

Handbuch zum Migrations- Koordinator von NSX-T Data Center

23. August 2019

VMware NSX-T Data Center 2.4



vmware®

Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

<https://docs.vmware.com/de/>

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Copyright © 2019 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

Handbuch zum Migrations-Koordinator von NSX-T Data Center 4

1 Migrieren von NSX Data Center for vSphere 5

- Grundlegendes zur NSX Data Center for vSphere-Migration 5
 - Vom Migrations-Koordinator unterstützte Funktionen 5
 - Vom Migrations-Koordinator unterstützte Topologien 28
 - Vom Migrationskoordinator unterstützte Grenzwerte 36
 - Überblick über die Migration mithilfe des Migrations-Koordinators 37
 - Bereitstellung einer virtuellen Maschine während der Migration 39
- Vorbereiten der Migration einer NSX Data Center for vSphere-Umgebung 39
 - Vorbereiten der NSX-T Data Center-Umgebung 40
 - Vorbereiten der NSX Data Center for vSphere-Umgebung auf die Migration 48
- Migrieren von NSX Data Center for vSphere auf NSX-T Data Center 52
 - Importieren der NSX Data Center for vSphere-Konfiguration 52
 - Abbrechen oder Neustarten der NSX for vSphere-Migration 53
 - Beheben von Konfigurationsproblemen und Bereitstellen von Edge-Knoten 54
 - Migrieren der NSX Data Center for vSphere-Konfiguration 61
 - Ändern der Edge-Konfiguration vor dem Migrieren von Edges 62
 - NSX Data Center for vSphere-Edges migrieren 63
 - Konfigurieren der Hostmigration 63
 - Abschließen der NSX Data Center for vSphere-Migration 68
- Deinstallieren von NSX for vSphere nach der Migration 68
- Fehlerbehebung bei der Migration von NSX Data Center for vSphere 71

2 Migration von vSphere-Netzwerken 75

- Grundlegendes zur Migration des vSphere-Netzwerks 75
- Vorbereiten der Migration des vSphere-Netzwerks 76
 - Hinzufügen eines Berechnungsmanagers 76
- Migrieren eines vSphere-Netzwerks zu NSX-T Data Center 77
 - Importieren der vSphere-Netzwerkkonfiguration 77
 - Abbrechen oder Neustarten der vSphere-Netzwerkmigration 78
 - Beheben von Problemen bei der Konfiguration des vSphere-Netzwerks 79
 - Migrieren einer vSphere-Netzwerkkonfiguration 80
 - Konfigurieren der Hostmigration 80
 - Abschließen der Migration 84

Handbuch zum Migrations-Koordinator von NSX-T Data Center

Das *Handbuch zum Migrations-Koordinator von NSX-T Data Center* bietet Informationen zum Migrieren einer VMware NSX[®] for vSphere[®]-Umgebung auf eine VMware NSX-T[™]-Umgebung mithilfe des Migrations-Koordinators.

Es enthält auch Informationen zum Migrieren von Netzwerkkonfigurationen aus VMware vSphere[®] auf eine NSX-T Data Center-Umgebung mithilfe des Migrations-Koordinators.

Zielgruppe

Dieses Handbuch richtet sich an Personen, die mithilfe des Migrations-Koordinators eine Migration einer NSX Data Center for vSphere-Umgebung oder eines vSphere-Netzwerks auf eine NSX-T Data Center-Umgebung durchführen möchten. Die Informationen sind für erfahrene Netzwerk- und Systemadministratoren bestimmt, die mit der VM-Technologie und Datencenter-Vorgängen vertraut sind.

Migrieren von NSX Data Center for vSphere

1

Sie können den Migrations-Koordinator verwenden, um Ihr NSX Data Center aus einer vorhandenen NSX for vSphere-Umgebung in eine leere NSX-T-Umgebung zu migrieren.

Wichtig Die Migration verursacht Ausfälle im Datenverkehr, während die Migrationsschritte für Edges und Hosts ausgeführt werden. Sie müssen die Migration innerhalb eines einzelnen Wartungsfensters abschließen. Wenden Sie sich an das VMware-Support-Team, bevor Sie eine Migration durchführen.

Dieses Kapitel enthält die folgenden Themen:

- [Grundlegendes zur NSX Data Center for vSphere-Migration](#)
- [Vorbereiten der Migration einer NSX Data Center for vSphere-Umgebung](#)
- [Migrieren von NSX Data Center for vSphere auf NSX-T Data Center](#)
- [Deinstallieren von NSX for vSphere nach der Migration](#)
- [Fehlerbehebung bei der Migration von NSX Data Center for vSphere](#)

Grundlegendes zur NSX Data Center for vSphere-Migration

Die Migration von NSX for vSphere zu NSX-T erfordert Planung und Vorbereitung. Sie sollten mit den Konzepten und Verwaltungsaufgaben in NSX-T vertraut sein, bevor Sie eine Migration durchführen.

Die Vorbereitung umfasst unter Umständen eine Änderung der vorhandenen NSX for vSphere-Umgebung sowie das Einrichten einer neuen NSX-T-Umgebung.

Vom Migrations-Koordinator unterstützte Funktionen

Ein Teil der NSX Data Center for vSphere-Funktionen wird vom Migrations-Koordinator unterstützt.

Für die meisten Funktionen gelten bestimmte Einschränkungen. Wenn Sie Ihre NSX Data Center for vSphere-Konfiguration in den Migrations-Koordinator importieren, erhalten Sie ein detailliertes Feedback darüber, welche Funktionen und Konfigurationen in Ihrer Umgebung unterstützt oder nicht unterstützt werden.

Ausführliche Informationen zu den vom Migrationskoordinator unterstützten Elementen finden Sie unter [Detaillierte Funktionsunterstützung für Migrationskoordinator](#).

Tabelle 1-1. Support-Matrix für Migrations-Koordinator

Funktion „NSX Data Center for vSphere“	Unterstützt	Details und Einschränkungen
VLAN-gestützte logische Switches	Ja	
Overlay-gestützte logische Switches	Ja	
L2-Bridges	Nein	
Transportzonen	Ja	
Routing	Ja	Weitere Informationen finden Sie unter Vom Migrations-Koordinator unterstützte Topologien .
Ost-West-Mikrosegmentierung	Ja	
Edge-Firewall	Ja	
NAT	Ja	
L2-VPN	Ja	
L3-VPN	Ja	
Load Balancer	Ja	
DHCP und DNS	Ja	
Verteilte Firewall	Ja	
Service Composer	Ja	Es werden nur Firewallregeln migriert. Guest Introspection-Regeln und Netzwerkselbstprüfungsregeln werden nicht migriert.
Objekte werden gruppiert	Ja	Zu den Einschränkungen gehören die Anzahl der Elemente und dynamische Ausdrücke, aus denen Sicherheitsgruppen bestehen.
Guest Introspection	Nein	
Netzwerkselbstprüfung	Nein	
Endpoint-Schutz	Nein	
Cross-vCenter NSX	Nein	
NSX Data Center for vSphere mit einer Cloud Management-Plattform, einer Integrated Stack- oder PaaS-Lösung.	Nein	Wenden Sie sich an Ihren VMware-Vertreter, bevor Sie mit der Migration fortfahren. Skripts und Integrationen werden bei der Migration unter Umständen abgebrochen.

Detaillierte Funktionsunterstützung für Migrationskoordinator

Plattformunterstützung

Weitere Informationen finden Sie in der VMware-Interoperabilitätsmatrix für unterstützte Versionen von ESXi und vCenter Server: http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php#interop&175=&1=&2=.

Konfiguration	Unterstützt	Details
Bereits vorhandene NSX-T-Konfiguration	Nein	Stellen Sie eine neue NSX-T-Umgebung als Ziel für die NSX for vSphere-Migration bereit. Während des Schritts Konfiguration importieren werden alle Edge-Knoten-Schnittstellen in der NSX-T-Zielumgebung heruntergefahren. Wenn die NSX-T-Zielumgebung bereits konfiguriert ist und verwendet wird, wird der Datenverkehr beim Starten des Konfigurationsimports unterbrochen.
Cross-vCenter NSX	Nein	
NSX for vSphere mit vSAN oder iSCSI auf vSphere Distributed Switch	Nein	
NSX for vSphere mit einer Cloud Management-Plattform, Integrated Stack- oder PaaS-Lösung	Nein	Wenden Sie sich an Ihren VMware-Vertreter, bevor Sie mit der Migration fortfahren. Skripts und Integrationen werden bei der Migration unter Umständen abgebrochen. Beispiel: <ul style="list-style-type: none"> ■ NSX for vSphere und vRealize Automation ■ NSX for vSphere und VMware Integrated OpenStack ■ NSX for vSphere und vCloud Director ■ NSX for vSphere mit Integrated Stack-Lösung ■ NSX for vSphere mit PaaS-Lösung wie Pivotal Cloud Foundry, RedHat OpenShift ■ NSX for vSphere mit vRealize Operations-Workflows

vSphere-und ESXi-Funktionen

Konfiguration	Unterstützt	Details
vSphere Standard-Switch	Nein	VMs und VMKernel-Schnittstellen auf VSS werden nicht migriert. NSX for vSphere-Funktionen, die auf den VSS angewendet werden, können nicht migriert werden.
Statusfreies ESXi	Nein	
Hostprofile	Nein	

Konfiguration	Unterstützt	Details
ESXi-Sperrmodus	Nein	Nicht in NSX-T unterstützt.
Wartungsmodus des ESXi-Hosts ausstehend.	Nein	
ESXi-Host befindet sich bereits im Wartungsmodus (keine VMs)	Ja	
Getrennter ESXi-Host im vCenter-Cluster	Nein	
vSphere Distributed Switch mit LACP-Teaming-Richtlinie	Ja	Die Spanning-Tree-Portfast-Funktion muss auf dem physischen Switch aktiviert sein
vSphere FT	Nein	
vSphere DRS vollständig automatisiert	Nein	DRS in den manuellen Modus versetzen, bevor der Migrationskoordinator ausgeführt wird
vSphere High Availability	Nein	
Zugriffskontrollliste für Datenverkehrsfilterung	Nein	
Network I/O Control (NIOC) Version 2	Nein	
Network I/O Control (NIOC) Version 3	Ja	
Network I/O Control (NIOC) mit vNIC mit Reservierung	Nein	
vSphere-Systemdiagnose	Nein	
SRIOV	Nein	
vmknics an physische Netzwerkkarte anheften	Nein	
Privates VLAN	Nein	
Flüchtige dvPortGroup	Nein	
DirectPath IO	Nein	
L2-Sicherheit	Nein	
Switch auf virtuellem Kabel erlernen	Nein	
Hardware-Gateway (Tunnel-Endpoint-Integration mit physischer Switching-Hardware)	Nein	
SNMP	Nein	
Getrennte vNIC in VM	Nein	Aufgrund der ESX 6.5-Einschränkung können veraltete Einträge in DVFilter für getrennte VMs vorhanden sein. Starten Sie die VM zur Problemumgehung neu.
Andere VXLAN-Portnummer als 4789	Nein	
Multicast-Filtermodus	Nein	

Systemkonfiguration der NSX Manager-Appliance

Konfiguration	Unterstützt	Details
FIPS	Nein	FIPS ein/aus wird von NSX-T nicht unterstützt.
Gebietsschema	Nein	NSX-T unterstützt nur das englische Gebietsschema
Appliance-Zertifikat	Nein	
NTP-Server/Zeiteinstellung	Ja	
Syslog-Serverkonfiguration	Ja	
Konfiguration sichern	Ja	<p>Ändern Sie bei Bedarf die NSX Data Center for vSphere-Passphrase entsprechend den Anforderungen von NSX-T Data Center. Sie muss mindestens 8 Zeichen lang sein und Folgendes enthalten:</p> <ul style="list-style-type: none"> ■ Mindestens ein Kleinbuchstabe ■ Mindestens ein Großbuchstabe ■ Mindestens ein numerisches Zeichen ■ mindestens ein Sonderzeichen

Rollenbasierte Zugriffssteuerung

Konfiguration	Unterstützt	Details
Lokale Benutzer	Nein	
NSX-Rollen, die einem vCenter-Benutzer, der über LDAP hinzugefügt wurde, zugewiesen werden	Ja	vSphere Identity Manager muss installiert und konfiguriert sein, um Benutzerrollen für LDAP-Benutzer zu migrieren.
Einer vCenter-Gruppe zugewiesene NSX-Rollen	Nein	

Zertifikate

Konfiguration	Unterstützt	Details
Zertifikate (Server, von Zertifizierungsstelle signiert)	Ja	Dies gilt nur für Zertifikate, die nur über Truststore-APIs hinzugefügt werden.

Betrieb

Details	Unterstützt	Anmerkungen
Discovery-Protokoll CDP	Nein	
Discovery-Protokoll LLDP	Ja	Der Listening-Modus ist standardmäßig aktiviert und kann in NSX-T nicht geändert werden. Nur der Ankündigungsmodus kann geändert werden.

Details	Unterstützt	Anmerkungen
PortMirroring: ■ Gekapselte Remotespiegelungsquelle (L3)	Ja	Nur L3-Sitzungstyp wird für die Migration unterstützt
PortMirroring: ■ Verteiltes PortMirroring ■ Remotespiegelungsquelle ■ Remotespiegelungsziel ■ Spiegelung verteilter Ports (Legacy)	Nein	
L2-IPFIX	Ja	Lag mit IPFIX wird nicht unterstützt
Verteilte Firewall und IPFIX	Nein	
MAC-Lernvorgang	Ja	Sie müssen gefälschte Übertragungen aktivieren (akzeptieren).
Hardware-VTEP	Nein	
Promiskuitiver Modus	Nein	
Ressourcenzuteilung	Nein	VmVnic mit aktivierter Ressourcenzuteilung wird nicht unterstützt
IpFix – interne Flows	Nein	IpFix mit InternalFlows wird nicht unterstützt

Switch

Konfiguration	Unterstützt	Details
L2-Bridging	Nein	
Trunk-VLAN	Ja	Trunk-Uplink-Portgruppen muss mit einem VLAN-Bereich von 0–4094 konfiguriert werden.
VLAN-Konfiguration	Ja	Nur die Verzögerung mit der VLAN-Konfiguration wird nicht unterstützt
Teaming und Failover: ■ Lastausgleich ■ Uplink-Failover-Reihenfolge	Ja	Unterstützte Optionen für den Lastausgleich (Teaming-Richtlinie): ■ Ausdrückliche Failover-Reihenfolge verwenden ■ Anhand des Quell-MAC-Hashs routen Andere Lastausgleichsoptionen werden nicht unterstützt.
Teaming und Failover: ■ Netzwerkausfallerkennung ■ Switches benachrichtigen ■ Umkehrrichtlinie ■ Fortlaufende Reihenfolge	Nein	

Switch-Sicherheit und IP-Ermittlung

Konfiguration	Unterstützt	Details
IP-Ermittlung (ARP, ND, DHCPv4 und DHCPv6)	Ja	Die folgenden Bindungsgrenzwerte gelten für NSX-T für die Migration: <ul style="list-style-type: none"> ■ 128 für per ARP erkannte IPs ■ 128 für per DHCPv4 erkannte IPs ■ 15 für per DHCPv6 erkannte IPs ■ 15 für per ND erkannte IPs
SpoofGuard (manuell, TOFU, deaktiviert)	Ja	
Switch-Sicherheit (BPDU-Filter, DHCP-Clientblock, DHCP-Serverblock, RA-Guard)	Ja	
Migrieren von Datenpfadbindungen vom Switch-Sicherheitsmodul in NSX for vSphere zum Switch-Sicherheitsmodul in NSX-T	Ja	Wenn SpoofGuard aktiviert ist, werden Bindungen aus dem Switch-Sicherheitsmodul migriert, um die ARP-Unterdrückung zu unterstützen. VSIP – Switch-Sicherheit wird nicht unterstützt, da VSIP-Bindungen als statisch konfigurierte Regeln migriert werden.
Ermittlungsprofile	Ja	Die ipdiscovery-Profile werden nach der Migration mithilfe der IP-Ermittlungskonfiguration für den logischen Switch und der globalen und Cluster-ARP- und DHCP-Konfiguration erstellt.

Zentrale Steuerungskomponente

Konfiguration	Unterstützt	Details
VTEP-Replikation pro logischem Switch (VNI) und Routing-Domäne	Ja	
MAC/IP-Replikation	Nein	
NSX for vSphere-Transportzonen mit Multicast-oder Hybrid-Replikationsmodus	Nein	
NSX for vSphere-Transportzonen mit Unicast-Replikationsmodus	Ja	

Funktionen von NSX Edge

Ausführliche Informationen zu unterstützten Topologien finden Sie unter [Vom Migrations-Koordinator unterstützte Topologien](#).

Konfiguration	Unterstützt	Details
Routing zwischen Edge Services Gateway und Northbound-Router oder virtueller Tunnelschnittstelle	Ja	BGP wird unterstützt. Statische Routen werden unterstützt. OSFP wird nicht unterstützt.
Routing zwischen Edge Services Gateway und Distributed Logical Router	Ja	Routen werden nach der Migration in statische Routen umgewandelt.
Load Balancer	Ja	Weitere Informationen finden Sie unter Vom Migrations-Koordinator unterstützte Topologien .
VLAN-gestützte Mikrosegmentierungs-Umgebung	Ja	Weitere Informationen finden Sie unter Vom Migrations-Koordinator unterstützte Topologien .
NAT64	Nein	Nicht in NSX-T unterstützt.
Einstellungen auf Knotenebene auf einem Edge Services Gateway oder einem Distributed Logical Router	Nein	Einstellungen auf Knotenebene, z. B. syslog oder NTP-Server, werden nicht unterstützt.
IPv6	Nein	
Konfiguration für umgekehrten Unicast-Pfadfilter (URPF) für Edge Services Gateway-Schnittstellen	Nein	URPF auf NSX-T-Gateway-Schnittstellen ist auf „Streng“ festgelegt.
Konfiguration der maximalen Übertragungseinheit (MTU) für Edge Services Gateway-Schnittstellen	Nein	Informationen zum Ändern der Standard-MTU auf NSX-T finden Sie unter Ändern der Edge-Konfiguration vor dem Migrieren von Edges .
IP-Multicast-Routing	Nein	
Präfixfilter für Route Redistribution	Nein	
Default Originate	Nein	Nicht in NSX-T unterstützt.

Edge-Firewall

Konfiguration	Unterstützt	Details
Abschnitt "Firewall": Anzeigename	Ja	Firewallabschnitte können maximal 1000 Regel aufweisen. Wenn ein Abschnitt mehr als 1000 Regeln enthält, wird er als mehrere Abschnitte migriert.
Aktion für Standardregel	Ja	NSX for vSphere-API: GatewayPolicy/action NSX-T-API: SecurityPolicy.action
Globale Firewallkonfiguration	Nein	Standard-Zeitüberschreitungen werden verwendet
Firewallregel	Ja	NSX for vSphere-API: firewallRule NSX-T-API: SecurityPolicy
Firewallregel: Name	Ja	

Konfiguration	Unterstützt	Details
Firewallregel: Regel-Tag	Ja	NSX for vSphere-API: ruleTag NSX-T-API: Rule_tag
Quellen und Ziele in Firewallregeln: ■ Objekte werden gruppiert ■ IP-Adressen	Ja	NSX for vSphere-API: ■ source/groupingObjectId ■ source/ipAddress NSX-T-API: ■ source_groups NSX for vSphere-API: ■ destination/groupingObjectId ■ destination/ipAddress NSX-T-API: ■ destination_groups
Firewallregelquellen und -ziele: ■ vNIC-Gruppe	Nein	
Dienste (Anwendungen) in Firewallregeln: ■ Dienst ■ Dienstgruppe ■ Protokoll/Port/Quellport	Ja	NSX for vSphere-API: ■ application/applicationId ■ application/service/protocol ■ application/service/port ■ application/service/sourcePort NSX-T-API: ■ Dienste
Firewallregel: Übersetzung zuordnen	Nein	Übersetzungszuordnung muss „false“ sein.
Firewallregel: Richtung	Ja	Beide APIs: direction
Firewallregel: Aktion	Ja	Beide APIs: action
Firewallregel: Aktiviert	Ja	Beide APIs: enabled
Firewallregel: Protokollierung	Ja	NSX for vSphere-API: logging NSX-T-API: logged
Firewallregel: Beschreibung	Ja	Beide APIs: description

Edge-NAT

Konfiguration	Unterstützt	Details
NAT-Regel	Ja	NSX for vSphere-API: natRule NSX-T-API: /nat/USER/nat-rules
NAT-Regel: Regel-Tag	Ja	NSX for vSphere-API: ruleTag NSX-T-API: rule_tag
NAT-Regel: Aktion	Ja	NSX for vSphere-API: action NSX-T-API: action

Konfiguration	Unterstützt	Details
NAT-Regel: ursprüngliche Adresse (Quelladresse für SNAT-Regeln und die Zieladresse für DNAT-Regeln.)	Ja	NSX for vSphere-API: originalAddress NSX-T-API: source_network für SNAT-Regel oder destination_network für DNAT-Regel
NAT-Regel: translatedAddress	Ja	NSX for vSphere-API: translatedAddress NSX-T-API: translated_network
NAT-Regel: Anwenden einer NAT-Regel auf eine bestimmte Schnittstelle	Nein	„Angewendet auf“ muss „Alle“ sein.
NAT-Regel: Protokollierung	Ja	NSX for vSphere-API: loggingEnabled NSX-T-API: logging
NAT-Regel: aktiviert	Ja	NSX for vSphere-API: enabled NSX-T-API: disabled
NAT-Regel: Beschreibung	Ja	NSX for vSphere-API: description NSX-T-API: description
NAT-Regel: Protokoll	Ja	NSX for vSphere-API: protocol NSX-T-API: Service
NAT-Regel: ursprünglicher Port (Quellport für SNAT-Regeln, Zielport für DNAT-Regeln)	Ja	NSX for vSphere-API: originalPort NSX-T-API: Service
NAT-Regel: übersetzter Port	Ja	NSX for vSphere-API: translatedPort NSX-T-API: Translated_ports
NAT-Regel: Quelladresse in DNAT-Regel	Ja	NSX for vSphere-API: dnatMatchSourceAddress NSX-T-API: source_network
NAT-Regel: Zieladresse in SNAT-Regel	Ja	NSX for vSphere-API: snatMatchDestinationAddress NSX-T-API: destination_network
NAT-Regel: Quellport in DNAT-Regel	Ja	NSX for vSphere-API: dnatMatchSourcePort NSX-T-API: Service
NAT-Regel: Zielport in SNAT-Regel	Ja	NSX for vSphere-API: snatMatchDestinationPort NSX-T-API: Service
NAT-Regel: Regel-ID	Ja	NSX for vSphere-API: ruleID NSX-T-API: id und display_name

L2 VPN

Konfiguration	Unterstützt	Details
L2VPN-Konfiguration basierend auf IPSec mithilfe von Pre-Shared Key (PSK)	Ja	Wird unterstützt, wenn das Netzwerk, das über L2VPN ausgedehnt wird, ein logischer Overlay-Switch ist. Wird nicht für VLAN-Netzwerke unterstützt.
L2VPN-Konfiguration basierend auf IPSec mithilfe der zertifikatbasierten Authentifizierung	Nein	
L2VPN-Konfiguration basierend auf SSL	Nein	
L2VPN-Konfigurationen mit lokalen Ausgangsoptimierungen	Nein	
L2VPN-Clientmodus	Nein	

L3VPN

Konfiguration	Unterstützt	Details
Erkennung inaktiver Peers	Ja	Die Erkennung inaktiver Peers unterstützt verschiedene Optionen auf NSX for vSphere und NSX-T. Es kann sinnvoll sein, BGP für eine schnellere Konvergenz zu verwenden oder einen Peer zur Durchführung von DPD zu konfigurieren, wenn dies unterstützt wird.
Die Standardwerte für die Erkennung inaktiver Peers (Dead Peer Detection, DPD) wurden geändert für: <ul style="list-style-type: none"> ■ dpdtimeout ■ dpdaction 	Nein	In NSX-T ist dpdaction auf „restart“ festgelegt und kann nicht geändert werden. Wenn die NSX for vSphere-Einstellung für dpdtimeout auf 0 festgelegt ist, wird dpd in NSX-T deaktiviert. Andernfalls werden alle dpdtimeout-Einstellungen ignoriert, und der Standardwert wird verwendet.
Die Standardwerte für die Erkennung inaktiver Peers (Dead Peer Detection, DPD) wurden geändert für: <ul style="list-style-type: none"> ■ dpddelay 	Ja	NSX for vSphere dpddelay wird NSX-T dpdinternal zugeordnet.
Überlappende lokale und Peer-Subnetze von zwei oder mehr Sitzungen.	Nein	NSX for vSphere unterstützt richtlinienbasierte IPSec-VPN-Sitzungen, in denen lokale und Peer-Subnetze von zwei oder mehr Sitzungen miteinander überlappen. Dieses Verhalten wird auf NSX-T nicht unterstützt. Sie müssen die Subnetze vor dem Start der Migration neu konfigurieren, damit sie sich nicht überlappen. Wenn dieses Konfigurationsproblem nicht behoben wird, schlägt der Schritt „Konfiguration migrieren“ fehl.

Konfiguration	Unterstützt	Details
IPsec-Sitzungen mit Peer-Endpoint als „Alle“ festgelegt.	Nein	Konfiguration wird nicht migriert.
Änderungen an der Erweiterung securelocaltrafficbyip.	Nein	Der NSX-T-Dienstrouter verfügt über keinen lokalen generierten Datenverkehr, der über den Tunnel gesendet werden muss.
Änderungen an diesen Erweiterungen: auto, sha2_truncbug, sarefttrack, leftid, leftsendcert, leftauthserver, leftauthclient, leftauthusername, leftmodecfgserver, leftmodecfgclient, modecfgpull, modecfgdns1, modecfgdns2, modecfgwins1, modecfgwins2, remote_peer_type, nm_configured, forceencaps,overlapip, aggrmode, rekey, rekeymargin, rekeyfuzz, compress, metric,disablearrivalcheck, failurehunt,leftnexthop, keyingtries	Nein	Diese Erweiterungen werden auf NSX-T nicht unterstützt, und Änderungen an ihnen werden nicht migriert.

Load Balancer

Konfiguration	Unterstützt	Details
Überwachung/Integritätsprüfungen für: ■ LDAP ■ DNS ■ MSSQL	Nein	Wenn eine nicht unterstützte Überwachung konfiguriert ist, wird die Überwachung ignoriert, und für den zugehörigen Pool ist keine Überwachung konfiguriert. Sie können ihn nach Abschluss der Migration an eine neue Überwachung anbinden.
Anwendungsregeln	Nein	NSX for vSphere verwendet Anwendungsregeln auf Basis von HAProxy zur Unterstützung von L7. In NSX-T basieren die Regeln auf NGINX. Die Anwendungsregeln können nicht migriert werden. Nach der Migration müssen Sie neue Regeln erstellen.
Portbereich des virtuellen L7-Servers	Nein	
IPv6	Nein	Wenn IPv6 in einem virtuellen Server verwendet wird, wird der gesamte virtuelle Server ignoriert. Wenn IPv6 im Pool verwendet wird, wird der Pool migriert, aber das zugehörige Poolmitglied entfernt.
URL-, URI-, HTTPHEADER-Algorithmen	Nein	Bei Verwendung in einem Pool wird der Pool nicht migriert.
Isolierter Pool	Nein	Der Pool wird nicht migriert.

Konfiguration	Unterstützt	Details
LB-Poolmitglied mit anderem Überwachungsport	Nein	Das Poolmitglied mit dem anderen Überwachungsport wird nicht migriert.
Poolmitglied minConn	Nein	Konfiguration wird nicht migriert.
Überwachungserweiterung	Nein	Konfiguration wird nicht migriert.
SSL-sessionID-Persistenz/-Tabelle	Nein	Die Konfiguration wird nicht migriert, und der zugeordnete virtuelle Server hat keine Persistenzeinstellung.
MSRDP-Persistenz/-Sitzungstabelle	Nein	Die Konfiguration wird nicht migriert, und der zugeordnete virtuelle Server hat keine Persistenzeinstellung.
Cookie-App-Sitzung/-Sitzungstabelle	Nein	Die Konfiguration wird nicht migriert, und der zugeordnete virtuelle Server hat keine Persistenzeinstellung.
App-Persistenz	Nein	Die Konfiguration wird nicht migriert, und der zugeordnete virtuelle Server hat keine Persistenzeinstellung.
Überwachen auf: <ul style="list-style-type: none"> ■ Explizites Escape ■ Beenden ■ Verzögerung 	Nein	
Überwachen auf: <ul style="list-style-type: none"> ■ Senden ■ Erwarten ■ Zeitüberschreitung ■ Intervall ■ maxRetries 	Ja	
Haproxy-Tuning/IPVS-Tuning	Nein	
Pool-IP-Filter <ul style="list-style-type: none"> ■ IPv4-Adressen 	Ja	IPv4-IP-Adressen werden unterstützt. Wenn „Alle“ verwendet wird, werden nur die IPv4-Adressen des IP-Pools migriert.
Pool-IP-Filter <ul style="list-style-type: none"> ■ IPv6-Adressen 	Nein	
Pool mit nicht unterstütztem Gruppierungsobjekt: <ul style="list-style-type: none"> ■ Cluster ■ Datacenter ■ Verteilte Portgruppe ■ MAC-Set ■ Virtuelle App 	Nein	Wenn ein Pool ein nicht unterstütztes Gruppierungsobjekt enthält, werden diese Objekte ignoriert, und der Pool wird mit unterstützten Gruppierungsobjektmitgliedern erstellt. Wenn keine unterstützten Gruppierungsobjektmitglieder vorhanden sind, wird ein leerer Pool erstellt.

DHCP und DNS

Tabelle 1-2. DHCP-Konfigurationstopologien

Konfiguration	Unterstützt	Details
DHCP-Relay, das auf Distributed Logical Router konfiguriert ist und auf einen DHCP-Server verweist, der auf einem direkt verbundenen Edge Services Gateway konfiguriert ist	Ja	<p>Die IP des DHCP-Relay-Servers muss eine der internen Schnittstellen-IPs des Edge Services Gateway sein.</p> <p>Der DHCP-Server muss auf einem Edge Services Gateway konfiguriert werden, das direkt mit dem Distributed Logical Router verbunden ist, der mit dem DHCP-Relay konfiguriert ist.</p> <p>DNAT kann nicht zum Übersetzen einer DHCP-Relay-IP verwendet werden, die nicht mit einer internen Schnittstelle des Edge Services Gateway übereinstimmt.</p>
DHCP-Relay, das nur auf Distributed Logical Router konfiguriert ist, keine DHCP-Serverkonfiguration auf verbundenem Edge Services Gateway	Nein	
DHCP-Server, der nur auf Edge Services Gateway konfiguriert ist, keine DHCP-Relay-Konfiguration auf verbundenem Distributed Logical Router	Nein	

Tabelle 1-3. DHCP-Funktionen

Konfiguration	Unterstützt	Details
IP-Pools	Ja	
Statische Bindungen	Ja	
DHCP-Leases	Ja	
Allgemeine DHCP-Optionen	Ja	
DHCP-Dienst deaktiviert	Nein	In NSX-T können Sie den DHCP-Dienst nicht deaktivieren. Ein deaktivierter DHCP-Dienst auf NSX for vSphere wird nicht migriert.
DHCP-Option: „Andere“	Nein	<p>Das Feld „Andere“ in den DHCP-Optionen wird für die Migration nicht unterstützt. Beispielsweise wird die DHCP-Option „80“ nicht migriert.</p> <pre><dhcpOptions> <other> <code>80</code> <value>2f766172</value> </other> </dhcpOptions></pre>

Tabelle 1-3. DHCP-Funktionen (Fortsetzung)

Konfiguration	Unterstützt	Details
Verwaiste IP-Pools/Bindungen	Nein	Wenn IP-Pools oder statische Bindungen auf einem DHCP-Server konfiguriert sind, aber nicht von verbundenen logischen Switches verwendet werden, werden diese Objekte bei der Migration übersprungen.
DHCP, das auf dem Edge Services Gateway mit direkt verbundenen logischen Switches konfiguriert ist	Nein	Während der Migration werden direkt verbundene Edge Services Gateway-Schnittstellen als zentralisierte Dienstports migriert. NSX-T unterstützt jedoch nicht den DHCP-Dienst auf einem zentralisierten Dienstport, sodass die DHCP-Dienstkonfiguration für diese Schnittstellen nicht migriert wird.

Tabelle 1-4. DNS-Funktionen

Konfiguration	Unterstützt	Details
DNS-Ansichten	Ja	Nur die erste dnsView wird in die standardmäßige DNS-Weiterleitungszone von NSX-T migriert.
DNS-Konfiguration	Ja	Sie müssen verfügbare DNS-Listener-IPs für alle Edge-Knoten bereitstellen. Während „Konfiguration auflösen“ wird eine Meldung angezeigt, die dazu auffordert.
DNS – L3-VPN	Ja	Sie müssen die neu konfigurierten NSX-T-DNS-Listener-IPs der Remote-L3-VPN-Präfixliste hinzufügen. Während „Konfiguration auflösen“ wird eine Meldung angezeigt, die dazu auffordert.
DNS, das auf dem Edge Services Gateway mit direkt verbundenen logischen Switches konfiguriert ist	Nein	Während der Migration werden direkt verbundene Edge Services Gateway-Schnittstellen als zentralisierte Dienstports migriert. NSX-T unterstützt jedoch nicht den DNS-Dienst auf einem zentralisierten Dienstport, sodass die DNS-Dienstkonfiguration für diese Schnittstellen nicht migriert wird.

Verteilte Firewall

Konfiguration	Unterstützt	Details
Identitätsbasierte Firewall	Nein	
Abschnitt – <ul style="list-style-type: none"> ■ Anzeigename ■ Beschreibung ■ Tcp_strict ■ Statusfrei 	Ja	Wenn ein Firewallabschnitt über mehr als 1000 Regeln verfügt, migriert der Migrator die Regeln in mehreren Abschnitten von jeweils 1000 Regeln.
Universelle Abschnitte	Nein	
Regel – Quelle/Ziel: <ul style="list-style-type: none"> ■ IP-Adresse/Bereich/CIDR ■ Logischer Port ■ Logischer Switch 	Ja	
Regel – Quelle/Ziel: <ul style="list-style-type: none"> ■ VM ■ Logischer Port ■ Sicherheitsgruppe/IP Set/MAC Set 	Ja	Zuordnung zu NSGroup
Regel – Quelle/Ziel: <ul style="list-style-type: none"> ■ Cluster ■ Datencenter ■ DVPD ■ vSS ■ Host ■ Globaler logischer Switch 	Nein	
Regel – Angewendet auf: <ul style="list-style-type: none"> ■ ANY 	Ja	Zuordnung zur verteilten Firewall
Regel – Angewendet auf: <ul style="list-style-type: none"> ■ Sicherheitsgruppe ■ Logischer Port ■ Logischer Switch ■ VM 	Ja	Zuordnung zu NSGroup
Regel – Angewendet auf: <ul style="list-style-type: none"> ■ Cluster ■ Datencenter ■ DVPD ■ vSS ■ Host ■ Globaler logischer Switch 	Nein	

Konfiguration	Unterstützt	Details
Regeln in verteilter Firewall deaktiviert	Ja	
Deaktivieren der verteilten Firewall auf Clusterebene	Nein	Wenn die verteilte Firewall auf NSX-T aktiviert ist, wird Sie auf allen Clustern aktiviert. Sie können sie nicht auf einigen Clustern aktivieren und auf anderen deaktivieren.

Gruppieren von Objekten und Service Composer

IP Sets und MAC Sets werden als Gruppen zu NSX-T Data Center migriert. Weitere Informationen finden Sie unter **Bestand > Gruppen** auf der NSX-T Manager-Weboberfläche.

Tabelle 1-5. IP Sets und MAC Sets

Konfiguration	Unterstützt	Details
IP Sets	Ja	IP Sets mit bis zu 2 Millionen Mitgliedern (IP-Adressen, Subnetze von IP-Adressen, IP-Bereiche) können migriert werden. IP Sets mit mehr Mitgliedern werden nicht migriert.
Mac Sets	Ja	MAC Sets mit bis zu 2 Millionen Mitgliedern können migriert werden. MAC Sets mit mehr Mitgliedern werden nicht migriert.

Sicherheitsgruppen werden für die Migration mit den aufgeführten Einschränkungen unterstützt.

Sicherheitsgruppen werden als Gruppen zu NSX-T Data Center migriert. Weitere Informationen finden Sie unter **Bestand > Gruppen** auf der NSX-T Manager-Weboberfläche.

NSX for vSphere verfügt über systemdefinierte und benutzerdefinierte Sicherheitsgruppen. Diese werden alle als benutzerdefinierte Gruppen zu NSX-T migriert.

Die Gesamtanzahl der „Gruppen“ nach der Migration ist möglicherweise nicht gleich der Anzahl der Sicherheitsgruppen auf NSX for vSphere. Beispielsweise würde eine Regel für eine verteilte Firewall, die eine virtuelle Maschine als Quelle enthält, in eine Regel migriert werden, die eine neue Gruppe mit der VM als Mitglied enthält. Dadurch wird die Gesamtanzahl der Gruppen auf NSX-T nach der Migration erhöht.

Tabelle 1-6. Sicherheitsgruppen

Konfiguration	Unterstützt	Details
Sicherheitsgruppe mit Mitgliedern, die nicht vorhanden sind	Nein	Wenn eines der Mitglieder der Sicherheitsgruppe nicht vorhanden ist, wird die Sicherheitsgruppe nicht migriert.
Sicherheitsgruppe, die eine Sicherheitsgruppe mit nicht unterstützten Mitgliedern enthält	Nein	Wenn Mitglieder der Sicherheitsgruppe nicht für die Migration unterstützt werden, wird die Sicherheitsgruppe nicht migriert. Wenn eine Sicherheitsgruppe eine Sicherheitsgruppe mit nicht unterstützten Mitgliedern enthält, wird die übergeordnete Sicherheitsgruppe nicht migriert.
Mitgliedschaft in Sicherheitsgruppe ausschließen	Nein	Sicherheitsgruppen mit einem direkt oder indirekt (über Schachtelung) auszuschließenden Mitglied werden nicht migriert
Statische Mitgliedschaft in einer Sicherheitsgruppe	Ja	<p>Eine Sicherheitsgruppe kann bis zu 500 statische Mitglieder enthalten. Allerdings werden vom System generierte statische Mitglieder hinzugefügt, wenn die Sicherheitsgruppe in den Regeln der verteilten Firewall verwendet wird, wodurch der effektive Grenzwert auf 499 oder 498 gesenkt wird.</p> <ul style="list-style-type: none"> ■ Wenn die Sicherheitsgruppe in Layer-2- oder Layer-3-Regeln verwendet wird, wird ein vom System generiertes statisches Mitglied zur Sicherheitsgruppe hinzugefügt. ■ Wenn die Sicherheitsgruppe sowohl in Layer-2- als auch in Layer-3-Regeln verwendet wird, werden zwei vom System generierte statische Mitglieder hinzugefügt. <p>Wenn Mitglieder während des Schritts „Konfiguration auflösen“ nicht vorhanden sind, wird die Sicherheitsgruppe nicht migriert.</p>
Mitgliedertypen der Sicherheitsgruppe („Statisch“ oder „Entität“ gehört zu): <ul style="list-style-type: none"> ■ Cluster ■ Datacenter ■ Verzeichnisgruppe ■ Verteilte Portgruppe ■ Legacy-Portgruppe/-Netzwerk ■ Ressourcenpool ■ vApp 	Nein	Wenn eine Sicherheitsgruppe einen der nicht unterstützten Mitgliedertypen enthält, wird die Sicherheitsgruppe nicht migriert.

Tabelle 1-6. Sicherheitsgruppen (Fortsetzung)

Konfiguration	Unterstützt	Details
Mitgliedertypen der Sicherheitsgruppe („Statisch“ oder „Entität“ gehört zu): <ul style="list-style-type: none"> ■ Sicherheitsgruppe ■ IP Sets ■ MAC Sets 	Ja	<p>Sicherheitsgruppen, IP Sets und MAC Sets werden als Gruppen auf NSX-T migriert. Wenn eine NSX for vSphere-Sicherheitsgruppe ein IP Set, ein MAC Set oder eine verschachtelte Sicherheitsgruppe als statisches Mitglied enthält, werden die entsprechenden Gruppen der übergeordneten Gruppe hinzugefügt.</p> <p>Wenn eines dieser statischen Mitglieder nicht zu NSX-T migriert wurde, wird die übergeordnete Sicherheitsgruppe nicht zu NSX-T migriert.</p> <p>Beispielsweise kann ein IP Set mit mehr als 2 Millionen Mitgliedern nicht zu NSX-T migriert werden. Aus diesem Grund kann eine Sicherheitsgruppe, die ein IP Set mit mehr als 2 Millionen Mitgliedern enthält, nicht migriert werden.</p>
Mitgliedertypen der Sicherheitsgruppe („Statisch“ oder „Entität“ gehört zu): <ul style="list-style-type: none"> ■ Logischer Switch (virtuelle Leitung) 	Ja	<p>Wenn eine Sicherheitsgruppe logische Switches enthält, die nicht auf NSX-T-Segmente migriert werden, wird die Sicherheitsgruppe nicht zu NSX-T migriert.</p>
Mitgliedertypen der Sicherheitsgruppe („Statisch“ oder „Entität“ gehört zu): <ul style="list-style-type: none"> ■ Sicherheits-Tag 	Ja	<p>Wenn der Sicherheitsgruppe ein Sicherheits-Tag als statisches Mitglied oder als dynamisches Mitglied mit „Entität gehört zu“ hinzugefügt wird, muss das Sicherheits-Tag vorhanden sein, damit die Sicherheitsgruppe migriert werden kann.</p> <p>Wenn das Sicherheits-Tag der Sicherheitsgruppe nicht als dynamisches Mitglied hinzugefügt wird (ohne „Entität gehört zu“), wird das Vorhandensein des Sicherheits-Tags vor der Migration der Sicherheitsgruppe nicht überprüft.</p>

Tabelle 1-6. Sicherheitsgruppen (Fortsetzung)

Konfiguration	Unterstützt	Details
Mitgliedertypen der Sicherheitsgruppe („Statisch“ oder „Entität“ gehört zu): <ul style="list-style-type: none"> ■ vNIC ■ Virtuelle Maschine 	Ja	<ul style="list-style-type: none"> ■ vNICs und VMs werden als ExternalIDExpression migriert. ■ Verwaiste VMs (von Hosts gelöschte VMs) werden bei der Migration von Sicherheitsgruppen ignoriert. ■ Sobald die Gruppen auf NSX-T angezeigt werden, werden die VM- und vNIC-Mitgliedschaften nach einiger Zeit aktualisiert. Während dieser Zwischenzeit können temporäre Gruppen vorhanden sein, und ihre temporären Gruppen werden möglicherweise als Mitglieder angezeigt. Wenn die Hostmigration jedoch abgeschlossen ist, werden diese zusätzlichen temporären Gruppen nicht mehr angezeigt.
Verwenden des Operators „Stimmt mit regulärem Ausdruck überein“ für die dynamische Mitgliedschaft	Nein	Dies betrifft nur das Sicherheits-Tag und den VM-Namen. „Stimmt mit regulärem Ausdruck überein“ ist für andere Attribute nicht verfügbar.
Verwenden anderer verfügbarer Operatoren für dynamische Mitgliedschaftskriterien für Attribute: <ul style="list-style-type: none"> ■ Sicherheits-Tag ■ VM-Name ■ Computername ■ Name des Computer-Betriebssystems 	Ja	<p>Die verfügbaren Operatoren für VM-Name, Computername und Name des Computer-Betriebssystems sind „Enthält“, „Endet mit“, „Gleich“, „Ungleich“, „Beginnt mit“.</p> <p>Die verfügbaren Operatoren für das Sicherheits-Tag sind „Enthält“, „Endet mit“, „Gleich“, „Beginnt mit“.</p>

Tabelle 1-6. Sicherheitsgruppen (Fortsetzung)

Konfiguration	Unterstützt	Details
Kriterien für „Entität gehört zu“	Ja	<p>Dieselben Einschränkungen für die Migration statischer Mitglieder gelten für die Kriterien für „Entität gehört zu“. Wenn beispielsweise eine Sicherheitsgruppe „Entität gehört zu“ für einen Cluster in der Definition verwendet, wird diese Sicherheitsgruppe nicht migriert.</p> <p>Sicherheitsgruppen, die Kriterien für „Entität gehört zu“ enthalten, die mit UND kombiniert werden, werden nicht migriert.</p>
Operatoren für dynamische Mitgliedschaftskriterien (UND, ODER) in der Sicherheitsgruppe	Ja.	<p>Wenn Sie die dynamische Mitgliedschaft für eine NSX Data Center for vSphere-Sicherheitsgruppe definieren, können Sie Folgendes konfigurieren:</p> <ul style="list-style-type: none"> ■ einen oder mehrere dynamische Sätze. ■ Jeder dynamische Satz kann mehrere dynamische Kriterien enthalten. Beispiel: „VM-Name enthält web“. ■ Sie können auswählen, ob beliebige oder alle dynamischen Kriterien innerhalb eines dynamischen Satzes übereinstimmen sollen. ■ Sie können auswählen, ob Sie dynamische Sätze mit UND oder ODER abgleichen. <p>NSX for vSphere begrenzt nicht die Anzahl der dynamischen Kriterien und dynamischen Sätze. Sie können beliebige Kombinationen von UND und ODER verwenden.</p> <p>In NSX-T Data Center können Sie eine Gruppe mit fünf Ausdrücken verwenden. NSX for vSphere Sicherheitsgruppen, die mehr als fünf Ausdrücke enthalten, werden nicht migriert.</p> <p>Beispiele für Sicherheitsgruppen, die migriert werden können:</p> <ul style="list-style-type: none"> ■ Bis zu 5 dynamische Sätze, die mit ODER verknüpft sind, bei denen jeder dynamische Satz bis zu 5 dynamische Kriterien, die mit UND verknüpft sind („Alle“ in NSX for vSphere), enthält. ■ 1 dynamischer Satz mit 5 dynamischen Kriterien, die mit ODER verknüpft sind oder (Beliebig in NSX for vSphere).

Tabelle 1-6. Sicherheitsgruppen (Fortsetzung)

Konfiguration	Unterstützt	Details
		<ul style="list-style-type: none"> ■ 1 dynamischer Satz mit 5 dynamischen Kriterien, die mit UND verknüpft sind (Alle in NSX for vSphere). Alle Mitgliedstypen müssen identisch sein. ■ 5 dynamische Sätze, die mit UND verknüpft sind und von denen jeder dynamische Satz genau 1 dynamisches Kriterium enthält. Alle Mitgliedstypen müssen identisch sein. <p>Die Verwendung von Kriterien für „Entität gehört zu“ mit UND-Operatoren wird nicht unterstützt.</p> <p>Alle anderen Kombinationen oder Definitionen einer Sicherheitsgruppe, die nicht unterstützte Szenarien enthält, werden nicht migriert.</p>

In NSX for vSphere sind Sicherheits-Tags Objekte, die auf VMs angewendet werden können. Bei der Migration zu NSX-T sind Sicherheits-Tags Attribute einer VM.

Tabelle 1-7. Sicherheits-Tags

Konfiguration	Unterstützt	Details
Sicherheits-Tags	Ja	<p>Wenn auf eine VM 25 oder weniger Sicherheits-Tags angewendet werden, wird die Migration von Sicherheits-Tags unterstützt. Wenn mehr als 25 Sicherheits-Tags angewendet werden, werden keine Tags migriert.</p> <p>Hinweis: Wenn Sicherheits-Tags nicht migriert werden, ist die VM nicht in Gruppen enthalten, die durch die Tag-Mitgliedschaft definiert sind.</p>

Dienste und Dienstgruppen werden als Dienste zu NSX-T Data Center migriert. Weitere Informationen finden Sie unter **Bestand > Dienste** auf der NSX-T Manager-Weboberfläche.

Tabelle 1-8. Dienste und Dienstgruppen

Konfiguration	Unterstützt	Details
Dienste und Dienstgruppen (Anwendungen und Anwendungsgruppen)	Ja	Die meisten Standarddienste und Dienstgruppen werden den NSX-T-Diensten zugeordnet. Wenn ein Dienst oder eine Dienstgruppe in NSX-T nicht vorhanden ist, wird ein neuer Dienst in NSX-T erstellt.
APP_ALL- und APP_POP2-Dienstgruppen	Nein	Diese vom System definierten Dienstgruppen werden nicht migriert.

Tabelle 1-8. Dienste und Dienstgruppen (Fortsetzung)

Konfiguration	Unterstützt	Details
Dienste und Dienstgruppen mit Benennungskonflikten	Ja	Wenn in NSX-T ein Namenskonflikt für einen geänderten Dienst oder eine geänderte Dienstgruppe identifiziert wird, wird ein neuer Dienst in NSX-T mit einem Namen im Format: <NSXv-Application-Name> erstellt.
Dienstgruppen, die Layer-2-Dienste mit Diensten in anderen Layern kombinieren	Nein	
Leere Dienstgruppen	Nein	NSX-T unterstützt keine leeren Dienste.
Layer-2-Dienste	Ja	NSX for vSphere-Layer-2-Dienste werden als NSX-T-Diensteintrag EtherTypeServiceEntry migriert.
Layer-3-Dienste	Ja	Basierend auf dem Protokoll werden NSX for vSphere-Layer-3-Dienste wie folgt auf den NSX-T-Diensteintrag migriert: <ul style="list-style-type: none"> ■ TCP/UDP-Protokoll: L4PortSetServiceEntry ■ ICMP/IPV6ICMP-Protokoll: ICMPTypeServiceEntry ■ IGMP-Protokoll: IGMPTypeServiceEntry ■ Andere Protokolle: IPProtocolServiceEntry
Layer-4-Dienste	Ja	Als NSX-T-Diensteintrag ALGTypeServiceEntry migriert.
Layer-7-Dienste	Ja	Als NSX-T-Diensteintrag PolicyContextProfile migriert Wenn für eine NSX for vSphere-Layer-7-Anwendung ein Port und ein Protokoll definiert sind, wird ein Dienst in NSX-T mit der entsprechenden Port- und Protokollkonfiguration erstellt und dem PolicyContextProfile zugeordnet.
Layer-7-Dienstgruppen	Nein	
Regeln für verteilte Firewall, Edge-Firewall oder NAT, die Port und Protokoll enthalten	Ja	NSX-T erfordert einen Dienst zum Erstellen dieser Regeln. Wenn ein angemessener Dienst vorhanden ist, wird er verwendet. Wenn kein angemessener Dienst vorhanden ist, wird ein Dienst mit dem in der Regel angegebenen Port und Protokoll erstellt.

Tabelle 1-9. Service Composer

Konfiguration	Unterstützt	Details
Service Composer-Sicherheitsrichtlinien	Ja	<p>In einer Sicherheitsrichtlinie definierte Firewallregeln werden als Regeln für verteilte Firewall zu NSX-T migriert.</p> <p>Deaktivierte Firewallregeln, die in einer Service Composer-Sicherheitsrichtlinie definiert sind, werden nicht migriert.</p> <p>Guest Introspection-Regeln oder Netzwerkselfstprüfungsregeln, die in einer Service Composer-Sicherheitsrichtlinie definiert sind, werden nicht migriert.</p> <p>Wenn der Service Composer-Status nicht synchronisiert ist, wird im Schritt „Konfiguration auflösen“ eine Warnung angezeigt.</p> <p>Sie können die Migration von Service Composer-Richtlinien überspringen, indem Sie die relevanten Abschnitte der verteilten Firewall überspringen. Alternativ können Sie die Migration abbrechen, Service Composer mit der verteilten Firewall synchronisieren und die Migration neu starten.</p>
Service Composer-Sicherheitsrichtlinien werden nicht auf Sicherheitsgruppen angewendet	Nein	

Active Directory-Serverkonfiguration

Konfiguration	Unterstützt	Details
Active Directory-(AD-)Server	Nein	

Vom Migrations-Koordinator unterstützte Topologien

Der Migrations-Koordinator kann eine NSX Data Center for vSphere-Umgebung migrieren, wenn sie in einer unterstützten Topologie konfiguriert wurde.

Nicht unterstützte Funktionen

In allen Topologien werden die folgenden Funktionen nicht unterstützt:

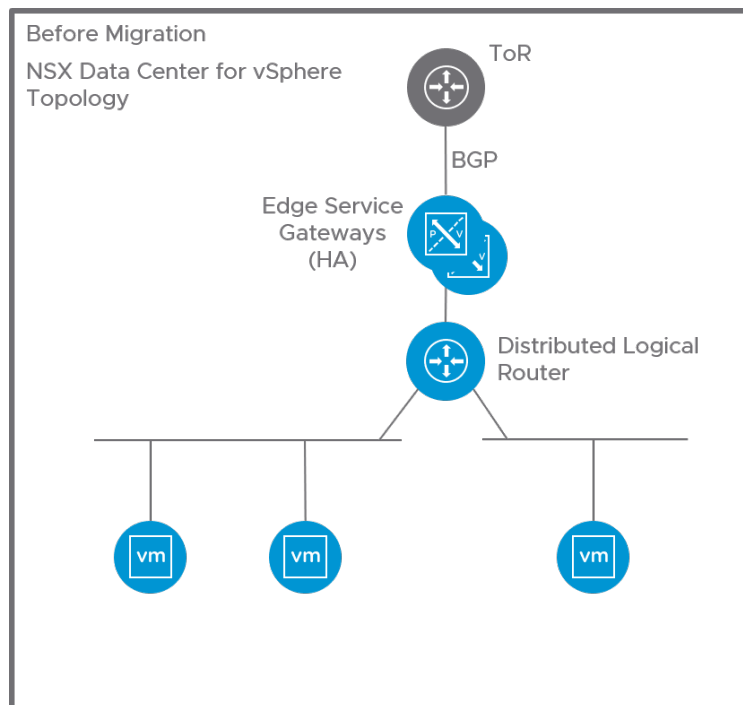
- OSPF zwischen Edge Services Gateways und Northbound-Routern. Sie müssen neu konfigurieren, um BGP zu verwenden.
- IP-Multicast.
- IPv6

Detaillierte Informationen darüber, welche Funktionen und Konfigurationen unterstützt werden, finden Sie unter [Detaillierte Funktionsunterstützung für Migrationskoordinator](#).

ESG mit Hochverfügbarkeit und L4-L7-Diensten

Diese Topologie enthält die folgenden Konfigurationen:

- Ein Distributed Logical Router, der mit einem Edge Services Gateway als Peer zusammenarbeitet.
- ECMP ist nicht konfiguriert.
- Die Edge Services Gateway befinden sich in einer Hochverfügbarkeitskonfiguration.
- BGP ist zwischen dem Edge Services Gateway und den Northbound-Routern konfiguriert.
- Edge Services Gateway kann L4-L7-Dienste ausführen:
 - VPN, NAT, DHCP-Server, DHCP-Relay, DNS-Weiterleitung, Edge-Firewall sind unterstützte Dienste.
 - Der Load Balancer wird in dieser Topologie nicht unterstützt.

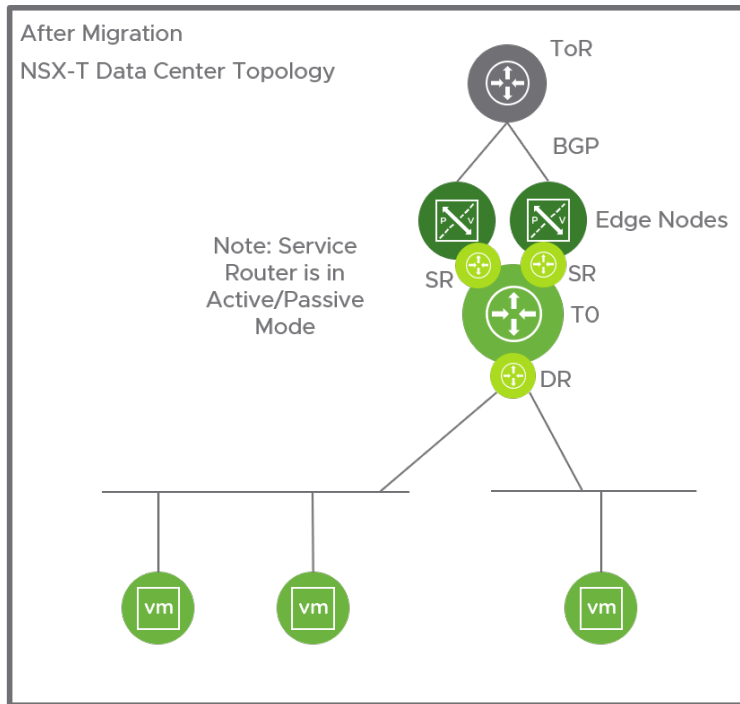


Nach der Migration wird diese Konfiguration durch ein Tier-0-Gateway ersetzt.

- Der Dienstrouter des Tier-0-Gateways wird im Modus „Aktiv/Standby“ ausgeführt.
- Die IP-Adressen der Distributed Logical Router-Schnittstellen werden als Downlinks auf dem Tier-0-Gateway konfiguriert.
- Die BGP-Konfiguration des ESG wird in eine BGP-Konfiguration auf dem Tier-0-Gateway übersetzt.

- Unterstützte Dienste werden auf das Tier-0-Gateway migriert.

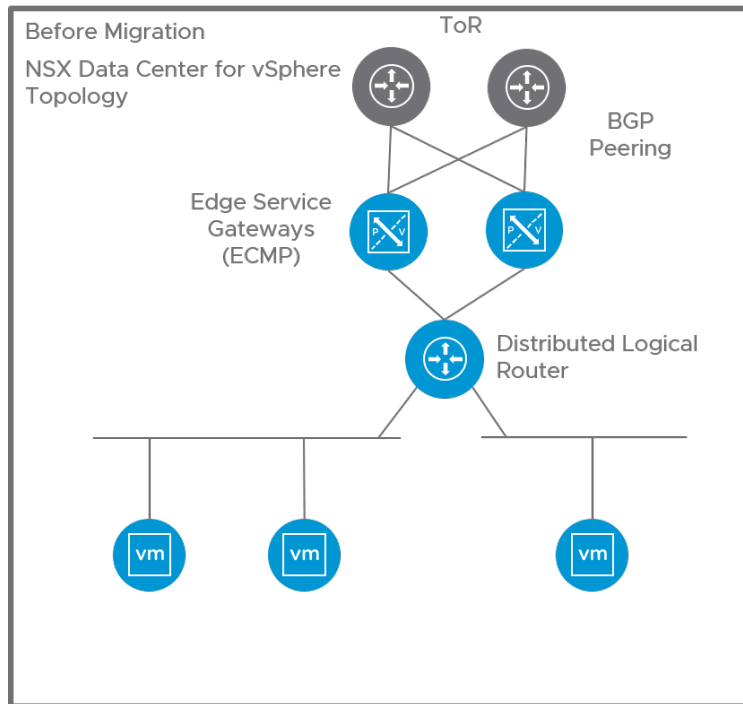
Hinweis Je nach Konfiguration müssen Sie unter Umständen neue IP-Adressen für die Uplinks des Tier-0-Gateways bereitstellen. Auf einem Edge Services Gateway können Sie beispielsweise dieselbe IP-Adresse für den Router-Uplink und für den VPN-Dienst verwenden. Auf einem Tier-0-Gateway müssen Sie die andere IP-Adresse für VPN und Uplinks verwenden. Weitere Informationen hierzu finden Sie unter [Konfigurationsprobleme – Beispiele](#).



ESG ohne L4-L7-Dienste

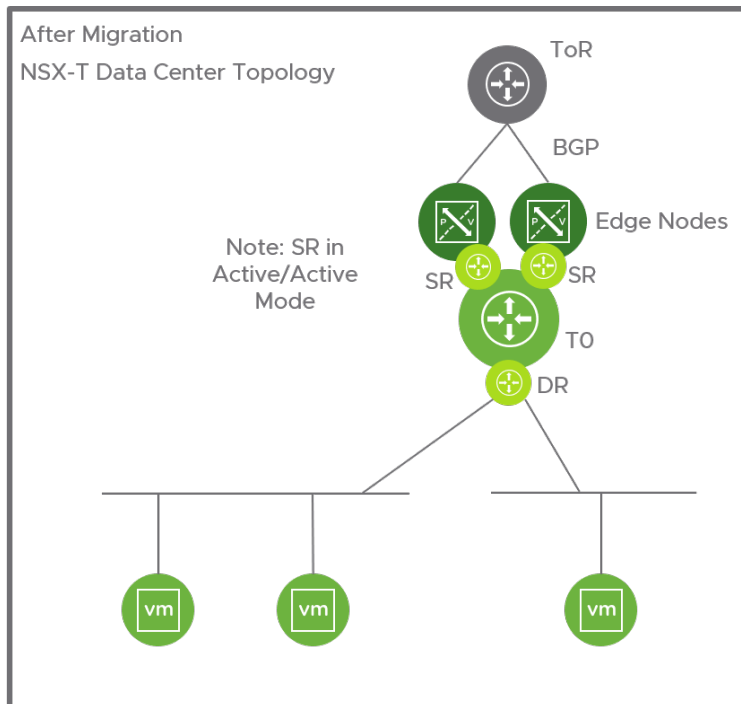
Diese Topologie enthält die folgenden Konfigurationen:

- Der Distributed Logical Router ist ECMP-fähig und arbeitet mit mehreren Edge Services Gateways zusammen.
- BGP ist zwischen dem Edge Services Gateway und den Northbound-Routern konfiguriert. Die Edge Services Gateways müssen mit denselben BGP-Nachbarn konfiguriert werden. Alle Edge Services Gateways müssen auf dasselbe autonome System (AS) verweisen.
- Wenn BGP zwischen dem Distributed Logical Router und dem Edge Services Gateway konfiguriert wird, müssen alle BGP-Nachbarn auf dem Distributed Logical Router dieselbe Gewichtung aufweisen.
- Edge Services Gateways dürfen keine L4-L7-Dienste ausführen.



Nach der Migration wird diese Konfiguration durch ein Tier-0-Gateway ersetzt.

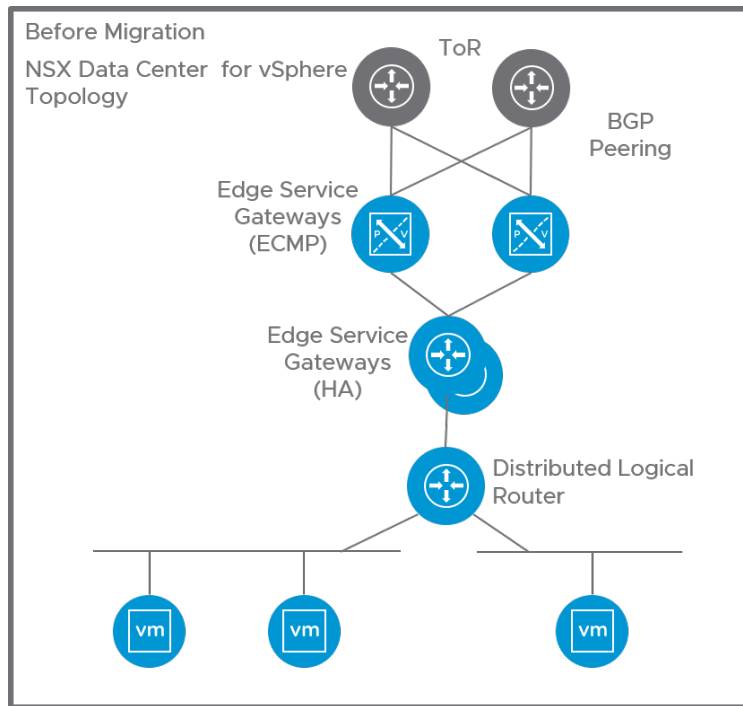
- Der Dienstrouter des Tier-0-Gateways wird im Modus „Aktiv/Aktiv“ ausgeführt.
- Die IP-Adressen der Distributed Logical Router-Schnittstellen werden als Downlinks auf dem Tier-0-Gateway konfiguriert.
- Die kombinierten BGP-Konfigurationen der Edge Services Gateways werden in eine BGP-Konfiguration auf dem Tier-0-Gateway übersetzt. Route Redistribution-Konfiguration wird übersetzt.
- Statische Routen von den Edge Services Gateways und den Distributed Logical Routers werden in statische Routen auf dem Tier-0-Gateway übersetzt.



Zwei Ebenen des ESG mit L4-L7-Diensten auf dem ESG der zweiten Ebene

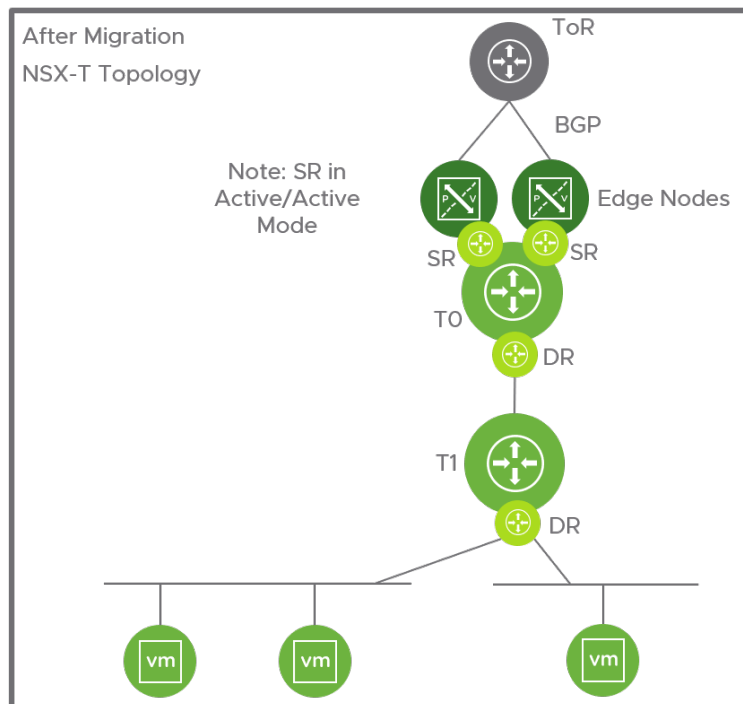
Diese Topologie enthält die folgenden Konfigurationen:

- Zwei Ebenen von Edge Services Gateways mit Distributed Logical Router.
- Auf dem Edge Services Gateways der ersten Ebene (dem Router zugewandt) dürfen keine L4-L7-Dienste ausgeführt werden.
- Die Edge Services Gateways der ersten Ebene müssen BGP-fähig sein und mindestens einen BGP-Nachbarn aufweisen.
- Die Edge Services Gateways der zweiten Ebene sind ECMP-fähig und arbeiten mit den Edge Services Gateways der ersten Ebene zusammen.
- Die Edge Services Gateways der zweiten Ebene können die L4-L7-Dienste ausführen:
 - NAT, DHCP-Server, DHCP-Relay, DNS-Weiterleitung, Inline-Load Balancer und Edge-Firewall werden unterstützt.
 - VPN wird nicht unterstützt.



Nach der Migration wird diese Konfiguration durch ein Tier-0- und ein Tier-1-Gateway ersetzt.

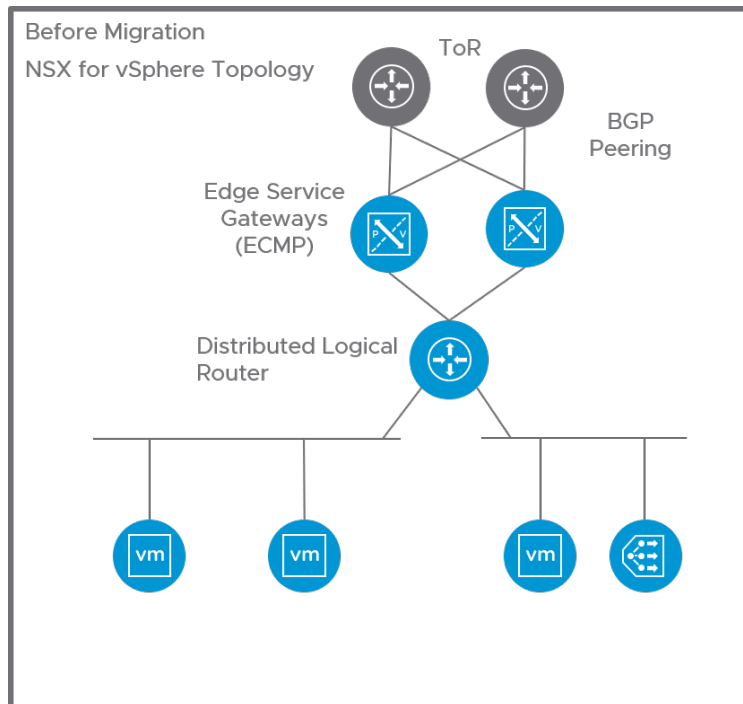
- Die Edge Services Gateways der ersten Ebene werden durch ein Tier-0-Gateway ersetzt. Der Dienstrouter wird im Modus „aktiv/aktiv“ ausgeführt.
- Die IP-Adressen der Uplinks des Edge Services Gateways auf erster Ebene werden für die Uplinks des Tier-0-Gateways verwendet.
- Das Tier-0-Gateway arbeitet unter Verwendung von BGP mit Northbound-Routern zusammen.
- Die Edge Services Gateways der zweiten Ebene werden in ein Tier-1-Gateway übersetzt, das mit dem Tier-0-Gateway verknüpft ist.
- Die IP-Adressen der Schnittstellen des verteilten logischen Routers werden als Downlinks auf dem Tier-1-Gateway konfiguriert.
- Alle Dienste, die auf dem Edge Services Gateway der zweiten Ebene ausgeführt werden, werden auf das Tier-1-Gateway migriert.
- Die BGP-Konfiguration auf den Edge Services Gateways der ersten Ebene wird in eine BGP-Konfiguration für das Tier-0-Gateway übersetzt. Route Redistribution-Konfiguration wird übersetzt.
- Statische Routen von den Edge Services Gateways und den Distributed Logical Routers werden in statische Routen auf dem Tier-0-Gateway übersetzt. Statische Routen zwischen dem Distributed Logical Router und den Edge Services Gateways auf der zweiten Ebene werden nicht benötigt und werden daher nicht übersetzt.



Einarmiger Load Balancer

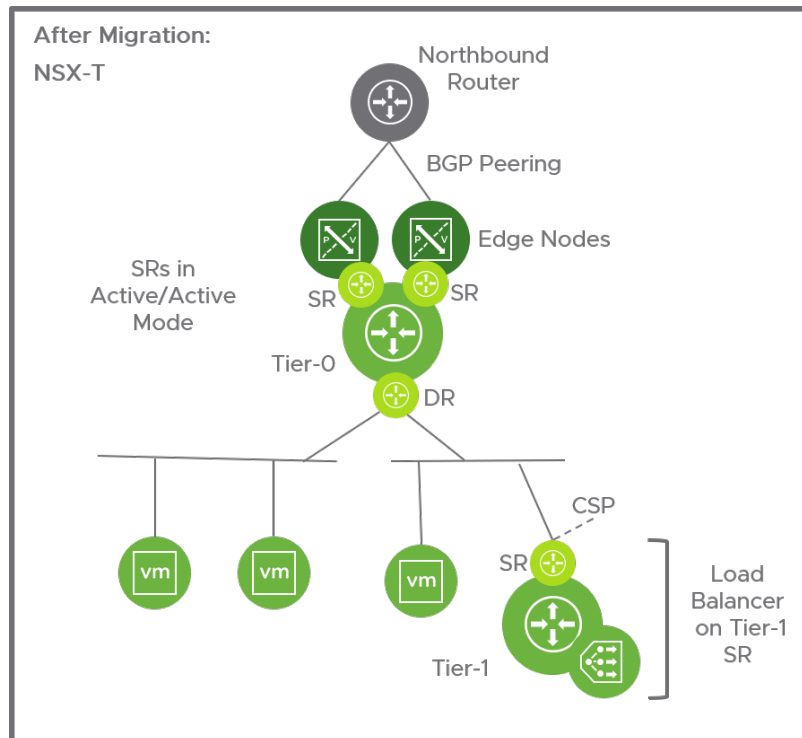
Diese Topologie enthält die folgenden Konfigurationen:

- Der Distributed Logical Router ist ECMP-fähig und arbeitet mit mehreren Edge Services Gateways zusammen.
- BGP ist zwischen dem Edge Services Gateway und den Northbound-Routern konfiguriert. Alle Edge Services Gateways müssen mit denselben BGP-Nachbarn konfiguriert werden. Alle Edge Services Gateways müssen auf dasselbe autonome System (AS) verweisen.
- Wenn BGP zwischen dem Distributed Logical Router und dem Edge Services Gateway konfiguriert wird, müssen alle BGP-Nachbarn auf dem Distributed Logical Router dieselbe Gewichtung aufweisen.
- Auf den dem Router zugewandten Edge Services Gateways dürfen keine L4-L7-Dienste ausgeführt werden.
- Ein Edge Services Gateway wird an den Distributed Logical Router angehängt, um Lastausgleichsdienste auszuführen. Es kann auch Edge-Firewall und DHCP ausführen.



Nach der Migration werden die Edge Services Gateways der obersten Ebene und der Distributed Logical Router durch ein Tier-0-Gateway ersetzt. Das Edge Services Gateway, das Lastausgleichsdienste durchführt, wird durch ein Tier-1-Gateway ersetzt.

- Der Dienstrouter des Tier-0-Gateways wird im Modus „Aktiv/Aktiv“ ausgeführt.
- Die IP-Adressen der Distributed Logical Router-Schnittstellen werden als Downlinks auf dem Tier-0-Gateway konfiguriert.
- Die kombinierten BGP-Konfigurationen der Edge Services Gateways auf oberster Ebene werden in eine BGP-Konfiguration auf dem Tier-0-Gateway übersetzt. Route Redistribution-Konfiguration wird übersetzt.
- Statische Routen von den Edge Services Gateways und den Distributed Logical Routers werden in statische Routen auf dem Tier-0-Gateway übersetzt.
- Die Lastausgleichskonfiguration auf dem Edge Services Gateway wird in eine Lastausgleichskonfiguration auf dem Tier-1-Gateway übersetzt.



VLAN-gestützte Mikrosegmentierung

Diese Topologie verwendet eine verteilte Firewall, um Firewallschutz für Arbeitslasten bereitzustellen, die mit VLAN-gestützten verteilten Portgruppen verbunden sind.

Diese Topologie verwendet die folgenden NSX Data Center for vSphere-Funktionen:

- NSX Manager
- Vorbereitung des Hosts (aber nicht VXLAN)
- Verteilte Firewall
- Service Composer
- Objekte werden gruppiert

Diese Topologie darf die folgenden Funktionen nicht enthalten:

- Transportzone
- VXLAN
- Logischer Switch
- Edge Services Gateway
- Verteilter logischer Router

Vom Migrationskoordinator unterstützte Grenzwerte

Der Migrationskoordinator unterstützt die Migration von NSX Data Center for vSphere-Umgebungen, die innerhalb dieser Grenzwerte liegen.

Tabelle 1-10. Grenzwerte für Migration

Funktion	Grenzwert (%)
Hosts pro NSX Manager (einzelnes vCenter – Transportzone)	64
vCenter-Cluster	8
Virtuelle Schnittstellen pro Hypervisor-Host	150
Logische Switches	1.400
Distributed Logical Router-Schnittstellen pro Distributed Logical Router	800
ECMP-Pfade	8
Statische Routen pro Edge Services Gateway	2.000
NAT-Regeln pro Edge Services Gateway	2.000
Edge-Firewallregeln pro Edge Services Gateway	2.000
DHCP-Leases pro Edge Services Gateway	800
Regeln für verteilte Firewalls pro NSX Manager	10.000
Abschnitte von verteilten Firewalls	1.300
Regeln für verteilte Firewalls pro Host	1.000
Sicherheitsgruppen pro NSX Manager	1.215
IP Sets	1.000
MAC Sets	200
Sicherheits-Tags	600
Sicherheits-Tags pro virtueller Maschine	25
Gruppierungsobjekte pro NSX Manager	1.250
Virtuelle Server pro Load Balancer	200
Pools pro Load Balancer	200
IPsec-Tunnel pro Edge Services Gateway	100
Von einem einzigen L2VPN-Server (Hub) verarbeitete L2VPN-Clients (Spoke)	1
Netzwerke pro L2VPN-Client-Server-Paar	100

Überblick über die Migration mithilfe des Migrations-Koordinators

Der Migrationsprozess umfasst das Einrichten einer neuen NSX-T-Umgebung und das Ausführen des Migrations-Koordinators. Darüber hinaus müssen Sie Ihre vorhandene NSX for vSphere-Umgebung gegebenenfalls ändern, um sicherzustellen, dass sie auf NSX-T migriert werden kann.

Vorsicht Stellen Sie eine neue NSX-T-Umgebung als Ziel für die NSX for vSphere-Migration bereit.

Während des Schritts **Konfiguration importieren** werden alle Edge-Knoten-Schnittstellen in der NSX-T-Zielumgebung heruntergefahren. Wenn die NSX-T-Zielumgebung bereits konfiguriert ist und verwendet wird, wird der Datenverkehr beim Starten des Konfigurationsimports unterbrochen.

Während der Migration werden Sie die folgenden Schritte durchführen:

- Erstellen Sie eine neue NSX-T-Umgebung.
 - Stellen Sie eine NSX Manager-Appliance zum Erstellen der NSX-T-Umgebung bereit.
Installieren Sie die NSX Manager-Appliances auf ESXi-Hosts, die nicht zu der NSX for vSphere-Umgebung gehören, die migriert wird.
 - Konfigurieren Sie einen Berechnungsmanager in der NSX-T-Umgebung. Fügen Sie den vCenter Server als Computing-Ressource hinzu. Verwenden Sie den genauen IP- oder Hostnamen, der in der NSX for vSphere vCenter Server-Registrierung angegeben wird.
 - Stellen Sie weitere NSX Manager-Appliances zum Erstellen eines Clusters bereit.
 - Starten Sie den Migrations-KoordinatorDienst.
 - Wenn Sie Benutzer von NSX for vSphere importieren möchten, richten Sie den VMware Identity Manager ein.
 - Erstellen Sie einen NSX-T-IP-Pool für die NSX-T Edge-TEPs. Diese IP-Adressen müssen mit allen vorhandenen NSX for vSphere-VTEPs kommunizieren können.
- Importieren Sie die Konfiguration von NSX for vSphere.
 - Geben Sie die Details Ihrer NSX for vSphere-Umgebung ein.
 - Die Konfiguration wird abgerufen und Vorabprüfungen werden ausgeführt.
- Beheben von Konfigurationsproblemen und Bereitstellen der NSX-T Edge-Knoten.
 - Überprüfen Sie die Nachrichten und die gemeldeten Konfigurationsprobleme, um alle blockierenden oder andere Probleme zu ermitteln, die eine Änderung der NSX for vSphere-Umgebung erfordern.
 - Wenn Sie Änderungen an NSX for vSphere vornehmen, müssen Sie die Migration neu starten und die Konfiguration erneut importieren.
 - Bereitstellen von NSX Edge-Knoten.
 - Stellen Sie die korrekte Anzahl der NSX-T Edge-Appliances mit geeigneter Größe bereit.
 - Verbinden Sie die Edge-Knoten über die Befehlszeile mit der Managementebene.
 - Beantworten Sie Fragen zur Systemkonfiguration. Erst nach Klärung der Fragen können Sie die NSX for vSphere-Umgebung auf NSX-T migrieren. Probleme können in mehreren Durchgängen von mehreren Personen behoben werden.
- Migrieren Sie die Konfiguration.
 - Nachdem alle Konfigurationsprobleme behoben sind, können Sie die Konfiguration in NSX-T importieren. Konfigurationsänderungen werden auf NSX-T vorgenommen, es werden jedoch noch keine Änderungen an der NSX for vSphere-Umgebung durchgeführt.

- Migrieren von Edges.

- Routing- und Edge-Dienste werden von NSX-T auf NSX for vSphere migriert.

Vorsicht Während des Schritts „Migrieren von Edges“ kommt es zu einer Unterbrechung des Nord-Süd-Datenverkehrs. Der gesamte Datenverkehr, der zuvor über die Edge Services Gateways (Nord-Süd-Datenverkehr) übertragen wurde, wird an die NSX-T-Edges weitergeleitet.

- Migrieren Sie die Hosts.

- Die NSX for vSphere-Software wird von den Hosts deinstalliert und die NSX-T-Software wird installiert. VM-Schnittstellen werden mit den neuen NSX-T-Segmenten verbunden.

Vorsicht Während des Schritts „Migrieren von Hosts“ kommt es zu einer Unterbrechung des Datenverkehrs.

- Schließen Sie die Migration ab.

- Nachdem Sie sichergestellt haben, dass die neue NSX-T-Umgebung ordnungsgemäß funktioniert, können Sie die Migration beenden, wodurch der Migrationsstatus gelöscht wird.

Bereitstellung einer virtuellen Maschine während der Migration

Wenn Sie während des Migrationsvorgangs VMs bereitstellen möchten, stellen Sie die VMs auf NSX-T-Hosts bereit, verbinden Sie die VMs mit NSX-T-Segmenten und installieren Sie VMware Tools auf den VMs.

Durch die Bereitstellung auf NSX-T mit installiertem VMware Tools wird sichergestellt, dass die VMs in Sicherheitsgruppen aufgefüllt werden und die beabsichtigten verteilten Firewall-Richtlinien erhalten.

Vorsicht VMs, die ohne installierten VMware Tools oder auf NSX for vSphere bereitgestellt wurden, erhalten die beabsichtigten verteilten Firewall-Richtlinien nicht.

Wenn Sie vSphere-Vorlagen zum Bereitstellen von VMs verwenden, aktualisieren Sie die Vorlagen, um NSX-T-Segmente für die VM-Netzwerkconfiguration zu verwenden. Durch die Angabe von NSX-T-Segmenten wird sichergestellt, dass alle mit den Vorlagen bereitgestellten VMs auf NSX-T-Hosts bereitgestellt werden.

Vorbereiten der Migration einer NSX Data Center for vSphere-Umgebung

Vor der Migration müssen Sie die Dokumentation lesen, sicherstellen, dass Sie über die benötigten Softwareversionen verfügen, Ihre vorhandene NSX for vSphere-Umgebung gegebenenfalls ändern und die Infrastruktur für die neue NSX-T-Umgebung bereitstellen.

Dokumentation

Prüfen Sie, ob die neueste Version dieses Handbuchs und die Versionshinweise für NSX-T Data Center und den Migrations-Koordinator zur Verfügung stehen. Die Dokumentation finden Sie hier: <https://docs.vmware.com/de/VMware-NSX-T-Data-Center/>.

Erforderliche Software und Versionen

- Stellen Sie sicher, dass die NSX for vSphere-Umgebung Version 6.4.4 aufweist.
- In den *VMware-Produktinteroperabilitätstabellen* erhalten Sie weitere Informationen zu den benötigten Versionen von vCenter Server und ESXi: http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php#interop&175=&1=&2=
- vSphere Distributed Switch 6.5.0 und 6.6.0 werden unterstützt.
- Die NSX for vSphere-Umgebung muss den NSX-T-Systemanforderungen für ESXi, vCenter Server und vSphere Distributed Switch entsprechen.
- Wenn Sie die Benutzerrollen von NSX for vSphere migrieren möchten, müssen Sie den VMware Identity Manager™ bereitstellen und konfigurieren. Finden Sie die kompatiblen Versionen in den *VMware-Interoperabilitätstabellen*: https://www.vmware.com/resources/compatibility/sim/interop_matrix.php#interop&175=&140=. Weitere Informationen finden Sie in der Dokumentation zum VMware Identity Manager.

Vorbereiten der NSX-T Data Center-Umgebung

Sie müssen eine neue NSX-T Data Center-Umgebung konfigurieren, um die NSX Data Center for vSphere-Umgebung zu migrieren.

Bereitstellen einer NSX-T Data CenterNSX Manager-Appliance

Sie müssen eine neue NSX Manager-Appliance zum Ausführen des Migrations-Koordinators bereitstellen. Verwenden Sie keine vorhandene NSX-T Data Center-Umgebung.

Wichtig Installieren Sie die NSX Manager-Appliances auf ESXi-Hosts, die nicht zu der NSX for vSphere-Umgebung gehören, die migriert wird.

Voraussetzungen

- Stellen Sie sicher, dass die Systemanforderungen erfüllt und die erforderlichen Ports geöffnet sind. Weitere Informationen hierzu finden Sie im *Installationshandbuch für NSX-T Data Center*.
- Stellen Sie sicher, dass auf dem ESXi-Host ein Datenspeicher konfiguriert und verfügbar ist. Für die Hochverfügbarkeit ist freigegebener Speicher erforderlich, damit der NSX Manager auf einem anderen Host neu gestartet werden kann, falls der ursprüngliche Host ausfällt.
- Stellen Sie sicher, dass Sie die IP-Adresse und das Gateway, die IP-Adressen des DNS-Servers, die Domänensuchliste und die IP-Adresse des NTP-Servers haben, die von NSX Manager verwendet werden.

- Erstellen Sie das Ziel-VM-Portgruppennetzwerk, wenn noch keines vorhanden ist. Platzieren Sie die NSX-T Data Center-Appliances in einem VM-Verwaltungsnetzwerk.

Wenn Sie über mehrere Verwaltungsnetzwerke verfügen, können Sie statische Routen von der NSX-T Data Center-Appliance zu den anderen Netzwerken hinzufügen.

- Planen Sie Ihr IPv4 oder IPv6-IP-Adressschema für NSX Manager.

Verfahren

- 1 Suchen Sie im VMware-Download-Portal nach der NSX-T Data Center-OVA-Datei.

Kopieren Sie die Download-URL oder laden Sie die OVA-Datei herunter.

- 2 Wählen Sie im vSphere Client den Host aus, auf dem NSX-T Data Center installiert werden soll.

- 3 Wählen Sie im Kontextmenü die Option **OVF-Vorlage bereitstellen** aus, um den Installationsassistenten zu starten.

- 4 Geben Sie die URL der herunterzuladenden OVA-Datei ein oder navigieren Sie zur OVA-Datei.

- 5 Geben Sie einen Namen für die NSX Manager-VM ein.

Der eingegebene Name wird in der vSphere-Bestandsliste angezeigt.

- 6 Wählen Sie eine Computing-Ressource für die NSX Manager-Appliance aus.

- 7 Überprüfen Sie die Details der OVF-Vorlage.

- 8 Reservieren Sie Arbeitsspeicher für die NSX Manager-Appliance, um eine optimale Leistung zu erreichen.

Legen Sie die Reservierung so fest, dass NSX Manager über ausreichend Arbeitsspeicher verfügt, um eine effiziente Ausführung sicherzustellen. Weitere Informationen finden Sie unter „NSX Manager-Systemanforderungen“ im *Installationshandbuch für NSX-T Data Center*.

- 9 Wählen Sie einen Datenspeicher für die Dateien der NSX Manager-Appliance aus.

- 10 Wählen Sie ein Zielnetzwerk für jedes Quellnetzwerk aus.

- 11 Wählen Sie die Portgruppe oder das Zielnetzwerk für NSX Manager.

- 12 Geben Sie die System-Root-, CLI-Admin- und Audit-Kennwörter für die NSX Manager ein.

Ihre Kennwörter müssen den Einschränkungen zur Kennwortkomplexität entsprechen.

- mindestens 12 Zeichen
- mindestens ein Kleinbuchstabe
- mindestens ein Großbuchstabe
- mindestens eine Zahl
- mindestens ein Sonderzeichen
- mindestens fünf unterschiedliche Zeichen
- keine Wörterbuchwörter

- keine Palindrome
- mehr als vier monotone Zeichenfolgen ist nicht zulässig

13 Geben Sie den Hostnamen des NSX Manager ein.

14 Akzeptieren Sie die **nsx-manager nsx-controller**-Standardrolle für VM.

15 Geben Sie das Standard-Gateway, die IPv4-Adresse und Netzmaske des Verwaltungsnetzwerks, die DNS- und NTP-IP-Adresse ein.

16 Aktivieren Sie SSH und lassen Sie gegebenenfalls Root-SSH-Anmeldung an der NSX Manager-Befehlszeile zu.

Standardmäßig sind diese Optionen aus Sicherheitsgründen deaktiviert.

17 Stellen Sie sicher, dass die gesamte Spezifikation der benutzerdefinierten OVF-Vorlage korrekt ist, und klicken Sie auf **Beenden**, um die Installation zu starten.

Die Installation kann 7 bis 8 Minuten dauern.

18 Öffnen Sie über den vSphere Client die VM-Konsole von NSX Manager, um den Startvorgang zu verfolgen.

19 Melden Sie sich nach dem Start von NSX Manager als Administrator bei der CLI an und führen Sie den Befehl `get interface eth0` aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

20 Geben Sie den Befehl `get services` ein, um sicherzustellen, dass alle Dienste ausgeführt werden.

Wenn die Dienste nicht ausgeführt werden, warten Sie, bis alle Dienste gestartet wurden.

Hinweis Die folgenden Dienste werden nicht standardmäßig ausgeführt: `liagent`, `migration-coordinator` und `snmp`. Sie können sie wie folgt starten:

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

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

21 Stellen Sie sicher, dass Ihr NSX Manager über die erforderliche Konnektivität verfügt.

Stellen Sie sicher, dass Sie die folgenden Aufgaben ausführen können.

- Führen Sie für Ihren NSX Manager von einer anderen Maschine aus einen Ping-Vorgang aus.
- Der NSX Manager kann einen Ping-Vorgang für das zugehörige Standard-Gateway ausführen.
- Der NSX Manager kann mithilfe der Verwaltungsschnittstelle einen Ping-Vorgang für die Hypervisor-Hosts ausführen, die sich im selben Netzwerk wie der NSX Manager befinden.
- Der NSX Manager kann einen Ping-Vorgang für den zugehörigen DNS-Server und NTP-Server ausführen.

- Wenn Sie SSH aktiviert haben, stellen Sie sicher, dass Sie eine SSH-Verbindung zu NSX Manager herstellen können.

Wenn keine Konnektivität hergestellt werden kann, stellen Sie sicher, dass sich der Netzwerkadapter der virtuellen Appliance im richtigen Netzwerk oder VLAN befindet.

Hinzufügen eines Compute Managers

Sie müssen das vCenter Server-System konfigurieren, das mit dem NSX Data Center for vSphere als Compute Manager in NSX-T verknüpft ist, bevor Sie den Migrationsprozess starten können.

Wenn Sie einen vCenter Server-Compute Manager hinzufügen, müssen Sie die Anmeldedaten eines vCenter Server-Benutzers angeben. Sie können die Anmeldedaten des vCenter Server-Administrators angeben oder eine Rolle und einen Benutzer speziell für NSX-T Data Center erstellen und die Anmeldedaten dieses Benutzers angeben. Diese Rolle muss über die folgenden vCenter Server-Berechtigungen verfügen:

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

Weitere Informationen zu vCenter Server-Rollen und -Berechtigungen finden Sie im Dokument *vSphere-Sicherheit*.

Voraussetzungen

Melden Sie sich bei der Webschnittstelle von NSX for vSphere NSX Manager an, um die für die Registrierung von vCenter Server verwendeten Einstellungen abzurufen. Sie müssen genau dieselben Einstellungen verwenden. Wenn beispielsweise eine IP-Adresse angegeben wird, verwenden Sie die IP-Adresse und nicht den FQDN.

Verfahren

- 1 Melden Sie sich über einen Browser bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Fabric > Berechnungsmanager > Hinzufügen** aus.
- 3 Vervollständigen Sie die Details zum Compute Manager.

Option	Beschreibung
Name und Beschreibung	Geben Sie den Namen zum Identifizieren von vCenter Server ein. Sie können optional spezielle Details wie z. B. die Anzahl Cluster in vCenter Serverbeschreiben.
Domänenname/IP-Adresse	Geben Sie die IP-Adresse für vCenter Server ein.
Typ	Behalten Sie die Standardoption bei.
Benutzername und Kennwort	Geben Sie die vCenter Server-Anmeldedaten ein.
Fingerabdruck	Geben Sie den Wert für den vCenter Server-SHA-256-Fingerabdruckalgorithmus ein.

Wenn Sie den Fingerabdruckwert leer lassen, werden Sie aufgefordert, den vom Server bereitgestellten Fingerabdruck zu akzeptieren.

Nachdem Sie den Fingerabdruck akzeptiert haben, dauert es einige Sekunden, bis NSX-T Data Center die vCenter Server-Ressourcen ermittelt und registriert.

- 4 Wenn sich das Symbol „Fortschritt“ von **In Bearbeitung** in **Nicht registriert** ändert, führen Sie die folgenden Schritte aus, um den Fehler zu beheben.
 - a Wählen Sie die Fehlermeldung und klicken Sie auf **Beheben**. Eine mögliche Fehlermeldung lautet:

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

- b Geben Sie die vCenter Server-Anmeldedaten ein und klicken Sie auf **Beheben**.

Wenn eine bestehende Registrierung vorhanden ist, wird sie ersetzt.

Es dauert einige Zeit, um den Compute Manager bei vCenter Server zu registrieren und bis der Verbindungsstatus als Aktiv angezeigt wird.

Sie können auf den Namen des Compute Managers klicken, um Details anzuzeigen, den Compute Manager zu bearbeiten oder um Tags zu verwalten, die für den Compute Manager gelten.

Bereitstellen zusätzlicher NSX Manager-Appliances

Sie können den Migrations-Koordinator mit nur einer bereitgestellten NSX Manager-Appliance ausführen. Stellen Sie jedoch zwei zusätzliche NSX Manager-Appliances bereit, bevor Sie Ihre NSX-T Data Center-Umgebung in der Produktion einsetzen.

Wichtig Installieren Sie die NSX Manager-Appliances auf ESXi-Hosts, die nicht zu der NSX for vSphere-Umgebung gehören, die migriert wird.

Nach der Bereitstellung der neuen Knoten stellen diese Knoten eine Verbindung zum übergeordneten NSX Manager-Knoten her, um einen Cluster zu erstellen. Die empfohlene Anzahl von geclusterten NSX Manager-Knoten beträgt drei.

Alle Repository-Details des übergeordneten NSX Manager-Knotens werden mit den neu bereitgestellten Knoten im Cluster synchronisiert.

Voraussetzungen

- Stellen Sie sicher, dass ein übergeordneter NSX Manager-Knoten installiert ist.
- Stellen Sie sicher, dass der Berechnungsmanager konfiguriert ist. Siehe [Hinzufügen eines Compute Managers](#).

Verfahren

- 1 Melden Sie sich in einem Browser mit Administratorrechten bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Übersicht > Knoten hinzufügen** aus.
- 3 Geben Sie die üblichen Attributdetails von NSX Manager an.

Option	Beschreibung
Berechnungsmanager	Der registrierte Ressourcenberechnungsmanager wird mit Daten befüllt.
SSH aktivieren	Schalten Sie die Schaltfläche um, um eine SSH-Anmeldung am neuen NSX Manager-Knoten zu ermöglichen.
Root-Zugriff aktivieren	Schalten Sie die Schaltfläche um, um den Root-Zugriff auf den neuen NSX Manager-Knoten zu ermöglichen.

Option	Beschreibung
CLI-Benutzername und Kennwortbestätigung	<p>Legen Sie das CLI-Kennwort und die Kennwortbestätigung für den neuen Knoten fest.</p> <p>Ihr Kennwort muss den Einschränkungen zur Kennwortkomplexität entsprechen.</p> <ul style="list-style-type: none"> ■ mindestens 12 Zeichen ■ mindestens ein Kleinbuchstabe ■ mindestens ein Großbuchstabe ■ mindestens eine Zahl ■ mindestens ein Sonderzeichen ■ mindestens fünf unterschiedliche Zeichen ■ keine Wörterbuchwörter ■ keine Palindrome ■ mehr als vier monotone Zeichenfolgen ist nicht zulässig <p>Der CLI-Benutzername ist bereits auf Admin festgelegt.</p>
Root-Kennwort und Kennwortbestätigung	<p>Legen Sie das Root-Kennwort und die Kennwortbestätigung für den neuen Knoten fest.</p> <p>Ihr Kennwort muss den Einschränkungen zur Kennwortkomplexität entsprechen.</p> <ul style="list-style-type: none"> ■ mindestens 12 Zeichen ■ mindestens ein Kleinbuchstabe ■ mindestens ein Großbuchstabe ■ mindestens eine Zahl ■ mindestens ein Sonderzeichen ■ mindestens fünf unterschiedliche Zeichen ■ keine Wörterbuchwörter ■ keine Palindrome ■ mehr als vier monotone Zeichenfolgen ist nicht zulässig
DNS-Server	Geben Sie die IP-Adresse des DNS-Servers ein, der im vCenter Server verfügbar ist.
NTP-Server	Geben Sie die IP-Adresse des NTP-Servers ein.

4 Geben Sie die Knotendetails zu NSX Manager ein.

Option	Beschreibung
Name	Geben Sie einen Namen für den NSX Manager-Knoten ein.
Cluster	Weisen Sie über das Dropdown-Menü den Cluster zu, dem der Knoten beitreten wird.
Ressourcenpool oder Host	Weisen Sie aus dem Dropdown-Menü entweder einen Ressourcenpool oder einen Host für den Knoten zu.
Datenspeicher	Wählen Sie einen Datenspeicher für die Knoten-Dateien aus dem Dropdown-Menü aus.
Netzwerk	Wählen Sie aus dem Dropdown-Menü das Netzwerk aus.
Verwaltungs-IP/Netmask	Geben Sie die IP-Adresse und Netzmaske ein.
Verwaltungs-Gateway	Geben Sie die Gateway-IP-Adresse ein.

- 5 (Optional) Klicken Sie auf **Neuer Knoten** und konfigurieren Sie einen anderen Knoten.

Wiederholen Sie die Schritte 3 bis 4.

- 6 Klicken Sie auf **Fertigstellen**.

Die neuen Knoten werden bereitgestellt. Sie können den Bereitstellungsvorgang auf der Seite **System > Übersicht** oder dem vCenter Server nachverfolgen.

Die Bereitstellung, die Clusterbildung und die Repository-Synchronisierung können bis zu 10 Minuten dauern.

- 7 Melden Sie sich nach dem Start von NSX Manager als Administrator bei der CLI an und führen Sie den Befehl `get interface eth0` aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

- 8 Geben Sie den Befehl `get services` ein, um sicherzustellen, dass alle Dienste ausgeführt werden.

Wenn die Dienste nicht ausgeführt werden, warten Sie, bis alle Dienste gestartet wurden.

- 9 Melden Sie sich beim übergeordneten NSX Manager-Knoten an und geben Sie den Befehl `get cluster status` ein, um sicherzustellen, dass die Knoten dem Cluster erfolgreich hinzugefügt wurden.

- 10 Stellen Sie sicher, dass Ihr NSX Manager über die erforderliche Konnektivität verfügt.

Stellen Sie sicher, dass Sie die folgenden Aufgaben ausführen können.

- Führen Sie für Ihren NSX Manager von einer anderen Maschine aus einen Ping-Vorgang aus.
- Der NSX Manager kann einen Ping-Vorgang für das zugehörige Standard-Gateway ausführen.
- Der NSX Manager kann mithilfe der Verwaltungsschnittstelle einen Ping-Vorgang für die Hypervisor-Hosts ausführen, die sich im selben Netzwerk wie der NSX Manager befinden.
- Der NSX Manager kann einen Ping-Vorgang für den zugehörigen DNS-Server und NTP-Server ausführen.
- Wenn Sie SSH aktiviert haben, stellen Sie sicher, dass Sie eine SSH-Verbindung zu NSX Manager herstellen können.

Wenn keine Konnektivität hergestellt werden kann, stellen Sie sicher, dass sich der Netzwerkadapter der virtuellen Appliance im richtigen Netzwerk oder VLAN befindet.

Erstellen eines IP-Pools für Edge-Tunnel-Endpoints

Sie müssen einen IP-Pool für die Edge-TEPs (Tunnel Endpoint) in der NSX-T-Umgebung erstellen, bevor Sie die Migration starten.

Voraussetzungen

- Geben Sie vorhandene IP-Pools an, die für NSX for vSphere-VTEPs verwendet werden.
- Legen Sie die IP-Adressen fest, die zum Erstellen des IP-Pools für Edge-TEPs verwendet werden sollen.

Der IP-Bereich und das VLAN dürfen in der NSX Data Center for vSphere-Umgebung nicht bereits in Verwendung sein.

- Stellen Sie sicher, dass die IP-Adressen des NSX-T-TEP über das Netzwerk mit den IP-Adressen des NSX for vSphere-VTEP verbunden sind.

Verfahren

- 1 Melden Sie sich über einen Browser bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **Netzwerk und Sicherheit – Erweitert > Bestandsliste > Gruppen > IP-Pools > Hinzufügen** aus.
- 3 Geben Sie einen Namen für den neuen IP-Pool ein.
- 4 (Optional) Geben Sie eine Beschreibung ein.
- 5 Klicken Sie auf **Hinzufügen**.
- 6 Klicken Sie auf die Zelle „IP-Bereiche“ und geben Sie die IP-Bereiche ein.
Setzen Sie den Mauszeiger oben rechts auf eine beliebige Zelle und klicken Sie auf das Bleistiftsymbol zur Bearbeitung.
- 7 (Optional) Geben Sie ein Gateway ein.
- 8 Geben Sie eine CIDR-IP-Adresse mit Suffix ein.
- 9 (Optional) Geben Sie DNS-Server ein.
- 10 (Optional) Geben Sie ein DNS-Suffix ein.
- 11 Klicken Sie auf **Speichern**.

Vorbereiten der NSX Data Center for vSphere-Umgebung auf die Migration

Sie müssen den Status der NSX Data Center for vSphere-Umgebung überprüfen und alle gefundenen Probleme beheben. Darüber hinaus müssen Sie je nach Umgebung gegebenenfalls Ihre NSX Data Center for vSphere-Konfiguration ändern, bevor Sie auf NSX-T Data Center migrieren können.

Systemstatus

Überprüfen Sie die folgenden Systemzustände:

- Stellen Sie sicher, dass der Status der NSX for vSphere-Komponenten im NSX-Dashboard auf „Grün“ gesetzt ist.
- Stellen Sie sicher, dass alle ESXi-Hosts betriebsbereit sind. Beheben Sie alle Probleme mit Hosts, einschließlich getrennter Zustände. Für den Eintritt in den Wartungsmodus dürfen weder ausstehende Neustarts noch ausstehende Aufgaben vorhanden sein.
- Überprüfen Sie den Veröffentlichungsstatus der verteilten Firewall und des Service Composers, um sicherzustellen, dass keine unveröffentlichten Änderungen vorliegen.

Allgemeine Konfiguration

- Sichern Sie die NSX for vSphere- und die vSphere-Umgebung. Weitere Informationen finden Sie unter „Sichern und Wiederherstellen von NSX“ im *Administratorhandbuch für NSX*.
- Der VXLAN-Port muss auf 4789 festgelegt sein. Wenn in der NSX for vSphere-Umgebung ein anderer Port verwendet wird, muss dieser vor der Migration geändert werden. Weitere Informationen finden Sie unter „Ändern des VXLAN-Ports“ im *NSX for vSphere Administratorhandbuch für NSX*.

Controller-Konfiguration

- Der Migrations-Koordinator bietet keine Unterstützung für NSX for vSphere-Transportzonen, die den Multicast- oder Hybrid-Replikationsmodus verwenden. Ein NSX Controller-Cluster ist erforderlich, wenn VXLAN verwendet wird. VLAN-gestützte Mikrosegmentierungs-Topologien verwenden kein VXLAN und benötigen daher keinen NSX Controller-Cluster.

Hostkonfiguration

- Überprüfen Sie diese Einstellungen auf allen Hostclustern in der NSX for vSphere-Umgebung und aktualisieren Sie sie gegebenenfalls:
 - vSphere-DRS auf manuell festlegen
 - Deaktivieren Sie die vSphere-Hochverfügbarkeit.
 - Die Exportversion des Filters für die verteilte Firewall auf 1.000 setzen. Siehe [Konfigurieren der Exportversion des Filters „Verteilte Firewall“ auf Hosts](#).
- Hosts, auf denen NSX for vSphere installiert ist, die aber keinem vSphere Distributed Switch hinzugefügt wurden, müssen zu Distributed Switches hinzugefügt werden, wenn sie auf NSX-T migriert werden sollen. Weitere Informationen hierzu finden Sie unter [Konfigurieren von nicht an vSphere Distributed Switches angehängten Hosts](#).
- Überprüfen Sie auf jedem Cluster, auf dem NSX for vSphere installiert ist, ob die verteilte Firewall aktiviert ist. Sie können den aktivierten Status unter **Installation und Upgrade > Hostvorbereitung** anzeigen.

Wenn die verteilte Firewall vor der Migration auf NSX for vSphere-Clustern aktiviert ist, wird sie auf allen Clustern aktiviert, wenn diese auf NSX-T migriert werden. Überprüfen Sie die Auswirkungen der Aktivierung der verteilten Firewall auf allen Clustern und ändern Sie gegebenenfalls die Konfiguration der verteilten Firewall.

- Stellen Sie sicher, dass für alle Hosts nur eine VTEP-Schnittstelle konfiguriert wurde. Überprüfen Sie alle Hosts in **Hosts und Cluster > Host > Konfigurieren > VMKernel-Adapter**. Stellen Sie sicher, dass pro Host nur eine Schnittstelle mit dem TCP/IP-Stack vxlan vorhanden ist. Das Migrieren von Hosts mit mehreren VTEPs wird nicht unterstützt.

Konfiguration des Edge Services Gateway

- Edge Services Gateways müssen BGP für Northbound-Routing verwenden. Bei Verwendung von OSPF müssen Sie die Konfiguration zur Verwendung von BGP abändern, bevor Sie die Migration starten.

- Sie müssen möglicherweise Änderungen an der NSX for vSphere Route Redistribution-Konfiguration vornehmen, bevor die Migration gestartet wird.
 - Auf der Neuverteilungsebene konfigurierte Präfixfilter werden nicht migriert. Fügen Sie alle benötigten Filter als BGP-Filter in der BGP-Nachbarkonfiguration des Edge Services Gateway hinzu.
 - Nach der Migration werden dynamisch erlernte Routen zwischen Distributed Logical Router und Edge Services Gateway in statische Routen konvertiert und alle statischen Routen werden in BGP neu verteilt. Wenn Sie eine dieser Routen filtern müssen, bevor Sie die Migration starten, konfigurieren Sie die BGP-Nachbarfilter, um diese Präfixe zu verweigern, während sie andere zulassen.
- NSX for vSphere unterstützt richtlinienbasierte IPSec-VPN-Sitzungen, in denen lokale und Peer-Subnetze von zwei oder mehr Sitzungen miteinander überlappen. Dieses Verhalten wird in NSX-T nicht unterstützt. Sie müssen die Subnetze vor dem Start der Migration neu konfigurieren, damit sie sich nicht überlappen. Wenn dieses Konfigurationsproblem nicht behoben wird, schlägt der Schritt **Konfiguration migrieren** fehl.
- Bei einem Edge Services Gateway, das als einarmiger Lastausgleichsdienst fungiert, müssen Sie die folgenden Konfigurationen (falls vorhanden) vor dem Importieren der Konfiguration ändern.
 - Wenn für das Edge Services Gateway eine Verwaltungsschnittstelle konfiguriert wurde, müssen Sie diese vor der Migration löschen. Sie können nur über eine verbundene Schnittstelle auf einem Edge Services Gateway verfügen, das eine Lastausgleichsfunktion mit einem Arm bereitstellt. Wenn mehrere Schnittstellen vorliegen, schlägt der Schritt **Konfiguration migrieren** fehl.
 - Wenn die Edge Services Gateway-Firewall deaktiviert und die Standardregel auf „Verweigern“ gesetzt ist, müssen Sie die Firewall aktivieren und die Standardregel in „Annehmen“ ändern. Nach der Migration wird die Firewall auf dem Tier-1-Gateway aktiviert und die Standardregel „Annehmen“ wird wirksam. Indem die Standardregel vor der Migration in „Annehmen“ geändert wird, verhindern Sie, dass eingehender Datenverkehr für den Lastausgleichsdienst blockiert wird.
- Stellen Sie sicher, dass alle Edge Services Gateways ordnungsgemäß mit der zu migrierenden Topologie verbunden sind. Wenn Edge Services Gateways als Teil der NSX for vSphere-Umgebung nicht ordnungsgemäß an die restliche Umgebung angeschlossen sind, werden sie nicht migriert.

Wenn ein Edge Services Gateway beispielsweise als einarmiger Lastausgleichsdienst konfiguriert ist, aber eine der folgenden Konfigurationen aufweist, wird das Gateway nicht migriert:

- Das Edge Services Gateway weist keine Uplink-Schnittstelle auf, die mit einem logischen Switch verbunden ist.
- Das Edge Services Gateway weist eine mit einem logischen Switch verbundene Uplink-Schnittstelle auf. Die IP-Adresse des Uplinks stimmt jedoch nicht mit dem Subnetz überein, das mit dem Distributed Logical Router verknüpft ist, der eine Verbindung zum logischen Switch herstellt.

Konfigurieren von nicht an vSphere Distributed Switches angehängten Hosts

Eine NSX for vSphere-Umgebung kann Hosts enthalten, auf denen NSX for vSphere installiert ist, die aber keinem vSphere Distributed Switch hinzugefügt wurden. Sie müssen die Hosts zu einem vSphere Distributed Switch hinzufügen, bevor Sie sie migrieren können.

Sie können einen bereits in Ihrer Umgebung vorhandenen Distributed Switch verwenden oder einen neuen Distributed Switch zu diesem Zweck erstellen. Klicken Sie mit der rechten Maustaste auf den Distributed Switch und wählen Sie **Hosts hinzufügen und verwalten** aus, um die Hosts zum Distributed Switch hinzuzufügen. Sie müssen dem Distributed Switch weder physische Uplinks noch VMkernel-Netzwerkadapter zuweisen.

Weitere Informationen finden Sie unter „Hinzufügen von Hosts zu einem vSphere Distributed Switch“ im *vSphere-Netzwerkhandbuch*.

Wenn Sie die Konfiguration importieren, bevor Sie diese Änderung vornehmen, müssen Sie die Migration neu starten, um die aktualisierte Konfiguration zu importieren. Siehe [Vornehmen von Änderungen an der NSX for vSphere-Umgebung](#).

Nach Abschluss der Migration müssen die Hosts nicht mehr an den Distributed Switch angehängt werden.

- Wenn Sie die Hosts zu einem vorhandenen Distributed Switch hinzugefügt haben, können Sie sie aus dem Distributed Switch entfernen.
- Wenn Sie die Hosts zu einem neuen Distributed Switch hinzugefügt haben, den Sie nicht für andere Zwecke verwenden, können Sie den Distributed Switch löschen.

Konfigurieren der Exportversion des Filters „Verteilte Firewall“ auf Hosts

Die Exportversion der verteilten Firewall muss auf Hosts auf 1.000 festgelegt werden, bevor Sie sie auf NSX-T Data Center migrieren. Sie müssen die Exportversion überprüfen und gegebenenfalls aktualisieren.

Verfahren

- ◆ Führen Sie für jeden Host die folgenden Schritte aus.
 - a Melden Sie sich bei der Befehlszeilenschnittstelle an.
 - b Rufen Sie den Filter „Verteilte Firewall“ für den Host ab.

```
[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 Verwenden Sie die Filterinformationen, um die Exportversion für den Host abzurufen.

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

- d Ist die Version nicht auf 1.000 festgelegt, richten Sie die Exportversion ein. Verwenden Sie eine der folgenden Methoden.

- Verwenden Sie den Befehl `vsipioctl setexportversion`, um die Exportversion festzulegen.

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

- Deaktivieren und aktivieren Sie anschließend die verteilte Firewall auf dem Host.

- e Stellen Sie sicher, dass die Exportversion aktualisiert wurde.

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

Migrieren von NSX Data Center for vSphere auf NSX-T Data Center

Verwenden Sie den Migrations-Koordinator zum Importieren der Konfiguration, zum Beheben von Problemen mit der Konfiguration und zum Migrieren von Edges und Hosts auf Ihre NSX-T Data Center-Umgebung.

Voraussetzungen

Stellen Sie sicher, dass Sie alle relevanten Vorbereitungsschritte abgeschlossen haben, bevor Sie mit der Migration beginnen. Siehe [Vorbereiten der Migration einer NSX Data Center for vSphere-Umgebung](#).

Importieren der NSX Data Center for vSphere-Konfiguration

Um Ihre NSX Data Center-Umgebung von NSX for vSphere auf NSX-T zu migrieren, müssen Sie Details zu Ihrer NSX for vSphere-Umgebung bereitstellen.

Der Migrations-Koordinator wird auf einem NSX Manager-Knoten ausgeführt. Führen Sie alle Migrationen vom Knoten aus, auf dem der Migrations-Koordinator ausgeführt wird.

Vorsicht Stellen Sie eine neue NSX-T-Umgebung als Ziel für die NSX for vSphere-Migration bereit.

Während des Schritts **Konfiguration importieren** werden alle Edge-Knoten-Schnittstellen in der NSX-T-Zielumgebung heruntergefahren. Wenn die NSX-T-Zielumgebung bereits konfiguriert ist und verwendet wird, wird der Datenverkehr beim Starten des Konfigurationsimports unterbrochen.

Voraussetzungen

- Stellen Sie sicher, dass das der NSX for vSphere-Umgebung zugewiesene vCenter Server-System als Compute Manager registriert ist. Siehe [Hinzufügen eines Compute Managers](#).
- Stellen Sie sicher, dass Sie einen IP-Pool erstellt haben, der für Edge-TEPs verwendet werden soll. Siehe [Erstellen eines IP-Pools für Edge-Tunnel-Endpoints](#).

Verfahren

- 1 Melden Sie sich bei der NSX Manager-Befehlszeilenschnittstelle als **admin** an und starten Sie den Migrations-KoordinatorDienst.

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

- 2 Melden Sie sich über einen Browser beim NSX Manager-Knoten an, auf dem der Migrations-KoordinatorDienst gestartet wurde. Melden Sie sich als **admin** an.
- 3 Navigieren Sie zu **System > Migrieren**.
- 4 Klicken Sie im Bereich **NSX für vSphere migrieren** auf **Erste Schritte**.
- 5 Klicken Sie auf der Seite **Konfiguration importieren** auf **NSX auswählen** und stellen Sie die Anmeldedaten für vCenter und NSX for vSphere bereit.

Hinweis Im Dropdown-Menü für vCenter werden alle vCenter Server-Systeme angezeigt, die als Compute Manager registriert sind. Klicken Sie auf **Neuen hinzufügen**, wenn Sie einen Compute Manager hinzufügen müssen.

- 6 Klicken Sie auf **Start**, um die Konfiguration zu importieren.
- 7 Wenn der Import abgeschlossen ist, klicken Sie auf **Weiter**, um mit der Seite **Probleme beheben** fortzufahren.

Abbrechen oder Neustarten der NSX for vSphere-Migration

Sie können den Migrationsprozess abbrechen. Dies ist möglicherweise erforderlich, wenn Sie Änderungen an der NSX for vSphere-Umgebung vorgenommen haben und die Migration neu starten müssen.

Auf jeder Seite der Migration steht die Schaltfläche **Abbrechen** zur Verfügung. Beim Abbrechen einer Migration werden alle Angaben zum Migrationsstatus aus dem System gelöscht.

Vorsicht Brechen Sie eine Migration nicht ab, wenn eine Edge- oder Hostmigration gestartet wurde. Durch Abbruch der Migration wird der gesamte Migrationsstatus gelöscht und der bisherige Fortschritt kann nicht angezeigt werden.

Wenn Sie Ihre Konfiguration importiert, aber noch nicht migriert haben, können Sie auf **Abbrechen** klicken, um neu zu starten.

Wenn Sie die Konfiguration migriert haben, müssen Sie die folgenden Schritte ausführen, um die Migration neu zu starten:

- 1 Brechen Sie die Migration ab.
- 2 Stellen Sie eine neue NSX-T-Umgebung mit NSX Manager- und NSX Edge-Appliances bereit.

3 Starten Sie eine neue Migration.

Vorsicht In NSX-T Data Center 2.4.0 gibt es eine **Rollback**-Schaltfläche für einige der Migrationsschritte. Die Verwendung der Schaltfläche **Rollback** kann zu unerwartetem Verhalten führen. Verwenden Sie stattdessen die Schaltfläche **Abbrechen**, um die Migration beim Schritt **Konfiguration importieren** oder **Konfiguration migrieren** abubrechen. Wenn Sie Edge-Knoten migriert haben und ein Rollback durchführen müssen, wenden Sie sich an den VMware-Support.

Beheben von Konfigurationsproblemen und Bereitstellen von Edge-Knoten

Nachdem Sie die Konfiguration aus Ihrer NSX Data Center for vSphere-Umgebung importiert haben, müssen Sie die gemeldeten Konfigurationsprobleme überprüfen und beheben, bevor Sie mit der Migration fortfahren können.

Überprüfen der Migrationsinformationen

Wenn Änderungen an der NSX for vSphere-Umgebung erforderlich sind, müssen Sie die Migration neu starten, um die neue Konfiguration aufzunehmen. Überprüfen Sie das gesamte Feedback zur Migration, bevor Sie mit der Eingabe beginnen. Hierdurch vermeiden Sie ein doppeltes Arbeitsaufkommen.

Hinweis Für einige NSX for vSphere-Funktionen sind möglicherweise automatische Konfigurationen wie z. B. Zertifikate vorhanden. Wenn diese Konfigurationen für Funktionen gelten, die für die spezifische Topologie nicht unterstützt werden, werden diese automatischen Konfigurationen als Probleme gekennzeichnet, die bei der Migration übersprungen werden müssen. In Topologien, die keine L4-L7-Dienste auf Edge Services Gateways unterstützen, werden beispielsweise die für VPN und DNS vorhandenen Zertifikate Probleme auslösen, um diese Konfigurationen bei der Migration zu überspringen.

Verfahren

- 1 Klicken Sie auf der Seite **Konfigurationsfehler beheben** auf **Nachrichten**, um Informationen zur Migration anzuzeigen.

Das Fenster **Nachrichten** enthält Details zu den NSX-T Edge-Knoten, die zum Ersetzen der NSX for vSphere-Edge Services Gateways benötigt werden. Die Anforderungen umfassen sowohl die Größe als auch die Anzahl der Edge-Knoten. Sie müssen die Edge-Knoten bereitstellen, bevor Sie den Schritt **Konfigurationsfehler beheben** abschließen können. Weitere Informationen hierzu finden Sie unter [Bereitstellen von NSX Edge-Knoten](#).

- 2 Überprüfen Sie die gemeldeten Probleme in jeder Kategorie, um blockierende Probleme oder andere Probleme zu ermitteln, die Änderungen an Ihrer NSX for vSphere-Umgebung erfordern.

Nächste Schritte

Wenn Sie blockierende Probleme oder andere Konfigurationen finden, die eine Änderung der NSX for vSphere-Umgebung erforderlich machen, führen Sie die entsprechenden Konfigurationen durch, bevor Sie fortfahren. Sie müssen die aktuelle Migration abbrechen und die neue Konfiguration importieren. Siehe [Vornehmen von Änderungen an der NSX for vSphere-Umgebung](#).

Wenn Sie keine blockierenden Probleme oder andere Konfigurationen finden, die eine Änderung der NSX for vSphere-Umgebung erforderlich machen, können Sie mit der Migration fortfahren. Siehe [Bereitstellen von NSX Edge-Knoten](#).

Vornehmen von Änderungen an der NSX for vSphere-Umgebung

Sie müssen unter Umständen Änderungen an Ihrer NSX for vSphere-Umgebung durchführen, um mit der Migration fortzufahren, wenn beispielsweise blockierende Probleme gefunden werden. Wenn Sie Änderungen vornehmen, müssen Sie die Konfiguration erneut importieren, damit der Migrations-Koordinator über die Änderungen informiert wird.

Voraussetzungen

Stellen Sie sicher, dass die Host- oder Edge-Migration nicht gestartet wurde. Weitere Informationen zum Neustarten der Migration finden Sie unter [Abbrechen oder Neustarten der NSX for vSphere-Migration](#).

Verfahren

- 1 Nehmen Sie die erforderlichen Änderungen in der NSX for vSphere-Umgebung vor.
- 2 Navigieren Sie zur Seite **Konfiguration importieren** und klicken Sie auf **Abbrechen**.
Durch den Abbruch wird der aktuelle Migrationsvorgang gelöscht. Alle zuvor vorgenommenen Eingaben werden entfernt.
- 3 Klicken Sie auf **Starten**, um die aktualisierte Konfiguration zu importieren.

Die Migration startet mit der neuen NSX for vSphere-Konfiguration.

Nächste Schritte

Setzen Sie die Migration fort. Siehe [Beheben von Konfigurationsproblemen und Bereitstellen von Edge-Knoten](#).

Bereitstellen von NSX Edge-Knoten

Bevor Sie die Migration abschließen können, müssen Sie Edge-Knoten in der entsprechenden Anzahl und Größe bereitstellen.

In einer neuen NSX-T-Umgebung stehen zahlreiche Optionen zur Bereitstellung von NSX Edge zur Verfügung. Wenn Sie die Migration jedoch mithilfe des Migrations-Koordinators durchführen, müssen Sie NSX Edge als virtuelle Maschine auf ESXi bereitstellen. Führen Sie eine Bereitstellung mithilfe einer OVA- oder OVF-Datei durch. Führen Sie keine Bare-Metal-Bereitstellung durch. Führen Sie keine Bereitstellung über die NSX Manager-Schnittstelle durch.

Sie müssen die NSX Edge-Knoten auf ESXi-Hosts bereitstellen, die nicht Teil der NSX for vSphere-Umgebung sind.

Weitere Informationen zu Edge-Netzwerken finden Sie unter „Einrichtung von NSX Edge-Netzwerken“ im *Installationshandbuch für NSX-T Data Center*.

Voraussetzungen

- Sie müssen über genügend ESXi-Hosts mit geeigneten Ressourcen verfügen, damit genügend Speicherplatz für die NSX Edge-Appliances vorhanden ist.

Verfahren

- 1 Suchen Sie im VMware-Download-Portal nach der OVA-Datei der NSX Edge-Appliance.
Kopieren Sie die Download-URL oder laden Sie die OVA-Datei auf Ihren Computer herunter.
- 2 Wählen Sie im vSphere Client den Host aus, auf dem die NSX Edge-Appliance installiert werden soll.
- 3 Wählen Sie im Kontextmenü die Option **OVF-Vorlage bereitstellen** aus, um den Installationsassistenten zu starten.
- 4 Geben Sie die URL der herunterzuladenden OVA-Datei ein oder navigieren Sie zur gespeicherten OVA-Datei.
- 5 Geben Sie einen Namen für die NSX Edge-VM ein.
Der eingegebene Name wird in der Bestandsliste angezeigt.
- 6 Wählen Sie eine Computing-Ressource für die NSX Edge-Appliance aus.
- 7 Reservieren Sie Arbeitsspeicher für die NSX Edge-Appliance, um eine optimale Leistung zu erreichen.
Legen Sie die Reservierung so fest, dass NSX Edge über ausreichend Arbeitsspeicher verfügt, um eine effiziente Ausführung sicherzustellen. Weitere Informationen finden Sie unter „Systemanforderungen der NSX Edge-VM“ im *Installationshandbuch für NSX-T Data Center*.
- 8 Überprüfen Sie die Details der OVF-Vorlage.
- 9 Wählen Sie einen Datenspeicher für die Dateien der NSX Edge-Appliance aus.
- 10 Akzeptieren Sie die Standardnetzwerkschnittstelle für die Quelle und das Ziel.
Sie können das Ziel des Standardnetzwerks für die restlichen Netzwerke übernehmen und die Netzwerkkonfiguration ändern, nachdem die NSX Edge bereitgestellt wurde.
- 11 Wählen Sie im Dropdown-Menü die IP-Zuteilung aus.
- 12 Geben Sie die System-Root-, CLI-Admin- und Audit-Kennwörter für die NSX Edge ein.
Ihre Kennwörter müssen den Einschränkungen zur Kennwortkomplexität entsprechen.
 - mindestens 12 Zeichen
 - mindestens ein Kleinbuchstabe
 - mindestens ein Großbuchstabe
 - mindestens eine Zahl
 - mindestens ein Sonderzeichen
 - mindestens fünf unterschiedliche Zeichen

- keine Wörterbuchwörter
- keine Palindrome
- mehr als vier monotone Zeichenfolgen ist nicht zulässig

- 13 Geben Sie das Standard-Gateway, die IPv4-Adresse und Netzmaske des Verwaltungsnetzwerks, die DNS- und NTP-IP-Adresse ein.
- 14 Geben Sie den Hostnamen der NSX Edge-VM ein.
- 15 Aktivieren Sie SSH und lassen Sie gegebenenfalls Root-SSH-Anmeldung an der NSX Edge-Befehlszeile zu.

Standardmäßig sind diese Optionen aus Sicherheitsgründen deaktiviert.

- 16 Stellen Sie sicher, dass die gesamte Spezifikation der benutzerdefinierten OVA-Vorlage korrekt ist, und klicken Sie auf **Beenden**, um die Installation zu starten.

Die Installation kann 7 bis 8 Minuten dauern.

- 17 Öffnen Sie die Konsole von NSX Edge, um den Startvorgang zu verfolgen.

Wenn das Konsolenfenster nicht geöffnet wird, stellen Sie sicher, dass Popups zulässig sind.

- 18 Nachdem der NSX Edge gestartet ist, melden Sie sich bei der CLI mit Admin-Anmeldedaten an.

Hinweis Wenn Sie sich nach dem Starten des NSX Edge nicht zum ersten Mal als Administrator anmelden, wird der Datenebenendienst nicht automatisch auf dem NSX Edge gestartet.

- 19 Führen Sie den Befehl `get interface eth0.<vlan_ID>` aus, um zu überprüfen, ob die IP-Adresse wie erwartet angewendet wurde.

```
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
...
```

Hinweis Wenn Sie NSX Edge-VMs auf einem nicht von NSX verwalteten Host erstellen, stellen Sie sicher, dass die MTU-Einstellung auf dem physischen Host-Switch für die Datennetzwerkkarte auf 1600 (statt 1500) festgelegt ist.

- 20 Stellen Sie sicher, dass die NSX Edge-Appliance über die erforderliche Konnektivität verfügt.

Wenn Sie SSH aktiviert haben, stellen Sie sicher, dass Sie eine SSH-Verbindung zu NSX Edge herstellen können.

- Sie können einen Ping-Vorgang für das NSX Edge ausführen.
- NSX Edge kann einen Ping-Vorgang für das zugehörige Standard-Gateway ausführen.

- Das NSX Edge kann einen Ping-Vorgang für die Hypervisor-Hosts ausführen, die im selben Netzwerk wie NSX Edge sind.
- NSX Edge kann einen Ping-Vorgang für den zugehörigen DNS-Server und NTP-Server ausführen.

21 Beheben Sie Konnektivitätsprobleme.

Hinweis Wenn keine Konnektivität hergestellt werden kann, stellen Sie sicher, dass sich der VM-Netzwerkadapter im richtigen Netzwerk oder VLAN befindet.

Standardmäßig beansprucht der NSX Edge-Datenpfad alle Netzwerkkarten (NICs) von virtuellen Maschinen mit Ausnahme der Management-NIC (derjenigen, die eine IP-Adresse und eine Standardroute aufweist). Wenn Sie eine Netzwerkkarte als Verwaltungsschnittstelle falsch zugewiesen haben, führen Sie die folgenden Schritte aus, um mit DHCP die Verwaltungs-IP-Adresse der korrekten Netzwerkkarte zuzuweisen.

- a Melden Sie sich bei der Befehlszeilenschnittstelle (CLI) an, und geben Sie den Befehl **stop service dataplane** ein.
- b Geben Sie den Befehl **set interface *Schnittstelle* dhcp plane mgmt** ein.
- c Platzieren Sie die *Schnittstelle* im DHCP-Netzwerk und warten Sie, bis dieser *Schnittstelle* eine IP-Adresse zugewiesen wurde.
- d Geben Sie den Befehl **start service dataplane** ein.

Die fp-ethX-Ports des Datenpfads, die für VLAN-Uplink und Tunnel-Overlay verwendet werden, werden mit den Befehlen **get interfaces** und **get physical-port** von NSX Edge angezeigt.

Verbinden von NSX Edge mit der Managementebene

Sie müssen die erstellten Edge-Knoten mit der Managementebene verbinden.

Verbinden Sie die Edge-Knoten ausschließlich unter Verwendung dieser Methode mit der Managementebene. Erstellen Sie keine Transportknoten anhand der Edge-Knoten.

Verfahren

- 1 Öffnen Sie eine SSH-Sitzung mit der NSX Manager-Appliance.
- 2 Öffnen Sie eine SSH-Sitzung mit NSX Edge.
- 3 Führen Sie den Befehl `get certificate api thumbprint` auf der NSX Manager-Appliance aus.

Die Befehlsausgabe besteht aus einer Reihe von alphanumerischen Zeichen, die für diesen NSX Manager eindeutig sind.

Beispiel:

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

4 Führen Sie auf NSX Edge den Befehl **join management-plane** aus.

Geben Sie die folgenden Informationen an:

- Hostname oder IP-Adresse von NSX Manager mit einer optionalen Portnummer
- NSX Manager-Benutzername
- Zertifikatsfingerabdruck von NSX Manager
- NSX Manager-Kennwort

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

Wiederholen Sie diesen Befehl auf jedem NSX Edge-Knoten.

5 Überprüfen Sie das Ergebnis, indem Sie den Befehl **get managers** auf den NSX Edges ausführen.

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

- 10.172.165.164 Standby

- 10.172.165.165 Standby
```

6 Wählen Sie auf der NSX Manager-Benutzeroberfläche die Seite **System > Fabric-Knoten > Edge-Cluster > Knoten** aus.

Die Konnektivität muss „Aktiv“ sein. Aktualisieren Sie andernfalls den Browserbildschirm.

Vornehmen von Eingaben zu Konfigurationsproblemen

Nachdem Sie die Migrationsinformationen überprüft haben und bereit sind, mit der Migration fortzufahren, können Sie Eingaben für die gemeldeten Konfigurationsprobleme vornehmen. Anhand der bereitgestellten Eingaben wird festgelegt, wie die NSX-T-Umgebung konfiguriert wird.

Einige Beispiele für Konfigurationsprobleme und die erforderlichen Eingaben, einschließlich des Edge-Knoten-Setups, finden Sie unter [Konfigurationsprobleme – Beispiele](#).

Hinweis Für einige NSX for vSphere-Funktionen sind möglicherweise automatische Konfigurationen wie z. B. Zertifikate vorhanden. Wenn diese Konfigurationen für Funktionen gelten, die für die spezifische Topologie nicht unterstützt werden, werden diese automatischen Konfigurationen als Probleme gekennzeichnet, die bei der Migration übersprungen werden müssen. In Topologien, die keine L4-L7-Dienste auf Edge Services Gateways unterstützen, werden beispielsweise die für VPN und DNS vorhandenen Zertifikate Probleme auslösen, um diese Konfigurationen bei der Migration zu überspringen.

Voraussetzungen

- Stellen Sie sicher, dass Sie alle Probleme und Migrationsnachrichten überprüft haben und bereit sind, mit der Migration fortzufahren.

- Alle blockierenden Probleme und andere Probleme, die eine Änderung an NSX for vSphere erfordern, müssen behoben werden.

Wichtig Wenn Sie seit dem letzten Import der Konfiguration aus einem beliebigen Grund eine Änderung an der NSX for vSphere-Umgebung durchgeführt haben, müssen Sie die Migration neu starten. Dies ist der Fall, wenn Sie beispielsweise eine neue VM mit einem logischen Switch verbunden, Änderungen an der Firewall durchgeführt oder NSX for vSphere auf neuen Hosts installiert haben. Informationen zum Neustarten der Migration finden Sie unter [Vornehmen von Änderungen an der NSX for vSphere-Umgebung](#).

Verfahren

- 1 Klicken Sie auf der Seite **Konfigurationsfehler beheben** auf jedes Problem und nehmen Sie eine Eingabe vor.

Jedes Problem kann mehrere Konfigurationselemente abdecken. Für jedes Element gibt es eine oder mehrere mögliche Problemlösungen, wie beispielsweise Überspringen, Konfigurieren oder die Auswahl eines bestimmten Werts.

Bei Problemen, die mehrere Konfigurationselemente betreffen, können Sie Eingaben für jedes einzelne Element vornehmen. Sie können aber auch alle Elemente auswählen und eine Antwort für alle Elemente bereitstellen.

Die Eingaben können von mehreren Benutzern über mehrere Sitzungen hinweg vorgenommen werden. Sie können zu gesendetem Feedback zurückkehren und dieses ändern.

- 2 Nach dem Bereitstellen der Eingaben wird die Schaltfläche **Übermitteln** auf der Seite **Konfigurationsfehler beheben** eingeblendet. Klicken Sie auf **Übermitteln**, um die Änderungen zu speichern.

- 3 Wenn Sie Eingaben für alle Konfigurationsprobleme bereitgestellt haben, klicken Sie auf **Übermitteln**.

Die Eingaben werden überprüft. Sie werden aufgefordert, jede ungültige Eingabe zu aktualisieren. Für bestimmte Konfigurationselemente sind möglicherweise zusätzliche Eingaben erforderlich.

- 4 Nachdem Sie alle geforderten Eingaben übermittelt haben, klicken Sie auf **Weiter**, um mit dem Schritt „Konfiguration migrieren“ fortzufahren.

Konfigurationsprobleme – Beispiele

Sie müssen Eingaben zu einer Vielzahl von Problemen vornehmen, einschließlich Konfigurationsdetails für die neuen NSX-T-Edge-Knoten.

Während des Schritts **Konfigurationsfehler beheben** stellen Sie Informationen zu den Edge-Knoten bereit, die Sie zum Ersetzen der NSX for vSphere-Edge Services Gateways erstellt haben. Die Konfiguration muss möglicherweise geändert werden, um auf NSX-T ordnungsgemäß ausgeführt werden zu können. Unter Umständen müssen Sie eine andere IP-Adresse und ein anderes VLAN als in NSX for vSphere verwenden.

Migrieren von Edge Services Gateways mit L4-L7-Diensten

Die Verwendung derselben Schnittstelle für den Router-Uplink und die Dienste, wie z. B. VPN, wird in NSX for vSphere unterstützt. Diese Konfiguration wird in NSX-T nicht unterstützt. Sie können neue IP-Adressen für die Uplinks der Edge-Knoten zuweisen, damit Sie die IP-Adresse für die auf dem Edge-Knoten ausgeführten Dienste nicht ändern müssen.

Migrieren von Edge Services Gateways in einer Hochverfügbarkeitskonfiguration

Die aus Edge Services Gateways in einer Hochverfügbarkeitskonfiguration bestehende NSX for vSphere-Topologie kann ein Edge Services Gateway mit zwei Uplinks enthalten, die mit zwei verschiedenen verteilten Portgruppen in unterschiedlichen Netzwerken verbunden sind.

In NSX-T wird diese Konfiguration durch zwei Edge-Knoten ersetzt, deren Uplinks beide im selben Netzwerk vorhanden sein müssen.

Ein Edge Services Gateway mit Hochverfügbarkeit kann unter Umständen folgende Konfiguration aufweisen:

- vnic1 verfügt über die IP-Adresse 192.178.14.2/24 und ist mit Portgruppe „Public-DVPG“ verbunden, die VLAN 11 verwendet.
- vnic4 verfügt über die IP-Adresse 192.178.44.2/24 und ist mit Portgruppe „Public-DVPG-2“ verbunden, die VLAN 15 verwendet.

Damit diese Konfiguration nach der Migration funktioniert, muss mindestens eine der IP-Adressen geändert werden, da sich beide im selben Netzwerk befinden müssen.

Dies ist ein Beispiel für die Informationen, die unter Umständen während des Behebens der Konfigurationsfehler bereitgestellt werden.

Für den ersten Edge-Knoten:

- Fabric-ID lautet fa3346d8-2502-11e9-8013-000c2936d594.
- IP-Adresse lautet 192.178.14.2/24.
- VLAN lautet 11.

Für den zweiten Edge-Knoten:

- Fabric-ID lautet fa2de198-2502-11e9-9d7a-000c295cfc6.
- IP-Adresse lautet 192.178.14.4/24.
- Sie müssen das VLAN nicht bereitstellen, da das VLAN des ersten Knotens verwendet wird.

Beide Edge-Knoten müssen mit diesem Netzwerk verbunden sein.

Migrieren der NSX Data Center for vSphere-Konfiguration

Nachdem Sie alle Konfigurationsprobleme behoben haben, können Sie die Konfiguration migrieren. Beim Migrieren der Konfiguration werden in der NSX-T-Umgebung Konfigurationsänderungen vorgenommen,

um die NSX for vSphere-Konfiguration zu replizieren. In der NSX for vSphere-Umgebung werden keine Konfigurationsänderungen vorgenommen.

Vorsicht In NSX-T Data Center 2.4.0 gibt es eine **Rollback**-Schaltfläche für einige der Migrationsschritte. Die Verwendung der Schaltfläche **Rollback** kann zu unerwartetem Verhalten führen. Verwenden Sie stattdessen die Schaltfläche **Abbrechen**, um die Migration beim Schritt **Konfiguration importieren** oder **Konfiguration migrieren** abzubrechen. Wenn Sie Edge-Knoten migriert haben und ein Rollback durchführen müssen, wenden Sie sich an den VMware-Support.

Weitere Informationen hierzu finden Sie unter [Abbrechen oder Neustarten der NSX for vSphere-Migration](#).

Voraussetzungen

Stellen Sie sicher, dass Sie den Schritt **Probleme beheben** abgeschlossen haben.

Verfahren

- 1 Klicken Sie auf der Seite **Konfiguration migrieren** auf **Starten**.
Die NSX for vSphere-Konfiguration wird auf NSX-T migriert.
- 2 Stellen Sie sicher, dass alle NSX for vSphere-Konfigurationen in der NSX-T NSX Manager-Schnittstelle oder -API angezeigt werden.

Wichtig Wenn die Konfiguration auf NSX-T migriert wird, werden die Konfigurationsänderungen in der NSX-T NSX Manager-Datenbank vorgenommen. Es kann allerdings einige Zeit dauern, bis die Konfiguration wirksam wird. Sie müssen sicherstellen, dass alle erwarteten NSX for vSphere-Konfigurationen auf der NSX-T NSX Manager-Schnittstelle oder -API angezeigt werden, bevor Sie mit dem Schritt **Edges migrieren** fortfahren. Beispielsweise Firewall-Konfiguration, logische Switches, Transportzonen.

Ändern der Edge-Konfiguration vor dem Migrieren von Edges

Wenn NSX for vSphere Edge Services Gateways zu NSX-T migriert werden, wird eine Standardkonfiguration für die MTU-Einstellungen der Schnittstelle verwendet. Wenn Sie diese Standardeinstellung ändern möchten, können Sie dies tun, bevor Sie den Schritt **Migrieren der Edges** starten.

Angepasste MTU-Einstellungen in den Routing-Schnittstellen der Edge Services Gateways werden nicht zu NSX-T migriert. Alle in NSX-T erstellten logischen Router-Schnittstellen verwenden die globale MTU-Standard-einstellung „1500“. Um sicherzustellen, dass alle logischen Router-Schnittstellen eine größere MTU aufweisen, können Sie die globale MTU-Standard-einstellung ändern. Sie können die Schnittstellen-MTUs auch für einzelne Fälle ändern.

Verfahren

- 1 Verwenden Sie GET `/api/v1/global-configs/RoutingGlobalConfig`, um die aktuelle Konfiguration abzurufen.

- 2 Ändern Sie den Wert der globalen Standard-MTU: `logical_uplink_mtu`
- 3 Verwenden Sie PUT `/api/v1/global-configs/RoutingGlobalConfig`, um die Konfiguration ändern.

NSX Data Center for vSphere-Edges migrieren

Nach der Migration der Konfiguration können Sie die NSX for vSphere-Edge-Dienste auf NSX-T migrieren. Dies ist der erste Schritt in der Migration, der Ihre Produktionsumgebung ändert.

Wenn Sie eine VLAN-gestützte Mikro-Segmentierungstopologie migrieren, stehen keine Edge Services Gateway-Appliances für die Migration zur Verfügung. Sie sollten dennoch auf **Starten** klicken, damit Sie mit dem Schritt **Hosts migrieren** fortfahren können.

Vorsicht In NSX-T Data Center 2.4.0 gibt es eine **Rollback**-Schaltfläche für einige der Migrationsschritte. Die Verwendung der Schaltfläche **Rollback** kann zu unerwartetem Verhalten führen. Verwenden Sie stattdessen die Schaltfläche **Abbrechen**, um die Migration beim Schritt **Konfiguration importieren** oder **Konfiguration migrieren** abubrechen. Wenn Sie Edge-Knoten migriert haben und ein Rollback durchführen müssen, wenden Sie sich an den VMware-Support.

Weitere Informationen hierzu finden Sie unter [Abbrechen oder Neustarten der NSX for vSphere-Migration](#).

Voraussetzungen

- Alle Konfigurationsprobleme müssen behoben werden.
- Die Konfiguration muss migriert werden.
- Stellen Sie sicher, dass Sie über eine Sicherungskopie von NSX for vSphere und vSphere verfügen, da die aktuellen Konfigurationsänderungen vorgenommen wurden.
- Stellen Sie sicher, dass alle NSX for vSphere-Konfigurationen, die migriert werden sollten, in der NSX-T NSX Manager-Schnittstelle oder -API angezeigt werden.
- Wenn Sie neue IP-Adressen für die NSX-T Edge-Knoten-Uplinks verwenden, müssen Sie die Northbound-Router mit diesen neuen IP-Adressen des BGP-Nachbarn konfigurieren.

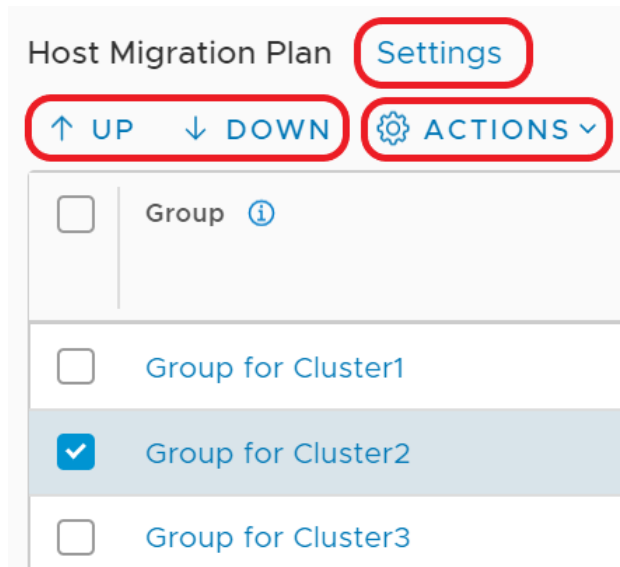
Verfahren

- ◆ Klicken Sie auf der Seite **Edges migrieren** auf **Starten**.

Alle Edges werden migriert. Die Uplinks auf den NSX for vSphere-Edge Services Gateways sind deaktiviert und die Uplinks auf den NSX-T Edge-Knoten werden im Online-Modus ausgeführt.

Konfigurieren der Hostmigration

Die Cluster in der NSX for vSphere-Umgebung werden auf der Seite **Migrieren der Hosts** angezeigt. Die Cluster sind in Migrationsgruppen angeordnet. Jede Migrationsgruppe enthält einen vSphere-Hostcluster. Es gibt mehrere Einstellungen, die steuern, wie die Hostmigration ausgeführt wird.



- Klicken Sie auf **Einstellungen**, um die globalen Einstellungen **Pause zwischen Gruppen** und **Gruppenübergreifende Migrationsreihenfolge** zu ändern.
- Wählen Sie eine einzelne Hostgruppe (Cluster) aus und verwenden Sie die Pfeile, um diese in der Migrationsreihenfolge nach oben oder unten zu verschieben.
- Wählen Sie eine oder mehrere Hostgruppen (Cluster) aus und klicken Sie auf **Aktionen**, um diese Hostgruppeneinstellungen zu ändern: **Migrationsreihenfolge innerhalb der Gruppe** und **Migrationsstatus**.

Pause zwischen Gruppen

Pause zwischen Gruppen ist eine globale Einstellung, die für alle Hostgruppen gilt. Wenn die Pause aktiviert ist, migriert der Migrationskoordinator eine Hostgruppe und wartet dann auf eine Eingabe. Sie müssen auf **Fortfahren** klicken, um mit der nächsten Hostgruppe fortzufahren. Wenn Sie den Status jedes Clusters überprüfen möchten, bevor Sie mit dem nächsten fortfahren, aktivieren Sie **Pause zwischen Gruppen**.

Standardmäßig ist **Pause zwischen Gruppen** deaktiviert.

Serielle oder parallele Migrationsreihenfolge

Sie können festlegen, ob die Migration in einer seriellen oder parallelen Reihenfolge erfolgt. Es gibt zwei Sortiereinstellungen:

■ Gruppenübergreifende Migrationsreihenfolge

Gruppenübergreifende Migrationsreihenfolge ist eine globale Einstellung, die für alle Hostgruppen gilt.

- **Seriell:** Es wird immer jeweils eine Hostgruppe (ein Cluster) migriert.
- **Parallel:** Es werden bis zu fünf Hostgruppen gleichzeitig migriert. Nachdem diese fünf Hostgruppen migriert wurden, wird der nächste Batch mit bis zu fünf Hostgruppen migriert.

■ Migrationsreihenfolge innerhalb der Gruppe

Migrationsreihenfolge innerhalb der Gruppe ist eine spezifische Einstellung für die Hostgruppe (das Cluster) und kann daher separat für jede Hostgruppe konfiguriert werden.

- **Seriell:** Es wird immer jeweils ein Host in der Hostgruppe (Cluster) migriert.
- **Parallel:** Es werden bis zu fünf Hosts in der Hostgruppe gleichzeitig migriert. Nachdem diese fünf Hosts migriert wurden, wird der nächste Batch mit bis zu fünf Hosts migriert.

Standardmäßig sind beide Einstellungen auf **Seriell** festgelegt. Gemeinsam legen die Einstellungen fest, wie viele Hosts gleichzeitig migriert werden.

Tabelle 1-11. Auswirkungen der Migrationseinstellungen auf die Anzahl der Hosts, die gleichzeitig migriert werden

Gruppenübergreifende Migrationsreihenfolge (Cluster)	Migrationsreihenfolge innerhalb der Gruppe (Cluster)	Maximale Anzahl der Hosts, die gleichzeitig migriert werden
Seriell	Seriell	1 Ein Host aus einer Hostgruppe
Seriell	Parallel	5 Fünf Hosts aus einer Hostgruppe
Parallel	Seriell	5 Ein Host aus fünf Hostgruppen
Parallel	Parallel	25 Fünf Hosts aus fünf Hostgruppen

Wichtig Wenn ein Host nicht migriert werden kann, wird der Migrationsvorgang angehalten, nachdem alle in Bearbeitung befindlichen Hostmigrationen abgeschlossen wurden. Wenn **Parallel** für die gruppenübergreifende Migration und die Migration innerhalb von Gruppen ausgewählt ist, kann es zu einem langen Ausfall des fehlgeschlagenen Hosts kommen, bevor Sie die Migration erneut versuchen können. Wählen Sie in einer Produktionsumgebung keine parallele Migrationsreihenfolge innerhalb von Gruppen aus.

Abfolge von Migrationsgruppen

Sie können eine Hostgruppe (ein Cluster) auswählen und diese mit den Pfeilen in der Liste der Gruppen nach oben oder unten verschieben.

Wenn bei der Migration eines Hosts ein Fehler auftritt, können Sie die Hostgruppe an das Ende der Liste der Gruppen verschieben. Die Migration anderer Hostgruppen kann fortgesetzt werden, während Sie das Problem mit dem fehlgeschlagenen Host beheben.

Gruppen aktivieren oder deaktivieren

Hostgruppen (Cluster) können einen von drei Zuständen aufweisen:

- **Aktiviert**

Hosts in diesen Gruppen werden zu NSX-T migriert, wenn Sie auf der Seite **Migrieren der Hosts** auf **Starten** klicken.

■ **Deaktiviert**

Hosts in diesen Gruppen werden nicht zu NSX-T migriert, wenn Sie auf der Seite **Migrieren der Hosts** auf **Starten** klicken. Wenn Sie jedoch für die Migration noch nicht auf **Fertigstellen** geklickt haben, können Sie zur Seite **Migrieren der Hosts** zurückkehren, um sie zu aktivieren und die Hostmigration erneut zu starten. Beenden Sie alle Hostmigrationsaufgaben und klicken Sie innerhalb desselben Wartungsfensters auf **Fertigstellen**.

■ **Nicht migrieren**

Hosts in diesen Gruppen wurden während des Schrittes **Konfiguration auflösen** als nicht für die Migration geeignet identifiziert.

Beispielsweise haben Hosts, auf denen NSX for vSphere nicht installiert ist, den Status **Nicht migrieren**.

Wenn Sie die Migration der Infrastruktur-VMs, wie z. B. NSX Manager, NSX Controller, Edge Services Gateway oder Distributed Logical Router, vermeiden möchten, können Sie deren Cluster für die Migration deaktivieren.

NSX Data Center for vSphere-Hosts migrieren

Nachdem Sie Edges auf NSX-T migriert und sichergestellt haben, dass das Routing und die Diensteseite ordnungsgemäß ausgeführt werden, können Sie Ihre NSX for vSphere-Hosts auf Transportknoten des NSX-T-Hosts migrieren.

Sie können verschiedene Einstellungen in Bezug auf die Hostmigration, einschließlich der Migrationsreihenfolge oder der Aktivierung von Hosts konfigurieren. Stellen Sie vor dem Ändern von Standardeinstellungen sicher, dass Sie die Auswirkungen dieser Einstellungen verstanden haben. Weitere Informationen hierzu finden Sie unter [Konfigurieren der Hostmigration](#).

Während der Hostmigration werden folgende Änderungen vorgenommen:

- NSX for vSphere wird deinstalliert.
- NSX-T wird installiert.
- Hosts werden mit N-VDS konfiguriert, um Distributed vSphere-Switches zu ersetzen:
 - Jeder N-VDS wird mit einem Namen erstellt, der auf den Namen des Distributed Switches verweist. Der Distributed Switch ComputeSwitchA wird beispielsweise als N-VDS `nvds.ComputeSwitchA` erstellt.
 - Wenn verschiedene Cluster unterschiedliche Distributed Switches verwenden, um logische Switches zu stützen, wird ein N-VDS mit einem Namen erstellt, der alle Namen der Distributed Switches kombiniert. Wenn `ComputeCluster1` und `ComputeCluster2` beispielsweise den Distributed Switch `ComputeSwitchA` zum Sichern logischer Switches und `ComputeCluster3` den Switch `ComputeSwitchB` zum Sichern logischer Switches verwendet, wird der N-VDS als `nvds.ComputeSwitchA.ComputeSwitchB` erstellt.

- PNICs, vmks und VTEPs im Distributed Switch werden zu N-VDS migriert.
- Mit den Distributed Switches verbundene VMs sind mit N-VDS verbunden.

Vorsicht Während der Hostmigration kommt es zu einer Unterbrechung des Datenverkehrs. Die Hostmigration sollte während desselben Wartungsfensters wie die Edge-Migration abgeschlossen werden.

Wenn Sie über Regeln für die verteilte Firewall verfügen, die auf eine VM angewendet werden, werden diese Regeln erst an den Host weitergeleitet, wenn der Host und alle seine VMs migriert wurden. Bis die Regeln an den Host weitergeleitet wurden, gilt Folgendes:

- Wenn Sie Whitelist-Vorgänge verwenden (die Standardregel lautet `deny`), ist Ihre Anwendung offline.
 - Wenn Sie Blacklisting-Vorgänge verwenden (die Standardregel lautet `accept`), wird die VM nicht durch die angewendeten Regeln geschützt.
-

Wenn bei der Migration eines Hosts ein Fehler auftritt, stoppt die Migration, nachdem alle laufenden Hostmigrationen abgeschlossen sind. Wenn Sie das Problem mit dem Host behoben haben, klicken Sie auf **Wiederholen**, um die Migration des fehlgeschlagenen Hosts erneut zu starten.

Wenn bei der Migration eines Hosts ein Fehler auftritt, können Sie die Hostgruppe an das Ende der Liste der Gruppen verschieben. Die Migration anderer Hostgruppen kann fortgesetzt werden, während Sie das Problem mit dem fehlgeschlagenen Host beheben.

Nachdem ein Host zu NSX-T migriert wurde, wird möglicherweise ein Alarm mit der Meldung **Netzwerkverbindungsunterbrechung** angezeigt. Der Alarm tritt auf, weil der Host nicht mehr über eine physische Netzwerkkarte (NIC) verfügt, die mit dem vSphere Distributed Switch verbunden ist, mit dem zuvor eine Verbindung hergestellt wurde.

Voraussetzungen

- Stellen Sie sicher, dass die Edge-Migration abgeschlossen ist und das gesamte Routing und die Dienste ordnungsgemäß ausgeführt werden.
- Stellen Sie sicher, dass alle ESXi-Hosts betriebsbereit sind. Beheben Sie alle Probleme mit Hosts, einschließlich getrennter Zustände. Für den Eintritt in den Wartungsmodus dürfen weder ausstehende Neustarts noch ausstehende Aufgaben vorhanden sein.

Hinweis Hosts werden während der Migration nicht in den Wartungsmodus versetzt.

Verfahren

- ◆ Klicken Sie auf **Starten**, um die Hostmigration zu starten.

Die NSX for vSphere-Hosts werden in Transportknoten des NSX-T-Hosts konvertiert. Die Netzwerkschnittstellen der VMs auf den Hosts werden von den logischen NSX for vSphere-Switches getrennt und mit den NSX-T-Segmenten verbunden.

Abschließen der NSX Data Center for vSphere-Migration

Nachdem Sie alle Edges und Hosts in der NSX-T Data Center-Umgebung migriert haben, vergewissern Sie sich, dass die neue Umgebung ordnungsgemäß funktioniert. Wenn alles ordnungsgemäß funktioniert, können Sie die Migration beenden.

Wichtig Stellen Sie sicher, dass alles funktioniert, und klicken Sie im Wartungsfenster auf **Beenden**. Durch Klicken auf **Beenden** wird eine Bereinigung nach der Migration durchgeführt. Beenden Sie den Migrations-Koordinator im Migrationsfenster.

Nach der Migration auf Hosts werden Fehler angezeigt. Die Fehlermeldung lautet:
`UserVars.RmqHostId'` ist ungültig oder überschreitet die maximale Anzahl an zulässigen Zeichen. Der Fehler tritt auf, weil dieser Host weiterhin Teil des NSX Data Center for vSphere-Bestands ist.

Voraussetzungen

- Stellen Sie sicher, dass alle erwarteten Elemente in die NSX-T Data Center-Umgebung migriert wurden.
- Stellen Sie sicher, dass die NSX-T Data Center-Umgebung ordnungsgemäß funktioniert.

Verfahren

- 1 Navigieren Sie zur Seite **Hosts migrieren** des Migrations-Koordinators.
- 2 Klicken Sie auf **Fertigstellen**.

Ein Dialogfeld wird angezeigt, um die Beendigung der Migration zu bestätigen. Wenn Sie die Migration abgeschlossen haben, werden alle Migrationsdetails gelöscht. Sie können die Einstellungen dieser Migration nicht mehr überprüfen. Wie beispielsweise, welche Eingaben auf der Seite **Probleme beheben** vorgenommen wurden, oder welche Hosts von der Migration ausgeschlossen wurden.

Nächste Schritte

Wenn Sie von NSX for vSphere 6.4.4 migriert haben, führen Sie einen Neustart aller Hosts durch, die zu NSX-T migriert wurden. Dies muss vor dem Upgrade auf eine neuere Version von NSX-T erfolgen.

Deinstallieren von NSX for vSphere nach der Migration

Wenn Sie sichergestellt haben, dass die Migration erfolgreich war, und auf **Fertigstellen** geklickt haben, um die Migration abzuschließen, können Sie Ihre NSX for vSphere-Umgebung deinstallieren.

Der Vorgang zum Deinstallieren von NSX for vSphere nach der Migration auf NSX-T unterscheidet sich von der Standarddeinstallation für NSX for vSphere.

Voraussetzungen

- Stellen Sie sicher, dass die Migration erfolgreich durchgeführt wurde und dass alle Funktionalitäten in der NSX-T-Umgebung funktionieren.

- Stellen Sie sicher, dass Sie auf der Seite **Migrieren der Hosts** auf **Fertigstellen** geklickt haben.

Verfahren

- 1 Löschen Sie die ESX Agent Manager-Agencys, die der NSX for vSphere-Umgebung zugeordnet sind.
 - a Navigieren Sie im vSphere Client zu **Menü > Verwaltung**. Klicken Sie unter **Lösungen** auf **vCenter Server-Erweiterungen**. Doppelklicken Sie auf **vSphere ESX Agent Manager** und klicken Sie auf die Registerkarte **Konfigurieren**.
 - b Wählen Sie für jede Agency, deren Namen mit `_NSX_` beginnt, die Agency aus, klicken Sie dann auf das Menü mit drei Punkten (⋮) und wählen Sie **Agency löschen** aus.
- 2 Entfernen Sie das NSX-Plug-In aus vCenter.
 - a Greifen Sie über den verwalteten Objektbrowser unter `https://<vcenter-ip>/mob/?moid=ExtensionManager` auf den Erweiterungsmanager zu.
 - b Klicken Sie auf **UnregisterExtension**.
 - c Geben Sie im Dialogfeld **UnregisterExtension** `com.vmware.vShieldManager` in das Textfeld **Wert** ein und klicken Sie auf **Methode aufrufen**.
 - d Geben Sie im Dialogfeld **UnregisterExtension** `com.vmware.nsx.ui.h5` in das Textfeld **Wert** ein und klicken Sie auf **Methode aufrufen**.
 - e Sie können überprüfen, ob Sie die Registrierung der Erweiterungen aufgehoben haben, indem Sie zur Erweiterungsmanager-Seite unter `https://<vcenter-ip>/mob/?moid=ExtensionManager` gehen und die Werte für die Eigenschaft **extensionList** anzeigen.

3 Löschen Sie die vSphere Web Client-Verzeichnisse und die vSphere Client (HTML5)-Verzeichnisse für NSX for vSphere und starten Sie die Clientdienste dann neu.

a Stellen Sie eine Verbindung zur Systembefehlszeile von vCenter Server her.

- Wenn Sie eine vCenter Server-Appliance verwenden, melden Sie sich mit der Konsole oder SSH als root an. Sie müssen sich als root anmelden und die Befehle aus der Bash-Shell ausführen. Sie können die Bash-Shell mit den folgenden Befehlen starten.

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

- Wenn Sie vCenter Server für Windows verwenden, melden Sie sich mit der Konsole oder RDP als Administrator an.

b Löschen Sie alle NSX for vSphere-Plug-In-Verzeichnisse.

Hinweis Möglicherweise ist ein Plug-In-Verzeichnis nicht vorhanden, wenn Sie den zugehörigen Client noch nie gestartet haben.

Löschen Sie auf der vCenter Server-Appliance die folgenden Verzeichnisse:

- Um das vSphere Web Client-Plug-In zu entfernen, löschen Sie das Verzeichnis `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/com.vmware.vShieldManager-<version>-<build>`.
- Um das vSphere Client-Plug-In zu entfernen, löschen Sie das Verzeichnis `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/com.vmware.nsx.ui.h5-<version>-<build>`.

Löschen Sie auf vCenter Server für Windows die folgenden Verzeichnisse:

- Um das vSphere Web Client-Plug-In zu entfernen, löschen Sie das Verzeichnis `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity\com.vmware.vShieldManager-<version>-<build>`.
- Um das vSphere Client-Plug-In zu entfernen, löschen Sie das Verzeichnis `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity\com.vmware.nsx.ui.h5-<version>-<build>`.

c Starten Sie die Clientdienste auf der vCenter Server-Appliance oder auf vCenter Server unter Windows neu.

Tabelle 1-12. Clientdienst-Befehle

Clientdienst	vCenter Server Appliance	vCenter Server für Windows
vSphere Web Client neu starten	<pre># service-control --stop vsphere-client # service-control --start vsphere-client</pre>	<pre>> cd C:\Program Files\VMware \vCenter Server\bin</pre>

Tabelle 1-12. Clientdienst-Befehle (Fortsetzung)

Clientdienst	vCenter Server Appliance	vCenter Server für Windows
		<pre>> service-control --stop vspherebclientsvc > service-control --start vspherebclientsvc</pre>
vSphere Client neu starten	<pre># service-control --stop vsphere-ui # service-control --start vsphere-ui</pre>	<pre>> cd C:\Program Files\VMware \vCenter Server\bin > service-control --stop vsphere-ui > service-control --start vsphere-ui</pre>

4 Schalten Sie die NSX for vSphere-Appliances aus und löschen Sie sie.

- a Navigieren Sie zu **Startseite > Hosts und Cluster**.
- b Suchen Sie die folgenden NSX for vSphere-Appliance-VMs. Klicken Sie mit der rechten Maustaste auf jede VM und wählen Sie **Ausschalten** aus, klicken Sie dann mit der rechten Maustaste und wählen Sie **Von Festplatte löschen** aus.
 - NSX Edge-VMs.
 - NSX Controller-VMs.
 - NSX Manager-VM.

Fehlerbehebung bei der Migration von NSX Data Center for vSphere

Beim Abschließen der Migration von NSX Data Center for vSphere treten unter Umständen Fehler auf. Die folgenden Informationen zur Fehlerbehebung bieten Unterstützung bei der Lösung dieser Probleme.

Zugreifen auf den Migrations-Koordinator

Problem	Lösung
Der Migrations-Koordinator wird bei System > Migrieren nicht angezeigt.	<p>Stellen Sie sicher, dass der Migrations-Koordinator auf NSX Manager ausgeführt wird.</p> <pre>manager> get service migration-coordinator Service name: migration-coordinator Service state: running</pre> <p>Wenn der Dienst nicht ausgeführt wird, starten Sie ihn mit <code>start service migration-coordinator</code>.</p>
Bei der Rückkehr zum Migrations-Koordinator wird die aktuell ausgeführte Migration nicht angezeigt.	<p>Die Anmeldedaten von vCenter Server oder NSX Manager werden vom Migrations-Koordinator nicht gespeichert. Wenn der Migrations-Koordinator während der Ausführung einer Migration neu gestartet wird, werden auf der Seite System > Migrieren gegebenenfalls veraltete oder keine Informationen angezeigt. Zur Anzeige des letzten Migrationsstatus beim Neustart des Migrations-Koordinators führen Sie folgende Schritte aus:</p> <ol style="list-style-type: none"> 1 Aktualisieren Sie die Seite System > Migrieren. 2 Klicken Sie auf Erste Schritte und geben Sie die Anmeldedaten für vCenter Server und NSX Manager ein.

Probleme beim Importieren der Konfiguration

Problem	Lösung
Die Konfiguration kann nicht importiert werden.	<ol style="list-style-type: none"> 1 Klicken Sie auf Wiederholen, um den Importvorgang zu wiederholen. Nur die fehlgeschlagenen Importschritte werden wiederholt.

Probleme bei der Hostmigration

Problem	Lösung
Die Hostmigration schlägt aufgrund einer fehlenden Berechnungsmanagerkonfiguration fehl.	<p>Die Berechnungsmanagerkonfiguration gilt als Voraussetzung für die Migration. Wenn die Berechnungsmanagerkonfiguration nach dem Start der Migration jedoch aus NSX Manager entfernt wird, bleibt die Einstellung im Migrations-Koordinator erhalten. Die Migration wird bis zu dem Schritt der Hostmigration fortgesetzt, der fehlschlägt.</p> <p>Fügen Sie einen Berechnungsmanager zu NSX Manager hinzu und geben Sie dieselben vCenter Server-Details ein, die beim erstmaligen Import der NSX for vSphere-Konfiguration verwendet wurden.</p>
<p>Die Hostmigration schlägt aufgrund veralteter dvFilter fehl.</p> <p>Beispiel für eine Fehlermeldung: Stale dvFilters present: ['port 33554463 (disconnected)', 'port 33554464 (disconnected)'] Stale dvfilters present. Aborting]</p>	<p>Melden Sie sich bei dem Host an, der nicht migriert werden konnte, ermitteln Sie die getrennten Ports und starten Sie die entsprechende VM neu oder verbinden Sie die getrennten Ports. Anschließend können Sie den Schritt „Hostmigration“ wiederholen.</p> <ol style="list-style-type: none"> 1 Melden Sie sich bei der Befehlszeilenschnittstelle des Hosts an, der nicht migriert werden konnte. 2 Führen Sie <code>summarize-dvfilter</code> aus und suchen Sie nach den Ports, die in der Fehlermeldung gemeldet wurden. <pre>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</pre> <ol style="list-style-type: none"> 3 Suchen Sie nach der betroffenen VM und dem betroffenen Port. <p>In der Fehlermeldung wird beispielsweise darauf hingewiesen, dass Port 33554463 getrennt wurde.</p> <ol style="list-style-type: none"> a Suchen Sie nach dem Abschnitt der <code>summarize-dvfilter</code>-Ausgabe, die diesem Port entspricht. Der VM-Name wird hier aufgeführt. In diesem Fall handelt es sich um <code>2-vm_RHEL-srv5.6.0.9-32-local-258-963adcb8-ab56-41d6-bd9e-2d1c329e7745</code>. b Suchen Sie nach dem Eintrag <code>name</code>, um die getrennte VM-Schnittstelle zu ermitteln. In diesem Fall handelt es sich um <code>eth1</code>. Die zweite Schnittstelle ist von <code>2-vm_RHEL-srv5.6.0.9-32-local-258-963adcb8-ab56-41d6-bd9e-2d1c329e7745</code> getrennt. <ol style="list-style-type: none"> 4 Beheben Sie das Problem mit diesem Port. Führen Sie einen der folgenden Schritte aus: <ul style="list-style-type: none"> ■ Starten Sie die betroffene VM neu.

Problem	Lösung
	<ul style="list-style-type: none">■ Verbinden Sie den getrennten Vnic-Port mit einem beliebigen Netzwerk. <p>5 Klicken Sie auf der Seite Hosts migrieren auf Wiederholen.</p>

Migration von vSphere-Netzwerken

2

Sie können den Migrations-Koordinator verwenden, um eine vorhandene vSphere Distributed Switch-Konfiguration zu einer NSX-T Data Center-Umgebung zu migrieren.

Der Migrations-Koordinator verschiebt den vSphere Distributed Switch, die Computing-Hosts, PNICs, vmkNICs und vNIC-Sicherungen zum N-VDS.

Hinweis Sie können den Migrations-Koordinator verwenden, um vSphere Distributed Switch-Konfigurationen nur dann auf NSX-T zu migrieren, wenn NSX for vSphere nicht auf dem Host installiert ist.

Dieses Kapitel enthält die folgenden Themen:

- [Grundlegendes zur Migration des vSphere-Netzwerks](#)
- [Vorbereiten der Migration des vSphere-Netzwerks](#)
- [Migrieren eines vSphere-Netzwerks zu NSX-T Data Center](#)

Grundlegendes zur Migration des vSphere-Netzwerks

Sie können jeweils nur einen vSphere-Distributed Switch auf NSX-T migrieren.

Übersicht des Migrationsprozesses

Während der Migration werden Sie die folgenden Schritte durchführen:

- Bereiten Sie Ihre NSX-T-Umgebung vor.
 - Konfigurieren Sie einen Berechnungsmanager in der NSX-T-Umgebung. Fügen Sie das vCenter Server-System hinzu, das den zu migrierenden vSphere Distributed Switch verwaltet.
 - Starten Sie den Migrations-KoordinatorDienst.
- Importieren Sie die Konfiguration von vSphere.
 - Geben Sie die Details Ihrer vSphere-Umgebung ein.
 - Die Konfiguration wird abgerufen und Vorabprüfungen werden ausgeführt.
- Wählen Sie den zu migrierenden vSphere Distributed Switch aus.
- Beheben Sie Probleme mit der Konfiguration.

Beantworten Sie Fragen zur Systemkonfiguration. Erst nach Klärung der Fragen können Sie die vSphere-Umgebung auf NSX-T migrieren. Probleme können in mehreren Durchgängen von mehreren Personen behoben werden.

- Migrieren Sie die Konfiguration.
 - Nachdem alle Konfigurationsprobleme behoben sind, können Sie die Konfiguration in NSX-T importieren. Konfigurationsänderungen werden auf NSX-T vorgenommen, es werden jedoch noch keine Änderungen an der vSphere-Umgebung durchgeführt.
- Migrieren Sie die Hosts.
 - Die NSX-T-Software wird auf den Hosts installiert. VM-Schnittstellen werden von den vSphere Distributed Switch-Portgruppen getrennt und mit den neuen NSX-T-Segmenten verbunden.

Vorsicht Während der Migration eines jeden Hosts kommt es zu einer Unterbrechung des Datenverkehrs.

- Schließen Sie die Migration ab.
 - Nachdem Sie sichergestellt haben, dass das migrierte Netzwerk ordnungsgemäß ausgeführt wird, können Sie auf **Fertigstellen** klicken, um den Migrationsstatus zu löschen. Sie können nun einen anderen vSphere Distributed Switch auf NSX-T migrieren.

Vorbereiten der Migration des vSphere-Netzwerks

Sie können vSphere Distributed Switches migrieren, die nicht zu einer NSX Data Center for vSphere-Umgebung gehören.

Erforderliche Software und Versionen

- In den *VMware-Produktinteroperabilitätstabellen* erhalten Sie weitere Informationen zu den benötigten Versionen von vCenter Server und ESXi: http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php#interop&175=&1=&2=
- vSphere Distributed Switch 6.5.0 und 6.6.0 werden unterstützt.

Hinzufügen eines Berechnungsmanagers

Um eine vSphere Distributed Switch zu migrieren, müssen Sie das zugeordnete vCenter Server-System als Berechnungsmanager in NSX-T konfigurieren, bevor Sie den Migrationsvorgang starten können.

Verfahren

- 1 Melden Sie sich über einen Browser bei einem NSX Manager unter `https://<nsx-manager-ip-address>` an.
- 2 Wählen Sie **System > Fabric > Berechnungsmanager > Hinzufügen** aus.

3 Vervollständigen Sie die Details zum Compute Manager.

Option	Beschreibung
Name und Beschreibung	Geben Sie den Namen zum Identifizieren von vCenter Server ein. Sie können optional spezielle Details wie z. B. die Anzahl Cluster in vCenter Serverbeschreiben.
Domänenname/IP-Adresse	Geben Sie die IP-Adresse für vCenter Server ein.
Typ	Behalten Sie die Standardoption bei.
Benutzername und Kennwort	Geben Sie die vCenter Server-Anmeldedaten ein.
Fingerabdruck	Geben Sie den Wert für den vCenter Server-SHA-256-Fingerabdruckalgorithmus ein.

Wenn Sie den Fingerabdruckwert leer lassen, werden Sie aufgefordert, den vom Server bereitgestellten Fingerabdruck zu akzeptieren.

Nachdem Sie den Fingerabdruck akzeptiert haben, dauert es einige Sekunden, bis NSX-T Data Center die vCenter Server-Ressourcen ermittelt und registriert.

4 Wenn sich das Symbol „Fortschritt“ von **In Bearbeitung** in **Nicht registriert** ändert, führen Sie die folgenden Schritte aus, um den Fehler zu beheben.

- a Wählen Sie die Fehlermeldung und klicken Sie auf **Beheben**. Eine mögliche Fehlermeldung lautet:

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

- b Geben Sie die vCenter Server-Anmeldedaten ein und klicken Sie auf **Beheben**.

Wenn eine bestehende Registrierung vorhanden ist, wird sie ersetzt.

Migrieren eines vSphere-Netzwerks zu NSX-T Data Center

Verwenden Sie den Migrations-Koordinator zum Importieren der Konfiguration, zum Beheben von Problemen mit der Konfiguration und zum Migrieren von Hosts zu Ihrer NSX-T Data Center-Umgebung.

Importieren der vSphere-Netzwerkconfiguration

Um vSphere Hosts und Netzwerke nach NSX-T Data Center zu migrieren, müssen Sie Details zu Ihrer Umgebung vSphere angeben.

Der Migrations-Koordinator wird auf einem NSX Manager-Knoten ausgeführt. Führen Sie alle Migrationsvorgänge von dem Knoten aus, auf dem der Migrations-Koordinator ausgeführt wird.

Voraussetzungen

- Stellen Sie sicher, dass das vCenter Server-System, das mit dem zu migrierenden vSphere Distributed Switch verknüpft ist, als Berechnungsmanager registriert ist. Siehe [Hinzufügen eines Berechnungsmanagers](#).

Verfahren

- 1 Melden Sie sich bei einer NSX Manager-CLI als **admin** an und starten Sie den Migrations-KoordinatorDienst.

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

- 2 Melden Sie sich über einen Browser beim NSX Manager-Knoten an, der den Migrations-KoordinatorDienst ausführt. Verwenden Sie für die Anmeldung ein Konto mit Administratorrechten.
- 3 Navigieren Sie zu **System > Migrieren**.
- 4 Klicken Sie im Bereich **vSphere-Netzwerke migrieren** auf **Erste Schritte**.
- 5 Klicken Sie auf der Seite **Konfiguration importieren** auf **vSphere wählen** und stellen Sie die angeforderten Informationen zu Ihrer vSphere-Umgebung bereit.

Hinweis Im Dropdown-Menü für vCenter werden alle vCenter Server-Systeme angezeigt, die als Berechnungsmanager registriert sind. Klicken Sie auf **Neuen hinzufügen**, wenn Sie einen Berechnungsmanager hinzufügen müssen.

- 6 Klicken Sie auf **Start**, um die Konfiguration zu importieren.
- 7 Wenn der Import abgeschlossen ist, klicken Sie auf **Weiter**, um mit der Seite **Probleme beheben** fortzufahren.

Abbrechen oder Neustarten der vSphere-Netzwerkmigration

Auf jeder Seite der Migration steht die Schaltfläche **Abbrechen** zur Verfügung. Beim Abbrechen einer Migration werden alle Angaben zum Migrationsstatus aus dem System gelöscht.

Vorsicht Brechen Sie eine Migration nicht ab, wenn die Hostmigration gestartet wurde. Durch Abbruch der Migration wird der gesamte Migrationsstatus gelöscht und der bisherige Fortschritt kann nicht angezeigt werden.

Wenn Sie Ihre Konfiguration importiert, aber noch nicht migriert haben, können Sie auf **Abbrechen** klicken, um neu zu starten.

Wenn Sie die Konfiguration migriert haben, müssen Sie die folgenden Schritte ausführen, um die Migration neu zu starten:

- 1 Brechen Sie die Migration ab.
- 2 Stellen Sie eine neue NSX-T-Umgebung mit NSX Manager- und NSX Edge-Appliances bereit.
- 3 Starten Sie eine neue Migration.

Vorsicht In NSX-T Data Center 2.4.0 gibt es eine **Rollback**-Schaltfläche für einige der Migrationsschritte. Die Verwendung der Schaltfläche **Rollback** kann zu unerwartetem Verhalten führen. Verwenden Sie stattdessen die Schaltfläche **Abbrechen**, um die Migration beim Schritt **Konfiguration importieren** oder **Konfiguration migrieren** abubrechen.

Beheben von Problemen bei der Konfiguration des vSphere-Netzwerks

Nachdem Sie die Netzwerkkonfiguration aus Ihrer vSphere-Umgebung importiert haben, müssen Sie die gemeldeten Konfigurationsprobleme überprüfen und beheben, bevor Sie mit der Migration fortfahren können.

Sie müssen Feedback für alle Konfigurationsprobleme geben, die behoben werden müssen, bevor die Migration fortgesetzt werden kann. Das Feedback kann von mehreren Personen über mehrere Sitzungen hinweg gegeben werden. Nachdem Sie Feedback für ein bestimmtes Problem bereitgestellt haben, können Sie zum Speichern auf **Übermitteln** klicken. Sie können zu gesendetem Feedback zurückkehren und dieses ändern.

Nachdem Sie das Feedback für alle Probleme gesendet haben, wird das Feedback validiert. Die Validierung kann zusätzliche Feedback-Anforderungen nach sich ziehen, bevor die Migration fortgesetzt werden kann.

Verfahren

- 1 Klicken Sie auf der Seite **Konfigurationsfehler beheben** auf **Switch auswählen**, um den zu migrierenden vSphere Distributed Switch auszuwählen.

Nach Auswahl eines Distributed Switch werden die Konfigurationsprobleme angezeigt.

- 2 Überprüfen Sie die gemeldeten Probleme.

Probleme sind in Gruppen organisiert. Jedes Problem kann mehrere Konfigurationselemente abdecken. Für jedes Element gibt es möglicherweise eine oder mehrere Problemlösungen, wie beispielsweise Überspringen, Konfigurieren oder die Auswahl eines bestimmten Werts.

- 3 Klicken Sie auf jedes Problem und geben Sie Feedback.

Bei Problemen, die für mehrere Konfigurationselemente gelten, können Sie Feedback individuell für jedes einzelne bereitstellen, oder eine Antwort für alle Elemente eingeben.

Die Eingaben können von mehreren Benutzern über mehrere Sitzungen hinweg vorgenommen werden. Sie können zu gesendetem Feedback zurückkehren und dieses ändern.

- 4 Nachdem Feedback bereitgestellt wurde, wird die Schaltfläche **Übermitteln** auf der Seite **Probleme beheben** eingeblendet. Klicken Sie auf **Übermitteln**, um die Änderungen zu speichern.

- 5 Wenn Sie Feedback für alle Konfigurationsprobleme bereitgestellt haben, klicken Sie auf **Übermitteln**.

Die Eingaben werden überprüft. Sie werden aufgefordert, jede ungültige Eingabe zu aktualisieren. Für bestimmte Konfigurationselemente sind möglicherweise zusätzliche Eingaben erforderlich.

- 6 Nachdem Sie alles geforderte Feedback übermittelt haben, klicken Sie auf **Weiter**, um mit dem Schritt „Konfiguration migrieren“ fortzufahren.

Migrieren einer vSphere-Netzwerkconfiguration

Nachdem Sie alle Konfigurationsprobleme behoben haben, können Sie die Konfiguration des vSphere-Netzwerks migrieren. Konfigurationsänderungen werden in der NSX-T-Umgebung vorgenommen, um die übersetzte vSphere-Konfiguration zu replizieren. In vSphere werden keine Konfigurationsänderungen vorgenommen.

Vorsicht In NSX-T Data Center 2.4.0 gibt es eine **Rollback**-Schaltfläche für einige der Migrationsschritte. Die Verwendung der Schaltfläche **Rollback** kann zu unerwartetem Verhalten führen. Verwenden Sie stattdessen die Schaltfläche **Abbrechen**, um die Migration beim Schritt **Konfiguration importieren** oder **Konfiguration migrieren** abzubrechen.

Weitere Informationen hierzu finden Sie unter [Abbrechen oder Neustarten der vSphere-Netzwerkmigration](#).

Voraussetzungen

Stellen Sie sicher, dass Sie den Schritt **Konfigurationsfehler beheben** abgeschlossen haben.

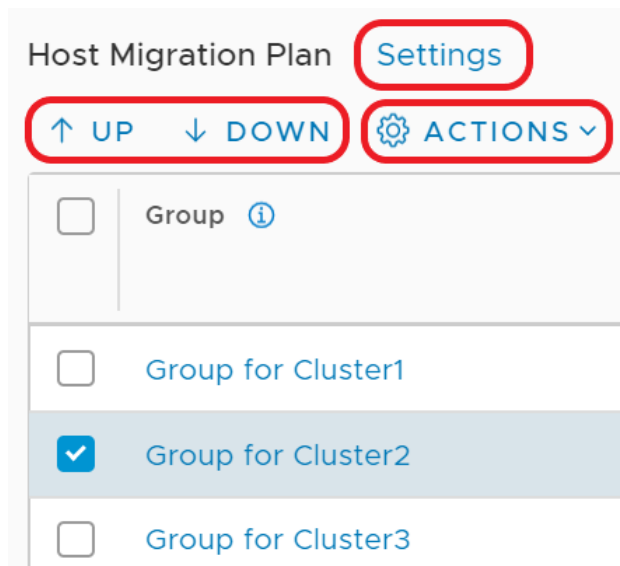
Verfahren

- ◆ Klicken Sie auf der Seite **Konfiguration migrieren** auf **Starten**.

Die Konfiguration des Distributed Switch wird auf NSX-T migriert.

Konfigurieren der Hostmigration

Die Cluster in der vSphere-Umgebung werden auf der Seite **Migrieren der Hosts** angezeigt. Die Cluster sind in Migrationsgruppen angeordnet. Jede Migrationsgruppe enthält einen vSphere-Hostcluster. Es gibt mehrere Einstellungen, die steuern, wie die Hostmigration ausgeführt wird.



- Klicken Sie auf **Einstellungen**, um die globalen Einstellungen **Pause zwischen Gruppen** und **Gruppenübergreifende Migrationsreihenfolge** zu ändern.

- Wählen Sie eine einzelne Hostgruppe (Cluster) aus und verwenden Sie die Pfeile, um diese in der Migrationsreihenfolge nach oben oder unten zu verschieben.
- Wählen Sie eine oder mehrere Hostgruppen (Cluster) aus und klicken Sie auf **Aktionen**, um diese Hostgruppeneinstellungen zu ändern: **Migrationsreihenfolge innerhalb der Gruppe** und **Migrationsstatus**.

Pause zwischen Gruppen

Pause zwischen Gruppen ist eine globale Einstellung, die für alle Hostgruppen gilt. Wenn die Pause aktiviert ist, migriert der Migrationskoordinator eine Hostgruppe und wartet dann auf eine Eingabe. Sie müssen auf **Fortfahren** klicken, um mit der nächsten Hostgruppe fortzufahren. Wenn Sie den Status jedes Clusters überprüfen möchten, bevor Sie mit dem nächsten fortfahren, aktivieren Sie **Pause zwischen Gruppen**.

Standardmäßig ist **Pause zwischen Gruppen** deaktiviert.

Serielle oder parallele Migrationsreihenfolge

Sie können festlegen, ob die Migration in einer seriellen oder parallelen Reihenfolge erfolgt. Es gibt zwei Sortiereinstellungen:

■ Gruppenübergreifende Migrationsreihenfolge

Gruppenübergreifende Migrationsreihenfolge ist eine globale Einstellung, die für alle Hostgruppen gilt.

- **Seriell:** Es wird immer jeweils eine Hostgruppe (ein Cluster) migriert.
- **Parallel:** Es werden bis zu fünf Hostgruppen gleichzeitig migriert. Nachdem diese fünf Hostgruppen migriert wurden, wird der nächste Batch mit bis zu fünf Hostgruppen migriert.

■ Migrationsreihenfolge innerhalb der Gruppe

Migrationsreihenfolge innerhalb der Gruppe ist eine spezifische Einstellung für die Hostgruppe (das Cluster) und kann daher separat für jede Hostgruppe konfiguriert werden.

- **Seriell:** Es wird immer jeweils ein Host in der Hostgruppe (Cluster) migriert.
- **Parallel:** Es werden bis zu fünf Hosts in der Hostgruppe gleichzeitig migriert. Nachdem diese fünf Hosts migriert wurden, wird der nächste Batch mit bis zu fünf Hosts migriert.

Standardmäßig sind beide Einstellungen auf **Seriell** festgelegt. Gemeinsam legen die Einstellungen fest, wie viele Hosts gleichzeitig migriert werden.

Tabelle 2-1. Auswirkungen der Migrationseinstellungen auf die Anzahl der Hosts, die gleichzeitig migriert werden

Gruppenübergreifende Migrationsreihenfolge (Cluster)	Migrationsreihenfolge innerhalb der Gruppe (Cluster)	Maximale Anzahl der Hosts, die gleichzeitig migriert werden
Seriell	Seriell	1 Ein Host aus einer Hostgruppe
Seriell	Parallel	5 Fünf Hosts aus einer Hostgruppe
Parallel	Seriell	5 Ein Host aus fünf Hostgruppen
Parallel	Parallel	25 Fünf Hosts aus fünf Hostgruppen

Wichtig Wenn ein Host nicht migriert werden kann, wird der Migrationsvorgang angehalten, nachdem alle in Bearbeitung befindlichen Hostmigrationen abgeschlossen wurden. Wenn **Parallel** für die gruppenübergreifende Migration und die Migration innerhalb von Gruppen ausgewählt ist, kann es zu einem langen Ausfall des fehlgeschlagenen Hosts kommen, bevor Sie die Migration erneut versuchen können. Wählen Sie in einer Produktionsumgebung keine parallele Migrationsreihenfolge innerhalb von Gruppen aus.

Abfolge von Migrationsgruppen

Sie können eine Hostgruppe (ein Cluster) auswählen und diese mit den Pfeilen in der Liste der Gruppen nach oben oder unten verschieben.

Wenn bei der Migration eines Hosts ein Fehler auftritt, können Sie die Hostgruppe an das Ende der Liste der Gruppen verschieben. Die Migration anderer Hostgruppen kann fortgesetzt werden, während Sie das Problem mit dem fehlgeschlagenen Host beheben.

Gruppen aktivieren oder deaktivieren

Hostgruppen (Cluster) können einen von drei Zuständen aufweisen:

■ Aktiviert

Hosts in diesen Gruppen werden zu NSX-T migriert, wenn Sie auf der Seite **Migrieren der Hosts** auf **Starten** klicken.

■ Deaktiviert

Hosts in diesen Gruppen werden nicht zu NSX-T migriert, wenn Sie auf der Seite **Migrieren der Hosts** auf **Starten** klicken. Wenn Sie jedoch für die Migration noch nicht auf **Fertigstellen** geklickt haben, können Sie zur Seite **Migrieren der Hosts** zurückkehren, um sie zu aktivieren und die Hostmigration erneut zu starten. Beenden Sie alle Hostmigrationsaufgaben und klicken Sie innerhalb desselben Wartungsfensters auf **Fertigstellen**.

■ Nicht migrieren

Hosts in diesen Gruppen wurden während des Schrittes **Konfiguration auflösen** als nicht für die Migration geeignet identifiziert.

vSphere-Hosts migrieren

Nach der Migration der Konfiguration können Sie die vSphere-Hosts auf NSX-T Data Center migrieren.

Sie können verschiedene Einstellungen in Bezug auf die Hostmigration, einschließlich der Migrationsreihenfolge oder der Aktivierung von Hosts konfigurieren. Stellen Sie vor dem Ändern von Standardeinstellungen sicher, dass Sie die Auswirkungen dieser Einstellungen verstanden haben. Weitere Informationen hierzu finden Sie unter [Konfigurieren der Hostmigration](#).

Vorsicht Während der Hostmigration kommt es zu einer Unterbrechung des Datenverkehrs. Führen Sie diesen Schritt während einer Wartungsperiode aus.

Wenn bei der Migration eines Hosts ein Fehler auftritt, stoppt die Migration, nachdem alle laufenden Hostmigrationen abgeschlossen sind. Wenn Sie das Problem mit dem Host behoben haben, klicken Sie auf **Wiederholen**, um die Migration des fehlgeschlagenen Hosts erneut zu starten.

Wenn bei der Migration eines Hosts ein Fehler auftritt, können Sie die Hostgruppe an das Ende der Liste der Gruppen verschieben. Die Migration anderer Hostgruppen kann fortgesetzt werden, während Sie das Problem mit dem fehlgeschlagenen Host beheben.

Nachdem ein Host zu NSX-T migriert wurde, wird möglicherweise ein Alarm mit der Meldung **Netzwerkverbindungsunterbrechung** angezeigt. Der Alarm tritt auf, weil der Host nicht mehr über eine physische Netzwerkkarte (NIC) verfügt, die mit dem vSphere Distributed Switch verbunden ist, mit dem zuvor eine Verbindung hergestellt wurde.

Voraussetzungen

- Stellen Sie sicher, dass alle ESXi-Hosts betriebsbereit sind. Beheben Sie alle Probleme mit Hosts, einschließlich getrennter Zustände. Für den Eintritt in den Wartungsmodus dürfen weder ausstehende Neustarts noch ausstehende Aufgaben vorhanden sein.

Hinweis Hosts werden während der Migration nicht in den Wartungsmodus versetzt.

Verfahren

- ◆ Klicken Sie auf **Starten**, um die Hostmigration zu starten.

Die vSphere-Hosts werden in Transportknoten des NSX-T-Hosts konvertiert. Die Netzwerkschnittstellen der VMs auf den Hosts werden von den Portgruppen des vSphere Distributed Switch getrennt und mit den logischen NSX-T-Segmenten verbunden.

Abschließen der Migration

Nachdem Sie alle Hosts zur NSX-T Data Center-Umgebung migriert haben, vergewissern Sie sich, dass die neue Umgebung ordnungsgemäß funktioniert. Wenn alles ordnungsgemäß funktioniert, können Sie die Migration beenden.

Wichtig Stellen Sie sicher, dass alles funktioniert, und klicken Sie im Wartungsfenster auf **Beenden**. Durch Klicken auf **Beenden** wird eine Bereinigung nach der Migration durchgeführt. Beenden Sie den Migrations-Koordinator im Migrationsfenster.

Voraussetzungen

Stellen Sie sicher, dass die NSX-T Data Center-Umgebung ordnungsgemäß funktioniert.

Verfahren

- 1 Navigieren Sie zur Seite **Hosts migrieren** des Migrations-Koordinators.
- 2 Klicken Sie auf **Fertigstellen**.

Ein Dialogfeld wird angezeigt, um die Beendigung der Migration zu bestätigen. Wenn Sie die Migration abgeschlossen haben, werden alle Migrationsdetails gelöscht. Sie können die Einstellungen dieser Migration nicht mehr überprüfen. So können Sie beispielsweise nicht mehr nachvollziehen, welche Eingaben auf der Seite **Behobene Probleme** vorgenommen wurden.