You can find the most up-to-date technical documentation on the VMware website at:
https://docs.vmware.com/
If you have comments about this documentation, submit your feedback to
docfeedback@vmware.com
Contents

NSX-T Data Center Installation Guide 5

1 Overview of NSX-T Data Center 6
   Key Concepts 7

2 NSX-T Data Center Installation Workflows 11
   NSX-T Data Center Workflow for vSphere 11
   NSX-T Data Center Installation Workflow for KVM 12
   NSX-T Data Center Configuration Workflow for Bare Metal Server 13

3 Preparing for Installation 14
   System Requirements 14
   Ports and Protocols 20
   Installing NSX-T Data Center Components 25

4 Installing NSX-T Data Center on vSphere 32
   Install NSX Manager and Available Appliances 32
   Install an NSX Edge on ESXi Using a vSphere GUI 47

5 Installing NSX-T Data Center on KVM 55
   Set Up KVM 55
   Manage Your Guest VMs in the KVM CLI 60
   Install NSX Manager on KVM 61
   Log In to the Newly Created NSX Manager 64
   Install Third-Party Packages on a KVM Host 64
   Verify Open vSwitch Version on RHEL KVM Hosts 66
   Deploy NSX Manager Nodes to Form a Cluster Using CLI 67
   Install NSX Edge Using ISO File or a PXE 68

6 Configuring Bare Metal Server to Use NSX-T Data Center 80
   Install Third-Party Packages on a Bare Metal Server 80
   Create Application Interface for Bare Metal Server Workloads 82

7 Configure the NSX Manager Cluster 83
   NSX Manager Cluster Requirements 83
   NSX Manager Cluster Requirements for Single, Dual, and Multiple Sites 84
8 Transport Zones and Transport Nodes 87
Create Transport Zones 87
Create an IP Pool for Tunnel Endpoint IP Addresses 89
Enhanced Data Path 91
Configuring Profiles 93
Create a Standalone Host or Bare Metal Server Transport Node 118
Manual Installation of NSX-T Data Center Kernel Modules 135
Create an NSX Edge Transport Node 139
Create an NSX Edge Cluster 142

9 Installing NSX Cloud Components 144
NSX Cloud Architecture and Components 144
Overview of Installing and Configuring NSX Cloud Components for your Public Cloud 146
Install CSM and Connect with NSX Manager 147
Connect Public Cloud with On-prem Deployment 149
Add your Public Cloud Account 153
Deploy or Link NSX Public Cloud Gateway s 163
Undeploy PCG 173

10 Uninstalling NSX-T Data Center 177
Unconfigure an NSX-T Data Center Overlay 177
Remove a Host From NSX-T Data Center or Uninstall NSX-T Data Center Completely 177
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 http://www.vmware.com/support/pubs.
Overview of NSX-T Data Center

In much the same way that server virtualization programmatically creates, snapshots, deletes, and restores software-based virtual machines (VMs), NSX-T Data Center network virtualization programmatically creates, deletes, and restores software-based virtual networks.

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

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

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

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

The NSX Manager appliance is available in three different sizes for different deployment scenarios. A small appliance for lab or proof-of-concept deployments. A medium appliance for deployments up to 64 hosts and a large appliance for customers who deploy to a large-scale environment. See NSX Manager VM System Requirements and Configuration maximums tool.

NSX-T Data Center provides a declarative policy model and imperative-based model.

The declarative policy model provides an easier approach to configure networking and security for applications which is platform-agnostic. You can specify the networking and security requirements for the application environment, which limits errors.

The imperative-based model is available in the Advanced Networking and Security tab, which allows you to configure tasks step-by-step.
Key Concepts

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

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

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

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

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

Fabric Node
Host that 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 fabric.

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

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

Logical Router
NSX-T Data Center routing entity.

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

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

In a multi-tenant cloud, many logical switches might exist side-by-side on the same hypervisor hardware, with each Layer 2 segment isolated from the others. Logical switches can be connected using logical routers, and logical routers can provide uplink ports connected to the external physical network.
<table>
<thead>
<tr>
<th><strong>Logical Switch Port</strong></th>
<th>Logical switch attachment point to establish a connection to a virtual machine network interface or a logical router interface. The logical switch port reports applied switching profile, port state, and link status.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management Plane</strong></td>
<td>Provides single API entry point to the system, persists user configuration, handles user queries, and performs operational tasks on all of the management, control, and data plane nodes in the system. Management plane is also responsible for querying, modifying, and persisting use configuration.</td>
</tr>
<tr>
<td><strong>NSX Edge Cluster</strong></td>
<td>Collection of NSX Edge node appliances that have the same settings as protocols involved in high-availability monitoring.</td>
</tr>
<tr>
<td><strong>NSX Edge Node</strong></td>
<td>Component with the functional goal is to provide computational power to deliver the IP routing and the IP services functions.</td>
</tr>
<tr>
<td><strong>NSX Managed Virtual Distributed Switch or KVM Open vSwitch</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>NSX Manager</strong></td>
<td>Node that hosts the API services, the management plane, and the agent services. NSX Manager is an appliance included in the NSX-T Data Center installation package. You can deploy the appliance in the role of nsx-manager nsx-controller or nsx-cloud-service-manager. Currently, the appliance only supports one role at a time.</td>
</tr>
<tr>
<td><strong>NSX Manager Cluster</strong></td>
<td>A cluster of NSX Managers that can provide high availability.</td>
</tr>
<tr>
<td><strong>Open vSwitch (OVS)</strong></td>
<td>Open source software switch that acts as a virtual switch within XenServer, Xen, KVM, and other Linux-based hypervisors.</td>
</tr>
<tr>
<td><strong>Overlay Logical Network</strong></td>
<td>Logical network implemented using Layer 2-in-Layer 3 tunneling such that the topology seen by VMs is decoupled from that of the physical network.</td>
</tr>
<tr>
<td><strong>Physical Interface (pNIC)</strong></td>
<td>Network interface on a physical server that a hypervisor is installed on.</td>
</tr>
<tr>
<td><strong>Segment</strong></td>
<td>Entity that provides virtual Layer 2 switching for VM interfaces and Gateway interfaces. A segment gives tenant network administrators the logical equivalent of a physical Layer 2 switch, allowing them to connect a set of VMs to a common broadcast domain. A segment is a logical entity independent of the physical hypervisor infrastructure and spans many hypervisors, connecting VMs regardless of their physical location. A segment is also known as a logical switch.</td>
</tr>
</tbody>
</table>
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**
Also known as Tier-0 logical router. It interfaces with the physical network and can be realized as active-active or active-standby cluster. The Tier-0 gateway runs BGP and peers with physical routers. In active-standby mode the gateway can also provide stateful services.

**Tier-0 Logical Router**
Provider logical router is also known as Tier-0 logical router interfaces with the physical network. Tier-0 logical router is a top-tier router and can be realized as active-active or active-standby cluster of services router. The logical router runs BGP and peers with physical routers. In active-standby mode the logical router can also provide stateful services.

**Tier-1 Gateway**
Also known as Tier-1 logical router. It connects to one Tier-0 gateway for northbound connectivity and one or more overlay networks for southbound connectivity. A Tier-1 gateway can be an active-standby cluster that provides stateful services.

**Tier-1 Logical Router**
Tier-1 logical router is the second tier router that connects to one Tier-0 logical router for northbound connectivity and one or more overlay networks for southbound connectivity. Tier-1 logical router can be an active-standby cluster of services router providing stateful services.

**Transport Zone**
Collection of transport nodes that defines the maximum span for logical switches. A transport zone represents a set of similarly provisioned hypervisors and the logical switches that connect VMs on those hypervisors.

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

**Uplink Profile**
Defines policies for the links from hypervisor hosts to NSX-T Data Center logical switches or from NSX Edge nodes to top-of-rack switches. The settings defined by uplink profiles might include teaming policies, active/standby links, the transport VLAN ID, and the MTU setting.
VM Interface (vNIC) Network interface on a virtual machine that provides connectivity between the virtual guest operating system and the standard vSwitch or vSphere distributed switch. The vNIC can be attached to a logical port. You can identify a vNIC based on its Unique ID (UUID).

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

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

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

This chapter includes the following topics:

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

NSX-T Data Center Workflow for vSphere

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

Follow the recommended order of procedures.

1. Review the NSX Manager installation requirements. See NSX Manager Installation.
2. Configure the necessary ports and protocols. See Ports and Protocols.
3. Install the NSX Manager. See Install NSX Manager and Available Appliances.
4. Log in to the newly created NSX Manager. See Log In to the Newly Created NSX Manager.
5. Configure a compute manager. See Add a Compute Manager.
6. Deploy additional NSX Manager nodes to form a cluster. See Deploy NSX Manager Nodes to Form a Cluster from UI.
7. Review the NSX Edge installation requirements. See NSX Edge Installation.
8. Install NSX Edges. See Install an NSX Edge on ESXi Using a vSphere GUI.
9. Create an NSX Edge cluster. See Create an NSX Edge Cluster.
11. Create host transport nodes. See Create a Standalone Host or Bare Metal Server Transport Node or Configure a Managed Host Transport Node.
A virtual switch is created on each host. The management plane sends the host certificates to the control plane, and the management plane pushes control plane information to the hosts. Each host connects to the control plane over SSL presenting its certificate. The control plane validates the certificate against the host certificate provided by the management plane. The controllers accept the connection upon successful validation.

**Post-Installation**

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

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

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

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

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

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

NSX-T Data Center Configuration Workflow for Bare Metal Server

Use the checklist to track your progress when configuring bare metal server to use NSX-T Data Center. Follow the recommended order of procedures.

1. Review the bare metal requirements. See Bare Metal Server System Requirements.
2. Configure the necessary ports and protocols. See Ports and Protocols.
3. Install the NSX Manager. See Install NSX Manager on KVM.
4. Configure third-party packages on the bare metal server. See Install Third-Party Packages on a Bare Metal Server.
5. Create host transport nodes. See Create a Standalone Host or Bare Metal Server Transport Node.
   
   A virtual switch is created on each host. The management plane sends the host certificates to the control plane, and the management plane pushes control plane information to the hosts. Each host connects to the control plane over SSL presenting its certificate. The control plane validates the certificate against the host certificate provided by the management plane. The controllers accept the connection upon successful validation.

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

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

This chapter includes the following topics:

- System Requirements
- Ports and Protocols
- Installing NSX-T Data Center Components

System Requirements

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

NSX Manager VM System Requirements

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

Hypervisor Host Requirements for Transport Nodes

<table>
<thead>
<tr>
<th>Hypervisor Host Requirements for Transport Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>vSphere</td>
</tr>
<tr>
<td>CentOS Linux KVM</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux (RHEL) KVM</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server KVM</td>
</tr>
<tr>
<td>Ubuntu KVM</td>
</tr>
</tbody>
</table>

Table 3-1. Supported Hosts for NSX Manager s

<table>
<thead>
<tr>
<th>Support Description</th>
<th>Hypervisor</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi</td>
<td>For supported hosts, see the VMware Product Interoperability Matrices.</td>
</tr>
<tr>
<td>KVM</td>
<td>RHEL 7.4 and Ubuntu 16.04 LTS</td>
</tr>
</tbody>
</table>
For ESXi hosts, NSX-T Data Center supports the Host Profiles and Auto Deploy features on vSphere 6.7 U1 or higher. See Understanding vSphere Auto Deploy in the VMware ESXi Installation and Setup documentation for more information.

**Caution** On RHEL, the `yum update` command might update the kernel version 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**

It is required that hypervisor hosts running NSX-T Data Center have a compatible NIC card. For supported NIC card, see the VMware Compatibility Guide.

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

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

**Enhanced Data Path NIC Drivers**

Download the supported NIC drivers from the My VMware page.

<table>
<thead>
<tr>
<th>NIC Card</th>
<th>NIC Driver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel 82599</td>
<td>ixgben 1.1.0.26-1OEM.670.0.0.7535516</td>
</tr>
<tr>
<td>Intel(R) Ethernet Controller X710 for 10GbE SFP+</td>
<td>i40en 1.2.0.0-1OEM.670.0.0.8169922</td>
</tr>
<tr>
<td>Intel(R) Ethernet Controller XL710 for 40GbE QSFP+</td>
<td></td>
</tr>
</tbody>
</table>

**NSX Manager VM Resource Requirements**

Thin virtual disk size is 3.8 GB and thick virtual disk size is 200 GB.

<table>
<thead>
<tr>
<th>Appliance Size</th>
<th>Memory</th>
<th>vCPU</th>
<th>Disk Space</th>
<th>VM Hardware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager Extra Small</td>
<td>8 GB</td>
<td>2</td>
<td>200 GB</td>
<td>10 or later</td>
</tr>
<tr>
<td>NSX Manager Small VM</td>
<td>16 GB</td>
<td>4</td>
<td>200 GB</td>
<td>10 or later</td>
</tr>
</tbody>
</table>
### Appliance Size

<table>
<thead>
<tr>
<th>Appliance Size</th>
<th>Memory</th>
<th>vCPU</th>
<th>Disk Space</th>
<th>VM Hardware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager Medium VM</td>
<td>24 GB</td>
<td>6</td>
<td>200 GB</td>
<td>10 or later</td>
</tr>
<tr>
<td>NSX Manager Large VM</td>
<td>48 GB</td>
<td>12</td>
<td>200 GB</td>
<td>10 or later</td>
</tr>
</tbody>
</table>

**Note**  As of NSX-T2.4, the 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.

- The NSX Manager Extra Small VM resource requirements apply only to the Cloud Service Manager.
- The NSX Manager Small VM appliance size is suitable for lab and proof-of-concept deployments, and must not be used in production.
- The NSX Manager Medium VM appliance size is suitable for typical production environments and can support up to 64 hypervisors.
- The NSX Manager Large VM appliance size is suitable for large-scale deployments with more than 64 hypervisors.

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

### NSX Manager Browser Support

<table>
<thead>
<tr>
<th>Browser</th>
<th>Windows 10</th>
<th>Windows 8.1</th>
<th>Ubuntu 14.04</th>
<th>Mac OS X 10.11. 10.12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer 11</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firefox 55</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Chrome 60</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safari 10</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Microsoft Edge 40</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Note**  Internet Explorer 11 in compatibility mode is not supported.

Supported Browser minimum resolution is 1280 x 800 px.

### Network Latency Requirements

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

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

### Storage Requirements

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

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

NSX Edge VM System Requirements

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

NSX Edge nodes are supported only on ESXi-based hosts with Intel-based chipsets. Otherwise, vSphere EVC mode may prevent NSX Edge nodes from starting, showing an error message in the console.

**Note** VMXNET 3 vNIC is supported only for the NSX Edge VM.

**NSX Edge VM Resource Requirements**

<table>
<thead>
<tr>
<th>Appliance Size</th>
<th>Memory</th>
<th>vCPU</th>
<th>Disk Space</th>
<th>VM Hardware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Edge Small</td>
<td>4 GB</td>
<td>2</td>
<td>200 GB</td>
<td>11 or later (vSphere 6.0 or later)</td>
</tr>
<tr>
<td>NSX Edge Medium</td>
<td>8 GB</td>
<td>4</td>
<td>200 GB</td>
<td>11 or later (vSphere 6.0 or later)</td>
</tr>
<tr>
<td>NSX Edge Large</td>
<td>32 GB</td>
<td>8</td>
<td>200 GB</td>
<td>11 or later (vSphere 6.0 or later)</td>
</tr>
</tbody>
</table>

**Note**
- The NSX Edge Small VM appliance size is suitable for lab and proof-of-concept deployments.
- The NSX Edge Medium appliance size is suitable for a typical production environments.
- The NSX Edge Large appliance size is suitable for environments with load balancing. See Scaling Load Balancer Resources in the NSX-T Data Center Administration Guide.

**NSX Edge VM CPU Requirements**

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

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

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel Xeon E7-xxxx (Westmere-EX and later CPU generation)</td>
</tr>
<tr>
<td></td>
<td>Intel Xeon 56xx (Westmere-EP)</td>
</tr>
<tr>
<td></td>
<td>Intel Xeon E5-xxxx (Sandy Bridge and later CPU generation)</td>
</tr>
<tr>
<td></td>
<td>Intel Xeon Platinum (all generations)</td>
</tr>
<tr>
<td></td>
<td>Intel Xeon Gold (all generations)</td>
</tr>
<tr>
<td></td>
<td>Intel Xeon Silver (all generations)</td>
</tr>
<tr>
<td></td>
<td>Intel Xeon Bronze (all generations)</td>
</tr>
</tbody>
</table>
NSX Edge Bare Metal Requirements

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

NSX Edge nodes are supported only on ESXi-based hosts with Intel-based chipsets. Otherwise, vSphere EVC mode may prevent Edge nodes from starting, showing an error message in the console.

NSX Edge Bare Metal Memory, CPU, and Disk Requirements

<table>
<thead>
<tr>
<th>Memory</th>
<th>CPU Cores</th>
<th>Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>32 GB</td>
<td>8</td>
<td>200 GB</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intel Xeon E7-xxxx (Westmere-EX and later CPU generation)</td>
</tr>
<tr>
<td></td>
<td>Intel Xeon 56xx (Westmere-EP)</td>
</tr>
<tr>
<td></td>
<td>Intel Xeon E5-xxxx (Sandy Bridge and later CPU generation)</td>
</tr>
<tr>
<td></td>
<td>Intel Xeon Platinum (all generations)</td>
</tr>
<tr>
<td></td>
<td>Intel Xeon Gold (all generations)</td>
</tr>
<tr>
<td></td>
<td>Intel Xeon Silver (all generations)</td>
</tr>
<tr>
<td></td>
<td>Intel Xeon Bronze (all generations)</td>
</tr>
</tbody>
</table>

NSX Edge Bare Metal Hardware Requirements

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

<table>
<thead>
<tr>
<th>NIC Type</th>
<th>Description</th>
<th>PCI Device ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel XXV710</td>
<td>I40E_DEV_ID_25G_B</td>
<td>0x158A</td>
</tr>
<tr>
<td></td>
<td>I40E_DEV_ID_25G_SFP28</td>
<td>0x158B</td>
</tr>
<tr>
<td>Intel X520/Intel 82599</td>
<td>IXGBE_DEV_ID_82599_KX4</td>
<td>0x10F7</td>
</tr>
<tr>
<td></td>
<td>IXGBE_DEV_ID_82599_KX4_MEZZ</td>
<td>0x1514</td>
</tr>
<tr>
<td></td>
<td>IXGBE_DEV_ID_82599_KR</td>
<td>0x1517</td>
</tr>
<tr>
<td></td>
<td>IXGBE_DEV_ID_82599_COMBO_BACK_PLANE</td>
<td>0x10F8</td>
</tr>
<tr>
<td></td>
<td>IXGBE_SUBDEV_ID_82599_KX4_KR_MEZZ</td>
<td>0x10F9</td>
</tr>
<tr>
<td></td>
<td>IXGBE_DEV_ID_82599_CX4</td>
<td>0x11A9</td>
</tr>
<tr>
<td></td>
<td>IXGBE_DEV_ID_82599_SFP</td>
<td>0x1F72</td>
</tr>
<tr>
<td></td>
<td>IXGBE_SUBDEV_ID_82599_SFP</td>
<td>0x17D0</td>
</tr>
<tr>
<td></td>
<td>IXGBE_SUBDEV_ID_82599_SFP_EM</td>
<td>0x0470</td>
</tr>
<tr>
<td></td>
<td>IXGBE_SUBDEV_ID_82599_SFP_SF2</td>
<td>0x1507</td>
</tr>
<tr>
<td></td>
<td>IXGBE_SUBDEV_ID_82599_SFP_SF_QP</td>
<td>0x154D</td>
</tr>
<tr>
<td></td>
<td>IXGBE_DEV_ID_82599EN_SFP</td>
<td>0x154A</td>
</tr>
<tr>
<td></td>
<td>IXGBE_DEV_ID_82599_XAUI_LOM</td>
<td>0x154A</td>
</tr>
<tr>
<td></td>
<td>IXGBE_DEV_ID_82599_XAUI_LOM</td>
<td>0x1558</td>
</tr>
<tr>
<td></td>
<td>IXGBE_SUBDEV_ID_82599_560FLR</td>
<td>0x1557</td>
</tr>
<tr>
<td></td>
<td>IXGBE_SUBDEV_ID_82599_ECNA_DP</td>
<td>0x1557</td>
</tr>
<tr>
<td></td>
<td>IXGBE_DEV_ID_82599_SFP_SF</td>
<td>0x1558</td>
</tr>
<tr>
<td></td>
<td>IXGBE_DEV_ID_82599_SFP_SF_QP</td>
<td>0x1557</td>
</tr>
<tr>
<td></td>
<td>IXGBE_DEV_ID_82599EN_SFP</td>
<td>0x10FC</td>
</tr>
<tr>
<td></td>
<td>IXGBE_DEV_ID_82599X_AU_LOM</td>
<td>0x151C</td>
</tr>
<tr>
<td>Intel X540</td>
<td>IXGBE_DEV_ID_X540T</td>
<td>0x1528</td>
</tr>
<tr>
<td></td>
<td>IXGBE_DEV_ID_X540T1</td>
<td>0x1560</td>
</tr>
<tr>
<td>Intel X550</td>
<td>IXGBE_DEV_ID_X550T</td>
<td>0x1563</td>
</tr>
<tr>
<td></td>
<td>IXGBE_DEV_ID_X550T1</td>
<td>0x15D1</td>
</tr>
<tr>
<td>Intel X710</td>
<td>I40E_DEV_ID_SFP_X710</td>
<td>0x1572</td>
</tr>
<tr>
<td></td>
<td>I40E_DEV_ID_KX_C</td>
<td>0x1581</td>
</tr>
<tr>
<td></td>
<td>I40E_DEV_ID_10G_BASE_T</td>
<td>0x1586</td>
</tr>
<tr>
<td>Intel XL710</td>
<td>I40E_DEV_ID_KX_B</td>
<td>0x1580</td>
</tr>
<tr>
<td></td>
<td>I40E_DEV_ID_QSFP_A</td>
<td>0x1583</td>
</tr>
<tr>
<td></td>
<td>I40E_DEV_ID_QSFP_B</td>
<td>0x1584</td>
</tr>
<tr>
<td></td>
<td>I40E_DEV_ID_QSFP_C</td>
<td>0x1585</td>
</tr>
<tr>
<td>Cisco VIC 1387</td>
<td>Cisco UCS Virtual Interface Card 1387</td>
<td>0x0043</td>
</tr>
</tbody>
</table>
Bare Metal Server System Requirements

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

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

### Bare Metal Server Requirements

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Version</th>
<th>CPU Cores</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS Linux</td>
<td>7.4</td>
<td>4</td>
<td>16 GB</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux (RHEL)</td>
<td>7.5 and 7.4</td>
<td>4</td>
<td>16 GB</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server</td>
<td>12 SP3</td>
<td>4</td>
<td>16 GB</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>18.04 and 16.04.2 LTS</td>
<td>4</td>
<td>16 GB</td>
</tr>
</tbody>
</table>

### 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.

**Note** The required ports and protocols must be open on both the physical and host hypervisor firewalls.
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, netcpa, nsx-agent, OVS
- ESXi: netcpa, ESX-DP (in the kernel)

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

**NSX Cloud Note** See [Enable Access to ports and protocols on CSM for Hybrid Connectivity](#) for a list of ports required for deploying NSX Cloud.

**TCP and UDP Ports Used by NSX Manager**

NSX Manager uses certain TCP and UDP ports to communicate with other components and products. These ports must be open in the firewall.

You can use an API call or CLI command to specify custom ports for transferring files (22 is the default) and for exporting Syslog data (514 and 6514 are the defaults). If you do, you will need to configure the firewall accordingly.
**Table 3-2. TCP and UDP Ports Used by NSX Manager**

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Controllers, NSX Edge nodes, Transport Nodes</td>
<td>NSX Manager</td>
<td>5671</td>
<td>TCP</td>
<td>NSX messaging</td>
</tr>
<tr>
<td>NSX Controllers, NSX Edge nodes, Transport Nodes, vCenter Server</td>
<td>NSX Manager</td>
<td>8080</td>
<td>TCP</td>
<td>Install-upgrade HTTP repository</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>Datastore</td>
<td>9000</td>
<td>TCP</td>
<td>Log Insight agent</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>DNS Servers</td>
<td>53</td>
<td>TCP</td>
<td>DNS</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>DNS Servers</td>
<td>53</td>
<td>UDP</td>
<td>DNS</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>Management SCP Servers</td>
<td>22</td>
<td>TCP</td>
<td>SSH (upload support bundle, backups, etc.)</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>NTP Servers</td>
<td>123</td>
<td>UDP</td>
<td>NTP</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>SNMP Servers</td>
<td>161, 162</td>
<td>TCP</td>
<td>SNMP</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>SNMP Servers</td>
<td>161, 162</td>
<td>UDP</td>
<td>SNMP</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>Syslog Servers</td>
<td>514</td>
<td>TCP</td>
<td>Syslog</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>Syslog Servers</td>
<td>514</td>
<td>UDP</td>
<td>Syslog</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>Syslog Servers</td>
<td>6514</td>
<td>TCP</td>
<td>Syslog</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>Syslog Servers</td>
<td>6514</td>
<td>UDP</td>
<td>Syslog</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>Traceroute Destination</td>
<td>3343, 4 - 3352, 3</td>
<td>UDP</td>
<td>Traceroute</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>vCenter Server</td>
<td>80</td>
<td>TCP</td>
<td>NSX Manager to compute manager (vCenter Server) communication, when configured.</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>vCenter Server</td>
<td>443</td>
<td>TCP</td>
<td>NSX Manager to compute manager (vCenter Server) communication, when configured.</td>
</tr>
<tr>
<td>NTP Servers</td>
<td>NSX Manager</td>
<td>123</td>
<td>UDP</td>
<td>NTP</td>
</tr>
<tr>
<td>Management Clients</td>
<td>NSX Manager</td>
<td>22</td>
<td>TCP</td>
<td>SSH (Disabled by default)</td>
</tr>
<tr>
<td>Management Clients</td>
<td>NSX Manager</td>
<td>443</td>
<td>TCP</td>
<td>NSX API server</td>
</tr>
<tr>
<td>SNMP Servers</td>
<td>NSX Manager</td>
<td>161</td>
<td>UDP</td>
<td>SNMP</td>
</tr>
</tbody>
</table>

**TCP and UDP Ports Used by NSX Edge**

NSX Edge uses certain TCP and UDP ports to communicate with other components and products. These ports must be open in the firewall.
You can use an API call or CLI command to specify custom ports for transferring files (22 is the default) and for exporting Syslog data (514 and 6514 are the defaults). If you do, you will need to configure the firewall accordingly.

Table 3-3. TCP and UDP Ports Used by NSX Edge

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Clients</td>
<td>NSX Edge nodes</td>
<td>22</td>
<td>TCP</td>
<td>SSH (Disabled by default)</td>
</tr>
<tr>
<td>NSX Agent</td>
<td>NSX Edge nodes</td>
<td>5555</td>
<td>TCP</td>
<td>NSX Cloud - Agent on instance communicates to NSX Cloud Gateway.</td>
</tr>
<tr>
<td>NSX Edge nodes</td>
<td>DNS Servers</td>
<td>53</td>
<td>UDP</td>
<td>DNS</td>
</tr>
<tr>
<td>NSX Edge nodes</td>
<td>Management SCP or SSH Servers</td>
<td>22</td>
<td>TCP</td>
<td>SSH</td>
</tr>
<tr>
<td>NSX Edge nodes</td>
<td>NSX Controller nodes</td>
<td>1235</td>
<td>TCP</td>
<td>netcpa</td>
</tr>
<tr>
<td>NSX Edge nodes</td>
<td>NSX Edge nodes</td>
<td>1167</td>
<td>TCP</td>
<td>DHCP backend</td>
</tr>
<tr>
<td>NSX Edge nodes</td>
<td>NSX Edge nodes</td>
<td>2480</td>
<td>TCP</td>
<td>Nestdb</td>
</tr>
<tr>
<td>NSX Edge nodes</td>
<td>NSX Edge nodes</td>
<td>6666</td>
<td>TCP</td>
<td>NSX Cloud - NSX Edge local communication.</td>
</tr>
<tr>
<td>NSX Edge nodes</td>
<td>NSX Edge nodes</td>
<td>50263</td>
<td>UDP</td>
<td>High-Availability</td>
</tr>
<tr>
<td>NSX Edge nodes</td>
<td>NSX Manager node</td>
<td>443</td>
<td>TCP</td>
<td>HTTPS</td>
</tr>
<tr>
<td>NSX Edge nodes</td>
<td>NSX Manager node</td>
<td>5671</td>
<td>TCP</td>
<td>NSX messaging</td>
</tr>
<tr>
<td>NSX Edge nodes</td>
<td>NSX Manager node</td>
<td>8080</td>
<td>TCP</td>
<td>NAPI, NSX-T Data Center upgrade</td>
</tr>
<tr>
<td>NSX Edge nodes</td>
<td>NTP Servers</td>
<td>123</td>
<td>UDP</td>
<td>NTP</td>
</tr>
<tr>
<td>NSX Edge nodes</td>
<td>OpenStack Nova API Server</td>
<td>3000 - 9000</td>
<td>TCP</td>
<td>Metadata proxy</td>
</tr>
<tr>
<td>NSX Edge nodes</td>
<td>SNMP Servers</td>
<td>161, 162</td>
<td>TCP</td>
<td>SNMP</td>
</tr>
<tr>
<td>NSX Edge nodes</td>
<td>SNMP Servers</td>
<td>161, 162</td>
<td>UDP</td>
<td>SNMP</td>
</tr>
<tr>
<td>NSX Edge nodes</td>
<td>Syslog Servers</td>
<td>514</td>
<td>TCP</td>
<td>Syslog</td>
</tr>
<tr>
<td>NSX Edge nodes</td>
<td>Syslog Servers</td>
<td>514</td>
<td>UDP</td>
<td>Syslog</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>Syslog Servers</td>
<td>6514</td>
<td>TCP</td>
<td>Syslog</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>Syslog Servers</td>
<td>6514</td>
<td>UDP</td>
<td>Syslog</td>
</tr>
</tbody>
</table>
Table 3-3. TCP and UDP Ports Used by NSX Edge (Continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Edge nodes</td>
<td>Traceroute Destination</td>
<td>33434 - 33523</td>
<td>UDP</td>
<td>Traceroute</td>
</tr>
<tr>
<td>NSX Edge nodes, Transport Nodes</td>
<td>NSX Edge nodes</td>
<td>3784, 3785</td>
<td>UDP</td>
<td>BFD between the Transport Node TEP IP address in the data.</td>
</tr>
<tr>
<td>NTP Servers</td>
<td>NSX Edge nodes</td>
<td>123</td>
<td>UDP</td>
<td>NTP</td>
</tr>
<tr>
<td>SNMP Servers</td>
<td>NSX Edge nodes</td>
<td>161</td>
<td>UDP</td>
<td>SNMP</td>
</tr>
</tbody>
</table>

TCP and UDP Ports Used by ESXi, KVM Hosts, and Bare Metal Server

ESXi, KVM hosts, and bare metal server when used as transport nodes need certain TCP and UDP ports available.

Table 3-4. TCP and UDP Ports Used by ESXi and KVM Hosts

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi host</td>
<td>NSX Controller</td>
<td>123</td>
<td>TCP</td>
<td>Control Plane - LCP to CCP communication</td>
</tr>
<tr>
<td>ESXi host</td>
<td>NSX Manager</td>
<td>567</td>
<td>TCP</td>
<td>AMPQ Communication channel to NSX Manager</td>
</tr>
<tr>
<td>ESXi host</td>
<td>NSX Manager</td>
<td>808</td>
<td>TCP</td>
<td>Install and upgrade HTTP repository</td>
</tr>
<tr>
<td>ESXi and KVM host</td>
<td>NSX Manager</td>
<td>443</td>
<td>TCP</td>
<td>Management and provisioning connection</td>
</tr>
<tr>
<td>ESXi and KVM host</td>
<td>NSX Manager</td>
<td>443</td>
<td>TCP</td>
<td>Install and upgrade HTTP repository</td>
</tr>
<tr>
<td>GENEVE Termination End Point (TEP)</td>
<td>GENEVE Termination End Point (TEP)</td>
<td>608</td>
<td>UDP</td>
<td>Transport network</td>
</tr>
<tr>
<td>KVM host</td>
<td>NSX Manager</td>
<td>567</td>
<td>TCP</td>
<td>AMPQ Communication channel to NSX Manager</td>
</tr>
<tr>
<td>KVM host</td>
<td>NSX Controller</td>
<td>123</td>
<td>TCP</td>
<td>Control Plane - LCP to CCP communication</td>
</tr>
<tr>
<td>KVM host</td>
<td>NSX Manager</td>
<td>808</td>
<td>TCP</td>
<td>Install and upgrade HTTP repository</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>ESXi host</td>
<td>443</td>
<td>TCP</td>
<td>Management and provisioning connection</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>KVM host</td>
<td>443</td>
<td>TCP</td>
<td>Management and provisioning connection</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>Syslog Servers</td>
<td>514</td>
<td>TCP</td>
<td>Syslog</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>Syslog Servers</td>
<td>514</td>
<td>UDP</td>
<td>Syslog</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>Syslog Servers</td>
<td>651</td>
<td>TCP</td>
<td>Syslog</td>
</tr>
</tbody>
</table>
Table 3-4. TCP and UDP Ports Used by ESXi and KVM Hosts (Continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager</td>
<td>Syslog Servers</td>
<td>651</td>
<td>UDP</td>
<td>Syslog</td>
</tr>
<tr>
<td>NSX-T Data Center transport</td>
<td>NSX-T Data Center transport node</td>
<td>378</td>
<td>UDP</td>
<td>BFD Session between TEPs, in the datapath using TEP interface</td>
</tr>
</tbody>
</table>

Installing NSX-T Data Center Components

You must install the NSX Manager and NSX Edge core components to use NSX-T Data Center.

NSX Manager Installation

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

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

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

NSX Manager Deployment, Platform, and Installation Requirements

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

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported deployment methods</td>
<td>OVA/OVF</td>
</tr>
<tr>
<td>Supported platforms</td>
<td>QCOW2</td>
</tr>
<tr>
<td>Supported platforms</td>
<td>See NSX Manager VM System Requirements.</td>
</tr>
<tr>
<td>IP address</td>
<td>An NSX Manager must have a static IP address. You cannot change the IP address after installation.</td>
</tr>
<tr>
<td>NSX-T Data Center appliance password</td>
<td>At least 12 characters</td>
</tr>
<tr>
<td></td>
<td>At least one lower-case letter</td>
</tr>
<tr>
<td></td>
<td>At least one upper-case letter</td>
</tr>
<tr>
<td></td>
<td>At least one digit</td>
</tr>
<tr>
<td></td>
<td>At least one special character</td>
</tr>
<tr>
<td></td>
<td>At least five different characters</td>
</tr>
<tr>
<td></td>
<td>No dictionary words</td>
</tr>
<tr>
<td></td>
<td>No palindromes</td>
</tr>
<tr>
<td></td>
<td>More than four monotonic character sequence is not allowed</td>
</tr>
<tr>
<td>Requirements</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Hostname</td>
<td>When installing NSX Manager, 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 <code>nsx-manager</code>. For more information about hostname restrictions, see <a href="https://tools.ietf.org/html/rfc952">https://tools.ietf.org/html/rfc952</a> and <a href="https://tools.ietf.org/html/rfc1123">https://tools.ietf.org/html/rfc1123</a>.</td>
</tr>
<tr>
<td>VMware Tools</td>
<td>The NSX Manager VM running on ESXi has VMTools installed. Do not remove or upgrade VMTools.</td>
</tr>
</tbody>
</table>
| System       | - Verify that the system requirements are met. See [System Requirements](#).  
                - Verify that the required ports are open. See [Ports and Protocols](#).  
                - Verify that a datastore is configured and accessible on the ESXi host.  
                - Verify that you have the IP address and gateway, DNS server IP addresses, domain search list, and the NTP server IP address for the NSX Manager to use.  
                - If you do not already have one, create the target VM port group network. Place the NSX-T Data Center appliances on a management VM network.  
                - If you have multiple management networks, you can add static routes to the other networks from the NSX-T Data Center appliance.  
                - Plan your NSX Manager IPv4 or IPv6 IP addressing scheme. |
| OVF Privileges| Verify that you have adequate privileges to deploy an OVF template on the ESXi host. A management tool that can deploy OVF templates, such as vCenter Server or the vSphere Client. The OVF deployment tool must support configuration options to allow for manual configuration.  
                OVF tool version must be 4.0 or later. |
| Client Plug-in| The Client Integration Plug-in must be installed. |

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

### NSX Manager Installation Scenarios

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

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

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

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

By enabling FQDN usage (DNS) on NSX Managers, the IP address of the Managers can change without affecting the transport nodes.

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

**Note** Enabling FQDN usage (DNS) on NSX Managers is required for multisite Lite and NSXNSX Cloud and deployments. (It is optional for all other deployment types.) See *Multisite Deployment of NSX-T Data Center* in the *NSX-T Data Center Administration Guide* and *Chapter 9 Installing NSX Cloud Components* in this guide.

### Publishing the FQDNs of the NSX Managers

After installing the NSX-T Data Center core components and CSM, to enable NAT using FQDN you would set up the entries for lookup and reverse lookup in the NSX-T DNS server in your deployment.

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

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

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

Example response:

```
{
    "publish_fqdns": true,
    "_revision": 1
}
```
See the *NSX-T Data Center API Guide* for details.

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

### Validating Access via FQDN by Transport Nodes

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

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

Example response:

<table>
<thead>
<tr>
<th>Controller IP</th>
<th>Port</th>
<th>SSL</th>
<th>Status</th>
<th>Is Physical Master</th>
<th>Session State</th>
<th>Controller FQDN</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.60.5</td>
<td>1235</td>
<td>enabled</td>
<td>connected</td>
<td>true</td>
<td>up</td>
<td>nsxmgr.corp.com</td>
</tr>
</tbody>
</table>

### NSX Edge Installation

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 load 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 3-5. NSX Edge Deployment, Platforms, and Installation Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported deployment methods</td>
<td>- OVA/VOF</td>
</tr>
<tr>
<td>Supported platforms</td>
<td>NSX Edge is supported only on ESXi or on bare metal. NSX Edge is not supported on KVM.</td>
</tr>
<tr>
<td>PXE installation</td>
<td>The Password string must be encrypted with sha-512 algorithm for the root and admin user password.</td>
</tr>
<tr>
<td>Requirements</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| NSX-T Data Center appliance password | - At least 12 characters  
- At least one lower-case letter  
- At least one upper-case letter  
- At least one digit  
- At least one special character  
- At least five different characters  
- No dictionary words  
- No palindromes  
- More than four monotonic character sequence is not allowed |
| Hostname                           | When installing NSX Edge, specify a hostname that does not contain invalid characters such as an underscore. If the hostname contains any invalid character, after deployment the hostname will be set to localhost. For more information about hostname restrictions, see https://tools.ietf.org/html/rfc952 and https://tools.ietf.org/html/rfc1123. |
| VMware Tools                       | The NSX Edge VM running on ESXi has VMTools installed. Do not remove or upgrade VMTools.                                                    |
| System                             | Verify that the system requirements are met. See NSX Edge VM System Requirements.                                                           |
| Ports                              | Verify that the required ports are open. See Ports and Protocols.                                                                           |
| IP Addresses                       | If you have multiple management networks, you can add static routes to the other networks from the NSX-T Data Center appliance.  
Plan your NSX Edge IPv4 or IPv6 IP addressing scheme.                                                                                     |
| OVF Template                        | - Verify that you have adequate privileges to deploy an OVF template on the ESXi host.  
- Verify that hostnames do not include underscores. Otherwise, the hostname is set to nsx-manager.  
- 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 servers in an Edge cluster.                                                           |
NSX Edge Installation Scenarios

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

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

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

- If the password for the **audit** user does not meet the complexity requirements, the user account is disabled. To enable the account, log in to NSX Edge through SSH or at the console as the **admin** user and run the command `set user audit` to set the **audit** user's password (the current password is an empty string).

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

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

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

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

Join NSX Edge with the Management Plane

Joining NSX Edges with the management plane ensures that the NSX Manager and NSX Edges can communicate with each other.

**Prerequisites**

Verify that you have admin privileges to log in to the NSX Edges and NSX Manager appliance.

**Procedure**

1. Open an SSH session to the NSX Manager appliance.
2. Open an SSH session to the NSX Edge.
3 On the NSX Manager appliance, run the `get certificate api thumbprint` command. The command output is a string of alphanumeric numbers that is unique to this NSX Manager. For example:

```
NSX-Manager1> get certificate api thumbprint
...
```

4 On the NSX Edge, run the `join management-plane` command. Provide the following information:

- Hostname or IP address of the NSX Manager with an optional port number
- Username of the NSX Manager
- Certificate thumbprint of the NSX Manager
- Password of the NSX Manager

```
NSX-Edge1> join management-plane NSX-Manager1 username admin thumbprint <NSX-Manager1's-thumbprint>
Password for API user: <NSX-Manager1's-password>
Node successfully registered and Edge restarted
```

Repeat this command on each NSX Edge node.

5 Verify the result by running the `get managers` command on your NSX Edges.

```
nsx-edge-1> get managers
- 192.168.110.47   Connected
```

6 In the NSX Manager UI, select **System > Fabric > Nodes > Edge Transport Nodes** page.

The NSX Manager connectivity should be Up. If NSX Manager connectivity is not Up, try refreshing the browser window.

**What to do next**

Add the NSX Edge as a transport node. See **Create an NSX Edge Transport Node**.
Installing NSX-T Data Center on vSphere

You can install the NSX-T Data Center components, NSX Manager and NSX Edge using the UI or CLI. Make sure that you have the supported vSphere version. See vSphere support.

This chapter includes the following topics:

- Install NSX Manager and Available Appliances
- Install an NSX Edge on ESXi Using a vSphere GUI

Install NSX Manager and Available Appliances

You can use the vSphere Client to deploy NSX Manager or the Cloud Service Manager as a virtual appliance.

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

Prerequisites

- Verify that the system requirements are met. See System Requirements.
- Verify that the required ports are open. See Ports and Protocols.
- Verify that a datastore is configured and accessible on the ESXi host.
- Verify that you have the IP address and gateway, DNS server IP addresses, domain search list, and the NTP server IP address for the NSX Manager to use.
- If you do not already have one, create the target VM port group network. Place the NSX-T Data Center appliances on a management VM network.
  - If you have multiple management networks, you can add static routes to the other networks from the NSX-T Data Center appliance.
- Plan your NSX Manager IPv4 or IPv6 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 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.

5 Enter a name for the NSX Manager VM.
   The name you enter appears in the vSphere inventory.

6 Select a compute resource for the NSX Manager appliance.
   - 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 Verify the OVF template details.

8 For an optimal performance, reserve memory for the NSX Manager appliance.
   Set the reservation to ensure that NSX Manager has sufficient memory to run efficiently. See **NSX Manager VM System Requirements**.

9 Select a datastore to store the NSX Manager appliance files.

10 Select a destination network for each source network.

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

12 Enter the NSX Manager system root, CLI admin, and audit passwords.
   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

13 Enter the hostname of the NSX Manager.

14 Accept the default **nsx-manager nsx-controller** role for VM.
   Select the **nsx-cloud-service-manager** role from the drop-down menu to install the NSX Cloud appliance.

15 Enter the default gateway, management network IPv4, management network netmask, DNS, and NTP IP address.
Enable SSH and allow root SSH login to the NSX Manager command line.

By default, these options are disabled for security reasons.

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

The installation might take 7-8 minutes.

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

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

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

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

**Note**  The following services are not running by default: liagent, migration-coordinator, and snmp. You can start them as follows:
- `start service liagent`
- `start service migration-coordinator`
- For SNMP:
  ```
  set snmp community <community-string>
  start service snmp
  ```

Verify that your NSX Manager has the required connectivity.

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

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

**What to do next**

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

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

If you prefer to automate or use CLI for the NSX Manager installation, you can use the VMware OVF Tool, which is a command-line utility.
By default, `nsx_isSSHEnabled` and `nsx_allowSSHRootLogin` are both disabled for security reasons. When they are disabled, you cannot SSH or log in to the NSX Manager command line. If you enable `nsx_isSSHEnabled` but not `nsx_allowSSHRootLogin`, you can SSH to NSX Manager but you cannot log in as root.

**Prerequisites**

- Verify that the system requirements are met. See System Requirements.
- Verify that the required ports are open. See Ports and Protocols.
- Verify that a datastore is configured and accessible on the ESXi host.
- Verify that you have the IP address and gateway, DNS server IP addresses, domain search list, and the NTP server IP address for the NSX Manager to use.
- If you do not already have one, create the target VM port group network. Place the NSX-T Data Center appliances on a management VM network.
  
  If you have multiple management networks, you can add static routes to the other networks from the NSX-T Data Center appliance.
- Plan your NSX Manager IPv4 or IPv6 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:
     - Windows example:

   ```
   C:\Program Files\VMware\VMware OVF Tool>ovftool 
   --sourceType=OVA 
   --name=nsx-manager 
   --X:injectOvfEnv 
   --X:logFile=<filepath>\nsxovftool.log 
   --allowExtraConfig 
   --datastore=<datastore name> 
   --network=<network name> 
   --acceptAllEulas 
   --noSSLVerify 
   --diskMode=thin 
   --powerOn 
   --prop:"nsx_role=nsx-manager nsx-controller" 
   --prop:"nsx_ip_0=10.168.110.75" 
   --prop:"nsx_netmask_0=255.255.255.0" 
   --prop:"nsx_gateway_0=10.168.110.1" 
   --prop:"nsx_dns1_0=10.168.110.10" 
   --prop:"nsx_domain_0=corp.local" 
   --prop:"nsx_ntp_0=10.168.110.10" 
   --prop:"nsx_isSSHEnabled=<True|False>" 
   --prop:"nsx_allowSSHRootLogin=<True|False>" 
   --prop:"nsx_passwd_0=<password>" 
   --prop:"nsx_cli_passwd_0=<password>" 
   ```
Note The above Windows code block uses the backslash (\) to indicate the continuation of the command line. In actual use, omit the backslash and put the entire command in a single line.

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

**Linux example:**

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

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

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

mgresxhost01="192.168.110.113"

ovftool --noSSLVerify --skipManifestCheck --powerOn
--deploymentOption=$mgrformfactor
--diskMode=thin
--allowExtraConfig
--ipProtocol=IPv4
--ipAllocationPolicy=$ipAllocationPolicy
--datastore=$mgrdatastore
--network=$mgrnetwork
--name=$mgrname01
--prop:nsx_hostname=$mgrhostname01
--prop:nsx_role="nsx-manager nsx-controller"
--prop:nsx_ip_0=$mgrip01
--prop:nsx_netmask_0=$mgrnetmask
--prop:nsx_gateway_0=$mgrgw
--prop:nsx_dns1_0=$mgrdns
--prop:nsx_ntp_0=$mgrntp
--prop:nsx_passwd_0=$mgrpasswd
--prop:nsx_cli_passwd_0=$mgrpasswd
```
Opening OVA source: nsx--<component>-.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://root:<password>@10.168.110.51
Deploying to VI: vi://root:<password>@10.168.110.51
Transfer Completed
Powering on VM: nsx-manager nsx-controller
Task Completed
Completed successfully

For a host managed by vCenter Server:

Windows example:

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

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

```bash
```
The result should look something like this:

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

2. For an optimal performance, reserve memory for the NSX Manager appliance.
   Set the reservation to ensure that NSX Manager has sufficient memory to run efficiently. See NSX Manager VM System Requirements.

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

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

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

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

What to do next

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

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

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

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

1. Log in to the VM as root.

2. Change the value for the parameter GRUB_HIDDEN_TIMEOUT in the /etc/default/grub file.
   
   \[GRUB_HIDDEN_TIMEOUT=2\]

3. Update the GRUB configuration.
   
   \[update-grub\]

4. (Optional) Change the GRUB password in the /etc/grub.d/40_custom file.
   
   The default password is VMware1.

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).
   
   After you upgrade the Management plane, 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, including how to join or leave the program.

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 find out about changes such as, the addition or removal of hosts or VMs and updates its inventory accordingly. It is optional to add a compute manager, because NSX-T Data Center gets the inventory information even without a compute manager, such as standalone hosts and VMs.

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

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

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

**Prerequisites**

- Verify that you use the supported vSphere version. See Supported vSphere version.
- IPv6 and IPv4 communication with vCenter Server.
Verify that you use the recommended number of compute managers. See https://configmax.vmware.com/home.

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

**Procedure**

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and Description</td>
<td>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.</td>
</tr>
<tr>
<td>Domain Name/IP Address</td>
<td>Type the IP address of the vCenter Server.</td>
</tr>
<tr>
<td>Type</td>
<td>Keep the default option.</td>
</tr>
<tr>
<td>Username and Password</td>
<td>Type the vCenter Server login credentials.</td>
</tr>
<tr>
<td>Thumbprint</td>
<td>Type the vCenter Server SHA-256 thumbprint algorithm value.</td>
</tr>
</tbody>
</table>

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.

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:

   ```plaintext
   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.

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.

**Deploy NSX Manager Nodes to Form a Cluster from UI**

You can deploy multiple NSX Manager nodes to provide high availability and reliability.
After the new nodes are deployed, these nodes connect to the NSX Manager node to form a cluster. The recommended number of clustered NSX Manager nodes is three.

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

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

**Prerequisites**
- Verify that an NSX Manager node is installed. See Install NSX Manager and Available Appliances.
- Verify that compute manager is configured. See Add a Compute Manager.
- Verify that the system requirements are met. See System Requirements.
- Verify that the required ports are open. See Ports and Protocols.
- Verify that a datastore is configured and accessible on the ESXi host.
- Verify that you have the IP address and gateway, DNS server IP addresses, domain search list, and the NTP server IP address for the NSX Manager to use.
- If you do not already have one, create the target VM port group network. Place the NSX-T Data Center appliances on a management VM network.
  - If you have multiple management networks, you can add static routes to the other networks from the NSX-T Data Center appliance.

**Procedure**
1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Select **System > Overview > Add Nodes**.
3. Enter the NSX Manager common attribute details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute Manager</td>
<td>Registered resource compute manager is populated.</td>
</tr>
<tr>
<td>Enable SSH</td>
<td>Toggle the button to allow an SSH login to the new NSX Manager node.</td>
</tr>
<tr>
<td>Enable Root Access</td>
<td>Toggle the button to allow the root access to the new NSX Manager node.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>CLI Username and Password</strong></td>
<td>Set the CLI password and password confirmation for the new node. Your password must comply with the password strength restrictions.</td>
</tr>
<tr>
<td><strong>Confirmation</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- At least 12 characters</td>
</tr>
<tr>
<td></td>
<td>- At least one lower-case letter</td>
</tr>
<tr>
<td></td>
<td>- At least one upper-case letter</td>
</tr>
<tr>
<td></td>
<td>- At least one digit</td>
</tr>
<tr>
<td></td>
<td>- At least one special character</td>
</tr>
<tr>
<td></td>
<td>- At least five different characters</td>
</tr>
<tr>
<td></td>
<td>- No dictionary words</td>
</tr>
<tr>
<td></td>
<td>- No palindromes</td>
</tr>
<tr>
<td></td>
<td>- More than four monotonic character sequence is not allowed</td>
</tr>
<tr>
<td></td>
<td>The CLI username is already set to admin.</td>
</tr>
<tr>
<td><strong>Root Password and Password</strong></td>
<td>Set the root password and password confirmation for the new node. Your password must comply with the password strength restrictions.</td>
</tr>
<tr>
<td><strong>Confirmation</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- At least 12 characters</td>
</tr>
<tr>
<td></td>
<td>- At least one lower-case letter</td>
</tr>
<tr>
<td></td>
<td>- At least one upper-case letter</td>
</tr>
<tr>
<td></td>
<td>- At least one digit</td>
</tr>
<tr>
<td></td>
<td>- At least one special character</td>
</tr>
<tr>
<td></td>
<td>- At least five different characters</td>
</tr>
<tr>
<td></td>
<td>- No dictionary words</td>
</tr>
<tr>
<td></td>
<td>- No palindromes</td>
</tr>
<tr>
<td></td>
<td>- More than four monotonic character sequence is not allowed</td>
</tr>
<tr>
<td><strong>DNS Servers</strong></td>
<td>Enter the DNS server IP address available in the vCenter Server.</td>
</tr>
<tr>
<td><strong>NTP Servers</strong></td>
<td>Enter the NTP server IP address.</td>
</tr>
</tbody>
</table>

4 Enter the NSX Manager node details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the NSX Manager node.</td>
</tr>
<tr>
<td><strong>Cluster</strong></td>
<td>Designate the cluster the node is going to join from the drop-down menu.</td>
</tr>
<tr>
<td><strong>Resource Pool or Host</strong></td>
<td>Assign either a resource pool or a host for the node from the drop-down menu.</td>
</tr>
<tr>
<td><strong>Datastore</strong></td>
<td>Select a datastore for the node files from the drop-down menu.</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>Assign the network from the drop-down menu.</td>
</tr>
<tr>
<td><strong>Management IP/Netmask</strong></td>
<td>Enter the IP address and netmask.</td>
</tr>
<tr>
<td><strong>Management Gateway</strong></td>
<td>Enter the gateway IP address.</td>
</tr>
</tbody>
</table>

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

Repeat steps 3-4.

6 Click **Finish**.

The new nodes are deployed. You can track the deployment process on the **System > Overview** page or the vCenter Server.
7 Wait for 10-15 minutes for the deployment, cluster formation, and repository synchronization to complete.

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

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

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

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

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

- `start service liagent`
- `start service migration-coordinator`
- For SNMP:

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

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

11 Verify that your NSX Manager has the required connectivity.

Make sure that you can perform the following tasks.

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

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

**What to do next**

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

**Deploy NSX Manager Nodes to Form a Cluster Using CLI**

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

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

Procedure

1. Open an SSH session to the first deployed NSX Manager node.
2. Log in with the administrator credentials.
3. On the NSX Manager node, run the `get certificate api thumbprint` command. The command output is a string of numbers that is unique to this NSX Manager.
4. Run the `get cluster config` command to get the first deployed NSX Manager cluster ID.
5. Add a NSX Manager node to the cluster.

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

   Provide the following NSX Manager information:
   - Hostname or IP address node that you want to join
   - Cluster ID
   - User name
   - Password
   - Certificate thumbprint

   You can use the CLI command or API call.

   **CLI command**
   ```
   host> join <NSX-Manager-IP> cluster-id <cluster-id> username<NSX-Manager-username>
   password<NSX-Manager-password> thumbprint <NSX-Manager1's-thumbprint>
   ```

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

   The joining and cluster stabilizing process might 10-15 minutes.
6. Add the third NSX Manager node to the cluster.
   Repeat step 5.
7. Verify the cluster status by running the `get cluster status` command on your hosts.
8. Select **System > Overview** and verify the cluster connectivity.

What to do next

Create a transport zone. See Create a Standalone Host or Bare Metal Server Transport Node.
Configure a Virtual IP Address for a Cluster

Assign a virtual IP address (VIP) to a member of the NSX-T cluster to provide fault tolerance and high availability to NSX-T manager nodes.

NSX-T managers of a cluster become part of an HTTPS group to service API and UI requests of users. 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.

If the leader node that owns VIP goes down, NSX-T elects a new leader. The new leader sends out a GARP request to assume ownership of the VIP. The new leader node receives any new API and UI requests from users.

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 went down, user must reauthenticate credentials so that API requests are directed to the new leader node.

**Note**  VIP is not designed to serve as a load-balancer.

**Procedure**

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Go to System > Overview.
3. Click Edit on the Virtual IP field.
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 `get cluster status verbose`.

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

Install an NSX Edge on ESXi Using a vSphere GUI

If you prefer an interactive NSX Edge installation, you can use the vSphere web client.

**Prerequisites**

- See NSX Edge network requirements in NSX Edge Installation.
Procedure

1. Locate the NSX Edge 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 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.

5. Enter a name for the NSX Edge VM.
   The name you type appears in the inventory.

6. Select a compute resource for the NSX Edge appliance.

7. For an optimal performance, reserve memory for the NSX Edge appliance.
   Set the reservation to ensure that NSX Edge has sufficient memory to run efficiently. See NSX Edge VM System Requirements.

8. Verify the OVF template details.

9. Select a datastore to store the NSX Edge appliance files.

10. Accept the default source and destination network interface.
    You can accept the default network destination for the rest of the networks and change the network configuration after the NSX Edge is deployed.

11. Select the IP allocation from the drop-down menu.

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

13. Enter the default gateway, management network IPv4, management network netmask, DNS, and NTP IP address.
14  (Optional) Register the NSX Edge with the management plane, if you have a NSX Manager available.
   a  Enter the parent NSX Manager node IP address and thumbprint.
   b  Run the API call POST https://<nsx-manager>/api/v1/aaa/registration-token to retrieve the NSX Manager token.

15  Enter the hostname of the NSX Edge VM.

16  Enable SSH and allow root SSH login to the NSX Edge command line.
    By default, these options are disabled for security reasons.

17  Verify that all your custom OVA template specification is accurate and click **Finish** to initiate the installation.
    The installation might take 7-8 minutes.

18  Open the console of the NSX Edge to track the boot process.
    If the console window does not open, make sure that pop-ups are allowed.

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

20  Run the `get interface eth0.<vlan_ID>` command to verify that the IP address was applied as expected

    ```
    nsx-edge-1> get interface eth0.100
    Interface: eth0.100
    Address: 192.168.110.37/24
    MAC address: 00:50:56:86:62:4d
    MTU: 1500
    Default gateway: 192.168.110.1
    Broadcast address: 192.168.110.255
    ...
    ```
    **Note**  When bringing up NSX Edge VMs on non-NSX managed host, verify that the MTU setting is set to 1600 (instead of 1500) on the physical host switch for the data NIC.

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

    ```
    -10.132.2.67  Connected
    ```

22  Verify that the NSX Edge appliance has the required connectivity.
    If you enabled SSH, make sure that you can SSH to your NSX Edge.
    - You can ping your NSX Edge.
    - NSX Edge can ping its default gateway.
- NSX Edge can ping the hypervisor hosts that are in the same network as the NSX Edge.
- NSX Edge can ping its DNS server and its NTP server.

Troubleshoot connectivity problems.

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

By default, the NSX Edge 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.

- Log in CLI and type the `stop service dataplane` command.
- Type the `set interface interface dhcp plane mgmt` command.
- Place `interface` into the DHCP network and wait for an IP address to be assigned to that `interface`.
- 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.

**What to do next**

Join the NSX Edge with the management plane. See [Join NSX Edge with the Management Plane](#).

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

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

**Prerequisites**

- Verify that the system requirements are met. See [System Requirements](#).
- Verify that the required ports are open. See [Ports and Protocols](#).
- Verify that a datastore is configured and accessible on the ESXi host.
- Verify that you have the IP address and gateway, DNS server IP addresses, domain search list, and the NTP server IP address for the NSX Manager to use.
- Plan your NSX Manager IPv4 or IPv6 IP addressing scheme.
- See NSX Edge network requirements in [NSX Edge Installation](#).
- 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.

**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
  --noSSLSVerify
  --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
  <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
  ```
For an optimal performance, reserve memory for the NSX Manager appliance. Set the reservation to ensure that NSX Manager has sufficient memory to run efficiently. See NSX Manager VM System Requirements.

Open the console of the NSX Edge to track the boot process.

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

Run the `get interface eth0.<vlan_ID>` command to verify that the IP address was applied as expected.

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

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

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

- Verify that the NSX Edge appliance has the required connectivity.
  - If you enabled SSH, make sure that you can SSH to your NSX Edge.
    - You can ping your NSX Edge.
    - NSX Edge can ping its default gateway.
    - NSX Edge can ping the hypervisor hosts that are in the same network as the NSX Edge.
    - NSX Edge can ping its DNS server and its NTP server.
  - Troubleshoot connectivity problems.

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

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

a) Log in CLI and type the `stop service dataplane` command.
b) Type the `set interface interface dhcp plane mgmt` command.
c) Place `interface` into the DHCP network and wait for an IP address to be assigned to that `interface`.
d) Type the `start service dataplane` command.

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

**What to do next**

Join the NSX Edge with the management plane. See [Join NSX Edge with the Management Plane](#).

**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.
- Join the NSX Edges with the management plane.
- Add the NSX Edges as transport nodes.
- Optionally, create an NSX Edge cluster profile for high availability (HA). You can also use the default NSX Edge cluster profile.

**Procedure**
1. From a browser, log in with admin privileges to an NSX Manager at `https://<nsx-manager-ip-address>`.
2. Select **System > Fabric Nodes > Edge Clusters > Add**.
3. Enter the NSX Edge cluster a name.
4. Select an NSX Edge cluster profile from the drop-down menu.
5. Select either NSX Edge Node from the Member Type drop-down menu.
   - If the virtual machine is deployed in a public cloud environment, select Public Cloud Gateway otherwise select NSX Edge Node.
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*.
Installing NSX-T Data Center on KVM

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 System Requirements.

This chapter includes the following topics:
- Set Up KVM
- Manage Your Guest VMs in the KVM CLI
- Install NSX Manager on KVM
- Log In to the Newly Created NSX Manager
- Install Third-Party Packages on a KVM Host
- Verify Open vSwitch Version on RHEL KVM Hosts
- Deploy NSX Manager Nodes to Form a Cluster Using CLI
- Install NSX Edge Using ISO File or a PXE

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 7.4. and 7.5.

### 4 Install KVM and bridge utilities.

<table>
<thead>
<tr>
<th>Linux Distribution</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubuntu</td>
<td><code>apt-get install -y qemu-kvm libvirt-bin ubuntu-vm-builder bridge-utils virtinst virt-manager virt-viewer libguestfs-tools</code></td>
</tr>
</tbody>
</table>
| 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 Verify the hardware virtualization capability.

```
cat /proc/cpuinfo | egrep "vmx|svm"
```

The output must contain vmx.

### 6 Verify that the KVM module is installed.

<table>
<thead>
<tr>
<th>Linux Distribution</th>
<th>Commands</th>
</tr>
</thead>
</table>
| Ubuntu             | `kvm-ok`  
                           `INFO: /dev/kvm exists`  
                           `KVM acceleration can be used` |
| RHEL or CentOS Linux | `lsmod | grep kvm`  
                             `kvm_intel 53484 6`  
                             `kvm 316506 1 kvm_intel` |
| SUSE Linux Enterprise Server |  |
For KVM to be used as a host for NSX Manager, prepare the bridge network, management interface, and NIC interfaces.

In the following example, the first Ethernet interface (eth0 or ens32) is used for connectivity to the Linux machine itself. Depending on your deployment environment, this interface can use DHCP or static IP settings. Before assigning uplink interfaces to the NSX-T Data Center hosts, ensure that the interfaces scripts used by these uplinks are already configured. Without these interface files on the system, you cannot successfully create a host transport node.

**Note** Interface names might vary in different environments.

<table>
<thead>
<tr>
<th>Linux Distribution</th>
<th>Network Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubuntu</td>
<td>Edit /etc/network/interfaces:</td>
</tr>
<tr>
<td></td>
<td>auto lo</td>
</tr>
<tr>
<td></td>
<td>iface lo inet loopback</td>
</tr>
<tr>
<td></td>
<td>auto eth0</td>
</tr>
<tr>
<td></td>
<td>iface eth0 inet manual</td>
</tr>
<tr>
<td></td>
<td>auto br0</td>
</tr>
<tr>
<td></td>
<td>iface br0 inet static</td>
</tr>
<tr>
<td></td>
<td>address 192.168.110.51</td>
</tr>
<tr>
<td></td>
<td>netmask 255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>network 192.168.110.0</td>
</tr>
<tr>
<td></td>
<td>broadcast 192.168.110.255</td>
</tr>
<tr>
<td></td>
<td>gateway 192.168.110.1</td>
</tr>
<tr>
<td></td>
<td>dns-nameservers 192.168.3.45</td>
</tr>
<tr>
<td></td>
<td>dns-search example.com</td>
</tr>
<tr>
<td></td>
<td>bridge_ports eth0</td>
</tr>
<tr>
<td></td>
<td>bridge_stp off</td>
</tr>
<tr>
<td></td>
<td>bridge_fd 0</td>
</tr>
<tr>
<td></td>
<td>bridge_maxwait 0</td>
</tr>
</tbody>
</table>

Create a network definition XML file for the bridge. For example, create /tmp/bridge.xml with the following lines:

```xml
<network>
    <name>bridge</name>
    <forward mode='bridge'/>
    <bridge name='br0'/>
</network>
```

Define and start the bridge network with the following commands:

```
virsh net-define bridge.xml
virsh net-start bridge
virsh net-autostart bridge
```
<table>
<thead>
<tr>
<th>Linux Distribution</th>
<th>Network Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Verify the status of the bridge network with the following command:</td>
</tr>
<tr>
<td></td>
<td><code>virsh net-list --all</code></td>
</tr>
<tr>
<td></td>
<td>Name</td>
</tr>
<tr>
<td>-------------------</td>
<td>------</td>
</tr>
<tr>
<td>bridge</td>
<td>active</td>
</tr>
<tr>
<td>default</td>
<td>active</td>
</tr>
</tbody>
</table>

**RHEL or CentOS Linux**

Edit `/etc/sysconfig/network-scripts/ifcfg-management_interface`:

```bash
DEVICE="ens32"
TYPE="Ethernet"
NAME="ens32"
UUID="<UUID>"
BOOTPROTO="none"
HWADDR="<HWADDR>"
ONBOOT="yes"
NM_CONTROLLED="no"
BRIDGE="br0"
```

Edit `/etc/sysconfig/network-scripts/ifcfg-eth1`:

```bash
DEVICE="eth1"
TYPE="Ethernet"
NAME="eth1"
UUID="<UUID>"
BOOTPROTO="none"
HWADDR="<HWADDR>"
ONBOOT="yes"
NM_CONTROLLED="no"
```

Edit `/etc/sysconfig/network-scripts/ifcfg-eth2`:

```bash
DEVICE="eth2"
TYPE="Ethernet"
NAME="eth2"
UUID="<UUID>"
BOOTPROTO="none"
HWADDR="<HWADDR>"
ONBOOT="yes"
NM_CONTROLLED="no"
```

Edit `/etc/sysconfig/network-scripts/ifcfg-br0`:

```bash
DEVICE="br0"
BOOTPROTO="dhcp"
NM_CONTROLLED="no"
ONBOOT="yes"
TYPE="Bridge"
```

**SUSE Linux Enterprise Server**
For KVM to be used as a transport node, prepare the network bridge.

In the following example, the first Ethernet interface (eth0 or ens32) is used for connectivity to the Linux machine itself. Depending on your deployment environment, this interface can use DHCP or static IP settings.

**Note** Interface names might vary in different environments.

<table>
<thead>
<tr>
<th>Linux Distribution</th>
<th>Network Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubuntu</td>
<td>Edit <code>/etc/network/interfaces</code>:</td>
</tr>
<tr>
<td></td>
<td>auto lo</td>
</tr>
<tr>
<td></td>
<td>iface lo inet loopback</td>
</tr>
<tr>
<td></td>
<td>auto eth0</td>
</tr>
<tr>
<td></td>
<td>iface eth0 inet manual</td>
</tr>
<tr>
<td></td>
<td>auto eth1</td>
</tr>
<tr>
<td></td>
<td>iface eth1 inet manual</td>
</tr>
<tr>
<td></td>
<td>auto br0</td>
</tr>
<tr>
<td></td>
<td>iface br0 inet dhcp</td>
</tr>
<tr>
<td></td>
<td>bridge_ports eth0</td>
</tr>
<tr>
<td>RHEL or CentOS</td>
<td>Edit <code>/etc/sysconfig/network-scripts/ifcfg-ens32</code>:</td>
</tr>
<tr>
<td>Linux</td>
<td>DEVICE=&quot;ens32&quot;</td>
</tr>
<tr>
<td></td>
<td>TYPE=&quot;Ethernet&quot;</td>
</tr>
<tr>
<td></td>
<td>NAME=&quot;ens32&quot;</td>
</tr>
<tr>
<td></td>
<td>UUID=&quot;&lt;something&gt;&quot;</td>
</tr>
<tr>
<td></td>
<td>BOOTPROTO=&quot;none&quot;</td>
</tr>
<tr>
<td></td>
<td>HWADDR=&quot;&lt;something&gt;&quot;</td>
</tr>
<tr>
<td></td>
<td>ONBOOT=&quot;yes&quot;</td>
</tr>
<tr>
<td></td>
<td>NM_CONTROLLED=&quot;no&quot;</td>
</tr>
<tr>
<td></td>
<td>BRIDGE=&quot;br0&quot;</td>
</tr>
<tr>
<td>RHEL or CentOS</td>
<td>Edit <code>/etc/sysconfig/network-scripts/ifcfg-ens33</code>:</td>
</tr>
<tr>
<td>Linux</td>
<td>DEVICE=&quot;ens33&quot;</td>
</tr>
<tr>
<td></td>
<td>TYPE=&quot;Ethernet&quot;</td>
</tr>
<tr>
<td></td>
<td>NAME=&quot;ens33&quot;</td>
</tr>
<tr>
<td></td>
<td>UUID=&quot;&lt;something&gt;&quot;</td>
</tr>
<tr>
<td></td>
<td>BOOTPROTO=&quot;none&quot;</td>
</tr>
<tr>
<td></td>
<td>HWADDR=&quot;&lt;something&gt;&quot;</td>
</tr>
<tr>
<td></td>
<td>ONBOOT=&quot;yes&quot;</td>
</tr>
<tr>
<td></td>
<td>NM_CONTROLLED=&quot;no&quot;</td>
</tr>
</tbody>
</table>
Linux Distribution | Network Configuration
---|---
Edit /etc/sysconfig/network-scripts/ifcfg-br0:

```
DEVICE="br0"
BOOTPROTO="dhcp"
NM_CONTROLLED="no"
ONBOOT="yes"
TYPE="Bridge"
```

SUSE Linux Enterprise Server

**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 the transport node creation failure.

After the KVM host is configured as a transport node, the bridge interface "nsx-vtep0.0" is created. In Ubuntu, `/etc/network/interfaces` 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 called `ifcfg-nsx-vtep0.0`, which 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,

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

**Manage Your Guest VMs in the KVM CLI**

NSX Manager can be installed as KVM VMs. In addition, KVM can be used as the hypervisor for NSX-T Data Center transport nodes.
KVM guest VM management is beyond the scope of this guide. However, here are some simple KVM CLI commands to get you started.

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

```
# List running
virsh list

# List all
virsh list --all

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

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

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

```
ifconfig
...

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

### Install NSX Manager on KVM

NSX Manager can be installed as a virtual appliance on a KVM host.

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

**Prerequisites**

- KVM set up. See [Set Up KVM](#).
- Privileges to deploy a QCOW2 image on the KVM host.
- Verify that the password in the guestinfo adheres to the password complexity requirements so that you can log in after installation. See [NSX Manager Installation](#).
Procedure

1. Download the NSX Manager QCOW2 image from the `nsx-unified-appliance > exports > kvm` folder.
2. Copy it 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:

```bash
adduser $USER libvirtd
```
4. In the same directory where you saved the QCOW2 image, create a file called `guestinfo.xml` and populate it with the NSX Manager VM's properties.

For example:

```xml
<?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>
    <Property oe:key="nsx_password_0" oe:value="<password>"/>
    <Property oe:key="nsx_hostname" oe:value="nsx-manager1"/>
    <Property oe:key="nsx_role" oe:value="nsx-manager nsx-controller"/>
    <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>
```

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.

   sudo virt-install --import --vnc --name nsx-manager1 --ram 24000 --vcpus 6 --
   network=bridge:br0,model=e1000 --disk path=/var/lib/libvirt/images/nsx-unified-
   appliance-2.4.<BuildNumber>.qcow2,format=qcow2

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

7  Verify that the NSX Manager is deployed.

   virsh list --all

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

8  Open the NSX Manager console and log in.

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

   nsx-manager1 login: admin
   Password:

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

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

11 Verify that your NSX Manager has the required connectivity.

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

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

12 Exit the KVM console.

control-\]

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

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).

After you upgrade the Management plane, 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, including how to join or leave the program.

4 Click Save

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 with the command `yum install glibc.i686 nspr` on a new installation.

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

  ```
  apt-get install qemu-kvm
  apt-get install libvirt-bin
  apt-get install virtinst
  apt-get install virt-manager
  apt-get install virt-viewer
  apt-get install ubuntu-vm-builder
  apt-get install 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, run `apt-get install <package_name>` to install the third-party packages manually.

<table>
<thead>
<tr>
<th>Ubuntu 18.04 Packages</th>
<th>Ubuntu 16.04 Packages</th>
</tr>
</thead>
<tbody>
<tr>
<td>traceroute</td>
<td>libboost-chrono1.58.0</td>
</tr>
<tr>
<td>python-mako</td>
<td>libboost-filesystem1.58.0</td>
</tr>
<tr>
<td>python-netaddr</td>
<td>libgoogle-glog0v5</td>
</tr>
<tr>
<td>python-simplejson</td>
<td>libgoogle-perftools4</td>
</tr>
<tr>
<td>python-unittest2</td>
<td>libprotobuf9v5</td>
</tr>
<tr>
<td>python-yaml</td>
<td>traceroute</td>
</tr>
<tr>
<td>python-openssl</td>
<td>python-mako</td>
</tr>
<tr>
<td>dkms</td>
<td>python-netaddr</td>
</tr>
<tr>
<td>make</td>
<td>python-simplejson</td>
</tr>
<tr>
<td></td>
<td>python-unittest2</td>
</tr>
<tr>
<td></td>
<td>python-yaml</td>
</tr>
<tr>
<td></td>
<td>python-openssl1</td>
</tr>
<tr>
<td></td>
<td>libboost-date-time1.58.0</td>
</tr>
<tr>
<td></td>
<td>libleveldb1v5</td>
</tr>
<tr>
<td></td>
<td>python-gevent</td>
</tr>
<tr>
<td></td>
<td>python-protobuf</td>
</tr>
<tr>
<td></td>
<td>libboost-program-options1.58.0</td>
</tr>
<tr>
<td></td>
<td>dkms</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>RHEL 7.6, 7.5, and 7.4</th>
<th>CentOS Linux 7.5 and 7.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>wget</td>
<td>wget</td>
</tr>
<tr>
<td>PyYAML</td>
<td>PyYAML</td>
</tr>
<tr>
<td>libunwind</td>
<td>libunwind</td>
</tr>
<tr>
<td>python-gevent</td>
<td>python-gevent</td>
</tr>
<tr>
<td>python-mako</td>
<td>python-mako</td>
</tr>
<tr>
<td>python-netaddr</td>
<td>python-netaddr</td>
</tr>
<tr>
<td>redhat-lsb-core</td>
<td>redhat-lsb-core</td>
</tr>
<tr>
<td>tcpdump</td>
<td>tcpdump</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>SUSE Linux Enterprise Server 12.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>python-simplejson</td>
</tr>
<tr>
<td>python-PyYAML</td>
</tr>
<tr>
<td>python-netaddr</td>
</tr>
<tr>
<td>lsb-release</td>
</tr>
</tbody>
</table>

Verify Open vSwitch Version on RHEL KVM Hosts

If OVS packages exist on the RHEL host, you must remove the existing packages and install the supported packages.

The supported Open vSwitch version is 2.9.1.8614397-1.

**Procedure**

1. Verify that the current version of the Open vSwitch installed on the host.
   
   `ovs-vsswitchd --version`
   
   If you have an Open vSwitch newer or older version, you must replace that Open vSwitch version with the supported one.

2. Open the Open vSwitch folder.

3. Delete the following Open vSwitch packages.
   
   - kmod-openvswitch
   - openvswitch
   - openvswitch-selinux-policy
Alternatively, add 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>--rhel75_x86_64.tar.gz
   ```
d. Navigate to the package directory.
   ```
   cd nsx-lcp-rhel75_x86_64/
   ```
e. Replace existing Open vSwitch version with the supported one.
   - For the newer Open vSwitch version, use the `--nodeps` command.
     ```
     rpm -Uvh kmod-openvswitch-<new version>.e17.x86_64.rpm --nodeps
     ```
     ```
     rpm -Uvh openvswitch-*.rpm --nodeps
     ```
   - For the older Open vSwitch version, use the `--force` command.
     ```
     rpm -Uvh kmod-openvswitch-<new version>.e17.x86_64.rpm --nodeps --force
     ```
     ```
     rpm -Uvh openvswitch-*.rpm --nodeps --force
     ```

### Deploy NSX Manager Nodes to Form a Cluster Using CLI

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

#### Prerequisites

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

#### Procedure

1. Open an SSH session to the first deployed NSX Manager node.
2. Log in with the administrator credentials.
3. On the NSX Manager node, run the `get certificate api thumbprint` command.
   - The command output is a string of numbers that is unique to this NSX Manager.
4. Run the `get cluster config` command to get the first deployed NSX Manager cluster ID.
5. Add a NSX Manager node to the cluster.

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

   Provide the following NSX Manager information:

   - Hostname or IP address node that you want to join
   - Cluster ID
User name
Password
Certificate thumbprint
You can use the CLI command or API call.

CLI command

```
host> join <NSX-Manager-IP> cluster-id <cluster-id> username<NSX-Manager-username>
       password<NSX-Manager-password> thumbprint <NSX-Manager1's-thumbprint>
```

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

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

6. Add the third NSX Manager node to the cluster.
   Repeat step 5.

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

8. Select System > Overview and verify the cluster connectivity.

What to do next
Create a transport zone. See Create a Standalone Host or Bare Metal Server Transport Node.

Install NSX Edge Using ISO File or a PXE

You can install NSX Edge devices in an automated fashion on bare metal or as a VM using PXE.

**Note** PXE boot installation is not supported for NSX Manager. You also cannot configure networking settings, such as the IP address, gateway, network mask, NTP, and DNS.

Install NSX Edge via ISO File as a Virtual Appliance

You can install NSX Edge VMs in a manual fashion using an ISO file.

**Important** The NSX-T Data Center component virtual machine installations include VMware Tools. Removal or upgrade of VMware Tools is not supported for NSX-T Data Center appliances.

**Prerequisites**
- See NSX Edge network requirements in NSX Edge Installation.

**Procedure**

1. Locate the NSX Edge appliance ISO file under the `nsx-edgenode > exports > xenial_amd64` folder.
   Download the ISO file onto your computer.
2. In the vSphere Client, select the host datastore.
3 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.

4 In the vSphere Client inventory, select the host you uploaded the ISO file. or in the vSphere Client,

5 Right-click and select New Virtual Machine.

6 Select a compute resource for the NSX Edge appliance.

7 Select a datastore to store the NSX Edge appliance files.

8 Accept the default compatibility for your NSX Edge VM.

9 Select the supported ESXi operating systems for your NSX Edge VM.

10 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.

11 Power on the new NSX Edge VM.

12 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.

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

Set the reservation to ensure that NSX Edge has sufficient memory to run efficiently. See [NSX Edge VM System Requirements](#).

14 After the NSX Edge starts, log in to the CLI with admin credentials.

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

15 There are three ways to configure a 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

16 **(Optional)** Start SSH service. Run `start service ssh`.

17 Run the `get interface eth0.<vlan_ID>` command to verify that the IP address was applied as expected.

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

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

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

18 (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.

19 Verify that the NSX Edge appliance has the required connectivity.

If you enabled SSH, make sure that you can SSH to your NSX Edge.

- You can ping your NSX Edge.
- NSX Edge can ping its default gateway.
- NSX Edge can ping the hypervisor hosts that are in the same network as the NSX Edge.
- NSX Edge can ping its DNS server and its NTP server.

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

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

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

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

d Type the `start service dataplane` command.

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

**What to do next**

Join the NSX Edge with the management plane. See [Join NSX Edge with the Management Plane](#).

**Install NSX Edge via ISO File on Bare Metal**

You can install NSX Edge devices in a manual fashion on bare metal using an ISO file. This includes configuring networking settings, such as IP address, gateway, network mask, NTP, and DNS.
Prerequisites

- Verify that the system BIOS mode is set to Legacy BIOS.
- See NSX Edge network requirements in NSX Edge Installation.

Procedure

1. Locate the NSX Edge appliance ISO file under the `nsx-edgenode > publish > xenial_amd64` folder. Download the ISO file onto your computer.
2. Log in to the ILO of the bare metal.
3. Click Launch in the virtual console preview.
4. Select Virtual Media > Connect Virtual Media. Wait a few seconds for the virtual media to connect.
5. Select Virtual Media > Map CD/DVD and browse to the ISO file.
6. Select Next Boot > Virtual CD/DVD/ISO.
7. Select Power > Reset System (warm boot). The installation duration depends on the bare metal environment.
8. Choose Automated installation. There might be a pause of 10 seconds after you press Enter.
9. Select the applicable primary network interface. During power-on, the installer requests a network configuration via DHCP. If DHCP is not available in your environment, the installer prompts you for IP settings.
   By default, the root login password is `vmware`, and the admin login password is `default`.
10. Open the console of the NSX Edge to track the boot process. If the console window does not open, make sure that pop-ups are allowed.
11. After the NSX Edge starts, log in to the CLI with admin credentials.

   **Note** After NSX Edge starts, if you do not log in with admin credentials for the first time, the data plane service does not automatically start on NSX Edge.
12. After the reboot, you can log in with either admin or root credentials. The default root password is `vmware`.
13. There are three ways to configure a 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

14 Run the `get interface eth0.<vlan_ID>` command to verify that the IP address was applied as expected.

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

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

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

15 (Tagged interface and In-band interface) Any existing VLAN management interface must be cleared before creating a new one.

clear interface eth0.<vlan_ID>

To set a new interface, refer to step 13.

16 Verify that the NSX Edge appliance has the required connectivity.

If you enabled SSH, make sure that you can SSH to your NSX Edge.

- You can ping your NSX Edge.
- NSX Edge can ping its default gateway.
- NSX Edge can ping the hypervisor hosts that are in the same network as the NSX Edge.
- NSX Edge can ping its DNS server and its NTP server.

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

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

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

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

d. Type the `start service dataplane` command.

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

**What to do next**

Join the NSX Edge with the management plane. See [Join NSX Edge with the Management Plane](#).

### Install NSX Edge on PXE Server

PXE is made up of several components: DHCP, HTTP, and TFTP. This procedure demonstrates how to set up a PXE server on Ubuntu.

DHCP dynamically distributes IP settings to NSX-T Data Center components, such as NSX Edge. In a PXE environment, the DHCP server allows NSX Edge to request and receive an IP address automatically.

TFTP is a file-transfer protocol. The TFTP server is always listening for PXE clients on the network. When it detects any network PXE client asking for PXE services, it provides the NSX-T Data Center component ISO file and the installation settings contained in a preseed file.

**Prerequisites**

- A PXE server must be available in your deployment environment. The PXE server can be set up on any Linux distribution. The PXE server must have two interfaces, one for external communication and another for providing DHCP IP and TFTP services.
  
  If you have multiple management networks, you can add static routes to the other networks from the NSX-T Data Center appliance.

- Verify that the preseeded configuration file has the parameters `net.ifnames=0` and `biosdevname=0` set after `--` to persist after reboot.

- See NSX Edge network requirements in [NSX Edge Installation](#).

**Procedure**

1. (Optional) Use a kickstart file to set up a new TFTP or DHCP services on an Ubuntu server.

   A kickstart file is a text file that contains CLI commands that you run on the appliance after the first boot.
Name the kickstart file based on the PXE server it is pointing to. For example:

```
nsxcli.install
```

The file must be copied to your Web server, for example at `/var/www/html/nsx-edge/nsxcli.install`.

In the kickstart file, you can add CLI commands. For example, to configure the IP address of the management interface:

```
stop dataplane
set interface eth0 <ip-cidr-format> plane mgmt
start dataplane
```

To change the admin user password:

```
set user admin password <new_password> old-password <old-password>
```

If you specify a password in the preseed.cfg file, use the same password in the kickstart file. Otherwise, use the default password, which is "default".

To join the NSX Edge with the management plane:

```
join management-plane <manager-ip> thumbprint <manager-thumbprint> username <manager-username>
password <manager-password>
```

2. Create two interfaces, one for management and another for DHCP and TFTP services.

Make sure that the DHCP/TFTP interface is in the same subnet that the NSX Edge resides in.

For example, if the NSX Edge management interfaces are going to be in the 192.168.210.0/24 subnet, place eth1 in that same subnet.

```
# The loopback network interface
auto lo
iface lo inet loopback

# PXE server's management interface
auto eth0
iface eth0 inet static
  address 192.168.110.81
  gateway 192.168.110.1
  netmask 255.255.255.0
  dns-nameservers 192.168.110.10

# PXE server's DHCP/TFTP interface
auto eth1
iface eth1 inet static
  address 192.168.210.82
  gateway 192.168.210.1
  netmask 255.255.255.0
  dns-nameservers 192.168.110.10
```
3 Install DHCP server software.

```
sudo apt-get install isc-dhcp-server -y
```

4 Edit the `/etc/default/isc-dhcp-server` file, and add the interface that provides the DHCP service.

```
INTERFACES="eth1"
```

5 (Optional) If you want this DHCP server to be the official DHCP server for the local network, uncomment the `authoritative;` line in the `/etc/dhcp/dhcpd.conf` file.

```
...
authoritative;
...
```

6 In the `/etc/dhcp/dhcpd.conf` file, define the DHCP settings for the PXE network.

For example:

```
subnet 192.168.210.0 netmask 255.255.255.0 {
    option subnet-mask 255.255.255.0;
    option domain-name-servers 192.168.110.10;
    option routers 192.168.210.1;
    option broadcast-address 192.168.210.255;
    default-lease-time 600;
    max-lease-time 7200;
}
```

7 Start the DHCP service.

```
sudo service isc-dhcp-server start
```

8 Verify that the DHCP service is running.

```
service --status-all | grep dhcp
```

9 Install Apache, TFTP, and other components that are required for PXE booting.

```
sudo apt-get install apache2 tftpd-hpa inetutils-inetd
```

10 Verify that TFTP and Apache are running.

```
service --status-all | grep tftpd-hpa
service --status-all | grep apache2
```
11 Add the following lines to the /etc/default/tftpd-hpa file.

```
RUN_DAEMON=yes
OPTIONS="-l -s /var/lib/tftpboot"
```

12 Add the following line to the /etc/inetd.conf file.

```
tftp    dgram    udp    wait    root    /usr/sbin/in.tftpd /usr/sbin/in.tftpd -s /var/lib/tftpboot
```

13 Restart the TFTP service.

```
sudo /etc/init.d/tftpd-hpa restart
```

14 Copy or download the NSX Edge installer ISO file to a temporary folder.

15 Mount the ISO file and copy the install components to the TFTP server and the Apache server.

```
sudo mount -o loop ~/nsx-edge.<build>.iso /mnt
cd /mnt
sudo cp -fr install/netboot/* /var/lib/tftpboot/
sudo mkdir /var/www/html/nsx-edge
sudo cp -fr /mnt/* /var/www/html/nsx-edge/
```
16 (Optional) Edit the `/var/www/html/nsx-edge/preseed.cfg` file to modify the encrypted passwords.

You can use a Linux tool such as `mkpasswd` to create a password hash.

```
sudo apt-get install whois
sudo mkpasswd -m sha-512
```

**a** Modify the root password, edit `/var/www/html/nsx-edge/preseed.cfg` and search for the following line:

```
d-i passwd/root-password-crypted password $6$tgmLNLMp$9BuAHhN...
```

**b** Replace the hash string.

You do not need to escape any special character such as $, ', " or \

**c** Add the `usermod` command to `preseed.cfg` to set the password for root, admin, or both.

For example, search for the `echo 'VMware NSX Edge'` line and add the following command.

```
usermod --password '\$6\$VS3exId0aKmzW\$U3g0V7BF0DXlRl lr0v/VgloxVotEDp00b02hUF8u/` root; 
usermod --password '\$6\$VS3exId0aKmzW\$U3g0V7BF0DXlRl lr0v/VgloxVotEDp00b02hUF8u/` admin; 
```

The hash string is an example. You must escape all special characters. The root password in the first `usermod` command replaces the password that is set in `d-i passwd/root-password-crypted password $6$tgm...`.

If you use the `usermod` command to set the password, the user is not prompted to change the password at the first login. Otherwise, the user must change the password at the first login.

17 Add the following lines to the `/var/lib/tftpboot/pxelinux.cfg/default` file.

Replace 192.168.210.82 with the IP address of your TFTP server.

```
label nsxedge
    kernel ubuntu-installer/amd64/linux
    ipappend 2
    append netcfg/dhcp_timeout=60 auto=true priority=critical vga=normal partman-
    lvm/device_remove_lvm=true netcfg/choose_interface=auto debian-
    mirror/country=manual mirror/http/hostname=192.168.210.82 nsx-
    initrd=ubuntu-installer/amd64/initrd.gz mirror/suite=xenial --
```
Add the following lines to the /etc/dhcp/dhcpd.conf file.

Replace 192.168.210.82 with the IP address of your DHCP server.

```plaintext
allow booting;
allow bootp;

next-server 192.168.210.82; #Replace this IP address
filename "pxelinux.0";
```

Restart the DHCP service.

```plaintext
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 via ISO File on Bare Metal or Install NSX Edge via ISO File as a Virtual Appliance.
Configuring Bare Metal Server to Use NSX-T Data Center

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

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

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

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

This chapter includes the following topics:

- Install Third-Party Packages on a Bare Metal Server
- Create Application Interface for Bare Metal Server Workloads

## Install Third-Party Packages on a Bare Metal Server

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

**Prerequisites**

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

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

<table>
<thead>
<tr>
<th>Ubuntu 18.04</th>
<th>Ubuntu 16.04</th>
</tr>
</thead>
<tbody>
<tr>
<td>traceroute</td>
<td>libunwind8</td>
</tr>
<tr>
<td>python-mako</td>
<td>libgflags2v5</td>
</tr>
<tr>
<td>python-netaddr</td>
<td>libgoogle-perftools4</td>
</tr>
<tr>
<td>python-simplejson</td>
<td>traceroute</td>
</tr>
<tr>
<td>python-unittest2</td>
<td>python-mako</td>
</tr>
<tr>
<td>python-yaml</td>
<td>python-simplejson</td>
</tr>
<tr>
<td>python-openssl</td>
<td>python-unittest2</td>
</tr>
<tr>
<td>dkms</td>
<td>python-yaml</td>
</tr>
<tr>
<td>libvirt0</td>
<td>python-netaddr</td>
</tr>
<tr>
<td></td>
<td>libboost-filesystem1.58.0</td>
</tr>
<tr>
<td></td>
<td>libboost-chrono1.58.0</td>
</tr>
<tr>
<td></td>
<td>libgoogle-glog0v5</td>
</tr>
<tr>
<td></td>
<td>dkms</td>
</tr>
<tr>
<td></td>
<td>libboost-date-time1.58.0</td>
</tr>
<tr>
<td></td>
<td>python-protobuf</td>
</tr>
<tr>
<td></td>
<td>python-gevent</td>
</tr>
<tr>
<td></td>
<td>libsnappy1v5</td>
</tr>
<tr>
<td></td>
<td>libleveldb1v5</td>
</tr>
<tr>
<td></td>
<td>libboost-program-options1.58.0</td>
</tr>
<tr>
<td></td>
<td>libboost-thread1.58.0</td>
</tr>
<tr>
<td></td>
<td>libboost-iostreams1.58.0</td>
</tr>
<tr>
<td></td>
<td>libvirt0</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>RHEL 7.4, 7.5, and 7.6</th>
<th>CentOS 7.4, 7.5, and 7.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcpdump</td>
<td>tcpdump</td>
</tr>
<tr>
<td>boost-filesystem</td>
<td>boost-filesystem</td>
</tr>
<tr>
<td>PyYAML</td>
<td>PyYAML</td>
</tr>
<tr>
<td>boost-iostreams</td>
<td>boost-iostreams</td>
</tr>
<tr>
<td>boost-chrono</td>
<td>boost-chrono</td>
</tr>
<tr>
<td>python-mako</td>
<td>python-mako</td>
</tr>
<tr>
<td>python-netaddr</td>
<td>python-netaddr</td>
</tr>
<tr>
<td>python-six</td>
<td>python-six</td>
</tr>
<tr>
<td>gperftools-libs</td>
<td>gperftools-libs</td>
</tr>
<tr>
<td>libunwind</td>
<td>libunwind</td>
</tr>
<tr>
<td>snappy</td>
<td>snappy</td>
</tr>
<tr>
<td>boost-date-time</td>
<td>boost-date-time</td>
</tr>
<tr>
<td>c-ares</td>
<td>c-ares</td>
</tr>
<tr>
<td>redhat-lsb-core</td>
<td>redhat-lsb-core</td>
</tr>
<tr>
<td>wget</td>
<td>wget</td>
</tr>
<tr>
<td>net-tools</td>
<td>net-tools</td>
</tr>
<tr>
<td>yum-utils</td>
<td>yum-utils</td>
</tr>
<tr>
<td>lsof</td>
<td>lsof</td>
</tr>
<tr>
<td>python-gevent</td>
<td>python-gevent</td>
</tr>
<tr>
<td>libev</td>
<td>libev</td>
</tr>
<tr>
<td>python-greenlet</td>
<td>python-greenlet</td>
</tr>
<tr>
<td>libvirt-libs</td>
<td>libvirt-libs</td>
</tr>
<tr>
<td>libvirt-libs</td>
<td>libvirt-libs</td>
</tr>
</tbody>
</table>
On SUSE, run `zypper install <package_name>` to install the third-party packages manually.

### SUSE 12.0

- net-tools
- tcpdump
- python-simplejson
- python-netaddr
- python-PyYAML
- python-six
- libunwind
- wget
- lsof
- libc-cap-progs
- libvirt-libs

---

## Create Application Interface for Bare Metal Server Workloads

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

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

### Procedure

1. Install the required third-party packages.
   
   See [Install Third-Party Packages on a Bare Metal Server](https://kb.vmware.com/s/article/67835).

2. Configure the TCP and UDP ports.
   
   See [TCP and UDP Ports Used by ESXi, KVM Hosts, and Bare Metal Server](https://kb.vmware.com/s/article/67835).

3. Add a bare metal server to the NSX-T Data Center fabric and create a transport node.
   
   See [Create a Standalone Host or Bare Metal Server Transport Node](https://kb.vmware.com/s/article/67835).

4. Use the Ansible playbook to create an application interface.
   
Configure the NSX Manager Cluster

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

This chapter includes the following topics:

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

NSX Manager Cluster Requirements

The following requirements apply to NSX Manager cluster configuration:

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

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

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

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

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

  **Important** The number of sites in an NSX-T Data Center deployment can affect requirements. See NSX Manager Cluster Requirements for Single, Dual, and Multiple Sites.
NSX Manager Cluster Requirements for Single, Dual, and Multiple Sites

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

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

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

### Single Site Requirements and Recommendations

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

- It is recommended that you place your NSX Managers on different hosts to avoid a single host failure impacting multiple managers.

- Maximum latency between NSX Managers is 10ms.

- You can place NSX Managers in different vSphere clusters or in a common vSphere cluster. However, when using vSphere HA, NSX Managers must be placed in a common cluster.

- It is recommended that you place NSX Managers in different management subnets or a shared management subnet. When using vSphere HA it is recommended to use a shared management subnet so NSX Managers that are recovered by vSphere can preserve their IP address.

- It is recommended that you place NSX Managers on shared storage also. For vSphere HA, please review the requirements for that solution.

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

**Scenario example:**

- A vSphere cluster in which all three NSX Managers are deployed.

- The vSphere cluster consists of four or more hosts:
  - Host-01 with nsxmgr-01 deployed
  - Host-02 with nsxmgr-02 deployed
  - Host-03 with nsxmgr-03 deployed
  - Host-04 with no NSX Manager deployed

- vSphere HA is configured to recover any lost NSX Manager (e.g., nsxmgr-01) from any host (e.g., Host-01) to Host-04.

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

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

- It is not recommended to deploy NSX Managers in a dual-site scenario without vSphere HA. In this scenario, one site requires the deployment of 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 can be done with the following considerations:
  - A single stretched vSphere cluster contains all the hosts for NSX Managers.
  - All three NSX Managers are deployed to a common management subnet/VLAN to allow IP address preservation upon recovery of a lost NSX Managers.
  - For latency between sites, see the storage product requirements.

Scenario example:
- A vSphere cluster in which all three NSX Managers are deployed.
- The vSphere cluster consists of six or more hosts, with three hosts in Site A and three hosts in Site B.
- The three NSX Managers are deployed to distinct hosts with additional hosts for placement of recovered NSX Managers:
  - **Site A:**
    - Host-01 with nsxmgr-01 deployed
    - Host-02 with nsxmgr-02 deployed
    - Host-03 with nsxmgr-03 deployed
  - **Site B:**
    - Host-04 with no NSX Manager deployed
    - Host-05 with no NSX Manager deployed
    - Host-06 with no NSX Manager deployed
- vSphere HA is configured to recover any lost NSX Manager (e.g., nsxmgr-01) from any host (e.g., Host-01) in Site A to one of the hosts in Site B.

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

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

Multiple (Three or More) Site Requirements and Recommendations

The following recommendations apply to multiple-site (Site A/Site B/Site C) NSX-T Data Center deployments.
In a scenario with three or more sites, you can deploy NSX Managers with or without vSphere HA.

If you deploy without vSphere HA:

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

Scenario example (three sites):

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

Failure scenarios:

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

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

Transport zones and transport nodes are important concepts in NSX-T Data Center.

This chapter includes the following topics:

- Create Transport Zones
- Create an IP Pool for Tunnel Endpoint IP Addresses
- Enhanced Data Path
- Configuring Profiles
- Create a Standalone Host or Bare Metal Server Transport Node
- Manual Installation of NSX-T Data Center Kernel Modules
- Create an NSX Edge Transport Node
- Create an NSX Edge Cluster

Create Transport Zones

Transport zones dictate which hosts and, therefore, which VMs can participate in the use of a particular network. A transport zone does this by limiting the hosts that can "see" a logical switch—and, therefore, which VMs can be attached to the logical switch. A transport zone can span one or more host clusters.

An NSX-T Data Center environment can contain one or more transport zones based on your requirements. A host can belong to multiple transport zones. A logical switch can belong to only one transport zone.

NSX-T Data Center does not allow connection of VMs that are in different transport zones in the Layer 2 network. The span of a logical switch is limited to a transport zone, so virtual machines in different transport zones cannot be on the same Layer 2 network.

The overlay transport zone is used by both host transport nodes and NSX Edges. When a host or NSX Edge transport node is added to an overlay transport zone, an N-VDS is installed on the host or NSX Edge.

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.

The N-VDS allows for virtual-to-physical packet flow by binding logical router uplinks and downlinks to physical NICs.
When you create a transport zone, you must provide a name for the N-VDS that will be installed on the transport nodes when they are later added to this transport zone. The N-VDS name can be whatever you want it to be.

**Procedure**

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Select **System > Fabric > Transport Zones > Add**.
3. Enter a name for the transport zone and optionally a description.
4. Enter a name for the N-VDS.
5. Select an N-VDS mode.
   - **Standard** mode that applies to all the supported hosts.
   - **Enhanced Datapath** is a networking stack mode that applies to only transport nodes of ESXi host version 6.7 and later type that can belong in a transport zone.
6. If the N-VDS mode is set to Standard, select a traffic type.
   The options are **Overlay** and **VLAN**.
7. If the N-VDS mode is set to Enhanced Datapath, select a traffic type.
   The options are **Overlay** and **VLAN**.

**Note** In the enhanced datapath mode, only specific NIC configurations are supported. Make sure that you configure the supported NICs.

8. Enter one or more uplink teaming policy names. These named teaming policies can be used by logical switches attached to the transport zone. If the logical switches do not find a matching named teaming policy, then the default uplink teaming policy is used.
9. View the new transport zone on the **Transport Zones** page.
10. (Optional) You can also view the new transport zone with the GET https://<nsx-mgr>/api/v1/transport-zones API call.

```json
{
  "cursor": "00369b661aed-1eaa-4567-9408-ccbcfe58b416tz-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": [
```
What to do next

Optionally, create a custom transport-zone profile and bind it to the transport zone. You can create custom transport-zone profiles using the POST /api/v1/transportzone-profiles API. There is no UI workflow for creating a transport-zone profile. After the transport-zone profile is created, you can find it to the transport zone with the PUT /api/v1/transport-zones/<transport-zone-id> API.

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

Create an IP Pool for Tunnel Endpoint IP Addresses

You can use an IP pool for the tunnel endpoints. Tunnel endpoints are the source and destination IP addresses used in the external IP header to identify the hypervisor hosts originating and end the NSX-T Data Center encapsulation of overlay frames. You can also use either DHCP or manually configured IP pools for tunnel endpoint IP addresses.
If you are using both ESXi and KVM hosts, one design option might be to use two different subnets for the ESXi tunnel endpoint IP pool (sub_a) and the KVM tunnel endpoint IP Pool (sub_b). In this case, on the KVM hosts a static route to sub_a must be added with a dedicated default gateway.

An example of the resulting routing table on an Ubuntu host where sub_a = 192.168.140.0 and sub_b = 192.168.150.0. (The management subnet, for example, might be 192.168.130.0).

**Kernel IP routing table:**

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Genmask</th>
<th>Iface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>192.168.130.1</td>
<td>0.0.0.0</td>
<td>eth0</td>
</tr>
<tr>
<td>192.168.122.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>virbr0</td>
</tr>
<tr>
<td>192.168.130.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>eth0</td>
</tr>
<tr>
<td>192.168.140.0</td>
<td>192.168.150.1</td>
<td>255.255.255.0</td>
<td>nsx-vtep0.0</td>
</tr>
<tr>
<td>192.168.150.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>nsx-vtep0.0</td>
</tr>
</tbody>
</table>

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 **Advanced Networking & Security > Inventory > Groups > IP Pools > Add**.
3. Enter the IP pool details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Parameter Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and Description</td>
<td>Enter the IP pool and optional description.</td>
</tr>
<tr>
<td>IP Ranges</td>
<td>IP allocation ranges 192.168.200.100 - 192.168.200.115</td>
</tr>
<tr>
<td>Gateway</td>
<td>192.168.200.1</td>
</tr>
<tr>
<td>CIDR</td>
<td>Network address in a CIDR notation 192.168.200.0/24</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>Comma-separated list of DNS servers 192.168.66.10</td>
</tr>
<tr>
<td>DNS Suffix</td>
<td>corp.local</td>
</tr>
</tbody>
</table>
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 requires the performance benefits provided by this mode.

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, you can configure:

- 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 ixbgen-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
3. Create an uplink policy.  
   See Create an Uplink Profile.

4. Create a transport zone with N-VDS in the enhanced data path mode.  
   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 the virtual machine MTU is set to a value less than 8900.

5. Create a host transport node. Configure the enhanced data path N-VDS with logical cores and NUMA nodes.  
   See Create a Standalone Host or Bare Metal Server Transport Node.

### Load Balanced Source Teaming Policy Mode Aware of NUMA

The Load Balanced Source teaming policy mode defined for an enhanced datapath N-VDS becomes aware of NUMA when the following conditions are met:

- The **Latency Sensitivity** on VMs is **High**.
- The network adapter type used is VMXNET3.

If the NUMA node location of either the VM or the physical NIC is not available, then the Load Balanced Source teaming policy does not consider NUMA awareness to align VMs and NICs.

The teaming policy functions without NUMA awareness in the following conditions:

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

### ENS Support for SCTP Applications

In SCTP environments, NFV workloads use multi-homing and redundancy features 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 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. So, traffic routed over SCTP protocol is provided redundant network paths by the Enhanced Data Path N-VDS.
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. Note that vNIC1 of VM 1 and VM 2 are on one subnet. Similarly, vNIC2 of VM 1 and VM 2 are on another subnet.

**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 profile defines policies for the links from hypervisor hosts to NSX-T Data Center logical switches or from NSX Edge nodes to top-of-rack switches.

The settings defined by uplink profiles might include teaming policies, active/standby links, the transport VLAN ID, and the MTU setting.

Standby uplinks are not supported with VM appliance-based NSX Edge. When you install NSX Edge as a virtual appliance, use the default uplink profile. For each uplink profile created for a VM-based NSX Edge, the profile must specify only one active uplink and no standby uplink.
NSX Edge VMs allows multiple uplinks on the same N-VDS. Each uplink can have one physical NIC with a distinct name and IP address. The physical NIC IP address must be in the same subnet. The uplinks can connect to different TOR switches. You must use the Load Balanced Source teaming policy for traffic load balancing.

Prerequisites

- See NSX Edge network requirements in NSX Edge Installation.
- 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>.
3 Complete the uplink profile details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and Description</td>
<td>Enter an uplink profile name. Add an optional uplink profile description.</td>
</tr>
<tr>
<td>LAGs</td>
<td>(Optional) In the LAGs section, click Add for Link aggregation groups (LAGs) using Link Aggregation Control Protocol (LACP) for the transport network.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>For LACP, multiple LAG is not supported on KVM hosts.</td>
</tr>
<tr>
<td>Teamings</td>
<td>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:</td>
</tr>
<tr>
<td><strong>Failover Order</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Load Balance Source</strong></td>
<td>A list of active uplinks is specified, and each interface on the transport node is pinned to one active uplink. This configuration allows use of several active uplinks at the same time.</td>
</tr>
</tbody>
</table>

**Note**
- On KVM hosts: Only Failover Order teaming policy is supported, whereas Load Balance Source and Load Balance Source MAC teaming policies are not supported.
- On NSX Edge: For default teaming policy, Load Balance Source and Failover Order teaming policies are supported. For named teaming policy, only Failover Order policy is supported.
- On ESXi hosts: Load Balance Source MAC, Load Balance Source, and Failover Order teaming policies are supported.

(ESXi hosts and NSX Edge) You can define the following policies for a transport zone:
- A Named teaming policy for every logical switch configured on the switch.
- A Default teaming policy for the entire switch.

Named teaming policy: A named teaming policy means that for every logical switch you can define a specific teaming policy mode and uplinks. This policy type gives you the flexibility to select uplinks depending on the bandwidth requirement.
- If you define a named teaming policy, N-VDS uses that named teaming policy if it is specified by the attached transport zone and logical switch in the host.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you do not define any named teaming policies, N-VDS uses the default teaming policy.</td>
<td></td>
</tr>
</tbody>
</table>

4. Enter a Transport VLAN value.

5. Enter the MTU value.

The uplink profile MTU default value is 1600.

The global physical uplink MTU configures the MTU value for all the N-VDS instances in the NSX-T Data Center domain. If the global physical uplink MTU value is not specified, the MTU value is inferred from the uplink profile MTU if configured or the default 1600 is used. The uplink profile MTU value can override the global physical uplink MTU value on a specific host.

The global logical interface MTU configures the MTU value for all the logical router interfaces. If the global logical interface MTU value is not specified, the MTU value is inferred from the tier-0 logical router. The logical router uplink MTU value can override on a specific port the global logical interface MTU value.

In addition to the UI, you can also view the uplink profiles with the API call GET /api/v1/host-switch-profiles.

**What to do next**

Create a transport zone. See [Create Transport Zones](#).

**Configuring Network I/O Control Profiles**

Use the Network I/O Control (NIOC) profile to allocate the network bandwidth to business-critical applications and to resolve situations where several types of traffic compete for common resources.

NIOC profile introduces a mechanism to reserve bandwidth for the system traffic based on the capacity of the physical adapters on a host. Version 3 of the Network I/O Control feature offers improved network resource reservation and allocation across the entire switch.

Network I/O Control version 3 for NSX-T Data Center supports the resource management of the system traffic related to virtual machines and to infrastructure services, such as vSphere Fault Tolerance. System traffic is strictly associated with an ESXi host.

**Bandwidth Guarantee to System Traffic**

Network I/O Control version 3 provisions bandwidth to the network adapters of virtual machines by using constructs of shares, reservation, and limit. These constructs can be defined in the NSX-T Data Center Manager UI. The bandwidth reservation for virtual machine traffic is also used in the admission control.

When you power on a virtual machine, admission control utility verifies that enough bandwidth is available before placing a VM on a host that can provide the resource capacity.
**Bandwidth Allocation for System Traffic**

You can configure Network I/O Control to allocate a certain amount of bandwidth for traffic generated by vSphere Fault Tolerance, vSphere vMotion, virtual machines, and so on.

- Management Traffic: is traffic for a host management
- Fault Tolerance (FT) traffic: is traffic for failover and recovery.
- NFS Traffic: is traffic related to a file transfer in the network file system.
- vSAN Traffic: is traffic generated by virtual storage area network.
- vMotion Traffic: is traffic for computing resource migration.
- vSphere Replication Traffic: is traffic for replication.
- vSphere Data Protection Backup Traffic: is traffic generated by backup of data.
- Virtual machine Traffic: is traffic generated by virtual machines.
- iSCSI Traffic: is traffic for Internet Small Computer System Interface.

vCenter Server propagates the allocation from the distributed switch to each physical adapter on the hosts that are connected to the switch.

**Bandwidth Allocation Parameters for System Traffic**

By using several configuration parameters, the Network I/O Control service allocates the bandwidth to traffic from basic vSphere system features. Allocation Parameters for System Traffic.

Allocation Parameters for System Traffic

- **Shares**: Shares, from 1 to 100, reflect the relative priority of a system traffic type against the other system traffic types that are active on the same physical adapter. The relative shares assigned to a system traffic type and the amount of data transmitted by other system features determine the available bandwidth for that system traffic type.

- **Reservation**: The minimum bandwidth, in Mbps, that must be guaranteed on a single physical adapter. The total bandwidth reserved among all system traffic types cannot exceed 75 percent of the bandwidth that the physical network adapter with the lowest capacity can provide. Reserved bandwidth that is unused becomes available to other types of system traffic. However, Network I/O Control does not redistribute the capacity that system traffic does not use to virtual machine placement.

- **Limit**: The maximum bandwidth, in Mbps or Gbps, that a system traffic type can consume on a single physical adapter.

**Note**  You can reserve no more than 75 percent of the bandwidth of a physical network adapter.

For example, if the network adapters connected to an ESXi host are 10 GbE, you can only allocate 7.5 Gbps bandwidth to the various traffic types. You might leave more capacity unreserved. The host can allocate the unreserved bandwidth dynamically according to shares, limits, and use. The host reserves only the bandwidth that is enough for the operation of a system feature.
Configure Network I/O Control and Bandwidth Allocation for System Traffic on an N-VDS

To guarantee the minimum bandwidth to the system traffic running on NSX-T Data Center hosts, enable and configure a network resource management on an N-VDS.

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Select **System > Fabric > Profiles > NIOC Profiles > Add**.
3. Enter the NIOC profile details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and Description</td>
<td>Enter a NIOC profile name. You can optionally enter the profile details such as, the traffic types enabled.</td>
</tr>
<tr>
<td>Status</td>
<td>Toggle to enable the bandwidth allocations listed in the traffic resources.</td>
</tr>
<tr>
<td>Host Infra Traffic Resource</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

```json
{
  "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"
"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"
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. The overall reservation among all traffic types should not exceed 75%. Otherwise, the API request will be rejected.",
    "id": "ResourceAllocation",
    "module_id": "NioProfile",
    "nsx_feature": "Nio",
    "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 and will be rejected by the API."
        },
        "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"
        }
    }
```
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>

```json
{
    "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-40f8-8cfd-c577aefe563a",
                        "key": "UplinkHostSwitchProfile"
                    },
                    {
                        "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
                        "key": "LldpHostSwitchProfile"
                    },
                    {
                        "value": "b0185999-8003-4678-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"
                    }
                ]
            }
        ]
    }
}
```
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.etherswitch.cdp = LLDP, propType = CONFIG
com.vmware.common.respools.version = version3, propType = CONFIG
com.vmware.common.respools.cfg:

netsched.pools.persist.ft:0:50:-1:255
netsched.pools.persist.hbr:0:50:-1:255
netsched.pools.persist.vmotion:0:50:-1:255
netsched.pools.persist.vm:0:100:-1:255
netsched.pools.persist.iscsi:0:50:-1:255
netsched.pools.persist.nfs:0:50:-1:255
```
netsched.pools.persist.mgmt:0:50:-1:255
netsched.pools.persist.vdp:0:50:-1:255
netsched.pools.persist.vsan:0:50:-1:255
propType = CONFIG

6 Verify NIOC profiles in the host kernel.

# [root@ host:] /get /net/portsets/DvsPortset-1/ports/50335755/niocVnicInfo

Vnic NIOC Info
{
    Uplink reserved on:vmnic4
    Reservation in Mbps:200
    Shares:50
    Limit in Mbps:4294967295
    World ID:1001400726
    vNIC Index:0
    Respool Tag:0
    NIOC Version:3
    Active Uplink Bit Map:15
    Parent Respool ID:netsched.pools.persist.vm
}

7 Verify the NIOC profile information.

# [root@ host:] /get /net/portsets/DvsPortset-1/uplinks/vmnic4/niocInfo

Uplink NIOC Info
{
    Uplink device:vmnic4
    Link Capacity in Mbps:750
    vm respool reservation:275
    link status:1
    NetSched Ready:1
    Infrastructure reservation:0
    Total VM reservation:200
    Total vnics on this uplink:1
    NIOC Version:3
    Uplink index in BitMap:0
}

NIOC profile is configured with a pre-defined bandwidth allocation for applications running on NSX-T Data Center hosts.

**Add an NSX Edge Cluster Profile**

The NSX Edge cluster profile defines the policies for the NSX Edge transport node.

**Prerequisites**

Verify that the NSX Edge cluster is available.
Procedure

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

2. Select **System > Fabric > Profiles > Edge Cluster Profiles > Add**.

3. Enter the NSX Edge cluster profile details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and Description</td>
<td>Enter a NSX Edge cluster profile name. You can optionally enter the profile details such as, the Bidirectional Forwarding Detection (BFD) setting.</td>
</tr>
<tr>
<td>BFD Probe Interval</td>
<td>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.</td>
</tr>
<tr>
<td>BFD Allowed Hops</td>
<td>Accept the default setting. You can set the number of multihop BFD sessions allowed for the profile.</td>
</tr>
<tr>
<td>BFD Declare Dead Multiple</td>
<td>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.</td>
</tr>
<tr>
<td>Stand By Relocation Threshold</td>
<td>Accept the default setting.</td>
</tr>
</tbody>
</table>

Add an NSX Edge Bridge Profile

The NSX Edge bridge profile defines the policies for the ESXi bridge cluster.

A bridge cluster is a collection of ESXi host transport nodes.

Prerequisites

- Verify that the NSX Edge cluster is available.
- Verify that the ESXi bridge cluster is available.

Procedure

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

2. Select **System > Fabric > Profiles > Edge Bridge Profiles > Add**.

3. Enter the NSX Edge cluster profile details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and Description</td>
<td>Enter a NSX Edge bridge cluster profile name. You can optionally enter the profile details such as, the primary and backup node details.</td>
</tr>
<tr>
<td>Edge Cluster</td>
<td>Select the NSX Edge cluster that you can to use.</td>
</tr>
<tr>
<td>Primary Node</td>
<td>Designate the preferred NSX Edge node from the cluster.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Backup Node</td>
<td>Designate the back up NSX Edge node if the primary node fails.</td>
</tr>
<tr>
<td>Failover Mode</td>
<td>Select either Preemptive or Non-Preemptive mode.</td>
</tr>
<tr>
<td></td>
<td>The default HA mode is preemptive, which can slowdown traffic when the</td>
</tr>
<tr>
<td></td>
<td>preferred NSX Edge node goes back online. The non-preemptive mode does not</td>
</tr>
<tr>
<td></td>
<td>cause any traffic slowdown.</td>
</tr>
</tbody>
</table>

Add a Transport Node Profile

A transport node profile captures the configuration required to create a transport node. The transport node profile can be applied to an existing vCenter Server cluster to create transport nodes for the member hosts. Transport node profiles define transport zones, member hosts, N-VDS switch configuration including uplink profile, IP assignment, mapping of physical NICs to uplink virtual interfaces and so on.

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.

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.

Considerations for Transport Node Profile Creation:

- You can add a maximum of four N-VDS switches for each configuration: enhanced N-VDS created for VLAN transport zone, standard N-VDS created for overlay transport zone, enhanced N-VDS created for overlay transport zone.
- There is no limit on the number of standard N-VDS switches created for VLAN transport zone.
- In a single host cluster topology running multiple standard overlay N-VDS switches and edge VM on the same host, NSX-T Data Center provides traffic isolation such that traffic going through the first N-VDS is isolated from traffic going through the second N-VDS and so on. The physical NICs on each N-VDS must be mapped to the edge VM on the host to allow the north-south traffic connectivity with the external world. Packets moving out of a VM on the first transport zone must be routed through an external router or an external VM to the VM on the second transport zone.
- Each N-VDS switch name must be unique. NSX-T Data Center does not allow use of duplicate switch names.
- Each transport zone ID must be unique. NSX-T Data Center does not allow use of duplicate IDs.
- You can add a maximum of 1000 transport zones in the transport node profile.
- To add a transport zone, it must be realized by any N-VDS present in the transport node profile.
Prerequisites

- Verify that the hosts are part of a vCenter Server cluster.
  
  vCenter Server must have at least one cluster.

- Verify that a transport zone is configured. See Create Transport Zones.

- Verify that a cluster is available. See Deploy NSX Manager Nodes to Form a Cluster from UI.

- Verify that an IP pool is configured, or DHCP must be available in the network deployment. See Create an IP Pool for Tunnel Endpoint IP Addresses.

- Verify that a compute manager is configured. See Add a Compute Manager.

Procedure

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


3. Enter a name to identify the transport node profile.

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

4. Select the available transport zones and click the > button to include the transport zones in the transport node profile.

   **Note** You can add multiple transport zones.

5. Click the N-VDS tab and enter the switch details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N-VDS Name</td>
<td>If the transport node is attached to a transport zone, then ensure the name entered for the N-VDS is the same as the N-VDS name specified in the transport zone. A transport node can be created without attaching it to a transport zone.</td>
</tr>
<tr>
<td>Associated Transport Zones</td>
<td>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.</td>
</tr>
<tr>
<td>NIOC Profile</td>
<td>Select the NIOC profile from the drop-down menu. The bandwidth allocations specified in the profile for the traffic resources are enforced.</td>
</tr>
<tr>
<td>Uplink Profile</td>
<td>Select an existing uplink profile from the drop-down menu or create a custom uplink profile.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The hosts in a cluster must have the same uplink profile. You can also use the default uplink profile.</td>
</tr>
<tr>
<td>LLDP Profile</td>
<td>Select enabled or disabled LLDP profile from the drop-down menu. The LLDP neighbor properties for a specific node interface are included in the profile.</td>
</tr>
</tbody>
</table>
### IP Assignment
Select **Use DHCP**, **Use IP Pool**, or **Use Static IP List** to assign an IP address to virtual tunnel endpoints (VTEPs) of the transport node.

If you select **Use Static IP List**, you must specify a list of comma-separated IP addresses, a gateway, and a subnet mask. All the VTEPs of the transport node must be in the same subnet otherwise bidirectional flow (BFD) session is not established.

### IP Pool
If you selected **Use IP Pool** for an IP assignment, specify the IP pool name.

### Physical NICs
Add physical NICs to the transport node. You can use the default uplink or assign an existing uplink from the drop-down menu.

Click **Add PNIC** to configure additional physical NICs to the transport node.

**Note**  Migration of the physical NICs that you add in this field depends on how you configure **PNIC only Migration**, **Network Mappings for Install**, and **Network Mappings for Uninstall**.

- To migrate a used physical NIC (for example, by a standard vSwitch or a vSphere distributed switch) without an associated VMkernel mapping, ensure that **PNIC only Migration** is enabled. Otherwise, the transport node state remains in **partial success**, and the fabric node LCP connectivity fails to establish.
- To migrate a used physical NIC with an associated VMkernel network mapping, disable **PNIC only Migration** and configure the VMkernel network mapping.
- To migrate a free physical NIC, enable **PNIC only Migration**.

### PNIC only Migration
Before setting this field, consider the following points:

- Know whether the physical NIC defined is a used NIC or a free NIC.
- Determine whether VMkernel interfaces of a host need to be migrated along with physical NICs.

Set the field:

- Enable **PNIC only Migration** if you only want to migrate physical NICs from a VSS or DVS switch to an N-VDS switch.
- Disable **PNIC only Migration** if you want to migrate a used physical NIC and its associated VMkernel interface mapping. A free or available physical NIC is attached to the N-VDS switch when a VMkernel interface migration mapping is specified.

On a host with multiple host switches:

- If all host switches are to migrate only PNICs, then you can migrate the PNICs in a single operation.
- If some hosts switches are to migrate VMkernel interfaces and the remaining host switches are to migrate only PNICs:
  1. In the first operation, migrate only PNICs.
  2. In the second operation, migrate VMkernel interfaces. Ensure that **PNIC only Migration** is disabled.

Both PNIC only migration and VMkernel interface migration are not supported at the same time across multiple hosts.

**Note**  To migrate a management network NIC, configure its associated VMkernel network mapping and keep **PNIC only Migration** disabled. If you only migrate the management NIC, the host loses connectivity.

For more information, see [VMkernel Migration to an N-VDS Switch](https://www.vmware.com/).
Option | Description
--- | ---
**Network Mappings for Install** | To migrate VMkernels to N-VDS switch during installation, map VMkernels to an existing logical switch. The NSX Manager migrates the VMkernel to the mapped logical switch on N-VDS.

**Caution** Ensure that the management NIC and management VMkernel interface are migrated to a logical switch that is connected to the same VLAN that the management NIC was connected to before migration. If vmnic<\(n\)> and VMkernel<\(n\)> are migrated to a different VLAN, then connectivity to the host is lost.

**Caution** For pinned physical NICs, ensure that the host switch mapping of physical NIC to a VMkernel interface matches the configuration specified in the transport node profile. As part of the validation procedure, NSX-T Data Center verifies the mapping and if the validation passes migration of VMkernel interfaces to an N-VDS switch is successful. It is also mandatory to configure the network mapping for uninstallation because NSX-T Data Center does not store the mapping configuration of the host switch after migrating the VMkernel interfaces to the N-VDS switch. If the mapping is not configured, connectivity to services, such as vSAN, can be lost after migrating back to the VSS or VDS switch.

For more information, see [VMkernel Migration to an N-VDS Switch](#).

**Network Mappings for Uninstall** | To revert the migration of VMkernels during uninstallation, map VMkernels to port groups on VSS or DVS, so that NSX Manager knows which port group the VMkernel must be migrated back to on the VSS or DVS. For a DVS switch, ensure that the port group is of the type Ephemeral.

**Caution** For pinned physical NICs, ensure that the transport node profile mapping of physical NIC to VMkernel interface matches the configuration specified in the host switch. It is mandatory to configure the network mapping for uninstallation because NSX-T Data Center does not store the mapping configuration of the host switch after migrating the VMkernel interfaces to the N-VDS switch. If the mapping is not configured, connectivity to services, such as vSAN, can be lost after migrating back to the VSS or VDS switch.

For more information, see [VMkernel Migration to an N-VDS Switch](#).

6. To add another N-VDS switch, click + **ADD N-VDS**.

7. Click **Save** to complete configuration.

**What to do next**

Apply the transport node profile to an existing vSphere cluster. See [Configure a Managed Host Transport Node](#).

**VMkernel Migration to an N-VDS Switch**

To migrate VMkernel interfaces from a VSS or DVS switch to an N-VDS switch at a cluster-level, configure the transport node profile with network-mapping details required for migration (map VMkernel interfaces to logical switches). Similarly, to migrate VMkernel interfaces on a host node, configure the transport node configuration. To revert migrate VMkernel interfaces back to a VSS or DVS switch, configure uninstall network-mapping (map logical ports to VMkernel interface) in the transport node profile to be realized during uninstallation.
During migration physical NICs currently in use are migrated to an N-VDS switch, while available or free physical NICs are attached to the N-VDS switch after migration.

**Note**  Transport node profiles are applied to all member hosts of a cluster. But if you want to limit migration of VMkernel interfaces on specific hosts, you can directly configure the host. After migration, N-VDS handles traffic on the VLAN and overlay network for those interfaces attached to the N-VDS switch.

**Important** Configurations done to individual hosts are marked with the *Overridden* flag. Any further updates to the transport node profile are not applied to these overridden hosts. These hosts remain in overridden state until NSX-T Data Center is uninstalled.

In the following figure, if a host has only two physical NICs, you might want to assign both those NICs to the N-VDS for redundancy and their associated VMkernel interfaces so that the interfaces do not lose connectivity with the host.

**Figure 8-2. 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 switch.

- **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 **Advanced Networking & Security > Networking > Switching**. On the **Switches** page, verify that the VMkernel interface is attached to the logical switch through a newly created logical port.
6. Go to **System > Nodes > Host Transport Node**. For each transport node, verify the status on the **Node Status** column is Success to confirm that the transport node configuration is successfully validated.
7. On the **Host Transport Node** page, verify the status on the **Configuration State** is Success to confirm that the host is successfully realized with the specified configuration.

After you migrate VMkernel interfaces and PNICS from a VDS to a N-VDS switch using NSX-T UI or transport node API, vCenter Server displays warnings for the VDS. If the host need be connected to the VDS, remove the host out of the VDS. The vCenter Server no longer displays any warning for VDS.

For details on errors that might encounter during migration, see VMkernel Migration Errors

### Revert Migration of VMkernel Interfaces to a VSS or DVS Switch

The high-level workflow to revert migration of VMkernel Interfaces from an N-VDS switch to a VSS or DVS switch during NSX-T Data Center uninstallation:

1. On the ESXi host, power off VMs connected to the logical ports that hosts the VMkernel interface after migration.
2 Configure the transport node profile with network mapping that is used to migrate the VMkernel interfaces during the uninstallation process. Network mapping during uninstallation maps the VMkernel interfaces to a port group on VSS or DVS switch on the ESXi host.

**Note** Reverting migration of a VMkernel to a port group on a DVS switch, ensure that the port group type is set to **Ephemeral**.

For more details, see [Add a Transport Node Profile](#).

3 Verify the network adapter mappings in vCenter Server reflect a new association of the VMkernel switch with a port group of VSS or DVS switch.

4 In NSX Manager, go to **Advanced Networking & Security > Networking > Switching**. On the **Switches** page, verify that the logical switch 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 **overridden**.

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 8-1. VMkernel Migration Errors

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Problem</th>
<th>Cause</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| 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. |
<p>| 8225       | VMkernel migration is in progress. | Migration is in progress. | Wait for the migration to complete before performing another action. |</p>
<table>
<thead>
<tr>
<th>Error Code</th>
<th>Problem</th>
<th>Cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>8226</td>
<td>VMkernel migration is only supported on a ESXi host.</td>
<td>Migration is only valid for ESXi hosts.</td>
<td>Ensure that the host is a ESXi host before you initiate migration.</td>
</tr>
<tr>
<td>8227</td>
<td>VMkernel interface is not appended with the host switch name.</td>
<td>On a host with multiple host switches, NSX-T Data Center cannot identify association of each VMkernel interface with its host switch.</td>
<td>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.</td>
</tr>
<tr>
<td>8228</td>
<td>Host switch used in the device_name field not found on the host.</td>
<td>Incorrect host switch name.</td>
<td>Enter the correct host switch name.</td>
</tr>
<tr>
<td>8229</td>
<td>Transport node did not specify the transport zone of the logical switch.</td>
<td>Transport zone not added.</td>
<td>Add the transport zone to the transport node configuration.</td>
</tr>
<tr>
<td>8230</td>
<td>No physical NIC on the host switch.</td>
<td>There must be at least one physical NIC on the host switch.</td>
<td>Specify at least one physical NIC to an uplink profile and the VMkernel network mapping configuration to a logical switch.</td>
</tr>
<tr>
<td>8231</td>
<td>Host switch name does not match.</td>
<td>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.</td>
<td>Ensure that the host switch name specified in the network mapping configuration matches the name used by the logical switch of the interface.</td>
</tr>
<tr>
<td>8232</td>
<td>Logical switch not realized on the host.</td>
<td>Realization of logical switch on the host was unsuccessful.</td>
<td>Synchronize the host with the NSX Manager.</td>
</tr>
<tr>
<td>8233</td>
<td>Unexpected logical switch in the network interface mapping.</td>
<td>The network interface mapping for installation and uninstallation lists both logical switches and port groups.</td>
<td>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.</td>
</tr>
<tr>
<td>8294</td>
<td>Logical switch does not exist in the network interface mapping.</td>
<td>Logical switches not specified.</td>
<td>Ensure that logical switches are specified in the network interface mapping configuration.</td>
</tr>
<tr>
<td>Error Code</td>
<td>Problem</td>
<td>Cause</td>
<td>Resolution</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
<td>-------</td>
<td>------------</td>
</tr>
<tr>
<td>8296</td>
<td>Host switch mismatch.</td>
<td>The network interface mapping for uninstallation is configured with the incorrect host switch name.</td>
<td>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.</td>
</tr>
<tr>
<td>8297</td>
<td>Duplicate VMkernel.</td>
<td>Duplicate VMkernels are specified for migration.</td>
<td>Ensure that no duplicate VMkernel interfaces are specified in the installation or uninstallation mapping configuration.</td>
</tr>
<tr>
<td>8298</td>
<td>Mismatch of number of VMkernel interfaces and destinations.</td>
<td>Incorrect configuration.</td>
<td>Ensure that each VMkernel interface has a corresponding destination specified in the configuration.</td>
</tr>
<tr>
<td>8299</td>
<td>Cannot delete transport node as the VMkernel interface is using ports on N-VDS.</td>
<td>VMkernel interfaces are using ports from the N-VDS switch.</td>
<td>Revert the migration of all VMkernel interfaces from the N-VDS switch to a VSS/DVS switch. Then attempt to delete the transport node.</td>
</tr>
<tr>
<td>9412</td>
<td>VMkernel cannot be migrated from one N-VDS to another N-VDS.</td>
<td>Unsupported action.</td>
<td>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.</td>
</tr>
<tr>
<td>9413</td>
<td>VMkernel interfaces cannot be migrated to a different logical switch.</td>
<td>On stateful hosts, a VMkernel connected to a logical switch cannot be migrated to another logical switch.</td>
<td>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.</td>
</tr>
<tr>
<td>9414</td>
<td>Duplicate VMkernel interfaces.</td>
<td>Duplicate VMkernel interfaces mapped in the installation and uninstallation mapping configuration.</td>
<td>Ensure that each VMkernel interface is unique in the installation and uninstallation mappings.</td>
</tr>
<tr>
<td>9415</td>
<td>Powered on VMs on the host.</td>
<td>With powered on VMs, migration does not proceed.</td>
<td>Power off the VMs on the host before you initiate migration of VMkernel interfaces.</td>
</tr>
<tr>
<td>9416</td>
<td>VMkernel cannot be found on the host.</td>
<td>Did not specify a VMkernel that exists on the host in the network mapping configuration.</td>
<td>Specify a VMkernel that exists in the network mapping configuration.</td>
</tr>
<tr>
<td>9417</td>
<td>Port group not found.</td>
<td>Did not specify a port group that exists on the host in the network mapping configuration.</td>
<td>Specify a port group that exists in the network mapping configuration.</td>
</tr>
<tr>
<td>9419</td>
<td>Logical switch not found during migration.</td>
<td>Did not find the logical switch defined in the network interface mapping configuration.</td>
<td>Specify a logical switch that exists in the network interface mapping configuration.</td>
</tr>
</tbody>
</table>
Table 8-1. VMkernel Migration Errors (Continued)

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Problem</th>
<th>Cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>9420</td>
<td>Logical port not found during migration.</td>
<td>During migration, NSX-T Data Center does not find the ports created on the logical switch.</td>
<td>Ensure that no logical ports are deleted from the logical switch for migration to be successful.</td>
</tr>
<tr>
<td>9421</td>
<td>Host information missing to validate the migration process.</td>
<td>Unable to retrieve host information from inventory.</td>
<td>Retry the migration process.</td>
</tr>
<tr>
<td>9423</td>
<td>Pinned physical NICs to a VMkernel interface are not migrated to the correct host switch.</td>
<td>A pinned physical NIC was found in the environment but the VMkernel and physical NIC are not being migrated to the same host switch.</td>
<td>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.</td>
</tr>
<tr>
<td>600</td>
<td>Object not found.</td>
<td>The specified transport zone used by the logical switch does not exist. The logical switch found in the VMK mapping destination cannot be found.</td>
<td>Specify a transport zone which exists in the environment. Create the desired logical switch or use an existing VLAN logical switch.</td>
</tr>
<tr>
<td>8310</td>
<td>The logical switch type is incorrect.</td>
<td>The logical switch type is Overlay.</td>
<td>Create a VLAN logical switch.</td>
</tr>
<tr>
<td>9424</td>
<td>Cannot migrate if both PNIC only Migration and Network Mapping for install or uninstall settings are configured at the same time.</td>
<td>Migration progresses only when one of these settings is configured.</td>
<td>Ensure that either the PNIC only Migration or Network Mapping for install or uninstall setting is configured.</td>
</tr>
</tbody>
</table>

Create a Standalone Host or Bare Metal Server Transport Node

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

A fabric node is a node that has been registered with the NSX-T Data Center management plane and has NSX-T Data Center modules installed. For a host or bare metal server to be part of the NSX-T Data Center overlay, it must first be added to the NSX-T Data Center fabric.

A transport node is a node that participates in an NSX-T Data Center overlay or NSX-T Data Center VLAN networking.

For a KVM host or bare metal server, you can preconfigure the N-VDS, or you can have NSX Manager perform the configuration. For a ESXi host, NSX Manager always configures the N-VDS.

Note If you plan to create transport nodes from a template VM, make sure that there are no certificates on the host in /etc/vmware/nxs/. The netcpa agent does not create a certificate if a certificate exists.

Bare metal server supports an overlay and VLAN transport zone. You can use the management interface to manage the bare metal server. The application interface allows you to access the applications on the bare metal server.

Single physical NICs provide an IP address for both the management and application IP interfaces.
Dual physical NICs provide a physical NIC and a unique IP address for the management interface. Dual physical NICs also provide a physical NIC and a unique IP address for the application interface.

Multiple physical NICs in a bonded configuration provide dual physical NICs and a unique IP address for the management interface. Multiple physical NICs in a bonded configuration also provide dual physical NICs and an unique IP address for the application interface.

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 and so on. The physical NICs on each N-VDS must be mapped to the edge VM on the host to allow the north-south traffic connectivity with the external world. Packets moving out of a VM on the first transport zone must be routed through an external router or an external VM to the VM on the second transport zone.

**Prerequisites**

- The host must be joined with the management plane, and connectivity must be Up.
- A transport zone must be configured.
- An uplink profile must be configured, or you can use the default uplink profile.
- An IP pool must be configured, or DHCP must be available in the network deployment.
- At least one unused physical NIC must be available on the host node.
- Hostname
- Management IP address
- User name
- Password
- *(Optional) (KVM) SHA-256 SSL thumbprint*
- *(Optional) (ESXi) SHA-256 SSL thumbprint*
- Verify that the required third-party packages are installed. See [Install Third-Party Packages on a KVM Host](#).
**Procedure**

1. **Optional** Retrieve the hypervisor thumbprint so that you can provide it when adding the host to the fabric.
   - Gather the hypervisor thumbprint information.
     - Use a Linux shell.
       ```bash
       # 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.
       ```bash
       [root@host:~] openssl x509 -in /etc/vmware/ssl/rui.crt -fingerprint -sha256 -noout
       ```
   - Retrieve the SHA-256 thumbprint from a KVM hypervisor, run the command in the KVM host.
     ```bash
     # awk '{print $2}' /etc/ssh/ssh_host_rsa_key.pub | base64 -d | sha256sum -b | sed 's/ .*$//' | xxd -r -p | base64
     ```

2. **Select System > Fabric > Nodes > Host Transport Nodes**.

3. From the Managed by field, select **Standalone Hosts** and click **Add**.

4. Enter the standalone host or bare metal server details to add to the fabric.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name and Description</strong></td>
<td>Enter the name to identify the standalone host or bare metal server. You can optionally add the description of the operating system used for the host or bare metal server.</td>
</tr>
<tr>
<td><strong>IP Addresses</strong></td>
<td>Enter the host or bare metal server IP address.</td>
</tr>
<tr>
<td><strong>Operating System</strong></td>
<td>Select the operating system from the drop-down menu. Depending on your host or bare metal server, you can select any of the supported operating systems. See System Requirements.</td>
</tr>
<tr>
<td><strong>Username and Password</strong></td>
<td>Enter the host user name and password.</td>
</tr>
<tr>
<td><strong>SHA-256 Thumbprint</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
5 For a KVM host or bare metal server, select the N-VDS type.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Created</td>
<td>NSX Manager creates the N-VDS. This option is selected by default.</td>
</tr>
<tr>
<td>Preconfigured</td>
<td>The N-VDS is already configured.</td>
</tr>
</tbody>
</table>

For a ESXi host, the N-VDS type is always set to **NSX Created**.

6 Enter the standard N-VDS details. Multiple N-VDS switches can be configured on a single host.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport Zone</td>
<td>Select the transport zone that this transport node belongs to from the drop-down menu.</td>
</tr>
<tr>
<td>N-VDS Name</td>
<td>Must be the same as the N-VDS name of the transport zone that this node belongs to.</td>
</tr>
<tr>
<td>NIOC Profile</td>
<td>For an ESXi host, select the NIOC profile from the drop-down menu.</td>
</tr>
<tr>
<td>Uplink Profile</td>
<td>Select an existing uplink profile from the drop-down menu or create a custom uplink profile. You can also use the default uplink profile.</td>
</tr>
<tr>
<td>LLDP Profile</td>
<td>Select the enabled or disabled LLDP profile for the firewall from the drop-down menu.</td>
</tr>
<tr>
<td>IP Assignment</td>
<td>Select <strong>Use DHCP</strong>, <strong>Use IP Pool</strong>, or <strong>Use Static IP List</strong>. If you select <strong>Use Static IP List</strong>, you must specify a list of comma-separated IP addresses, a gateway, and a subnet mask.</td>
</tr>
<tr>
<td>IP Pool</td>
<td>If you selected <strong>Use IP Pool</strong> for IP assignment, specify the IP pool name.</td>
</tr>
<tr>
<td>Physical NICs</td>
<td>Add physical NICs to the transport node. You can use the default uplink or assign an existing uplink from the drop-down menu. Click <strong>Add PNIC</strong> to configure additional physical NICs to the transport node.</td>
</tr>
</tbody>
</table>

**Note** Migration of the physical NICs that you add in this field depends on how you configure **PNIC only Migration**, **Network Mappings for Install**, and **Network Mappings for Uninstall**.

- To migrate a used physical NIC (for example, by a standard vSwitch or a vSphere distributed switch) without an associated VMkernel mapping, ensure that **PNIC only Migration** is enabled. Otherwise, the transport node state remains in **partial success**, and the fabric node LCP connectivity fails to establish.
- To migrate a used physical NIC with an associated VMkernel network mapping, disable **PNIC only Migration** and configure the VMkernel network mapping.
- To migrate a free physical NIC, enable **PNIC only Migration**.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PNIC only Migration</td>
<td>Before setting this field, consider the following points:</td>
</tr>
<tr>
<td></td>
<td>▪ Know whether the physical NIC defined is a used NIC or a free NIC.</td>
</tr>
<tr>
<td></td>
<td>▪ Determine whether VMkernel interfaces of a host need to be migrated along with physical NICs.</td>
</tr>
<tr>
<td></td>
<td>Set the field:                                                                INDOW</td>
</tr>
<tr>
<td></td>
<td>▪ Enable PNIC only Migration if you only want to migrate physical NICs from a VSS or DVS switch to an N-VDS switch.</td>
</tr>
<tr>
<td></td>
<td>▪ 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.</td>
</tr>
<tr>
<td></td>
<td>On a host with multiple host switches:</td>
</tr>
<tr>
<td></td>
<td>▪ If all host switches are to migrate only PNICs, then you can migrate the PNICs in a single operation.</td>
</tr>
<tr>
<td></td>
<td>▪ If some hosts switches are to migrate VMkernel interfaces and the remaining host switches are to migrate only PNICs:</td>
</tr>
<tr>
<td></td>
<td>1 In the first operation, migrate only PNICs.</td>
</tr>
<tr>
<td></td>
<td>2 In the second operation, migrate VMkernel interfaces. Ensure that PNIC only Migration is disabled.</td>
</tr>
<tr>
<td></td>
<td>Both PNIC only migration and VMkernel interface migration are not supported at the same time across multiple hosts.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>For more information, see VMkernel Migration to an N-VDS Switch.</td>
</tr>
</tbody>
</table>
### Network Mappings for Install

To migrate VMkernels to N-VDS switch during installation, map VMkernels to an existing logical switch. The NSX Manager migrates the VMkernel to the mapped logical switch on N-VDS.

**Caution** Ensure that the management NIC and management VMkernel interface are migrated to a logical switch that is connected to the same VLAN that the management NIC was connected to before migration. If vmnic<\n> and VMkernel<\n> are migrated to a different VLAN, then connectivity to the host is lost.

**Caution** For pinned physical NICs, ensure that the transport node profile mapping of physical NIC to VMkernel interface matches the configuration specified in the transport node profile. As part of the validation procedure, NSX-T Data Center checks the mapping and if the validation passes migration of VMkernel interfaces to an N-VDS switch is successful. At the same time it is mandatory to configure the network mapping for uninstallation because NSX-T Data Center does not store the mapping configuration of the host switch after migrating the VMkernel interfaces to the N-VDS switch. If the mapping is not configured, connectivity to services, such as vSAN, can be lost after migrating back to the VSS or VDS switch.

For more information, see [VMkernel Migration to an N-VDS Switch](#).

### Network Mappings for Uninstall

To revert the migration of VMkernels during uninstallation, map VMkernels to port groups on VSS or DVS, so that NSX Manager knows which port group the VMkernel must be migrated back to on the VSS or DVS. For a DVS switch, ensure the port group is of the type Ephemeral.

**Caution** For pinned physical NICs, ensure that the transport node profile mapping of physical NIC to VMkernel interface matches the configuration specified in the host switch. It is mandatory to configure the network mapping for uninstallation because NSX-T Data Center does not store the mapping configuration of the host switch after migrating the VMkernel interfaces to the N-VDS switch. If the mapping is not configured, connectivity to services, such as vSAN, can be lost after migrating back to the VSS or VDS switch.

For more information, see [VMkernel Migration to an N-VDS Switch](#).

7. Enter the enhanced datapath N-VDS details. Multiple N-VDS switches can be configured on a single host.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N-VDS Name</td>
<td>Must be the same as the N-VDS name of the transport zone that this node belongs to.</td>
</tr>
<tr>
<td>IP Assignment</td>
<td>Select Use DHCP, Use IP Pool, or Use Static IP List. If you select Use Static IP List, you must specify a list of comma-separated IP addresses, a gateway, and a subnet mask.</td>
</tr>
<tr>
<td>IP Pool</td>
<td>If you selected Use IP Pool for an IP assignment, specify the IP pool name.</td>
</tr>
</tbody>
</table>
### Physical NICs
Add physical NICs to the transport node. You can use the default uplink or assign an existing uplink from the drop-down menu.

Click **Add PNIC** to configure additional physical NICs to the transport node.

**Note** Migration of the physical NICs that you add in this field depends on how you configure **PNIC only Migration**, **Network Mappings for Install**, and **Network Mappings for Uninstall**.

- To migrate a used physical NIC (for example, by a standard vSwitch or a vSphere distributed switch) without an associated VMkernel mapping, ensure that **PNIC only Migration** is enabled. Otherwise, the transport node state remains in **partial success**, and the fabric node LCP connectivity fails to establish.
- To migrate a used physical NIC with an associated VMkernel network mapping, disable **PNIC only Migration** and configure the VMkernel network mapping.
- To migrate a free physical NIC, enable **PNIC only Migration**.

### Uplink
Select the uplink profile from the drop-down menu.

### CPU Config
In the NUMA Node Index drop-down menu, select the NUMA node that you want to assign to an N-VDS switch. The first NUMA node present on the node is represented with the value 0.

You can find out the number for NUMA nodes on your host by running the `esxcli hardware memory get` command.

**Note** If you want to change the number of NUMA nodes that have affinity with an N-VDS switch, you can update the NUMA Node Index value.

In the Lcore per NUMA node drop-down menu, select the number of logical cores that must be used by enhanced datapath.

You can find out the maximum number of logical cores that can be created on the NUMA node by running the `esxcli network ens maxLcores get` command.

**Note** If you exhaust the available NUMA nodes and logical cores, any new switch added to the transport node cannot be enabled for ENS traffic.

---

8 For a preconfigured N-VDS, provide the following details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N-VDS External ID</td>
<td>Must be the same as the N-VDS name of the transport zone that this node belongs to.</td>
</tr>
<tr>
<td>VTEP</td>
<td>Virtual tunnel endpoint name.</td>
</tr>
</tbody>
</table>

9 View the connection status on the **Host Transport Nodes** page.

After adding the host or bare metal server as a transport node, the connection to NSX Manager changes to the Up status in 3-4 minutes.
Alternatively, view the connection status using CLI commands.

- For ESXi, type the `esxcli network ip connection list | grep 1234` command.

  ```bash
  # esxcli network ip connection list | grep 1234
  tcp 0 0 192.168.210.53:20514 192.168.110.34:1234 ESTABLISHED 1000144459 newreno
  netcpa
  ```

- For KVM, type the command `netstat -anp --tcp | grep 1234`.

  ```bash
  user@host:~$ netstat -anp --tcp | grep 1234
  tcp 0 0 192.168.210.54:57794 192.168.110.34:1234 ESTABLISHED -
  ```

Verify that the NSX-T Data Center modules are installed on your host or bare metal server.

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

The modules on different hosts are packaged as follows:

- KVM on RHEL or CentOS - RPMs.
- KVM on Ubuntu - DEBs
- On ESXi, enter the command `esxcli software vib list | grep nsx`.
  The date is the day you performed the installation.
- On RHEL or CentOS, enter the command `yum list installed` or `rpm -qa`.
- On Ubuntu, enter the command `dpkg --get-selections`.

(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.

```bash
python aggsvc_change_intervals.py -m '<NSX ManagerIPAddress>' -u 'admin' -p '<password>' -i 900
```

b Run the script, which is located in the NSX-T Data Center file store.

```bash
python aggsvc_change_intervals.py -m '<NSX ManagerIPAddress>' -u 'admin' -p '<password>' -r
```
Note  For an NSX-T Data Center created N-VDS, after the transport node is created, if you want to change the configuration, such as IP assignment to the tunnel endpoint, you must do it through the NSX Manager GUI and not through the CLI on the host.

What to do next

Migrate network interfaces from a vSphere Standard Switch to an N-VDS. See VMkernel Migration to an N-VDS Switch.

Configure a Managed Host Transport Node

If you have a vCenter Server cluster, you can automate the installation and creation of transport nodes on all the NSX-T Data Center hosts in single or multiple clusters instead of configuring manually.

If the transport node is already configured, then automated transport node creation is not applicable for that node.

Prerequisites

- Verify that all hosts in the vCenter Server cluster are powered on.
- Verify that the system requirements are met. See System Requirements.
- Verify that a transport zone is available. See Create Transport Zones.
- Verify that a transport node profile is configured. See Add a Transport Node Profile.

Procedure

1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Select System > Fabric > Nodes > Host Transport Nodes.
3. From the Managed drop-down menu, select an existing compute manager.
4. Select a cluster and click Configure NSX.
5. Select the transport node profile from the drop-down menu and click Save.

   NSX-T Data Center installation and transport node creation on each host in the cluster starts in parallel. The entire process depends on the number of hosts in the cluster.

6. (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  netcpa

7. 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.

   You can also see that the transport zone is applied to the hosts in the cluster.
(Optional) Remove an NSX-T Data Center installation and transport node from a host in the cluster.

a Select a cluster and click **Actions > Detach TN Profile** to detach the applied NSX-T Data Center configuration from the cluster.

b 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. Any new host added to the vCenter Server cluster will not be automatically configured until the transport node profile is reapplied to the cluster.

Detach a transport node profile applied to a cluster. The NSX-T Data Center configuration applied to the hosts is removed.

a Select a cluster and click **Actions > Detach TN Profile**.

b Select one or more hosts and click **Actions > Detach TN Profile** to detach the applied NSX-T Data Center configuration.

The transport node profile is detached from the cluster. However, the host continues to be attached to the transport zone and N-VDS switch.

What to do next
Create a logical switch and assign logical ports. See the Advanced Switching section in the *NSX-T Data Center Administration Guide*.

### Configure an ESXi Host Transport Node with Link Aggregation

This procedure describes how to create an uplink profile that has a link aggregation group configured, and how to configure an ESXi host transport node to use that uplink profile.

**Prerequisites**

- Familiarize yourself with the steps to create an uplink profile. See [Create an Uplink Profile](#).
- Familiarize yourself with the steps to create a host transport node. See [Create a Standalone Host or Bare Metal Server Transport Node](#).

**Procedure**

1. From a browser, log in with admin privileges to an NSX Manager at `https://<nsx-manager-ip-address>`.
2. Select **System > Fabric > Profiles > Uplink Profiles > Add**.
3. Enter a name and optionally a description.
   For example, you enter the name `uplink-profile1`.
4. Under **LAGs**, click **Add** to add a link aggregation group.
   For example, you add an LAG called `lag1` with 2 uplinks.
5. Under **Teamings**, select **Default Teaming**.
6  In the **Active Uplinks** field, enter the name of the LAG that you added in the step 4. In this example, the name is `lag1`.

7  Enter a value for the **Transport VLAN** and **MTU**.

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

9  Under **Teamings**, click **Add** to add an entry for link aggregation.

10 Select **Fabric > Nodes > Host Transport Nodes > Add**.

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

12 In the **N-VDS** tab, select the uplink profile `uplink-profile1` that was created in step 3.

13 In the **Physical NICs** field, the physical NICs and uplinks dropdown list reflects the new NICs and uplink profile. Specifically, the uplinks `lag1-0` and `lag1-1`, corresponding to the LAG `lag1` that was created in step 4 are displayed. Select a physical NIC for `lag1-0` and a physical NIC for `lag1-1`.

14 Enter information for the other fields.

### Configure a Host with a Single N-VDS Switch

Server configurations supporting four physical NICs (four X 10G NICs) and two physical NICs (two X 25G NICs) can run both edge and compute VMs on the same host. The compute VMs, Edge VM, and Management VM can be hosted on a single N-VDS switch. The N-VDS manages traffic through a single teaming policy or pin VLANs to a teaming policy.

If vDS/vSS switches currently manage the VMkernel traffic on the host, then migrate the VMkernel and virtual NICs from vDS/vSS to N-VDS switch. Moving to a single N-VDS in a single cluster topology involves migrating VMkernel ports, port groups, virtual machine NICs to an N-VDS switch. After migration, ensure that traffic from the NSX Edge VM can reach the host and back from the host to the NSX Edge VM as the NSX Edge VM is configured on the same N-VDS as the host.

**Topology**
Prerequisites

Figure 8-3. Host with a Single N-VDS Switch

Procedure

1. Install NSX Manager and NSX Edge VM on the same host.
2. Prepare the host as a NSX-T Data Center transport node.
   a. Prepare a VLAN transport zone.
   b. Create an IP pool for tunnel endpoint IP addresses.
   c. Create an uplink profile.
   d. Add a transport node profile.

See Add a Transport Node Profile
3 Migrate VMkernel and port group from VSS or VDS to N-VDS using NSX Manager UI.
   To know more about migrating VMkernel and physical NICs to an N-VDS switch, see VMkernel Migration to an N-VDS Switch.

4 Alternatively, migrate VMkernel and physical NICs from VSS or VDS to N-VDS by making the following API call.

   ```
   https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-ID>?vnic=<vmk0,vmk1,..><VMInstanceUUID:DeviceID>&vnic_migration_dest=<vmknetworkID><VIF_NSXlogicalports>
   ```

   **Note** When migrating interfaces into logical switches, logical ports and vif IDs must be created in advance because `vnic_migration_dest` must contain existing vif IDs.

   Where,
   - `vnic` represents the ESXi vSphere VMkernel interfaces and one VM NIC ID. For example, the supported format is `<vmk0, vmk1,...><VMInstanceUUID:DeviceID>`.
   - `vnic_migration_dest` represents the migration destination of ESXi vSphere VMkernel interfaces.
   - When migrating VMkernel interfaces to a logical switch, the `<VIF_NSXlogicalports>` must represent the virtual IDs of the logical ports created in logical switches.
   - When migrating VMkernel interfaces to a DVS or VSS host switch, the `<VIF IDs>` must represent the port group names in DVS or VSS host switch.

5 Migrate only VMkernel interfaces by making the following API call.

   ```
   https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-ID>?if_id=<vmk0,vmk1,..>&esx_mgmt_if_migration_dest=<vmknetworkID0, vmknetworkID1,..>
   ```

   Where,
   - `esx_mgmt_if_migration_dest` represents network IDs to which the ESXi vSphere VMkernel interfaces are migrated to.
   - When migrating VMkernel interfaces to a logical switch, the network IDs are virtual IDs of logical ports created in logical switches.
   - When migrating VMkernel interfaces to a VDS or VSS host switch, the network IDs are the port group names in VDS or VSS host switch.
   - `if_ID` represents the ESXi vSphere VMkernel interfaces to migrate to a logical switch on N-VDS or a port group on a VDS or VSS host switch.

6 Verify on the host whether the VMkernel interfaces and physical NICs are successfully migrated from a VSS or DVS switch to an N-VDS switch.
   Verify that vSS or vDS entry is removed in the vCenter Server.

7 Prepares an NSX Edge transport node and create an NSX Edge cluster.
8 Verify that a BFD session is established between an NSX Edge VM TEP and host TEP.

The BFD protocol is a simple hello mechanism that detects failures in a network. Hello packets are sent from the routing device to a neighbor device at a specified, regular interval. A neighbor failure is detected when the routing device stops receiving a reply after a specified interval.

As a single host cluster manages both NSX Edge VM and Host, it becomes important to monitor network communication between NSX Edge VM and Host. BFD mechanism is used to detect a network failure between NSX Edge VM TEP and Host TEP.

   a Considering the Host and NSX Edge are connected to the same N-VDS, ensure that the host uplink profile is configured with transport VLAN ID 73.
   b The NSX Edge VM TEP is connected to the VLAN logical switch 75. With the NSX Edge TEP on VLAN 75, configure its uplink profile to connect to transport VLAN 0.
   c Ensure that an external router is configured in the network for switching and routing traffic between the Host and NSX Edge.
   d Verify that NSX establishes BFD session between NSX Edge TEP and host TEP.
   e Log in to the host.
   f Run `get bfd-session` and `get vteps` to verify whether the BFD session is up on the NSX Edge and the Host.

9 Verify that transport node status of the NSX Edge VM is Up.

A single N-VDS switch is configured on a single host cluster that hosts the host and management VMs, and NSX Edge VMs.

**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.

```bash
# 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
<table>
<thead>
<tr>
<th>Name</th>
<th>IPv4 Address</th>
<th>IPv4 Netmask</th>
<th>IPv4 Broadcast</th>
<th>Address Type</th>
<th>DHCP DNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmk1</td>
<td>10.20.20.53</td>
<td>255.255.255.0</td>
<td>10.20.20.255</td>
<td>STATIC</td>
<td>false</td>
</tr>
<tr>
<td>vmk10</td>
<td>192.168.250.3</td>
<td>255.255.255.0</td>
<td>192.168.250.255</td>
<td>STATIC</td>
<td>false</td>
</tr>
</tbody>
</table>
```
In KVM, you can verify the tunnel endpoint and IP allocation with the `ifconfig` command.

```bash
# 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:

```json
{
   "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"
}
```

**Visual Representation of N-VDS**

You get a granular view of N-VDS at an individual host level. NSX-T Data Center provides a visual representation of the connectivity status between the uplink of the N-VDS and VMs associated to a transport zone. The objects represented visually include the teaming policy - uplink and physical NIC that provide connectivity to VMs. The other set of objects represented visually are VMs, associated logical ports and switches, and status of VMs. The visual representation makes it easier to manage N-VDS.

**Note** Only ESXi hosts support visualization of N-VDS object.
**Figure 8-4. N-VDS Visualization**

**Procedure**

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

2. Select **System > Fabric > Nodes > Host Transport Nodes**.

3. From the Managed by field, select **Standalone Host** or a **compute manager**.

4. Select the host.

5. Click the **N-VDS Visualization** tab.

6. Select an N-VDS.

   NSX-T visually represents uplink profiles connected to VMs, logical ports associated to VMs, logical switches connected to a transport zone.
To view uplink profiles connected to a VM and the logical port to which a VM is connected, select a VM. NSX-T visually represents the connectivity between a VM and an uplink profile.

To view which VMs are connected to an uplink profile, select the uplink profile.

To view logical ports associated to a VM, expand the logical switch, click the VM. The logical port details are displayed in a separate dialog box.

**Note** The admin status of a logical port is displayed on the dialog box. If the operational status is down it is not displayed on the dialog box.

---

**Manual Installation of NSX-T Data Center Kernel Modules**

As an alternative to using the NSX-T Data Center Fabric > Nodes > Hosts > Add UI or the POST /api/v1/fabric/nodes API, you can install NSX-T Data Center kernel modules manually from the hypervisor command line.

**Note** You cannot manually install of NSX-T Data Center kernel modules on a bare metal server.

---

**Manually Install NSX-T Data Center Kernel Modules on ESXi Hypervisors**

To prepare hosts to participate in NSX-T Data Center, you must install NSX-T Data Center kernel modules on ESXi hosts. This allows you to build the NSX-T Data Center control-plane and management-plane fabric. NSX-T Data Center kernel modules packaged in VIB files run within the hypervisor kernel and provide services such as distributed routing, distributed firewall, and bridging capabilities.

You can download the NSX-T Data Center VIBs manually and make them part of the host image. The download paths can change for each release of NSX-T Data Center. Always check the NSX-T Data Center downloads page to get the appropriate VIBs.

**Procedure**

1. Log in to the host as root or as a user with administrative privileges
2. Navigate to the /tmp directory.
   ```
   [root@host:~]: cd /tmp
   ```
3. Download and copy the nsx-lcp file into the /tmp directory.
4. Run the install command.
   ```
   [root@host:/tmp]: esxcli software vib install -d /tmp/nsx-lcp-<release>.zip
   ```

**Installation Result**

Message: Operation finished successfully.
Reboot Required: false
VIBs Installed: VMware_bootbank_nsx-aggservice_<release>, VMware_bootbank_nsx-da_<release>,

---
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'.

As a result of adding an ESXi host to the NSX-T Data Center fabric, the following VIBs get installed on the host.

- **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-da**—Collects discovery agent (DA) data about the hypervisor OS version, virtual machines, and network interfaces. Provides the data to the management plane, to be used in troubleshooting tools.
- **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-lldp**—Provides support for the Link Layer Discovery Protocol (LLDP), which is a link layer protocol used by network devices for advertising their identity, capabilities, and neighbors on a LAN.
- **nsx-mpa**—Provides communication between NSX Manager and hypervisor hosts.
- **nsx-netcpa**—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-python-protobuf**—Provides Python bindings for protocol buffers.
- **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.
- **nsxa**—Performs host-level configurations, such as N-VDS creation and uplink configuration.
- **nsxcli**—Provides the NSX-T Data Center CLI on hypervisor hosts.
- **nsx-support-bundle-client**—Provides the ability to collect support bundles.

To verify, you can run the `esxcli software vib list | grep nsx` or `esxcli software vib list | grep <yyyy-mm-dd>` command on the ESXi host, where the date is the day that you performed the installation.
What to do next

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

Manually Install NSX-T Data Center Kernel Modules 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.

To verify, you can run the `dpkg -l | grep nsx` command.

```
user@host:~$ dpkg -l | grep nsx

ii  nsx-agent                           <release>     amd64        NSX Agent
ii  nsx-aggservice                      <release>     all          NSX Aggregation Service Lib
ii  nsx-cli                             <release>     all          NSX CLI
ii  nsx-da                               <release>     amd64        NSX Inventory Discovery Agent
ii  nsx-host                            <release>     all          NSX host meta package
ii  nsx-host-node-status-reporter       <release>     amd64        NSX Host Status Reporter for Aggregation Service
ii  nsx-lldp                            <release>     amd64        NSX LLDP Daemon
ii  nsx-logical-exporter                <release>     amd64        NSX Logical Exporter
ii  nsx-mpa                              <release>     amd64        NSX Management Plane Agent Core
ii  nsx-netcpa                           <release>     amd64        NSX Netcpa
ii  nsx-sfhc                             <release>     amd64        NSX Service Fabric Host Component
ii  nsx-transport-node-status-reporter   <release>     amd64        NSX Transport Node Status Reporter
ii  nsxa                                 <release>     amd64        NSX L2 Agent
```

Any errors are most likely caused by incomplete dependencies. The `apt-get install -f` command can attempt to resolve dependencies and re-run the NSX-T Data Center installation.

**What to do next**

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

**Manually Install NSX-T Data Center Kernel Modules on RHEL and CentOS KVM Hypervisors**

To prepare hosts to participate in NSX-T Data Center, you can manually install NSX-T Data Center kernel modules on RHEL or CentOS KVM hosts.

This allows you to build the NSX-T Data Center control-plane and management-plane fabric. NSX-T Data Center kernel modules packaged in RPM files run within the hypervisor kernel and provide services such as distributed routing, distributed firewall, and bridging capabilities.

You can download the NSX-T Data Center RPMs manually and make them part of the host image. Be aware that download paths can change for each release of NSX-T Data Center. Always check the NSX-T Data Center downloads page to get the appropriate RPMs.

**Prerequisites**

Ability to reach a RHEL or CentOS repository.
Procedure

1. Log in to the host as an administrator.
2. Download and copy the nsx-lcp file into the /tmp directory.
3. Untar the package.
   ```
   tar -zxvf nsx-lcp--<release>--rhel7.4_x86_64.tar.gz
   ```
4. Navigate to the package directory.
   ```
   cd nsx-lcp-rhel74_x86_64/
   ```
5. Install the packages.
   ```
   sudo yum install *.rpm
   ```
   When you run the yum install command, any NSX-T Data Center dependencies are resolved, assuming the RHEL or CentOS hosts can reach their respective repositories.
6. Reload the OVS kernel module.
   ```
   /etc/init.d/openvswitch force-reload-kmod
   ```
   If the hypervisor uses DHCP on OVS interfaces, restart the network interface on which DHCP is configured. You can manually stop the old dhclient process on the network interface and restart a new dhclient process on that interface.
7. To verify, you can run the `rpm -qa | egrep 'nsx|openvswitch|nicira'` command.
   The installed packages in the output must match the packages in the nsx-rhel74 or nsx-centos74 directory.

What to do next

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

Create an NSX Edge Transport Node

You can add an NSX Edge to the NSX-T Data Center fabric and proceed to configure the NSX Edge 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.

**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/`. The netcpa agent does not create a certificate if a certificate already exists.

**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 > Add Edge VM**.
3. Type a name for the NSX Edge.
4. Type the Host name or FQDN from vCenter Server.
5. For an optimal performance, reserve memory for the NSX Edge appliance.
   - Set the reservation to ensure that NSX Edge has sufficient memory to run efficiently. See NSX Edge VM System Requirements.
6. 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

7 Enter the NSX Edge details.

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

8 Enter the NSX Edge interface details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Assignment</td>
<td>Select <strong>DHCP</strong> or <strong>Static</strong> IP.</td>
</tr>
<tr>
<td></td>
<td>If you select <strong>Static</strong>, you must specify a list of comma-separated IP addresses, a gateway, and a subnet mask.</td>
</tr>
<tr>
<td>Management Interface</td>
<td>Select the VM Network interface from the drop-down menu.</td>
</tr>
</tbody>
</table>

9 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.

10 Enter the N-VDS information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge Switch Name</td>
<td>Select the overlay switch from the drop-down menu.</td>
</tr>
<tr>
<td>Uplink Profile</td>
<td>Select the uplink profile from the drop-down menu.</td>
</tr>
<tr>
<td></td>
<td>The available uplinks depend on the configuration in the selected uplink profile.</td>
</tr>
<tr>
<td>IP Assignment</td>
<td>Select <strong>Use IP Pool</strong> or <strong>Use Static IP List</strong> for the overlay N-VDS.</td>
</tr>
<tr>
<td></td>
<td>If you select <strong>Use Static IP List</strong>, you must specify a list of comma-separated IP addresses, a gateway, and a subnet mask.</td>
</tr>
<tr>
<td>IP Pool</td>
<td>If you selected <strong>Use IP Pool</strong> for IP assignment, specify the IP pool name.</td>
</tr>
<tr>
<td>Datapath Interfaces</td>
<td>Select the data path interface name for the uplink interface.</td>
</tr>
</tbody>
</table>

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.

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.
- Join the NSX Edges with the management plane.
- Add the NSX Edges as transport nodes.
- Optionally, create an NSX Edge cluster profile for high availability (HA). You can also use the default NSX Edge cluster profile.

Procedure
1. From a browser, log in with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. Select System > Fabric Nodes > Edge Clusters > Add.
3. Enter the NSX Edge cluster a name.
4. Select an NSX Edge cluster profile from the drop-down menu.
5. Select either NSX Edge Node from the Member Type drop-down menu.
   If the virtual machine is deployed in a public cloud environment, select Public Cloud Gateway otherwise select NSX Edge Node.
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*. 
Installing NSX Cloud Components

NSX Cloud provides a single pane of glass for managing your public cloud networks.

NSX Cloud is agnostic of provider-specific networking that does not require hypervisor access in a public cloud.

It offers several benefits:

- You can develop and test applications using the same network and security profiles used in the production environment.
- Developers can manage their applications until they are ready for deployment.
- With disaster recovery, you can recover from an unplanned outage or a security threat to your public cloud.
- If you migrate your workloads between public clouds, NSX Cloud ensures that similar security policies are applied to workload VMs regardless of their new location.

This chapter includes the following topics:

- NSX Cloud Architecture and Components
- Overview of Installing and Configuring NSX Cloud Components for your Public Cloud
- Install CSM and Connect with NSX Manager
- Connect Public Cloud with On-prem Deployment
- Add your Public Cloud Account
- Deploy or Link NSX Public Cloud Gateways
- Undeploy PCG

NSX Cloud Architecture and Components

NSX Cloud integrates the NSX-T Data Center core components with your public cloud to provide network and security across your implementations.
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.

- **NSX 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. See [Deploy or Link NSX Public Cloud Gateways](#) for details.

- **NSX Agent** functionality that provides NSX-managed datapath for workload VMs.

### Modes of Deployment

The NSX Public Cloud Gateway can either be a standalone gateway appliance or a shared between your public cloud VPCs or VNets to achieve a hub and spoke topology.

**Self-managed VPC or VNet serves as a Transit VPC:** 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. This VPC or VNet also qualifies as a Transit VPC or VNet because you can use the PCG deployed on it to onboard VMs hosted in other VPCs or VNets.

**Compute VPC or VNet links to Transit VPC or VNet:** VPCs or VNets that do not have the PCG deployed on them but link to a Transit VPC or VNet are called *Compute* VPCs or VNets.

### Overview of Installing and Configuring NSX Cloud Components for your Public Cloud

Refer to the checklist for an overview of the steps involved in enabling NSX-T Data Center to manage your workload VMs in the public cloud.

### Day-0 Workflow for Connecting NSX Cloud with your Public Cloud

This workflow provides an overview of the steps required to get started with NSX Cloud for your public cloud.

**Note** While planning your deployment, ensure that the on-prem NSX-T Data Center appliances have good connectivity with the PCG deployed in the public cloud. Also, Transit VPCs/VNets must be in the same region as the Compute VPCs/VNets.

#### Table 9-1. Day-0 Workflow for connecting NSX Cloud with your public cloud

<table>
<thead>
<tr>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install CSM and connect with NSX Manager.</td>
<td>See <a href="#">Install CSM and Connect with NSX Manager</a>.</td>
</tr>
<tr>
<td>Add one or more of your public cloud accounts in CSM.</td>
<td>See <a href="#">Add your Public Cloud Account</a>.</td>
</tr>
</tbody>
</table>
Table 9-1. Day-0 Workflow for connecting NSX Cloud with your public cloud (Continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy PCG in your Transit VPCs or VNets and link to your Compute VPCs or VNets.</td>
<td>See Deploy or Link NSX Public Cloud Gateways.</td>
</tr>
<tr>
<td>Onboard workload VMs by tagging in your public cloud and installing the NSX Agent on them.</td>
<td>Follow instructions at Onboard Workload VMs in the NSX-T Data Center Administration Guide.</td>
</tr>
</tbody>
</table>

Install CSM and Connect with NSX Manager

Use the Setup Wizard to connect CSM with NSX Manager and set up proxy servers, if any.

Install CSM

The Cloud Service Manager (CSM) is an essential component of NSX Cloud.

Install CSM after installing the core NSX-T Data Center components.

See Install NSX Manager and Available Appliances for detailed instructions.

**Note** Installing NSX Cloud requires you to enable FQDN usage (DNS) on NSX Managers. See Publishing the FQDNs of the NSX Managers.

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**.
Enter the following details in the NSX Manager Credentials screen:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager Host Name</td>
<td>Enter the fully qualified domain name (FQDN) of the NSX Manager, if available. You may also enter the IP address of NSX Manager.</td>
</tr>
<tr>
<td>Admin Credentials</td>
<td>Enter an Enterprise Administrator username and password for NSX Manager.</td>
</tr>
<tr>
<td>Manager Thumbprint</td>
<td>Optionally, enter the NSX Manager's thumbprint value. If you leave this field blank, the system identifies the thumbprint and displays it in the next screen.</td>
</tr>
</tbody>
</table>

(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.

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.

(Optional) Set up the Proxy server. See instructions in (Optional) Configure Proxy Servers.

(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.
In the Configure Proxy Servers screen, enter the following details:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Use this radio button to indicate the default proxy server.</td>
</tr>
<tr>
<td>Profile Name</td>
<td>Provide a proxy server profile name. This is mandatory.</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>Enter the proxy server’s IP address. This is mandatory.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the proxy server's port. This is mandatory.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Optional. If you want to set up additional authentication, select this box and provide valid username and password.</td>
</tr>
<tr>
<td>Username</td>
<td>This is required if you select the Authentication checkbox.</td>
</tr>
<tr>
<td>Password</td>
<td>This is required if you select the Authentication checkbox.</td>
</tr>
<tr>
<td>Certificate</td>
<td>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.</td>
</tr>
<tr>
<td>No Proxy</td>
<td>Select this option if you do not want to use any of the proxy servers configured.</td>
</tr>
</tbody>
</table>

(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 Public Cloud with On-prem Deployment

You must use suitable connectivity options to connect your on-prem deployment with your public cloud accounts or subscriptions.
Enable Access to ports and protocols on CSM for Hybrid Connectivity

Open up necessary network ports and allow the required protocols on NSX Manager to enable public cloud connectivity.

Allow access to NSX Manager from the Public Cloud

Open up the following network ports and protocols to allow connectivity with your on-prem NSX Manager deployment:

Table 9-2.

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol/Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCG</td>
<td>NSX Manager</td>
<td>TCP/5671</td>
<td>Inbound traffic from public cloud to on-prem NSX-T Data Center for Management Plane Communication.</td>
</tr>
<tr>
<td>PCG</td>
<td>NSX Manager</td>
<td>TCP/8080</td>
<td>Inbound traffic from public cloud to on-prem NSX-T Data Center for access to an HTTP repository for upgrading NSX Cloudcomponents.</td>
</tr>
<tr>
<td>PCG</td>
<td>NSX Controller</td>
<td>TCP/1234, TCP/1235</td>
<td>Inbound traffic from public cloud to on-prem NSX-T Data Center for Control Plane Communication.</td>
</tr>
<tr>
<td>PCG</td>
<td>DNS</td>
<td>UDP/53</td>
<td>Inbound traffic from public cloud to on-prem NSX-T Data Center, (if you are using the on-prem DNS Server).</td>
</tr>
<tr>
<td>CSM</td>
<td>PCG</td>
<td>TCP/7442</td>
<td>CSM Config Push</td>
</tr>
<tr>
<td>Any</td>
<td>NSX Manager</td>
<td>TCP/443</td>
<td>NSX Manager UI</td>
</tr>
<tr>
<td>Any</td>
<td>CSM</td>
<td>TCP/443</td>
<td>CSM UI.</td>
</tr>
</tbody>
</table>

**Important** All NSX-T Data Center infrastructure communication leverages SSL-based encryption. Ensure your firewall allows SSL traffic over non-standard ports.
Connect your Microsoft Azure Network with your On-prem NSX-T Data Center Deployment

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. See 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 the Azure Security Center Documentation.

**Configure your VNet**

In Microsoft Azure, create routable CIDR blocks and set up the required subnets.
- One management subnet with a recommended range of at least /28, to handle:
  - control traffic to on-prem appliances
  - API traffic to cloud-provider API endpoints
- One downlink subnet with a recommended range of /24, for the workload VMs.
- One, or two for HA, uplink subnets with a recommended range of /24, for routing of north-south traffic leaving from or entering the VNet.

See Deploy or Link NSX Public Cloud Gateways for details on how these subnets are used.
Connect your Amazon Web Services (AWS) Network with your On-prem NSX-T Data Center Deployment

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. See [AWS reference documentation](#) for details.

**Note** You must review and implement the applicable security considerations and best practices by AWS; see [AWS Security Best Practices](#).

**Configure your VPC**

You need the following configurations:

- six subnets for supporting PCG with High Availability
- an Internet gateway (IGW)
- a private and a public route table
- subnet association with route tables
- DNS resolution and DNS hostnames enabled

Follow these guidelines to configure your VPC:

1. Assuming your VPC uses a /16 network, for each gateway that needs to be deployed, set up three subnets.

   **Important** If using High Availability, set up three additional subnets in a different Availability Zone.

- **Management subnet**: This subnet is used for management traffic between on-prem NSX-T Data Center and PCG. The recommended range is /28.
- **Uplink subnet**: This subnet is used for north-south internet traffic. The recommended range is /24.
- **Downlink subnet**: This subnet encompasses the workload VM's IP address range, and should be sized accordingly. Bear in mind that you may need to incorporate additional interfaces on the workload VMs for debugging purposes.

  **Note**  Label the subnets appropriately, for example, *management-subnet*, *uplink-subnet*, *downlink-subnet*, because you will need to select the subnets when deploying PCG on this VPC. See [Deploy or Link NSX Public Cloud Gateways](#) 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.

### Add your Public Cloud Account

To add your public cloud inventory, you need to create roles in your public cloud to allow access to NSX Cloud and then add the required information in CSM.

### Set Up Secure Access to Your Microsoft Azure Inventory

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.

  **Note**  If you already added an AWS account to CSM, update the MTU in NSX Manager > Fabric > Profiles > Uplink Profiles > PCG-Uplink-HostSwitch-Profile to 1500 before adding the Microsoft Azure account. This can also be done using the NSX Manager REST APIs.

**Overview:**
- Your Microsoft Azure subscription contains one or more VNets that you want to bring under NSX-T Data Center management. The VNet might be in Transit mode or Compute mode. Transit VNet is one in which you deploy the PCG. You can link other VNets to the Transit VNet and onboard workload VMs hosted in them. The VNets linked to the Transit VNet are called Compute VNets.
- NSX Cloud provides a PowerShell script to generate the Service Principal and roles that use the managed identity feature of Microsoft Azure to manage authentication while keeping your Microsoft Azure credentials secure. You can also include multiple subscriptions under one Service Principal using this script.
- You have the option of reusing the Service Principal for all your subscriptions, or to create new Service Principals as required. There is an additional script if you want to create separate Service Principals for additional subscriptions.
For multiple subscriptions, whether you are using a single Service Principal for all, or multiple Service Principals, you must update the JSON files for the CSM and PCG roles to add each additional subscription name under the section AssignableScopes.

If you already have an NSX Cloud Service Principal in your VNet, you can update it by running the scripts again and leaving out the Service Principal name from the parameters.

The Service Principal name must be unique for your Microsoft Azure Active Directory. You may use the same Service Principal in different subscriptions under the same Active Directory domain, or different Service Principals per subscription. But you cannot create two Service Principals with the same name.

You must either be the owner of or have permissions to create and assign roles in all the Microsoft Azure subscriptions.

The following scenarios are supported:

Scenario 1: You have a single Microsoft Azure Subscription that you want to enable with NSX Cloud.

Scenario 2: You have multiple Microsoft Azure Subscriptions under the same Microsoft Azure Directory, that you want to enable with NSX Cloud, but want to use one NSX Cloud Service Principal across all your subscriptions.

Scenario 3: You have multiple Microsoft Azure Subscriptions under the same Microsoft Azure Directory, that you want to enable with NSX Cloud, but want to use different NSX Cloud Service Principal names for different subscriptions.

Here is an outline of the process:

1. Use the NSX Cloud PowerShell script to:
   - Create a Service Principal account for NSX Cloud.
   - Create a role for CSM.
   - Create a role for PCG.
2. (Optional) Create Service Principals for other subscriptions you want to link.
3. Add the Microsoft Azure subscription in CSM.

   **Note** If using multiple subscriptions, whether using the same or different Service Principals, you must add each subscription separately in CSM.

**Generate the Service Principal and Roles**

NSX Cloud provides PowerShell scripts that help you generate the required service principal and roles for one or multiple subscriptions.

**Prerequisites**

- You must have PowerShell 5.0+ with the AzureRM Module installed.
You must either be the owner of or have permissions to create and assign roles in all the Microsoft Azure subscriptions.

**Note** The response time from Microsoft Azure can cause the script to fail when you run it the first time. If the script fails, try running it again.

**Procedure**

1. On a Windows desktop or server, download the ZIP file named `CreateNSXCloudCredentials.zip` from the NSX-T Data Center Download page > Drivers & Tools > NSX Cloud Scripts > Microsoft Azure.

2. Extract the following contents of the ZIP file in your Windows system:

<table>
<thead>
<tr>
<th>Script/File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateNSXRoles.ps1</td>
<td>The PowerShell script to generate the NSX Cloud Service Principal and managed identity roles for CSM and PCG. This script takes the following parameters:</td>
</tr>
<tr>
<td></td>
<td>-subscriptionId &lt;the Transit_VNet's_Azure_subscription_ID&gt;</td>
</tr>
<tr>
<td></td>
<td>(optional) -servicePrincipalName &lt;Service_Principal_Name&gt;</td>
</tr>
<tr>
<td></td>
<td>(optional) -useOneServicePrincipal</td>
</tr>
<tr>
<td>AddServicePrincipal.ps1</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>-computeSubscriptionId &lt;the_Compute_VNet's_Azure_subscription_ID&gt;</td>
</tr>
<tr>
<td></td>
<td>-transitSubscriptionId &lt;the_Transit_VNet's_Azure_Subscription_ID&gt;</td>
</tr>
<tr>
<td></td>
<td>-csmRoleName &lt;CSM_Role_Name&gt;</td>
</tr>
<tr>
<td></td>
<td>-servicePrincipalName &lt;Service_Principal_Name&gt;</td>
</tr>
<tr>
<td>nsx_csm_role.json</td>
<td>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.</td>
</tr>
<tr>
<td>nsx_pcg_role.json</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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:

   ```json
   "AssignableScopes": [
     "/subscriptions/aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeeee",
     "/subscriptions/aaaaaaaa-bbbb-cccc-dddd-fffffffffffffff",
     "/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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>-computeSubscriptionId</td>
<td>The Compute_VNet's Azure Subscription ID</td>
</tr>
<tr>
<td>-transitSubscriptionId</td>
<td>The Transit VNet's Azure Subscription ID</td>
</tr>
<tr>
<td>-csmRoleName</td>
<td>Get this value from the file <code>nsx_csm_role.JSON</code></td>
</tr>
<tr>
<td>-servicePrincipalName</td>
<td>New Service Principal name</td>
</tr>
</tbody>
</table>

```
./AddServicePrincipal.ps1 -computeSubscriptionId <the_Compute_VNet's_Azure_subscription_ID>
-transitSubscriptionId <the_Transit_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

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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 and you can name them appropriately in CSM, for example, Azure-DevOps-Account, Azure-Finance-Account, etc.</td>
</tr>
<tr>
<td>Client ID</td>
<td>Copy paste this value from the output of the PowerShell script.</td>
</tr>
<tr>
<td>Key</td>
<td>Copy paste this value from the output of the PowerShell script.</td>
</tr>
<tr>
<td>Subscription ID</td>
<td>Copy paste this value from the output of the PowerShell script.</td>
</tr>
<tr>
<td>Tenant ID</td>
<td>Copy paste this value from the output of the PowerShell script.</td>
</tr>
</tbody>
</table>
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway Role Name</td>
<td>The default value is <code>nsx-pcg-role</code>. This value is available from the <code>nsx_pcg_role.json</code> file if you changed the default.</td>
</tr>
<tr>
<td>Cloud Tags</td>
<td>By default this option is enabled and allows your Microsoft Azure tags to be visible in NSX Manager</td>
</tr>
</tbody>
</table>

4. Click **Save**.

CSM adds the account and you can see it in the **Accounts** section within three minutes.

### What to do next

**Deploy PCG in a Self-Managed or Transit VNet**

### Set Up Secure Access to Your AWS Inventory

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:**

- You can use the Transit/Compute VPC topology where you deploy the PCG in one VPC, making it the Transit VPC, and link other VPCs to it, which are called Compute VPCs.
- NSX Cloud provides a shell script that you can run from the AWS CLI of your AWS account to create the IAM profile and role, and create a trust relationship for Transit and Compute VPCs.
- The following scenarios are supported:
  - **Scenario 1:** You want to use a single AWS account with NSX Cloud.
  - **Scenario 2:** You want to use multiple sub-accounts in AWS that are managed by a master AWS account.
  - **Scenario 3:** You want to use multiple AWS accounts with NSX Cloud.

Here is an outline of the process:

1. Use the NSX Cloud shell script, that requires AWS CLI, to do the following:
   - 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
- `jq` (A JSON parser)
- `openssl`

**Note** If using multiple AWS accounts, the accounts must be peered using a suitable method.

**Procedure**

1. 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.

2. **Scenario 1:** You want to use a single AWS account with NSX Cloud.
   a. Run the script, for example:
      
      ```bash
      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 Self-Managed or Transit VPC to finish the process of setting up a Transit or Self-Managed VPC.
3 **Scenario 2**: You want to use multiple sub-accounts in AWS that are managed by one master AWS account.

a Run the script from your AWS master account.

   ```bash
nenx_csm_iam_script.sh
```

b Enter `yes` when prompted with the question *Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no]*

c Enter a name for the IAM user when asked *What do you want to name the IAM User?*

*Note* The IAM user name must be unique in your AWS account.

d Enter `no` when asked *Do you want to add trust relationship for any Transit VPC account? [yes/no]*

*Note* With a master AWS account, if your Transit VPC has permission to view Compute VPCs in the sub-accounts, you do not need to establish a trust relationship with your sub-accounts. If not, follow the steps for **Scenario 3** to set up multiple accounts.

When the script runs successfully, the IAM profile and a role for PCG is created in your AWS master account. The values are saved in the output file in the same directory where you ran the script. The filename is `aws_details.txt`. Next, follow instructions at Add your AWS Account in CSM and then Deploy PCG in a Self-Managed or Transit VPC to finish the process of setting up a Transit or Self-Managed VPC.

4 **Scenario 3**: You want to use multiple AWS accounts with NSX Cloud.

*Note* Verify that the AWS accounts are peered before you proceed.

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 and deploying a PCG in it.

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.

*Note* 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 Enter `yes` when asked *Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no]*

*Note* If you already added this AWS account into CSM and want to reuse the script to connect to a different AWS account, you can enter `no` and skip the creation of the IAM user.
e. 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.

f. Enter *yes* when asked *Do you want to add trust relationship for any Transit VPC account? [yes/no]*

g. Enter or copy-paste the 12-digit AWS account number that you noted in step 1 when asked *What is the Transit VPC account number?*

An IAM Trust Relationship is established between the two AWS accounts and an ExternalID is generated by the script.

When the script runs successfully, the IAM profile and a role for PCG is created in your AWS master account. The values are saved in the output file in the same directory where you ran the script. The filename is `aws_details.txt`. Next, follow instructions at Add your AWS Account in CSM and then Link to a Transit VPC or VNet to finish the process of linking to a Transit VPC.

**Add your AWS Account in CSM**

Add your AWS account using values generated by the script.

**Procedure**

1. Log in to CSM using the Enterprise Administrator role.

2. Go to CSM > Clouds > AWS.

3. Click *Add* and enter the following details using the output file `aws_details.txt` generated from the NSX Cloud script:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name for this AWS Account</td>
</tr>
<tr>
<td>Access Key</td>
<td>Enter your account's Access Key</td>
</tr>
<tr>
<td>Secret Key</td>
<td>Enter your account's Secret Key</td>
</tr>
<tr>
<td>Cloud Tags</td>
<td>By default this option is enabled and allows your AWS tags to be visible in NSX Manager</td>
</tr>
<tr>
<td>Gateway Role Name</td>
<td>The default value is <code>nsx_pcg_service</code>. You can find this value in the output of the script in the file <code>aws_details.txt</code>.</td>
</tr>
</tbody>
</table>

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.

**What to do next**

Deploy PCG in a Self-Managed or Transit VPC
Deploy or Link NSX Public Cloud Gateway(s)

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.

The PCG can either be a standalone gateway appliance or shared between your public cloud VPCs or VNets to achieve a hub and spoke topology.

Figure 9-2. NSX Public Cloud Gateway Architecture

Transit or Self-managed VPC or 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. This VPC or VNet also qualifies as a Transit VPC or VNet because you can use the PCG deployed on it to onboard VMs hosted in other VPCs or VNets. The PCG utilizes the following subnets that you set up in your VPC/VNet. See Connect your Microsoft Azure Network with your On-prem NSX-T Data Center Deployment or Connect your Amazon Web Services (AWS) Network with your On-prem NSX-T Data Center Deployment.

- 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.

**Compute VPC or VNet**: VPCs or VNets that do not have the PCG deployed on them but link to a Transit VPC or VNet are called *Compute* VPCs or VNets.

PCG deployment aligns with your network addressing plan with FQDNs for the NSX-T Data Center components and a DNS server that can resolve these FQDNs.

**Note**: It is not recommended to use IP addresses for connecting the public cloud with NSX-T Data Center using PCG, but if you choose that option, do not change your IP addresses.

### Deploy PCG in a Self-Managed or Transit VNet

Follow these instructions to deploy PCG in your Microsoft Azure VNet.

The VNet in which you deploy a PCG can act as a Transit VNet to which other VNets can connect (known as Compute VNets). This VNet can also manage VMs and act as a self-managed VNet.

Follow these instructions to deploy a PCG. If you want to link to an existing Transit VNet, see [Link to a Transit VPC or VNet](#).

**Prerequisites**

- Your public cloud accounts must be already added into CSM.
- The VNet on which you are deploying PCG must have the required subnets appropriately adjusted for High Availability: *uplink*, *downlink*, and *management*.

**Procedure**

1. Log in to CSM using an account with the Enterprise Administrator role.

2. Click **Clouds > Azure** and go to the **VNets** tab.

3. Click a VNet where you want to deploy PCG.

4. Click **Deploy Gateways**. The **Deploy Primary Gateway** wizard opens.

5. For General Properties, use the following guidelines:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSH Public Key</strong></td>
<td>Provide an SSH public key that can be validated while deploying PCG. This is required for each PCG deployment.</td>
</tr>
<tr>
<td><strong>Quarantine Policy on the Associated VNet</strong></td>
<td>Leave this in the default <code>disabled</code> mode when you first deploy PCG. You can change this value after onboarding VMs. See <a href="#">Manage Quarantine Policy</a> in the <em>NSX-T Data Center Administration Guide</em> for details.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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.                                                                                                      |
| Advanced                       | The advanced DNS settings provide flexibility in selecting DNS servers for resolving NSX-T Data Center management components.                                                                                                                                                                                                                                                                                       |
| Obtain via Public Cloud Provider's DHCP | Select this option if you want to use Microsoft Azure DNS settings. This is the default DNS setting if you do not pick either of the options to override it.                                                                                                                                                                                                                                                                                  |
| Override Public Cloud Provider's DNS Server | Select this option if you want to manually provide the IP address of one or more DNS servers to resolve NSX-T Data Center appliances as well as the workload VMs in this VNet.                                                                                                                                                                                                                                                                               |
| Use Public Cloud Provider's DNS server only for NSX-T Data Center Appliances | Select this option if you want to use the Microsoft Azure DNS server for resolving the NSX-T Data Center management components. With this setting, you can use two DNS servers: one for PCG that resolves NSX-T Data Center appliances; the other for the VNet that resolves your workload VMs in this VNet.                                                                 |

6 Click **Next**.

7 For **Subnets**, use the following guidelines:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable HA for NSX Cloud Gateway</td>
<td>Select this option to enable High Availability.</td>
</tr>
<tr>
<td>Subnets</td>
<td>Select this option to enable High Availability.</td>
</tr>
<tr>
<td>Public IP on Mgmt NIC</td>
<td>Select <strong>Allocate New IP address</strong> 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.</td>
</tr>
<tr>
<td>Public IP on Uplink NIC</td>
<td>Select <strong>Allocate New IP address</strong> 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.</td>
</tr>
</tbody>
</table>

**What to do next**

Onboard your workload VMs. See **Onboarding and Managing Workload VMs** in the *NSX-T Data Center Administration Guide* for the Day-N workflow.
Deploy PCG in a Self-Managed or Transit VPC

Follow these instructions to deploy PCG in your AWS VPC.

The VPC in which you deploy a PCG can act as a Transit VPC to which other VPCs can connect (known as Compute VPCs). This VPC can also manage VMs and act as a self-managed VPC.

Follow these instructions to deploy a PCG. If you want to link to an existing Transit VPC, see Link to a Transit VPC or VNet.

Prerequisites

- Your public cloud accounts must be already added into CSM.
- The VPC on which you are deploying PCG must have the required subnets appropriately adjusted for High Availability: uplink, downlink, and management.
- The configuration for your VPC's network ACL must include an ALLOW inbound rule.

Procedure

1. Log in to CSM using an account with the Enterprise Administrator role.
2. Click Clouds > AWS > <AWS_account_name> and go to the VPCs tab.
3. In the VPCs tab, select an AWS region name, for example, us-west. The AWS region must be the same where you created the compute VPC.
4. Select a compute VPC configured for NSX Cloud.
5. Click Deploy Gateways.
6. Complete the general gateway details:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEM File</td>
<td>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.</td>
</tr>
<tr>
<td>Quarantine Policy on the Associated VPC</td>
<td>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.</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>Advanced</td>
<td>The advanced settings provide extra options if required.</td>
</tr>
<tr>
<td>Override AMI ID</td>
<td>Use this advanced feature to provide a different AMI ID for the PCG from the one that is available in your AWS account.</td>
</tr>
<tr>
<td>Obtain via Public Cloud Provider's DHCP</td>
<td>Select this option if you want to use AWS settings. This is the default DNS setting if you do not pick either of the options to override it.</td>
</tr>
</tbody>
</table>
Override Public Cloud Provider’s DNS Server
Select this option if you want to manually provide the IP address of one or more DNS servers to resolve NSX-T Data Center appliances as well as the workload VMs in this VPC.

Use Public Cloud Provider’s DNS server only for NSX-T Data Center Appliances
Select this option if you want to use the AWS DNS server for resolving the NSX-T Data Center management components. With this setting, you can use two DNS servers: one for PCG that resolves NSX-T Data Center appliances; the other for the VPC that resolves your workload VMs in this VPC.

7 Click **Next**.

8 Complete the Subnet details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable HA for Public Cloud Gateway</td>
<td>The recommended setting is Enable, that sets up a High Availability Active/Standby pair to avoid an unscheduled downtime.</td>
</tr>
<tr>
<td>Primary gateway settings</td>
<td>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.</td>
</tr>
<tr>
<td>Secondary gateway settings</td>
<td>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.</td>
</tr>
<tr>
<td>Public IP on Mgmt NIC</td>
<td>Select <strong>Allocate New IP address</strong> 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.</td>
</tr>
<tr>
<td>Public IP on Uplink NIC</td>
<td>Select <strong>Allocate New IP address</strong> 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.</td>
</tr>
</tbody>
</table>

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**

Onboard your workload VMs. See **Onboarding and Managing Workload VMs** in the **NSX-T Data Center Administration Guide** for the Day-N workflow.

**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 in the Up state.
- Verify that the VPC/VNet you want to link is connected to the Transit VPC or VNet through VPN or peering.
- Verify that the Transit VPC/VNet in the same region as the Compute 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 or 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Transit VPC or VNet   | Select a Transit VPC or VNet from the dropdown menu. The Transit VPC or VNet you select must be already linked with this VPC by way of VPN or peering.  
**Note** If connecting to Transit VNet, you must have a DNS forwarder configured in that VNet. See Microsoft Azure documentation for more information. |
| 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. |

**What to do next**

Onboard your workload VMs. See Onboarding and Managing Workload VMs in the NSX-T Data Center Administration Guide for the Day-N workflow.

**Auto-Created Logical Entities and Cloud-native Security Groups**

The deployment of PCG in a Transit VPC/VNet and linking a compute VPC/VNet to it triggers necessary configurations in NSX-T Data Center and the public cloud.
Auto-created NSX-T Logical Entities

In the NSX-T Data Center, a set of logical entities are created.

**Important**  Do not delete any of these auto-created entities.

**System Entities**

You can see the following entities under **System**:

**Table 9-3. Auto-Created System Entities**

<table>
<thead>
<tr>
<th>Logical System Entity</th>
<th>How many are created?</th>
<th>Nomenclature</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport Zones</td>
<td>Two Transport Zones are created for each Transit VPC/VNet</td>
<td>TZ-&lt;VPC/VNet-ID&gt;-OVERLAY&lt;br&gt;TZ-&lt;VPC/VNet-ID&gt;-VLAN</td>
<td>Scope: Global</td>
</tr>
<tr>
<td>Edge Transport Nodes</td>
<td>One Edge Transport Node is created for each deployed PCG, two if deployed in high availability mode.</td>
<td>PublicCloudGatewayTNN-&lt;VPC/VNET-ID&gt;&lt;br&gt;PublicCloudGatewayTNN-&lt;VPC/VNET-ID&gt;-preferred</td>
<td>Scope: Global</td>
</tr>
<tr>
<td>Edge Cluster</td>
<td>One Edge Cluster is created per deployed PCG, whether one or in a high availability pair.</td>
<td>PCG-cluster-&lt;VPC/VNet-ID&gt;</td>
<td>Scope: Global</td>
</tr>
</tbody>
</table>

**Inventory Entities**

The following entities are created under **Inventory**:
### Table 9-4. Auto-Created Inventory Entities

<table>
<thead>
<tr>
<th>Logical Inventory Entity</th>
<th>How many are created?</th>
<th>Nomenclature</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>One per Transit VPC/VNet</td>
<td>cloud-&lt;Transit VPC/VNet-ID&gt;</td>
<td>Scope: shared across all PCGs.</td>
</tr>
<tr>
<td><strong>Note</strong> The Domain object is an experimental feature in NSX-T Data Center 2.4 and the auto-created Domains are visible in the user interface. However, Domains are no longer visible in the NSX-T Data Center 2.4.1 user interface.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Groups</td>
<td>Two Groups under the default Domain</td>
<td>cloud-default-route, cloud-metadata services</td>
<td>Scope: Shared across all PCGs</td>
</tr>
<tr>
<td><strong>Note</strong> In NSX-T Data Center you can see the default Domain. However, in NSX-T Data Center 2.4.1, the Domain object is not visible.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Groups</td>
<td>One Group created at Transit VPC/VNet level as a parent group for individual segments created at the Compute VPC/VNet level.</td>
<td>cloud-&lt;Transit VPC/VNet ID&gt;-all-segments</td>
<td>Scope: shared across all Compute VPCs/VNets</td>
</tr>
<tr>
<td>Groups</td>
<td>Two Groups:</td>
<td></td>
<td>Scope: shared across all Compute VPCs/VNets</td>
</tr>
<tr>
<td>Network CIDR Group for all CIDRs of the Compute VPC/VNet</td>
<td>cloud-&lt;Compute VPC/VNet ID&gt;-cidr</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Segment Group for all managed segments within the Compute VPC/VNet</td>
<td>cloud-&lt;Compute VPC/VNet ID&gt;-local-segments</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Security Entities

### Table 9-5. Auto-Created Security Entities

<table>
<thead>
<tr>
<th>Logical Security Entity</th>
<th>How many are created?</th>
<th>Nomenclature</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed Firewall (East-West)</td>
<td>Two per Transit VPC/VNet:</td>
<td>cloud-stateless-&lt;VPC/VNet ID&gt;, cloud-stateful-&lt;VPC/VNet ID&gt;</td>
<td>Stateful rule to allow traffic within local managed segments, Stateful rule to reject traffic from unmanaged VMs</td>
</tr>
<tr>
<td></td>
<td>Stateless</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stateful</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gateway Firewall (North-South)</td>
<td>One per Transit VPC/VNet</td>
<td>cloud-&lt;Transit VPC/VNet ID&gt;</td>
<td></td>
</tr>
</tbody>
</table>
Networking Entities

The following entities are created at different stages of onboarding:

**Figure 9-3. Auto-created NSX-T Data Center Networking Entities After PCG is Deployed**

<table>
<thead>
<tr>
<th>NSX-T Data Center</th>
<th>Public Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Tier 0 Gateway created when PCG is deployed in the Transit VPC/VNet</td>
<td></td>
</tr>
<tr>
<td>Transit VPC/VNet</td>
<td></td>
</tr>
<tr>
<td>One Tier 1 Gateway created for a self-managed Transit VPC/VNet and for each compute VPC/VNet linked to Transit</td>
<td></td>
</tr>
<tr>
<td>Transit VPC/VNet</td>
<td></td>
</tr>
<tr>
<td>One Segment created for the subnet in the VPC/VNet in which a workload VM is tagged with nsx.network=default</td>
<td></td>
</tr>
<tr>
<td>Subnet 1</td>
<td></td>
</tr>
<tr>
<td>Subnet 2</td>
<td></td>
</tr>
<tr>
<td>One Segment Port created each time a workload VM is onboarded in the same subnet in the VPC/VNet</td>
<td></td>
</tr>
<tr>
<td>VM1</td>
<td></td>
</tr>
<tr>
<td>VM2</td>
<td></td>
</tr>
<tr>
<td>VM3</td>
<td></td>
</tr>
</tbody>
</table>

**Table 9-6. Auto-Created Networking Entities**

<table>
<thead>
<tr>
<th>Onboarding Task</th>
<th>Logical Entities Created in NSX-T Data Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCG deployed on Transit VPC/VNet</td>
<td>Tier-0 Gateway, Infra Segment (Default VLAN switch), Tier-1 router</td>
</tr>
<tr>
<td>Compute VPC or VNet linked to the Transit VPC/VNet</td>
<td>Tier-1 router</td>
</tr>
<tr>
<td>A workload VM with the NSX agent installed on it is tagged with the &quot;nsx.network:default&quot; key:value in a subnet of a compute or self-managed VPC/VNet</td>
<td>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</td>
</tr>
<tr>
<td>More workload VMs are tagged in the same subnet of the Compute or self-managed VPC/VNet</td>
<td>Hybrid ports are created for each tagged workload VM that has the NSX agent installed on it</td>
</tr>
</tbody>
</table>

Forwarding Policies
The following three forwarding rules are set up for a Compute VPC/VNet, including Self-managed Transit VPC/VNet:

- Access any CIDR of the same Compute VPC over the public cloud's network (underlay)
- Route traffic pertaining to public cloud metadata services over the public cloud's network (underlay)
- Route everything not in the Compute VPC/VNet's CIDR block, or a known service, through the NSX-T Data Center network (overlay)

Auto-created cloud-native SGs

In your public clouds, cloud-native security groups are created.

Public Cloud Configurations

In 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.

In AWS and Microsoft Azure:

The gw security groups are applied to the respective PCG interfaces.

**Table 9-7. Public Cloud Security Groups created by NSX Cloud for PCG interfaces**

<table>
<thead>
<tr>
<th>Security Group name</th>
<th>Available in Microsoft Azure?</th>
<th>Available in AWS?</th>
<th>Full Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>gw-mgmt-sg</td>
<td>Yes</td>
<td>Yes</td>
<td>Gateway Management Security Group</td>
</tr>
<tr>
<td>gw-uplink-sg</td>
<td>Yes</td>
<td>Yes</td>
<td>Gateway Uplink Security Group</td>
</tr>
<tr>
<td>gw-vtep-sg</td>
<td>Yes</td>
<td>Yes</td>
<td>Gateway Downlink Security Group</td>
</tr>
</tbody>
</table>
### Public Cloud Security Groups created by NSX Cloud for Workload VMs

<table>
<thead>
<tr>
<th>Security Group name</th>
<th>Available in Microsoft Azure?</th>
<th>Available in AWS?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>quarantine</td>
<td>Yes</td>
<td>No</td>
<td>Quarantine security group for Microsoft Azure</td>
</tr>
<tr>
<td>default</td>
<td>No</td>
<td>Yes</td>
<td>Quarantine security group for AWS</td>
</tr>
<tr>
<td>vm-underlay-sg</td>
<td>Yes</td>
<td>Yes</td>
<td>VM Non-Overlay security group</td>
</tr>
<tr>
<td>vm-override-sg</td>
<td>Yes</td>
<td>Yes</td>
<td>VM Override Security Group</td>
</tr>
<tr>
<td>vm-overlay-sg</td>
<td>Yes</td>
<td>Yes</td>
<td>VM Overlay security group (this is not used in the current release)</td>
</tr>
<tr>
<td>vm-outbound-bypass-sg</td>
<td>Yes</td>
<td>Yes</td>
<td>VM Outbound Bypass Security Group (this is not used in the current release)</td>
</tr>
<tr>
<td>vm-inbound-bypass-sg</td>
<td>Yes</td>
<td>Yes</td>
<td>VM Inbound Bypass Security Group (this is not used in the current release)</td>
</tr>
</tbody>
</table>

### Undeploy PCG

Refer to this flowchart for the steps involved in undeploying PCG.

Before undeploying PCG, you must do the following:

- Make sure that no workload VMs in the VPC or VNet are NSX-managed.
- Disable the Quarantine Policy.
- Delete all user-created logical entities associated with the PCG.

**Figure 9-4. Undeploying PCG**

1. **Untag VMs in the Public Cloud**
   Before you can undeploy PCG, all VMs must be unmanaged.

2. **Disable Quarantine Policy, if Enabled**
   If previously enabled, Quarantine Policy must be disabled to undeploy PCG.

3. **Delete User-created Logical Entities**
   All user-created logical entities associated with the PCG must be deleted.

4. **Undeploy from CSM**
   To undeploy PCG after completing the prerequisites, click **Undeploy Gateway** from **Clouds > <Public_Cloud> > <VNet/VPC>** in CSM.

**Untag VMs in the Public Cloud**

Before you can undeploy PCG, all VMs must be unmanaged.

Go to the VPC or VNet in your public cloud and remove the `nsx.network` tag from the managed VMs.
Disable Quarantine Policy, if Enabled

If previously enabled, Quarantine Policy must be disabled to undeploy PCG.

With Quarantine Policy enabled, your VMs are assigned security groups defined by NSX Cloud. When you undeploy PCG, you need to disable Quarantine Policy and specify a fallback security group that the VMs can be assigned to when they are removed from the NSX Cloud security groups.

**Note**  The fallback security group must be an existing user-defined security group in your public cloud. You cannot use any of the NSX Cloud security groups as a fallback security group. See Auto-Created Logical Entities and Cloud-native Security Groups for a list of NSX Cloud security groups.

Disable Quarantine Policy for the VPC or VNet from which you are undeploying PCG:

- Go to the VPC or VNet in CSM.
- From **Actions > Edit Configurations >**, turn off the setting for **Default Quarantine**.
- Enter a value for a fallback security group that VMs will be assigned.

- All VMs that are unmanaged or quarantined in this VPC or VNet will get the fallback security group assigned to them.
- If all VMs are unmanaged, they get assigned to the fallback security group.
- 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` tag from such VMs to take them out from NSX management, they are also assigned the fallback security group.

**Note**  See Managing Quarantine Policy in the NSX-T Data Center Administration Guide for instructions and more information on the effects of enabling and disabling the Quarantine Policy.
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 Gateway** from CSM. See **Auto-Created Logical Entities and Cloud-native Security Groups** for the list of auto-created logical entities.

**Undeploy from CSM**

To undeploy PCG after completing the prerequisites, click **Undeploy Gateway** from **Clouds > <Public_Cloud> > <VNet/VPC>** in CSM.

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 Gateway**.

The default entities created by NSX Cloud are removed automatically when a PCG is undeployed.
You can remove elements of an NSX-T Data Center overlay, remove a hypervisor host from NSX-T Data Center, or uninstall NSX-T Data Center completely.

This chapter includes the following topics:

- Unconfigure an NSX-T Data Center Overlay
- Remove a Host From NSX-T Data Center or Uninstall NSX-T Data Center Completely

### Unconfigure an NSX-T Data Center Overlay

If you want to delete an overlay but keep your transport nodes in place, follow these steps.

**Procedure**

1. Log in to the vSphere Client.
2. In your VM management tool, detach all VMs from any logical switches and connect the VMs to non-NSX-T Data Center networks.
3. For KVM hosts, SSH to the hosts and power off the VMs.
   ```
   shutdown -h now
   ```
4. In the NSX Manager UI or API, delete all logical routers.
5. In the NSX Manager UI or API, delete all logical switch ports and then all logical switches.
6. In the NSX Manager UI or API, delete all NSX Edges and then all NSX Edge clusters.
7. Configure a new NSX-T Data Center overlay, as needed.

### Remove a Host From NSX-T Data Center or Uninstall NSX-T Data Center Completely

If you want to uninstall NSX-T Data Center completely or just remove a hypervisor host from NSX-T Data Center so that the host can no longer take part in the NSX-T Data Center overlay, follow these steps.

The following procedure describes how to perform a clean uninstall of NSX-T Data Center.
Prerequisites

If the VM management tool is vCenter Server, put the vSphere host in maintenance mode.

Procedure

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

2. In the NSX Manager, select **System > Fabric > Nodes > Host Transport Nodes** and click **Delete Host**.

   Make sure **Uninstall NSX Components** is checked. This causes the NSX-T Data Center modules to be uninstalled on the host. It might take up to 5 minutes for all NSX-T Data Center modules to be removed.

   Note that using the **Uninstall NSX Components** option unchecked is not meant to be used to unregister a host. It is only meant as a workaround for hosts that are in a bad state.

   Deleting the transport node causes the N-VDS to be removed from the host. You can confirm this by running the following command.

   ```bash
   [root@host:] esxcli network vswitch dvs vmware list
   ```

   On KVM, the command is:

   ```bash
   ovs-vsctl show
   ```

3. For hosts managed by a compute manager, select **System > Fabric > Nodes > Host Transport Nodes**.
   
   a. Select host transport node and detach the node from the cluster.
   
   b. Detach the host transport node from the cluster.

4. Use CLI for removing NSX-T Data Center from vSphere host.
   
   a. Get the NSX Manager thumbprint.

      ```bash
      manager> get certificate api thumbprint
      ```

   b. On the host's NSX-T Data Center CLI, run the following command to detach the host from the management plane.

      ```bash
      host> nsxcli detach management-plane <MANAGER> username <ADMIN-USER> \ password <ADMIN-PASSWORD> thumbprint <MANAGER-THUMBPRINT>
      ```

   c. On the host, run the following command to remove filters.

      ```bash
      [root@host:] vsipioctl clearallfilters
      ```
d  On the host, run the following command to stop netcpa.

    [root@host:-] /etc/init.d/netcpad stop

e  Power off the VMs on the host or migrate them to another host.

f  On the host, run the following command to manually uninstall the NSX-T Data Center configuration and modules. This command is supported on all host types.

    [root@host:-] del nsx

    This command removes all transport and fabric node configurations and all NSX-T Data Center packages without affecting third-party packages on the host.

What to do next

After making this change, the host is removed from the management plane and can no longer take part in the NSX-T Data Center overlay.

If you are removing NSX-T Data Center completely, in your VM management tool, shut down NSX Manager, NSX Controllers, and NSX Edges and delete them from the disk.