

NSX Installation and Upgrade Guide

NSX 6.1 for vSphere

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see <http://www.vmware.com/support/pubs>.

EN-001544-00

vmware[®]

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

<http://www.vmware.com/support/>

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

Copyright © 2010 – 2014 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

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

Contents

About this Book	5
1 Overview of NSX	7
NSX Components	8
NSX Services	10
2 Preparing for Installation	13
System Requirements for NSX	13
Ports Required for NSX Communication	14
About VMware Tools on NSX Components	14
3 Installing the NSX Manager	15
Obtain the NSX Manager OVA File	15
Install the NSX Manager Virtual Appliance	16
Log In to the NSX Manager Virtual Appliance	17
Register vCenter Server with NSX Manager	17
4 Installing NSX Components	19
Install and Assign NSX for vSphere License	19
Set Up the Control Plane	20
Prepare Clusters for Network Virtualization	21
Configure VXLAN Transport Parameters	21
Assign Segment ID Pool and Multicast Address Range to NSX Manager	23
Prepare New Hosts and Clusters to Work with NSX	23
Install NSX Edge	24
Install Guest Introspection	32
Install Data Security	34
5 Deploy a Partner Service	37
6 Upgrading NSX	39
Upgrade vShield 5.5 to NSX 6.1	39
Upgrade NSX 6.0.x to NSX 6.1	44
Upgrade NSX 6.1 to NSX 6.1.1	48
7 Uninstalling NSX Components	53
Uninstall an NSX Edge	53
Uninstall an NSX Data Security Virtual Machine	53
Uninstall a Guest Introspection Module	54
Uninstall Network Virtualization Components	54

8	Troubleshooting Installation Issues	55
	Unable to Configure Lookup Service	55
	Unable to Configure vCenter Server	55
	Index	57

About this Book

This manual, the *NSX Installation and Upgrade Guide*, describes how to install and upgrade the VMware® NSX™ system by using the vSphere Web Client. The information includes step-by-step configuration instructions, and suggested best practices.

Intended Audience

This manual is intended for anyone who wants to install or use NSX in a VMware vCenter environment. The information in this manual is written for experienced system administrators who are familiar with virtual machine technology and virtual datacenter operations. This manual assumes familiarity with VMware Infrastructure 5.x, including VMware ESX, vCenter Server, and the vSphere Web Client.

VMware 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>.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

Technical Support and Education Resources

The following technical support resources are available to you. To access the current version of this book and other books, go to <http://www.vmware.com/support/pubs>.

Online and Telephone Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to <http://www.vmware.com/support>.

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to http://www.vmware.com/support/phone_support.html.

Support Offerings

To find out how VMware support offerings can help meet your business needs, go to <http://www.vmware.com/support/services>.

VMware Professional Services

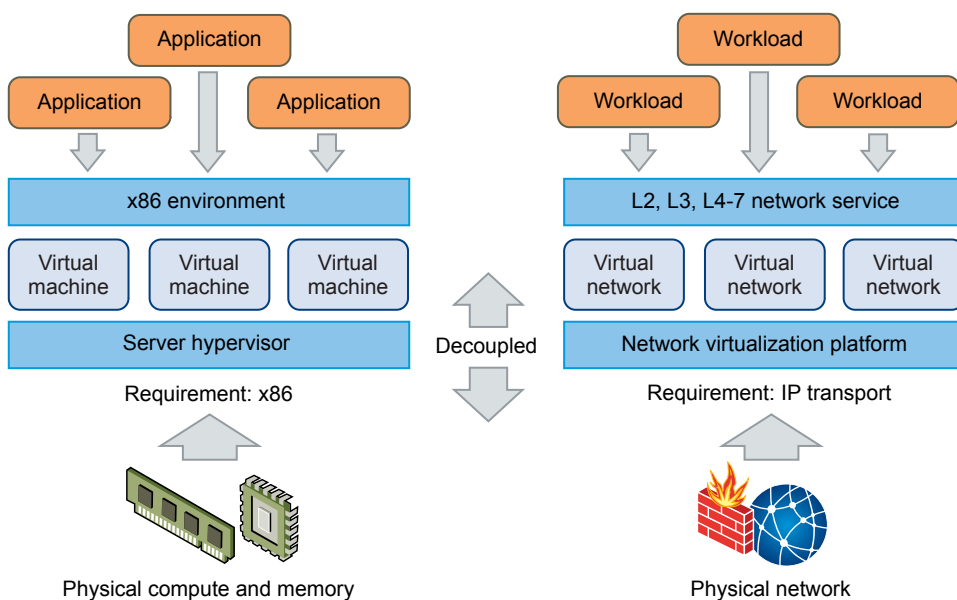
VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices,

VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to <http://www.vmware.com/services>.

Overview of NSX

IT organizations have gained significant benefits as a direct result of server virtualization. Server consolidation reduced physical complexity, increased operational efficiency and the ability to dynamically re-purpose underlying resources to quickly and optimally meet the needs of increasingly dynamic business applications.

VMware's Software Defined Data Center (SDDC) architecture is now extending virtualization technologies across the entire physical data center infrastructure. VMware NSX[®], the network virtualization platform, is a key product in the SDDC architecture. With NSX, virtualization delivers for networking what it has already delivered for compute and storage. In much the same way that server virtualization programmatically creates, snapshots, deletes and restores software-based virtual machines (VMs), NSX network virtualization programmatically creates, snapshots, deletes, and restores software-based virtual networks. The result is a completely transformative approach to networking that not only enables data center managers to achieve orders of magnitude better agility and economics, but also allows for a vastly simplified operational model for the underlying physical network. With the ability to be deployed on any IP network, including both existing traditional networking models and next-generation fabric architectures from any vendor, NSX is a completely non-disruptive solution. In fact, with NSX, the physical network infrastructure you already have is all you need to deploy a software-defined data center.



The figure above draws an analogy between compute and network virtualization. With server virtualization, a software abstraction layer (server hypervisor) reproduces the familiar attributes of an x86 physical server (for example, CPU, RAM, Disk, NIC) in software, allowing them to be programmatically assembled in any arbitrary combination to produce a unique VM in a matter of seconds.

With network virtualization, the functional equivalent of a network hypervisor reproduces the complete set of Layer 2 through Layer 7 networking services (for example, switching, routing, access control, firewalling, QoS, and load balancing) 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.

With network virtualization, benefits similar to server virtualization are derived. For example, just as VMs are independent of the underlying x86 platform and allow IT to treat physical hosts as a pool of compute capacity, virtual networks are independent of the underlying IP network hardware and allow IT to treat the physical network as a pool of transport capacity that can be consumed and repurposed on demand. Unlike legacy architectures, virtual networks can be provisioned, changed, stored, deleted, and restored programmatically without reconfiguring the underlying physical hardware or topology. By matching the capabilities and benefits derived from familiar server and storage virtualization solutions, this transformative approach to networking unleashes the full potential of the software-defined data center.

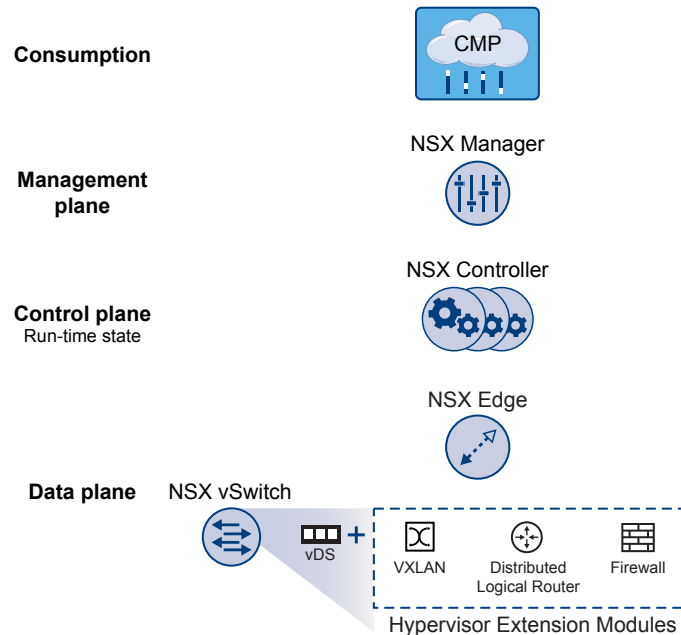
NSX can be configured through the vSphere Web Client, a command-line interface (CLI), and a REST API.

This chapter includes the following topics:

- [“NSX Components,”](#) on page 8
- [“NSX Services,”](#) on page 10

NSX Components

This section describes the components of the NSX solution.



Data Plane

The NSX Data plane consists of the NSX vSwitch, which is based on the vSphere Distributed Switch (VDS) with additional components to enable services. Kernel modules (VIBs) run within the hypervisor kernel to provide services such as distributed routing and logical firewall and to enable VXLAN bridging capabilities.

The NSX vSwitch (vDS-based) abstracts the physical network and provides access-level switching in the hypervisor. It is central to network virtualization because it enables logical networks that are independent of physical constructs, such as VLANs. Some of the benefits of the vSwitch are:

- Support for overlay networking with protocols (such as VXLAN) and centralized network configuration. Overlay networking enables the following capabilities:
 - Creation of a flexible logical Layer 2 (L2) overlay over existing IP networks on existing physical infrastructure without the need to re-architect any of the data center networks
 - Provision of communication (east–west and north–south), while maintaining isolation between tenants
 - Application workloads and virtual machines that are agnostic of the overlay network and operate as if they were connected to a physical L2 network
- Facilitates massive scale of hypervisors
- Multiple features—such as Port Mirroring, NetFlow/IPFIX, Configuration Backup and Restore, Network Health Check, QoS, and LACP—provide a comprehensive toolkit for traffic management, monitoring, and troubleshooting within a virtual network

Additionally, the data plane consists of gateway devices that can provide L2 bridging from the logical networking space (VXLAN) to the physical network (VLAN). The gateway device is typically an NSX Edge virtual appliance. NSX Edge offers L2, L3, perimeter firewall, load balancing, and other services such as SSL VPN and DHCP.

Control Plane

The NSX control plane runs in the NSX controller. NSX controller is an advanced distributed state management system that controls virtual networks and overlay transport tunnels. It is the central control point for all logical switches within a network and maintains information about all virtual machines, hosts, logical switches, and VXLANs.

The controller does not have any dataplane traffic passing through it. Controller nodes are deployed in a cluster of odd-numbered members to enable high-availability and scale. Any failure of the controller nodes does not impact any data-plane traffic.

Management Plane

The NSX management plane is built by the NSX Manager, the centralized network management component of NSX. It provides the single point of configuration and REST API entry-points.

The NSX Manager is installed as a virtual appliance on any ESX™ host in your vCenter Server environment.

Consumption Platform

The consumption of NSX can be driven directly through the NSX Manager user interface. In a vSphere environment, this is available in the vSphere Web Client. Typically end users tie network virtualization to their cloud management platform for deploying applications. NSX provides rich integration into virtually any CMP through REST APIs. Out-of-the-box integration is also available through VMware vCloud Automation Center, vCloud Director, and OpenStack with the Neutron plug-in for NSX.

NSX Services

The NSX components work together to provide the following functional services.

Logical Switches

A cloud deployment or a virtual data center has a variety of applications across multiple tenants. These applications and tenants require isolation from each other for security, fault isolation, and non-overlapping IP addresses. The NSX logical switch creates logical broadcast domains or segments to which an application or tenant virtual machine can be logically wired. This allows for flexibility and speed of deployment while still providing all the characteristics of a physical network's broadcast domains (VLANs) without physical Layer 2 sprawl or spanning tree issues.

A logical switch is distributed and can span arbitrarily large compute clusters. This allows for virtual machine mobility (vMotion) within the data center without limitations of the physical Layer 2 (VLAN) boundary. The physical infrastructure is not constrained by MAC/FIB table limits, because the logical switch contains the broadcast domain in software.

Logical Routers

Dynamic routing provides the necessary forwarding information between Layer 2 broadcast domains, thereby allowing you to decrease the size of Layer 2 broadcast domains and improve network efficiency and scale. NSX extends this intelligence to where the workloads reside for East-West routing. This allows more direct VM-to-VM communication without the costly or timely need to extend hops. At the same time, NSX logical routers provide North-South connectivity, thereby enabling tenants to access public networks.

Logical Firewall

Logical Firewall provides security mechanisms for dynamic virtual data centers. The Distributed Firewall component of Logical Firewall allows you to segment virtual datacenter entities like virtual machines based on VM names and attributes, user identity, vCenter objects like datacenters, and hosts, as well as traditional networking attributes like IP addresses, VLANs, and so on. The Edge Firewall component helps you meet key perimeter security requirements, such as building DMZs based on IP/VLAN constructs, tenant-to-tenant isolation in multi-tenant virtual data centers, Network Address Translation (NAT), partner (extranet) VPNs, and user-based SSL VPNs.

The Flow Monitoring feature displays network activity between virtual machines at the application protocol level. You can use this information to audit network traffic, define and refine firewall policies, and identify threats to your network.

Logical Virtual Private Networks (VPN)s

SSL VPN-Plus allows remote users to access private corporate applications. IPSec VPN offers site-to-site connectivity between an NSX Edge instance and remote sites. L2 VPN allows you to extend your datacenter by allowing virtual machines to retain network connectivity across geographical boundaries.

Logical Load Balancer

The NSX Edge load balancer enables network traffic to follow multiple paths to a specific destination. It distributes incoming service requests evenly among multiple servers in such a way that the load distribution is transparent to users. Load balancing thus helps in achieving optimal resource utilization, maximizing throughput, minimizing response time, and avoiding overload. NSX Edge provides load balancing up to Layer 7.

Service Composer

Service Composer helps you provision and assign network and security services to applications in a virtual infrastructure. You map these services to a security group, and the services are applied to the virtual machines in the security group.

Data Security provides visibility into sensitive data stored within your organization's virtualized and cloud environments. Based on the violations reported by NSX Data Security, you can ensure that sensitive data is adequately protected and assess compliance with regulations around the world.

NSX Extensibility

VMware partners can integrate their solutions with the NSX platform, thus enabling customers to have an integrated experience across VMware products and partner solutions. Data center operators can provision complex, multi-tier virtual networks in seconds, independent of the underlying network topology or components.

Preparing for Installation

This section describes the system requirements for NSX as well as the ports that must be open.

This chapter includes the following topics:

- [“System Requirements for NSX,”](#) on page 13
- [“Ports Required for NSX Communication,”](#) on page 14
- [“About VMware Tools on NSX Components,”](#) on page 14

System Requirements for NSX

Before you install NSX in your vCenter Server environment, consider your network configuration and resources. You can install one NSX Manager per vCenter Server, one Guest Introspection per ESX™ host, and multiple NSX Edge instances per datacenter.

Hardware

Table 2-1. Hardware Requirements

Component	Minimum
Memory	<ul style="list-style-type: none"> ■ NSX Manager: 12 GB ■ NSX Controller: 4 GB ■ NSX Edge Compact: 512 MB, Large: 1 GB, Quad Large: 1 GB, and X-Large: 8 GB ■ Guest Introspection: 1 GB ■ NSX Data Security: 512 MB
Disk Space	<ul style="list-style-type: none"> ■ NSX Manager: 60 GB ■ NSX Controller: 20 GB ■ NSX Edge Compact, Large, and Quad Large: 512 MB, X-Large: 4.5 GB (with 4 GB swap) ■ Guest Introspection: 4GB ■ NSX Data Security: 6 GB per ESX host
vCPU	<ul style="list-style-type: none"> ■ NSX Manager: 4 ■ NSX Controller: 4 ■ NSX Edge Compact: 1, Large: 2, Quad Large: 4, and X-Large: 6 ■ Guest Introspection: 2 ■ NSX Data Security: 1

Software

For the latest interoperability information, see the Product Interoperability Matrix at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

These are the minimum required versions of VMware products.

- VMware vCenter Server 5.5 or later
- VMware ESXi 5.1 or later for each server
- VMware Tools

For Guest Introspection and NSX Data Security, you must upgrade your virtual machines to hardware version 7 or 8 and install VMware Tools 9.1.0 released with ESXi 5.1 Update 2. For more information, see [“Install VMware Tools on the Guest Virtual Machines,”](#) on page 34.

Client and User Access

- If you added ESX hosts by name to the vSphere inventory, ensure that forward and reverse name resolution is working. Otherwise, NSX Manager cannot resolve the IP addresses.
- Permissions to add and power on virtual machines
- Access to the datastore where you store virtual machine files, and the account permissions to copy files to that datastore
- Cookies enabled on your Web browser, to access the NSX Manager user interface
- From NSX Manager, port 443 accessible from the ESX host, the vCenter Server, and the NSX appliances to be deployed. This port is required to download the OVF file on the ESX host for deployment.
- One of the following Web browsers:
 - Microsoft Internet Explorer 8, 9 (64-bit only), and 10
 - Mozilla Firefox: the latest browser version, and the one previous version at the time NSX 6.1 is produced
 - Google Chrome: the latest browser version, and the one previous version at the time NSX 6.1 is produced.

Ports Required for NSX Communication

The following ports must be open on NSX Manager.

Table 2-2.

Port	Required for
443/TCP	<ul style="list-style-type: none"> ■ Downloading the OVA file on the ESX host for deployment ■ Using REST APIs ■ Using the NSX Manager user interface
80/TCP	<ul style="list-style-type: none"> ■ Initiating connection to the vSphere SDK ■ Messaging between NSX Manager and NSX host modules
1234/TCP	Communication between ESX Host and NSX Controller Clusters
5671	Rabbit MQ (messaging bus technology)
22/TCP	Console access (SSH) to CLI. By default, this port is closed.

About VMware Tools on NSX Components

Each NSX virtual appliance includes VMware Tools. Do not upgrade or uninstall the version of VMware Tools included with an NSX virtual appliance.

Installing the NSX Manager

The NSX Manager is the centralized management component of NSX and runs as a virtual appliance on an ESXi host.

VMware recommends that you install NSX Manager on a dedicated management cluster separate from the cluster(s) that NSX Manager manages. Each NSX Manager works with a single vCenter Server environment. The NSX Manager requires connectivity to the vCenter Server, ESXi host, and NSX Edge instances, NSX Guest Introspection module, and the NSX Data Security virtual machine. NSX components can communicate over routed connections and on different LANs.

The NSX Manager should be run on an ESX host that is not affected by down time, such as frequent reboots or maintenance-mode operations. You can use HA or DRS to increase the resilience of the NSX Manager. If the ESX host on which the NSX Manager resides is expected to require downtime, vMotion the NSX Manager virtual appliance to another ESX host. Thus, having more than one ESX host available for NSX Manager is recommended.

You should synchronize the time for all ESXi hosts in the NSX environment with NTP server(s) to ensure that:

- Timestamps in all logs are aligned correctly.
- Certificate-based authentication used by NSX control plane operates correctly.
- Kerberos-based authentication used by SSO is functional

For information on time synchronization, see [Edit Time Configuration for a Host in the vSphere Web Client](#).

This chapter includes the following topics:

- [“Obtain the NSX Manager OVA File,”](#) on page 15
- [“Install the NSX Manager Virtual Appliance,”](#) on page 16
- [“Log In to the NSX Manager Virtual Appliance,”](#) on page 17
- [“Register vCenter Server with NSX Manager,”](#) on page 17

Obtain the NSX Manager OVA File

The NSX Manager virtual machine is packaged as an Open Virtualization Appliance (OVA) file, which allows you to use the vSphere Web Client to import the NSX Manager into the datastore and virtual machine inventory.

Install the NSX Manager Virtual Appliance

You can install the NSX Manager virtual machine on an ESX host in a cluster configured with DRS.

You can install the NSX Manager in a different vCenter than the one that the NSX Manager will be interoperating with. A single NSX Manager serves a single vCenter Server environment.

The NSX Manager virtual machine installation includes VMware Tools. Do not attempt to upgrade or install VMware Tools on the NSX Manager.

Prerequisites

Required ports must be open. See [“Ports Required for NSX Communication,”](#) on page 14.

Procedure

- 1 Log in to the vSphere Web Client.
- 2 Select **vCenter** and then select **Hosts**.
The NSX Manager management interface, vCenter Server, and ESXi hosts must be reachable by all future NSX Edge and NSX Guest Introspection instances.
- 3 Right-click the host where you want to install NSX Manager and select **Deploy OVA Template**.
It may take a few seconds for the **Deploy OVA Template** option to be displayed.
- 4 Enter the URL to download and install the OVA file from the internet or click **Browse** to locate the folder on your computer that contains the NSX Manager OVA file and click **Next**.
- 5 Review the OVA template details and click **Next**.
- 6 Click **Accept** to accept the VMware license agreements and click **Next**.
- 7 Edit the name (if required) and select the location for the NSX Manager that you are installing.
- 8 Click **Next**.
- 9 Select the location to run the template.
- 10 On the Select storage page, select the storage for the NSX Manager and click **Next**.
- 11 On the Setup networks page, confirm that the NSX Manager adapter has been mapped to the correct host network and click **Next**.
- 12 Specify whether you want to configure IPv4 only, IPv6 only, or dual-stack network configuration.
If you are configuring a dual-stack network, the host name of the NSX Manager will be used by other entities. Hence, the NSX Manager host name must be mapped to the right IP address in the DNS servers used in that network.
- 13 On the Customized template page, specify the following values.
 - a Type and re-type the CLI password.
 - b Type and re-type the CLI privilege mode password.
 - c Click **Network Properties** and type the hostname for the NSX Manager virtual machine.
 - d Type the network IPv4 address, netmask, and default gateway.
 - e Type the network IPv6 address, prefix, and default gateway.
 - f Click **DNS** and type the IP addresses for DNS servers and domain search list.
 - g Click **Services Configuration** and type the NTP server list for the NSX Manager virtual machine.

- h To enable SSH, select the **Enable SSH** checkbox.
- i Click **Next**.
- 14 On the Ready to complete page, review the NSX Manager settings and click **Finish**.
The NSX Manager is installed as a virtual machine in your inventory.
- 15 Power on the NSX Manager virtual machine.

Log In to the NSX Manager Virtual Appliance

After you have installed and configured the NSX Manager virtual machine, log in to the NSX Manager virtual appliance to review the settings specified during installation.

Procedure

- 1 Open a Web browser window and type the IP address assigned to the NSX Manager. For example, **https://11.111.11.11**.

The NSX Manager user interface opens in a web browser window using SSL.

- 2 Accept the security certificate.

NOTE You can use an SSL certificate for authentication. Refer to the *NSX Administration Guide*.

The NSX Manager login screen appears.

- 3 Log in to the NSX Manager virtual appliance by using the user name **admin** and the password you set during installation.
- 4 Click **Log In**.

Register vCenter Server with NSX Manager

You must login to the NSX Manager virtual appliance to register a vCenter Server and review the settings specified during installation.

Prerequisites

- You must have a vCenter Server user account with administrative access to synchronize NSX Manager with the vCenter Server . If your vCenter password has non-Ascii characters, you must change it before synchronizing the NSX Manager with the vCenter Server.
- To use SSO on NSX Manager, you must have vCenter Server 5.5 or later and single sign on service must be installed on the vCenter Server.

Procedure

- 1 Log in to the NSX Manager virtual appliance.
- 2 Under Appliance Management, click **Manage Appliance Settings**.
- 3 From the left panel, select **NSX Management Service** and click **Configure** next to vCenter Server.
- 4 Type the IP address of the vCenter Server.
- 5 Type the vCenter Server user name and password.
- 6 Click **OK**.

Confirm that the vCenter Server status is Connected.

What to do next

Login to the vSphere Web Client and click the **Networking & Security** tab. You can now install and configure NSX components.

VMware recommends that you schedule a backup of NSX Manager data right after installing NSX Manager. See *NSX Administration Guide*.

Installing NSX Components

After the NSX Manager is installed, you can obtain licenses to activate the NSX Guest Introspection, NSX Edge, and NSX Data Security components. The NSX Manager OVA package includes the drivers and files required to install these add-on components.

NSX virtual appliances include VMware Tools. Do not attempt to alter or upgrade the VMware Tools software on an NSX virtual appliance.

This chapter includes the following topics:

- [“Install and Assign NSX for vSphere License,”](#) on page 19
- [“Set Up the Control Plane,”](#) on page 20
- [“Prepare Clusters for Network Virtualization,”](#) on page 21
- [“Configure VXLAN Transport Parameters,”](#) on page 21
- [“Assign Segment ID Pool and Multicast Address Range to NSX Manager,”](#) on page 23
- [“Prepare New Hosts and Clusters to Work with NSX,”](#) on page 23
- [“Install NSX Edge,”](#) on page 24
- [“Install Guest Introspection,”](#) on page 32
- [“Install Data Security,”](#) on page 34

Install and Assign NSX for vSphere License

You can install and assign an NSX for vSphere license after NSX Manager installation is complete by using the vSphere Web Client.

Before purchasing and activating an NSX for vSphere license, you can install and run the software in evaluation mode. When run in evaluation mode, intended for demonstration and evaluation purposes, NSX components are completely operational immediately after installation, do not require any licensing configuration, and provide full functionality for 60 days from the time you first activate them.

Procedure

- 1 Log in to the vSphere Web Client.
- 2 Click **Administration** and then click **Licenses**.
- 3 Click the **Solutions** tab.
- 4 From the drop-down menu at the top, select **Assign a new license key**.
- 5 Type the license key and an optional label for the new key.

6 Click **Decode**.

Decode the license key to verify that it is in the correct format, and that it has enough capacity to license the assets.

7 Click **OK**.**What to do next**


Obtain and install an NSX for vSphere license within the evaluation period.

Set Up the Control Plane

The controller cluster is the control plane component responsible for managing the switching and routing modules in the hypervisors. It consists of controller nodes to manage specific logical switches. Using a controller cluster to manage VXLAN-based logical switches eliminates the need for multicast support from the physical network infrastructure. You don't have to provision multicast group IP addresses, and you also don't need to enable PIM routing or IGMP snooping features on physical switches or routers. Selecting the **Unicast** check box while creating the logical switch enables this mode of VXLAN operation.

VMware recommends that you add three controllers for scale and redundancy.

Procedure

- 1 On the **Installation** tab, ensure that the **Management** tab is selected.
- 2 In the NSX Controller nodes section, click the **Add Node** () icon.
- 3 In the Add Controller dialog box, select the datacenter on which you are adding the node.
- 4 Select the cluster or resource pool where the controller is to be deployed.
- 5 Select the datastore and host.
- 6 Select the logical switch, portgroup, or distributed portgroup to which the node is to be connected.
The network that the controller is connected to is the management port group on the Distributed Virtual Switch that spans the environment.
- 7 Select the IP pool from which IP addresses are to be assigned to the node.

NOTE The IP address of the controller must be reachable from the NSX Manager and the management network of the vSphere hosts communicating with the controller.

- 8 Type and re-type a password for the controller.

The password must be 8 characters and must follow 3 of the following 4 rules:

- At least one upper case letter
- At least one lower case letter
- At least one number
- At least one special character

- 9 Click **OK**.

When deployed, the controller has a **Normal** status and displays a green check mark.

The NSX controller can now control the traffic flow through your logical switch.

What to do next

Deploy two additional controllers to ensure a greater level of resiliency. Three is the recommended number by VMware.

If you need to delete a controller, first stop using the logical router or logical switch based on this controller before deleting it.

Prepare Clusters for Network Virtualization

Network virtualization allows you to place virtual workloads on any available infrastructure in the data center regardless of the underlying physical network infrastructure. This eliminates the need for any network configurations that tie a virtual machine to its physical location in the network.

To prepare your environment for network virtualization, you must install network infrastructure components on a per-cluster level for each vCenter server. This deploys the required software on all hosts in the cluster. When a new host is added to this cluster, the required software is automatically installed on the newly added host.

After the network infrastructure is installed on a cluster, Logical Firewall is enabled on that cluster.

Prerequisites

All hosts in the cluster must be in the vSphere Distributed Switch being leveraged by NSX.

Procedure

- 1 In the **Installation** tab, click **Host Preparation**.
- 2 For each cluster, click **Install** in the Installation Status column.

NOTE While the installation is in progress, do not deploy, upgrade, or uninstall any service or component.

- 3 Monitor the installation until the **Installation Status** column displays a green check mark.

If the **Installation Status** column displays a red warning icon and says **Not Ready**, click **Resolve**. Clicking **Resolve** might result in a reboot of the host. If the installation is still not successful, click the warning icon. All errors are displayed. Take the required action and click **Resolve** again.

When the installation is complete, the **Installation Status** column displays 6.1 and the **Firewall** column displays **Enabled**. Both columns have a green check mark. If you see **Resolve** in the **Installation Status** column, click **Resolve** and then refresh your browser window.

Three VIBs are installed and registered with all hosts within the prepared cluster: VXLAN, Distributed Firewall, and Logical Routing.

Configure VXLAN Transport Parameters

The VXLAN network is used for Layer 2 Logical Switching across hosts. You configure VXLAN on a per-cluster basis, where you map each cluster that is to participate in a logical network to a vDS. When you map a cluster to a switch, each host in that cluster is enabled for logical switches. The settings chosen here will be used in creating the VMkernel interface.

Prerequisites

- All hosts in the cluster must be connected to a vDS.
- Network virtualization components must be installed.

Procedure

- 1 Ensure that you are on the **Installation > Host Preparation** tab.
- 2 For the cluster on which you want to configure VXLAN, click **Configure** in the **VXLAN** column.
- 3 In the Configuring VXLAN networking dialog box, select the switch to which you want to map the cluster.
- 4 Type the VLAN transport.
- 5 Type the Maximum Transmission Units (MTU) for the virtual distributed switch.

MTU is the maximum amount of data that can be transmitted in one packet before it is divided into smaller packets. VXLAN traffic frames are slightly larger in size because of encapsulation, so the MTU for each switch must be set to 1550 or higher.

- 6 In **VMKNic IP Addressing**, specify the IP pool to be used for the Management and Edge cluster.

Select	To
Use DHCP	Assign an IP address to the VXLAN VTEPs through Dynamic Host Configuration Protocol (DHCP).
Use IP pool	Assign a static IP address to the VXLAN VTEPs from the selected IP pool, or create a new IP pool.

- 7 If you selected **Use IP Pool**, select an IP pool.
- 8 Select the **VMKNic Teaming Policy** for the vSwitch. The NIC teaming policy determines the load balancing and failover settings of the virtual switch.

It is important to choose the right teaming policy to avoid packet loss. See [“Teaming Policy for Virtual Distributed Switches,”](#) on page 22.

- 9 Edit the VTEP value, if required.

VTEP (VXLAN Tunnel End Points) is the number of dvUplinks on the switch, which load balances traffic between multiple PNICs. VMware recommends that you do not edit the default VTEP value. This field is disabled if the teaming policy you selected does not require multiple VTEPs (ether channel, failover, LACPv1, or LACPv2).

- 10 Click **OK**.

Teaming Policy for Virtual Distributed Switches

You should choose a teaming policy for VXLAN transport based on the topology of your physical switches.

For certain teaming modes, VMware software creates multiple VTEPs to load balance traffic among the physical vNICs.

For information on teaming mode descriptions, refer to the VMware vSphere documentation.

Table 4-1. Teaming Policy table

Teaming Mode	Multiple VTEPs Created	vDS Version
Ether channel NOTE If you are using blade chassis, ensure that it supports ether channel before choosing this teaming mode.	No	5.1 and later
Failover	No	5.1 and later
LACPv1	No	5.1

Table 4-1. Teaming Policy table (Continued)

Teaming Mode	Multiple VTEPs Created	vDS Version
LACPv2	No	5.5
Source MAC (MAC Hash)	Yes	5.5

NOTE LBT mode is not supported.

Assign Segment ID Pool and Multicast Address Range to NSX Manager

You must specify a segment ID pool for each NSX Manager to isolate your network traffic. If an NSX controller is not deployed in your environment, you must add a multicast address range to spread traffic across your network and avoid overloading a single multicast address.

The Segment ID Pool specifies a range of VXLAN Network Identifiers (VNIs) for use when building Logical Network segments.

Procedure

- 1 On the **Installation** tab, click **Logical Network Preparation** and then click **Segment ID**.
- 2 Click the **Edit** (✎) icon
- 3 Type a range for segment IDs. For example, **5000–5200**.
The segment ID range determines the maximum number of logical switches that can be created in your infrastructure.
- 4 If you do not have a deployed NSX controller in your environment, select **Enable multicast addressing** and type an address range. For example, **239.1.1.10–239.1.1.20**.

NOTE You must specify a multicast address range for VMware ESX 5.1 hosts or when using the hybrid mode.

- 5 Click **OK**.

Prepare New Hosts and Clusters to Work with NSX

After the initial deployment of NSX, you may want to add hosts and clusters in vCenter Server so that they work with NSX.

Add a Host to a Prepared Cluster

This section describes how to add a host to a cluster prepared for network virtualization.

Procedure

- 1 Add the host to vCenter Server as a standalone host.
See *ESXi and vCenter Server 5.5 Documentation*.
- 2 Add the host to the vSphere Distributed Switch mapped to the cluster where you want to add the host.
All hosts in the cluster must be in the vSphere Distributed Switch being leveraged by NSX.
- 3 Place the host into maintenance mode.

- 4 Add the host to the cluster.

Since this is a prepared cluster, the required software is automatically installed on the newly added host.

- 5 Remove the host from maintenance mode.

DRS balances virtual machines onto the host.

Add a Host to an Unprepared Cluster

This section describes how to add a host to a cluster not yet prepared for network virtualization.

Procedure

- 1 Add the host to vCenter as a standalone host or to an unprepared cluster.
See *ESXi and vCenter Server 5.5 Documentation*.
- 2 Add the host to a vSphere Distributed Switch.
- 3 If you added the host as a standalone host, add it to the appropriate cluster.

Remove a Host from an NSX Prepared Cluster

This section describes how to remove a host from a cluster prepared for network virtualization.

Procedure

- 1 Place host into maintenance mode.
See *ESXi and vCenter Server 5.5 Documentation*.
- 2 Remove host from the prepared cluster.
NSX uninstalls the network virtualization components from the host.
- 3 Reboot the host either by clicking **Resolve** next to the appropriate cluster on the **Installation > Host Preparation** tab or from vCenter Server.

Install NSX Edge

You can install NSX Edge as a services gateway or as a logical router.

NSX Edge Services Gateway

The services gateway gives you access to all NSX Edge services such as firewall, NAT, DHCP, VPN, load balancing, and high availability. You can install multiple NSX Edge services gateway virtual appliances in a datacenter. Each NSX Edge virtual appliance can have a total of ten uplink and internal network interfaces. The internal interfaces connect to secured port groups and act as the gateway for all protected virtual machines in the port group. The subnet assigned to the internal interface can be a publicly routed IP space or a NATed/routed RFC 1918 private space. Firewall rules and other NSX Edge services are enforced on traffic between network interfaces.

Uplink interfaces of NSX Edge connect to uplink port groups that have access to a shared corporate network or a service that provides access layer networking. Multiple external IP addresses can be configured for load balancer, site-to-site VPN, and NAT services.

Logical Router

The NSX Edge logical router provides East-West distributed routing with tenant IP address space and data path isolation. Virtual machines or workloads that reside on the same host on different subnets can communicate with one another without having to traverse a traditional routing interface.

A logical router can have eight uplink interfaces and up to a thousand internal interfaces.

Install an NSX Edge Services Gateway

You can install multiple NSX Edge services gateway virtual appliances in a data center. Each NSX Edge virtual appliance can have a total of ten uplink and internal network interfaces. The internal interfaces connect to secured port groups and act as the gateway for all protected virtual machines in the port group. The subnet assigned to the internal interface can be a publicly routed IP space or a NATed/routed RFC 1918 private space. Firewall rules and other NSX Edge services are enforced on traffic between interfaces.


Uplink interfaces of NSX Edge connect to uplink port groups that have access to a shared corporate network or a service that provides access layer networking.

Multiple external IP addresses can be configured for load balancer, site-to-site VPN, and NAT services. Overlapping IP addresses are not allowed for internal interfaces, and overlapping subnets are not allowed for internal and uplink interfaces.

Open the Add Edge Wizard

Open the Add Edge wizard to install and configure an NSX Edge instance.

Procedure

- 1 On the **Networking & Security** tab, click **NSX Edges**.
- 2 Click the **Add** () icon.
- 3 In the Add Edge Gateway wizard, select **Edge Services Gateway**.
- 4 Type a name for the NSX Edge virtual machine.
This name appears in your vCenter inventory. The name should be unique across all Edges within a single tenant.
- 5 (Optional) Type a host name for the NSX Edge virtual machine.
This name appears in the CLI. If you do not specify the host name, the Edge ID is displayed in the CLI.
- 6 (Optional) Type a description and tenant for this NSX Edge.
- 7 Click **Next**.

Specify the CLI Credentials

Edit the credentials to be used for logging in to the Command Line Interface (CLI).

Procedure

- 1 On the CLI Credentials page, specify the CLI credentials for your NSX Edge virtual machine.

Option	Action
CLI user name	Edit if required.
CLI password	Type a password.

- 2 (Optional) Click **Enable SSH access** if required.

- 3 Click **Next**.

The Edge Appliances page appears.

Configure Deployment

You must add an appliance before you can deploy a NSX Edge. If you do not add an appliance when you install NSX Edge, NSX Edge remains in an offline mode until you add an appliance.

Prerequisites

Verify that the resource pool has enough capacity for the Edge virtual machine to be deployed. See [“System Requirements for NSX,”](#) on page 13.

Procedure

- 1 On the Deployment Configuration page, select the datacenter where you want to place the NSX Edge virtual machine.
- 2 Select the size of the NSX Edge instance based on your system resources.

The **Large** NSX Edge has more CPU, memory, and disk space than the **Compact** NSX Edge, and supports a bigger number of concurrent SSL VPN-Plus users. The **X-Large** NSX Edge is suited for environments which have Load Balancer with millions of concurrent sessions. The Quad Large NSX Edge is recommended for high throughput and requires a high connection rate.

See [“System Requirements for NSX,”](#) on page 13.

- 3 Click **Enable auto rule generation** to add firewall, NAT, and routing routes to enable control traffic to flow for these services..

If you do not select **Enable auto rule generation**, you must manually add firewall, NAT, and routing configuration to allow control channel traffic for NSX Edge services such as Load Balancing, VPN, etc.

NOTE Auto rule generation does not create rules for data-channel traffic.

- 4 In **NSX Edge Appliances**, click the **Add** (+) icon to add an appliance.
If you had selected **Enable HA** on the Name and Description page, you can add two appliances. If you add a single appliance, NSX Edge replicates its configuration for the standby appliance and ensures that the two HA NSX Edge virtual machines are not on the same ESX host even after you use DRS and vMotion (unless you manually vMotion them to the same host).
- 5 In the Add Edge Appliance dialog box, select the cluster or resource pool and datastore for the appliance.
- 6 (Optional) Select the host on which the appliance is to be added.
- 7 (Optional) Select the vCenter folder within which the appliance is to be added.
- 8 Click **OK**.
- 9 Click **Next**.

The Interface Configuration page appears.

Add Internal and Uplink Interfaces

You can add up to ten (internal and uplink) interfaces to an NSX Edge virtual machine.

Procedure

- 1 On the Configure Interfaces page, click the **Add** (+) icon and type a name for the interface.
- 2 Type a name for the interface.

- 3 Select **Internal** or **Uplink** to indicate whether this is an internal or external interface.

NOTE You must add at least one internal interface for HA to work.

- 4 Select the port group or logical switch to which this interface should be connected.
 - a Click **Select** next to the **Connected To** field.
 - b Depending on what you want to connect to the interface, click the **Logical Switch**, **Standard Portgroup**, or **Distributed Portgroup** tab.
 - c Select the appropriate virtual wire or portgroup.
 - d Click **Select**.

- 5 Select the connectivity status for the interface.

- 6 In **Configure Subnets**, click the **Add** (+) icon to add a subnet for the interface.

NOTE An interface can have multiple non-overlapping subnets.

- a In **Add Subnet**, click the **Add** (+) icon and type IP address for the subnet.

NOTE If you enter more than one IP address, you can select the Primary IP address. An interface can have one primary and multiple secondary IP addresses. NSX Edge considers the Primary IP address as the source address for locally generated traffic.

You must add an IP address to an interface before using it on any feature configuration.

- b Type the subnet mask for the interface and click **OK**.
- 7 Type the MAC address for the interface. If HA is enabled, type two management IP addresses in CIDR format.

NOTE Heartbeats of the two NSX Edge HA virtual machines are communicated through these management IP addresses. The management IP addresses must be in the same L2/subnet and be able to communicate with each other.

- 8 Change the default MTU if required.
- 9 In **Options**, select the required options.

Option	Description
Enable Proxy ARP	Supports overlapping network forwarding between different interfaces
Send ICMP Redirect	Conveys routing information to hosts

- 10 Type the fence parameters and click **OK**.
- 11 (Optional) Repeat the above steps to add additional interfaces.
- 12 Click **Next**.

Configure the Default Gateway

If you installing an NSX Edge services gateway, provide the IP address for the NSX Edge default gateway.

Procedure

- 1 On the Default Gateway page, select **Configure Default Gateway**.
- 2 Select the interface that can communicate with the next hop or gateway IP address.

- 3 Type the IP address for the default gateway.
- 4 In **MTU**, the default MTU for the interface you selected in [Step 2](#) is displayed. You can edit this value, but it cannot be more than the configured MTU on the interface.
- 5 Click **Next**.

The Firewall & HA page appears.

Configure Firewall Policy and High Availability

Configure the default firewall policy and HA parameters.

If you do not configure the firewall policy, the default policy is set to deny all traffic and logs are disabled.

You must configure HA parameters for high availability to work on network configurations on NSX Edge. NSX Edge supports two virtual machines for high availability, both of which are kept up to date with user configurations. If a heartbeat failure occurs on the primary virtual machine, the secondary virtual machine state is changed to active. Thus, one NSX Edge virtual machine is always active on the network.

Procedure

- 1 On the Firewall & HA page, select **Configure Firewall default policy**.
- 2 Specify whether to accept or deny incoming traffic by default.
- 3 Select whether to log incoming traffic.

Enabling default logging may generate too many logs and affect the performance of your NSX Edge. Hence, it is recommended that you enable default logging only while troubleshooting or debugging.

- 4 If you selected **Enable HA** on the Name & Description page, complete the **Configure HA parameters** section.

NSX Edge replicates the configuration of the primary appliance for the standby appliance and ensures that the two HA NSX Edge virtual machines are not on the same ESX host even after you use DRS and vMotion. Two virtual machines are deployed on vCenter in the same resource pool and datastore as the appliance you configured. Local link IPs are assigned to HA virtual machines in the NSX Edge HA so that they can communicate with each other. You can specify management IP addresses to override the local links.

- a Select the internal interface for which to configure HA parameters.
- b (Optional) Type the period in seconds within which, if the backup appliance does not receive a heartbeat signal from the primary appliance, the primary appliance is considered inactive and the back up appliance takes over.

The default interval is 15 seconds.

- c (Optional) Type two management IP addresses in CIDR format to override the local link IPs assigned to the HA virtual machines.

Ensure that the management IP addresses do not overlap with the IPs used for any other interface and do not interfere with traffic routing. You should not use an IP that exists somewhere else on your network, even if that network is not directly attached to the NSX Edge.

- 5 Click **Next**.

The Summary page appears.

Confirm Settings and Install the NSX Edge Gateway

Before you install the NSX Edge gateway, review the settings you entered.

Procedure

- 1 On the Summary page, review the settings for the NSX Edge.
- 2 Click **Back** to modify the settings.
- 3 Click **Finish** to accept the settings and install the NSX Edge gateway.

Install a Logical (Distributed) Router

An NSX Edge logical router provides routing and bridging functionality only.

With distributed routing, virtual machines or workloads that reside on the same host on different subnets can communicate with one another without having to traverse a traditional routing interface such as the NSX Edge services gateway.

You must have one, three, or five controller nodes and one logical switch in your environment before installing a logical router. See [“Set Up the Control Plane,”](#) on page 20.


Open the Add Edge Wizard Page for a Logical Router

Open the Add Edge wizard to install and configure a logical router instance.

Prerequisites

You must have at least three controller nodes and one logical switch in your environment before installing a logical router.

Procedure

- 1 In the **Networking & Security** tab, click **NSX Edges**.
- 2 Click the **Add** () icon.
- 3 In the Add Edge Gateway wizard, select **Logical (Distributed) Router**.
- 4 Type a name for the NSX Edge virtual machine.
This name appears in your vCenter inventory. The name should be unique across all Edges within a single tenant.
- 5 (Optional) Type a host name for the NSX Edge virtual machine.
This name appears in the CLI. If you do not specify the host name, the Edge ID is displayed in the CLI.
- 6 (Optional) Type a description and tenant for this NSX Edge.
- 7 Click **Next**.

Specify Settings

Specify settings for the router.

Procedure

- 1 On the CLI Credentials page, specify the CLI credentials for your NSX Edge virtual machine.

Option	Action
CLI user name	Edit if required.
CLI password	Type a password.

- 2 (Optional) Click **Enable SSH access**, if required.
- 3 Select **Enable High Availability** to enable and configure high availability (HA).
- 4 Specify the logging level for the router.
- 5 Click **Next**.

The Edge Appliances page appears.

Configure Deployment for Logical Router

You must add an appliance before you can deploy a NSX Edge.

Prerequisites

For high availability, verify that the resource pool has enough capacity for both HA virtual machines to be deployed.

Procedure

- 1 On the Deployment Configuration page, select the datacenter where you want to place the NSX Edge virtual machine.
- 2 In **NSX Edge Appliances**, click the **Add** (+) icon to add an appliance.

If you had selected **Enable HA** on the Name and Description page, you can add two appliances. If you add a single appliance, NSX Edge replicates its configuration for the standby appliance ensures that the two HA NSX Edge virtual machines are not on the same ESX host even after you use DRS and vMotion (unless you manually vMotion them to the same host).
- 3 In the Add Edge Appliance dialog box, select the cluster or resource pool and datastore for the appliance.
- 4 (Optional) Select the host on which the appliance is to be added.
- 5 (Optional) Select the vCenter folder within which the appliance is to be added.
- 6 Click **OK**.
- 7 Click **Next**.

The Interfaces Configuration page appears.

Configure Interfaces for a Logical Router

You must specify the management interface for the router. You use this interface for out-of-band (meaning not over the same network your data travels) access to NSX Edge. Unlike other network interfaces on the device, which receive and transmit traffic flowing between different network interfaces on the device (transit traffic), the out-of-band management interface accepts traffic only to and from the router itself. Using a separate, dedicated interface for managing the router is a best practice, because management traffic should not interfere with network traffic, and the management interface remains available even if other network interfaces go down.

You can configure up to 999 interfaces, with a maximum of 8 uplinks.

Procedure

- 1 (Optional) On the **Interfaces** page, type the IP address for the management interface.
- 2 (Optional) In **Management Interface Configuration**, click **Select** next to the **Connected To** field and select the logical switch or port group that you want to set as the management interface. Click the **Add** (+) icon to add a subnet for the management interface.
- 3 In the **Add Subnet** dialog box, click the **Add** (+) icon.
- 4 Type the IP address of the subnet and click **OK**. If you add more than one subnet, select the primary subnet.
- 5 Type the subnet prefix length and click **OK**.
- 6 In **Configure Interfaces**, click the **Add** (+) icon to add a traffic interface and type a name for the interface.
- 7 Select **Internal** or **Uplink** to indicate whether this is an internal or external interface.
- 8 Select the port group or VXLAN virtual wire to which this interface should be connected.
 - a Click **Select** next to the **Connected To** field.
 - b Depending on what you want to connect to the interface, click the **Logical Switch** or the **Distributed Portgroup** tab.
 - c Select the appropriate logical switch or port group.
 - d Click **OK**.
- 9 Select the connectivity status for the interface.
- 10 In **Configure Subnets**, click the **Add** (+) icon to add a subnet for the interface.
- 11 In **Add Subnet**, click the **Add** (+) icon to add an IP address.
- 12 Type the IP address.

You must assign an IP address to an interface before using it on any feature configuration.

- 13 Click **OK**.
- 14 Type the subnet prefix length.
- 15 Click **OK** and then click **OK** again.
- 16 Click **Next**.

The **Default Gateway** page appears.

Configure HA for Logical Router

Enable or disable HA.

If you selected **Enable HA** on the Name & Description page, complete the Configure HA parameters section. NSX Edge replicates the configuration of the primary appliance for the standby appliance and ensures that the two HA NSX Edge virtual machines are not on the same ESX host even after you use DRS and vMotion. Two virtual machines are deployed on vCenter in the same resource pool and datastore as the appliance you configured. Local link IPs are assigned to HA virtual machines in the NSX Edge HA so that they can communicate with each other. You can specify management IP addresses to override the local links.

Procedure

- 1 Type the period in seconds within which, if the backup appliance does not receive a heartbeat signal from the primary appliance, the primary appliance is considered inactive and the back up appliance takes over. The default interval is 15 seconds.
- 2 (Optional) Type two management IP addresses in CIDR format to override the local link IPs assigned to the HA virtual machines.

Ensure that the management IP addresses do not overlap with the IPs used for any other interface and do not interfere with traffic routing. You should not use an IP that exists somewhere else on your network, even if that network is not directly attached to the NSX Edge.

- 3 Click **Next**.

Confirm Settings and Install the Logical Router

Before you install the NSX Edge router, review the settings you entered.

Procedure

- 1 On the Summary page, review the settings for the NSX Edge.
- 2 Click **Previous** to modify the settings
- 3 Click **Finish** to accept the settings and install the NSX Edge router.

The logical router control virtual machine is deployed. Logical router instances are instantiated on each host that has the logical switches being routed.

Install Guest Introspection

Installing Guest Introspection installs a new vib and a service virtual machine on each host in the cluster. Guest Introspection is required for NSX Data Security, Activity Monitoring, and several third-party security solutions.


Prerequisites

The installation instructions that follow assume that you have the following system:

- A datacenter with supported versions of vCenter Server and ESXi installed on each host in the cluster. For information on the required versions, see [“System Requirements for NSX,”](#) on page 13.
- Network virtualization components must have been installed on the hosts in the cluster where you want to install Guest Introspection. Guest Introspection cannot be installed on standalone hosts.
- NSX Manager 5.5 installed and running.

If you want to assign an IP address to the NSX Guest Introspection service virtual machine from an IP pool, create the IP pool before installing NSX Guest Introspection. See Grouping Objects in *NSX Administration Guide*.

Procedure

- 1 On the **Installation** tab, click **Service Deployments**.
- 2 Click the **New Service Deployment** () icon.
- 3 In the Deploy Network and Security Services dialog box, select **Guest Introspection**.
- 4 In **Specify schedule** (at the bottom of the dialog box), select **Deploy now** to deploy Guest Introspection as soon as it is installed or select a deployment date and time.
- 5 Click **Next**.
- 6 Select the datacenter and cluster(s) where you want to install Guest Introspection, and click **Next**.
- 7 On the Select storage and Management Network Page, select the datastore on which to add the service virtual machines storage or select **Specified on host**. It is recommended that you use shared datastores and networks instead of "specified on host" so that deployment workflows are automated.

The selected datastore must be available on all hosts in the selected cluster.

If you selected **Specified on host**, follow the steps below for each host in the cluster.

- a On the vSphere Web Client home page, click **vCenter** and then click **Hosts**.
 - b Click a host in the **Name** column and then click the **Manage** tab.
 - c Click **Agent VM Settings** and click **Edit**.
 - d Select the datastore and click **OK**.
- 8 Select the distributed virtual port group to host the management interface. If the datastore is set to **Specified on host**, the network must also be **Specified on host**.

The selected port group must be able to reach the NSX Manager's port group and must be available on all hosts in the selected cluster.

If you selected **Specified on host**, follow the substeps in Step 8 to select a network on the host. When you add a host (or multiple hosts) to the cluster, the datastore and network must be set before each host is added to the cluster.

- 9 In IP assignment, select one of the following:

Select	To
DHCP	Assign an IP address to the NSX Guest Introspection service virtual machine through Dynamic Host Configuration Protocol (DHCP).
An IP pool	Assign an IP address to the NSX Guest Introspection service virtual machine from the selected IP pool.

- 10 Click **Next** and then click **Finish** on the Ready to complete page.
- 11 Monitor the deployment until the **Installation Status** column displays **Succeeded**.
- 12 If the **Installation Status** column displays **Failed**, click the icon next to Failed. All deployment errors are displayed. Click **Resolve** to fix the errors. In some cases, resolving the errors displays additional errors. Take the required action and click **Resolve** again.

What to do next

Install VMware Tools on guest virtual machines.

Install VMware Tools on the Guest Virtual Machines

VMware Tools include the NSX Thin Agent that must be installed on each guest virtual machine to be protected. Virtual machines with VMware Tools installed are automatically protected whenever they are started up on an ESX host that has the security solution installed. That is, protected virtual machines retain the security protection through shut downs and restarts, and even after a vMotion move to another ESX host with the security solution installed.

Prerequisites

Ensure that the guest virtual machine has ESX 5.1 or later and a supported version of Windows installed. The following Windows operating systems are supported for NSX Guest Introspection:

- Windows Vista (32 bit)
- Windows 7 (32/64 bit)
- Windows XP SP3 and above (32 bit)
- Windows 2003 SP2 and above (32/64 bit)
- Windows 2003 R2 (32/64 bit)
- Windows 2008 (32/64 bit)
- Windows 2008 R2 (64 bit)
- Windows 8 (32/64) -- from vSphere 5.5 and later
- Win2012 (64) -- from vSphere 5.5 and later
- Windows 8.1 (32/64) -- from vSphere 5.5 Patch 2 and later
- Win2012 R2 (64) -- from vSphere 5.5 Patch 2 and later

Procedure

- 1 Follow the procedure [Manually Install or Upgrade VMware Tools in a Windows Virtual Machine](#).
- 2 After you select **Custom** setup in step 7, expand the **VMCI Driver** section, select **vShield Drivers**, and select **This feature will be installed on the local hard drive**.
- 3 Follow the remaining steps in the procedure.


Install Data Security

Prerequisites

NSX Guest Introspection must be installed on the cluster where you are installing Data Security.

If you want to assign an IP address to the Data Security service virtual machine from an IP pool, create the IP pool before installing Data Security. See Grouping Objects in *NSX Administration Guide*.

Procedure

- 1 In the **Installation** tab, click **Service Deployments**.
- 2 Click the **New Service Deployment** () icon.
- 3 In the Deploy Network and Security Services dialog box, select **Data Security** and click **Next**.
- 4 In **Specify schedule** (at the bottom of the dialog box), select **Deploy now** to deploy Data Security as soon as it is installed or select a deployment date and time.
- 5 Click **Next**.

- 6 Select the datacenter and cluster(s) where you want to install Data Security and click **Next**.
- 7 On the Select storage and Management Network page, select the datastore on which to add the service virtual machines storage or select **Specified on host**.

The selected datastore must be available on all hosts in the selected cluster.

If you selected **Specified on host**, the datastore for the ESX host must be specified in the **AgentVM Settings** of the host before it is added to the cluster. See *vSphere API/SDK Documentation*.

- 8 Select the distributed virtual port group to host the management interface. This port group must be able to reach the NSX Manager's port group.

If the datastore is set to **Specified on host**, the network to be used must be specified in the **agentVmNetwork** property of each host in the cluster. See *vSphere API/SDK Documentation*.

When you add a host(s) to the cluster, the **agentVmNetwork** property for the host must be set before it is added to the cluster.

The selected port group must be available on all hosts in the selected cluster.

- 9 In IP assignment, select one of the following:

Select	To
DHCP	Assign an IP address to the Data Security service virtual machine through Dynamic Host Configuration Protocol (DHCP).
An IP pool	Assign an IP address to the Data Security service virtual machine from the selected IP pool.

Note that static IP address are not supported.

- 10 Click **Next** and then click **Finish** on the Ready to complete page.
- 11 Monitor the deployment until the **Installation Status** column displays **Succeeded**.
- 12 If the **Installation Status** column displays **Failed**, click the icon next to Failed. All deployment errors are displayed. Click **Resolve** to fix the errors. In some cases, resolving the errors displays additional errors. Take the required action and click **Resolve** again.

Deploy a Partner Service


If the partner solution includes a host-resident virtual appliance, you can deploy the service after the solution is registered with NSX Manager.

Prerequisites

Ensure that:

- The partner solution is registered with NSX Manager.
- NSX Manager can access the partner solution's management console.

Procedure

- 1 Click **Networking & Security** and then click **Installation**.
- 2 Click the **Service Deployments** tab and click the **New Service Deployment** () icon.
- 3 In the Deploy Network and Security Services dialog box, select the appropriate solution(s).
- 4 In **Specify schedule** (at the bottom of the dialog box), select **Deploy now** to deploy the solution immediately or select a deployment date and time.
- 5 Click **Next**.
- 6 Select the datacenter and cluster(s) where you want to deploy the solution and click **Next**.
- 7 On the Select storage page, select the datastore on which to add the solution service virtual machines storage or select **Specified on host**.

The selected datastore must be available on all hosts in the selected cluster.

If you selected **Specified on host**, the datastore for the ESX host must be specified in the **AgentVM Settings** of the host before it is added to the cluster. See *vSphere API/SDK Documentation*.

- 8 Click **Next**.
- 9 On the Configure management network page, select the distributed virtual port group to host the management interface. This port group must be able to reach the NSX Manager's port group.

If the network is set to **Specified on host**, the network to be used must be specified in the **Agent VM Settings > Network** property of each host in the cluster. See *vSphere API/SDK Documentation*.

When you add a host(s) to the cluster, the **Agent VM Settings > Network** property for the host must be set before it is added to the cluster.

The selected port group must be available on all hosts in the selected cluster.

- 10 In IP assignment, select one of the following:

Select	To
DHCP	Assign an IP address to the service virtual machine through Dynamic Host Configuration Protocol (DHCP).
An IP pool	Assign an IP address to the service virtual machine from the selected IP pool.

- 11 Click **Next** and then click **Finish** on the Ready to complete page.
- 12 Monitor the deployment until the **Installation Status** displays Successful. If the status displays Failed, click the icon next to Failed and take action to resolve the error.

What to do next

You can now consume the partner service through NSX UI or NSX API.

Upgrading NSX

Follow the upgrade procedure appropriate to the current software version installed in your environment.

Before upgrading, check the latest interoperability information in the Product Interoperability Matrix at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

This chapter includes the following topics:

- “Upgrade vShield 5.5 to NSX 6.1,” on page 39
- “Upgrade NSX 6.0.x to NSX 6.1,” on page 44
- “Upgrade NSX 6.1 to NSX 6.1.1,” on page 48

Upgrade vShield 5.5 to NSX 6.1

To upgrade to NSX 6.1, you must first upgrade the NSX Manager, and then upgrade the other components in the order in which they are documented.

NSX components must be upgraded in the following order:

- 1 NSX Manager
- 2 Virtual switches
- 3 vShield App
- 4 vShield Edge
- 5 vShield Endpoint

Upgrade to NSX Manager 6.1

You can upgrade to NSX Manager 6.1 only from vShield Manager 5.5. If you have a prior version of vShield Manager in your infrastructure, you must first upgrade to version 5.5 and then to NSX Manager 6.1. For information on upgrading to version 5.5, see *vShield Installation and Upgrade Guide* version 5.5.

Prerequisites

- You have upgraded to vCenter Server 5.5.
- vShield Data Security has been uninstalled. For information on uninstalling the current Data Security software, see the documentation for that version.
- vShield Edge instances prior to version 5.5, if any, have been upgraded to version vShield 5.5.

Pre-5.5 vShield Edge instances cannot be managed or deleted after vShield Manager has been upgraded to NSX Manager.

- It is recommended that you back up your current configuration before upgrading. See Operations and Management in *NSX Administration Guide*.



CAUTION Do not uninstall a deployed instance of vShield Manager appliance.

Procedure

- 1 Download the NSX upgrade bundle to a location to which vShield Manager can browse. The name of the upgrade bundle file is something like `VMware-vShield-Manager-upgrade-bundle-to-NSX-buildNumber.tar.gz`.
- 2 From the vShield Manager 5.5 inventory panel, click **Settings & Reports**.
- 3 Click the **Updates** tab and then click **Upload Upgrade Bundle**.
- 4 Click **Browse**, select the `VMware-vShield-Manager-upgrade-bundle-to-NSX-6.1-buildNumber.tar.gz` file, and click **Open**.
- 5 Click **Upload File**.

Uploading the file takes a few minutes.

- 6 Click **Install** to begin the upgrade process.
- 7 Click **Confirm Install**. The upgrade process reboots vShield Manager, so you might lose connectivity to the vShield Manager user interface. None of the other vShield components are rebooted.
- 8 After the reboot, log in to the NSX Manager virtual appliance by opening a Web browser window and typing the same IP address as that of the vShield Manager. For example, `https://11.111.11.11`.

The Summary tab displays the version of NSX Manager that you just installed.

Close any existing browser sessions accessing the vSphere Web Client. Wait a few minutes and clear the browser cache before logging back in to the vSphere Web Client.

If SSH was enabled on vShield manager 5.5, you must enable it on NSX Manager after the upgrade. Log in to the NSX Manager virtual appliance and click **View Summary**. In System-level components, click **Start** for SSH service.

- 9 Shut down the NSX Manager virtual machine and increase the memory to 12 GB and vCPU to 4.

All grouping objects from vShield Manager 5.5 are carried over to NSX. Objects that were created at datacenter or port group level are now visible and applicable at the global scope. For information on how to view grouping objects in the vSphere Web Client, see Grouping Objects in *NSX Administration Guide*.

All users and associated roles are carried over to NSX as well. For information on viewing roles in the vSphere Web Client, see User Management in *NSX Administration Guide*.

Prepare Clusters for Network Virtualization and upgrade Virtual Wires to Logical Switches 6.1

You must prepare your environment for network virtualization by installing network infrastructure components on a per-cluster level for each vCenter server. This deploys the required software on all hosts in the cluster and upgrades virtual Wires from a 5.5 environment to NSX logical switches.

Prerequisites

- vShield Manager has been upgraded to NSX Manager.
- It is recommended that you upgrade to logical switches in a datacenter maintenance window.

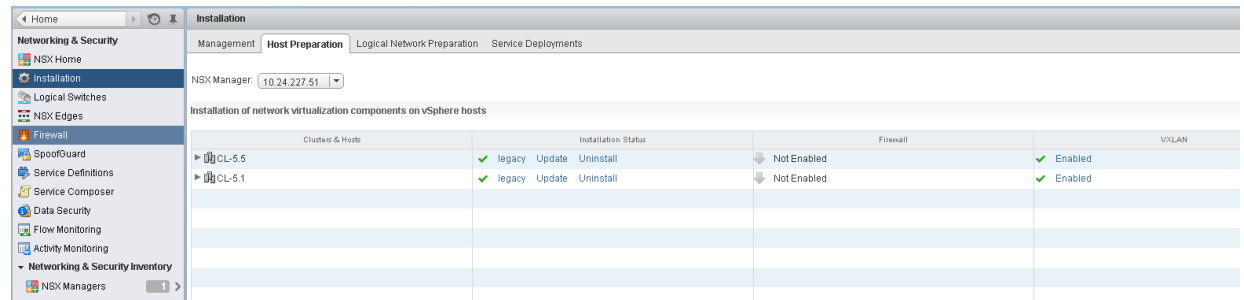
Procedure

- 1 Log in to the vSphere Web Client.
- 2 Click **Networking & Security** and then click **Installation**.
- 3 Click the **Host Preparation** tab.

All clusters in your infrastructure are displayed.

If you had Virtual Wires in your 5.5 environment, the **Installation Status** column displays **legacy**, **Update**, and **Uninstall**.

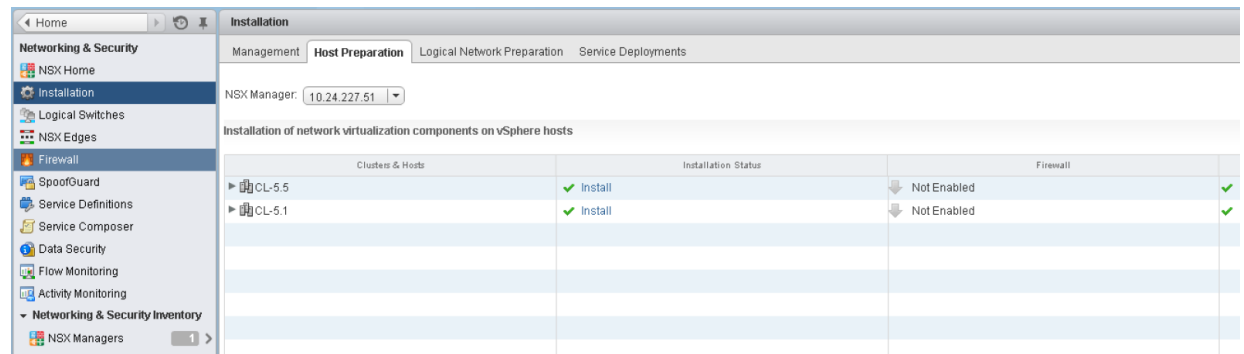
Figure 6-1. Installation Status displays Update when you have Virtual Wires in your 5.5 environment



Clusters & Hosts	Installation Status	Firewall	VXLAN
CL-5.5	legacy Update Uninstall	Not Enabled	Enabled
CL-5.1	legacy Update Uninstall	Not Enabled	Enabled

If you did not have Virtual Wires in your 5.5 environment, the **Installation Status** column displays **Install**.

Figure 6-2. Installation Status displays Install when you do not have Virtual Wires in your 5.5 environment



Clusters & Hosts	Installation Status	Firewall	VXLAN
CL-5.5	Install	Not Enabled	Enabled
CL-5.1	Install	Not Enabled	Enabled

- 4 For each cluster, click **Update** or **Install** in the Installation Status column.
Each host in the cluster receives the new logical switch software.
- 5 Monitor the installation until the **Installation Status** column displays a green check mark.
- 6 If the **Installation Status** column displays a red warning icon and says **Not Ready**, click **Resolve**. If the installation is still not successful, click the warning icon. All errors are displayed. Take the required action and click **Resolve** again.

NSX reboots the hosts after moving them to maintenance mode and leveraging DRS to vMotion active virtual machines to other hosts. If an error message is displayed, you may need to reboot the hosts in the cluster manually or take other action according to the error message.

While the upgrade is in progress, do not deploy, upgrade, or uninstall any service or component.

All virtual wires from your 5.5 infrastructure are upgraded to NSX logical switches, and the VXLAN column for the cluster says **Enabled**. You can now add a controller and change the control plane setting for the transport zone to **Unicast** or **Hybrid** at the logical switch level or transport zone level. See [“Set Up the Control Plane,”](#) on page 20.

Upgrade to Logical Firewall 6.1

You can upgrade to Logical Firewall only from vShield App version 5.5. If you have a prior version of vShield App in your infrastructure, you must upgrade to version 5.5 before upgrading to version 6.1. For information on upgrading to version 5.5, see *vShield Installation and Upgrade Guide* version 5.5.

Prerequisites

- 1 vShield Manager has been upgraded to NSX Manager.
- 2 Virtual wires have been upgraded to NSX Logical Switches. For non-VXLAN users, network virtualization components have been installed.
- 3 If you want to migrate vShield App 5.5 rules to Logical Firewall, do not delete the vShield App appliances before upgrading to Logical Firewall.

Procedure

- 1 After you prepare all clusters in your environment for network virtualization components, a pop up message indicates that Firewall is ready to be upgraded.

- 2 Click **Upgrade**.

vShield App 5.5 rules are migrated to NSX in the following way:

- a A new section is created in the central firewall table for each namespace (datacenter and virtual wire) configured in vShield App version 5.5. Each section includes the corresponding firewall rules.
- b All rules in each section have the same value in the **AppliedTo** field - datacenter ID for datacenter namespace, virtual wire ID for virtual wire namespace, and port group ID for port group based namespace.
- c Containers created at different namespace levels are moved to the global level.
- d Section order is as below to ensure that firewall behavior after the upgrade remains the same:

Section_Namespace_Portgroup-1

.....

Section_Namespace_Portgroup-N

Section_Namespace_VirtualWire-1

.....

Section_Namespace_VirtualWire-N

Section_Namespace_Datacenter_1

.....

Section_Namespace_Datacenter_N

Default_Section_DefaultRule

After the upgrade is complete, the Firewall column displays **Enabled**.

- 3 Inspect each upgraded section and rule to ensure it works as intended.

What to do next

Navigate to the **Installation > Service Deployments** tab and ensure that all alarms are resolved and that the legacy vShield App service status displays **Succeeded**. You can then delete the legacy vShield App service virtual machines.

Upgrade to NSX Edge 6.1

You can upgrade only from version vShield 5.5 to NSX Edge 6.1. If you have a prior version of vShield Edge in your infrastructure, you must upgrade to version 5.5 before upgrading to version 6.0. For information on upgrading to version 5.5, see *vShield Installation and Upgrade Guide* version 5.5.

Prerequisites

- vShield Manager has been upgraded to NSX Manager.
- Virtual wires have been upgraded to NSX Logical Switches.
- System requirements for NSX Edge X-Large have been changed in NSX. See [Chapter 2, “Preparing for Installation,”](#) on page 13.

Procedure

- 1 In the vSphere Web Client, click **Networking & Security > NSX Edges**.

The NSX Edges page shows all Edge 5.5 instances.

- 2 For each NSX Edge instance, select **Upgrade Version** from the **Actions** menu.

After the NSX Edge is upgraded successfully, the **Version** column displays 6.1 and **Status** displays Deployed.

NSX Edge firewall rules do not support sourcePort, so version 5.5 Edge rules containing sourcePort are modified during the upgrade as follows.

- If there are no applications used in the rule, a service is created with protocol=any, port=any and sourcePort=asDefinedInTheRule.
- If there are applications or applicationGroups used in the rule, these grouping objects are duplicated by adding the sourcePort to them. Because of this, the groupingObjectIds used in the firewall rule change after the upgrade.

Upgrade to Guest Introspection 6.1

You can upgrade only from vShield Endpoint 5.5 to Guest Introspection 6.1. If you have a prior version of vShield Endpoint in your infrastructure, you must first upgrade to version 5.5 and then to version 6.1. For information on upgrading to version 5.5, see *vShield Installation and Upgrade Guide* version 5.5.

Prerequisites


- dvSwitch has been created and all hosts are connected to the dvSwitch and dvPort group.
- Shared data store has been attached to the hosts.
- vShield Manager has been upgraded to NSX Manager.
- Virtual wires have been upgraded to NSX logical switches.

Procedure

- 1 In the **Installation** tab, click **Service Deployments**.

vShield Endpoint 5.5 deployments are displayed and the **Installation Status** column says **Upgrade Available**.

- 2 Select the vShield Endpoint 5.5 deployment that you want to upgrade.

The **Upgrade** () icon in the toolbar above the services table is enabled.

3 Click the **Upgrade** () icon.

4 Select the Datastore and Network and click **OK**.

After Guest Introspection is upgraded, the Guest Introspection service virtual machines are visible in the vCenter Server inventory.

Upgrade to NSX Data Security 6.1

NSX Data Security does not support a direct upgrade. You must uninstall the current Data Security software before upgrading to NSX Manager. After NSX Manager is upgraded, you can install NSX Data Security version 6.0. If you upgraded to NSX Manager without uninstalling Data Security, you must uninstall Data Security using a REST call.

Pre-NSX Data Security policies and violation reports are carried over to the vSphere Web Client, but you can run a Data Security scan only after installing NSX Data Security version 6.1.

For information on installing Data Security, see [“Install Data Security,”](#) on page 34.

Upgrade Partner Solutions to NSX 6.1

There is no upgrade path for partner solutions. Legacy partner solutions work at a global level, but you cannot add these solutions to a Service Composer policy.

When an upgrade is available for a partner solution installed through the Service Deployments tab, the status column displays Upgrade available. You can upgrade the solution through this tab.

Upgrade NSX 6.0.x to NSX 6.1

To upgrade to NSX 6.0.x, you must first upgrade the NSX Manager, and then upgrade the other components in the order in which they are documented.

NSX components must be upgraded in the following order:

- 1 NSX Manager
- 2 NSX controller
- 3 Clusters and Logical Switches
- 4 NSX Edge
- 5 Guest Introspection and Data Security

The upgrade process is managed by the NSX Manager. If the upgrade of a component fails or is interrupted and you need to repeat or restart the upgrade, the process begins from the point at which it stopped; it does not start over from the beginning.

The upgrade status is updated for each node and at the cluster level.

Upgrade NSX Manager from 6.0.x to 6.1

Prerequisites

It is recommended that you back up your current configuration before upgrading. See Operations and Management in *NSX Administration Guide*.

Procedure

- 1 Download the NSX vSphere 6.1 upgrade bundle to a location to which NSX Manager can browse. The name of the upgrade bundle file is something like `VMware-NSX-Manager-upgrade-bundle-releaseNumber-NSXbuildNumber.tar.gz`.

- 2 Log in to the NSX Manager Virtual Appliance.
- 3 On the NSX Manager Virtual Appliance Management page, click **Upgrade**.
- 4 Click **Upgrade** next to Upgrade NSX Management Service.
- 5 Click **Browse** and select the `VMware-NSX-Manager-upgrade-bundle-releaseNumber-NSXbuildNumber.tar.gz` file you downloaded in Step 1.
- 6 Click **Continue**.
- 7 In the Upgrade dialog box, specify whether you want to enable SSH and click **Upgrade**.
Wait until the upgrade procedure completes and the NSX Manager login page appears.
- 8 Log in to the NSX Manager Virtual Appliance again and confirm that version and build number on the top right matches the upgrade bundle you just installed.

Upgrade Controllers

The controllers in your environment are upgraded at the cluster level. If an upgrade is available for a controller node, an upgrade link appears in the NSX Manager.

It is recommended that you upgrade the controllers during a maintenance window.

Prerequisites

- Ensure that all of the controllers are in the normal state. Upgrading is not possible when the controllers are in the disconnected state.
- Ensure that the cluster has formed a majority (quorum). The upgrade cannot be launched without a majority. A majority is best achieved with an odd number, such as three or five nodes.

During the upgrade, when there is a temporary non-majority state, existing virtual machines do not lose networking. However, newly created virtual machines might drop traffic. We recommend that you not provision new VMs, move VMs, or allow DRS to move VMs during the upgrade.

New network creation is automatically blocked during the upgrade.

- Back up the controller data by taking a snapshot before you start the upgrade process.
 - a Note the controller ID (Name column in the NSX Controller nodes table) and IP addresses (Node column) of each controller.
 - b Take a snapshot of each controller using the following REST API call:

GET `https://NSXManagerIPAddress/api/2.0/vdn/controller/controllerID/snapshot`

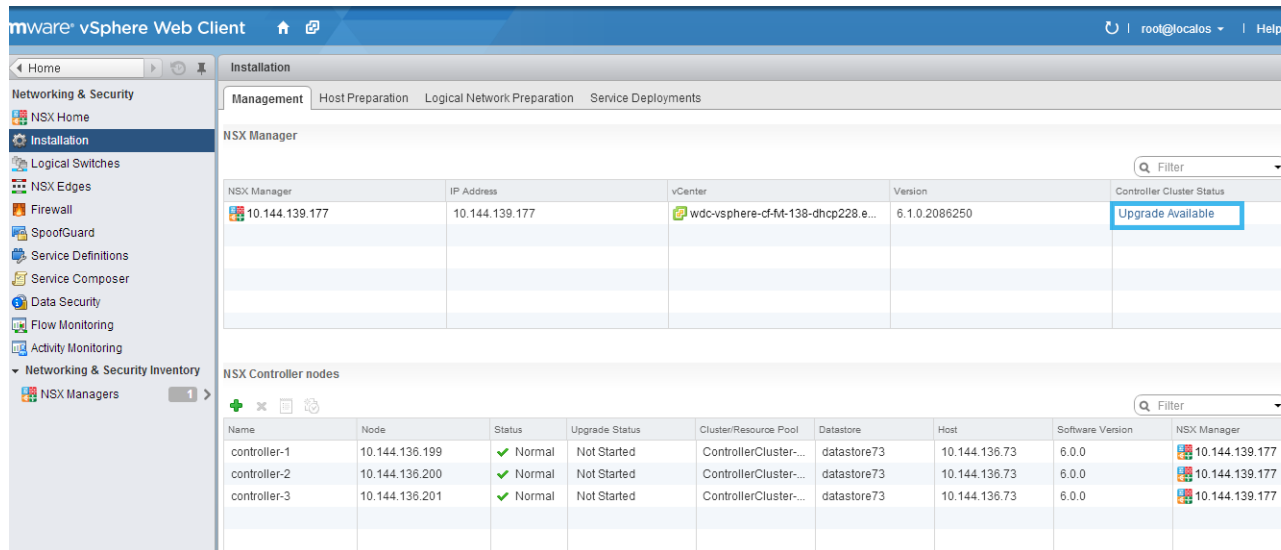
The output of the GET call is an octet stream containing the controller snapshot. To download the snapshot, use the following REST API call:

```
curl -u admin:default -H "Accept: application/octet-stream" -X GET -k
https://NSXManagerIPAddress/api/2.0/vdn/controller/controllerID/snapshot >
controller_backup.snapshot
```

Procedure

- 1 Log in to the vCenter Web Client.
- 2 Click **Networking & Security** and then click **Installation**.

- 3 In the NSX Manager section, click **Upgrade Available** in the **Controller Cluster Status** column.



The controllers in your environment are upgraded and rebooted one at a time. After you initiate the upgrade, the system downloads the upgrade file, upgrades each controller, reboots each controller, and updates the upgrade status of each controller. The following fields display controller status:

- The **Controller Cluster Status** column in the NSX Manager section displays the upgrade status of the cluster. When the upgrade begins, the status says **Downloading upgrade file**. When the upgrade file has been downloaded on all controllers in the cluster, the status changes to **In progress**. After all the controllers in the cluster have been upgraded, the status displayed is **Complete**, and then this column is no longer displayed.
- The **Status** column in the NSX Controller nodes section displays the status of each controller, which is **Normal** to begin with. When the controller services are shut down and the controller is rebooted, the status changes to **Disconnected**. After the upgrade for that controller is complete, the status is **Normal** again.
- The **Upgrade Status** column in the NSX Controller nodes section displays the upgrade status for each controller. The status displays **Downloading upgrade file** to begin with, then displays **Upgrade in progress**, and then **Rebooting**. After the controller is upgraded, the status displays **Upgraded**.

When the upgrade is complete, the **Software Version** column in the NSX Controller nodes section displays **6.1.buildNumber** for each controller.

The average upgrade time for each upgrade does not complete within the timeout period (30 minutes), the **Upgrade Status** column displays **Failed**. Click **Upgrade Available** in the NSX Manager section again to resume the upgrade. If the controller upgrade does not complete within the timeout period (30 minutes), the **Upgrade Status** column displays **Failed**. Click **Upgrade Available** in the NSX Manager section again to resume the upgrade process from the point where it stopped.

If network issues are preventing a successful upgrade within the 30-minute timeout period, you may need to configure a longer timeout period. Work with VMware Support to diagnose and resolve any underlying issues and, if needed, configure longer timeout period.

If the controller upgrade fails, relaunch the upgrade or contact VMware support for help in restoring the controller snapshot. The snapshot is only for controller data of the same version. Snapshots cannot be restored on a newer version. In other words, do not try to apply a snapshot to a successfully upgraded controller.

There is a scenario in which the first controller upgrades successfully, and the second controller does not. Assume you have three controllers in a cluster, the first controller is successfully upgraded to the new version, and the second controller is being upgraded. If the upgrade of the second controller fails, the second controller might be left in a disconnected state. At the same time, the first and third controllers now have two different versions (one upgraded, one not) and are therefore unable to form a majority. At this point, the upgrade cannot be relaunched. To work around this scenario, create another controller. The newly created controller will be of the older version (matching controller three) and will therefore form a majority with controller three. At this point, you can relaunch the upgrade procedure.

Upgrade Clusters from 6.0.x to 6.1

After upgrading NSX Manager and NSX controllers to version 6.1, you must update the appropriate clusters in your environment. During this process, each host in the cluster receives a software update and is then rebooted.

Prerequisites

NSX Manager and NSX controllers have been upgraded.

Procedure

- 1 On the **Installation** tab, click **Host Preparation**.
- 2 For each cluster that you want to upgrade, click **Update**.

Each host in the cluster is put into maintenance mode (which vMotions all running virtual machines to other hosts in the cluster) and is then rebooted. If hosts require manual intervention to enter maintenance mode (for example, due to HA requirements or DRS rules), the upgrade process stops and the cluster **Installation Status** displays **Not Ready**. Click ▲ to display the errors. You may need to migrate the virtual machines manually and then click **Resolve** to complete the upgrade.

When the cluster is updated, the **Installation Status** column displays the software version that you have updated to.

Upgrade NSX Edge from 6.0.x to 6.1

Prerequisites

- NSX Manager has been upgraded to 6.1.
- Controllers and prepared clusters have been upgraded to 6.1.

Procedure

- 1 In the vSphere Web Client, select **Networking & Security** > **NSX Edges**.
- 2 For each NSX Edge instance, select **Upgrade Version** from the **Actions** menu.

After the NSX Edge is upgraded successfully, the **Version** column displays the 6.1 version that you upgraded to.

Upgrade Guest Introspection and Data Security from 6.0.x to 6.1

Prerequisites

NSX Manager, controllers, prepared clusters, and NSX Edges must have been upgraded to 6.1.

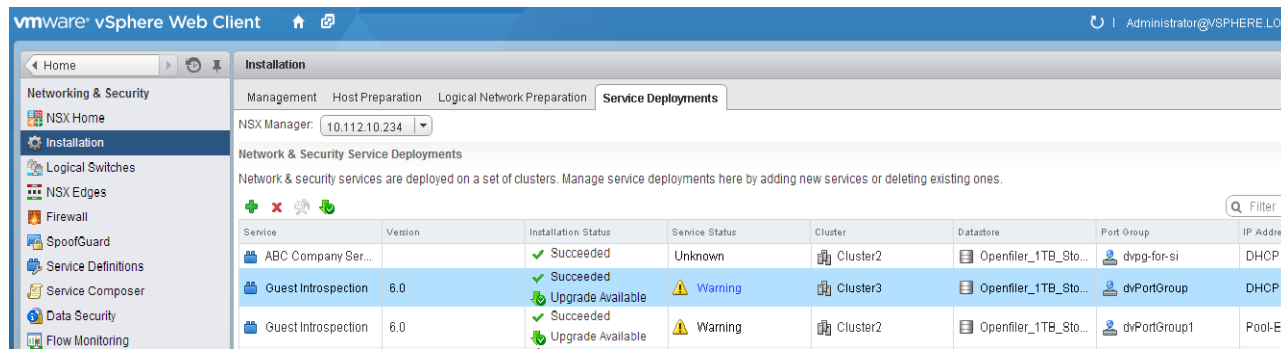
Procedure

- 1 In the **Installation** tab, click **Service Deployments**.

Guest Introspection and Data security 6.0 deployments are displayed, and the **Installation Status** column says **Upgrade Available**.

- 2 Select the Guest Introspection deployment that you want to upgrade.

The **Upgrade** (📌) icon in the toolbar above the services table is enabled.



- 3 Click the **Upgrade** (📌) icon and follow the UI prompts.

After Guest Introspection is upgraded, the Guest Introspection service virtual machines are visible in the vCenter Server inventory.

- 4 Select the Data Security deployment that you want to upgrade.
- 5 Click the **Upgrade** (📌) icon and follow the UI prompts.

Upgrade NSX 6.1 to NSX 6.1.1

You can upgrade to NSX 6.1.1 only from NSX 6.1. If you have a prior version of NSX in your infrastructure, you must first upgrade to version 6.1 and then to NSX 6.1.1.

NSX components must be upgraded in the following order:

- 1 NSX Manager
- 2 NSX controller
- 3 Clusters and Logical Switches
- 4 NSX Edge
- 5 Guest Introspection and Data Security

The upgrade process is managed by the NSX Manager. If the upgrade of a component fails or is interrupted and you need to repeat or restart the upgrade, the process begins from the point at which it stopped; it does not start over from the beginning.

The upgrade status is updated for each node and at the cluster level.

Upgrade NSX Manager from 6.1 to 6.1.1

Prerequisites

It is recommended that you back up your current configuration before upgrading. See Operations and Management in *NSX Administration Guide*.

Procedure

- 1 Download the NSX vSphere 6.1.1 upgrade bundle to a location to which NSX Manager can browse. The name of the upgrade bundle file is something like `VMware-NSX-Manager-upgrade-bundle-releaseNumber-NSXbuildNumber.tar.gz`.
- 2 Log in to the NSX Manager Virtual Appliance.
- 3 On the NSX Manager Virtual Appliance Management page, click **Upgrade**.
- 4 Click **Upgrade** next to Upgrade NSX Management Service.
- 5 Click **Browse** and select the `VMware-NSX-Manager-upgrade-bundle-releaseNumber-NSXbuildNumber.tar.gz` file you downloaded in Step 1.
- 6 Click **Continue**.
- 7 In the Upgrade dialog box, specify whether you want to enable SSH and click **Upgrade**.
Wait until the upgrade procedure completes and the NSX Manager login page appears.
- 8 Log in to the NSX Manager Virtual Appliance again and confirm that version and build number on the top right matches the upgrade bundle you just installed.

Upgrade Controllers from 6.1 to 6.1.1

The controllers in your environment are upgraded at the cluster level. If an upgrade is available for a controller node, an upgrade link appears in the NSX Manager.

It is recommended that you upgrade the controllers during a maintenance window.

Prerequisites

- Ensure that all of the controllers are in the normal state. Upgrading is not possible when the controllers are in the disconnected state.
- Ensure that the cluster has formed a majority (quorum). The upgrade cannot be launched without a majority. A majority is best achieved with an odd number, such as three or five nodes.

During the upgrade, when there is a temporary non-majority state, existing virtual machines do not lose networking. However, newly created virtual machines might drop traffic. We recommend that you not provision new VMs, move VMs, or allow DRS to move VMs during the upgrade.

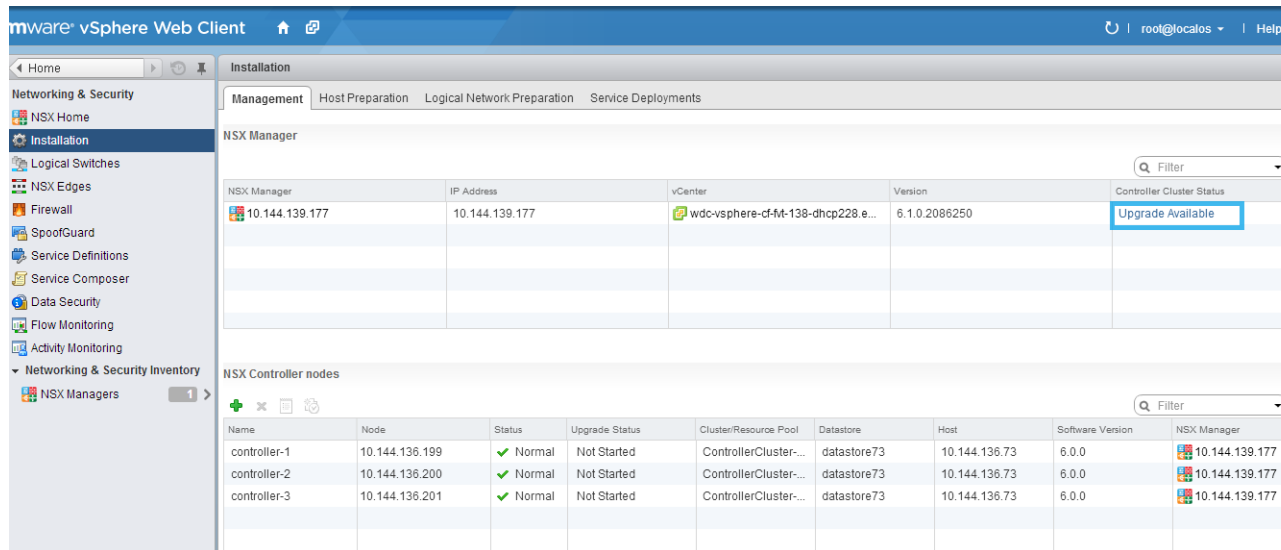
New network creation is automatically blocked during the upgrade.

- Back up the controller data by taking a snapshot before you start the upgrade process.

Procedure

- 1 Log in to the vCenter Web Client.
- 2 Click **Networking & Security** and then click **Installation**.

- 3 In the NSX Manager section, click **Upgrade Available** in the **Controller Cluster Status** column.



The controllers in your environment are upgraded and rebooted one at a time. After you initiate the upgrade, the system downloads the upgrade file, upgrades each controller, reboots each controller, and updates the upgrade status of each controller. The following fields display controller status:

- The **Controller Cluster Status** column in the NSX Manager section displays the upgrade status of the cluster. When the upgrade begins, the status says **Downloading upgrade file**. When the upgrade file has been downloaded on all controllers in the cluster, the status changes to **In progress**. After all the controllers in the cluster have been upgraded, the status displayed is **Complete**, and then this column is no longer displayed.
- The **Status** column in the NSX Controller nodes section displays the status of each controller, which is **Normal** to begin with. When the controller services are shut down and the controller is rebooted, the status changes to **Disconnected**. After the upgraded for that controller is complete, the status is **Normal** again.
- The **Upgrade Status** column in the NSX Controller nodes section displays the upgrade status for each controller. The status displays **Downloading upgrade file** to begin with, then displays **Upgrade in progress**, and then **Rebooting**. After the controller is upgraded, the status displays **Upgraded**.

When the upgrade is complete, the **Software Version** column in the NSX Controller nodes section displays **6.1.1.buildNumber** for each controller.

The average upgrade time for ea upgrade does not complete within the timeout period (30 minutes), the **Upgrade Status** column displays **Failed**. Click **Upgrade Available** in the NSX Manager section again to resume the ch controller is 6-8 minutes. If the controller upgrade does not complete within the timeout period (30 minutes), the **Upgrade Status** column displays **Failed**. Click **Upgrade Available** in the NSX Manager section again to resume the upgrade process from the point where it stopped.

If network issues are preventing a successful upgrade within the 30-minute timeout period, you may need to configure a longer timeout period. Work with VMware Support to diagnose and resolve any underlying issues and, if needed, configure longer timeout period.

If the controller upgrade fails, relaunch the upgrade or contact VMware support for help in restoring the controller snapshot. The snapshot is only for controller data of the same version. Snapshots cannot be restored on a newer version. In other words, do not try to apply a snapshot to a successfully upgraded controller.

There is a scenario in which the first controller upgrades successfully, and the second controller does not. Assume you have three controllers in a cluster, the first controller is successfully upgraded to the new version, and the second controller is being upgraded. If the upgrade of the second controller fails, the second controller might be left in a disconnected state. At the same time, the first and third controllers now have two different versions (one upgraded, one not) and are therefore unable to form a majority. At this point, the upgrade cannot be relaunched. To work around this scenario, create another controller. The newly created controller will be of the older version (matching controller three) and will therefore form a majority with controller three. At this point, you can relaunch the upgrade procedure.

Upgrade Clusters from 6.1 to 6.1.1

After upgrading NSX Manager and NSX controllers to version 6.1, you must update the appropriate clusters in your environment. During this process, each host in the cluster receives a software update and is then rebooted.

Prerequisites

NSX Manager and NSX controllers have been upgraded.

Procedure

- 1 In the **Installation** tab, click **Host Preparation**.
- 2 For each cluster that you want to upgrade, click **Update**.

Each host in the cluster is put into maintenance mode (which vMotions all running virtual machines to other hosts in the cluster) and is then rebooted. If hosts require manual intervention to enter maintenance mode (for example, due to HA requirements or DRS rules), the upgrade process stops and the cluster **Installation Status** displays **Not Ready**. Click ▲ to display the errors. You may need to migrate the virtual machines manually and then click **Resolve** to complete the upgrade.

When the cluster is updated, the **Installation Status** column displays the software version that you have updated to.

Upgrade NSX Edge from 6.1 to 6.1.1

Prerequisites

- NSX Manager has been upgraded to 6.1.
- Controllers and prepared clusters have been upgraded to 6.1.

Procedure

- 1 In the vSphere Web Client, select **Networking & Security** > **NSX Edges**.
- 2 For each NSX Edge instance, select **Upgrade Version** from the **Actions** menu.

After the NSX Edge is upgraded successfully, the **Version** column displays the 6.1.1 version that you upgraded to.

Upgrade Guest Upgrade Guest Introspection and Data Security from 6.1 to 6.1.1

Prerequisites


NSX Manager, controllers, prepared clusters, and NSX Edges must have been upgraded to 6.1.


Procedure

- 1 In the **Installation** tab, click **Service Deployments**.

Guest Introspection and Data security 6.0 deployments are displayed, and the **Installation Status** column says **Upgrade Available**.


- 2 Select the Guest Introspection deployment that you want to upgrade.

The **Upgrade** () icon in the toolbar above the services table is enabled.

- 3 Click the **Upgrade** () icon and follow the UI prompts.

After Guest Introspection is upgraded, the Guest Introspection service virtual machines are visible in the vCenter Server inventory.

- 4 Select the Data Security deployment that you want to upgrade.

- 5 Click the **Upgrade** () icon and follow the UI prompts.

Uninstalling NSX Components

This chapter details the steps required to uninstall NSX components from your vCenter inventory.

This chapter includes the following topics:

- [“Uninstall an NSX Edge,”](#) on page 53
- [“Uninstall an NSX Data Security Virtual Machine,”](#) on page 53
- [“Uninstall a Guest Introspection Module,”](#) on page 54
- [“Uninstall Network Virtualization Components,”](#) on page 54

Uninstall an NSX Edge

You can uninstall an NSX Edge from the vSphere Web Client.

Prerequisites

You must have been assigned the Enterprise Administrator or NSX Administrator role.

Procedure

- 1 Log in to the vSphere Web Client.
- 2 Click **Networking & Security** and then click **NSX Edges**.
- 3 Select an NSX Edge and click the **Delete** (✖) icon.

Uninstall an NSX Data Security Virtual Machine

After you uninstall the NSX Data Security virtual machine, you must uninstall the virtual appliance according to the instructions from the VMware partner.

Procedure

- 1 In the **Installation** tab, click **Service Deployments**.
- 2 Select the NSX Data Security service and click the **Delete Service Deployment** (✖) icon.
- 3 In the Confirm Delete dialog box, click **Delete now** or select a date and time for the delete to take effect.
- 4 Click **OK**.

Uninstall a Guest Introspection Module

To uninstall Guest Introspection, you must perform these steps in the following order.



CAUTION If NSX Data security or any partner services dependent on Guest Introspection are installed on a cluster, you must uninstall them before uninstalling the Guest Introspection service.

Uninstall Products that Use Guest Introspection

Before you uninstall a Guest Introspection module from a cluster, you must uninstall all products that are using Guest Introspection from the hosts on that cluster. Use the instructions from the solution provider.

Uninstall the Guest Introspection Module from the vSphere Client

Uninstalling a Guest Introspection module removes the Guest Introspection Module from a cluster.

Procedure

- 1 In the **Installation** tab, click **Service Deployments**.
- 2 Select the Guest Introspection service and click the **Delete Service Deployment** (✖) icon.
- 3 In the Confirm Delete dialog box, confirm that there are no warnings displayed.
- 4 Click **Delete now** or select a date and time for the delete to take effect.
- 5 Click **OK**.

Uninstall Network Virtualization Components

Uninstalling the network virtualization components from a cluster removes all VXLAN configuration and disables the ability to use logical switches, NSX Controller, Logical Router, and Firewall. VMware recommends that you uninstall the network virtualization components from a cluster before removing it from vCenter Server.

Prerequisites

Ensure that the cluster from which you are uninstalling network virtualization components is not part of any transport zone.

Procedure

- 1 In the **Installation** tab, click **Host Preparation**.
- 2 For the appropriate cluster, select **Uninstall** in the Installation Status column.

Troubleshooting Installation Issues

This section describes installation issues.

This chapter includes the following topics:

- [“Unable to Configure Lookup Service,”](#) on page 55
- [“Unable to Configure vCenter Server,”](#) on page 55

Unable to Configure Lookup Service

Problem

Cannot configure lookup service.

Solution

- 1 Confirm that the user has **admin** privileges.
- 2 Verify whether NSX Manager and Lookup service appliances are in time sync. To achieve this, use same NTP server configurations at NSX Manager and Lookup service.
- 3 Check DNS settings for name resolution.

Unable to Configure vCenter Server

Problem

Cannot configure vCenter Server.

Solution

- 1 Check DNS settings.
- 2 Confirm that user has administrative privileges.

Index

C

client requirements **13**

D

default gateway, configuring IP address **27**

G

GUI, logging in **17**

I

install

Guest Introspection **32**

partner appliance **37**

installation

licenses **19**

NSX Endpoint thin agent **34**

NSX Manager **16**

installing, NSX Edge **25**

introduction, NSX **8**

L

licensing, installation **19**

logging in to the GUI **17**

Logical Firewall **21**

logical switch

add NSX controller **20**

assign segment ID pool & multicast address
range **23**

configure VXLAN **21**

N

NSX

consumption platform **9**

control plane **9**

data plane **9**

management plane **9**

overview **7**

services **10**

NSX Edge

install as router **29**

install as services gateway **25**

installation **25**

licensing **19**

uninstall **53**

NSX Endpoint

licensing **19**

thin agent installation **34**

NSX Manager

installation **16**

logging in to GUI **17**

syncing with vCenter **17**

NSX vSwitch, install **21**

NSX controller **20**

S

synchronizing with vCenter **17**

system requirements **13**

T

thin agent installation **34**

troubleshoot, configure lookup service **55**

troubleshooting, unable to configure vCenter
Server **55**

U

uninstall

firewall **54**

network virtualization components **54**

NSX Data Security **53**

NSX Edge **53**

vShield Endpoint module **54**

unregister a vShield Endpoint SVM **54**

upgrade, controller **45**

V

vCenter, syncing from NSX Manager **17**

vShield Endpoint

uninstall **54**

unregister SVM **54**

