploy NSX Cloud Components in Microsoft Azure using the NSX Cloud Marketplace Image

Starting in version 3.1.1, you can use the Terraform scripts to deploy management components – NSX Manager and CSM – within your Microsoft Azure subscription.

provides Terraform scripts that deploy components in your Microsoft subscription. See Deploy NSX Cloud Components in Microsoft Azure using Terraform scripts.

If you cannot use Terraform scripts to deploy components, you can also manually deploy them in your Microsoft Azure subscription. See Deploy NSX Cloud Components in Microsoft Azure without using Terraform scripts.

Figure 16-2. NSX Cloud Components Deployed in Microsoft Azure



Accepting Azure Marketplace Terms

As the NSX Cloud images are published at the Azure Marketplace, you must first accept the legal terms for the images.

To accept the terms, you can use the PowerShell command. For details, see https://docs.microsoft.com/en-us/powershell/module/az.marketplaceordering/set-azmarketplaceterms?view=azps-6.2.0.

Use the following values for the PowerShell command. Note that the product value is based on the marketplace image.

Parameter	Description
Publisher	vmware-inc
Name	byol_release-3-1
Product For Public Cloud Gateway (PCG)	nsx-public-cloud-gateway

Parameter	Description
Product For Management Plane (MP)	nsx-policy-manager
Product For Cloud Service Manager (CSM)	nsx-cloud-service-manager

Following is an example for accepting terms for CSM using the PowerShell command:

```
Set-AzMarketplaceTerms -Publisher "vmware-inc" -Product "nsx-cloud-service-manager" -Name
"byol_release-3-1" -Terms $agreementTerms -Accept
```

Deploy NSX Cloud Components in Microsoft Azure using Terraform scripts

Follow these steps to deploy NSX Cloud using the NSX Cloud Marketplace image in Microsoft Azure using the Terraform scripts provided by NSX Cloud.

Prerequisites

- Verify that you have access to the NSX Cloud Marketplace image in your Microsoft subscription.
- Verify that you have accepted Microsoft Azure's Marketplace legal terms in the subscription where you are deploying NSX cloud appliances.
- You must have Microsoft Azure CLI installed and configured on the system. This is required for authenticating and running Azure APIs that are used in the Terraform scripts.

  If possible, use the same system to run the Terraform scripts that you use to access your Microsoft subscription from. This ensure that your Microsoft Azure credentials can be used from within the system and you do not have share this information with a different system.

  Also, as a security recommendation, run these scripts on a Linux/Unix or macOS system that supports the Python crypt module.
- Verify that you have binaries of Terraform 0.13 or higher on the system where you plan to run the Terraform scripts.
- You must have Python 3.0 or higher installed on this system.

Procedure

1. Download the Terraform scripts by logging in to your **My VMware** account and navigating to: **Products > VMware NSX-T Data Center > Drivers and Tools > VMware NSX Cloud Scripts for Adding Public Cloud Accounts for NSX 3.1.1 > Go To Downloads > Download Now**. For example, after you log in to your My VMware account, this link takes you to the Download page for Drivers and Tools.

2 Extract the contents of the file named `NSXCloudScriptsforAddingPublicCloudAccounts.tar.gz`. The Terraform scripts and related files are in the folder `NSXCloudScripts/cloud-native-deployment/azure/igw`.

3 Update the Terraform configuration files.

a In `config.auto.vars`, add the following information:

Parameter	Description
`subscription_id`	Provide the subscription ID for your Microsoft Azure account.
`location`	Specify the Microsoft Azure location that the NSX Cloud Management VNet will be deployed in.
`deployment_prefix`	This is the deployment name that will be prefixed to all auto-created entities. Ensure that this is unique for each Microsoft `subscription_id` and `location`.

b In `credentials_nsx.auto.tfvars`, add the following information:

Parameter	Description
`mgr_public_key_path`	This is the path to the public key to be applied to the NSX Manager appliance.
`csm_public_key_path`	This is the path to the public key to be applied to the CSM appliance.
`license_key`	This is the license key for NSX Manager. You must have the NSX Data Center Enterprise Plus license.

c Verify advanced configuration information, and update as necessary, in the file `advanced_config.auto.tfvars`:

Parameter	Description
`mgmt_vnet_address_space`	This is the address space for the newly deployed NSX Cloud Management VNet.
`mgmt_subnet_address_prefix`	This is the subnet for the NSX Cloud management appliances deployed in the NSX Cloud Management VNet.

4 Run the following commands in the specified order:

`~/terraform init`	This command collects all the modules required for deployment.
`~/terraform plan`	This command displays the list of steps or a blueprint of the procedure involved in the deployment.
`~/terraform apply`	This command executes the script. If something goes wrong during execution, you are shown the corresponding error messages. After you fix the errors, you can resume the deployment from where it stopped.

5 Follow these steps to change the passwords generated for NSX Manager and CSM by the Terraform scripts.

a After the scripts run successfully, make a note of the following passwords for NSX Manager and CSM:

- `admin_password`
- `root_password`

These passwords are displayed on the screen at the end of the deployment. You can also find these passwords in the file `NSXCloudScripts/cloud-native-deployment/azure/igw/terraform.tfstate`, under the section `"outputs"`, for example:

```
"outputs": {
  "csm": {
    "value": {
      "admin_password": "<pwd>",
      "admin_username": "nsxadmin",
      "private_ip": "<private IP>",
      "public_ip": "<public IP>",
      "root_password": "<pwd>"
    },
  "mgrs": {
    "value": [
      {
        "admin_password": "<pwd>",
        "admin_username": "nsxadmin",
        "private_ip": "<private IP",
        "public_ip": "<public IP>",
        "root_password": "<pwd>"
      },
```

b In Microsoft Azure, navigate to the Network Security Groups created for NSX Manager and CSM, named `<deployment_prefix>-nsx-mgr-sg` and `<deployment_prefix>-nsx-csm-sg`, and add the following temporary inbound "allow" rule for SSH:

Priority	Name	Port	Protocol	Source	Destination	Action
1010	AllowInboundRuleSSH	22	TCP	Any	Any	Allow

c Log in to the NSX Manager appliance using your private key and change the password generated by the Terraform scripts:

```
$ ssh -i <nsx_mgr_key> nsxadmin@<NSX Manager public IP address>
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for nsxadmin.
(current) UNIX password: <Enter mgr_admin_pwd from the Terraform scripts>
New password: <Enter new password conforming to NSX-T Data Center password complexity>
Retype new password:
passwd: password updated successfully
```

d Log in to CSM using your private key and change the password generated by Terraform scripts:

```
$ ssh -i <nsx_csm_key> nsxadmin@<CSM public IP address>
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for nsxadmin.
(current) UNIX password: <Enter csm_admin_pwd from the Terraform scripts>
New password: <Enter new password conforming to NSX-T Data Center password complexity>
Retype new password:
passwd: password updated successfully
```

6 Log in to the CSM appliance using the new password you have set and run the following NSX CLI command to join CSM with the NSX Manager cluster:

```
join <nsx-manager-ip-address & port(optional)> cluster-id <nsx-manager-cluster-id>
username <username> password <password> thumbprint <nsx-manager-api-thumbprint> csm-
username <csm-username> csm-password <csm-password>
```

You can run the NSX CLI command `get cluster status` from any NSX Manager node to get the cluster-id. You can get the NSX Manager thumbprint by running the `get certificate api thumbprint` command on the specified NSX Manager. See the NSX-T Data Center CLI reference for details on CLI commands.

Note If the NSX Manager node that you joined the CSM appliance to is lost, you can either run this NSX CLI command to join CSM with one of the other healthy NSX Manager nodes, or you can redeploy the lost NSX Manager node using its image file named, `<deployment_prefix>nsx-mgr-image` and CSM will automatically rejoin this node when this node is back online. See *Redeploying NSX Manager from nsx_mgr_image in Microsoft Azure* in the *NSX-T Data Center Administration Guide* for details.

Results

The scripts deploy the following in your Microsoft Azure subscription:

- A VNet to host the NSX Cloud management appliances. This VNet is named `<deployment_prefix>-nsx-mgmt-vnet`.

- An Availability Set in which the three nodes of the NSX Manager cluster are deployed. This Availability Set is named `<deployment_prefix>-nsx-aset`.
- Microsoft Azure Resource Group named `<deployment_prefix>nsx-mgmt-rg`.
- The following resources for the each of the NSX Manager nodes and for the CSM appliance:
  a VMs named `<deployment_prefix>nsx-csm` for CSM, and `<deployment_prefix>nsx-mgr0`, `<deployment_prefix>nsx-mgr1` and `<deployment_prefix>nsx-mgr2` for the NSX Manager cluster.
  b OS Disk for each VM.
  c Network interface (NIC) for each VM.
  d Public IP address for each VM.
  e Data disk for each VM.
- Network Security Groups for NSX Cloud management components that allow connectivity for these appliances.
  - `<deployment_prefix>-nsx-mgr-sg`:

Table 16-2. Inbound Rules for NSX Manager deployed using the Terraform scripts

Priority	Name	Port	Protocol	Source	Destination	Action
1000	AllowInboundRuleAPI	443	TCP	Any	Any	Allow

Table 16-3. Outbound Rules for NSX Manager deployed using the Terraform scripts

Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowOutboundRuleAPI	Any	TCP	Any	Any	Allow

- `<deployment_prefix>-nsx-csm-sg`:

  Table 16-4. Inbound Rules for CSM deployed using the Terraform scripts

Priority	Name	Port	Protocol	Source	Destination	Action
1000	AllowInboundRuleAPI	443	TCP	Any	Any	Allow

  Table 16-5. Outbound Rules for CSM deployed using the Terraform scripts

Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowOutboundRuleAPI	80,443	TCP	Any	Any	Allow

  Note Consider updating the `Source` field of these auto-created network security groups to a restricted set of CIDRs from which you want to access NSX Manager and CSM. The default `Any` is not safe.

- A Microsoft Azure Recovery Service Vault with a vault policy to perform a recurring backup of all three NSX Manager nodes and the CSM appliance. The vault policy is named `<deployment_prefix>-nsx-vault` and the default backup schedule is set to: daily recurring at 11PM UTC.

  See *Managing Backup and Restore of NSX Manager and CSM in Microsoft Azure* in the *NSX-T Data Center Administration Guide* for details on restore options.

What to do next

Deploy PCG in a VNet

Deploy NSX Cloud Components in Microsoft Azure without using Terraform scripts

Follow these steps to manually deploy NSX Cloud components in Microsoft Azure using the Microsoft Azure marketplace image, without using Terraform scripts provided by NSX Cloud.

The following steps are performed in your Microsoft Azure subscription:

1 Create a resource group for NSX Cloud management resources with a descriptive name, for example, **`nsx-mgmt-rg`**.

2 In this resource group, create an availability set in which you will deploy three NSX Manager nodes.

3 In this resource group, create a VNet where you will deploy NSX Cloud management components.

4 In this VNet, create a subnet for NSX Cloud management components.

5 Create Security groups for NSX Manager and CSM appliances.

- Security groups for NSX Manager named like **`nsx-mgr-sg`**:

  Table 16-6. Inbound Rules for NSX Manager

Priority	Name	Port	Protocol	Source	Destination	Action
1000	AllowInboundRuleAPI	443	TCP	Any	Any	Allow

  Table 16-7. Outbound Rules for NSX Manager

Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowOutboundRuleAPI	Any	TCP	Any	Any	Allow

- Security groups for CSM named like **`nsx-csm-sg`**:

  Table 16-8. Inbound Rules for CSM

Priority	Name	Port	Protocol	Source	Destination	Action
1000	AllowInboundRuleAPI	443	TCP	Any	Any	Allow

  Table 16-9. Outbound Rules for CSM

Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowOutboundRuleAPI	80,443	TCP	Any	Any	Allow

6 Deploy one CSM VM using the CSM marketplace image URN with a public IP address. Use the following configurations as specified. For all other configurations you can select the default values or the best options for your requirements.

Parameter	Value
	Basic
Virtual machine name	Any descriptive name.
Size	The minimum requirement is: Standard_D4s_v3-4vcpus, 16 GB memory.
Authentication type	SSH
Username	Enter the default NSX Manager username: `nsxadmin`.
SSH Public Key Source	Provide the public key of the SSH key-pair you will use to log in to the appliance over SSH.
	Networking
Public IP	Click **Create new** and select **Static** for the **Assignment** option.

Parameter	Value
NIC network security group	Select **Advanced**
Configure network security group	Select the network security group created for CSM, for example, **`nsx-csm-sg`** as described in an earlier step.
	Advanced

Custom data	Copy-paste the following, ensuring that you use your deployment's username and password:
	`#cloud-config`
	`hostname: <hostname>`
	`chpasswd:`
	`expire: false`
	`list:`
	`- nsxadmin:<admin_password>`
	`- root:<root_password>`
	For example:
	`#cloud-config`
	`hostname: nsx-datacenter1-csm`
	`chpasswd:`
	`expire: false`
	`list:`
	`- nsxadmin:MySecretNsxAdminPassword`
	`- root:MySecretNsxRootPassword`

7 Deploy three NSX Manager VMs using the NSX Manager marketplace image URN with a public IP address. Use the following configurations as specified. For all other configurations you can select the default values or the best options for your requirements.

Parameter	Value
	Basic
Virtual machine name	Any descriptive name.
Size	The minimum requirement is: Standard_D4s_v3-4vcpus, 16 GB memory.
Authentication type	SSH
Username	Enter the default NSX Manager username: `nsxadmin`.
SSH Public Key Source	Provide the public key of the SSH key-pair you will use to log in to the appliance over SSH.
	Disks
OS Disk type	Standard HDD
Data disks	Click **Create and attach a new disk** and select **Standard HDD.** for **Disk SKU** with a custom size of `100 GiB`. **Note** Ensure that the data disk host caching is set to read/write.
	Networking

Parameter	Value
Public IP	Click **Create new** and select **Static** for the **Assignment** option.
NIC network security group	Select **Advanced**
Configure network security group	Select the network security group created in a previous step, from the example in this topic: `nsx-mgr-sg`
	Advanced

Custom data	Copy-paste the following, ensuring that you use your deployment's username and password:
	`#cloud-config`
	`hostname: <hostname>`
	`bootcmd:`
	`- [cloud-init-per, instance, lvmdiskscan, lvmdiskscan]`
	`- [cloud-init-per, instance, secondary_partition, /opt/vmware/nsx-node-api/bin/set_secondary_partition.sh]`
	`chpasswd:`
	`expire: false`
	`list:`
	`- nsxadmin:<admin_password>`
	`- root:<root_password>`

8 Configure a Microsoft Azure Recovery Service Vault with a vault policy to perform a recurring backup of all three NSX Manager nodes and the CSM appliance. For example, you could use this policy named **`nsx-vault`** and the default backup schedule set to daily recurring at 11PM UTC.

See *Managing Backup and Restore of NSX Manager and CSM in Microsoft Azure* in the *NSX-T Data Center Administration Guide* for details on restore options.

9 Add a temporary network security group to allow SSH access for NSX Manager and CSM.

Table 16-10. Temporary rule for both NSX Manager and CSM to allow SSH access

Priority	Name	Port	Protocol	Source	Destination	Action
1010	AllowInboundRuleSSH	22	TCP	Any	Any	Allow

10 Log in to the NSX Manager and CSM appliances using your private key and the passwords you provided in user data when launching the VMs.

11 Create an NSX Manager cluster with the three NSX Manager nodes deployed. See Form an NSX Manager Cluster Using the CLI .

12 Add an NSX-T Data Center license:

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

b Select **System > Licenses > Add License**.

c Enter a license key. You must have the NSX-T Data Center Enterprise Plus license.

13 Log in to the CSM appliance and run the following NSX-T Data Center CLI command to join CSM with the NSX Manager cluster:

```
join <nsx-manager-ip-address & port(optional)> cluster-id <nsx-manager-ip-address>
username <username> password <password> thumbprint <nsx-manager-api-thumbprint> csm-
username <csm-username> csm-password <csm-password>
```

Add your Public Cloud Account

Create roles with appropriate permissions in your public cloud account to add the account into CSM.

Overview

For each public cloud account that you want to bring under the control of NSX-T Data Center, you have the option of creating appropriate roles with appropriate permissions. NSX Cloud provides scripts that you can use to generate these roles.

If you want to restrict public clouds that can be added into CSM, run the following CSM API:

```
PUT /api/v1/csm/desired-clouds

Example Request:
PUT https://<nsx-csm>/api/v1/csm/desired-clouds
{
  "cloud_types": [
    {
        "cloud_type": "aws"
        "enabled": true,
    }
    {
        "cloud_type": "azure",
        "enabled": true,
    }
    {
        "cloud_type": "aws-gov-us-east"
        "enabled": false,
    }
    {
        "cloud_type": "aws-gov-us-west",
        "enabled": false,
    }
    {
        "cloud_type": "azure-gov-us",
        "enabled": false,
    }
  ]
}
```

See the latest version of the *NSX-T Data Center API Guide* at https://code.vmware.com/ for API details.

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. If you have the new Azure Powershell Az module, you must run the `Enable-AzureRmAlias` command to ensure that the AzureRM cmdlets for NSX Cloud run successfully .
- 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>`

Script/File	Description
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 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 (Optional) If you have a brownfield deployment, mark all the VMs as **User Managed** in the VNet where you want VMs managed to prevent automatic security group assignment under the Quarantine Policy.

6 (Optional) Manage access to regions. See Managing Regions in CSM.

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 primary 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 NSX Public Cloud Gateway: Architecture and Modes of Deployment 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 primary AWS account.

  a Run the script from your AWS primary 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 primary 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 primary 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 NSX Public Cloud Gateway: Architecture and Modes of Deployment 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 primary 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 (Optional) If you have a brownfield deployment, mark all the VMs as **User Managed** in the VPC where you want VMs managed to prevent automatic security group assignment under the Quarantine Policy.

5 (Optional) Manage access to regions. See Managing Regions in CSM.

What to do next

Deploy PCG in a VPC

Managing Regions in CSM

For your public cloud account added in CSM, you can get a list of supported regions and restrict access to specific regions.

- To get a list of specific regions, run the following API:

```
GET https://<csm-IP>/csmapi/api/v1/csm/supported-regions
```

Note If you do not see all the available regions in your AWS account, check whether you have enabled regions in your AWS account. See AWS documentations for details on enabling regions.

- To restrict regions in Microsoft Azure, run the following API:

```
PUT https://<csm-IP>/api/v1/csm/azure/accounts/<account_id>/desired-regions

Example Request:
PUT https://<nsx-csm>/api/v1/csm/azure/accounts/9174ffd1-41b1-42d6-a28d-05c61a0698e2/
desired-regions
{
  "regions": [
    {
      "id": "westus",
      "display_name": "westus",
      "enabled": true,
    },
    {
      "id": "eastus2",
      "display_name": "eastus2",
      "enabled": false,
    }
  ]
}
```

- To restrict regions in AWS, run the following API:

```
PUT https://<csm-IP>/api/v1/csm/aws/accounts/<account_id>/desired-regions

Example Request:
PUT https://<nsx-csm>/api/v1/csm/aws/accounts/9174ffd1-41b1-42d6-a28d-05c61a0698e2/desired-regions
{
  "default_client_region": "us-east-1",
  "regions": [
    {
      "id": "us-west-2",
      "display_name": "Oregon",
      "enabled": false,
    },
    {
      "id": "us-east-1",
      "display_name": "N. Virginia",
      "enabled": true,
    }
  ]
}
```

See the latest version of the *NSX-T Data Center REST API Guide* at https://code.vmware.com/ for API details.

NSX Public Cloud Gateway: Architecture and Modes of Deployment

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`. Some regions might not support this instance type. Refer to AWS documentation for details. **Note** If you see high CPU usage alerts with this instance type, resize PCG instances to c5.2xlarge. If you have a high availability pair of PCG instances, resize the standby PCG first by stopping, resizing and restarting it. Stop the currently active PCG next and wait until the standby PCG becomes active. Resize and restart this PCG and it should become active. See AWS documentation for details on resizing instance types.
Microsoft Azure	`Standard DS3 v.2`

Architecture

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.

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-managed 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.

AWS Transit Gateway with PCG: Starting in NSX-T Data Center 3.1.1, you can use AWS Transit Gateway to connect a Transit VPC with Compute VPCs. See Using PCG with AWS Transit Gateway for details.

Subnets Required in Your VPC/VNet to deploy PCG

The PCG uses 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. Example range: /28.
- **Uplink subnet**: This subnet is used for north-south internet traffic. Example range: /24.
- **Downlink subnet**: This subnet encompasses the workload VM's IP address range. Size this subnet bearing in mind that you might need 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.

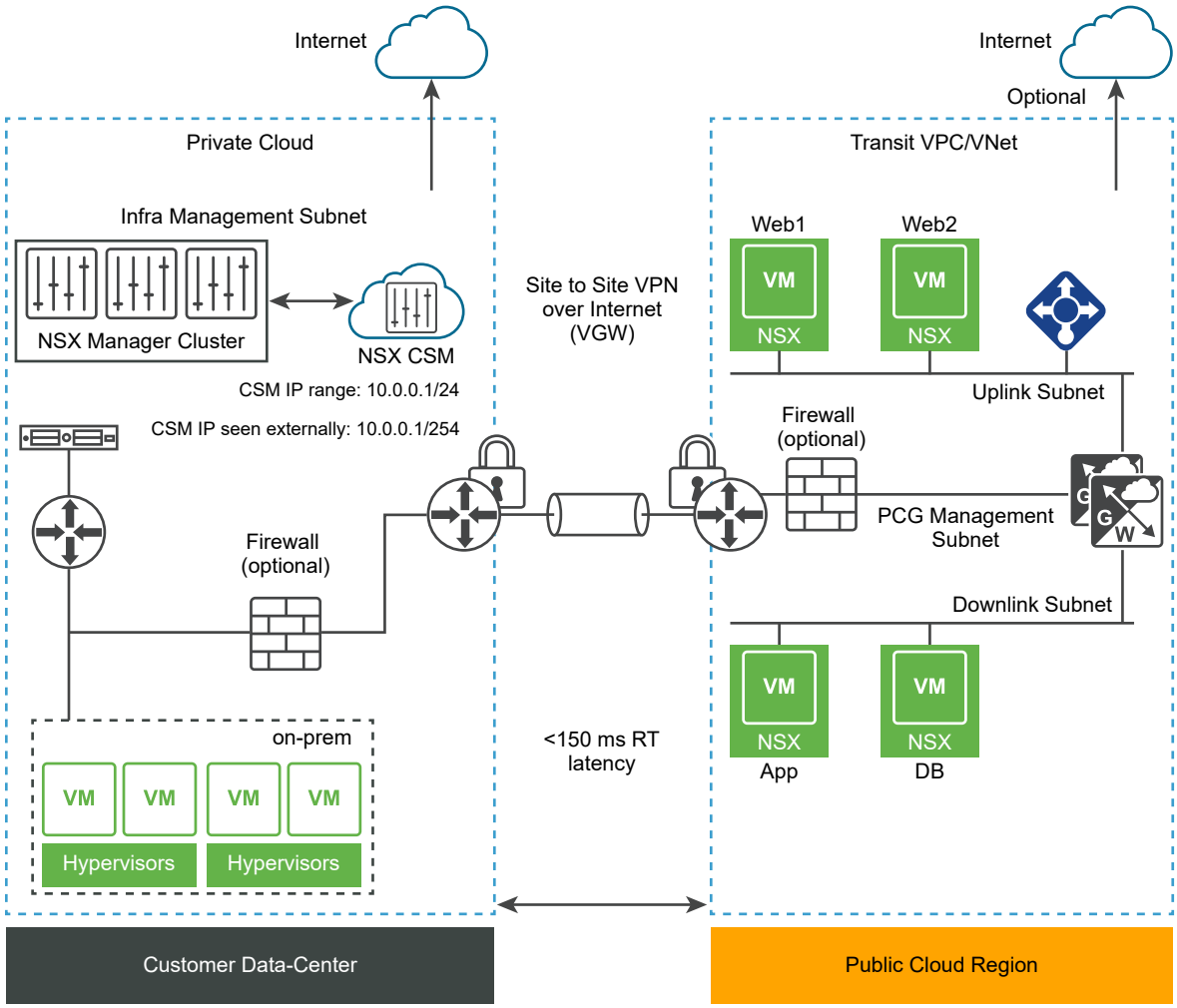
Note It is not recommended to use IP addresses for connecting the public cloud with NSX-T Data Center using PCG, but if you do, you must not change your IP addresses.

Impact of on-prem and public cloud connectivity mode on PCG's discovery of CSM

After PCG is deployed in your public cloud, it must interact with CSM as the management interface for your public cloud inventory. To ensure that PCG can reach the IP address of CSM, follow these guidelines:

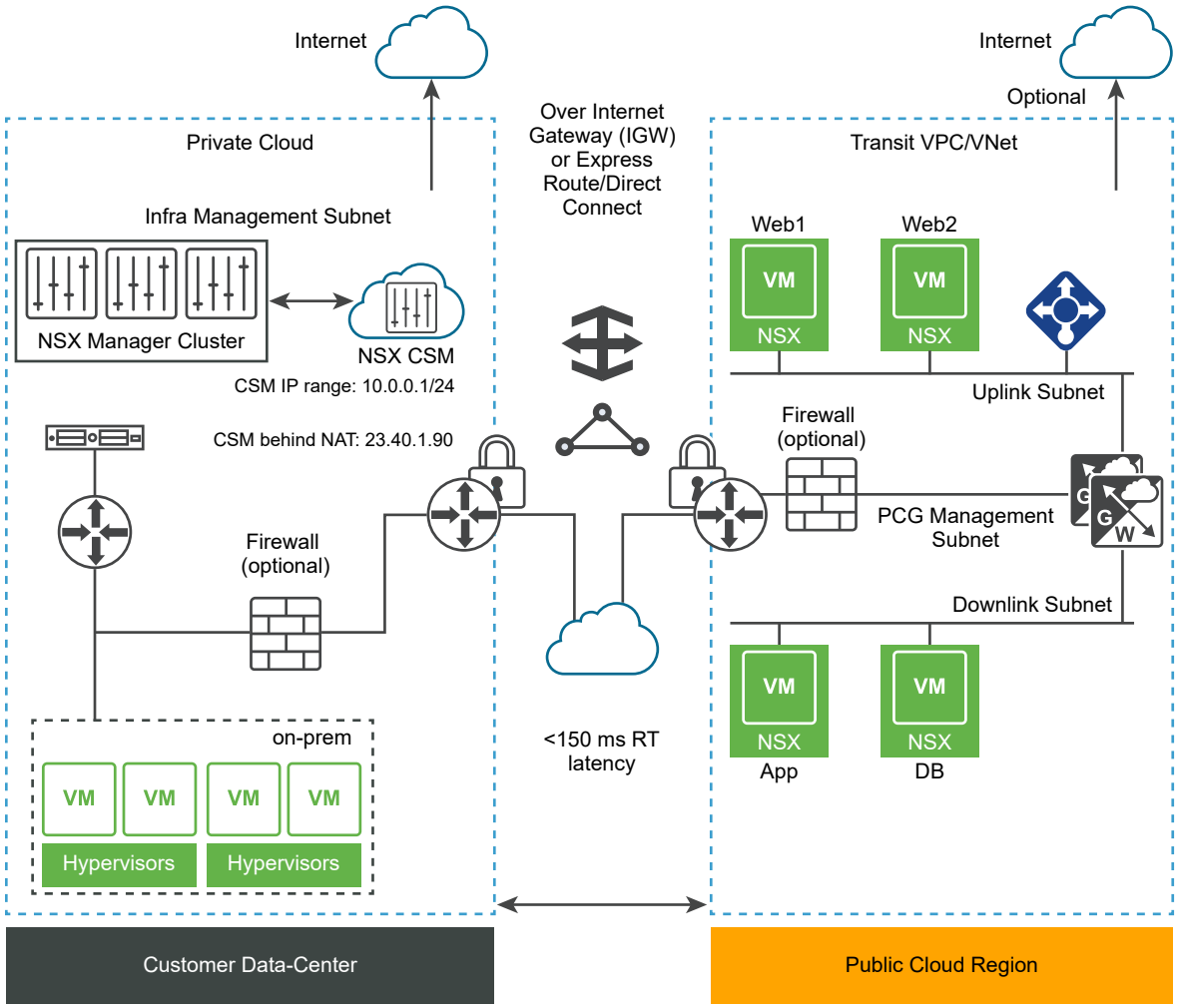
- For PCG deployed in Private IP mode (VGW): PCG discovers CSM with either the actual CSM IP address or with one of the IP addresses in the subnet range provided.

Figure 16-3. NSX Public Cloud Gateway Architecture with VGW Connectivity



- For PCG deployed in Public IP mode (IGW): PCG can discover CSM using CSM's NAT-translated IP address that allows access to the real IP address or subnet range for CSM.

Figure 16-4. NSX Public Cloud Gateway Architecture with IGW Connectivity



Modes of VM-management

NSX Enforced Mode: In this mode, workload VMs are brought under NSX management by installing NSX Tools on each workload VM to which you apply the tag **`nsx.network=default`** in your public cloud.

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: 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. As a best practice, disable Quarantine Policy and add all your VMs to the **User Managed** list when onboarding workload VMs.

- In the Native Cloud Enforced Mode Quarantine Policy is always enabled and cannot be disabled.

Design Options

Regardless of the mode you deploy the PCG in, you can link a Compute VPC/VNet to it in either mode.

Table 16-11. Design Options with PCG Deployment Modes

PCG Deployment Mode in Transit VPC/VNet	Supported Modes when linking 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.

Deploy PCG or Link to a PCG

Follow these instructions for deploying PCG or linking to a PCG.

NSX Cloud creates networking and security constructs in NSX Manager and your public cloud after PCG is deployed. See Auto-Configurations after PCG Deployment or Linking .

If you are using AWS Transit Gateway, see Using PCG with AWS Transit Gateway.

Note For Native Cloud PCG deployment, the default *admin* and *root* password is same and is set as *NSX-<instance-ID>*. The instance-ID of the AWS or Azure VM is prefixed. For example, if the instance ID is *i-0349f21e34dc27b08*, the initial password is set as *NSX-i-0349f21e34dc27b08*

The *root* password gets expired by default. If you want to access root shell of the PCG appliance, you must reset the password using the initial password which is *NSX-<instance-ID>*.

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

- If you have deployed NSX Cloud components on-prem, ensure the VNet is connected with your on-prem NSX-T Data Center.

  If you have deployed NSX Cloud components in Microsoft Azure, ensure that the VNet is peered with the NSX Cloud Management VNet. See deployment architecture details at Deploy NSX Cloud Components in Microsoft Azure using the NSX Cloud Marketplace Image.
- Verify that your Microsoft Azure subscription is added into CSM.
- Verify that you have the required subnets in the VNet where you are deploying PCG: *uplink*, *downlink*, and *management*. For High Availability, you must have an uplink subnet for the secondary PCG that is different from the primary PCG.

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.
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.
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.
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.
Gateway Connectivity Mode	The PCG can be accessed from CSM using a public IP address or a private IP address depending on the connectivity mode between your public cloud and your on-prem NSX-T Data Center installation. If you select **Auto Detect**, they system attempts to connect with CSM over VGW first, and if that fails, over IGW. If the system cannot connect with CSM, the deployment fails. See Impact of on-prem and public cloud connectivity mode on PCG's discovery of CSM for details.

Option	Description
Use Marketplace Image	This option is only available in NSX-T Data Center 3.1.1. It is enabled by default when a compatible marketplace image is available to deploy in Microsoft Azure. See Deploy NSX Cloud Components in Microsoft Azure using the NSX Cloud Marketplace Image for details.
Azure Marketplace Terms	If you are using the marketplace image to deploy PCG, you must accept Microsoft Azure terms of use. NSX Cloud provides the terms for you to download and read. Select the checkbox to accept the terms to proceed.
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.
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.

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*.

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 .

If you are using AWS Transit Gateway, see Using PCG with AWS Transit Gateway.

Prerequisites

- Ensure the VPC is connected with your on-prem NSX-T Data Center.
- Verify that your AWS account is already added into CSM.
- Verify that the VPC on which you are deploying PCG has the required subnets appropriately adjusted for High Availability: *uplink*, *downlink*, and *management*.
- Verify that the configuration for your VPC's network ACL includes 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.
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.
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.

Option	Description
Gateway Connectivity Mode	The PCG can be accessed from CSM using a public IP address or a private IP address depending on the connectivity mode between your public cloud and your on-premises NSX-T Data Center installation. If you select **Auto Detect**, they system attempts to connect with CSM over VGW first, and if that fails, over IGW. If the system cannot connect with CSM, the deployment fails. See Impact of on-prem and public cloud connectivity mode on PCG's discovery of CSM for details.
InstanceType	Select any one of the sizes from the drop-down menu list based on your requirement. There are four Intance Type sizes available: ■ Small ■ Medium ■ Large ■ Extra Large See NSX Public Cloud Gateway: Architecture and Modes of Deployment for more information on PCG instance type. **Note** You can enable Firewall features like Application ID, IDPS, and URL Enforcement only on Large and Extra Large size PCG deployment. However, in NSX-T Data Center 3.2, Firewall features are available in Tech Preview mode. Use these features only for experimental purposes and VMware does not officially provide support for these features.
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.
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.

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.

Option	Description
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*.

Using PCG with AWS Transit Gateway

If you use AWS Transit Gateway, you can deploy the PCG in any VPC and connect this VPC with the Transit Gateway.

Follow instructions at Deploy PCG in a VPC.

Any other VPCs connected to the Transit Gateway can have their workload VMs managed by NSX-T Data Center for micro-segmentation.

NSX Cloud does not manage networking between the Transit and Compute VPCs or the workload VMs. All NSX-T Data Center networking constructs are created upon PCG deployment but only the Security constructs are valid if you are working with AWS Transit Gateway. See Security Entities for a list of auto-created security policies after PCG deployment.

- Currently only NSX Enforced Mode is supported. You must install NSX Tools in your workload VMs. See *NSX Enforced Mode* in the *NSX-T Data Center Administration Guide* for instructions.
- The VPC where you deploy PCG – Transit VPC – must have the same subnets as required by a Transit VPC that is not using the AWS Transit Gateway. See Subnets Required in Your VPC/VNet to deploy PCG for details.
- You must link compute VPCs to the Transit VPC. See Link to a Transit VPC or VNet for instructions.
- You must ensure that workload VMs with NSX Tools installed on them have connectivity with the management subnet of the Transit VPC.
- To utilize micro-segmentation, you must add a Forwarding Policy with the following values:

Option	Value
Sources	A Group in NSX Manager that contains all NSX-Managed VMs from your Transit and Compute VPCs
Destinations	All (0.0.0.0/0)

Option	Value
Services	Any
Action	Route to Underlay

See *Add or Edit Forwarding Policies* in the *NSX-T Data Center Administration Guide* for details about Forwarding Policies.

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.
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 Data Center 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 16-12. 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.	■ PublicCloudGateway TN-<VPC/VNET-ID> ■ PublicCloudGateway TN-<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 16-13. 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 16-13. 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.

Networking Entities

The following entities are created at different stages of onboarding and can be found under the **Networking** tab:

Figure 16-5. Auto-created NSX-T Data Center Networking Entities After PCG is Deployed

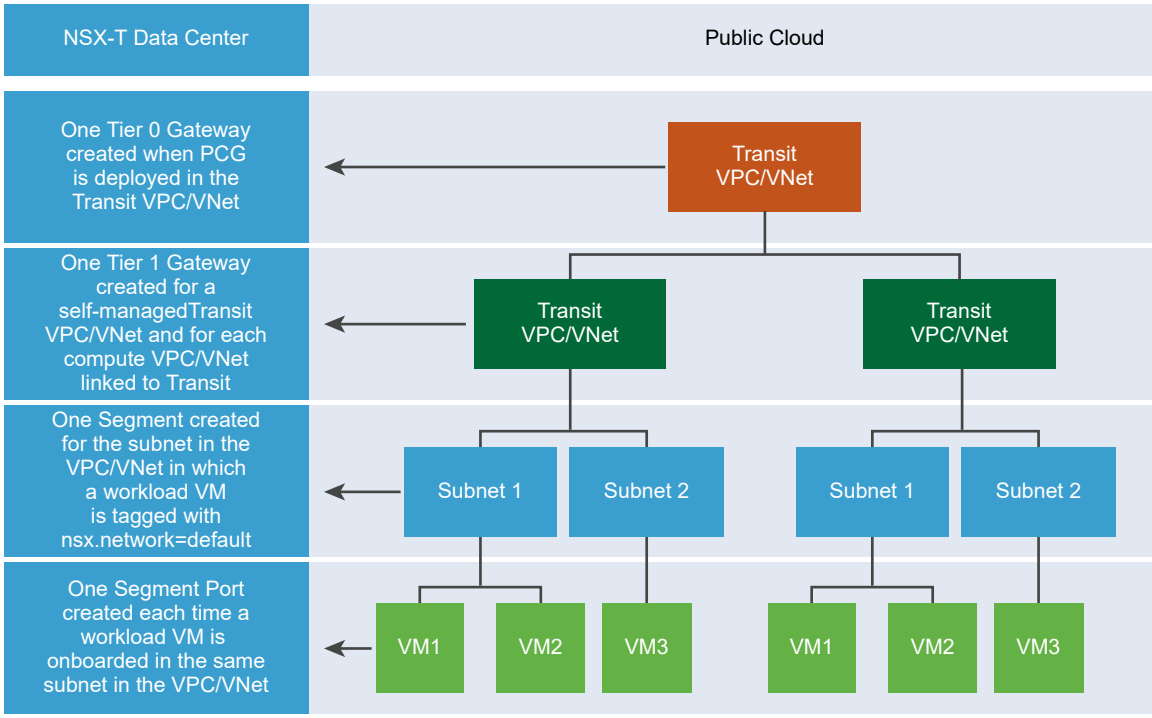


Table 16-14. Auto-Created Networking Entities

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)

Security Entities

The following entities are available under the **Security** tab:

Table 16-15. 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>	

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 16-16. 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 16-17. 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)

Integrate Horizon Cloud Service with NSX Cloud

Starting in NSX-T Data Center 3.1.1, you can integrate your Horizon Cloud deployment with NSX Cloud with fewer manual steps than in earlier releases.

Horizon Cloud integration is supported with NSX Cloud management components – NSX Manager and Cloud Service Manager (CSM) – deployed either on-premise, or natively in Microsoft Azure, starting in NSX-T Data Center 3.1.1.

The diagrams depict the options available to deploy NSX Cloud management components and shared subnets between PCG and Horizon Cloud Management components as possible scenarios for this integration.

Figure 16-6. Horizon Cloud Integration with NSX Cloud Components deployed On-prem

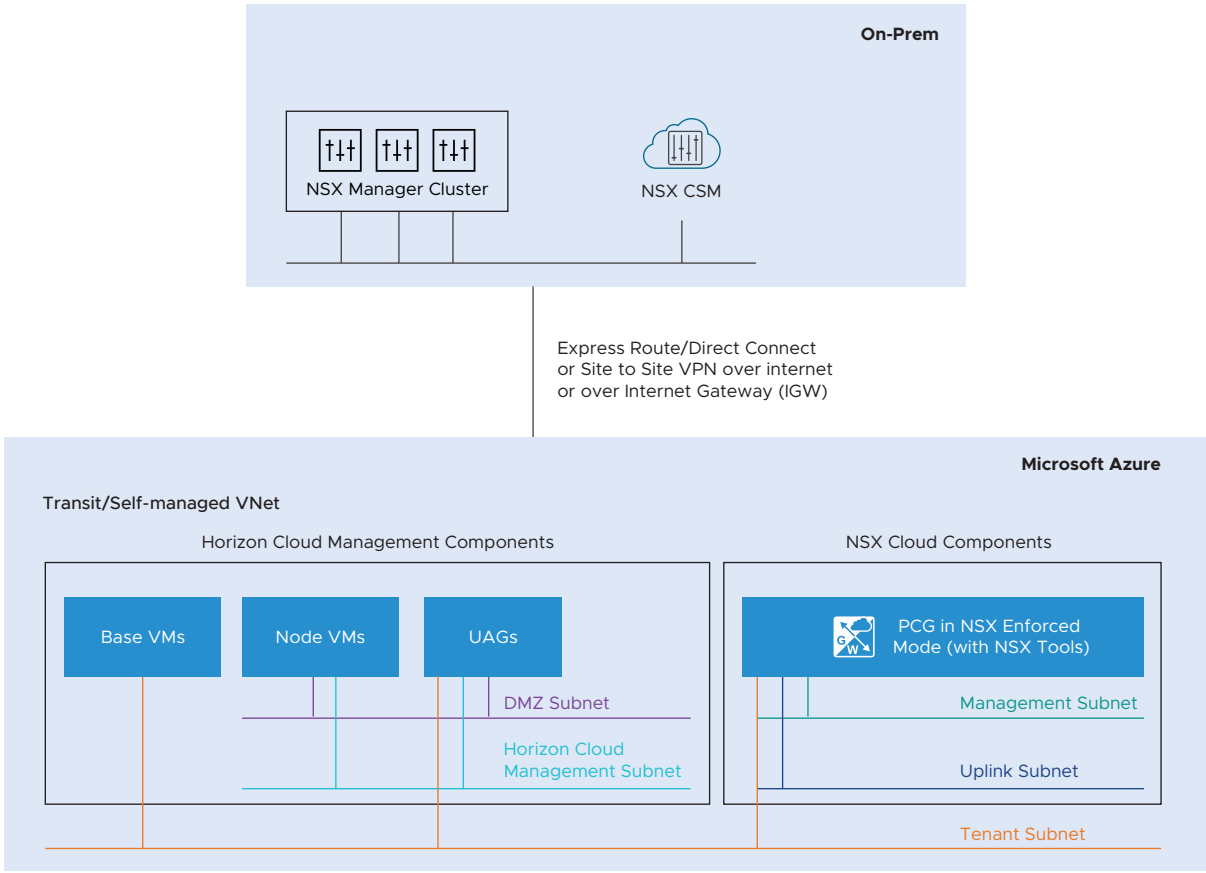
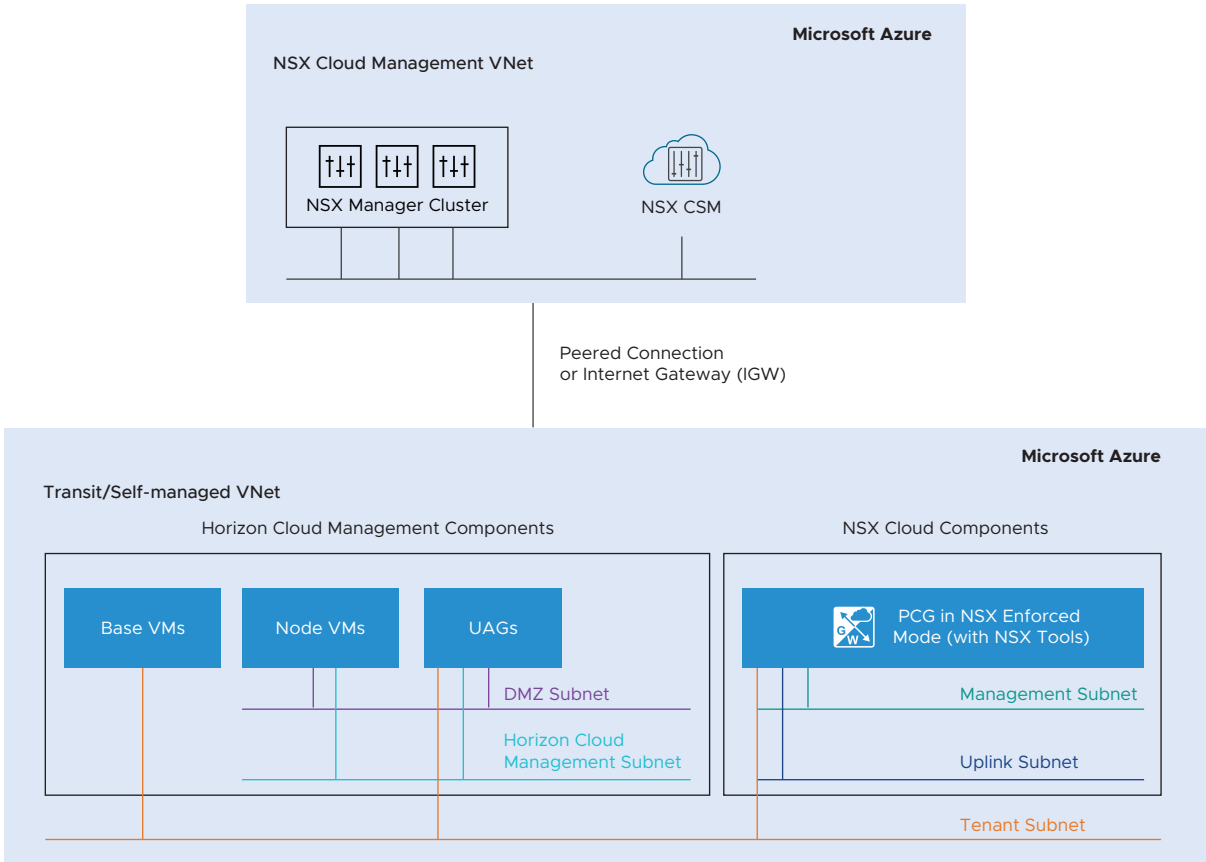


Figure 16-7. Horizon Cloud Integration with NSX Cloud with NSX Cloud Components deployed in Microsoft Azure



You must deploy your Horizon Cloud pod in the same Self-managed/Transit VNet where you have deployed the PCG. After deploying the Horizon Cloud pod in a Self-managed/Transit VNet, the system auto-creates the necessary NSX-T Data Center policies to enable communication between Horizon Cloud management components and VDIs deployed in Microsoft Azure. You can create security policies for VDIs as necessary.

Note Auto-creation of entities is a feature of NSX-T Data Center version 3.1.1 and later only.

Prerequisites

- Verify that NSX Cloud management components are already deployed and active. See Deploy NSX-T Data Center On-Prem Components or Deploy NSX Cloud Components in Microsoft Azure using the NSX Cloud Marketplace Image for relevant instructions for your deployment model.
- Verify that a PCG is already deployed in the same VNet where you are deploying the Horizon Cloud pod. A VNet that has the PCG deployed in it is called a Self-managed or Transit VNet in NSX Cloud terminology. See NSX Public Cloud Gateway: Architecture and Modes of Deployment .

- If NSX Cloud management components are deployed on-prem, verify that you have a Self-managed or Transit VNet connected with the on-prem components using VGW or IGW connectivity.
- If you are deploying NSX Cloud management components in the public cloud, verify that you have a peering connection between the VNet where NSX Cloud components are deployed and the Self-managed/ Transit VNet.

Procedure

1 From your Microsoft Azure subscription, deploy the Horizon Cloud pod in a Self-managed/ Transit VNet. See Horizon Pods on Microsoft Azure - Using the Horizon Cloud Administration Console Capacity Page to Add More Pods to Your Pod Fleet in the *Horizon Cloud Service Product Documentation* for detailed steps. Note the following configurations in the **Add Microsoft Azure Capacity** wizard that are specific to integration with NSX Cloud:

   a In the **Subscription** tab, select the Microsoft Azure subscription where PCG is deployed.

   b In the **Pod Setup** tab, under the section **Networking** for **Virtual Network**, select the Microsoft Azure VNet in which PCG is deployed.

   Use subnets that allow communication between the PCG and Horizon Cloud management components.

   c Click **Validate and Proceed**

2 Create a base image with NSX Tools installed.

   If you are using pod manifest 2632.0 or later, and your customer record has access to the new Image Management feature that auto-installs NSX Tools into the base image, enable **Install NSX Tools**.

   If you are using pod manifests prior to 2632.0, follow the steps described at Install the NSX Agent in the Horizon Cloud Imported Image VM to manually install NSX Tools in the base image.

3 Use the base image to create the VDI desktop assignment, enabling **NSX Cloud Managed**. See Horizon Cloud Workflows and NSX Cloud for details.

What to do next

Verify the Auto-Created Entities After Horizon Cloud Integration .

Auto-Created Entities After Horizon Cloud Integration

After you deploy your Horizon Cloud pod in a Self-managed/Transit VNet, the following entities are auto-created in CSM and NSX Manager.

Note Auto-creation of entities is a feature of NSX-T Data Center version 3.1.1 and later only.

Horizon Cloud VMs in CSM

- Horizon Cloud VMs can be management VMs or VDIs for end users.
- CSM distinguishes Horizon Cloud management VMs from end-user consumable VDIs as follows:
  - The three types of Horizon Cloud management VMs – UAG, Base, and Node are labeled as **Horizon Management VMs** in **CSM > Clouds > Azure > Instances**. The Horizon Cloud administrator has complete control over the security groups assigned to these VMs in Microsoft Azure.
  - All VDIs launched in the Horizon Cloud pod, using any image with NSX Cloud enabled, are NSX-managed if they enable NSX Cloud when launched. NSX Tools are installed on such VDIs and they are managed like other managed VMs in the NSX Enforced mode. In **CSM > Clouds > Azure > Instances**, you can see these VDIs with the label **Horizon VDI**.

    See "Managing VMs in the NSX Enforced Mode" in the *NSX-T Data Center Administration Guide* for details.

    Also see "VMware NSX Cloud and Horizon Cloud Pods in Microsoft Azure" in the Horizon Cloud Service Product Documentation.

Horizon Cloud Entities Created in NSX Manager

NSX Manager Component	Auto-created Entities	Details
Inventory > Services	HorizonUAGPolicyService	This service allows communication between the Horizon Cloud UAG and VDIs. See this table for details: Table 16-18. DFW Policy Auto-created for Horizon Cloud Integration under the Infrastructure category
Inventory > Services	HorizonNodeVMPolicyService	This service is used to allow communication from the VDIs to Horizon Cloud Management Node VMs. See this table for details: Table 16-18. DFW Policy Auto-created for Horizon Cloud Integration under the Infrastructure category

NSX Manager Component	Auto-created Entities	Details
Inventory > Groups	■ `vmw-hcs-<pod-id>-base` ■ `vmw-hcs-<pod-id>-node` ■ `vmw-hcs-<pod-id>-uag` ■ `vmw-hcs-<pod-id>-vdi`	The group definition for these groups is as follows: ■ instance-type label that Horizon Cloud applies to these VMs in Microsoft Azure. ■ Microsoft Azure ID of the Self-managed/Transit VNet that also hosts the Horizon Cloud pod. You manage the VDIs that are included in the `vmw-hcs-<id>-vdi` group. The other groups are managed by Horizon Cloud. The Horizon Cloud jumpbox VMs are grouped under `vmw-hcs-<id>-node`
Inventory > Virtual Machines	Horizon Cloud VDIs with names provided by Horizon Cloud	These are the VDIs in Horizon Cloud that are categorized as Virtual Machines in NSX Manager. All security policies and other configurations in NSX Manager are targeted towards these Virtual Machines.

Inventory > Tags	■ Tag Scope: `azure:instance_type`
	■ Tag Values:
	  ■ `HORIZON_MGMT`
	  ■ `HORIZON_BASE`
	  ■ `HORIZON_UAG`
	  ■ `HORIZON_VDI`
		These system tags are used to create groups for security policies.

Security Policy

Under **Security > Distributed Firewall > Infrastructure** a DFW policy is created with the name: **vmw-hcs-<pod_id>-security-policy**. This policy has the following **Allow** rules.

.

Table 16-18. DFW Policy Auto-created for Horizon Cloud Integration under the Infrastructure category

DFW Rule Name	Source	Destination	Service/Ports	Protocols
AllowHCSUAGToVDI	Unified Access Gateway	VDI	HorizonUAGPolicyService TCP (Source: Any; Destination: 22443,32111,4172,443,8443,9427) UDP (Source: Any | Destination: 22443,4172)	TCP and UDP
AllowVDIToHCSNode	VDI	Node VMs	HorizonNodeVMPolicyService (Source: Any; Destination: 3099,4001,4002)	TCP

Note All networking for NSX-managed VDIs within the VNet is through Microsoft Azure. NSX-T Data Center only manages traffic going out of the VNet.

See "Group VMs using NSX-T Data Center and Public Cloud Tags" in the *NSX-T Data Center Administration Guide* for details on discovered tags: these are tags that you apply in Microsoft Azure to your VDIs and they are visible in NSX Manager to enable tag-based grouping.

(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*.

Un-deploy NSX Cloud

You must un-deploy NSX Cloud configurations before decommissioning the CSM appliance.

To un-deploy NSX Cloud, perform the following steps:

1 Undeploy or Unlink PCG.

  For any issues, see Troubleshooting PCG Undeployment.

2 Decommission the CSM appliance.

  a Log in to the vSphere Client using your administrator credentials.

  b Power off the CSM appliance VM.

  c To delete the CSM appliance VM from the datastore, right-click the appliance VM.

  d Select **Delete from Disk,** and then click **OK**. For details, refer to the vSphere documentation.

Note In case of Azure deployment, you must delete the entire Resource Group that contains three MPs and one CSM.

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.

What to read next

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.
  - For Microsoft Azure, also delete the NSX Cloud-created Resource Group named like **`nsx-gw-<vnet ID>-rg`**.
- Delete the auto-created entities with the VPC/VNet ID in NSX Manager as listed here: Auto-created NSX-T Data Center 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.
- Restart the CSM Service. Log in to the CSM appliance CLI and run the `restart service cloud-service-manager` command.

Important If the PCG un-deployment fails even after performing the steps mentioned in this topic or you need to redeploy in same VPC/VNet, a database cleanup for PCG may be required. The database cleanup needs engineering assistance. If you want to clean-up the PCG database, contact the VMware support team.

Uninstalling NSX-T Data Center from a Host Transport Node

17

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.

- Migrate Out VMkernels and Physical NICs from a vSphere Distributed Switch

  To prepare a transport node using vSphere Distributed Switch for uninstallation, migrate out any VMkernel adapters and physical NICs on a vSphere Distributed Switch (NSX Switch in vCenter Server) to vSwitch0.

- 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 Managed 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 ESXi Host

  You can uninstall NSX-T Data Center from a ESXi host.

- Uninstall NSX-T Data Center from a Physical Host

  You can uninstall NSX-T Data Center from a physical host.

- 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.

- Uninstall NSX-T Data Center from a Physical Server

  You can uninstall NSX-T Data Center from a physical server host.

- Uninstall NSX-T from a vSphere Lifecycle Manager cluster through NSX Manager

  You can trigger uninstallation of NSX-T on a host that is part of a vSphere Lifecycle Manager cluster through NSX Manager.

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.

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.

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.

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 Navigate the UI based on the NSX-T Data Center version and select a host:

- (NSX-T Data Center 3.2.2 or later) **System > Fabric > Hosts** and select the **Cluster** tab.
- (NSX-T Data Center 3.2.1 or earlier) **System > Fabric > Nodes > Host Transport Nodes**

  and from the Managed by dropdown menu, select a vCenter Server.

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.

Migrate Out VMkernels and Physical NICs from a vSphere Distributed Switch

To prepare a transport node using vSphere Distributed Switch for uninstallation, migrate out any VMkernel adapters and physical NICs on a vSphere Distributed Switch (NSX Switch in vCenter Server) to vSwitch0.

In contrast, on a transport node prepared using a N-VDS switch, the uninstall wizard allows you to specify mapping of VMkernel adapters and physical NICs, that are migrated to a vSwitch0 during uninstallation. See Verify Host Network Mappings for Uninstall.

In this task, there is no restriction on the type of switch chosen to migrate back physical NICs and VMkernel adapters. The switch can be of the type: Static Binding or Ephemeral.

Scenarios during migrating back VMkernels and physical NICs:

1 In the procedure below, consider a host with two physical NICs and VMkernel adapters:

- NSX Switch has vmnic0 and vmnic1 configured to uplink 1 and 2 respectively and the port group is connected to vmk1 and vmk0.
- vSwitch0 does not have any vmnic or VMkernel adapter configured on it. During migration, vCenter Server does not restrict to migrate back vmks to an Ephemeral switch. At the end of the procedure, vmnic0, vmnic1, and vmk0, vmk1 are migrated back to vSwitch0.

2 (Scenarios not covered in this task) If the host only has a single physical NIC and a VMkernel adapter configured to the NSX-T Data Center switch, you might choose to do one of the following:

- To migrate out the physical NIC and VMkernel adapter to vSwitch0, run vSphere API (use the `updateNetworkConfig` method of `NetworkSystem` interface) to migrate both the physical NIC and VMkernel adapter at the same time. vSphere Client does not support this type of migration.
- To migrate out only the VMkernel adapter to another distributed virtual port group on the NSX Switch (a VDS switch), you can use the vSphere Client to migrate out the VMkernel adapter to another port group on the NSX Switch.

At the end of the procedure, vmnic0, vmnic1 and vmk0, vmk1 are migrated back to vSwitch0.

Prerequisites

- ESXi hosts are prepared as transport nodes using vSphere Distributed Switch.
- VMkernels and physical NICs are migrated to the vSphere Distributed Switch as part of installation.

Procedure

1 From a browser, log in with admin privileges to a vCenter Server at https://<vCenterServer-ip-address>.

2 Navigate to **Host → Configure → Virtual Switches**.

3 Make a note of the vmknics to be migrated to the vSwitch0.

4 Navigate to **Home → Networking**, to view all switches configured in the data center.

5 In the Switch page, click **Actions → Add and Manage Hosts**.

6 Select **Manage Host Networking**.

7 Click **Next**.

8 In the Select Member Hosts window, select **`hosts`**.

9 Click **Ok**.

10 In the Manage physical adapters window, select **vmnic1** and click **Unassign adapter**.

11 To apply the same configuration on other hosts of the cluster, in the Confirm Unassign Adapter popup window, select **Apply this operation to all other hosts**.

12 Finish the wizard.

All vmnic1 on hosts are free.

13 To migrate back vmnic1 to vSwitch0.

a navigate to **Host → Configure → Virtual Switches**.

b In the vSwitch0 section, click Manage Physical Adapters.

c Add vmnic1 to vSwitch0.

d Finish the wizard by accepting defaults.

Verify vCenter Server migrated vmnic1 to vSwitch0 and assigned it an IP address.

14 To migrate back vmk1 to vSwitch0.

a navigate to **Host → Configure → Virtual Switches**.

b In the vSwitch0 section, click Migrate VMkernel Adapters.

c Add vmk1 to vSwitch0.

d Finish the wizard by accepting defaults.

Verify vCenter Server migrated vmk1 to vSwitch0 and assigned it an IP address.

15 Similarly, migrate back vmnic0 to vSwitch0 and vmk0 to an existing or a new port group on vSwitch0.

Verify vmnic0 and vmk0 are assigned new IP addresses.

16 Verify there are no vmks on the NSX switch. All vmks must be migrated to the vSwitch 0 or another port group on the NSX switch.

What to do next

Navigate to NSX Manager and uninstall the transport node. At the end of uninstallation process, verify configuration status of the host is `Not Configured`. This completes the uninstallation of NSX-T Data Center on the host.

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.

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 Managed Host in a vSphere Cluster.

Note Follow these instructions to uninstall NSX-T Data Center from a host in a cluster: Uninstall NSX-T Data Center from a Managed Host in a vSphere Cluster.

Prerequisites

- In vCenter Server, put the hosts in maintenance mode and power off VMs running on the hosts if you want to migrate VMkernel adapters during uninstallation.

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Navigate the UI based on the NSX-T Data Center version and select a host:
   - (NSX-T Data Center 3.2.2) **System > Fabric > Hosts** and select the **Cluster** tab.
   - (NSX-T Data Center 3.2.1 or earlier) **System > Fabric > Nodes > Host Transport Node** and from the Managed by dropdown menu, select a vCenter Server.
3. Select the cluster you want to uninstall, and select **Remove NSX**.

   Note If NSX Intelligence is also deployed on the host, uninstallation of NSX-T Data Center will fail because all transport nodes become part of a default network security group. To successfully uninstall NSX-T Data Center, you also need to select the **Force Delete** option before proceeding with uninstallation.
4. 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'
```

5 (Host on an N-VDS switch) If the host goes into a failed state and NSX-T Data Center VIBs cannot be removed, run the `nsxcli -c del nsx` command to remove NSX-T Data Center from the host.

a Before running the `del nsx` command, do the following:

- If there are VMkernel adapters on NSX port groups on the VDS switch, you must manually migrate or remove vmks from NSX port group to DV port groups on the VDS switch. If there are any vmks available on the NSX port groups, `del nsx` command execution fails.
- Put the ESXi host in maintenance mode. The vCenter Server does not allow the host to be put in maintenance mode unless all running VMs on the host are in powered off state or moved to a different host.
- Permanently disconnect the ESXi host transport node from NSX Manager by stopping nsx-proxy service running on the ESX host transport node. Log in to the ESXi CLI terminal and run `/etc/init.d/nsx-proxy stop`.
- Refresh the NSX Manager UI.
- Verify that the state of the ESXi host transport node is `Disconnected` from NSX Manager.

b Log in to the ESXi CLI terminal.

c Run `nsxcli -c del nsx`.

d Read the warning message. Enter **`Yes`** if you want to go ahead with NSX-T Data Center uninstallation.

```
Carefully read the requirements and limitations of this command:
1. Read NSX documentation for 'Remove a Host from NSX or Uninstall NSX Completely'.
2. Deletion of this Transport Node from the NSX UI or API failed, and this is the last
resort.
3. If this is an ESXi host:
   a. The host must be in maintenance mode.
   b. All resources attached to NSXPGs must be moved out.
   If the above conditions for ESXi hosts are not met, the command WILL fail.
4. For command progress check /scratch/log/nsxcli.log on ESXi host or /var/log/
nsxcli.log on non-ESXi host.
Are you sure you want to remove NSX on this host? (yes/no)
```

Important After running the `del nsx` command, do not use the **Resolve** functionality in the NSX Manager UI to reprepare the host that is in **Disconnected** state. If you use the **Resolve** functionality, the host might go into **Degraded** state.

e Verify that the existing VMkernel and physical NICs on the N-VDS switch are migrated to a new vSwitch. If there are more than one N-VDS switches on the host, each N-VDS switch is migrated to a separate vSwitch. For example, if there are N-VDS1, and N-VDS2 switches on the host, the VMkernel adapters and physical NICs are migrated to vSwitch1 and vSwitch 2.

f In NSX Manager, if a transport node profile (TNP) is attached to the cluster, detach the profile.

g Select each host and click **Remove NSX**.

h In the popup window, select **Force Delete** and begin uninstallation.

i On the ESXi host, verify that system message displayed is `Terminated`. This message indicates that NSX-T Data Center is completely removed from the host.

After running `del nsx`, all existing host switches are removed, VMkernels and physical NICs are migrated to newly created vSwitches, transport node is detached from NSX Manager, and NSX-T Data Center VIBs are removed. If any NSX-T Data Center VIBs remain on the host, contact VMware support.

6 (Host on a VDS 7.0 switch) If the host goes into failed state and NSX-T Data Center VIBs cannot be removed, run the `nsxcli -c del nsx` command to remove NSX from the host.

a Before running the `del nsx` command, do the following:

- If there are VMkernel adapters on NSX port groups on the VDS switch, you must manually migrate or remove vmks from NSX port group to DV port groups on the VDS switch. If there are any vmks available on the NSX port groups, `del nsx` command execution fails.
- Put the ESXi host in maintenance mode. The vCenter Server does not allow the host to be put in maintenance mode unless all running VMs on the host are in powered off state or moved to a different host.
- Permanently disconnect the ESXi host transport node from NSX Manager by stopping nsx-proxy service running on the ESX host transport node. Log in to the ESXi CLI terminal and run `/etc/init.d/nsx-proxy stop`.
- Refresh the NSX Manager UI.
- Verify that the state of the ESXi host transport node is `Disconnected` from NSX Manager.

b Log in to the ESXi CLI terminal.

c Run `nsxcli -c del nsx`.

d Read the warning message. Enter **Yes** if you want to go ahead with NSX-T Data Center uninstallation.

```
Carefully read the requirements and limitations of this command:
1. Read NSX-T documentation for 'Remove a Host from NSX-T Data Center or Uninstall
NSX-T Data Center Completely'.
2. Deletion of this Transport Node from the NSX-T UI or API failed, and this is the
last resort.
3. If this is an ESXi host:
   a. The host must be in maintenance mode.
   b. All resources attached to NSXPGs must be moved out.
   If the above conditions for ESXi hosts are not met, the command WILL fail.
4. For command progress check /scratch/log/nsxcli.log on ESXi host or /var/log/
nsxcli.log on non-ESXi host.
Are you sure you want to remove NSX-T on this host? (yes/no)
```

Important After running the `del nsx` command, do not use the **Resolve** functionality in the NSX Manager UI to reprepare the host that is in **Disconnected** state . If you use the **Resolve** functionality, the host might go into **Degraded** state.

e In the NSX Manager UI, if a TNP is attached to the cluster, detach the profile.

f Select each host and click **Remove NSX**.

g In the popup window, select **Force Delete** and begin uninstallation.

h On the ESXi host, verify that system message displayed is `Terminated`. This message indicates that NSX-T Data Center is completely removed from the host.

All existing host switches are removed, transport node is detached from NSX Manager, and NSX-T Data Center VIBs are removed. If any NSX-T Data Center VIBs remain on the host, contact VMware support.

Uninstall NSX-T Data Center from a Managed 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.

Prerequisites

- In vCenter Server, put the hosts in maintenance mode and power off VMs running on the hosts if you want to migrate VMkernel adapters during uninstallation.
- On an ESXi host that is put into `Locked` state, ensure that the root user is added to the exception list, so that an SSH session can be established with the host.

Procedure

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

2 Navigate the UI based on the NSX-T Data Center version and select a host:

   - (NSX-T Data Center 3.2.2) **System > Fabric > Hosts** and select the **Cluster** tab.
   - (NSX-T Data Center 3.2.1 or earlier) **System > Fabric > Nodes > Host Transport Nodes** and from the Managed by dropdown menu, select a vCenter Server.

3 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.

4 Select the host 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'
   ```

6 If a Transport Node Profile is applied to the cluster, and you want to reapply it, select the cluster, click **Configure NSX**, and select the profile from the **Select Deployment Profile** drop-down menu.

7 (Host on an N-VDS switch) If the host goes into a failed state and NSX-T Data Center VIBs cannot be removed, run the `nsxcli -c del nsx` command to remove NSX-T Data Center from the host.

   a Before running the `del nsx` command, do the following:

      - If there are VMkernel adapters on NSX port groups on the VDS switch, you must manually migrate or remove vmks from NSX port group to DV port groups on the VDS switch. If there are any vmks available on the NSX port groups, `del nsx` command execution fails.
      - Put the ESXi host in maintenance mode. The vCenter Server does not allow the host to be put in maintenance mode unless all running VMs on the host are in powered off state or moved to a different host.
      - Permanently disconnect the ESXi host transport node from NSX Manager by stopping nsx-proxy service running on the ESX host transport node. Log in to the ESXi CLI terminal and run `/etc/init.d/nsx-proxy stop`.
      - Refresh the NSX Manager UI.
      - Verify that the state of the ESXi host transport node is `Disconnected` from NSX Manager.

   b Disable SNMP on the ESXi host.

   ```
   esxcli system snmp set --enable false
   ```

c Log in to the ESXi CLI terminal.

d Run `nsxcli -c del nsx`.

e Read the warning message. Enter **`Yes`** if you want to go ahead with NSX-T Data Center uninstallation.

```
Carefully read the requirements and limitations of this command:
1. Read NSX documentation for 'Remove a Host from NSX or Uninstall NSX Completely'.
2. Deletion of this Transport Node from the NSX UI or API failed, and this is the last
resort.
3. If this is an ESXi host:
   a. The host must be in maintenance mode.
   b. All resources attached to NSXPGs must be moved out.
   If the above conditions for ESXi hosts are not met, the command WILL fail.
4. For command progress check /scratch/log/nsxcli.log on ESXi host or /var/log/
nsxcli.log on non-ESXi host.
Are you sure you want to remove NSX on this host? (yes/no)
```

Important After running the `del nsx` command, do not use the **Resolve** functionality in the NSX Manager UI to re-prepare the host that is in **Disconnected** state . If you use the **Resolve** functionality, the host might go into **Degraded** state.

f Verify that the existing VMkernel and physical NICs on the N-VDS switch are migrated to a new vSwitch. If there are more than one N-VDS switches on the host, each N-VDS switch is migrated to a separate vSwitch. For example, If there are N-VDS1, and N-VDS2 switches on the host, the VMkernel adapters and physical NICs are migrated to vSwitch1 and vSwitch 2.

g Select each host and click **Remove NSX**.

h In the popup window, select **Force Delete** and begin uninstallation.

i On the ESXi host, verify that system message displayed is `Terminated`. This message indicates that NSX-T Data Center is completely removed from the host.

After running `del nsx`, all existing host switches are removed, VMkernels and physical NICs are migrated to newly created vSwitches, transport node is detached from NSX Manager, and NSX-T Data Center VIBs are removed. If any NSX-T Data Center VIBs remain on the host, contact VMware support.

8 (Host on a VDS 7.0 switch) If the host goes into failed state and NSX-T Data Center VIBs cannot be removed, run the `nsxcli -c del nsx` command to remove NSX from the host.

a Before running the `del nsx` command, do the following:

- If there are VMkernel adapters on NSX port groups on the VDS switch, you must manually migrate or remove vmks from NSX port group to DV port groups on the VDS switch. If there are any vmks available on the NSX port groups, `del nsx` command execution fails.
- Put the ESXi host in maintenance mode. The vCenter Server does not allow the host to be put in maintenance mode unless all running VMs on the host are in powered off state or moved to a different host.
- Permanently disconnect the ESXi host transport node from NSX Manager by stopping nsx-proxy service running on the ESX host transport node. Log in to the ESXi CLI terminal and run `/etc/init.d/nsx-proxy stop`.
- Refresh the NSX Manager UI.
- Verify that the state of the ESXi host transport node is `Disconnected` from NSX Manager.

b Disable SNMP on the ESXi host.

```
esxcli system snmp set --enable false
```

c Log in to the ESXi CLI terminal.

d Run `nsxcli -c del nsx`.

e Read the warning message. Enter **`Yes`** if you want to go ahead with NSX-T Data Center uninstallation.

```
Carefully read the requirements and limitations of this command:
1. Read NSX documentation for 'Remove a Host from NSX or Uninstall NSX Completely'.
2. Deletion of this Transport Node from the NSX UI or API failed, and this is the last
resort.
3. If this is an ESXi host:
   a. The host must be in maintenance mode.
   b. All resources attached to NSXPGs must be moved out.
   If the above conditions for ESXi hosts are not met, the command WILL fail.
4. For command progress check /scratch/log/nsxcli.log on ESXi host or /var/log/
nsxcli.log on non-ESXi host.
Are you sure you want to remove NSX on this host? (yes/no)
```

Important After running the `del nsx` command, do not use the **Resolve** functionality in the NSX Manager UI to re-prepare the host that is in **Disconnected** state . If you use the **Resolve** functionality, the host might go into **Degraded** state.

f Select each host and click **Remove NSX**.

g In the pop-up window, select **Force Delete** and begin uninstallation.

h On the ESXi host, verify that system message displayed is `Terminated`. This message indicates that NSX-T Data Center is completely removed from the host.

- All existing host switches are removed, transport node is detached from NSX Manager, and NSX-T Data Center VIBs are removed. If any NSX-T Data Center VIBs remain on the host, contact VMware support.
- On a host part of a vSphere Lifecycle Manager, after you perform `del nsx` and **Remove NSX** from NSX Manager, the host status in vCenter Server is compliant with the cluster image. The system displays, `All hosts in the cluster are compliant`.

Uninstall NSX-T Data Center from a Standalone ESXi Host

You can uninstall NSX-T Data Center from a ESXi host.

Prerequisites

If you are uninstalling NSX-T Data Center from a standalone ESXi host, verify the following settings:

- In vCenter Server, put the hosts in maintenance mode and power off VMs running on the hosts if you want to migrate VMkernel adapters during uninstallation.

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Navigate the UI based on the NSX-T Data Center version and select a host:
   - (NSX-T Data Center 3.2.2 or later) **System > Fabric > Hosts** and select the **Cluster** tab.
   - (NSX-T Data Center 3.2.1 or earlier) **System > Fabric > Nodes > Host Transport Nodes**

     and from the Managed by dropdown menu, select **None: Standalone Hosts** or a vCenter Server.
3. Select the host and click **Delete**. In the confirmation dialog box, by default **Uninstall NSX Components** is selected. Uncheck **Force Delete** and 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.
4. If the uninstall fails, select the host and click **Delete** again. In the confirmation dialog box, check **Force Delete** and click **Delete**.

   The host transport node is deleted from the management plane, but the host might still have NSX-T Data Center software installed.

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 To check for NSX-T Data Center software packages on the ESXi host, run `esxcli software vib list | grep -E 'nsx|vsipfwlib'`.

6 (Host on an N-VDS switch) If the host goes into a failed state and NSX-T Data Center VIBs cannot be removed, then run the `del nsx` command to remove NSX-T Data Center from the host.

   a Before running the `del nsx` command, put the ESXi host in maintenance mode. The vCenter Server does not allow the host to be put in maintenance mode unless all running VMs on the host are in powered off state or moved to a different host.

   b Log in to the ESXi CLI terminal, run `nsxcli -c del nsx`.

   c Read the warning message. Enter **`Yes`** if you want to go ahead with NSX-T Data Center uninstallation.

```
Carefully read the requirements and limitations of this command:
1.Read NSX-T documentation for 'Remove a Host from NSX-T Data Center or Uninstall NSX-T Data Center Completely'.
2.Deletion of this Transport Node from the NSX-T UI or API failed, and this is the last resort.
3.If this is an ESXi host:
a.The host must be in maintenance mode.
b. All resources attached to NSXPGs must be moved out.
If the above conditions for ESXi hosts are not met, the command WILL fail.
4. For command progress check /scratch/log/nsxcli.log on ESXi host or /var/log/nsxcli.log on non-ESXi host.
Are you sure you want to remove NSX-T on this host? (yes/no)
```

   Important After running the `del nsx` command, do not use the **Resolve** functionality in the NSX Manager UI to reprepare the host that is in **Disconnected** state . If you use the **Resolve** functionality, the host might go into **Degraded** state.

   d Verify that the existing VMkernel and physical NICs on the N-VDS switch are migrated to a new vSwitch. If there are more than one N-VDS switches on the host, each N-VDS switch is migrated to a separate vSwitch. For example, if the host has N-VDS1and N-VDS2, the VMkernel adapters and physical NICs are migrated to vSwitch1 and vSwitch 2.

   e Select each host and click **Remove NSX**.

f In the popup window, select **Force Delete** and begin uninstallation.

g On the ESXi host, verify that system message displayed is `Terminated`. This message indicates that NSX-T Data Center is completely removed from the host.

After running `del nsx`, NSX-T Data Center removes all existing host switches, migrates VMkernels and physical NICs to the newly created vSwitches, detaches the transport node from NSX Manager and removes NSX-T Data Center VIBs from the host.

Results

When 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.

Uninstall NSX-T Data Center from a Physical Host

You can uninstall NSX-T Data Center from a physical host.

Prerequisites

If you are uninstalling NSX-T Data Center from a standalone physical host, verify the following settings:

Procedure

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

2 Navigate the UI based on the NSX-T Data Center version and select a host:

- (NSX-T Data Center 3.2.2 or later) **System > Fabric > Hosts** and select the **Cluster** tab.
- (NSX-T Data Center 3.2.1 or earlier) **System > Fabric > Nodes > Host Transport Nodes**

  and from the Managed by dropdown menu, select **None: Standalone Hosts**.

3 Select the physical host, click **Delete**. In the confirmation dialog box, by default **Uninstall NSX Components** is selected. Uncheck **Force Delete**, click **Delete**.

The NSX-T Data Center software is removed from the host.

4 If the uninstall fails, select the host and click **Delete** again. In the confirmation dialog box, check **Force Delete** and click **Delete**.

The system deletes the host transport node from the management plane, but the host might still have NSX-T Data Center software installed.

5 Verify that the NSX-T Data Center software is removed from the host.

```
rpm -qa | grep -E 'nsx|vsipfwlib'
```

6 If the host goes into a failed state and NSX-T Data Center VIBs cannot be removed, then to forcefully remove NSX-T Data Center from the host, run the `del nsx` command .

a Log into the host's command-line interface as root.

b Run `nsxcli -c del nsx`.

c Read the warning message. Enter **`Yes`** if you want to go ahead with NSX-T Data Center uninstallation.

```
Carefully read the requirements and limitations of this command:
1.Read NSX documentation for 'Remove a Host from NSX or Uninstall NSX Completely'.
2.Deletion of this Transport Node from the NSX UI or API failed, and this is the last resort.
3.If this is an ESXi host:
a.The host must be in maintenance mode.
b. All resources attached to NSXPGs must be moved out.
If the above conditions for ESXi hosts are not met, the command WILL fail.
4.If this is a Linux host:
a. This command should be run from the host console and may fail if run from an SSH client or any other network based shell client.
b. The 'nsxcli -c del nsx' form of this command is not supported.
5. For command progress check /scratch/log/nsxcli.log on ESXi host or /var/log/nsxcli.log on non-ESXi host.
Are you sure you want to remove NSX on this host? (yes/no)
```

Important After running the `del nsx` command, do not use the **Resolve** functionality in the NSX Manager UI to reprepare the host that is in **Disconnected** state . If you use the **Resolve** functionality, the host might go into **Degraded** state.

d Go back to the NSX Manager, on the **Host Transport Nodes** page, select each host and click **Remove NSX**.

e In the popup window, select **Force Delete** and begin uninstallation.

f On the physical host, verify that system message displayed is `Terminated`. This message indicates that NSX-T Data Center is completely removed from the host including the application interface that was created for the physical host.

After running `del nsx`, NSX-T Data Center packages and the application interface are removed from the host.

Results

When 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.

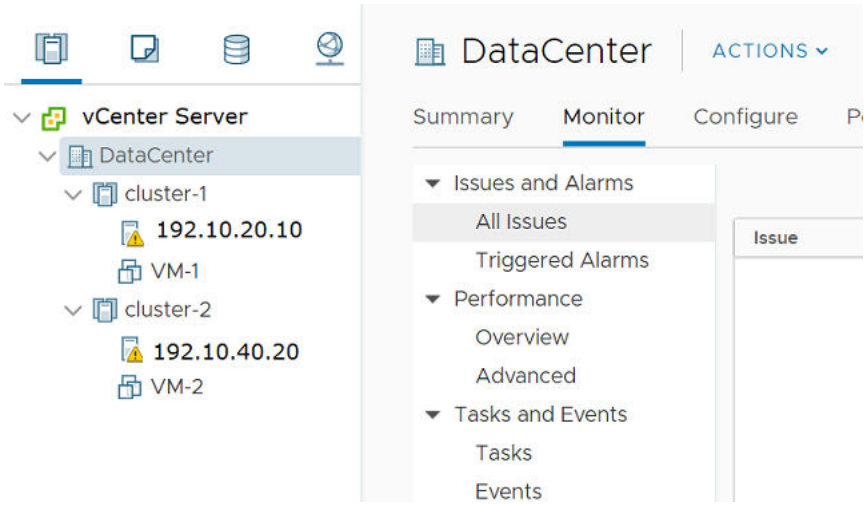
What to do next

Remove the segment port that was connected to the application interface of the physical host.

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 Data Center 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 Data Center is uninstalled from the host.

Uninstall NSX-T Data Center from a Physical Server

You can uninstall NSX-T Data Center from a physical server host.

Procedure

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

2 Navigate the UI based on the NSX-T Data Center version and select a host:

- (NSX-T Data Center 3.2.2 or later) **System > Fabric > Hosts** and select the **Cluster** tab.
- (NSX-T Data Center 3.2.1 or earlier) **System > Fabric > Nodes > Host Transport Nodes** and from the Managed by dropdown menu, select **None: Standalone Hosts**.

3 Select the host and click **Delete**.

4 On the Delete Transport Node popup window, click **Delete**.

5 If the host goes into a failed state and NSX-T Data Center VIBs cannot be removed, then run the `del nsx` command to remove NSX-T Data Center from the host.

   a Before running the `del nsx` command, power off all tenant VMs running on the physical server host.

   b On the physical server host, log in to the console. At the CLI terminal, run `nsxcli`.

   c Enter `del nsx`.

   Important Do not run `nsxcli -c del nsx` as a single command on the physical server host.

   d Read the warning message. Enter **`Yes`** if you want to go ahead with NSX-T Data Center uninstallation.

   ```
   Are you sure you want to remove NSX on this host? (yes/no)
   ```

   e Verify NSX-T Data Center VIBs are deleted on the physical server host by running the following command.

   - (RHEL/SLES/CentOS host) Run `rpm - qa | grep nsx`.
   - (Ubuntu host) Run `dpkg -l | grep nsx`.

   If the NSX-T Data Center VIBs are deleted on the host, the CLI terminal displays success message.

   f To debug errors after running the del nsx command, see logs at `/var/log/nsxcli.log` on the host.

6 In NSX Manager, navigate to the physical server host, and click **Delete**.

7 In the popup window, select **Force Delete** and begin uninstallation.

8 Verify the **Configuration Status** of the host is `Not Configured` state. This state indicates that NSX-T Data Center is completely removed from the host.

Results

After running `del nsx`, all existing host switches are removed, and the host transport node is un-prepared. If any NSX-T Data Center VIBs remain on the host, contact VMware support.

Uninstall NSX-T from a vSphere Lifecycle Manager cluster through NSX Manager

You can trigger uninstallation of NSX-T on a host that is part of a vSphere Lifecycle Manager cluster through NSX Manager.

Procedure

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

2 Select the cluster and click **Remove NSX**.

vSphere Lifecycle Manager removes the NSX solution applied to the cluster in vCenter Server.

Important You cannot detach a transport node profile on a vSphere Lifecycle Manager-enabled cluster. You must remove NSX on the cluster.

3 If vSphere Lifecycle Manager fails to remove the NSX Solution applied to the cluster in vCenter Server or remove NSX-T on one or more transport nodes, then vSphere Lifecycle Manager marks the cluster and or transport nodes in `Uninstall Failed` state.

a Select the cluster and click **Remove NSX** on the cluster to retry uninstallation.

Troubleshooting Installation Issues

18

A list of issues related to NSX-T Data Center installation and configuration

Issue	Solution
Installation Fails Due to Insufficient Space in Bootbank on ESXi host.	https://kb.vmware.com/s/article/74864

Read the following topics next:

- Installation Fails Due to Insufficient Space in Bootbank on ESXi Host
- Host Fails to Install as Transport Node
- NSX Agent Times Out Communicating with NSX Manager
- Troubleshooting Installation
- Node Status of KVM Transport Node is Degraded

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.

Host Fails to Install as Transport Node

Problem

When many hosts are are prepared simultaneously (in non vLCM way) some hosts may fail in the internal step of downloading nsx lcp bundle to the host. Error seen is "Failed to download NSX components on host.

Solution

1. Check the host connectivity and ensure that the "/tmp" folder has enough space.
2. If it is fine then check if there are many hosts getting prepared at this time. Wait for host prep of other hosts to complete.
3. Follow the usual error resolution steps from the UI or API to re trigger the operation on the failed host.

NSX Agent Times Out Communicating with NSX Manager

In a large-scale environment with many transport nodes and VMs on ESXi hosts, NSX agents, which run on ESXi hosts, might time out when communicating with NSX Manager.

Problem

Some operations, such as when a VM vnic tries to attach to a logical switch, fail.
The `/var/run/log/nsx-opsagent.log` has messages such as:

```
level="ERROR" errorCode="MPA41542"] [MP_AddVnicAttachment] RPC call [0e316296-13-14] to NSX
management plane timout
2017-05-15T05:32:13Z nsxa: [nsx@6876 comp="nsx-esx" subcomp="NSXA[VifHandlerThread:-2282640]"
tid="1000017079" level="ERROR" errorCode="MPA42003"] [DoMpVifAttachRpc]
MP_AddVnicAttachment() failed: RPC call to NSX management plane timout
```

Cause

In a large-scale environment, some operations might take longer than usual and fail because the default timeout values are exceeded.

Solution

1 Increase the NSX agent timeout (seconds) value.

   a On the ESXi host, stop the NSX ops agent with the following command:

   ```
   /etc/init.d/nsx-opsagent stop
   ```

   b Edit the file `/etc/vmware/nsx-opsagent/nsxa.json` and change the `vifOperationTimeout` value from 25 seconds to, for example, 55 seconds.

   ```
   "mp" : {
       /* timeout for VIF operation */
       "vifOperationTimeout" : 25,
   ```

   Note This timeout value must be less than the hostd timeout value that you set in step 2.

   c Start the NSX ops agent with the following command:

   ```
   /etc/init.d/nsx-opsagent start
   ```

2 Increase the hostd timeout (seconds) value.

   a On the ESXi host, stop the hostd agent with the following command:

   ```
   /etc/init.d/hostd stop
   ```

   b Edit the file `/etc/vmware/hostd/config.xml`. Under `<opaqueNetwork>`, uncomment the entry for `<taskTimeout>` and change the value from 30 seconds to, for example, 60 seconds.

   ```
   <opaqueNetwork>
       <!-- maximum message size allowed in opaque network manager IPC, in bytes. -->
       <!-- <maxMsgSize> 65536 </maxMsgSize> -->
       <!-- maximum wait time for opaque network response -->
       <!-- <taskTimeout> 30 </taskTimeout> -->
   ```

   c Start the hostd agent with the following command:

   ```
   /etc/init.d/hostd start
   ```

Troubleshooting Installation

This section provides information about troubleshooting installation issues.

Basic Infrastructure Services

The following services must be running on the appliances and hypervisors, also on vCenter Server if it is used as a compute manager.

- NTP

- DNS

Make sure that firewall is not blocking traffic between NSX-T Data Center components and hypervisors. Make sure that the required ports are open between the components.

To flush the DNS cache on the NSX Manager, SSH as root to the manager and run the following command:

```
root@nsx-mgr-01:~# /etc/init.d/resolvconf restart
[ ok ] Restarting resolvconf (via systemctl): resolvconf.service.
```

You can then check the DNS configuration file.

```
root@nsx-mgr-01:~# cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.253.1
search mgt.sg.lab
```

Log in as root user and run `su admin` to launch `nsxcli` on NSX manager. As an admin user, `nsxcli` is default prompt.

Check DNS servers using following `nsxcli` command:

`get name-servers`

```
198.10.10.1
198.10.10.2
198.10.10.3
```

Checking Communication from Host to Controller and Manager

On an ESXi host using NSX-T Data Center CLI commands:

```
esxi-01.corp.local> get managers
- 192.168.110.19   Connected

esxi-01.corp.local> get controllers
 Controller IP    Port     SSL         Status       Is Physical Master   Session State
Controller FQDN
 192.168.110.16   1235   enabled     connected             true
up               NA
```

On a KVM host using NSX-T Data Center CLI commands:

```
kvm-01> get managers
- 192.168.110.19   Connected

kvm-01> get controllers
 Controller IP    Port     SSL         Status       Is Physical Master   Session State
Controller FQDN
 192.168.110.16   1235   enabled     connected             true
up               NA
```

On an ESXi host using host CLI commands:

```
[root@esxi-01:~] esxcli network ip  connection list | grep 1235
tcp         0       0  192.168.110.53:42271                      192.168.110.16:1235
ESTABLISHED     67702  newreno  nsx-proxy
[root@esxi-01:~]
[root@esxi-01:~] esxcli network ip  connection list | grep 5671
tcp         0       0  192.168.110.253:11721             192.168.110.19:5671   ESTABLISHED
2103688  newreno  mpa
tcp         0       0  192.168.110.253:30977             192.168.110.19:5671   ESTABLISHED
2103688  newreno  mpa
```

On a KVM host using host CLI commands:

```
root@kvm-01:/home/vmware# netstat -nap | grep 1235
tcp        0      0 192.168.110.55:53686    192.168.110.16:1235     ESTABLISHED 2554/nsx-proxy
root@kvm-01:/home/vmware#
root@kvm-01:/home/vmware#
root@kvm-01:/home/vmware# netstat -nap | grep 5671
tcp        0      0 192.168.110.55:50108    192.168.110.19:5671     ESTABLISHED 2870/mpa
tcp        0      0 192.168.110.55:50110    192.168.110.19:5671     ESTABLISHED 2870/mpa

root@kvm-01:/home/vmware# tcpdump -i ens32 port 1235 | grep kvm-01
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens32, link-type EN10MB (Ethernet), capture size 262144 bytes
<truncated output>
03:46:27.040461 IP nsxcontroller01.corp.local.1235 > kvm-01.corp.local.38754: Flags [P.], seq
3315301231:3315301275, ack 2671171555, win 323, length 44
03:46:27.040509 IP kvm-01.corp.local.38754 > nsxcontroller01.corp.local.1235: Flags [.], ack
44, win 1002, length 0
^C
<truncated output>
root@kvm-01:/home/vmware#

root@kvm-01:/home/vmware# tcpdump -i ens32 port 5671 | grep kvm-01
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens32, link-type EN10MB (Ethernet), capture size 262144 bytes
03:51:16.802934 IP kvm-01.corp.local.58954 > nsxmgr01.corp.local.amqps: Flags [P.], seq
1153:1222, ack 1790, win 259, length 69
03:51:16.823328 IP nsxmgr01.corp.local.amqps > kvm-01.corp.local.58954: Flags [P.], seq
1790:1891, ack 1222, win 254, length 101
^C
<truncated output>
```

Host Registration Failure

If NSX-T Data Center uses the wrong IP address, host registration will fail. This can happen when a host has multiple IP addresses. Trying to delete the transport node leaves it in the Orphaned state. To resolve the issue:

- On the NSX-T Data Center UI, edit the host and remove all IP addresses except the management one.
- Click on the errors and select **Resolve**.

KVM Host Issues

KVM host issues are sometimes caused by not enough disk space. The `/boot` directory can fill up quickly and cause errors such as:

- Failed to install software on host
- No space left on device

You can run the command **df -h** to check available storage. If the `/boot` directory is at 100%, you can do the following:

- Run `sudo dpkg --list 'linux-image*' | grep ^ii` to see all the kernels installed.
- Run `uname -r` to see your currently running kernel. Do not remove this kernel (linux-image).
- Use `apt-get purge` to remove images you don't need anymore. For example, run `sudo apt-get purge linux-image-3.13.0-32-generic linux-image-3.13.0-33-generic`.
- Reboot the host.
- In NSX Manager, check the errors and select **Resolve**.
- Make sure the VMs are powered on.

Configuration Error when Deploying an Edge VM

After deploying an Edge VM, NSX Manager shows the VM's status as **configuration error**. The manager log has a message similar to the following:

```
nsx-manager NSX - FABRIC [nsx@6876 comp="nsx-manager" errorCode="MP16027" subcomp="manager"]
Edge 758ad396-0754-11e8-877e-005056abf715 is not ready for configuration error occurred,
error detail is NSX Edge configuration has failed. The host does not support required cpu
features: ['aes'].
```

Restarting the edge datapath service and then the VM should resolve the issue.

Force Removing a Transport Node

You can remove a transport node that is stuck in the Orphaned state by making the following API call:

```
DELETE https://<NSX Manager>/api/v1/transport-nodes/<TN ID>?force=true
```

NSX Manager will not do any validations as to whether you have any active VMs running on the host. You are responsible for deleting the N-VDS and VIBs. If you have the node added through Compute Manager, delete the Compute Manager first and then delete the node. The transport node will be deleted as well.

Node Status of KVM Transport Node is Degraded

After performing RHEL upgrade on the transport node, the status of transport node is in `Degraded` state because the physical NICs and Bond status is `Down`.

Problem

After performing RHEL upgrade, the status of transport node goes into `Degraded` state. Physical NICs are `Up`. But the internal span ports created when running packet capture CLI command are in `Down` state.

Cause

The span ports created after running the packet capture CLI went into `Down` state because the CLI command was not terminated gracefully. The span ports were not cleaned up from the database.

Solution

1. Verify presence of internal ports on the transport node. In the KVM LCP, run `ovs-vsctl show`.
2. Delete the span ports by running the `ovs-vsctl del-port <bridge-name> <port-name>`.
3. After deleting the span ports, refresh the host transport node page.
4. Verify that the PNIC/Bond status on the host transport node.

   The transport node status changes from `Degraded` to `Up`.