NSX-T Data Center Migration Coordinator Guide

Modified on 10 SEPTEMBER 2020
VMware NSX-T Data Center 2.5

vmware®

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

https://docs.vmware.com/

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

Contents

NSX-T Data Center Migration Coordinator Guide

The *NSX-T Data Center Migration Coordinator Guide* provides information about migrating a VMware NSX® for vSphere® environment to an VMware NSX-T™ environment using the migration coordinator utility.

It also includes information about migrating networking configurations from VMware vSphere® to an NSX-T Data Center environment using the migration coordinator.

Intended Audience

This manual is intended for anyone who wants to use the migration coordinator utility to migrate an NSX Data Center for vSphere environment or vSphere networking to an NSX-T Data Center environment. The information is written for experienced network and system administrators who are familiar with virtual machine technology and datacenter operations.

Migrating NSX Data Center for vSphere

1

You can use the migration coordinator to migrate your NSX Data Center from an existing NSX for vSphere environment to an empty NSX-T environment.

Important The migration causes traffic outages during Edge and Host migration steps. You must complete the migration within a single maintenance window. Contact your VMware support team before attempting the migration.

This chapter includes the following topics:

Understanding the NSX Data Center for vSphere Migration

Migrating from NSX for vSphere to NSX-T requires planning and preparation. You should be familiar with NSX-T concepts and administration tasks before you migrate.

Preparation might involve modifying your existing NSX for vSphere environment in addition to setting up the new NSX-T environment.

Features Supported by Migration Coordinator

A subset of NSX Data Center for vSphere features are supported by migration coordinator.

Most features have some limitations. If you import your NSX Data Center for vSphere configuration to migration coordinator you get detailed feedback of what features and configurations in your environment are supported or not supported.

See Detailed Feature Support for Migration Coordinator for detailed information about what is supported by migration coordinator.

Table 1-1. Support Matrix for Migration Coordinator

NSX Data Center for vSphere Feature	Supported	Details and Limitations
VLAN-backed logical switches	Yes	
Overlay-backed logical switches	Yes	
L2 Bridges	No	
Transport Zones	Yes	
Routing	Yes	See Topologies Supported by Migration Coordinator for details.
East-West Micro-Segmentation	Yes	
Edge Firewall	Yes	
NAT	Yes	
L2 VPN	Yes	
L3 VPN	Yes	
Load Balancer	Yes	
DHCP and DNS	Yes	
Distributed Firewall	Yes	
Service Composer	Yes	Only firewall rules are migrated. Guest Introspection rules and Network Introspection rules are not migrated.
Grouping objects	Yes	Limitations include number of items, and dynamic expressions making up security groups.
Guest Introspection	No	
Network Introspection	No	
Endpoint Protection	No	
Cross-vCenter NSX	No	
NSX Data Center for vSphere with a Cloud Management Platform, Integrated Stack Solution, or PaaS Solution.	No	Contact your VMware representative before proceeding with migration. Scripts and integrations might break if you migrate.

Detailed Feature Support for Migration Coordinator

Platform Support

See the VMware Interoperability Matrix for supported versions of ESXi and vCenter Server: http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php#interop&175=&1=&2=.

Configuration	Supported	Details
NSX Data Center for vSphere with vSAN or iSCSI on vSphere Distributed Switch	Yes	
Pre-existing NSX-T configuration	No	Deploy a new NSX-T environment to be the destination for the NSX for vSphere migration. During the **Import Configuration** step, all Edge node interfaces in the destination NSX-T environment are shut down. If the destination NSX-T environment is already configured and is in use, starting the configuration import will interrupt traffic.
Cross vCenter NSX	No	
NSX Data Center for vSphere with a Cloud Management Platform, Integrated Stack Solution, or PaaS Solution	No	Contact your VMware representative before proceeding with migration. Scripts and integrations might break if you migrate. For example: ■ NSX Data Center for vSphere and vRealize Automation ■ NSX for vSphere and VMware Integrated Openstack ■ NSX for vSphere and vCloud Director ■ NSX for vSphere with Integrated Stack Solution ■ NSX for vSphere with PaaS Solution such as Pivotal Cloud Foundry, RedHat OpenShift ■ NSX for vSphere with vRealize Operations workflows

vSphere and ESXi Features

Configuration	Supported	Details
ESXi host already in maintenance mode (no VMs)	Yes	
Network I/O Control (NIOC) version 3	Yes	
Network I/O Control (NIOC) version 2	No	
Network I/O Control (NIOC) having vNIC with reservation	No	
vSphere Standard Switch	No	VMs and VMKernel interfaces on VSS are not migrated. NSX Data Center for vSphere features applied to the VSS cannot be migrated.

Configuration	Supported	Details
Stateless ESXi	No	
Host profiles	No	
ESXi lockdown mode	No	Not supported in NSX-T.
ESXi host pending maintenance mode task.	No	
Disconnected ESXi host in vCenter cluster	No	
vSphere FT	No	
vSphere DRS fully automated	No	Put DRS into manual mode before running migration coordinator
vSphere High Availability	No	
Traffic filtering ACL	No	
vSphere Health Check	No	
SRIOV	No	
vmknic pinning to physical NIC	No	
Private VLAN	No	
Ephemeral dvPortGroup	No	
DirectPath IO	No	
L2 security	No	
Learn switch on virtual wire	No	
Hardware Gateway (Tunnel endpoint integration with physical switching hardware)	No	
SNMP	No	
Disconnected vNIC in VM	No	Due to ESX 6.5 limitation, stale entries might present on DVFilter for disconnected VMs. Reboot the VM as a work-around.
VXLAN port number other than 4789	No	
Multicast Filtering Mode	No	

NSX Manager Appliance System Configuration

Configuration	Supported	Details
NTP server/time setting	Yes	
Syslog server configuration	Yes	

Configuration	Supported	Details
Backup configuration	Yes	If needed, change NSX Data Center for vSphere passphrase to match NSX-T Data Center requirements. It must be at least 8 characters long and contain the following: ■ At least one lowercase letter ■ At least one uppercase letter ■ At least one numeric character ■ At least one special character
FIPS	No	FIPS on/off not supported by NSX-T.
Locale	No	NSX-T only supports English locale
Appliance certificate	No	

Role-Based Access Control

Configuration	Supported	Details
Local users	No	
NSX roles assigned to a vCenter user added via LDAP	Yes	vSphere Identity Manager must be installed and configured to migrate user roles for LDAP users.
NSX roles assigned to a vCenter group	No	

Certificates

Configuration	Supported	Details
Certificates (Server, CA signed)	Yes	This applies to certificates added through truststore APIs only.

Operations

Details	Supported	Notes
Discovery protocol CDP	No	
Discovery protocol LLDP	Yes	The listen mode is turned on by default and can't be changed in NSX-T. Only the Advertise mode can be modified.
PortMirroring: ■ Encapsulated remote Mirroring Source (L3)	Yes	Only L3 session type is supported for migration
PortMirroring: ■ Distributed PortMirroring ■ Remote Mirroring Source ■ Remote Mirroring Destination ■ Distributed Port Mirroring (legacy)	No	
L2 IPFIX	Yes	Lag with IPFIX is not supported

Details	Supported	Notes
Distributed Firewall IPFIX	No	
MAC Learning	Yes	You must enable (accept) forged transmits.
Hardware VTEP	No	
Promiscuous Mode	No	
Resource Allocation	No	vNIC enabled with resource allocation is not supported
IpFix – Internal flows	No	IpFix with InternalFlows is not supported

Switch

Configuration	Supported	Details
L2 Bridging	No	
Trunk VLAN	Yes	Trunk uplink portgroups must be configured with a VLAN range of 0-4094. NSX Edgenodes require to be connected through trunk portgroups.
VLAN Configuration	Yes	Only Lag with VLAN configuration is not supported
Teaming and Failover: ■ Load Balancing ■ Uplink Failover Order	Yes	Supported options for load balancing (teaming policy): ■ Use explicit failover order ■ Route based on source MAC hash Other load balancing options are not supported.
Teaming and Failover: ■ Network Failure Detection ■ Notify Switches ■ Reverse Policy ■ Rolling Order	No	

Switch Security and IP Discovery

Configuration	Supported	Details
IP Discovery (ARP, ND, DHCPv4 and DHCPv6)	Yes	The following binding limits apply on NSX-T for migration: ■ 128 for ARP discovered IPs ■ 128 for DHCPv4 discovered IPs ■ 15 for DHCPv6 discovered IPs ■ 15 for ND discovered IPs
SpoofGuard (Manual, TOFU, Disabled)	Yes	

Configuration	Supported	Details
Switch Security (BPDU Filter, DHCP client block, DHCP server block, RA guard)	Yes	
Migrating datapath bindings from Switch Security module in NSX Data Center for vSphere to Switch security module in NSX-T	Yes	If SpoofGuard is enabled, bindings are migrated from the Switch Security module to support ARP suppression. VSIP – Switch security not supported as VSIP bindings are migrated as statically configured rules.
Discovery profiles	Yes	The ipdiscovery profiles are created after migration using the IP Discovery configuration for the logical switch and the global and cluster ARP and DHCP configuration.

Central Control Plane

Configuration	Supported	Details
VTEP replication per logical switch (VNI) and routing domain	Yes	
MAC/IP replication	No	
NSX Data Center for vSphere transport zones using multicast or hybrid replication mode	No	
NSX Data Center for vSphere transport zones using unicast replication mode	Yes	

NSX Edge Features

For full details on supported topologies, see Topologies Supported by Migration Coordinator.

Configuration	Supported	Details
Routing between Edge Service Gateway and northbound router or virtual tunnel interface	Yes	BGP is supported. Static routes are supported. OSFP is not supported.
Routing between Edge Services Gateway and Distributed Logical router	Yes	Routes are converted to static routes after migration.
Load balancer	Yes	See Topologies Supported by Migration Coordinator for details.
VLAN-backed Micro-Segmentation environment	Yes	See Topologies Supported by Migration Coordinator for details.
NAT64	No	Not supported in NSX-T.

Configuration	Supported	Details
Node level settings on Edge Services Gateway or Distributed Logical Router	No	Node level settings, for example, syslog or NTP server, are not supported.
IPv6	No	
Unicast Reverse Path Filter (URPF) configuration for Edge Services Gateway interfaces	No	URPF on NSX-T gateway interfaces is set to Strict.
Maximum Transmission Unit (MTU) configuration Edge Services Gateway interfaces	No	See Modify NSX Edge Node Configuration Before Migrating Edges for information about changing the default MTU on NSX-T.
IP Multicast routing	No	
Route Redistribution Prefix Filters	No	
Default originate	No	Not supported in NSX-T.

Edge Firewall

Configuration	Supported	Details
Firewall Section: Display name	Yes	Firewall sections can have a maximum of 1000 rules. If a section contains more than 1000 rules, it is migrated as multiple sections.
Action for default rule	Yes	NSX Data Center for vSphere API: GatewayPolicy/action NSX-T API: SecurityPolicy.action
Firewall Global Configuration	No	Default timeouts are used
Firewall Rule	Yes	NSX Data Center for vSphere API: firewallRule NSX-T API: SecurityPolicy
Firewall Rule: name	Yes	
Firewall Rule: rule tag	Yes	NSX Data Center for vSphere API: ruleTag NSX-T API: Rule_tag
Sources and destinations in firewall rules: ■ Grouping objects ■ IP addresses	Yes	NSX Data Center for vSphere API: ■ source/groupingObjectId ■ source/ipAddress NSX-T API: ■ source_groups NSX Data Center for vSphere API: ■ destination/groupingObjectId ■ destination/ipAddress NSX-T API: ■ destination_groups

Configuration	Supported	Details
Firewall rule sources and destinations: ■ vNIC Group	No	
Services (applications) in firewall rules: ■ Service ■ Service Group ■ Protocol/port/source port	Yes	NSX Data Center for vSphere API: ■ application/applicationId ■ application/service/protocol ■ application/service/port ■ application/service/sourcePort NSX-T API: ■ Services
Firewall Rule: Match translated	No	Match translated must be ‘false’.
Firewall Rule: Direction	Yes	Both APIs: direction
Firewall Rule: Action	Yes	Both APIs: action
Firewall Rule: Enabled	Yes	Both APIs: enabled
Firewall Rule: Logging	Yes	NSX Data Center for vSphere API: logging NSX-T API: logged
Firewall Rule: Description	Yes	Both APIs: description

Edge NAT

Configuration	Supported	Details
NAT rule	Yes	NSX Data Center for vSphere API: natRule NSX-T API: /nat/USER/nat-rules
NAT rule: rule tag	Yes	NSX Data Center for vSphere API: ruleTag NSX-T API: rule_tag
NAT rule: action	Yes	NSX Data Center for vSphere API: action NSX-T API: action
NAT rule: original address (Source address for SNAT rules, and the destination address for DNAT rules.)	Yes	NSX Data Center for vSphere API: originalAddress NSX-T API: source_network for SNAT rule or destination_network for DNAT rule
NAT rule: translatedAddress	Yes	NSX Data Center for vSphere API: translatedAddress NSX-T API: translated_network
NAT rule: Applying NAT rule on a specific interface	No	Applied on must be “any”.
NAT rule: logging	Yes	NSX Data Center for vSphere API: loggingEnabled NSX-T API: logging

Configuration	Supported	Details
NAT rule: enabled	Yes	NSX Data Center for vSphere API: enabled NSX-T API: disabled
NAT rule: description	Yes	NSX Data Center for vSphere API: description NSX-T API: description
NAT rule: protocol	Yes	NSX Data Center for vSphere API: protocol NSX-T API: Service
NAT rule: original port (source port for SNAT rules, destination port for DNAT rules)	Yes	NSX Data Center for vSphere API: originalPort NSX-T API: Service
NAT rule: translated port	Yes	NSX Data Center for vSphere API: translatedPort NSX-T API: Translated_ports
NAT rule: Source address in DNAT rule	Yes	NSX Data Center for vSphere API: dnatMatchSourceAddress NSX-T API: source_network
NAT rule: Destination address in SNAT rule	Yes	NSX Data Center for vSphere API: snatMatchDestinationAddress NSX-T API: destination_network
NAT rule: Source port in DNAT rule	Yes	NSX Data Center for vSphere API: dnatMatchSourcePort NSX-T API: Service
NAT rule: Destination port in SNAT rule	Yes	NSX Data Center for vSphere API: snatMatchDestinationPort NSX-T API: Service
NAT rule: rule ID	Yes	NSX Data Center for vSphere API: ruleID NSX-T API: id and display_name

L2VPN

Configuration	Supported	Details
L2VPN configuration based on IPSec using pre-shared key (PSK)	Yes	Supported if the networking being stretched over L2VPN is an overlay logical switch. Not supported for VLAN networks.
L2VPN configuration based on IPSec using certificate-based authentication	No	
L2VPN configuration based on SSL	No	

Configuration	Supported	Details
L2VPN configurations with local egress optimizations	No	
L2VPN client mode	No	

L3VPN

Configuration	Supported	Details
Dead Peer Detection	Yes	Dead Peer Detection supports different options on NSX Data Center for vSphere and NSX-T. You might want to consider using BGP for faster convergence or configure a peer to perform DPD if it is supported.
Changed Dead Peer Detection (dpd) default values for: ■ dpdtimeout ■ dpdaction	No	In NSX-T, dpdaction is set to “restart” and cannot be changed. If NSX Data Center for vSphere setting for dpdtimeout is set to 0, dpd is disabled in NSX-T. Otherwise, any dpdtimeout settings are ignored and the default value is used.
Changed Dead Peer Detection (dpd) default values for: ■ dpddelay	Yes	NSX Data Center for vSphere dpdelay maps to NSX-T dpdinternal.
Overlapping local and peer subnets of two or more sessions.	No	NSX Data Center for vSphere supports policy-based IPSec VPN sessions where the local and peer subnets of two or more sessions overlap with each other. This behavior is not supported on NSX-T. You must reconfigure the subnets so they do not overlap before you start the migration. If this configuration issue is not resolved, the Migrate Configuration step fails.
IPSec sessions with peer endpoint set as any.	No	Configuration is not migrated.

Configuration	Supported	Details
Changes to the extension securelocaltrafficbyip.	No	NSX-T Service Router doesn't have any local generated traffic that needs to be sent over tunnel.
Changes to these extensions: auto, sha2_truncbug, sareftrack, leftid, leftsendcert, leftxauthserver, leftxauthclient, leftxauthusername, leftmodecfgserver, leftmodecfgclient, modecfgpull, modecfgdns1, modecfgdns2, modecfgwins1, modecfgwins2, remote_peer_type, nm_configured, forceencaps,overlapip, aggrmode, rekey, rekeymargin, rekeyfuzz, compress, metric,disablearrivalcheck, failureshunt,leftnexthop, keyingtries	No	Those extensions are not supported on NSX-T and changes to them are not migrated.

Load Balancer

Configuration	Supported	Details
Monitor / health-checks for: ■ LDAP ■ DNS ■ MSSQL	No	If an unsupported monitor is configured, the monitor is ignored and the associated pool has no monitor configured. You can attach it to a new monitor after migration has finished.
Application rules	No	NSX Data Center for vSphere uses application rules based on HAProxy to support L7. In NSX-T, the rules are based on NGINX. The application rules cannot be migrated. You must create new rules after migration.
L7 virtual server port range	No	
IPv6	No	If IPv6 is used in virtual server, the whole virtual server would be ignored. If IPv6 is used in pool, the pool would be still migrated, however, the related pool member would be removed.
URL, URI, HTTPHEADER algorithms	No	If used in a pool, the pool is not migrated.
Isolated pool	No	The pool is not migrated.
LB pool member with different monitor port	No	The pool member which has different monitor port is not migrated.
Pool member minConn	No	Configuration is not migrated.
Monitor extension	No	Configuration is not migrated.

Configuration	Supported	Details
SSL sessionID persistence / table	No	Configuration is not migrated, and the associated virtual server has no persistence setting.
MSRDP persistence / session table	No	Configuration is not migrated, and the associated virtual server has no persistence setting.
Cookie app session / session table	No	Configuration is not migrated, and the associated virtual server has no persistence setting.
App persistence	No	Configuration is not migrated, and the associated virtual server has no persistence setting.
Monitor for: ■ Explicit escape ■ Quit ■ Delay	No	
Monitor for: ■ Send ■ Expect ■ Timeout ■ Interval ■ maxRetries	Yes	
Haproxy Tuning/IPVS Tuning	No	
Pool IP filter ■ IPv4 addresses	Yes	IPv4 IP addresses are supported. If Any is used, only the IPv4 addresses of the IP pool are migrated.
Pool IP Filter ■ IPv6 addresses	No	
Pool containing unsupported grouping object: ■ Cluster ■ Datacenter ■ Distributed port group ■ MAC set ■ Virtual App	No	If a pool includes an unsupported grouping object, those objects are ignored, and the pool is created with supported grouping object members. If there are no supported grouping object members, then an empty pool is created.

DHCP and DNS

Table 1-2. DHCP Configuration Topologies

Configuration	Supported	Details
DHCP Relay configured on Distributed Logical Router pointing to a DHCP Server configured on a directly connected Edge Services Gateway	Yes	The DHCP Relay server IP must be one of the Edge Services Gateway's internal interface IPs. The DHCP Server must be configured on an Edge Services Gateway that is directly connected to the Distributed Logical Router configured with the DHCP relay. It is not supported to use DNAT to translate a DHCP Relay IP that does not match an Edge Services Gateway internal interface.
DHCP Relay configured on Distributed Logical Router only, no DHCP Server configuration on connected Edge Services Gateway	No	
DHCP Server configured on Edge Services Gateway only, no DHCP Relay configuration on connected Distributed Logical Router	No	

Table 1-3. DHCP Features

Configuration	Supported	Details
IP Pools	Yes	
Static bindings	Yes	
DHCP leases	Yes	
General DHCP options	Yes	
Disabled DHCP service	No	In NSX-T you cannot disable the DHCP service. If there is a disabled DHCP service on NSX Data Center for vSphere it is not migrated.

DHCP option: "other"	No	The "other" field in dhcp options is not supported for migration.
		For example, dhcp option '80' is not migrated.
		`<dhcpOptions>`
		`  <other>`
		`  <code>80</code>`
		`  <value>2f766172</value>`
		`  </other>`
		`</dhcpOptions>`

Table 1-3. DHCP Features (continued)

Configuration	Supported	Details
Orphaned ip-pools/bindings	No	If ip-pools or static-bindings are configured on a DHCP Server but are not used by any connected logical switches, these objects are skipped from migration.
DHCP configured on Edge Service Gateway with directly connected logical switches	No	During migration, directly connected Edge Service Gateway interfaces are migrated as centralized service ports. However, NSX-T doesn't support DHCP service on a centralized service port, so the DHCP service configuration is not migrated for these interfaces.

Table 1-4. DNS Features

Configuration	Supported	Details
DNS views	Yes	Only the first dnsView is migrated to the NSX-T default DNS forwarder zone.
DNS configuration	Yes	You must provide available DNS listener IPs for all Edge Nodes. A message is displayed during Resolve Configuration to prompt for this.
DNS – L3 VPN	Yes	You must add the newly configured NSX-T DNS listener IPs into the remote L3 VPN prefix list. A message is displayed during Resolve Configuration to prompt for this.
DNS configured on Edge Service Gateway with directly connected logical switches	No	During migration, directly connected Edge Service Gateway interfaces are migrated as centralized service ports. However, NSX-T doesn't support DNS Service on a centralized service port, so the DNS Service configuration is not migrated for these interfaces.

Distributed Firewall

Configuration	Supported	Details
Identity-based Firewall	No	
Section - ■ Display name ■ Description ■ Tcp_strict ■ Stateless	Yes	If a firewall section has more than 1000 rules, then the migrator will migrate the rules in multiple sections of 1000 rules each.

Configuration	Supported	Details
Universal Sections	No	
Rule – Source / Destination: ■ IP Address / Range / CIDR ■ Logical Port ■ Logical Switch	Yes	
Rule – Source / Destination: ■ VM ■ Logical Port ■ Security Group / IP Set / MAC Set	Yes	maps to NSGroup
Rule – Source / Destination: ■ Cluster ■ Datacenter ■ DVPG ■ vSS ■ Host ■ Universal Logical Switch	No	
Rule – Applied To: ■ ANY	Yes	maps to Distributed Firewall
Rule – Applied To: ■ Security Group ■ Logical Port ■ Logical Switch ■ VM	Yes	maps to NSGroup
Rule – Applied To: ■ Cluster ■ Datacenter ■ DVPG ■ vSS ■ Host ■ Universal Logical Switch	No	
Rules Disabled in Distributed Firewall	Yes	
Disabling Distributed Firewall on a cluster level	No	When Distributed Firewall is enabled on NSX-T, it is enabled on all clusters. You cannot enable it on some clusters and disable on others.

Grouping Objects and Service Composer

IP Sets and MAC Sets are migrated to NSX-T Data Center as groups. See **Inventory > Groups** in the NSX-T Manager web interface.

Table 1-5. IP Sets and MAC Sets

Configuration	Supported	Details
IP Sets	Yes	IP sets with up to 2 million members (IP addresses, IP address subnets, IP ranges) can be migrated. IP sets with more members are not migrated.
Mac Sets	Yes	MAC sets with up to 2 million members can be migrated. MAC sets with more members are not migrated.

Security Groups are supported for migration with the limitations listed. Security Groups are migrated to NSX-T Data Center as Groups. See **Inventory > Groups** in the NSX-T Manager web interface.

NSX Data Center for vSphere has system-defined and user-defined Security Groups. These are all migrated to NSX-T as user-defined Groups.

The total number of 'Groups' after migration might not be equal to the number of Security Groups on NSX for vSphere. For example, a Distributed Firewall rule containing a VM as its source would be migrated into a rule containing a new Group with the VM as its member. This increases the total number of groups on NSX-T after migration.

Table 1-6. Security Groups

Configuration	Supported	Details
Security Group with members that don't exist	No	If any of the members of the Security Group do not exist, then the Security Group is not migrated.
Security Group that contains a Security Group with unsupported members	No	If any members of the Security Group are not supported for migration, the Security Group is not migrated. If a Security Group contains a Security Group with unsupported members, the parent Security Group is not migrated.
Exclude membership in Security Group	No	Security Groups with an exclude member directly or indirectly (via nesting) are not migrated

Table 1-6. Security Groups (continued)

Configuration	Supported	Details
Security Group Static Membership	Yes	A Security Group can contain up to 500 static members. However, system-generated static members are added if the Security Group is used in Distributed Firewall rules, lowering the effective limit to 499 or 498. ■ If the Security Group is used in either layer 2 or layer 3 rules, one system-generated static member is added to the Security Group. ■ If the Security Group is used in both layer 2 and layer 3 rules, two system-generated static members are added. If any members do not exist during the Resolve Configuration step, the security group is not migrated.
Security Group Member Types (Static or Entity Belongs To): ■ Cluster ■ Datacenter ■ Directory Group ■ Distributed Port Group ■ Legacy Port Group / Network ■ Resource Pool ■ vApp	No	If a security group contains any of the unsupported member types, the security group is not migrated.
Security Group Member Types (Static or Entity Belongs To): ■ Security Group ■ IP Sets ■ MAC Sets	Yes	Security groups, IP sets, and MAC sets are migrated to NSX-T as Groups. If an NSX for vSphere security group contains an IP set, MAC set, or nested security group as a static member, the corresponding Groups are added to the parent Group. If one of these static members was not migrated to NSX-T, the parent security group does not migrate to NSX-T. For example, an IP set with more than 2 million members cannot migrate to NSX-T. Therefore, a security group that contains an IP set with more than 2 million members cannot migrate.
Security Group Member Types (Static or Entity Belongs To): ■ Logical Switch (Virtual Wire)	Yes	If a security group contains logical switches that do not migrate to NSX-T segments, the security group does not migrate to NSX-T.

Table 1-6. Security Groups (continued)

Configuration	Supported	Details
Security Group Member Types (Static or Entity Belongs To): ■ Security tag	Yes	If a security tag is added to the security group as a static member or as a dynamic member using Entity Belongs To, the security tag must exist for the security group to be migrated. If the security tag is added to the security group as a dynamic member (not using Entity Belongs To), the existence of the security tag is not checked before migrating the security group.
Security Group Member Types (Static or Entity Belongs To): ■ vNIC ■ Virtual Machine	Yes	■ vNICs and VMs are migrated as an ExternalIDExpression. ■ Orphaned VMs (VMs deleted from hosts) are ignored during Security Group migration. ■ Once the Groups appear on NSX-T, the VM and vNIC memberships are updated after some time. During this intermediate time, there can be temporary groups and their temporary groups might appear as members. However, once the Host Migration has finished, these extra temporary groups are no longer seen.
Using “Matches regular expression” operator for dynamic membership	No	This affects Security Tag and VM Name only. “Matches regular expression” is not available for other attributes.
Using other available operators for dynamic membership criteria for attributes: ■ Security Tag ■ VM Name ■ Computer Name ■ Computer OS Name	Yes	Available operators for VM Name, Computer Name, and Computer OS Name are Contains, Ends with, Equals to, Not equals to, Starts with. Available operators for Security Tag are Contains, Ends with, Equals to, Starts with.

Table 1-6. Security Groups (continued)

Configuration	Supported	Details
Entity Belongs to criteria	Yes	The same limitations for migrating static members apply to Entity Belongs to criteria. For example, if you have a Security Group that uses Entity Belongs to a cluster in the definition, the Security Group is not migrated. Security Groups that contain Entity Belongs to criteria that are combined with AND are not migrated.
Dynamic membership criteria operators (AND, OR) in Security Group	Yes.	When you define dynamic membership for an NSX Data Center for vSphere Security Group, you can configure the following: ■ One or more dynamic sets. ■ Each dynamic set can contain one or more dynamic criteria. For example, “VM Name Contains web”. ■ You can select whether to match Any or All dynamic criteria within a dynamic set. ■ You can select to match with AND or OR across dynamic sets. NSX Data Center for vSphere does not limit the number of dynamic criteria, dynamic sets, and you can have any combinations of AND and OR. In NSX-T Data Center, you can have a group with five expressions. NSX Data Center for vSphere security groups which contain more than five expressions are not migrated. Examples of security groups that can be migrated: ■ Up to 5 dynamic sets related with OR where each dynamic set contains up to 5 dynamic criteria related with AND (All in NSX Data Center for vSphere). ■ 1 dynamic set containing 5 dynamic criteria related with OR (Any in NSX Data Center for vSphere). ■ 1 dynamic set containing 5 dynamic criteria related with AND (All in NSX Data Center for vSphere). All member types must be the same.

Table 1-6. Security Groups (continued)

Configuration	Supported	Details
		■ 5 dynamic sets related with AND and each dynamic set containing exactly 1 dynamic criteria. All member types must be the same. Using “Entity belongs to” criteria with AND operators is not supported. All other combinations or definitions of a security group containing unsupported scenarios are not migrated.

In NSX Data Center for vSphere, security tags are objects which can be applied to VMs. When migrated to NSX-T security tags are attributes of a VM.

Table 1-7. Security Tags

Configuration	Supported	Details
Security Tags	Yes	If a VM has 25 or fewer security tags applied, migration of security tags is supported. If more than 25 security tags are applied, no tags are migrated. Note: If security tags are not migrated, the VM is not included in any groups defined by tag membership.

Services and Service Groups are migrated to NSX-T Data Center as Services. See **Inventory > Services** in the NSX-T Manager web interface.

Table 1-8. Services and Service Groups

Configuration	Supported	Details
Services and Service Groups (Applications and Application Groups)	Yes	Most of the default Services and Service Groups are mapped to NSX-T Services. If any Service or Service Group is not present in NSX-T, a new Service is created in NSX-T.
APP_ALL and APP_POP2 Service Groups	No	These system-defined service groups are not migrated.
Services and Service Groups with naming conflicts	Yes	If a name conflict is identified in NSX-T for a modified Service or Service Group a new Service is created in NSX-T with a name in format: <NSXv-Application-Name> migrated from NSX-V
Service Groups that combine layer 2 services with services in other layers	No	
Empty Service Groups	No	NSX-T does not support empty Services.

Table 1-8. Services and Service Groups (continued)

Configuration	Supported	Details
Layer 2 Services	Yes	NSX Data Center for vSphere layer 2 Services are migrated as NSX-T Service Entry EtherTypeServiceEntry.
Layer 3 Services	Yes	Based on the protocol, NSX Data Center for vSphere layer 3 Services are migrated to NSX-T Service Entry as follows: ■ TCP/UDP protocol: L4PortSetServiceEntry ■ ICMP / IPV6ICMP protocol: ICMPTypeServiceEntry ■ IGMP protocol: IGMPTypeServiceEntry ■ Other protocols: IPProtocolServiceEntry
Layer 4 Services	Yes	Migrated as NSX-T Service Entry ALGTypeServiceEntry.
Layer 7 Services	Yes	Migrated as NSX-T Service Entry PolicyContextProfile If an NSX Data Center for vSphere Layer 7 application has a port and protocol defined, a Service is created in NSX-T with the appropriate port and protocol configuration and mapped to the PolicyContextProfile.
Layer 7 Service Groups	No	
Distributed Firewall, Edge Firewall, or NAT rules that contain port and protocol	Yes	NSX-T requires a Service to create these rules. If an appropriate Service exists, it is used. If no appropriate Service exists, a Service is created using the port and protocol specified in the rule.

Table 1-9. Service Composer

Configuration	Supported	Details
Service Composer Security Policies	Yes	Firewall rules defined in a Security Policy are migrated to NSX-T as Distributed Firewall rules. Disabled firewall rules defined in a Service Composer Security Policy are not migrated. Guest Introspection rules or Network Introspection rules defined in a Service Composer Security Policy are not migrated. If the Service Composer status is not in sync, the Resolve Configuration step warns of this. You can either skip the migration of Service Composer policies by skipping the relevant Distributed Firewall sections. Or you can Cancel the migration, get Service Composer in sync with Distributed Firewall, and restart the migration.
Service Composer Security Policies not applied to any Security Groups	No	

Active Directory Server Configuration

Configuration	Supported	Details
Active Directory (AD) server	No	

Topologies Supported by Migration Coordinator

The migration coordinator can migrate an NSX Data Center for vSphere environment if it is configured in a supported topology.

Unsupported Features

In all topologies, the following features are not supported:

- OSPF between Edge Services Gateways and northbound routers. You must reconfigure to use BGP.
- IP Multicast.
- IPv6.

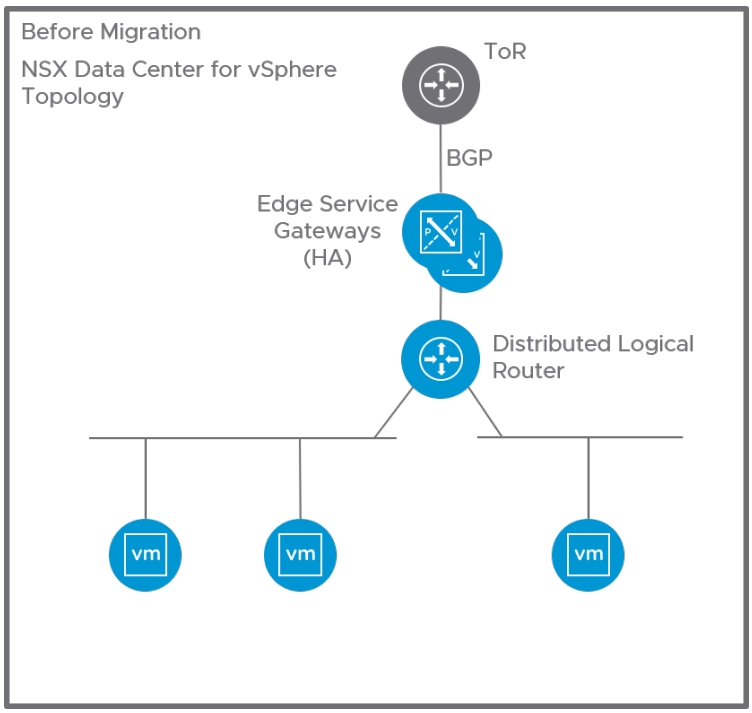
For detailed information about which features and configurations are supported, see Detailed Feature Support for Migration Coordinator.

ESG with High Availability and L4-L7 Services (Topology 1)

This topology contains the following configurations:

- A Distributed Logical Router peering with Edge Services Gateway.
- ECMP is not configured.
- The Edge Services Gateways are in a high availability configuration.
- BGP is configured between the Edge Services Gateway and northbound routers.
- Edge Services Gateway can be running L4-L7 services:
  - VPN, NAT, DHCP server, DHCP relay, DNS forwarding, Edge Firewall are supported services.
  - Load balancer is not supported in this topology.

Figure 1-1. Topology 1: Before Migration - NSX Data Center for vSphere



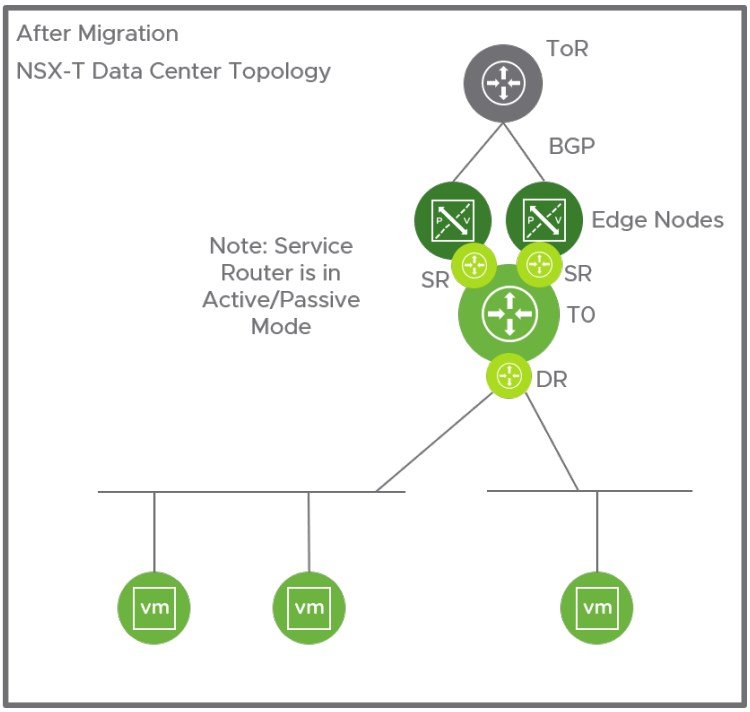
After migration, this configuration is replaced with a tier-0 gateway.

- The tier-0 gateway service router is in active/standby mode.
- The IP addresses of the Distributed Logical Router interfaces are configured as downlinks on the tier-0 gateway.
- The BGP configuration of the ESG is translated to a BGP configuration on the tier-0 gateway.

- Supported services are migrated to the tier-0 gateway.

Note Depending on your configuration, you might need to provide new IP addresses for the tier-0 gateway uplinks. For example, on an Edge Services Gateway, you can use the same IP address for the router uplink and for the VPN service. On a tier-0 gateway, you must use the different IP address for VPN and uplinks. See Example Configuration Issues for more information.

Figure 1-2. Topology 1: After Migration - NSX-T Data Center

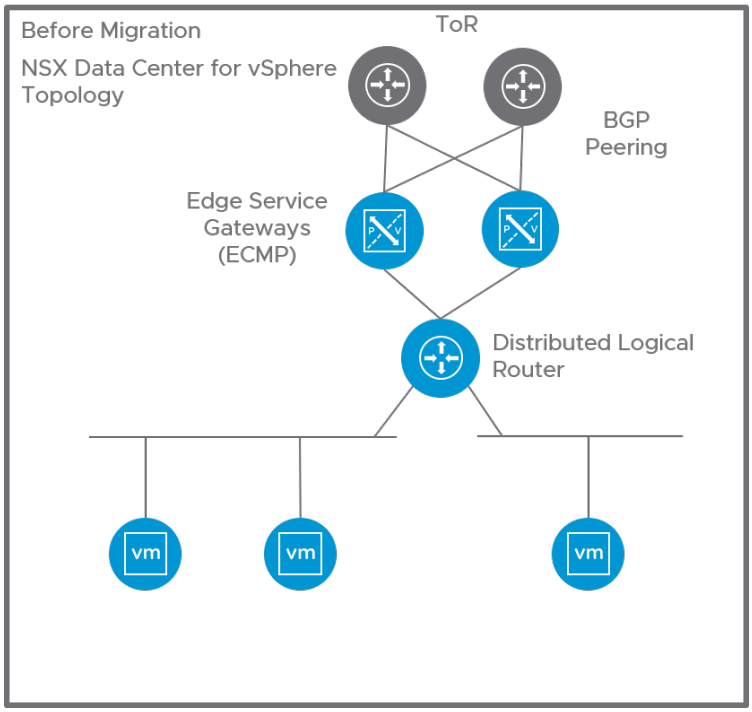


ESG with No L4-L7 Services (Topology 2)

This topology contains the following configurations:

- The Distributed Logical Router has ECMP enabled and peers with multiple Edge Services Gateways.
- BGP is configured between the Edge Services Gateway and northbound routers. The Edge Services Gateways must be configured with the same BGP neighbors. All Edge Services Gateways must point to the same autonomous system (AS).
- If BGP is configured between the Distributed Logical Router and Edge Services Gateway, all BGP neighbors on the Distributed Logical Router must have the same weight.
- Edge Services Gateways must not run L4-L7 services.

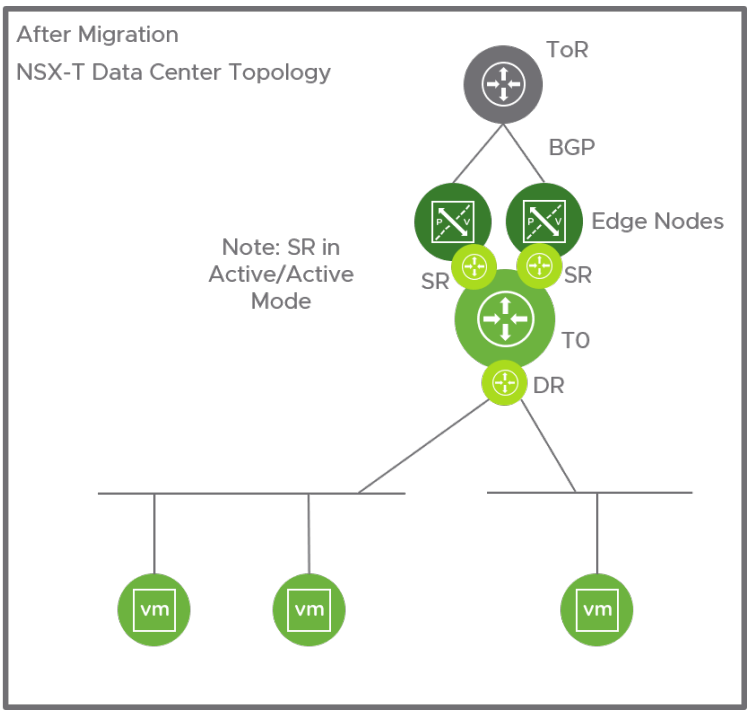
Figure 1-3. Topology 2: Before Migration - NSX Data Center for vSphere



After migration, this configuration is replaced with a tier-0 gateway.

- The tier-0 gateway service router is in active/active mode.
- The IPs of the Distributed Logical Router interfaces are configured as downlinks on the tier-0 Gateway.
- The combined BGP configurations of the Edge Services Gateways are translated to a BGP configuration on the tier-0 gateway. Route redistribution configuration is translated.
- Static routes from Edge Services Gateways and Distributed Logical Routers are translated to static routes on the tier-0 gateway.

Figure 1-4. Topology 2: After Migration - NSX-T Data Center

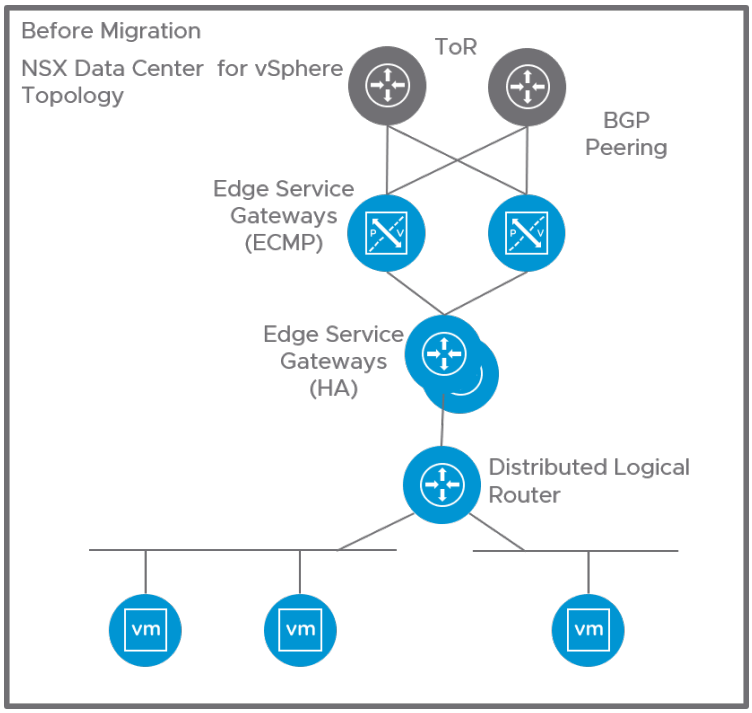


Two Levels of ESG with L4-L7 Services on Second-Level ESG (Topology 3)

This topology contains the following configurations:

- Two levels of Edge Services Gateways with Distributed Logical Router.
- The first-level (router-facing) Edge Services Gateways must not run L4-L7 services.
- The first-level Edge Services Gateways must have BGP enabled and have at least one BGP neighbor.
- The second-level Edge Services Gateways have ECMP enabled and peer with the first-level Edge Services Gateways.
- The second-level Edge Services Gateways can run L4-L7 services:
  - NAT, DHCP server, DHCP relay, DNS forwarding, inline load balancer, and Edge firewall are supported.
  - VPN is not supported.

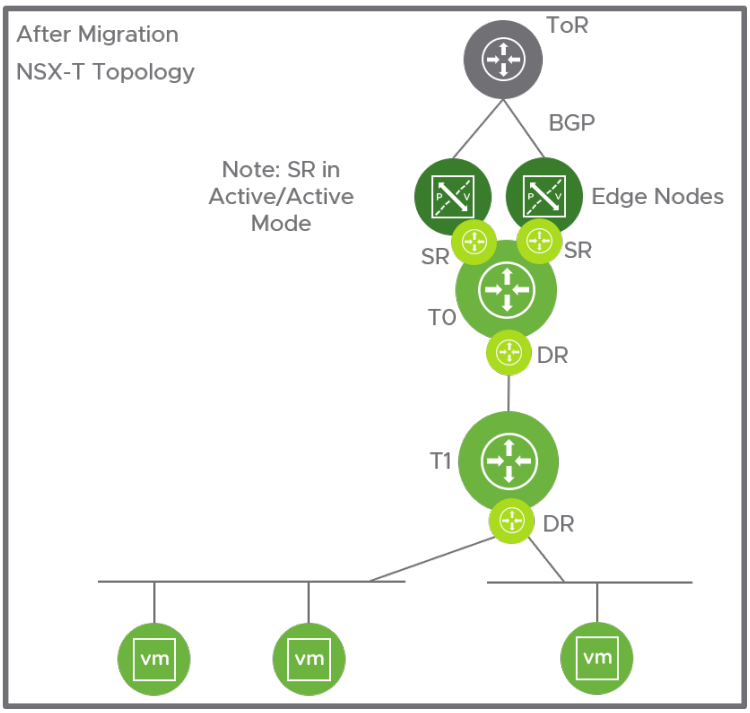
Figure 1-5. Topology 3: Before Migration - NSX Data Center for vSphere



After migration, this configuration is replaced with a tier-0 gateway and a tier-1 gateway.

- The first-level Edge Services Gateways are replaced with a tier-0 gateway. The service router is in active/active mode.
- The IPs of the first-level Edge Services Gateway uplinks are used for the tier-0 gateway uplinks.
- The tier-0 gateway peers with northbound routers using BGP.
- The second-level Edge Services Gateways are translated to a tier-1 gateway, which is linked to the tier-0 gateway.
- The IPs of the Distributed Logical Router interfaces are configured as downlinks on the tier-1 Gateway.
- Any services running on the second-level Edge Services Gateway are migrated to the tier-1 gateway.
- The BGP configuration on the first-level Edge Services Gateways is translated to a BGP configuration for the tier-0 gateway. Route redistribution configuration is translated.
- Static routes from Edge Services Gateways and Distributed Logical Routers are translated to static routes on the tier-0 gateway. Static routes between the Distributed Logical Router and second-level Edge Services Gateways are not needed, and so are not translated.

Figure 1-6. Topology 3: After Migration - NSX-T Data Center

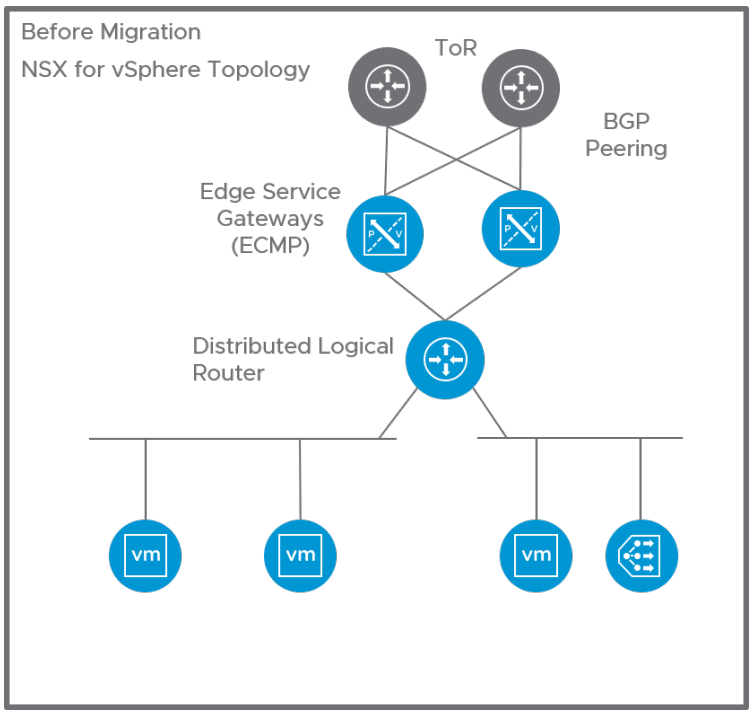


One-Armed Load Balancer (Topology 4)

This topology contains the following configurations:

- The Distributed Logical Router has ECMP enabled and peers with multiple Edge Services Gateway.
- BGP is configured between the Edge Services Gateway and northbound routers. All Edge Services Gateways must be configured with the same BGP neighbors. All Edge Services Gateways must point to the same autonomous system (AS).
- If BGP is configured between the Distributed Logical Router and Edge Services Gateway, all BGP neighbors on the Distributed Logical Router must have the same weight.
- The router-facing Edge Services Gateways must not run L4-L7 services.
- An Edge Services Gateway is attached to the Distributed Logical Router to perform load balancing services. It can also run Edge firewall and DHCP.

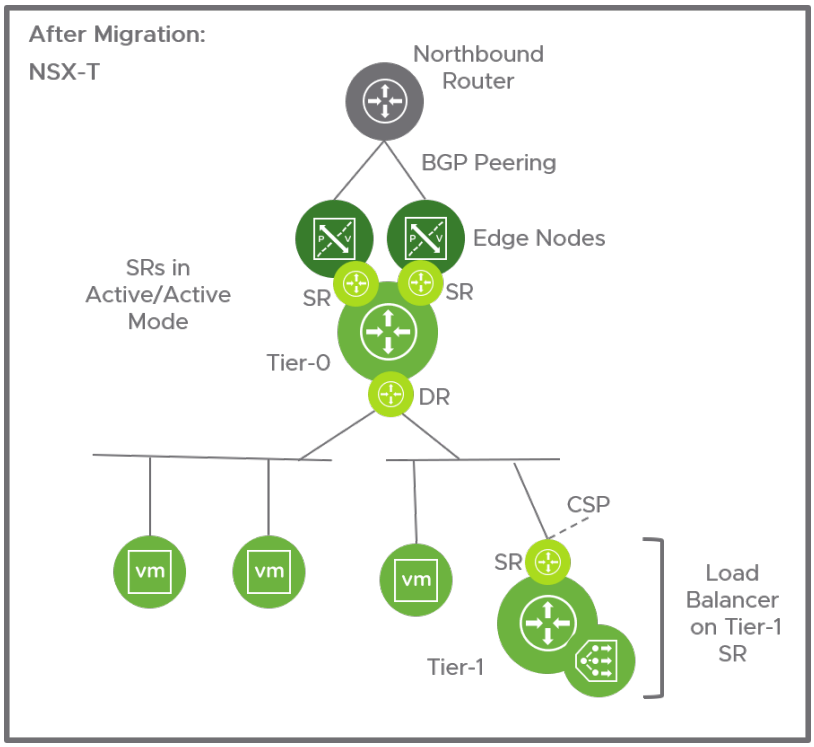
Figure 1-7. Topology 4: Before Migration - NSX Data Center for vSphere



After migration, the top-level Edge Services Gateways and the Distributed Logical Router are replaced with a tier-0 gateway. The Edge Services Gateway performing load balancing services is replaced with a tier-1 gateway.

- The tier-0 gateway service router is in active/active mode.
- The IPs of the Distributed Logical Router interfaces are configured as downlinks on the tier-0 Gateway.
- The combined BGP configurations of the top-level Edge Services Gateways are translated to a BGP configuration on the tier-0 gateway. Route redistribution configuration is translated.
- Static routes from the top-level Edge Services Gateways and Distributed Logical Routers are translated to static routes on the tier-0 gateway.
- The load balancing configuration on the Edge Services Gateway is translated to a one-arm load balancer configuration on the tier-1 Service Router.

Figure 1-8. Topology 4: After Migration - NSX-T Data Center



VLAN-Backed Micro-Segmentation (Topology 5)

This topology uses Distributed Firewall to provide firewall protection to workloads connected to VLAN-backed distributed port groups.

This topology uses the following NSX Data Center for vSphere features:

- NSX Manager
- Host Preparation Distributed Firewall only)
- Distributed Firewall
- Service Composer
- Grouping Objects

This topology must not contain the following features:

- Transport Zone
- VXLAN
- Logical Switch
- Edge Services Gateway
- Distributed Logical Router

Limits Supported by Migration Coordinator

Migration coordinator supports migrating NSX Data Center for vSphere environments that fall within these limits.

Table 1-10. Limits for Migration

Feature	Limit
Hosts per NSX Manager (Single vCenter - Transport Zone)	64
vCenter Clusters	8
Virtual Interfaces per Hypervisor Host	150
Logical switches	1,400
Distributed Logical Router interfaces per Distributed Logical Router	800
ECMP paths	8
Static routes per Edge Service Gateway	2,000
NAT rules per Edge Service Gateway	2,000
Edge firewall rules per Edge Services Gateway	2,000
DHCP leases per Edge Service Gateway	800
Distributed Firewall rules per NSX Manager	10,000
Distributed Firewall sections	1,300
Distributed Firewall rules per host	1,000
Security Groups per NSX Manager	1,215
IP Sets	1,000
MAC Sets	200
Security Tags	600
Security Tags per virtual machine	25
Grouping objects per NSX Manager	3,015
Virtual servers per load balancer	200
Pools per load balancer	200
IPsec tunnels per Edge Service Gateway	100
L2VPN Clients (spoke) handled by a single L2VPN Server (hub)	1
Networks per L2VPN Client-Server Pair	100

Overview of Migration Using Migration Coordinator

The migration process includes setting up a new NSX-T environment and running the migration coordinator. You also might need to change your existing NSX for vSphere environment to ensure that it can migrate to NSX-T.

Caution Deploy a new NSX-T environment to be the destination for the NSX for vSphere migration.

During the **Import Configuration** step, all Edge node interfaces in the destination NSX-T environment are shut down. If the destination NSX-T environment is already configured and is in use, starting the configuration import will interrupt traffic.

During the migration you will complete the following steps:

- Create a new NSX-T environment.
  - Deploy a single NSX Manager appliance to create the NSX-T environment.
  - Configure a compute manager in the NSX-T environment. Add the vCenter Server as a compute resource. Use the exact IP or hostname specified in NSX for vSphere vCenter Server registration.
  - Start the migration coordinator service.
  - If you want to import users from NSX for vSphere, set up VMware Identity Manager.
  - If your NSX Data Center for vSphere topology uses Edge Services Gateways, create an NSX-T IP pool to use for the NSX-T Edge TEPs. These IPs must be able to communicate with all existing NSX for vSphere VTEPs.
  - Deploy NSX Edge nodes.
    - Deploy the correct number of appropriately sized NSX-T Edge appliances.
    - Join the Edge nodes to the management plan from the command line.
- Import configuration from NSX for vSphere.
  - Enter the details of your NSX for vSphere environment.
  - The configuration is retrieved and pre-checks are run.
- Resolve issues with the configuration and deploy NSX-T Edge nodes.
  - Review Messages and the reported configuration issues to identify any blocking issues or other issues that require a change to the NSX for vSphere environment.
    - If you make any changes to the NSX for vSphere environment, you must restart the migration and import the configuration again.
  - Provide answers to configuration questions that must be resolved before you can migrate your NSX for vSphere environment to NSX-T. Resolving issues can be done in multiple passes by multiple people.

- Migrate configuration.
  - After all configuration issues are resolved, you can import the configuration to NSX-T. Configuration changes are made on NSX-T, but no changes are made to the NSX for vSphere environment yet.
- Migrate Edges.
  - Routing and Edge services are migrated from NSX for vSphere to NSX-T.

    Caution There is an interruption of North-South traffic during the Migrate Edges step. All traffic that was previously traversing through the Edge Services Gateways (North-South traffic) moves to the NSX-T Edges.
- Migrate Hosts.
  - NSX for vSphere software is removed from the hosts, and NSX-T software is installed. VM interfaces are connected to the new NSX-T segments.
- Finish Migration.
  - After you have verified that the new NSX-T environment is working correctly, you can finish the migration, which clears the migration state.
- Perform post-migration tasks.
  - Deploy two additional NSX Manager appliances before you use your NSX-T Data Center environment in production environment.
  - Uninstall NSX for vSphere environment.

Virtual Machine Deployment During Migration

After you start a migration, do not change the NSX for vSphere environment. If you want to deploy VMs during the migration, wait until some of the NSX for vSphere hosts have migrated to NSX-T and deploy the VMs on NSX-T hosts. Connect the VMs to NSX-T segments and install VMware Tools on the VMs.

Deploying on NSX-T with VMware Tools installed ensures that the VMs are populated into security groups and receive the intended Distributed Firewall policies.

Caution VMs deployed without VMware Tools installed, or deployed on NSX for vSphere do not receive the intended Distributed Firewall policies.

If you use vSphere templates to deploy VMs, update the templates to use NSX-T segments for the VM network configuration. Specifying NSX-T segments ensures that any VMs deployed using the templates are deployed on NSX-T hosts.

If you use automation tools to deploy VMs on vSphere, but do not use vSphere templates, you might need to change your automation tool configuration to ensure that the VMs are deployed on NSX-T.

Preparing to Migrate an NSX Data Center for vSphere Environment

Before you migrate you must review the documentation, verify that you have the required software versions, modify your existing NSX for vSphere environment if needed, and deploy the infrastructure for the new NSX-T environment.

Documentation

Check for the latest version of this guide and the release notes for NSX-T Data Center and migration coordinator. You can find the documentation here: https://docs.vmware.com/en/VMware-NSX-T-Data-Center/.

Required Software and Versions

- Verify that the NSX for vSphere environment has version 6.4.4 or 6.4.5.
- See the *VMware Product Interoperability Matrices* for required versions of vCenter Server and ESXi: http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php#interop&175=&1=&2=
- vSphere Distributed Switch version 6.5.0 and 6.6.0 are supported.
- The NSX for vSphere environment must match the NSX-T system requirements for ESXi, vCenter Server, and vSphere Distributed Switch.
- If you want to migrate the user roles from NSX for vSphere, you must deploy and configure VMware Identity Manager™. See the *VMware Interoperability Matrices* for compatible versions: https://www.vmware.com/resources/compatibility/sim/interop_matrix.php#interop&175=&140=. See the VMware Identity Manager documentation for more information.

Prepare NSX-T Data Center Environment

You must configure a new NSX-T Data Center environment to migrate NSX Data Center for vSphere environment.

To start migration, you must have the following configurations deployed:

- At least one NSX Manager appliance running in NSX-T Data Center.
- The vCenter Server associated with the NSX Data Center for vSphere environment configured as a compute manager on NSX-T Data Center.
- An IP pool to provide IPs for the Edge Tunnel End Points (TEPs). This step is required only when your NSX Data Center for vSphere environment uses Edge Services Gateways.
- The correct number and size of Edge nodes.

Deploy NSX-T Data Center NSX Manager Appliance

You must deploy a new NSX Manager appliance to run the migration coordinator. Do not use an existing NSX-T Data Center environment.

In other words, you cannot merge your NSX for vSphere environment into an existing NSX-T Data Center environment, which has NSX-T already installed on the vSphere host clusters.

For details on deploying a licensed version of the NSX Manager appliance, see *Install NSX Manager and Available Appliances* in the *NSX-T Data Center Installation Guide*.

Install one appliance to perform the migration. Deploy additional appliances to form a cluster after the migration is finished. See Finish Deploying the NSX Manager Cluster.

Add a Compute Manager

You must configure the vCenter Server system that is associated with the NSX Data Center for vSphere as a compute manager in NSX-T before you can start the migration process.

Prerequisites

Log into the NSX for vSphere NSX Manager web interface to retrieve the settings used for vCenter Server registration. You must use exactly the same settings, for example, if an IP is specified, use the IP, not the FQDN.

Procedure

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

Option	Description
Name and Description	Type the name to identify the vCenter Server. You can optionally describe any special details such as, the number of clusters in the vCenter Server.
Domain Name/IP Address	Type the IP address of the vCenter Server.
Type	Keep the default option.
Username and Password	Type the vCenter Server login credentials.
Thumbprint	Type the vCenter Server SHA-256 thumbprint algorithm value.

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

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

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

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

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

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

   If an existing registration exists, it will be replaced.

Results

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

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

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

Create an IP Pool for Edge Tunnel End Points

If your NSX Data Center for vSphere environment uses Edge Services Gateways, you must create an IP pool in the NSX-T environment for the Edge Tunnel End Points (TEP) before you start the migration.

Prerequisites

- Identify existing IP pools or DHCP ranges for NSX for vSphere VTEPs.
- Determine which IP addresses to use to create an IP pool for Edge TEPs.

  The IP range and VLAN must not already be in use in the NSX Data Center for vSphere environment.
- Verify that the NSX-T TEP IP addresses have network connectivity to the NSX for vSphere VTEP IP addresses.

Procedure

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

2 Select **Networking > IP Management > IP Address Pools**.

3 Click **Add IP Address Pool**.

4 Enter a name for the new IP pool.

5 (Optional) Enter a description.

6 In the **Subnets** column, click **Set** to add subnets.

7 Specify the IP ranges.

   a Select **Add Subnets > IP Ranges**.

   b Enter IPv4 or IPv6 ranges.

   c Enter the subnet address in a CIDR format.

   d Enter the Gateway IP address for this subnet.

   e (Optional) Enter DNS servers.

   f (Optional) Enter DNS suffix.

   g Click **Add**, and then click **Apply**.

8 Click **Save**.

Determining NSX Edge Requirements

You must deploy sufficient NSX Edge node resources to replace the Edge Services Gateways in the NSX for vSphere environment.

Use the following guidelines to determine in advance the number and size of NSX Edge resources required for a successful migration.

Note If your determination is incorrect, the migration will fail but the error message will detail the missing resources, enabling you to try again with the correct information. See Import the NSX Data Center for vSphere Configuration.

Number of Edge Nodes

If high availability is not configured, you need one NSX Edge node to replace each Edge Services Gateway with a northbound connection outside of the NSX for vSphere environment. If high availability is configured, you need two NSX Edge nodes.

You do not need to replace any Edge Services Gateways that are connected to a Distributed Logical Router to provide one-arm load balancer services, but are not providing routing services.

Size of Edge Nodes When Load Balancer Is Not Deployed

All NSX Edge nodes are added to the same NSX Edge cluster. All nodes in an NSX Edge cluster must be the same size.

If you do not have load balancers deployed, deploy NSX Edge nodes to provide sufficient capacity to replace the current Edge Services Gateway in NSX for vSphere.

If all NSX for vSphere in your environment are the same size, you can figure out the correct size of NSX Edge node using this table.

Table 1-11. Equivalent NSX Edge Sizes in NSX for vSphere and NSX-T

NSX for vSphere	NSX-T
Compact and Large	Small
Quad Large	Medium
X-Large	Large

All NSX Edge nodes must be of the same size so that they can be members of the same cluster. If there are different sizes of Edge Services Gateways in your environment, you must calculate the correct size to deploy. Calculate the total memory and vCPU resources required for all Edge Services Gateways in the environment, and then divide by the number of NSX Edge nodes required for migration. Compare the calculated requirements to the NSX Edge size requirements to choose the correct size.

Note During the Resolve Configuration phase of the migration process, the Migrate page displays a message that indicates which NSX Edge node size is required for migration. Confirm that the installed NSX Edge are sized accordingly.

Table 1-12. NSX for vSphere Edge Size Requirements

Edge Services Gateway Size	Memory	vCPU
Compact	512 MB	1
Large	1 GB	2
Quad Large	2 GB	4
X-Large	8 GB	6

Table 1-13. NSX Edge Size Requirements

NSX Edge Node Size	Memory	vCPU
Small	4 GB	2
Medium	8 GB	4
Large	32 GB	8

Size of NSX Edge Nodes When Load Balancer Is Deployed

If you have a load balancer deployed, you must deploy NSX Edge nodes that have the sufficient resources for your configuration.

See "Scaling Load Balancer Resources" in the *NSX-T Data Center Administration Guide*.

All NSX Edge nodes must be of the same size so that they can be members of the same cluster.

Deploy NSX Edge Nodes

You must deploy NSX Edge nodes of the appropriate number and size before you can complete the migration.

In a new NSX-T environment, there are many options for deploying NSX Edge nodes. However, if you are migrating using migration coordinator, you must deploy NSX Edge nodes as a virtual machine on ESXi. Deploy using an OVA or OVF file. Do not deploy on bare metal. Do not deploy from the NSX Manager user interface.

NSX Edge nodes must be connected to trunk portgroups. To learn more about NSX Edge networking, see "NSX Edge Networking Setup" in the *NSX-T Data Center Installation Guide*.

Prerequisites

- You must have sufficient ESXi hosts with appropriate resources available to accommodate the NSX Edge appliances.
- Determine what number and size of Edge nodes are needed. If you start a migration with no Edge nodes deployed on NSX-T, and run the **Import Configuration** step, the required number and size of Edge nodes is displayed. See Determining NSX Edge Requirements for more information.

Procedure

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

   Either copy the download URL or download the OVA file onto your computer.
2. In the vSphere Client, select the host on which to install NSX Edge node appliance.
3. Right-click and select **Deploy OVF template** to start the installation wizard.
4. Enter the download OVA URL or navigate to the saved OVA file, and click **Next**.
5. Enter a name and location for the NSX Edge node , and click **Next**.

   The name you type appears in the vCenter Server and vSphere inventory.
6. Select a compute resource for the NSX Edge node appliance, and click **Next**.
7. Review and verify the OVF template details, and click **Next**.
8. Select a deployment configuration and click **Next**.

   See the **Import Configuration** step for details on the size of Edge nodes you must deploy.
9. Select storage for the configuration and disk files, and click **Next**.
   a. Select the virtual disk format.
   b. Select the VM storage policy.
   c. Specify the datastore to store the NSX Edge node appliance files.
10. Select a destination network for each source network.
    a. For network 0, select the VDS management portgroup.
    b. For networks 1, 2, and 3, select the previously configured VDS trunk portgroups.

Post-migration, the NSX Edge node is connected to one of these three trunk networks using only a single fastpath interface. The network settings can be adjusted or verified after the NSX Edge node is deployed.

11 Configure IP Allocation settings.

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

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

12 Click **Next**.

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

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

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

14 Enter the hostname of the NSX Edge.

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

   Skip any VMC network settings.

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

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

   By default, SSH access is disabled for security reasons.

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

   The installation might take 7-8 minutes.

19 Start the NSX Edge node VM manually.

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

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

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

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

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

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

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

23 Verify that the NSX Edge node has the required connectivity.

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

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

24 Troubleshoot connectivity problems.

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

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

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

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

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

d Type the **`start service dataplane`** command.

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

Join NSX Edge Node VM with the Management Plane

You must join the NSX Edge node VM you created to the management plane.

Do not join the NSX Edge node VM to the management plane using any other method. Do not create transport nodes from the NSX Edge node VM.

Procedure

1 Open an SSH session or console session to the NSX Manager appliance.

2 Open an SSH session or console session to the NSX Edge node VM.

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

The command output is a string of alphanumeric numbers that is unique to this NSX Manager. For example:

```
NSX-Manager1> get certificate api thumbprint
659442c1435350edbbc0e87ed5a6980d892b9118f851c17a13ec76a8b985f57
```

4 On the NSX Edge node VM, run the **join management-plane** command.

Provide the following information:

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

```
NSX-Edge1> join management-plane <Manager-IP> thumbprint <Manager-thumbprint> username admin
```

Repeat this command on each NSX Edge node VM.

5 Verify the result by running the `get managers` command on your NSX Edge node VMs.

```
nsx-edge-1> get managers
10.173.161.17 Connected (NSX-RPC)
```

6 In the NSX Manager UI, navigate to **System > Fabric > Nodes > Edge Transport Nodes**.

On the NSX Edge Transport Node page:

- The **Configuration State** column displays `Configure NSX`. Click `Configure NSX` to begin configuration on the node. If the **NSX Version** column does not display the version number installed on the node, try refreshing the browser window.
- Do not click **Configure NSX**. Migration Coordinator will configure the NSX Edge node as an Edge Transport Node during the migration.

Prepare NSX Data Center for vSphere Environment for Migration

You must check the state of the NSX Data Center for vSphere environment and fix any problems found. Also, depending on your environment, you might need to change your NSX Data Center for vSphere configuration before you can migrate to NSX-T Data Center.

System State

Check the following system states:

- Verify that the NSX for vSphere components are in a green state on the NSX Dashboard.
- Verify that all ESXi hosts are in an operational state. Address any problems with hosts including disconnected states. There must be no pending reboots or pending tasks for entering maintenance mode.
- Verify the publish status of Distributed Firewall and Service Composer to make sure that there are no unpublished changes.

General Configuration

- Back up the NSX for vSphere and vSphere environments. See "NSX Backup and Restore" in the *NSX Administration Guide*.
- The VXLAN port must be set to 4789. If your NSX for vSphere environment uses a different port, you must change it before you can migrate. See "Change VXLAN Port" in the NSX for vSphere *NSX Administration Guide*.

Controller Configuration

- Migration coordinator does not support NSX for vSphere transport zones using multicast or hybrid replication mode. An NSX Controller cluster is required if VXLAN is in use. VLAN-backed micro-segmentation topologies do not use VXLAN and so do not require an NSX Controller cluster.

Host Configuration

- On all host clusters in the NSX for vSphere environment, check these settings and update if needed:
  - Set vSphere DRS to Manual
  - Disable vSphere High Availability.
  - Set the export version of Distributed Firewall filter to 1000. See Configure Export Version of Distributed Firewall Filter on Hosts.
- If you have hosts that have NSX for vSphere installed, but are not added to a vSphere Distributed Switch, you must add them to distributed switches if you want to migrate them to NSX-T. See Configure Hosts Not Attached to vSphere Distributed Switches for more information.
- On each cluster that has NSX for vSphere installed, check whether Distributed Firewall is enabled. You can view the enabled status at **Installation & Upgrade > Host Preparation**.

  If Distributed Firewall is enabled on any NSX for vSphere clusters before migration, Distributed Firewall is enabled on all clusters when they migrate to NSX-T. Determine the impact of enabling Distributed Firewall on all clusters and change the Distributed Firewall configuration if needed.

- Verify that all hosts have only one VTEP interface configured. Check each host in **Hosts and Clusters > *Host* > Configure > VMKernel adapters**. Verify that there is only one interface with TCP/IP stack `vxlan` per host. Migrating hosts with multiple VTEPs is not supported.

Edge Services Gateway Configuration

- Edge Services Gateways must use BGP for northbound routing. If OSPF is used, you must reconfigure to use BGP before you start the migration.
- You might need to make changes to your NSX for vSphere route redistribution configuration before migration starts.
  - Prefix filters configured at the redistribution level are not migrated. Add any filters you need as BGP filters in the Edge Service Gateway's BGP neighbor configuration.
  - After migration, dynamically-learned routes between Distributed Logical Router and Edge Services Gateway are converted to static routes and all static routes are redistributed into BGP. If you need to filter any of these routes, before you start the migration configure BGP neighbor filters to deny these prefixes while permitting others.
- NSX for vSphere supports policy-based IPSec VPN sessions where the local and peer subnets of two or more sessions overlap with each other. This behavior is not supported on NSX-T. You must reconfigure the subnets so they do not overlap before you start the migration. If this configuration issue is not resolved, the **Migrate Configuration** step fails.
- If you have an Edge Services gateway performing one-armed load balancer function, you must change the following configurations if present before you import the configuration:
  - If the Edge Services Gateway has an interface configured for management, you must delete it before migration. You can have only one connected interface on an Edge Services Gateway providing one-arm load balancer function. If it has more than one interface, the **Migrate Configuration** step fails.
  - If the Edge Services Gateway firewall is disabled, and the default rule is set to deny, you must enable the firewall and change the default rule to accept. After migration the firewall is enabled on the tier-1 gateway, and the default rule accept takes effect. Changing the default rule to accept before migration prevents incoming traffic to the load balancer from being blocked.
- Verify that Edge Services Gateways are all connected correctly to the topology being migrated. If Edge Services Gateways are part of the NSX for vSphere environment, but are not correctly attached to the rest of the environment, they are not migrated.

  For example, if an Edge Services Gateway is configured as a one-armed load balancer, but has one of the following configurations, it is not migrated:
  - The Edge Services Gateway does not have an uplink interface connected to a logical switch.

- The Edge Services Gateway has an uplink interface connected to a logical switch, but the uplink IP address not does match the subnet associated with the distributed logical router that connects to the logical switch.

Configure Hosts Not Attached to vSphere Distributed Switches

An NSX for vSphere environment can contain hosts that have NSX for vSphere installed, but are not added to a vSphere Distributed Switch. You must add the hosts to a vSphere Distributed Switch before you can migrate them.

You can use a distributed switch you already have in your environment, or create a new distributed switch for this purpose. Right click the distributed switch and select **Add and Manage Hosts** to add the hosts to the distributed switch. You do not need to assign physical uplinks or VMkernel network adapters to the distributed switch.

See "Add Hosts to a vSphere Distributed Switch" in the *vSphere Networking Guide* for more information.

If you import the configuration before you make this change, you must restart the migration to import the updated configuration. See Make Changes to the NSX for vSphere Environment.

After the migration has finished, the hosts are no longer required to be attached to the distributed switch.

- If you added the hosts to an existing distributed switch, you can remove them from the distributed switch.
- If you added the hosts to a new distributed switch that you are not using for another purpose, you can delete the distributed switch.

Configure Export Version of Distributed Firewall Filter on Hosts

The export version of Distributed Firewall must be set to 1000 on hosts before you migrate them to NSX-T Data Center. You must verify the export version and update if necessary.

This configuration is required for **Maintenance** migration mode.

Procedure

- For each host, complete the following steps.
  a. Log into the command-line interface.
  b. Retrieve the Distributed Firewall filter for the host.

```
[root@esxi:~] vsipioctl getfilters | grep "Filter Name" | grep "sfw.2"
   name: nic-2112467-eth0-vmware-sfw.2
   name: nic-2112467-eth1-vmware-sfw.2
   name: nic-2112467-eth2-vmware-sfw.2
[root@esxi:~]
```

c Use the filter information to retrieve the export version for the host.

```
[root@esxi:~] vsipioctl getexportversion -f nic-2112467-eth0-vmware-sfw.2
Current export version: 500
[root@esxi:~]
```

d If the version is not 1000, set the export version. Use one of the following methods.

- Use the `vsipioctl setexportversion` command to set the export version.

  ```
  [root@esxi:~] vsipioctl setexportversion -f nic-2112467-eth0-vmware-sfw.2 -e 1000
  ```

- Disable and then enable Distributed Firewall on the host.

e Verify that the export version is updated.

```
[root@esxi:~] vsipioctl getexportversion  -f nic-2112467-eth0-vmware-sfw.2
Current export version: 1000
```

Migrate NSX Data Center for vSphere to NSX-T Data Center

Use the migration coordinator to import your configuration, resolve issues with the configuration, and migrate Edges and hosts to your NSX-T Data Center environment.

Prerequisites

Verify that you have completed all relevant preparation steps before you start the migration. See Preparing to Migrate an NSX Data Center for vSphere Environment.

Note It is recommended that you first practice the migration process by completing the procedures in this guide through Resolve Configuration Issues. This will highlight most unresolved issues without committing you to complete the migration process. Until that point, you can roll back or cancel the migration. See Roll Back or Cancel the NSX for vSphere Migration.

Import the NSX Data Center for vSphere Configuration

To migrate your NSX Data Center environment from NSX for vSphere to NSX-T, you must provide details about your NSX for vSphere environment.

The migration coordinator service runs on one NSX Manager node.

Caution Deploy a new NSX-T environment to be the destination for the NSX for vSphere migration.

During the **Import Configuration** step, all Edge node interfaces in the destination NSX-T environment are shut down. If the destination NSX-T environment is already configured and is in use, starting the configuration import will interrupt traffic.

Prerequisites

- Verify that the vCenter Server system associated with the NSX for vSphere environment is registered as a compute manager. See Add a Compute Manager.
- If your NSX for vSphere environment uses Edge Services Gateways, verify that you have created an IP pool in the NSX-T environment to use for Edge TEPs. See Create an IP Pool for Edge Tunnel End Points.

Procedure

1. Using SSH, log in as **admin** to the NSX Manager VM and start the migration coordinator service.

   ```
   NSX-Manager1> start service migration-coordinator
   ```

2. From a browser, log in to the NSX Manager node on which you started the migration coordinator service. Log in as **admin**.
3. Navigate to **System > Migrate**.
4. On the **Migrate NSX for vSphere** pane, click **Get Started**.
5. From the **Import Configuration** page, click **Select NSX** and provide the credentials for vCenter and NSX for vSphere.

   Note The drop-down menu for vCenter displays all vCenter Server systems that are registered as compute managers. Click **Add New** if you need to add a compute manager.

6. Click **Start** to import the configuration.
7. When the import has finished, click **Continue** to proceed to the **Resolve Configuration** page.

   If the import fails due to incorrect edge node configuration translation, click the **Failed** flag to view information about the number and size of the required NSX Edge resources. After you deploy the correct number and size of edge nodes, click **Rollback** to roll back this migration attempt and restart the configuration import.

Roll Back or Cancel the NSX for vSphere Migration

After you have started the migration process, you can roll back the migration to undo some or all of your progress. You can also cancel the migration, which removes all migration state.

You can roll back or undo the migration from some of the migration steps. After the migration has started, you can click **Rollback** on the furthest step completed. The button is disabled on all other pages.

Table 1-14. Rolling Back NSX Data Center for vSphere Migration

Migration Step	Rollback Details
Import Configuration	Click **Rollback** on this page to roll back the **Import Configuration** step.
Resolve Configuration	Rollback is not available here. Click **Rollback** from the **Import Configuration** page.
Migrate Configuration	Click **Rollback** on this page to roll back the migration of the configuration to NSX-T and the input provided on the **Resolve Configuration** page. Verify that the rollback was successful before you start a new migration. Log into the NSX Manager web interface and switch to **Manager** mode. Verify that all configurations have been removed. For more information about Manager mode, see *Overview of the NSX Manager* in the *NSX-T Data Center Administration Guide*. **Note** If you experience problems rolling back the **Migrate Configuration** step, you can start a new migration instead. 1 Cancel the current migration. 2 Delete the current NSX-T appliance. 3 Deploy a new NSX-T environment with NSX Manager and NSX Edge appliances. 4 Start a new migration. Do not cancel the migration if Edge or Host migration has started.
Migrate Edges	Click **Rollback** on this page to roll back the migration of Edge routing and services to NSX-T. **Caution** If you roll back the **Migrate Edges** step, verify that the traffic is going back through the NSX for vSphere Edge Services Gateways. You might need to take manual action to assist the rollback.
Migrate Hosts	Rollback is not available here.

There is a **Cancel** button on every page of the migration. Canceling a migration deletes all migration state from the system. The migration coordinator shows the following warning message when you cancel a migration at any step:

```
Canceling the migration will reset the migration coordinator.
It is advisable to rollback this step first or it might leave the
the system in a partially migrated state. Do you want to continue?
```

Caution Do not cancel a migration if Edge or Host migration has started. Canceling the migration deletes all migration state and prevents you from rolling back the migration or viewing past progress. If needed, roll back first to a point before Edge migration has occurred, and then cancel.

Resolve Configuration Issues

After you have imported the configuration from your NSX Data Center for vSphere environment, you must review and resolve the reported configuration issues before you can continue with the migration.

Review Migration Information

The **Resolve Configuration** page contains information about what features and configurations are not supported for migration, what must be changed in your NSX for vSphere before you can migrate.

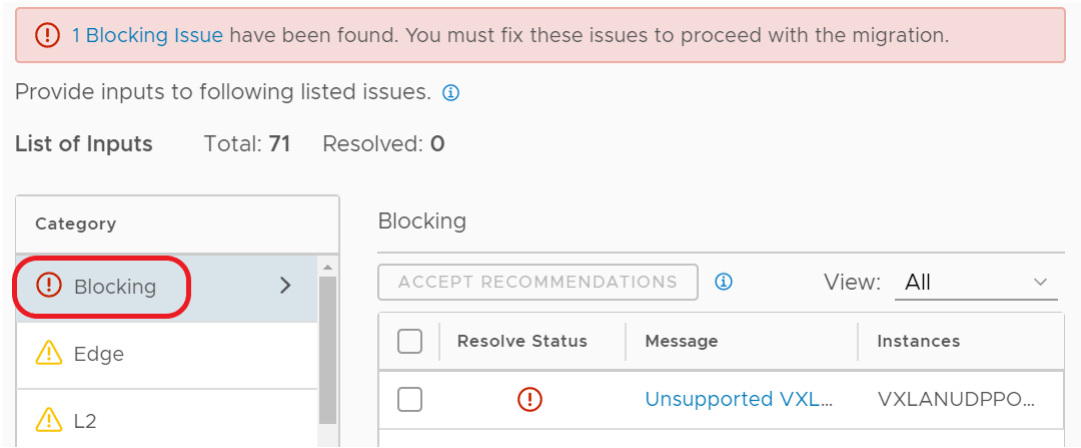
After reviewing these messages, you might need to change configurations in your NSX for vSphere environment before you can migrate to NSX-T. If you change the NSX for vSphere environment, you must restart the migration to pick up the new configuration. Review all migration feedback before you provide input to avoid duplication of work.

Note For some NSX for vSphere features, there might be automatic configurations such as certificates present. If these configurations are for features that are not supported for the specific topology, these automatic configurations are flagged as issues that need to be skipped from migration. For example, in topologies that don't support L4-L7 services on Edge Services Gateways, the certificates present for VPN and DNS will raise issues to skip these configurations from migration.

Procedure

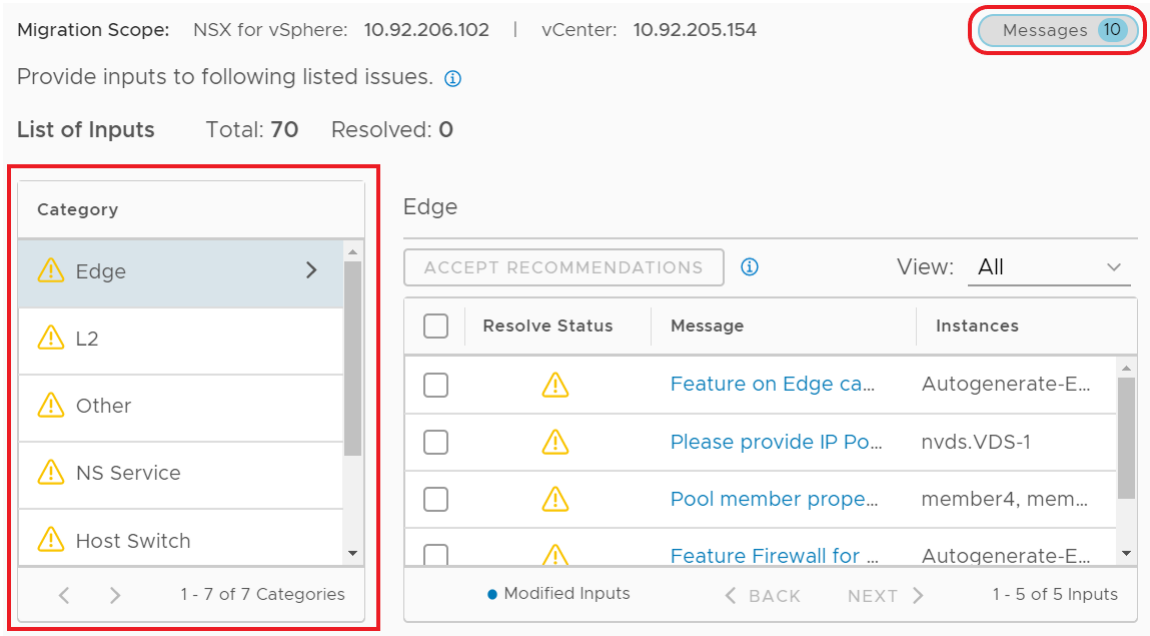
1 From the **Resolve Configuration** page, review the reported issues in the **Blocking** category to identify blocking issues that require changes to your NSX for vSphere environment.

Figure 1-9. Blocking Issues on the **Resolve Configuration** Page



2 Review the messages and issues reported in each category.

Figure 1-10. Messages and Categories of Issues on the Resolve Configuration Page



a Click **Messages** and review the information there.

b Review the reported issues in all categories.

What to do next

If you found blocking issues or other configurations that require a change in the NSX for vSphere environment, make those configurations before proceeding further. You must cancel the current migration and import the new configuration. See Make Changes to the NSX for vSphere Environment.

If you did not find any blocking issues or other configurations that require a change in the NSX for vSphere environment, you can proceed with the migration. See Provide Input for Configuration Issues.

Make Changes to the NSX for vSphere Environment

You might need to make changes to your NSX for vSphere environment to proceed with migration, for example, if blocking issues are found. If you make changes, you must import the configuration again so that the migration coordinator is aware of the changes.

Prerequisites

Verify that Host or Edge migration has not started. See Roll Back or Cancel the NSX for vSphere Migration for more information about restarting the migration.

Procedure

1 Make the required changes in the NSX for vSphere environment.

2 Navigate to the **Import Configuration** page and click **Cancel**.

Canceling clears the current migration process. Any input previously provided is removed.

3 Click **Start** to import the updated configuration.

Results

The migration starts over with the new NSX for vSphere configuration.

What to do next

Continue the migration process. See Resolve Configuration Issues.

Provide Input for Configuration Issues

After you have reviewed the migration information and are ready to proceed with the migration, you can provide input for the reported configuration issues. The input you provide determines how the NSX-T environment is configured.

Multiple people can provide the input over multiple sessions. You can return to a submitted input and modify it. Depending on your configuration, you might run through the **Resolve Issues** process multiple times, updating your NSX for vSphere environment as needed, and restarting the migration.

Important If you have changed the NSX for vSphere environment for any reason since you last imported the configuration, you must restart the migration. For example, if you have connected a new VM to a logical switch, made a firewall rule change, or installed NSX for vSphere on new hosts. See Make Changes to the NSX for vSphere Environment for information on restarting the migration.

For some examples of configuration issues and the required input, including Edge node setup, see Example Configuration Issues.

Note For some NSX for vSphere features, there might be automatic configurations such as certificates present. If these configurations are for features that are not supported for the specific topology, these automatic configurations are flagged as issues that need to be skipped from migration. For example, in topologies that don't support L4-L7 services on Edge Services Gateways, the certificates present for VPN and DNS will raise issues to skip these configurations from migration.

Prerequisites

- Verify that you have reviewed all issues and migration messages and are ready to continue with the migration.
- Verify that you have addressed all blocking issues and other issues requiring a change to the NSX for vSphere.

Procedure

1. Navigate to **System > Migrate**. Click **Resolve Configuration** on the **Migrate NSX for vSphere** pane.
2. From the **Resolve Configuration** page, click each issue and provide input.

   Each issue can cover multiple configuration items. For each item there might be one or more possible resolutions to the issue, for example, skip, configure, or select a specific value.

   For issues that apply to multiple configuration items, you can provide input for each item individually, or select all and provide one answer for all items.
3. After input has been provided, a **Submit** button is displayed on the **Resolve Configuration** page. Click **Submit** to save your progress.
4. When you have provided input for all configuration issues, click **Submit**.

   The input is validated. You are prompted to update any invalid input. Additional input might be required for some configuration items.
5. After you have submitted all requested input, click **Continue** to proceed to the Migrate Configuration step.

Example Configuration Issues

You must provide input on various configuration issues, such as configuration details for the new NSX-T Edge nodes.

Edge Node Networking Configuration

During **Resolve Configuration**, you provide information about the Edge Nodes that you have created to replace your NSX for vSphere Edge Services Gateways. The configuration might have to change to work correctly on NSX-T. You might need to use a different IP address and VLAN than you used in NSX for vSphere.

Migrating Edge Services Gateway with L4-L7 Services

Using the same interface for the router uplink and services such as VPN is supported in NSX for vSphere. This configuration is not supported in NSX-T. You can assign new IP addresses for the Edge node uplinks so that you do not need to change the IP address for the services running on the Edge node.

Migrating Edge Services Gateway in a High Availability Configuration

The NSX for vSphere topology that contains Edge Services Gateways in a high availability configuration can contain an Edge Services Gateway with two uplinks connected to two different distributed port groups on different networks.

In NSX-T, this configuration is replaced by two NSX Edge nodes, both of which must have their uplinks on the same network.

For example, an Edge Services Gateway with HA might have this configuration:

- vnic1 has IP address 192.178.14.2/24 and is attached to port group Public-DVPG which uses VLAN 11.
- vnic4 has IP address 192.178.44.2/24 and is attached to port group Public-DVPG-2 which uses VLAN 15.

To work after migration, at least one of these IP addresses has to change, as they both must be on the same network.

Here is an example of the information that might be provided during Resolve Configuration.

For the first NSX Edge node:

- ID is fa3346d8-2502-11e9-8013-000c2936d594.
- IP address is 192.178.14.2/24.
- VLAN is 11.

For the second NSX Edge node:

- ID is fa2de198-2502-11e9-9d7a-000c295cffc6.
- IP address is 192.178.14.4/24.
- You do not need to provide the VLAN because the same VLAN configured for the first NSX Edge node is assumed for the second node.

Both NSX Edge nodes must have connectivity to this network.

Migrate the NSX Data Center for vSphere Configuration

After you have resolved all configuration issues, you can migrate the configuration. When the configuration is migrated, configuration changes are made in the NSX-T environment to replicate the NSX for vSphere configuration.

If needed, you can roll back the configuration that is migrated. Rolling back does the following:

- Remove the migrated configuration from NSX-T.
- Roll back all the resolved issues in the previous step.

See Roll Back or Cancel the NSX for vSphere Migration for more information.

Prerequisites

Verify that you have completed the **Resolve Configuration** step.

Procedure

1 From the **Migrate Configuration** page, click **Start**.

The NSX for vSphere configuration is migrated to NSX-T.

2 Verify that all NSX for vSphere configurations are displayed on the NSX-T NSX Manager interface or API.

Important When the configuration is migrated to NSX-T, the configuration changes are made in the NSX Manager database, but it might take some time for the configuration to take effect. You must verify that all expected NSX for vSphere configurations appear on the NSX Manager interface or API in NSX-T before you proceed to the **Migrate Edges** step. For example, firewall configuration, logical switches, transport zones.

Modify NSX Edge Node Configuration Before Migrating Edges

When NSX for vSphere Edge Services Gateways are migrated to NSX-T, a default configuration is used for interface MTU settings. If you want to change this default, you can do this before you start the **Migrate Edges** step.

Customized MTU settings in the Edge Services Gateways routing interfaces are not migrated to NSX-T. Any logical router interfaces created in NSX-T use the global default MTU setting, which is 1500. If you want to ensure that all logical router interfaces have a larger MTU, you can change the global default MTU setting. You can also modify interface MTUs on a case-by-case basis.

Procedure

1 Use `GET /api/v1/global-configs/RoutingGlobalConfig` to retrieve the current configuration.

2 Modify the value of the global default MTU: `logical_uplink_mtu`

3 Use `PUT /api/v1/global-configs/RoutingGlobalConfig` to make the configuration change.

Migrate NSX Data Center for vSphere Edges

After you have migrated the configuration, you can migrate the NSX for vSphere Edge Services Gateway to NSX-T Data Center.

If you are migrating a VLAN-backed micro-segmentation topology, you do not have any Edge Service Gateway appliances to migrate. You should still click **Start** so you can proceed to the **Migrate Hosts** step.

If needed, you can roll back the Edge migration to use the Edge Services Gateway in the NSX for vSphere environment. See Roll Back or Cancel the NSX for vSphere Migration for more information.

Caution If you roll back the **Migrate Edges** step, verify that the traffic is going back through the NSX for vSphere Edge Services Gateways. You might need to take manual action to assist the rollback.

Prerequisites

- All configuration issues must be resolved.
- The NSX for vSphere configuration must be migrated to NSX-T.

- Verify that you have a backup of NSX for vSphere and vSphere since the most recent configuration changes were made.
- Verify that all NSX for vSphere configurations that you expected to migrate appear on the NSX Manager UI or API in NSX-T Data Center.
- If you are using new IP addresses for the NSX-T Edge node uplinks, you must configure the northbound routers with these new BGP neighbor IP addresses.
- Verify that you have created an IP pool for Edge Tunnel End Points (TEP). See Create an IP Pool for Edge Tunnel End Points.

Procedure

1 From the **Migrate Edges** page, click **Start**.

   All Edges are migrated. The uplinks on the NSX for vSphere Edge Services Gateways are internally disconnected, and the uplinks on the NSX-T Edge nodes are brought online.

2 Verify that routing and services are working correctly in the new NSX-T Data Center environment.

   If so, you can migrate the hosts. See Configuring NSX Data Center for vSphere Host Migration.

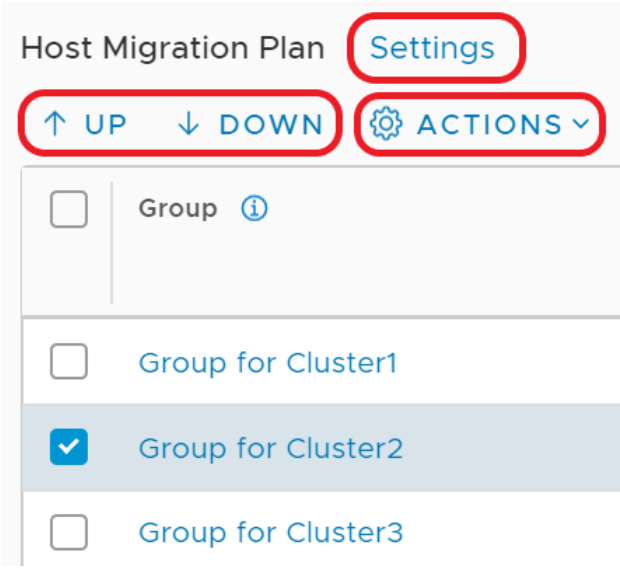
Results

The following changes result from the migration process:

- The routing and service configuration from NSX for vSphere Edge Services Gateway (ESG) are transferred to the newly created NSX-T Data Center Edge nodes.
- The new TEP IP addresses for the newly created NSX-T Data Center Edge nodes are configured from a newly created IP pool for Edge Tunnel End Points.
- The NSX for vSphere VTEP IP pool is migrated to the NSX-T Data Center environment.

Configuring NSX Data Center for vSphere Host Migration

The clusters in the NSX for vSphere environment are displayed on the **Migrate Hosts** page. The clusters are arranged into migration groups, each migration group contains one vSphere host cluster. There are several settings which control how the host migration is performed.



- Click **Settings** to change the global settings: **Pause Between Groups** and **Migration Order Across Groups**.
- Select a single host group (cluster) and use the arrows to move it up or down in the migration sequence.
- Select one or more host groups (clusters) and click **Actions** to change these host groups settings: **Migration Order Within Groups**, **Migration State**, and **Migration Mode**.

Pause Between Groups

Pause Between Groups is a global setting that applies to all host groups. If pausing is enabled, the migration coordinator migrates one host group, and then waits for input. You must click **Continue** to continue to the next host group. If you want to verify the status of each cluster before proceeding to the next one, enable **Pause Between Groups**.

By default, **Pause Between Groups** is disabled.

Note This feature is useful because it verifies the application on the current cluster before migrating the next cluster.

Serial or Parallel Migration Order

You can define whether migration happens in a serial or parallel order. There are two ordering settings:

- **Migration Order Across Groups** is a global setting that applies to all host groups.
  - **Serial**: One host group (cluster) at a time is migrated.
  - **Parallel**: Up to five host groups at a time are migrated. After those five host groups are migrated, the next batch of up to five host groups are migrated.

- **Migration Order Within Groups** is a host group (cluster) specific setting, so can be configured separately on each host group.
  - **Serial**: One host within the host group (cluster) at a time is migrated.
  - **Parallel**: Up to five hosts within the host group are migrated at a time. After those hosts are migrated, the next batch of up to five hosts are migrated.

    Important Do not select parallel migration order within groups for a cluster if you plan to use **Maintenance** migration mode for that cluster.

By default, both settings are set to **Serial**. Together, the settings determine how many hosts are migrated at a time.

Table 1-15. Effects of Migration Settings on Number of Hosts Attempting Migration Simultaneously

Migration Order Across Groups (Clusters)	Migration Order Within Groups (Clusters)	Maximum Number of Hosts Attempting Migration Simultaneously
Serial	Serial	1 One host from one host group
Serial	Parallel	5 Five hosts from one host group
Parallel	Serial	5 One host from five host groups
Parallel	Parallel	25 Five hosts from five host groups

Important If there is a failure to migrate a host, the migration process will pause after all in-progress host migrations have finished. If **Parallel** is selected for both migration across groups and migration within groups, there might be a long outage for the failed host before you can retry migration.

Sequence of Migration Groups

You can select a host group (cluster) and use the arrows to move it up or down in the list of groups.

If migration fails for a host, you can move its host group to the bottom of the list of groups. The migration of other host groups can proceed while you resolve the problem with the failed host.

Migration State

Host groups (clusters) can have one of three migration states:

- **Enabled**

  Hosts groups with a migration state of **Enabled** are migrated to NSX-T when you click **Start** on the **Migrate Hosts** page.

- **Disabled**

  You can temporarily exclude host groups from migration by setting the migration state for the groups to **Disabled**. Hosts in disabled groups are not migrated to NSX-T when you click **Start** on the **Migrate Hosts** page. However, you must enable and migrate all **Disabled** host groups before you can click **Finish**. Finish all host migration tasks and click **Finish** within the same maintenance window.

- **Do not migrate**

  Hosts that were identified as ineligible for migration in the **Resolve Configuration** step are assigned the migration state of **Do not migrate**.

  For example, hosts that do not have NSX for vSphere installed have the status of **Do not migrate**.

  You can also set the migration state of a group to **Do not migrate** to permanently exclude this host group from migration. Once you have clicked **Finish**, you cannot change the migration state of any host groups.

  Restarting the migration after you click **Finish** is not supported.

  If you permanently exclude a host group from migration, the VMs on that host cluster lose access to NSX features after host migration finishes.

Migration Mode

Migration Mode is a host group (cluster) specific setting, and can be configured separately on each host group. You can select one of two migration modes, **In-Place** or **Maintenance**.

Note If you use Distributed Firewall, select **In-Place** or **Automated Maintenance** migration mode. Using **Manual Maintenance** migration mode is not supported.

- **In-Place**

  NSX components are migrated while VMs are running on the hosts. Hosts are not put in maintenance mode during migration. Virtual machines experience a short network outage and network storage I/O outage during the migration.

- **Maintenance**

  A task of entering maintenance mode is automatically queued. To allow the host to enter maintenance mode, do one of the following tasks:

  - Power off all VMs on the hosts.
  - Move the VMs to another host.

    Caution Using vMotion to move powered-on VMs to NSX-T is not supported.

Migrate NSX Data Center for vSphere Hosts

After you have migrated Edge Services Gateway VMs to NSX-T Edge nodes, and verified that routing and services are working correctly, you can migrate your NSX for vSphere hosts to NSX-T host transport nodes.

You can configure several settings related to the host migration, including migration order and enabling hosts. Before you change any default settings, make sure that you understand the effects of these settings. See Configuring NSX Data Center for vSphere Host Migration for more information.

Caution If you use Distributed Firewall, select **In-Place** migration mode. Using **Maintenance** migration mode is not supported.

During the host migration, the following changes are made:

- NSX for vSphere software is uninstalled.
- NSX-T software is installed.
- Hosts are configured with N-VDS to replace vSphere Distributed Switches:
  - Each N-VDS is created with a name that references the distributed switch name. For example, distributed switch `ComputeSwitchA` is created as N-VDS `nvds.ComputeSwitchA`.
  - If different clusters use different distributed switches to back logical switches, an N-VDS is created with a name that combines all the distributed switch names. For example, if `ComputeCluster1` and `ComputeCluster2` use distributed switch `ComputeSwitchA` to back logical switches and `ComputeCluster3` uses `ComputeSwitchB` to back logical switches, the N-VDS is created as `nvds.ComputeSwitchA.ComputeSwitchB`.
- PNICs, vmks, and VTEPs in the vSphere Distributed Switch are migrated to N-VDS.
- NSX for vSphere VTEPs are migrated to NSX-T Data Center TEPs.
- VMs connected to the vSphere Distributed Switches are connected to N-VDS (for **In-Place** migration only).

Caution There is a traffic interruption during the host migration. Host migration should be completed during the same maintenance window as Edge migration.

If you have Distributed Firewall rules that are applied to a VM, those rules are not pushed to the host until the host and all its VMs are migrated. Until the rules are pushed to the host, the following applies:

- If the NSX-T default rule is `deny`, the VM is not accessible.
- If the NSX-T default rule is `accept`, the VM is not protected by the applied-to rules.

If migration fails for a host, the migration pauses after all in-progress host migrations finish. When you have resolved the problem with the host, click **Retry** to retry migration of the failed host.

If migration fails for a host, you can move its host group to the bottom of the list of groups. The migration of other host groups can proceed while you resolve the problem with the failed host.

After a host has migrated to NSX-T you might see an alarm with message `Lost network connectivity`. The alarm occurs because the host no longer has a physical NIC connected to the vSphere Distributed Switch it was previously connected to.

Prerequisites

- Verify that Edge migration has finished and all routing and services are working correctly.
- Verify that all ESXi hosts are in an operational state. Address any problems with hosts including disconnected states. There must be no pending reboots or pending tasks for entering maintenance mode.

Procedure

1 Click **Start** to start the host migration.

If you selected the **In-Place** migration mode for all hosts groups, the host migration starts.

2 If you selected the **Maintenance** migration mode for any host groups, you must complete one of the following tasks for each VM so that the hosts can enter maintenance mode.

Option	Action
Power off or suspend VMs.	a Right click the VM and select **Power > Power off** , **Power > Shut Down Guest OS**, or **Power > Suspend**. b After the host has migrated, attach the VM interfaces to the appropriate NSX-T segments and power on the VM.
Move VMs to an NSX for vSphere host using vMotion or cold migration.	a (Optional) To cold migrate, right click the VM and select **Power > Power off** , **Power > Shut Down Guest OS**, or **Power > Suspend**. b Right click the VM and select Migrate. Follow the prompts to move the VM to a different host.
Move VMs to an NSX-T host using cold migration.	a Right click the VM and select **Power > Power off** , **Power > Shut Down Guest OS**, or **Power > Suspend**. b Right click the VM and select Migrate. Follow the prompts to move the VM to a different host, connecting the VM interfaces to the appropriate NSX-T segments.

Caution Using vMotion to move powered-on VMs to NSX-T is not supported.

The host enters maintenance mode after all VMs are powered off or suspended. If you want to use cold migration to move the VMs to a different host before the migrating host enters maintenance mode, you must leave at least one VM running while you move VMs. When the last VM is powered off or suspended, the host enters maintenance mode, and migration of the host to NSX-T starts.

Changes Made During Host Migration

During the host migration, changes are made to migrate NSX for vSphere hosts to NSX-T hosts.

- NSX for vSphere software is uninstalled.
- NSX-T software is installed.
- For vSphere Distributed Switch versions 6.5.0 and 6.6.0:

  Hosts are configured with N-VDS to replace vSphere Distributed Switches:

  - Each N-VDS is created with a name that references the distributed switch name. For example, distributed switch `ComputeSwitchA` is created as N-VDS `nvds.ComputeSwitchA`.
  - If different clusters use different distributed switches to back logical switches, an N-VDS is created with a name that combines all the distributed switch names. For example, if `ComputeCluster1` and `ComputeCluster2` use distributed switch `ComputeSwitchA` to back logical switches and `ComputeCluster3` uses `ComputeSwitchB` to back logical switches, the N-VDS is created as `nvds.ComputeSwitchA.ComputeSwitchB`.
  - PNICs and vmks in the vSphere Distributed Switch are migrated to N-VDS.
  - NSX for vSphere VTEPs are migrated to NSX-T Data Center TEPs.
- For vSphere Distributed Switches version 7.0:

  Hosts configured for vSphere Distributed Switch version 7.0 continue using the same switch after migration.

  - PNICs and vmks in the vSphere Distributed Switch remain connected on the same vSphere Distributed Portgroups.
  - NSX for vSphere VTEPs are migrated to NSX-T Data Center TEPs and connected to standalone ports on the same vSphere Distributed Switch.

Finish the NSX Data Center for vSphere Migration

After you have migrated all Edge Services Gateway VMs and hosts to the NSX-T Data Center environment, confirm that the new environment is working correctly. If everything is functioning correctly, you can finish the migration.

Important Verify everything is working and click **Finish** within the maintenance window. Clicking **Finish** performs some post-migration clean-up. Do not leave the migration coordinator in a unfinished state beyond the migration window.

You will see errors on hosts after the migration. The error message is: `UserVars.RmqHostId' is invalid or exceeds the maximum number of characters permitted`. The error occurs because this host is still part of the NSX Data Center for vSphere inventory.

Prerequisites

- Verify that all expected items have been migrated to the NSX-T Data Center environment.

- Verify that the NSX-T Data Center environment is working correctly.

Procedure

1. Navigate to the **Migrate Hosts** page of the migration coordinator.
2. Click **Finish**

   A dialog box appears to confirm finishing the migration. If you finish the migration, all migration details are cleared. You can no longer review the settings of this migration. For example, which inputs were made on the **Resolve Configuration** page, or which hosts were excluded from the migration.

Post-Migration Tasks

After migration has finished, some additional actions might be required.

- If you migrated from NSX for vSphere 6.4.4, perform a reboot of all hosts that have migrated to NSX-T. The reboot must be done before you upgrade to a later version of NSX-T.
- During migration, all transport nodes are added to a group called `NSGroup with TransportNode for CPU Mem Threshold`. This group ensures that the transport nodes have the correct CPU memory threshold settings in NSX-T. This group is required after migration has completed. If you need to remove a transport node from NSX-T after migration, you must first remove the transport node from this group.

  Make sure you are in **Manager** mode and then select **Inventory > Groups** to remove the transport node from the `NSGroup with TransportNode for CPU Mem Threshold` group. For more information about Manager mode, see *Overview of the NSX Manager* in the *NSX-T Data Center Administration Guide*.
- Verify that you have a valid backup and restore configuration. See "Backing Up and Restoring the NSX Manager" in the *NSX-T Data Center Administration Guide*.

Finish Deploying the NSX Manager Cluster

You can run the migration coordinator tool with only one NSX Manager appliance deployed. Deploy two additional NSX Manager appliances before you use your NSX-T Data Center environment in production.

See the *NSX-T Data Center Installation Guide* for the following information:

- *NSX Manager Cluster Requirements*
- *Deploy NSX Manager Nodes to Form a Cluster from UI*
- *Configure a Virtual IP (VIP) Address for a Cluster*

Uninstalling NSX for vSphere After Migration

When you have verified that the migration is successful, and have clicked **Finish** to finish the migration, you can uninstall your NSX for vSphere environment.

The process for uninstalling NSX for vSphere after migration to NSX-T is different from the standard uninstall for NSX for vSphere.

Prerequisites

- Verify that the migration is successful, and all functionality is working in the NSX-T environment.
- Verify that you have clicked **Finish** on the **Migrate Hosts** page.

Procedure

1. Delete the ESX Agent Manager agencies that are associated with the NSX for vSphere environment.
   a. In the vSphere Client, navigate to **Menu > Administration**. Under **Solutions**, click **vCenter Server Extensions**. Double-click **vSphere ESX Agent Manager** and click the **Configure** tab.
   b. For each agency that has a name starting with `_NSX_`, select the agency, then click the three dots menu **(⋮)** and select **Delete Agency**.
2. Remove the NSX for vSphere plug-in from vCenter Server.
   a. Access the Extension Manager from the Managed Object Browser at `https://<vcenter-ip>/mob/?moid=ExtensionManager`.
   b. Click **UnregisterExtension**.
   c. In the **UnregisterExtension** dialog box, enter **`com.vmware.vShieldManager`** in the **Value** text box and click **Invoke Method**.
   d. In the **UnregisterExtension** dialog box, enter **`com.vmware.nsx.ui.h5`** in the **Value** text box and click **Invoke Method**.
   e. You can verify that you unregistered the extensions by going to the Extension Manager page at `https://<vcenter-ip>/mob/?moid=ExtensionManager` and viewing the values for the **extensionList** property.

3 Delete the vSphere Web Client directories and vSphere Client (HTML5) directories for NSX for vSphere and then restart the client services.

a Connect to the vCenter Server system command line.

- If you are using a vCenter Server Appliance, log in as root using the console or SSH. You must log in as root and run the commands from the Bash shell. You can start the Bash shell using the following commands.

```
> shell.set --enabled True
> shell
```

- If you are using vCenter Server for Windows, log in as an administrator using the console or RDP.

b Delete all NSX for vSphere plug-in directories.

Note A plug-in directory might not be present if you have never launched the associated client.

On vCenter Server Appliance, delete the following directories:

- To remove the vSphere Web Client plug-in, delete the `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/com.vmware.vShieldManager-<version>-<build>` directory.
- To remove the vSphere Client plug-in, delete the `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/com.vmware.nsx.ui.h5-<version>-<build>` directory.

On vCenter Server for Windows, delete the following directories:

- To remove the vSphere Web Client plug-in, delete the `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity\com.vmware.vShieldManager-<version>-<build>` directory.
- To remove the vSphere Client plug-in, delete the `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity\com.vmware.nsx.ui.h5-<version>-<build>` directory.

c Restart the client services on the vCenter Server Appliance or vCenter Server on Windows.

Table 1-16. Client Service Commands

Client Service	vCenter Server Appliance	vCenter Server for Windows
Restart vSphere Web Client	`# service-control --stop vsphere-client` `# service-control --start vsphere-client`	`> cd C:\Program Files\VMware\vCenter Server\bin`

Table 1-16. Client Service Commands (continued)

Client Service	vCenter Server Appliance	vCenter Server for Windows
		`> service-control --stop vspherewebclientsvc` `> service-control --start vspherewebclientsvc`

Restart vSphere Client	`# service-control --stop vsphere-ui`
	`# service-control --start vsphere-ui`
		`> cd C:\Program Files\VMware \vCenter Server\bin`
		`> service-control --stop vsphere-ui`
		`> service-control --start vsphere-ui`

4 Power off and delete the NSX for vSphere appliances.

   a Navigate to **Home > Hosts and Clusters**.

   b Locate the following NSX for vSphere appliance VMs. On each VM, right click and select **Power Off** then right click and select **Delete from Disk**.

   - Edge Services Gateway VM.
   - DLR Control VM.
   - NSX Controller VMs.
   - NSX Manager VM.

Troubleshooting NSX Data Center for vSphere Migration

You might see errors while trying to complete the NSX Data Center for vSphere migration. This troubleshooting information might help resolve the issues.

Accessing Migration Coordinator

Problem	Solution

Migration coordinator is not visible at **System > Migrate**.	Verify if the migration coordinator service is running on NSX Manager.
	`manager> get service migration-coordinator`
	`Service name: migration-coordinator`
	`Service state: running`
	If the service is not running, start it with `start service migration-coordinator`.

When returning to migration coordinator, the migration in progress is not visible.	The migration coordinator does not store the credentials of vCenter Server or NSX Manager. If the migration coordinator service is restarted when a migration is in progress, the **System > Migrate** page might display stale setup information, or no setup information. To display the latest migration status if the migration coordinator service is restarted, do the following: 1 Refresh the **System > Migrate** page. 2 Click **Get Started** and enter the credentials for vCenter Server and NSX Manager.

Import Configuration Problems

Problem	Solution
Import configuration fails.	1 Click **Retry** to try importing again. Only the failed import steps are retried.

Host Migration Problems

Problem	Solution
Host migration fails due to a missing compute manager configuration.	The compute manager configuration is a prerequisite for migration. However, if the compute manager configuration is removed from the NSX Manager after the migration is started, the migration coordinator retains the setting. The migration proceeds until the host migration step, which fails. Add a compute manager to NSX Manager and enter the same vCenter Server details that were used for the initial NSX for vSphere configuration import.

Host migration fails due to stale dvFilters present.
Example error message: `Stale dvFilters present: ['port 33554463 (disconnected)', 'port 33554464 (disconnected)'] Stale dvfilters present. Aborting ]`
	Log in to the host which failed to migrate, identify the disconnected ports, and either reboot the appropriate VM or connect the disconnected ports. Then you can retry the Host Migration step.
	1 Log into the command-line interface of the host which failed to migrate.
	2 Run `summarize-dvfilter` and look for the ports reported in the error message.
	`world 1000057161 vmm0:2-vm_RHEL-srv5.6.0.9-32-local-258-963adcb8-ab56-41d6-bd9e-2d1c329e7745 vcUuid:'96 3a dc b8 ab 56 41 d6-bd 9e 2d 1c 32 9e 77 45'`
	`port 33554463 (disconnected)`
	`vNic slot 2`
	`name: nic-1000057161-eth1-vmware-sfw.2`
	`agentName: vmware-sfw`
	`state: IOChain Detached`
	`vmState: Detached`
	`failurePolicy: failClosed`
	`slowPathID: none`
	`filter source: Dynamic Filter Creation`
	3 Locate the affected VM and port.
	For example, the error message says port `33554463` is disconnected.
	a Find the section of the `summarize-dvfilter` output that corresponds to this port. The VM name is listed here. In this case it is `2-vm_RHEL-srv5.6.0.9-32-local-258-963adcb8-ab56-41d6-bd9e-2d1c329e7745`.
	b Look for the `name` entry to determine which VM interface is disconnected. In this case, it is `eth1`. So the second interface of `2-vm_RHEL-srv5.6.0.9-32-local-258-963adcb8-ab56-41d6-bd9e-2d1c329e7745` is disconnected.
	4 Resolve the issue with this port. Do one of the following steps:
	■ Reboot the affected VM.
	■ Connect the disconnected vnic port to any network.

Problem	Solution
	5 On the **Migrate Hosts** page, click **Retry**.
After host migration using vMotion, VMs might experience traffic outage if SpoofGuard is enabled in NSX for vSphere. Symptoms: The `vmkernel.log` file on the host at `/var/run/log/` shows a drop in traffic due to SpoofGuard. For example, the log file shows: `WARNING: swsec.throttle: SpoofGuardMatchWL:296:[nsx@6876 comp="nsx-esx" subcomp="swsec"]Filter 0x8000012 [P]DROP sgType 4 vlan 0 mac 00:50:56:84:ee:db` Cause: The logical switch and the logical switch port configuration are migrated through the migration coordinator, which migrates the SpoofGuard configuration. However, the discovered port bindings are not migrated through vMotion. Therefore, SpoofGuard drops the packets.	If SpoofGuard is enabled in NSX for vSphere before migration, do any one of these workaround steps after vMotion of VMs: ■ Disable SpoofGuard policies. ■ Add the port IP and MAC address bindings as manual bindings. ■ If ARP snooping is enabled, wait for the VM IP addresses to be snooped by ARP. In the first two options, network traffic is restored immediately. In the third option: ■ Traffic downtime is observed until the VM sends an ARP request or reply. ■ If DHCP snooping is also enabled and the VM IP address was assigned by the DHCP server, then it will most likely be snooped as an ARP first and later as a DHCP-snooped IP address.

Migrating vSphere Networking 2

You can use the migration coordinator to migrate an existing vSphere Distributed Switch configuration to an NSX-T Data Center environment.

Migration coordinator moves the vSphere Distributed Switch, compute hosts, PNICs, vmkNICs, and vNIC backings to the N-VDS.

Note You can use migration coordinator to migrate vSphere Distributed Switch configurations to NSX-T only if NSX for vSphere is not installed on the host.

This chapter includes the following topics:

Understanding the vSphere Networking Migration

You can migrate one vSphere Distributed Switch at a time to NSX-T.

Overview of Migration Process

During the migration you will complete the following steps:

- Prepare your NSX-T environment.
  - Configure a compute manager in the NSX-T environment. Add the vCenter Server system that manages the vSphere Distributed Switch you want to migrate.
  - Start the migration coordinator service.
- Import configuration from vSphere.
  - Enter the details of your vSphere environment.
  - The configuration is retrieved and pre-checks are run.
- Select the vSphere Distributed Switch that you want to migrate.
- Resolve issues with the configuration.

Provide answers to configuration questions that must be resolved before you can migrate your vSphere environment to NSX-T. Resolving issues can be done in multiple passes by multiple people.

- Migrate configuration.
  - After all configuration issues are resolved, you can import the configuration to NSX-T. Configuration changes are made on NSX-T, but no changes are made to the vSphere environment yet.
- Migrate Hosts.
  - NSX-T software is installed on the hosts. VM interfaces are disconnected from vSphere Distributed Switch port groups and connected to the new NSX-T segments.

    Caution There is a traffic interruption during the migration of each host.
- Finish Migration.
  - After you have verified that the migrated networking is working correctly, you can click **Finish** to clear the migration state. You can now migrate another vSphere Distributed Switch to NSX-T.

Preparing to Migrate vSphere Networking

You can migrate vSphere Distributed Switches that are not part of an NSX Data Center for vSphere environment.

Required Software and Versions

- See the *VMware Product Interoperability Matrices* for required versions of vCenter Server and ESXi: http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php#interop&175=&1=&2=
- vSphere Distributed Switch version 6.5.0 and 6.6.0 are supported.

Add a Compute Manager

To migrate a vSphere Distributed Switch, you must configure the associated vCenter Server system as a compute manager in NSX-T before you can start the migration process.

Procedure

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

3 Complete the compute manager details.

Option	Description
Name and Description	Type the name to identify the vCenter Server. You can optionally describe any special details such as, the number of clusters in the vCenter Server.
Domain Name/IP Address	Type the IP address of the vCenter Server.
Type	Keep the default option.
Username and Password	Type the vCenter Server login credentials.
Thumbprint	Type the vCenter Server SHA-256 thumbprint algorithm value.

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

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

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

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

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

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

If an existing registration exists, it will be replaced.

Results

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

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

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

Migrate vSphere Networking to NSX-T Data Center

Use the migration coordinator to import your configuration, resolve issues with the configuration, and migrate hosts to your NSX-T Data Center environment.

Import the vSphere Networking Configuration

To migrate vSphere hosts and networking to NSX-T Data Center, you must provide details about your vSphere environment.

The migration coordinator service runs on one NSX Manager node. Perform all migration operations from the node that is running the migration coordinator service.

Prerequisites

- Verify that the vCenter Server system associated with the vSphere Distributed Switch you want to migrate is registered as a compute manager. See Add a Compute Manager.

Procedure

1. Log in to an NSX Manager CLI as **admin** and start the migration coordinator service.

```
nsx-manager> start service migration-coordinator
```

2. From a browser, log in to the NSX Manager node which is running the migration coordinator service. Log in using an account with admin privileges.
3. Navigate to **System > Migrate**.
4. On the **Migrate vSphere Networking** pane, click **Get Started**.
5. From the **Import Configuration** page, click **Select vSphere** and provide the requested information about your vSphere environment.

   Note The drop-down menu for vCenter displays all vCenter Server systems that are registered as compute managers. Click **Add New** if you need to add a compute manager.
6. Click **Start** to import the configuration.
7. When the import has finished, click **Continue** to proceed to the **Resolve Issues** page.

Roll Back or Cancel the vSphere Networking Migration

After you have started the migration process, you can roll back the migration to undo some or all of your progress. You can also cancel the migration, which removes all migration state.

You can roll back or undo the migration from some of the migration steps. After the migration has started, you can click **Rollback** on the furthest step completed. The button is disabled on all other pages.

Table 2-1. Rolling Back vSphere Networking Migration

Migration Step	Rollback Details
Import Configuration	Click **Rollback** on this page to roll back the Import Configuration step.
Resolve Configuration	Rollback is not available here. Click **Rollback** from the **Import Configuration** page.
Migrate Configuration	Click **Rollback** on this page to roll back the migration of the configuration to NSX-T and the input provided on the **Resolve Configuration** page.
Migrate Hosts	Rollback is not available here.

There is a **Cancel** button on every page of the migration. Canceling a migration deletes all migration state from the system. The migration coordinator shows the following warning message when you cancel a migration at any step:

```
Canceling the migration will reset the migration coordinator.
It is advisable to rollback this step first or it might leave the
the system in a partially migrated state. Do you want to continue?
```

Caution Do not cancel a migration if Host migration has started. Canceling the migration deletes all migration state and prevents you from rolling back the migration or viewing past progress.

Resolve Issues with the vSphere Networking Configuration

After you have imported the networking configuration from your vSphere environment, you must review and resolve the reported configuration issues before you can continue with the migration.

You must provide feedback for all configuration issues that must be resolved before the migration can continue. Multiple people can provide the feedback over multiple sessions. After you provide feedback for a given issue, you can click **Submit** to save it. You can return to a submitted input and modify it.

After you have submitted feedback for all issues, the feedback is validated. The validation might result in additional requests for feedback before the migration can proceed.

Procedure

1. From the **Resolve Configuration** page, click **Select Switch** to select which vSphere Distributed Switch to migrate.

   Once a distributed switch is selected, the configuration issues are displayed.

2. Review the reported issues.

   Issues are organized into groups. Each issue can cover multiple configuration items. For each item there might be one or more possibly resolutions to the issue, for example, skip, configure, or select a specific value.

3. Click each issue and provide feedback.

   For issues that apply to multiple configuration items, you can provide feedback for each individually, or select all and provide one answer for all items.

   Multiple people can provide the input over multiple sessions. You can return to a submitted input and modify it.

4. After some feedback has been provided, a **Submit** button appears on the **Resolve Issues** page. Click **Submit** to save your progress.

5. When you have provided feedback for all configuration issues, click **Submit**.

   The input is validated. You are prompted to update any invalid input. Additional input might be required for some configuration items.

6 After you have submitted all requested feedback, click **Continue** to proceed to the Migrate Configuration step.

Migrate vSphere Networking Configuration

After you have resolved all configuration issues, you can migrate the vSphere networking configuration. Configuration changes are made in the NSX-T environment to replicate the translated vSphere configuration.

If needed, you can roll back the configuration migration. This will do the following:

- Remove the migrated configuration from NSX-T.
- Roll back all the resolved issues in the previous step.

See Roll Back or Cancel the vSphere Networking Migration for more information.

Prerequisites

Verify you have completed the **Resolve Configuration** step.

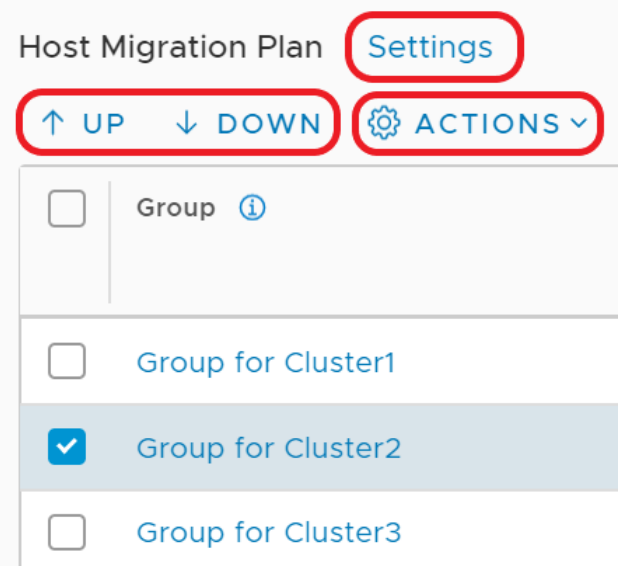
Procedure

- From the **Migrate Configuration** page, click **Start**.

  The distributed switch configuration is migrated to NSX-T.

Configuring vSphere Host Migration

The clusters in the vSphere environment are displayed on the **Migrate Hosts** page. The clusters are arranged into migration groups, each migration group contains one vSphere host cluster. There are several settings which control how the host migration is performed.



- Click **Settings** to change the global settings: **Pause Between Groups** and **Migration Order Across Groups**.

- Select a single host group (cluster) and use the arrows to move it up or down in the migration sequence.
- Select one or more host groups (clusters) and click **Actions** to change these host groups settings: **Migration Order Within Groups**, **Migration State**, and **Migration Mode**.

Pause Between Groups

Pause Between Groups is a global setting that applies to all host groups. If pausing is enabled, the migration coordinator migrates one host group, and then waits for input. You must click **Continue** to continue to the next host group. If you want to verify the status of each cluster before proceeding to the next one, enable **Pause Between Groups**.

By default, **Pause Between Groups** is disabled.

Note This feature is useful because it verifies the application on the current cluster before migrating the next cluster.

Serial or Parallel Migration Order

You can define whether migration happens in a serial or parallel order. There are two ordering settings:

- **Migration Order Across Groups** is a global setting that applies to all host groups.
  - **Serial**: One host group (cluster) at a time is migrated.
  - **Parallel**: Up to five host groups at a time are migrated. After those five host groups are migrated, the next batch of up to five host groups are migrated.
- **Migration Order Within Groups** is a host group (cluster) specific setting, so can be configured separately on each host group.
  - **Serial**: One host within the host group (cluster) at a time is migrated.
  - **Parallel**: Up to five hosts within the host group are migrated at a time. After those hosts are migrated, the next batch of up to five hosts are migrated.

    Important Do not select parallel migration order within groups for a cluster if you plan to use **Maintenance** migration mode for that cluster.

By default, both settings are set to **Serial**. Together, the settings determine how many hosts are migrated at a time.

Table 2-2. Effects of Migration Settings on Number of Hosts Attempting Migration Simultaneously

Migration Order Across Groups (Clusters)	Migration Order Within Groups (Clusters)	Maximum Number of Hosts Attempting Migration Simultaneously
Serial	Serial	1 One host from one host group
Serial	Parallel	5 Five hosts from one host group
Parallel	Serial	5 One host from five host groups
Parallel	Parallel	25 Five hosts from five host groups

Important If there is a failure to migrate a host, the migration process will pause after all in-progress host migrations have finished. If **Parallel** is selected for both migration across groups and migration within groups, there might be a long outage for the failed host before you can retry migration.

Sequence of Migration Groups

You can select a host group (cluster) and use the arrows to move it up or down in the list of groups.

If migration fails for a host, you can move its host group to the bottom of the list of groups. The migration of other host groups can proceed while you resolve the problem with the failed host.

Migration State

Host groups (clusters) can have one of three states:

- **Enabled**

  Hosts groups with a migration state of **Enabled** are migrated to NSX-T when you click **Start** on the **Migrate Hosts** page.

- **Disabled**

  You can temporarily exclude host groups from migration by setting the migration state for the groups to **Disabled**. Hosts in disabled groups are not migrated to NSX-T when you click **Start** on the **Migrate Hosts** page. However, you must enable and migrate all **Disabled** host groups before you can click **Finish**. Finish all host migration tasks and click **Finish** within the same maintenance window.

Migrate vSphere Hosts

After you have migrated the configuration, you can migrate the vSphere hosts to NSX-T Data Center.

You can configure several settings related to the host migration, including migration order and enabling hosts. Before you change any default settings, make sure that you understand the effects of these settings. See Configuring vSphere Host Migration for more information.

Caution There is a traffic interruption during the host migration. Perform this step during a maintenance window.

If migration fails for a host, the migration pauses after all in-progress host migrations finish. When you have resolved the problem with the host, click **Retry** to retry migration of the failed host.

If migration fails for a host, you can move its host group to the bottom of the list of groups. The migration of other host groups can proceed while you resolve the problem with the failed host.

After a host has migrated to NSX-T, you might see an alarm with message `Lost network connectivity`. The alarm occurs because the host no longer has a physical NIC connected to the vSphere Distributed Switch it was previously connected to.

Prerequisites

- Verify that all ESXi hosts are in an operational state. Address any problems with hosts including disconnected states. There must be no pending reboots or pending tasks for entering maintenance mode.

Procedure

1 Click **Start** to start the host migration.

If you selected the **In-Place** migration mode for all hosts groups, the host migration starts.

2 If you selected the **Maintenance** migration mode for any host groups, you must complete one of the following tasks for each VM so that the hosts can enter maintenance mode.

Option	Action
Power off or suspend VMs.	a Right click the VM and select **Power > Power off** , **Power > Shut Down Guest OS**, or **Power > Suspend**. b After the host has migrated, attach the VM interfaces to the appropriate NSX-T segments and power on the VM.
Move VMs to a vSphere host using cold migration or vMotion.	a (Optional) To cold migrate, right click the VM and select **Power > Power off** , **Power > Shut Down Guest OS**, or **Power > Suspend**. b Right click the VM and select Migrate. Follow the prompts to move the VM to a different host.
Move VMs to an NSX-T host using cold migration.	a Right click the VM and select **Power > Power off** , **Power > Shut Down Guest OS**, or **Power > Suspend**. b Right click the VM and select Migrate. Follow the prompts to move the VM to a different host, connecting the VM interfaces to the appropriate NSX-T segments.

Caution Using vMotion to move powered-on VMs to NSX-T is not supported.

The host enters maintenance mode after all VMs are powered off or suspended. If you want to use cold migration to move the VMs to a different host before the migrating host enters maintenance mode, you must leave at least one VM running while you move VMs. When the last VM is powered off or suspended, the host enters maintenance mode, and migration of the host to NSX-T starts.

Finish Migration

After you have migrated hosts to the NSX-T Data Center environment, confirm that the new environment is working correctly. If everything is functioning correctly, you can finish the migration.

Important Verify everything is working and click **Finish** within the maintenance window. Clicking **Finish** performs some post-migration clean-up. Do not leave the migration coordinator in a unfinished state beyond the migration window.

Prerequisites

Verify that the NSX-T Data Center environment is working correctly.

Procedure

1. Navigate to the **Migrate Hosts** page of the migration coordinator.
2. Click **Finish**

   A dialog box appears to confirm finishing the migration. If you finish the migration, all migration details are cleared. You can no longer review the settings of this migration. For example, which inputs were made on the **Resolve Issues** page.