

Guide du coordinateur de migration de NSX-T Data Center

23 août 2019

VMware NSX-T Data Center 2.4



vmware®

Vous trouverez la documentation technique la plus récente sur le site Web de VMware, à l'adresse :

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

Si vous avez des commentaires à propos de cette documentation, envoyez-les à l'adresse suivante :

docfeedback@vmware.com

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

VMware France SAS.
Tour Franklin
100-101 Terrasse Boieldieu
92042 Paris La Défense 8 Cedex
France
www.vmware.com/fr

Copyright © 2019 VMware, Inc. Tous droits réservés. [Informations relatives aux copyrights et marques commerciales.](#)

Table des matières

Guide du coordinateur de migration de NSX-T Data Center 4

1 Migration de NSX Data Center for vSphere 5

- Présentation du processus de migration de NSX Data Center for vSphere 5
 - Fonctionnalités prises en charge par le coordinateur de migration 5
 - Topologies prises en charge par le coordinateur de migration 28
 - Limites prises en charge par le coordinateur de migration 36
 - Présentation de la migration à l'aide du coordinateur de migration 38
 - Déploiement de machine virtuelle pendant la migration 39
- Préparation de la migration d'un environnement NSX Data Center for vSphere 40
 - Préparer l'environnement NSX-T Data Center 40
 - Préparer la migration d'un environnement NSX Data Center for vSphere 48
- Migration de NSX Data Center for vSphere vers NSX-T Data Center 52
 - Importer la configuration de NSX Data Center for vSphere 52
 - Annuler ou redémarrer la migration de NSX for vSphere 53
 - Résoudre les problèmes de configuration et déployer des nœuds Edge 54
 - Migrer la configuration de NSX Data Center for vSphere 61
 - Modifier la configuration du dispositif Edge avant la migration des dispositifs Edge 62
 - Migrer les dispositifs Edge NSX Data Center for vSphere 63
 - Configuration de la migration d'hôtes 63
 - Terminer la migration NSX Data Center for vSphere 68
- Désinstallation de NSX for vSphere après la migration 68
- Dépannage de la migration NSX Data Center for vSphere 71

2 Migration de la mise en réseau vSphere 75

- Présentation de la migration de la Mise en réseau vSphere 75
- Préparation de la migration de la Mise en réseau vSphere 76
 - Ajouter un gestionnaire de calcul 76
- Migrer la mise en réseau vSphere vers NSX-T Data Center 77
 - Importer la configuration de la mise en réseau vSphere 77
 - Annuler ou redémarrer la migration de la mise en réseau vSphere 78
 - Résoudre les problèmes de la configuration de la Mise en réseau vSphere 79
 - Migrer la configuration de la mise en réseau vSphere 79
 - Configuration de la migration d'hôte 80
 - Terminer la migration 83

Guide du coordinateur de migration de NSX-T Data Center

Le *Guide du coordinateur de migration de NSX-T Data Center* fournit des informations sur la migration d'un environnement VMware NSX[®] for vSphere[®] vers un environnement VMware NSX-T[™] à l'aide du coordinateur de migration.

Il inclut également des informations sur la migration des configurations de mise en réseau de VMware vSphere[®] vers un environnement NSX-T Data Center à l'aide du coordinateur de migration.

Public visé

Ce manuel est destiné à toute personne qui souhaite utiliser le coordinateur de migration pour migrer un environnement NSX Data Center for vSphere ou une mise en réseau vSphere vers un environnement NSX-T Data Center. Les informations sont destinées à des administrateurs réseau et système expérimentés, qui connaissent bien les technologies de machine virtuelle et les opérations de centre de données.

Migration de NSX Data Center for vSphere

1

Vous pouvez utiliser le coordinateur de migration pour migrer NSX Data Center d'un environnement NSX for vSphere existant vers un environnement NSX-T vide.

Important La migration entraîne des interruptions de trafic au cours des étapes de migration d'instances Edge et d'hôtes. Vous devez effectuer la migration dans une fenêtre de maintenance unique. Contactez l'équipe du support VMware avant de lancer la migration.

Ce chapitre contient les rubriques suivantes :

- [Présentation du processus de migration de NSX Data Center for vSphere](#)
- [Préparation de la migration d'un environnement NSX Data Center for vSphere](#)
- [Migration de NSX Data Center for vSphere vers NSX-T Data Center](#)
- [Désinstallation de NSX for vSphere après la migration](#)
- [Dépannage de la migration NSX Data Center for vSphere](#)

Présentation du processus de migration de NSX Data Center for vSphere

La migration de NSX for vSphere vers NSX-T requiert planification et préparation. Vous devez connaître les concepts et les tâches d'administration de NSX-T avant d'entreprendre une migration.

La préparation peut impliquer la modification de votre environnement NSX for vSphere existant en plus de la configuration du nouvel environnement NSX-T.

Fonctionnalités prises en charge par le coordinateur de migration

Un sous-ensemble de fonctionnalités de NSX Data Center for vSphere sont prises en charge par le coordinateur de migration.

La plupart des fonctionnalités présentent certaines limitations. Si vous importez votre configuration NSX Data Center for vSphere vers le coordinateur de migration, vous obtenez des informations détaillées sur les fonctionnalités et les configurations de votre environnement qui sont prises en charge et qui ne le sont pas.

Reportez-vous à la section [Prise en charge détaillée des fonctionnalités du coordinateur de migration](#) pour obtenir des informations détaillées sur les éléments pris en charge par le coordinateur de migration.

Tableau 1-1. Matrice de prise en charge du coordinateur de migration

Fonctionnalité de NSX Data Center for vSphere	Pris en charge	Détails et limitations
Commutateurs logiques supportés par VLAN	Oui	
Commutateurs logiques supportés par la superposition	Oui	
Ponts L2	Non	
Zones de transport	Oui	
Routage	Oui	Reportez-vous à Topologies prises en charge par le coordinateur de migration pour plus de détails.
Microsegmentation horizontale	Oui	
Edge Firewall	Oui	
NAT	Oui	
VPN de couche 2	Oui	
VPN L3	Oui	
Équilibrage de charge	Oui	
DHCP et DNS	Oui	
Pare-feu distribué	Oui	
Service Composer	Oui	Seules les règles de pare-feu sont migrées. Les règles Guest Introspection et les règles d'introspection du réseau ne sont pas migrées.
Regroupement des objets	Oui	Les limitations incluent le nombre d'éléments, et des expressions dynamiques composant des groupes de sécurité.
Guest Introspection	Non	
Introspection réseau	Non	
Protection du point de terminaison	Non	
Cross-vCenter NSX	Non	
NSX Data Center for vSphere avec une plate-forme de gestion du cloud, une solution Stack intégrée ou une solution PaaS.	Non	Contactez votre représentant VMware avant de passer à la migration. La migration peut rompre les scripts et les intégrations.

Prise en charge détaillée des fonctionnalités du coordinateur de migration

Prise en charge de plate-forme

Consultez la matrice d'interopérabilité VMware pour voir les versions prises en charge d'ESXi et de vCenter Server : http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php#interop&175=&1=&2=.

Configuration	Pris en charge	Détails
Configuration pré-existante de NSX-T	Non	Déployez un nouvel environnement NSX-T en tant que destination pour la migration de NSX for vSphere. Pendant l'étape Importer une configuration , toutes les interfaces de nœud Edge dans l'environnement NSX-T de destination sont arrêtées. Si l'environnement NSX-T de destination est déjà configuré et est en cours d'utilisation, le démarrage de l'importation de la configuration entraînera l'interruption du trafic.
Cross-vCenter NSX	Non	
NSX for vSphere avec vSAN ou iSCSI sur vSphere Distributed Switch	Non	
NSX for vSphere avec une plate-forme de gestion du cloud, une solution Stack intégrée ou une solution PaaS	Non	Contactez votre représentant VMware avant de passer à la migration. La migration peut rompre les scripts et les intégrations. Par exemple : <ul style="list-style-type: none"> ■ NSX for vSphere et vRealize Automation ■ NSX for vSphere et VMware Integrated OpenStack ■ NSX for vSphere et vCloud Director ■ NSX for vSphere avec solution Stack intégrée ■ NSX for vSphere avec une solution PaaS, telle que Pivotal Cloud Foundry, RedHat OpenShift ■ NSX for vSphere avec des workflows vRealize Operations

Fonctionnalités de vSphere et d'ESXi

Configuration	Pris en charge	Détails
Commutateur standard vSphere	Non	Les machines virtuelles et les interfaces VMKernel sur un VSS ne sont pas migrées. Les fonctionnalités de NSX for vSphere appliquées au VSS ne peuvent pas être migrées.
ESXi sans état	Non	

Configuration	Pris en charge	Détails
Profils d'hôte	Non	
Mode de verrouillage ESXi	Non	Non pris en charge dans NSX-T.
Hôte ESXi en attente de la tâche en mode de maintenance.	Non	
Hôte ESXi déjà en mode de maintenance (aucune VM)	Oui	
Hôte ESXi déconnecté dans le cluster vCenter	Non	
vSphere Distributed Switch avec la stratégie d'association LACP	Oui	La fonctionnalité PortFast d'arborescence doit être activée sur le commutateur physique
FT vSphere	Non	
vSphere DRS entièrement automatisé	Non	Mettre DRS en mode manuel avant d'exécuter le coordinateur de migration
vSphere High Availability	Non	
ACL de filtrage du trafic	Non	
Network I/O Control (NIOC) version 2	Non	
Network I/O Control (NIOC) version 3	Oui	
Network I/O Control (NIOC) avec vNIC avec réservation	Non	
Contrôle de santé vSphere	Non	
SRIOV	Non	
Épinglage de vmknic à la carte réseau physique	Non	
VLAN privé	Non	
dvPortGroup éphémère	Non	
E/S DirectPath	Non	
Sécurité L2	Non	
Apprendre le commutateur sur le câble virtuel	Non	
Passerelle matérielle (intégration du point de terminaison de tunnel avec le matériel de commutation physique)	Non	
SNMP	Non	
vNIC déconnecté dans la VM	Non	En raison de la limitation d'ESX 6.5, des entrées périmées peuvent être présentes sur DVFilter pour les VM déconnectées. Comme solution, redémarrez la VM.

Configuration	Pris en charge	Détails
Numéro de port VXLAN autre que 4789	Non	
Mode de filtrage multidiffusion	Non	

Configuration système du dispositif NSX Manager

Configuration	Pris en charge	Détails
FIPS	Non	Activation/désactivation de FIPS non prise en charge par NSX-T.
Paramètre régional	Non	NSX-T ne prend en charge que les paramètres régionaux anglais
Certificat du dispositif	Non	
Paramètre de serveur/heure NTP	Oui	
Configuration du serveur Syslog	Oui	
Configuration de sauvegarde	Oui	<p>Si nécessaire, modifiez la phrase secrète de NSX Data Center for vSphere pour respecter les exigences de NSX-T Data Center. Elle doit comporter au moins 8 caractères et contenir les éléments suivants :</p> <ul style="list-style-type: none"> ■ Au moins une lettre minuscule ■ Au moins une lettre majuscule ■ Au moins un caractère numérique ■ Au moins un caractère spécial

Contrôle d'accès basé sur les rôles

Configuration	Pris en charge	Détails
Utilisateurs locaux	Non	
Rôles NSX attribués à un utilisateur vCenter ajouté via LDAP	Oui	vSphere Identity Manager doit être installé et configuré pour migrer des rôles d'utilisateur pour les utilisateurs LDAP.
Rôles NSX attribués à un groupe vCenter	Non	

Certificats

Configuration	Pris en charge	Détails
Certificats (serveur, signés par une autorité de certification)	Oui	Cela s'applique aux certificats ajoutés via des API de magasin d'approbations uniquement.

Opérations

Détails	Pris en charge	Remarques
CDP de protocole de découverte	Non	
LLDP de protocole de découverte	Oui	Le mode d'écoute est activé par défaut et ne peut pas être modifié dans NSX-T. Seul le mode Annonce peut être modifié.
PortMirroring : ■ Source de mise en miroir distante encapsulée (L3)	Oui	Seul le type de session L3 est pris en charge pour la migration
PortMirroring : ■ PortMirroring distribué ■ Source de mise en miroir distante ■ Destination de mise en miroir distante ■ Mise en miroir de port distribué (héritage)	Non	
IPFIX L2	Oui	Lag with IPFIX n'est pas pris en charge
IPFIX du Pare-feu distribué	Non	
Apprentissage MAC	Oui	Vous devez activer (accepter) les transmissions forgées.
VTEP matériel	Non	
Mode promiscuité	Non	
Allocation des ressources	Non	VmVnic activé avec l'allocation de ressources n'est pas pris en charge
IpFix – Flux internes	Non	IpFix avec flux internes n'est pas pris en charge

Commutateur

Configuration	Pris en charge	Détails
Pontage L2	Non	
VLAN de jonction	Oui	Des groupes de port de liaison montante de jonction doivent être configurés avec une plage VLAN comprise entre 0 et 4094.
Configuration VLAN	Oui	Seule la configuration Lag with VLAN n'est pas prise en charge

Configuration	Pris en charge	Détails
Association et basculement : <ul style="list-style-type: none"> ■ Équilibrage de charge ■ Ordre de basculement de liaison montante 	Oui	Options prises en charge pour l'équilibrage de charge (stratégie d'association) : <ul style="list-style-type: none"> ■ Utiliser la commande de basculement explicite ■ Route basée sur le hachage MAC source Les autres options d'équilibrage de charge ne sont pas prises en charge.
Association et basculement : <ul style="list-style-type: none"> ■ Détection de panne réseau ■ Notifier les commutateurs ■ Stratégie inverse ■ Ordre de restauration 	Non	

Sécurité des commutateurs et découverte d'adresses IP

Configuration	Pris en charge	Détails
Découverte d'adresses IP (ARP, ND, DHCPv4 et DHCPv6)	Oui	Les limites de liaison suivantes s'appliquent sur NSX-T pour la migration : <ul style="list-style-type: none"> ■ 128 pour les adresses IP découvertes par ARP ■ 128 pour les adresses IP découvertes par DHCPv4 ■ 15 pour les adresses IP découvertes par DHCPv6 ■ 15 pour les adresses IP découvertes par ND
SpoofGuard (manuel, TOFU, désactivé)	Oui	
Sécurité des commutateurs (filtre BPDU, bloc de client DHCP, bloc de serveur DHCP, Protection contre les annonces du routeur)	Oui	
Migration des liaisons de chemin de données à partir du module Sécurité des commutateurs dans NSX for vSphere vers le module Sécurité des commutateurs dans NSX-T	Oui	Si SpoofGuard est activé, les liaisons sont migrées à partir du module Sécurité des commutateurs pour prendre en charge la suppression ARP. VSIP : la sécurité du commutateur n'est pas prise en charge, car les liaisons VSIP sont migrées en tant que règles configurées de manière statique.
Profils de découverte	Oui	Les profils ipdiscovery sont créés après la migration à l'aide de la configuration de découverte d'adresses IP pour le commutateur logique et de la configuration ARP et DHCP globale et de cluster.

Plan de contrôle central

Configuration	Pris en charge	Détails
Réplication VTEP par commutateur logique (VNI) et domaine de routage	Oui	
Réplication MAC/IP	Non	
Zones de transport NSX for vSphere utilisant le mode de réplication multidiffusion ou hybride	Non	
Zones de transport NSX for vSphere utilisant le mode de réplication monodiffusion	Oui	

Fonctionnalités NSX Edge

Pour obtenir des informations complètes sur les topologies prises en charge, reportez-vous à la section [Topologies prises en charge par le coordinateur de migration](#).

Configuration	Pris en charge	Détails
Routage entre la passerelle Edge Service Gateway et le routeur ascendant ou l'interface de tunnel virtuel	Oui	BGP est pris en charge. Les routes statiques sont prises en charge. OSFP n'est pas pris en charge.
Routage entre la passerelle Edge Services Gateway et le routeur logique distribué	Oui	Les routes sont converties en routes statiques après la migration.
Équilibrage de charge	Oui	Reportez-vous à la section Topologies prises en charge par le coordinateur de migration pour plus de détails.
Environnement de microsegmentation supporté par VLAN	Oui	Reportez-vous à la section Topologies prises en charge par le coordinateur de migration pour plus de détails.
NAT64	Non	Non pris en charge dans NSX-T.
Paramètres de niveau de nœud sur la passerelle Edge Services Gateway ou le routeur logique distribué	Non	Les paramètres de niveau de nœud, par exemple, serveur Syslog ou NTP, ne sont pas pris en charge.
IPv6	Non	
Configuration du filtre de chemin inverse de monodiffusion (URPF) pour les interfaces de la passerelle Edge Services Gateway	Non	URPF sur les interfaces de passerelle NSX-T est défini sur Strict.
Interfaces de la passerelle Edge Services Gateway de configuration de l'unité de transmission maximale (MTU)	Non	Reportez-vous à Modifier la configuration du dispositif Edge avant la migration des dispositifs Edge pour plus d'informations sur la modification de la MTU par défaut sur NSX-T.
Routage de multidiffusion IP	Non	

Configuration	Pris en charge	Détails
Filtres de préfixe de redistribution de routes	Non	
Provenance par défaut	Non	Non pris en charge dans NSX-T.

Edge Firewall

Configuration	Pris en charge	Détails
Section de pare-feu : nom complet	Oui	Les sections de pare-feu peuvent contenir un maximum de 1 000 règles. Si une section contient plus de 1 000 règles, elle est migrée sous forme de plusieurs sections.
Action pour la règle par défaut	Oui	API NSX for vSphere : GatewayPolicy/action API NSX-T : SecurityPolicy.action
Configuration globale de pare-feu	Non	Des délais d'expiration par défaut sont utilisés
Règle de pare-feu	Oui	API NSX for vSphere : firewallRule API NSX-T : SecurityPolicy
Règle de pare-feu : nom	Oui	
Règle de pare-feu : balise de règle	Oui	API NSX for vSphere : ruleTag API NSX-T : Rule_tag
Sources et destinations dans les règles de pare-feu : <ul style="list-style-type: none"> ■ Regroupement des objets ■ Adresses IP 	Oui	API NSX for vSphere : <ul style="list-style-type: none"> ■ source/groupingObjectId ■ source/ipAddress API NSX-T : <ul style="list-style-type: none"> ■ source_groups API NSX for vSphere : <ul style="list-style-type: none"> ■ destination/groupingObjectId ■ destination/ipAddress API NSX-T : <ul style="list-style-type: none"> ■ destination_groups
Sources et destinations de règles de pare-feu : <ul style="list-style-type: none"> ■ Groupe de vNIC 	Non	
Services (applications) dans les règles de pare-feu : <ul style="list-style-type: none"> ■ Service ■ Groupe de service ■ Protocole/port/port source 	Oui	API NSX for vSphere : <ul style="list-style-type: none"> ■ application/applicationId ■ application/service/protocol ■ application/service/port ■ application/service/sourcePort API NSX-T : <ul style="list-style-type: none"> ■ Services
Règle de pare-feu : correspondance traduite	Non	La correspondance traduite doit être « false ».

Configuration	Pris en charge	Détails
Règle de pare-feu : direction	Oui	Les deux API : direction
Règle de pare-feu : action	Oui	Les deux API : action
Règle de pare-feu : activé	Oui	Les deux API : activé
Règle de pare-feu : journalisation	Oui	API NSX for vSphere : journalisation API NSX-T : journalisée
Règle de pare-feu : description	Oui	Les deux API : description

NAT Edge

Configuration	Pris en charge	Détails
Règle NAT	Oui	API NSX for vSphere : natRule API NSX-T : /nat/USER/nat-rules
Règle NAT : balise de règle	Oui	API NSX for vSphere : ruleTag API NSX-T : rule_tag
Règle NAT : action	Oui	API NSX for vSphere : action API NSX-T : action
Règle NAT : adresse d'origine (adresse source pour les règles SNAT et adresse de destination pour les règles DNAT.)	Oui	API NSX for vSphere : originalAddress API NSX-T : source_network pour règle SNAT ou destination_network pour règle DNAT
Règle NAT : translatedAddress	Oui	API NSX for vSphere : translatedAddress API NSX-T : translated_network
Règle NAT : application d'une règle NAT sur une interface spécifique	Non	Appliqué à doit être « any ».
Règle NAT : journalisation	Oui	API NSX for vSphere : loggingEnabled API NSX-T : journalisation
Règle NAT : activé	Oui	API NSX for vSphere : activé API NSX-T : désactivé
Règle NAT : description	Oui	API NSX for vSphere : description API NSX-T : description
Règle NAT : protocole	Oui	API NSX for vSphere : protocole API NSX-T : service
Règle NAT : port d'origine (port source pour les règles SNAT, port de destination pour les règles DNAT)	Oui	API NSX for vSphere : originalPort API NSX-T : service
Règle NAT : port traduit	Oui	API NSX for vSphere : translatedPort API NSX-T : Translated_ports
Règle NAT : adresse source dans la règle DNAT	Oui	API NSX for vSphere : dnatMatchSourceAddress API NSX-T : source_network

Configuration	Pris en charge	Détails
Règle NAT : adresse de destination dans la règle SNAT	Oui	API NSX for vSphere : snatMatchDestinationAddress API NSX-T : destination_network
Règle NAT : port source dans la règle DNAT	Oui	API NSX for vSphere : dnatMatchSourcePort API NSX-T : service
Règle NAT : port de destination dans la règle SNAT	Oui	API NSX for vSphere : snatMatchDestinationPort API NSX-T : service
Règle NAT : ID de règle	Oui	API NSX for vSphere : ruleID API NSX-T : id et display_name

VPN L2

Configuration	Pris en charge	Détails
Configuration L2VPN basée sur IPSec à l'aide d'une clé prépartagée (PSK)	Oui	Pris en charge si la mise en réseau en cours d'étirement sur L2VPN est un commutateur logique de superposition. Non pris en charge pour les réseaux VLAN.
Configuration L2VPN basée sur IPSec à l'aide de l'authentification basée sur un certificat	Non	
Configuration L2VPN basée sur SSL	Non	
Configurations L2VPN avec optimisations de sortie locale	Non	
Mode client L2VPN	Non	

L3VPN

Configuration	Pris en charge	Détails
Dead Peer Detection	Oui	Dead Peer Detection prend en charge différentes options sur NSX for vSphere et NSX-T. Vous pouvez envisager d'utiliser BGP pour une convergence plus rapide ou de configurer un homologue pour qu'il exécute DPD s'il est pris en charge.
Valeurs par défaut de Dead Peer Detection (DPD) modifiées pour : <ul style="list-style-type: none"> ■ dpdtimeout ■ dpdaction 	Non	Dans NSX-T, dpdaction est défini sur « restart » et ne peut pas être modifié. Si le paramètre de NSX for vSphere pour dpdtimeout est défini sur 0, DPD est désactivé dans NSX-T. Dans le cas contraire, tous les paramètres dpdtimeout sont ignorés et la valeur par défaut est utilisée.

Configuration	Pris en charge	Détails
Valeurs par défaut de Dead Peer Detection (DPD) modifiées pour : ■ dpdelay	Oui	dpdelay de NSX for vSphere correspond à dpdinternal de NSX-T.
Chevauchement de sous-réseaux locaux et homologues de deux sessions ou plus.	Non	NSX for vSphere prend en charge les sessions de VPN IPSec basé sur les stratégies dans lequel les sous-réseaux locaux et homologues de deux ou plusieurs sessions se chevauchent mutuellement. Ce comportement n'est pas pris en charge sur NSX-T. Vous devez reconfigurer les sous-réseaux afin qu'ils ne se chevauchent pas avant de commencer la migration. Si ce problème de configuration n'est pas résolu, l'étape Migrer la configuration échoue.
Sessions IPSec dont le point de terminaison homologue est défini sur any.	Non	La configuration n'est pas migrée.
Modifications apportées à l'extension securelocaltrafficbyip.	Non	Le routeur de service NSX-T ne dispose pas de trafic généré localement qui doit être envoyé sur le tunnel.
Modifications apportées à ces extensions : auto, sha2_truncbug, sarefrack, leftid, leftsendcert, leftxauthserver, leftxauthclient, leftxauthusername, leftmodecfgserver, leftmodecfgclient, modecfgpull, modecfgdns1, modecfgdns2, modecfgwins1, modecfgwins2, remote_peer_type, nm_configured, forceencaps,overlapip, aggrmode, rekey, rekeymargin, rekeyfuzz, compress, metric,disablearrivalcheck, failureshunt,leftnexthop, keyingtries	Non	Ces extensions ne sont pas prises en charge sur NSX-T et les modifications apportées ne sont pas migrées.

Équilibrage de charge

Configuration	Pris en charge	Détails
Moniteur/contrôles de santé pour : ■ LDAP ■ DNS ■ MSSQL	Non	Si un moniteur non pris en charge est configuré, il est ignoré et aucun moniteur n'est configuré sur le pool associé. Vous pouvez l'attacher à un nouveau moniteur après la migration.
Règles d'application	Non	NSX for vSphere utilise des règles d'application basées sur HAProxy pour prendre en charge L7. Dans NSX-T, les règles sont basées sur NGINX. Les règles d'application ne peuvent pas être migrées. Vous devez créer des règles après la migration.

Configuration	Pris en charge	Détails
Plage de ports du serveur virtuel L7	Non	
IPv6	Non	Si IPv6 est utilisé dans le serveur virtuel, l'intégralité du serveur virtuel est ignorée. Si IPv6 est utilisé dans le pool, le pool serait toujours migré, mais le membre du pool associé serait supprimé.
Algorithmes URL, URI, HTTPHEADER	Non	S'il est utilisé dans un pool, le pool n'est pas migré.
Pool isolé	Non	Le pool n'est pas migré.
Membre du pool d'équilibrage de charge avec un port de moniteur différent	Non	Le membre du pool qui a un port de moniteur différent n'est pas migré.
MinConn de membres du pool	Non	La configuration n'est pas migrée.
Extension de moniteur	Non	La configuration n'est pas migrée.
Persistence des ID de session SSL/table	Non	La configuration n'est pas migrée et le serveur virtuel associé n'a pas de paramètre de persistance.
Persistence MSRDP/table de session	Non	La configuration n'est pas migrée et le serveur virtuel associé n'a pas de paramètre de persistance.
Session d'application de cookie/table de session	Non	La configuration n'est pas migrée et le serveur virtuel associé n'a pas de paramètre de persistance.
Persistence d'application	Non	La configuration n'est pas migrée et le serveur virtuel associé n'a pas de paramètre de persistance.
Surveiller pour : <ul style="list-style-type: none"> ■ Caractère d'échappement explicite ■ Quitter ■ Retard 	Non	
Surveiller pour : <ul style="list-style-type: none"> ■ Envoyer ■ Attendre ■ Délai d'expiration ■ Intervalle ■ maxRetries 	Oui	
Réglage de Haproxy/IPVS	Non	
Filtre d'adresse IP du pool <ul style="list-style-type: none"> ■ Adresses IPv4 	Oui	Les adresses IP IPv4 sont prises en charge. Si Any est utilisé, seules les adresses IPv4 du pool d'adresses IP sont migrées.

Configuration	Pris en charge	Détails
Filtre d'adresse IP du pool ■ Adresses IPv6	Non	
Pool contenant un objet de regroupement non pris en charge : ■ Cluster ■ Centre de données ■ Groupe de ports distribués ■ Ensembles d'adresses MAC ■ Application virtuelle	Non	Si un pool inclut un objet de regroupement non pris en charge, ces objets sont ignorés et le pool est créé avec des membres d'objets de regroupement pris en charge. Si aucun membre d'objet de regroupement n'est pris en charge, un pool vide est créé.

DHCP et DNS

Tableau 1-2. Topologies de configuration DHCP

Configuration	Pris en charge	Détails
Relais DHCP configuré sur un routeur logique distribué pointant vers un serveur DHCP configuré sur une passerelle Edge Services Gateway directement connectée	Oui	L'adresse IP du serveur de relais DHCP doit être l'une des adresses IP de l'interface interne de la passerelle Edge Services Gateway. Le serveur DHCP doit être configuré sur une passerelle Edge Services Gateway qui est directement connectée au routeur logique distribué configuré avec le relais DHCP. L'utilisation de DNAT n'est pas prise en charge pour traduire une adresse IP de relais DHCP qui ne correspond pas à une interface interne de la passerelle Edge Services Gateway.
Relais DHCP configuré sur le routeur logique distribué uniquement, aucune configuration de serveur DHCP sur la passerelle Edge Services Gateway connectée	Non	
Serveur DHCP configuré sur la passerelle Edge Services Gateway uniquement, aucune configuration de relais DHCP sur le routeur logique distribué connecté	Non	

Tableau 1-3. Fonctionnalités de DHCP

Configuration	Pris en charge	Détails
Pools d'adresses IP	Oui	
Liaisons statiques	Oui	
Baux DHCP	Oui	
Options de DHCP générales	Oui	

Tableau 1-3. Fonctionnalités de DHCP (suite)

Configuration	Pris en charge	Détails
Service DHCP désactivé	Non	Dans NSX-T, vous ne pouvez pas désactiver le service DHCP. Si un service DHCP est désactivé sur NSX for vSphere, il n'est pas migré.
Option DHCP : « autre »	Non	Le champ « autre » des options DHCP n'est pas pris en charge pour la migration. Par exemple, l'option DHCP « 80 » n'est pas migrée. <pre><dhcpOptions> <other> <code>80</code> <value>2f766172</value> </other> </dhcpOptions></pre>
Pools d'adresses IP/liaisons orphelins	Non	Si des pools d'adresses IP ou des liaisons statiques sont configurés sur un serveur DHCP, mais ne sont utilisés par aucun commutateur logique connecté, ces objets sont ignorés lors de la migration.
DHCP configuré sur la passerelle Edge Service Gateway avec des commutateurs logiques connectés directement	Non	Pendant la migration, les interfaces de la passerelle Edge Service Gateway directement connectée sont migrées en tant que ports de service centralisés. Toutefois, NSX-T ne prend pas en charge le service DHCP sur un port de service centralisé, donc la configuration du service DHCP n'est pas migrée pour ces interfaces.

Tableau 1-4. Fonctionnalités de DNS

Configuration	Pris en charge	Détails
Vues de DNS	Oui	Seul le premier dnsView est migré vers la zone du redirecteur DNS par défaut de NSX-T.
Configuration de DNS	Oui	Vous devez fournir les adresses IP de l'écouteur DNS disponibles pour tous les nœuds Edge. Un message vous y invitant s'affiche lors de la résolution de la configuration.

Tableau 1-4. Fonctionnalités de DNS (suite)

Configuration	Pris en charge	Détails
DNS : VPN L3	Oui	Vous devez ajouter les adresses IP de l'écouteur DNS NSX-T récemment configurées dans la liste de préfixes de VPN L3 distants. Un message vous y invitant s'affiche lors de la résolution de la configuration.
DNS configuré sur la passerelle Edge Service Gateway avec des commutateurs logiques connectés directement	Non	Pendant la migration, les interfaces de la passerelle Edge Service Gateway directement connectée sont migrées en tant que ports de service centralisés. Toutefois, NSX-T ne prend pas en charge le service DNS sur un port de service centralisé, donc la configuration du service DNS n'est pas migrée pour ces interfaces.

Pare-feu distribué

Configuration	Pris en charge	Détails
Pare-feu basé sur l'identité	Non	
Section - <ul style="list-style-type: none"> ■ Nom complet ■ Description ■ Tcp_strict ■ Sans état 	Oui	Si une section de pare-feu comporte plus de 1 000 règles, l'outil de migration migre les règles dans plusieurs sections de 1 000 règles chacune.
Sections universelles	Non	
Règle : source/destination : <ul style="list-style-type: none"> ■ Adresse IP/Plage/CIDR ■ Port logique ■ Commutateur logique 	Oui	
Règle : source/destination : <ul style="list-style-type: none"> ■ Machine virtuelle ■ Port logique ■ Groupe de sécurité/ensemble d'adresses IP/ensemble d'adresses MAC 	Oui	correspond à NSGroup
Règle : source/destination : <ul style="list-style-type: none"> ■ Cluster ■ Centre de données ■ DVPG ■ vSS ■ Hôte ■ Commutateur logique universel 	Non	

Configuration	Pris en charge	Détails
Règle : Appliqué à : ■ ANY	Oui	correspond à Pare-feu distribué
Règle : Appliqué à : ■ Groupe de sécurité ■ Port logique ■ Commutateur logique ■ Machine virtuelle	Oui	correspond à NSGroup
Règle : Appliqué à : ■ Cluster ■ Centre de données ■ DVPG ■ vSS ■ Hôte ■ Commutateur logique universel	Non	
Règles désactivées dans le pare-feu distribué	Oui	
Désactivation du pare-feu distribué au niveau du cluster	Non	Lorsque le pare-feu distribué est activé sur NSX-T, il est activé sur tous les clusters. Vous ne pouvez pas l'activer sur certains clusters et le désactiver sur d'autres.

Objets de regroupement et Service Composer

Les ensembles d'adresses IP et d'adresses MAC sont migrés vers NSX-T Data Center sous forme de groupes. Consultez **Inventaire > Groupes** dans l'interface Web de NSX-T Manager.

Tableau 1-5. Ensembles d'adresses IP et d'adresses MAC

Configuration	Pris en charge	Détails
Ensembles d'adresses IP	Oui	Les ensembles d'adresses IP comportant jusqu'à 2 millions de membres (adresses IP, sous-réseaux d'adresses IP et plages d'adresses IP) peuvent être migrés. Les ensembles d'adresses IP avec plus de membres ne sont pas migrés.
Ensembles d'adresses MAC	Oui	Les ensembles d'adresses MAC comportant jusqu'à 2 millions de membres peuvent être migrés. Les ensembles d'adresses MAC avec plus de membres ne sont pas migrés.

Les groupes de sécurité sont pris en charge pour la migration avec les limites répertoriées. Les groupes de sécurité sont migrés vers NSX-T Data Center sous forme de groupes. Consultez **Inventaire > Groupes** dans l'interface Web de NSX-T Manager.

NSX for vSphere dispose de groupes de sécurité définis par l'utilisateur et définis par le système. Ils sont tous migrés vers NSX-T sous forme de groupes définis par l'utilisateur.

Le nombre total de « Groupes » après la migration peut ne pas être égal au nombre de groupes de sécurité sur NSX for vSphere. Par exemple, une règle de pare-feu distribué contenant une machine virtuelle comme source serait migrée vers une règle contenant un nouveau groupe avec la machine virtuelle comme membre. Cela augmente le nombre total de groupes sur NSX-T après la migration.

Tableau 1-6. Groupes de sécurité

Configuration	Pris en charge	Détails
Groupe de sécurité avec des membres qui n'existent pas	Non	Si l'un des membres du groupe de sécurité n'existe pas, le groupe de sécurité n'est pas migré.
Groupe de sécurité qui contient un groupe de sécurité avec des membres non pris en charge	Non	Si des membres du groupe de sécurité ne sont pas pris en charge pour la migration, le groupe de sécurité n'est pas migré. Si un groupe de sécurité contient un groupe de sécurité dont des membres ne sont pas pris en charge, le groupe de sécurité parent n'est pas migré.
Exclure l'appartenance au groupe de sécurité	Non	Les groupes de sécurité avec un membre exclu directement ou indirectement (via l'imbrication) ne sont pas migrés
Adhésion statique au groupe de sécurité	Oui	Un groupe de sécurité peut contenir jusqu'à 500 membres statiques. Toutefois, les membres statiques générés par le système sont ajoutés si le groupe de sécurité est utilisé dans des règles de pare-feu distribué, diminuant ainsi la limite effective à 499 ou 498. <ul style="list-style-type: none"> ■ Si le groupe de sécurité est utilisé dans des règles de couche 2 ou de couche 3, un membre statique généré par le système est ajouté au groupe de sécurité. ■ Si le groupe de sécurité est utilisé dans des règles de couche 2 et de couche 3, deux membres statiques générés par le système sont ajoutés. Si des membres n'existent pas au cours de l'étape de résolution de la configuration, le groupe de sécurité n'est pas migré.

Tableau 1-6. Groupes de sécurité (suite)

Configuration	Pris en charge	Détails
Types de membres du groupe de sécurité (Statique ou Entité appartient à) : <ul style="list-style-type: none"> ■ Cluster ■ Centre de données ■ Groupe d'annuaires ■ Groupe de ports distribués ■ Groupe de ports hérité/réseau ■ Pool de ressources ■ vApp 	Non	Si un groupe de sécurité contient l'un des types de membres non pris en charge, le groupe de sécurité n'est pas migré.
Types de membres du groupe de sécurité (Statique ou Entité appartient à) : <ul style="list-style-type: none"> ■ Groupe de sécurité ■ Ensembles d'adresses IP ■ Ensembles d'adresses MAC 	Oui	<p>Les groupes de sécurité, les ensembles d'adresses IP et les ensembles d'adresses MAC sont migrés vers NSX-T sous forme de groupes. Si un groupe de sécurité NSX for vSphere contient un ensemble d'adresses IP, un ensemble d'adresses MAC ou un groupe de sécurité imbriqué comme membre statique, les groupes correspondants sont ajoutés au groupe parent.</p> <p>Si l'un de ces membres statiques n'a pas été migré vers NSX-T, le groupe de sécurité parent ne migre pas vers NSX-T. Par exemple, un ensemble d'adresses IP contenant plus de 2 millions de membres ne peut pas migrer vers NSX-T. Par conséquent, un groupe de sécurité contenant un ensemble d'adresses IP contenant plus de 2 millions de membres ne peut pas migrer.</p>
Types de membres du groupe de sécurité (Statique ou Entité appartient à) : <ul style="list-style-type: none"> ■ Commutateur logique (câble virtuel) 	Oui	Si un groupe de sécurité contient des commutateurs logiques qui ne migrent pas vers des segments NSX-T, le groupe de sécurité ne migre pas vers NSX-T.
Types de membres du groupe de sécurité (Statique ou Entité appartient à) : <ul style="list-style-type: none"> ■ Balise de sécurité 	Oui	<p>Si une balise de sécurité est ajoutée au groupe de sécurité en tant que membre statique ou en tant que membre dynamique utilisant Entité appartient à, la balise de sécurité doit exister pour que le groupe de sécurité soit migré.</p> <p>Si la balise de sécurité est ajoutée au groupe de sécurité en tant que membre dynamique (n'utilisant pas Entité appartient à), l'existence de la balise de sécurité n'est pas vérifiée avant la migration du groupe de sécurité.</p>

Tableau 1-6. Groupes de sécurité (suite)

Configuration	Pris en charge	Détails
Types de membres du groupe de sécurité (Statique ou Entité appartient à) : <ul style="list-style-type: none"> ■ vNIC ■ Machine virtuelle 	Oui	<ul style="list-style-type: none"> ■ Les vNIC et les VM sont migrées en tant que ExternalIDExpression. ■ Les VM orphelines (VM supprimées des hôtes) sont ignorées lors de la migration du groupe de sécurité. ■ Une fois que les groupes apparaissent sur NSX-T, les appartenances de VM et vNIC sont mises à jour après un certain temps. Pendant cette période intermédiaire, il peut y avoir des groupes temporaires et leurs groupes temporaires peuvent apparaître en tant que membres. Toutefois, une fois la migration de l'hôte terminée, ces groupes temporaires supplémentaires ne sont plus visibles.
Utilisation de l'opérateur « Correspond à l'expression régulière » pour l'appartenance dynamique	Non	Cela affecte la balise de sécurité et le nom de la VM uniquement. « Correspond à l'expression régulière » n'est pas disponible pour d'autres attributs.
Utilisation d'autres opérateurs disponibles pour les critères d'appartenance dynamique pour les attributs : <ul style="list-style-type: none"> ■ Balise de sécurité ■ Nom de la machine virtuelle ■ Nom de l'ordinateur ■ Nom du SE de l'ordinateur 	Oui	Les opérateurs disponibles pour Nom de la machine virtuelle, Nom de l'ordinateur et Nom du SE de l'ordinateur sont Contient, Se termine par, Est égal à, Est différent de, Commence par. Les opérateurs disponibles pour la balise de sécurité sont Contient, Se termine par, Est égal à, Commence par.

Tableau 1-6. Groupes de sécurité (suite)

Configuration	Pris en charge	Détails
Critères d'Entité appartient à	Oui	<p>Les mêmes limitations pour la migration des membres statiques s'appliquent aux critères d'Entité appartient à. Par exemple, si vous disposez d'un groupe de sécurité qui utilise une entité appartenant à un cluster dans la définition, le groupe de sécurité n'est pas migré.</p> <p>Les groupes de sécurité qui contiennent des critères d'Entité appartient à combinés avec AND ne sont pas migrés.</p>
Opérateurs de critères d'appartenance dynamique (AND, OR) dans le groupe de sécurité	Oui.	<p>Lorsque vous définissez l'appartenance dynamique pour un groupe de sécurité NSX Data Center for vSphere, vous pouvez configurer les éléments suivants :</p> <ul style="list-style-type: none"> ■ Un ou plusieurs ensembles dynamiques. ■ Chaque ensemble dynamique peut contenir un ou plusieurs critères dynamiques. Par exemple, « Nom de la machine virtuelle contient Web ». ■ Vous pouvez choisir de faire correspondre un ou tous les critères dynamiques d'un ensemble dynamique. ■ Vous pouvez choisir de rechercher des correspondances avec AND ou OR entre des ensembles dynamiques. <p>NSX for vSphere ne limite pas le nombre de critères dynamiques, des jeux dynamiques, et vous pouvez avoir des combinaisons de AND et OR.</p> <p>Dans NSX-T Data Center, vous pouvez avoir un groupe comportant cinq expressions. Les groupes de sécurité NSX for vSphere qui contiennent plus de cinq expressions ne sont pas migrés.</p> <p>Exemples de groupes de sécurité pouvant être migrés :</p> <ul style="list-style-type: none"> ■ Jusqu'à 5 ensembles dynamiques liés avec OR où chaque ensemble dynamique contient jusqu'à 5 critères dynamiques liés avec AND (tous dans NSX for vSphere). ■ 1 ensemble dynamique contenant 5 critères dynamiques liés avec OR (Any dans NSX for vSphere).

Tableau 1-6. Groupes de sécurité (suite)

Configuration	Pris en charge	Détails
		<ul style="list-style-type: none"> ■ 1 ensemble dynamique contenant 5 critères dynamiques liés avec AND (All dans NSX for vSphere). Tous les types de membres doivent être identiques. ■ 5 ensembles dynamiques liés avec AND et chaque ensemble dynamique contenant exactement 1 critère dynamique. Tous les types de membres doivent être identiques. <p>L'utilisation de critères « Entité appartient à » avec des opérateurs AND n'est pas prise en charge.</p> <p>Toutes les autres combinaisons ou définitions d'un groupe de sécurité contenant des scénarios non pris en charge ne sont pas migrées.</p>

Dans NSX for vSphere, les balises de sécurité sont des objets qui peuvent être appliqués à des VM. Lors de la migration vers NSX-T, les balises de sécurité sont des attributs d'une VM.

Tableau 1-7. Balises de sécurité

Configuration	Pris en charge	Détails
Balises de sécurité	Oui	<p>Si une VM dispose d'au moins 25 balises de sécurité appliquées, la migration des balises de sécurité est prise en charge. Si plus de 25 balises de sécurité sont appliquées, aucune balise n'est migrée.</p> <p>Remarque : si les balises de sécurité ne sont pas migrées, la VM n'est pas incluse dans les groupes définis par l'appartenance à une balise.</p>

Les services et les groupes de services sont migrés vers NSX-T Data Center en tant que services. Consultez **Inventaire > Services** dans l'interface Web de NSX-T Manager.

Tableau 1-8. Services et groupes de services

Configuration	Pris en charge	Détails
Services et groupes de services (applications et groupes d'applications)	Oui	La plupart des services et des groupes de services par défaut sont mappés à des services NSX-T. Si un service ou un groupe de services n'est pas présent dans NSX-T, un service est créé dans NSX-T.
Groupes de services APP_ALL et APP_POP2	Non	Ces groupes de services définis par le système ne sont pas migrés.

Tableau 1-8. Services et groupes de services (suite)

Configuration	Pris en charge	Détails
Services et groupes de services avec des conflits de noms	Oui	Si un conflit de nom est identifié dans NSX-T pour un service ou un groupe de services modifié, un service est créé dans NSX-T avec un nom au format suivant : <NSXv-Application-Name> migré à partir de NSX-V
Groupes de services qui combinent des services de couche 2 à des services dans d'autres couches	Non	
Groupes de services vides	Non	NSX-T ne prend pas en charge les services vides.
Services de couche 2	Oui	Les services de couche 2 NSX for vSphere sont migrés en tant qu'entrée de service NSX-T EtherTypeServiceEntry.
Services de couche 3	Oui	En fonction du protocole, les services de couche 3 NSX for vSphere sont migrés vers l'entrée de service NSX-T comme suit : <ul style="list-style-type: none"> ■ Protocole TCP/UDP : L4PortSetServiceEntry ■ Protocole ICMP/IPV6ICMP : ICMPTypeServiceEntry ■ Protocole IGMP : IGMPTypeServiceEntry ■ Autres protocoles : IPProtocolServiceEntry
Services de couche 4	Oui	Migré en tant qu'entrée de service NSX-T ALGTypeServiceEntry.
Services de couche 7	Oui	Migré en tant qu'entrée de service NSX-T PolicyContextProfile Si un port et un protocole ont été définis pour une application de couche 7 NSX for vSphere, un service est créé dans NSX-T avec la configuration de port et de protocole appropriée et mappé à PolicyContextProfile.
Groupes de services de couche 7	Non	
Règles de pare-feu distribué, de pare-feu Edge ou NAT qui contiennent le port et le protocole	Oui	NSX-T nécessite un service pour créer ces règles. S'il existe un service approprié, il est utilisé. Si aucun service approprié n'existe, un service est créé à l'aide du port et du protocole spécifiés dans la règle.

Tableau 1-9. Service Composer

Configuration	Pris en charge	Détails
Stratégies de sécurité de Service Composer	Oui	<p>Les règles de pare-feu définies dans une stratégie de sécurité sont migrées vers NSX-T en tant que règles de pare-feu distribué.</p> <p>Les règles de pare-feu désactivées définies dans une stratégie de sécurité de Service Composer ne sont pas migrées.</p> <p>Les règles de Guest Introspection ou les règles d'introspection du réseau définies dans une stratégie de sécurité de Service Composer ne sont pas migrées.</p> <p>Si l'état de Service Composer n'est pas synchronisé, l'étape de résolution de la configuration vous en avertit.</p> <p>Vous pouvez ignorer la migration des stratégies de Service Composer en ignorant les sections appropriées du pare-feu distribué. Ou bien vous pouvez annuler la migration, synchroniser Service Composer avec le pare-feu distribué et redémarrer la migration.</p>
Les stratégies de sécurité de Service Composer ne s'appliquent à aucun groupe de sécurité	Non	

Configuration du serveur Active Directory

Configuration	Pris en charge	Détails
Serveur Active Directory (AD)	Non	

Topologies prises en charge par le coordinateur de migration

Le coordinateur de migration peut migrer un environnement NSX Data Center for vSphere s'il est configuré dans une topologie prise en charge.

Fonctionnalités non prises en charge

Dans toutes les topologies, les fonctionnalités suivantes ne sont pas prises en charge :

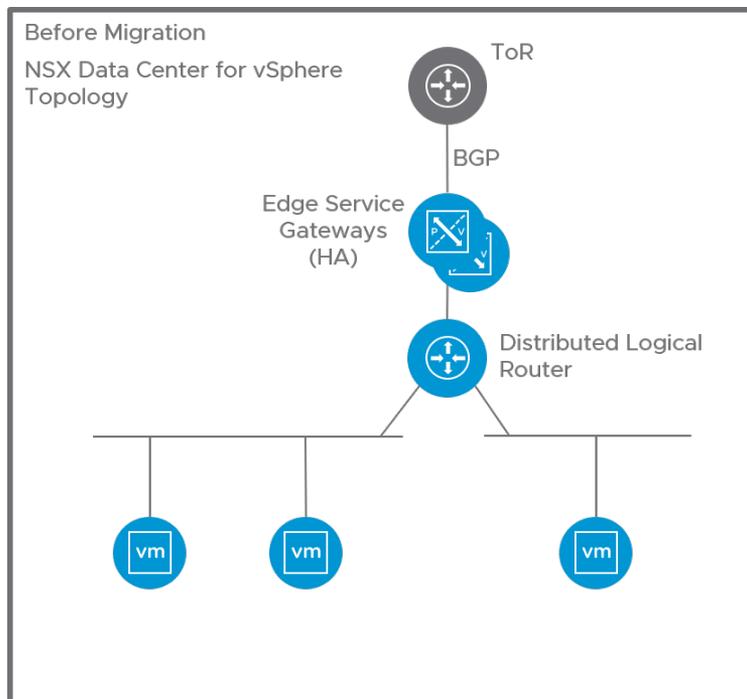
- OSPF entre les passerelles Edge Services Gateways et les routeurs ascendants. Vous devez reconfigurer pour utiliser BGP.
- Multidiffusion IP.
- IPv6

Pour obtenir des informations détaillées sur les fonctionnalités et les configurations prises en charge, reportez-vous à la section [Prise en charge détaillée des fonctionnalités du coordinateur de migration](#).

ESG avec les services Haute disponibilité et L4-L7

Cette topologie contient les configurations suivantes :

- Un échange de routeur logique distribué avec la passerelle Edge Services Gateway.
- ECMP n'est pas configuré.
- Les passerelles Edge Services Gateway sont dans une configuration à haute disponibilité.
- BGP est configuré entre la passerelle Edge Service Gateway et les routeurs ascendants.
- La passerelle Edge Services Gateway peut exécuter des services L4-L7 :
 - Les services VPN, NAT, serveur DHCP, relais DHCP, transfert DNS et pare-feu Edge sont pris en charge.
 - L'équilibrage de charge n'est pas pris en charge dans cette topologie.

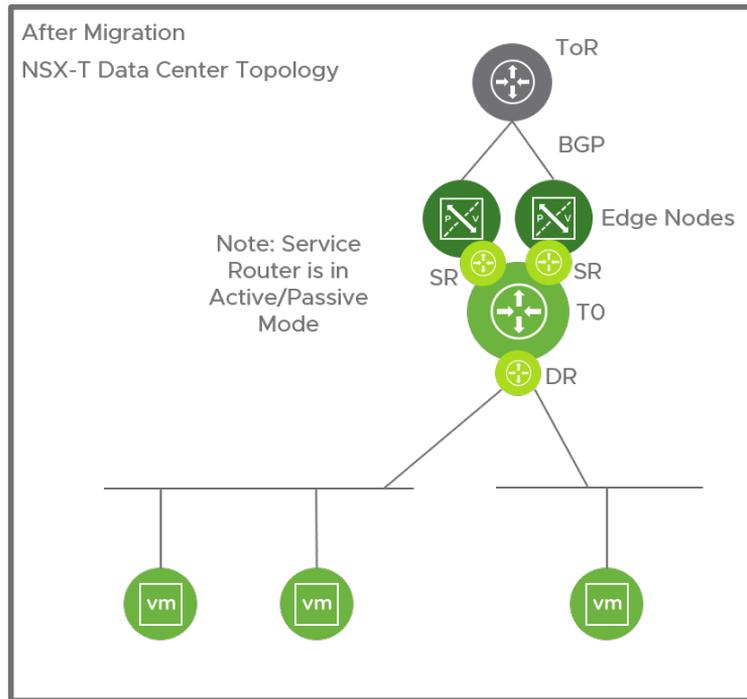


Après la migration, cette configuration est remplacée par une passerelle de niveau 0.

- Le routeur de services de passerelle de niveau 0 est en mode actif/en veille.
- Les adresses IP des interfaces de routeur logique distribué sont configurées comme des liaisons descendantes sur la passerelle de niveau 0.
- La configuration BGP des passerelles ESG est convertie en une configuration BGP sur la passerelle de niveau 0.

- Les services pris en charge sont migrés vers la passerelle de niveau 0.

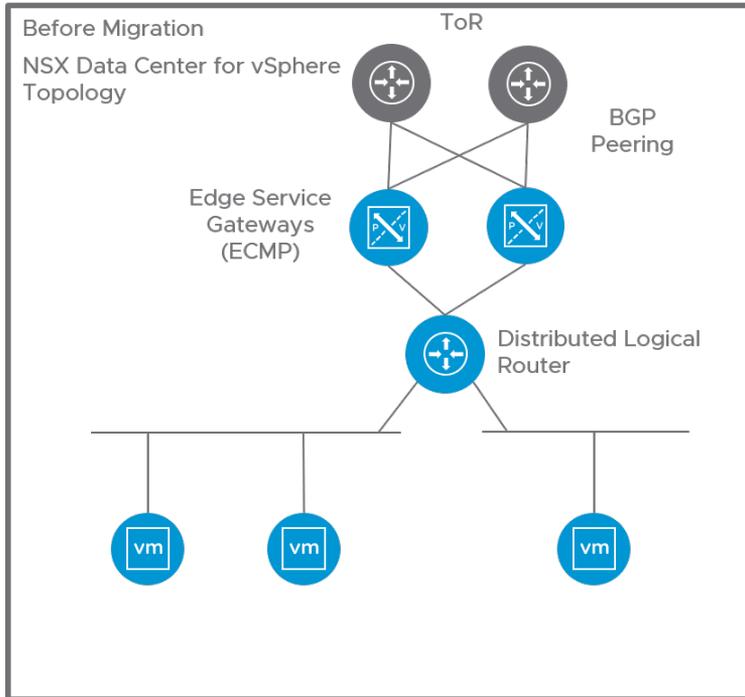
Note Selon votre configuration, vous devrez fournir de nouvelles adresses IP pour les liaisons montantes de passerelle de niveau 0. Par exemple, sur une passerelle Edge Services Gateway, vous pouvez utiliser la même adresse IP pour la liaison montante du routeur et pour le service VPN. Sur une passerelle de niveau 0, vous devez utiliser une adresse IP différente pour le VPN et les liaisons montantes. Pour plus d'informations, reportez-vous à la section [Exemple de problèmes de configuration](#).



ESG sans services L4-L7

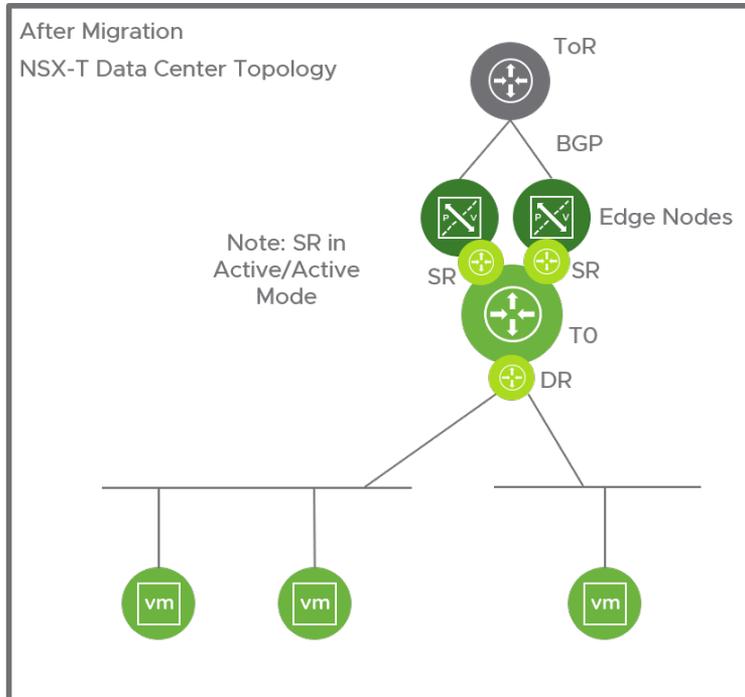
Cette topologie contient les configurations suivantes :

- L'ECMP est activé sur le routeur logique distribué et ce dernier est compatible avec plusieurs passerelles Edge Services Gateways.
- BGP est configuré entre la passerelle Edge Service Gateway et les routeurs ascendants. Les passerelles Edge Services Gateways doivent être configurées avec les mêmes voisins BGP. Toutes les passerelles Edge Services Gateways doivent pointer vers le même système autonome (AS).
- Si BGP est configuré entre le routeur logique distribué et la passerelle Edge Services Gateway, tous les voisins BGP sur le routeur logique distribué doivent avoir le même poids.
- Les passerelles Edge Services Gateway ne doivent pas exécuter les services L4-L7.



Après la migration, cette configuration est remplacée par une passerelle de niveau 0.

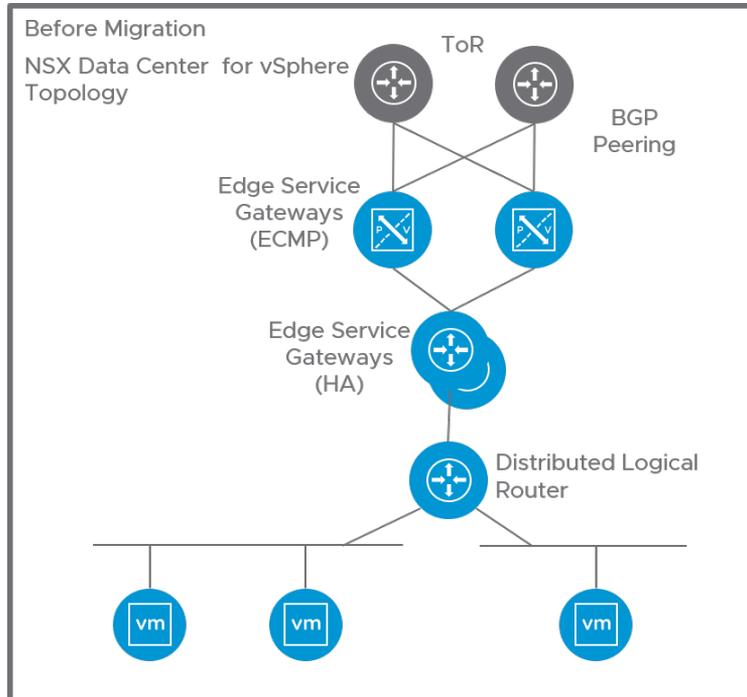
- Le routeur de services de passerelle de niveau 0 est en mode actif/actif.
- Les adresses IP des interfaces de routeur logique distribué sont configurées comme des liaisons descendantes sur la passerelle de niveau 0.
- Les configurations BGP combinées des passerelles Edge Services Gateways sont converties en une configuration BGP sur la passerelle de niveau 0. La configuration de la redistribution d'itinéraire est traduite.
- Les routes statiques des passerelles Edge Services Gateways et des routeurs logiques distribués sont traduites en routes statiques sur la passerelle de niveau 0.



Deux niveaux de passerelle ESG avec les services L4-L7 sur la passerelle ESG de second niveau

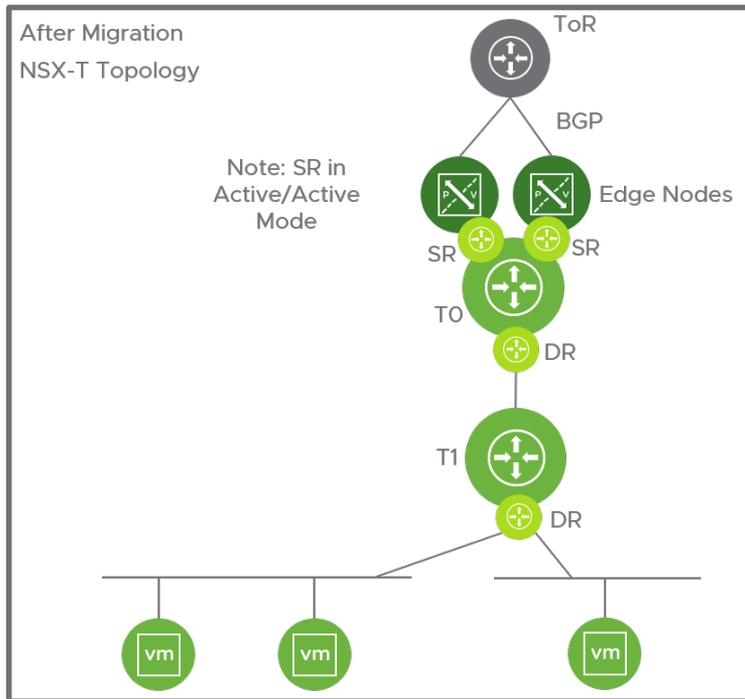
Cette topologie contient les configurations suivantes :

- Deux niveaux de passerelles Edge Services Gateways avec le routeur logique distribué.
- Les passerelles Edge Services Gateways de premier niveau (orientées routeur) ne doivent pas exécuter des services L4-L7.
- BGP doit être activé sur les passerelles Edge Services Gateways de premier niveau et ces dernières doivent disposer d'au moins un voisin BGP.
- ECMP doit être activé sur les passerelles Edge Services Gateways de second niveau et ces dernières doivent être compatibles avec les passerelles Edge Services Gateways de premier niveau.
- Les passerelles Edge Services Gateways de second niveau peuvent exécuter des services L4-L7 :
 - NAT, le serveur DHCP, le relais DHCP, le transfert DNS, l'équilibrage de charge en ligne et le pare-feu Edge sont pris en charge.
 - VPN n'est pas pris en charge.



Après la migration, cette configuration est remplacée par une passerelle de niveau 0 et une passerelle de niveau 1.

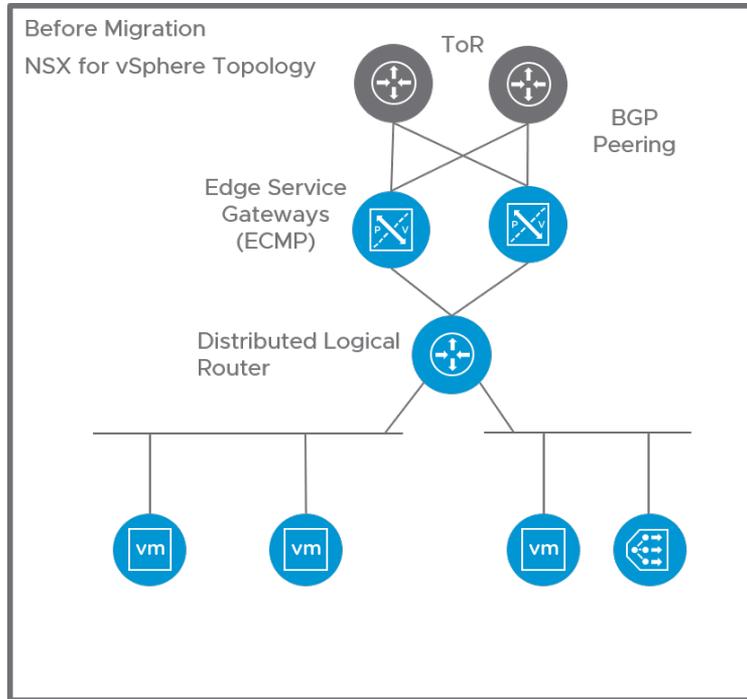
- Les passerelles Edge Services Gateways de premier niveau sont remplacées par une passerelle de niveau 0. Le routeur de service est en mode actif/actif.
- Les adresses IP des liaisons montantes des passerelles Edge Services Gateways de premier niveau sont utilisées pour les liaisons montantes de passerelles de niveau 0.
- La passerelle de niveau 0 est compatible avec les routeurs ascendants utilisant BGP.
- Les passerelles Edge Services Gateways de second niveau sont traduites en passerelle de niveau 1, qui est liée à la passerelle de niveau 0.
- Les adresses IP des interfaces de routeur logique distribué sont configurées comme des liaisons descendantes sur la passerelle de niveau 1.
- Tous les services en cours d'exécution sur la passerelle Edge Services Gateway de second niveau sont migrés vers la passerelle de niveau 1.
- La configuration de BGP sur les passerelles Edge Services Gateways de premier niveau est convertie en une configuration de BGP pour la passerelle de niveau 0. La configuration de la redistribution d'itinéraire est traduite.
- Les routes statiques des passerelles Edge Services Gateways et des routeurs logiques distribués sont traduites en routes statiques sur la passerelle de niveau 0. Les routes statiques entre le routeur logique distribué et les passerelles Edge Services Gateways de second niveau ne sont pas nécessaires et ne sont donc pas converties.



Équilibreur de charge en mode One-Armed

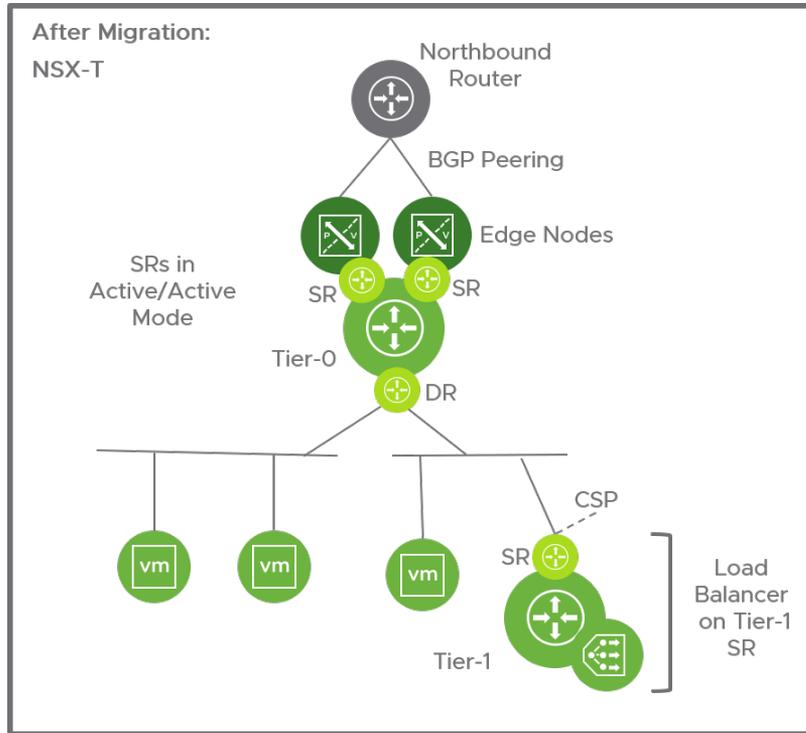
Cette topologie contient les configurations suivantes :

- L'ECMP est activé sur le routeur logique distribué et ce dernier est compatible avec plusieurs passerelles Edge Services Gateways.
- BGP est configuré entre la passerelle Edge Service Gateway et les routeurs ascendants. Toutes les passerelles Edge Services Gateways doivent être configurées avec les mêmes voisins BGP. Toutes les passerelles Edge Services Gateways doivent pointer vers le même système autonome (AS).
- Si BGP est configuré entre le routeur logique distribué et la passerelle Edge Services Gateway, tous les voisins BGP sur le routeur logique distribué doivent avoir le même poids.
- Les passerelles Edge Services Gateways orientées routeur ne doivent pas exécuter des services L4-L7.
- Une passerelle Edge Services Gateway est attachée au routeur logique distribué pour effectuer les services d'équilibrage de charge. Elle peut également exécuter le pare-feu Edge et DHCP.



Après la migration, les passerelles Edge Services Gateways et le Routeur logique distribué de premier niveau sont remplacés par une passerelle de niveau 0. La passerelle Edge Services Gateway qui exécute les services d'équilibrage de charge est remplacée par une passerelle de niveau 1.

- Le routeur de services de passerelle de niveau 0 est en mode actif/actif.
- Les adresses IP des interfaces de routeur logique distribué sont configurées comme des liaisons descendantes sur la passerelle de niveau 0.
- Les configurations BGP combinées des passerelles Edge Services Gateways de premier niveau sont converties en une configuration de BGP sur la passerelle de niveau 0. La configuration de la redistribution d'itinéraire est traduite.
- Les routes statiques des passerelles Edge Services Gateways de niveau supérieur et des routeurs logiques distribués sont traduites en routes statiques sur la passerelle de niveau 0.
- La configuration d'équilibrage de charge sur la passerelle Edge Services Gateway est convertie en une configuration d'équilibrage de charge sur la passerelle de niveau 1.



Microsegmentation supportée par VLAN

Cette topologie prise en charge utilise le pare-feu distribué pour fournir une protection de pare-feu aux charges de travail connectées à des groupes de ports distribués supportés par VLAN.

Cette topologie utilise les fonctionnalités NSX Data Center for vSphere suivantes :

- NSX Manager
- Préparation de l'hôte (mais pas VXLAN)
- Pare-feu distribué
- Service Composer
- Regroupement des objets

Cette topologie ne doit pas contenir les fonctionnalités suivantes :

- Zone de transport
- VXLAN
- Commutateur logique
- Edge Services Gateway
- Routeur logique distribué

Limites prises en charge par le coordinateur de migration

Le coordinateur de migration prend en charge la migration d'environnements NSX Data Center for vSphere qui tombent dans ces limites.

Tableau 1-10. Limites de la migration

Fonctionnalité	Limite
Hôtes par instance de NSX Manager (un seul vCenter - Zone de transport)	64
Clusters vCenter	8
Interfaces virtuelles par hôte d'hyperviseur	150
Commutateurs logiques	1 400
Interfaces des routeurs logiques distribués par routeur logique distribué	800
Chemins ECMP	8
Routes statiques par passerelle Edge Service Gateway	2 000
Règles NAT par passerelle Edge Service Gateway	2 000
Règles de pare-feu Edge par passerelle Edge Service Gateway	2 000
Baux DHCP par passerelle Edge Service Gateway	800
Règles de pare-feu distribué par instance de NSX Manager	10 000
Sections de pare-feu distribué	1 300
Règles de pare-feu distribué par hôte	1 000
Groupes de sécurité par instance de NSX Manager	1 215
Ensembles d'adresses IP	1 000
Ensembles d'adresses MAC	200
Balises de sécurité	600
Balises de sécurité par machine virtuelle	25
Objets de regroupement par instance de NSX Manager	1 250
Serveurs virtuels par équilibrage de charge	200
Pools par équilibrage de charge	200
Tunnels IPsec par passerelle Edge Service Gateway	100
Clients L2VPN (spoke) gérés par un seul serveur L2VPN (hub)	1
Réseaux par paire client-serveur L2VPN	100

Présentation de la migration à l'aide du coordinateur de migration

Le processus de migration inclut la configuration d'un nouvel environnement NSX-T et l'exécution du coordinateur de migration. Vous devrez peut-être modifier également l'environnement NSX for vSphere existant pour vous assurer qu'il peut migrer vers NSX-T.

Attention Déployez un nouvel environnement NSX-T en tant que destination pour la migration de NSX for vSphere.

Pendant l'étape **Importer une configuration**, toutes les interfaces de nœud Edge dans l'environnement NSX-T de destination sont arrêtées. Si l'environnement NSX-T de destination est déjà configuré et est en cours d'utilisation, le démarrage de l'importation de la configuration entraînera l'interruption du trafic.

Lors de la migration, vous allez effectuer les étapes suivantes :

- Créez un environnement NSX-T.
 - Déployez un dispositif NSX Manager pour créer l'environnement NSX-T.
Installez les dispositifs NSX Manager sur les hôtes ESXi qui ne font pas partie de l'environnement de NSX for vSphere en cours de migration.
 - Configurez un gestionnaire de calcul dans l'environnement NSX-T. Ajoutez le dispositif vCenter Server comme ressource de calcul. Utilisez l'adresse IP ou le nom d'hôte exact spécifié dans l'enregistrement de vCenter Server auprès de NSX for vSphere.
 - Déployez des dispositifs NSX Manager supplémentaires pour créer un cluster.
 - Démarrez le service de coordinateur de migration.
 - Si vous souhaitez importer des utilisateurs à partir de NSX for vSphere, configurez VMware Identity Manager.
 - Créez un pool d'adresses IP NSX-T à utiliser pour les TEP NSX-T Edge. Ces adresses IP doivent être en mesure de communiquer avec tous les VTEP NSX for vSphere existants
- Importez la configuration à partir de NSX for vSphere.
 - Entrez les détails de votre environnement NSX for vSphere.
 - La configuration est récupérée et les vérifications préalables sont exécutées.
- Résolvez les problèmes liés à la configuration et déployez des nœuds Edge NSX-T.
 - Passez en revue les Messages et les problèmes de configuration signalés afin d'identifier des problèmes de blocage ou d'autres problèmes qui nécessitent une modification de l'environnement de NSX for vSphere.
 - Si vous apportez des modifications à NSX for vSphere, vous devez redémarrer la migration et importer de nouveau la configuration.
 - Déployer les nœuds NSX Edge
 - Déployez le nombre adéquat de dispositifs Edge NSX-T de taille appropriée.

- Reliez les nœuds Edge au plan de gestion via la ligne de commande.
- Avant de pouvoir migrer votre environnement NSX for vSphere vers NSX-T, fournissez des réponses aux questions de configuration à résoudre. La résolution des problèmes peut être effectuée en plusieurs passes et par plusieurs personnes.
- Migrez la configuration.
 - Une fois tous les problèmes de configuration résolus, vous pouvez importer la configuration vers NSX-T. Les modifications de configuration sont effectuées sur NSX-T, mais à ce stade, aucune modification n'est apportée à l'environnement NSX for vSphere.
- Migrez les dispositifs Edge.
 - Les services Edge et de routage sont migrés de NSX for vSphere vers NSX-T.

Attention Le trafic vertical est interrompu pendant l'étape de migration des dispositifs Edge. L'ensemble du trafic qui traversait précédemment les passerelles Edge Services Gateway (trafic vertical) se déplace vers les dispositifs NSX-T Edge.

- Migrez les hôtes.
 - Le logiciel NSX for vSphere est supprimé des hôtes, et le logiciel NSX-T est installé. Les interfaces de machine virtuelle sont connectées aux nouveaux segments NSX-T.

Attention Pendant l'étape de migration des hôtes, le trafic est interrompu.

- Terminez la migration.
 - Après avoir vérifié que le nouvel environnement NSX-T fonctionne correctement, vous pouvez achever la migration, ce qui efface l'état de migration.

Déploiement de machine virtuelle pendant la migration

Si vous souhaitez déployer des machines virtuelles pendant le processus de migration, déployez les machines virtuelles sur des hôtes NSX-T, connectez les machines virtuelles aux segments NSX-T et installez VMware Tools sur les machines virtuelles.

Le déploiement sur NSX-T avec VMware Tools installé garantit que les machines virtuelles sont remplies dans des groupes de sécurité et reçoivent les stratégies de pare-feu distribué prévues.

Attention Les machines virtuelles déployées sans VMware Tools installé ou déployées sur NSX for vSphere ne reçoivent pas les stratégies de pare-feu distribué prévues.

Si vous utilisez des modèles vSphere pour déployer des machines virtuelles, mettez à jour les modèles afin d'utiliser les segments NSX-T pour la configuration réseau de la machine virtuelle. La spécification de segments NSX-T garantit que toutes les machines virtuelles déployées à l'aide des modèles sont déployées sur des hôtes NSX-T.

Préparation de la migration d'un environnement NSX Data Center for vSphere

Avant de migrer, vous devez consulter la documentation, vérifier que vous disposez des versions logicielles requises, modifier votre environnement de NSX for vSphere existant si nécessaire et déployer l'infrastructure pour le nouvel environnement NSX-T.

Documentation

Recherchez la dernière version de ce guide et les notes de mise à jour de NSX-T Data Center et du coordinateur de migration. Vous trouverez la documentation ici : <https://docs.vmware.com/fr/VMware-NSX-T-Data-Center/>.

Logiciels et versions requises

- Assurez-vous que l'environnement NSX for vSphere comporte la version 6.4.4.
- Reportez-vous aux *matrices d'interopérabilité de VMware* pour connaître les versions de vCenter Server et d' ESXi : http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php#interop&175=&1=&2=
- Les versions 6.5.0 et 6.6.0 de vSphere Distributed Switch sont prises en charge.
- L'environnement de NSX for vSphere doit correspondre à la configuration système NSX-T requise pour ESXi, vCenter Server et le vSphere Distributed Switch.
- Si vous souhaitez migrer les rôles d'utilisateur à partir de NSX for vSphere, vous devez déployer et configurer VMware Identity Manager™. Reportez-vous aux *matrices d'interopérabilité de VMware* pour connaître les versions compatibles : https://www.vmware.com/resources/compatibility/sim/interop_matrix.php#interop&175=&140=. Pour plus d'informations, reportez-vous à la documentation de VMware Identity Manager.

Préparer l'environnement NSX-T Data Center

Vous devez configurer un nouvel environnement de NSX-T Data Center pour migrer l'environnement NSX Data Center for vSphere.

Déployer le dispositif NSX ManagerNSX-T Data Center

Vous devez déployer un nouveau dispositif de NSX Manager pour exécuter le coordinateur de migration. N'utilisez pas un environnement NSX-T Data Center existant.

Important Installez les dispositifs NSX Manager sur les hôtes ESXi qui ne font pas partie de l'environnement de NSX for vSphere en cours de migration.

Conditions préalables

- Vérifiez que la configuration système requise est satisfaite et les ports nécessaires ouverts. Consultez le *Guide d'installation de NSX-T Data Center* pour plus d'informations.

- Assurez-vous qu'une banque de données est configurée et accessible sur l'hôte ESXi. HA nécessite un stockage partagé afin que NSX Manager puisse être redémarré sur un autre hôte si l'hôte d'origine est en panne.
- Vérifiez que vous disposez de l'adresse IP et de la passerelle, des adresses IP du serveur DNS, de la liste de recherche de domaines et de l'adresse IP du serveur NTP que NSX Manager utilisera.
- Créez le réseau du groupe de ports de machines virtuelles cible, si celui-ci n'existe pas déjà. Placez les dispositifs NSX-T Data Center sur un réseau de machines virtuelles de gestion.

Si vous disposez de plusieurs réseaux de gestion, vous pouvez ajouter des itinéraires statiques aux autres réseaux à partir du dispositif NSX-T Data Center.

- Planifiez votre schéma d'adressage IP IPv4 ou IPv6 NSX Manager.

Procédure

- 1 Localisez le fichier OVA de NSX-T Data Center sur le portail de téléchargement de VMware.

Copiez l'URL de téléchargement ou téléchargez le fichier OVA.

- 2 Dans vSphere Client, sélectionnez l'hôte sur lequel installer NSX-T Data Center.

- 3 Cliquez avec le bouton droit et sélectionnez **Déployer un modèle OVF** pour démarrer l'Assistant d'installation.

- 4 Entrez l'URL de téléchargement de l'OVA ou accédez au fichier OVA.

- 5 Entrez un nom pour la machine virtuelle NSX Manager.

Le nom entré s'affiche dans l'inventaire vSphere.

- 6 Sélectionnez une ressource de calcul pour le dispositif NSX Manager.

- 7 Vérifiez les informations du modèle OVF.

- 8 Pour des performances optimales, réservez de la mémoire pour le dispositif NSX Manager.

Définissez la réservation de manière à garantir que NSX Manager dispose de suffisamment de mémoire pour s'exécuter efficacement. Reportez-vous à la section « Configuration système requise de NSX Manager » du *Guide d'installation de NSX-T Data Center*.

- 9 Sélectionnez une banque de données pour stocker les fichiers du dispositif NSX Manager.

- 10 Sélectionnez un réseau de destination pour chaque réseau source.

- 11 Sélectionnez le groupe de ports ou le réseau de destination du dispositif NSX Manager.

- 12 Entrez les mots de passe de racine système de NSX Manager, d'administrateur de l'interface de ligne de commande et d'audit.

Vos mots de passe doivent respecter les indications relatives au niveau de sécurité du mot de passe.

- Au moins 12 caractères
- Au moins une lettre minuscule
- Au moins une lettre majuscule

- Au moins un chiffre
- Au moins un caractère spécial
- Au moins cinq caractères différents
- Aucun mot issu du dictionnaire
- Aucun palindrome
- Une séquence de plus de quatre caractères monotones n'est pas autorisée

13 Entrez le nom d'hôte de NSX Manager.

14 Acceptez le rôle **nsx-manager nsx-controller** par défaut pour la machine virtuelle.

15 Entrez la passerelle par défaut, l'adresse IPv4 du réseau de gestion, le masque du réseau de gestion, le DNS et l'adresse IP NTP.

16 Activez SSH et, si nécessaire, autorisez une connexion SSH racine à la ligne de commande NSX Manager.

Par défaut, ces options sont désactivées pour des raisons de sécurité.

17 Vérifiez que l'ensemble des spécifications de votre modèle OVF personnalisé sont correctes et cliquez sur **Terminer** pour lancer l'installation.

L'installation peut prendre 7 à 8 minutes.

18 À partir de vSphere Client, ouvrez la console de machine virtuelle NSX Manager pour suivre le processus de démarrage.

19 Dès que NSX Manager a démarré, connectez-vous à l'interface de ligne de commande en tant qu'administrateur et exécutez la commande `get interface eth0` pour vérifier que l'adresse IP a été appliquée comme prévu.

20 Entrez la commande `get services` pour vérifier que tous les services sont en cours d'exécution.

Si des services ne sont pas en cours d'exécution, attendez qu'ils aient tous démarré.

Note Les services suivants ne sont pas exécutés par défaut : `liagent`, `migration-coordinator` et `snmp`. Vous pouvez les démarrer comme suit :

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

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

21 Vérifiez que votre NSX Manager dispose de la connectivité requise.

Assurez-vous que vous pouvez effectuer les tâches suivantes.

- Effectuez un test ping de votre NSX Manager à partir d'une autre machine.

- NSX Manager peut effectuer un test ping de sa passerelle par défaut.
- NSX Manager peut effectuer un test ping des hôtes d'hyperviseur qui se trouvent dans le même réseau que NSX Manager à l'aide de l'interface de gestion.
- NSX Manager peut effectuer un test ping de son serveur DNS et de son serveur NTP.
- Si vous avez activé le protocole SSH, assurez-vous de pouvoir l'utiliser avec votre dispositif NSX Manager.

Si la connectivité n'est pas établie, vérifiez que l'adaptateur réseau du dispositif virtuel se trouve sur le réseau ou le VLAN adéquat.

Ajouter un gestionnaire de calcul

Avant d'entamer le processus de migration, vous devez configurer le système vCenter Server associé à NSX Data Center for vSphere en tant que gestionnaire de calcul dans NSX-T.

Lorsque vous ajoutez un gestionnaire de calcul vCenter Server, vous devez fournir les informations d'identification de l'utilisateur de vCenter Server. Vous pouvez fournir les informations d'identification de l'administrateur de vCenter Server ou créer un rôle et un utilisateur spécifiquement pour NSX-T Data Center et fournir les informations d'identification de cet utilisateur. Vous devez avoir les privilèges de vCenter Server suivants :

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

Pour plus d'informations sur les rôles et les privilèges de vCenter Server, consultez le document *Sécurité vSphere*.

Conditions préalables

Connectez-vous à l'interface Web NSX Manager NSX for vSphere pour récupérer les paramètres utilisés pour l'enregistrement de vCenter Server. Vous devez utiliser exactement les mêmes paramètres ; par exemple, si une adresse IP est indiquée, utilisez cette adresse IP et non le nom de domaine complet.

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Système > Infrastructure > Gestionnaires de calcul > Ajouter**.
- 3 Indiquez les détails des gestionnaires de calcul.

Option	Description
Nom et description	Tapez le nom pour identifier l'instance de vCenter Server. Vous pouvez éventuellement indiquer des détails, tels que le nombre de clusters dans l'instance de vCenter Server.
Nom de domaine/adresse IP	Tapez l'adresse IP de l'instance de vCenter Server.
Type	Conservez l'option par défaut.
Nom d'utilisateur et mot de passe	Tapez les informations d'identification de connexion de vCenter Server.
Empreinte numérique	Tapez la valeur de l'algorithme d'empreinte numérique SHA-256 de vCenter Server.

Si la valeur d'empreinte est vide, vous êtes invité à accepter l'empreinte numérique du serveur fournie.

Une fois que vous acceptez l'empreinte numérique, quelques secondes sont nécessaires pour que NSX-T Data Center découvre et enregistre les ressources de vCenter Server.

- 4 Si l'icône de progression passe de **En cours** à **Non enregistré**, suivez les étapes décrites ci-dessous pour résoudre l'erreur.
 - a Sélectionnez le message d'erreur et cliquez sur **Résoudre**. Un message d'erreur possible est le suivant :

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

- b Entrez les informations d'identification de vCenter Server et cliquez sur **Résoudre**.
S'il existe déjà un enregistrement, il sera remplacé.

Il faut un certain temps pour enregistrer le gestionnaire de calcul auprès de vCenter Server et pour que l'état de connexion s'affiche en tant que **ACTIF**.

Vous pouvez cliquer sur le nom du gestionnaire de calcul pour voir ses détails, le modifier ou pour gérer les balises qui s'y appliquent.

Déployer des dispositifs supplémentaires de NSX Manager

Vous pouvez exécuter l'outil de coordinateur de migration avec un seul dispositif de NSX Manager déployé. Cependant, déployez deux dispositifs NSX Manager supplémentaires avant d'utiliser votre environnement NSX-T Data Center en production.

Important Installez les dispositifs NSX Manager sur les hôtes ESXi qui ne font pas partie de l'environnement de NSX for vSphere en cours de migration.

Une fois les nouveaux nœuds déployés, ils se connectent au nœud NSX Manager parent pour former un cluster. Le nombre de nœuds NSX Manager en cluster recommandé est trois.

Tous les détails de référentiel du nœud NSX Manager parent sont synchronisés avec les nœuds qui viennent d'être déployés sur le cluster.

Conditions préalables

- Vérifiez qu'un nœud NSX Manager parent est installé.
- Vérifiez qu'un gestionnaire de calcul est configuré. Reportez-vous à la section [Ajouter un gestionnaire de calcul](#).

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Système > Présentation > Ajouter des nœuds**.
- 3 Entrez les détails des attributs communs de NSX Manager.

Option	Description
Gestionnaire de calcul	Le gestionnaire de calcul de la ressource enregistrée est renseigné.
Activer SSH	Basculez le bouton pour autoriser une connexion SSH sur le nouveau nœud NSX Manager.
Activer l'accès à la racine	Basculez le bouton pour autoriser l'accès racine au nouveau nœud NSX Manager.

Option	Description
Nom d'utilisateur de la ligne de commande et confirmation du mot de passe	<p>Définissez le mot de passe CLI et la confirmation de celui-ci pour le nouveau nœud.</p> <p>Votre mot de passe doit respecter les indications relatives au niveau de sécurité du mot de passe.</p> <ul style="list-style-type: none"> ■ Au moins 12 caractères ■ Au moins une lettre minuscule ■ Au moins une lettre majuscule ■ Au moins un chiffre ■ Au moins un caractère spécial ■ Au moins cinq caractères différents ■ Aucun mot issu du dictionnaire ■ Aucun palindrome ■ Une séquence de plus de quatre caractères monotones n'est pas autorisée <p>Le nom d'utilisateur de la ligne de commande est déjà défini sur admin.</p>
Mot de passe racine et confirmation du mot de passe	<p>Définissez le mot de passe racine et la confirmation de ce dernier pour le nouveau nœud.</p> <p>Votre mot de passe doit respecter les indications relatives au niveau de sécurité du mot de passe.</p> <ul style="list-style-type: none"> ■ Au moins 12 caractères ■ Au moins une lettre minuscule ■ Au moins une lettre majuscule ■ Au moins un chiffre ■ Au moins un caractère spécial ■ Au moins cinq caractères différents ■ Aucun mot issu du dictionnaire ■ Aucun palindrome ■ Une séquence de plus de quatre caractères monotones n'est pas autorisée
Serveurs DNS	Entrez l'adresse IP du serveur DNS disponible dans vCenter Server.
Serveurs NTP	Entrez l'adresse IP du serveur NTP.

4 Entrez les détails du nœud NSX Manager.

Option	Description
Nom	Entrez un nom pour le nœud NSX Manager.
Cluster	Désignez le cluster que le nœud va rejoindre à partir du menu déroulant.
Pool de ressources ou hôte	Attribuez un pool de ressources ou un hôte pour le nœud à partir du menu déroulant.
Banque de données	Sélectionnez une banque de données pour les fichiers du nœud dans le menu déroulant.
Réseau	Attribuez un réseau à partir du menu déroulant.
Adresse IP de gestion/Masque de réseau	Entrez l'adresse IP et le masque de réseau.
Passerelle de gestion	Entrez l'adresse IP de la passerelle.

- 5 (Facultatif) Cliquez sur **Nouveau nœud** et configurez un autre nœud.

Répétez les étapes 3 à 4.

- 6 Cliquez sur **Terminer**.

Les nouveaux nœuds sont déployés. Vous pouvez suivre le processus de déploiement sur la page **Système > Présentation** ou sur vCenter Server.

Le déploiement, la formation de cluster et la synchronisation de référentiel peuvent prendre jusqu'à 10 minutes.

- 7 Dès que NSX Manager a démarré, connectez-vous à l'interface de ligne de commande en tant qu'administrateur et exécutez la commande `get interface eth0` pour vérifier que l'adresse IP a été appliquée comme prévu.

- 8 Entrez la commande `get services` pour vérifier que tous les services sont en cours d'exécution.

Si des services ne sont pas en cours d'exécution, attendez qu'ils aient tous démarré.

- 9 Connectez-vous au nœud NSX Manager parent et entrez la commande `get cluster status` pour vous assurer que les nœuds sont correctement ajoutés au cluster.

- 10 Vérifiez que votre NSX Manager dispose de la connectivité requise.

Assurez-vous que vous pouvez effectuer les tâches suivantes.

- Effectuez un test ping de votre NSX Manager à partir d'une autre machine.
- NSX Manager peut effectuer un test ping de sa passerelle par défaut.
- NSX Manager peut effectuer un test ping des hôtes d'hyperviseur qui se trouvent dans le même réseau que NSX Manager à l'aide de l'interface de gestion.
- NSX Manager peut effectuer un test ping de son serveur DNS et de son serveur NTP.
- Si vous avez activé le protocole SSH, assurez-vous de pouvoir l'utiliser avec votre dispositif NSX Manager.

Si la connectivité n'est pas établie, vérifiez que l'adaptateur réseau du dispositif virtuel se trouve sur le réseau ou le VLAN adéquat.

Créer un pool d'adresses IP pour les points de terminaison de tunnel Edge

Vous devez créer un pool d'adresses IP dans l'environnement de NSX-T pour les points de terminaison de tunnel (TEP) Edge avant de démarrer la migration.

Conditions préalables

- Identifiez les pools d'adresses IP existants utilisés pour les VTEP NSX for vSphere.
- Déterminez quelles adresses IP utiliser afin de créer le pool d'adresses IP pour les TEP Edge.

La plage d'adresses IP et le réseau VLAN ne doivent pas être en cours d'utilisation dans l'environnement de NSX Data Center for vSphere.

- Vérifiez que les adresses IP des TEP NSX-T disposent d'une connectivité réseau vers les adresses IP des VTEP NSX for vSphere.

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Inventaire > Groupes > IP Pools > Ajouter**.
- 3 Entrez le nom que vous souhaitez attribuer au nouveau pool d'adresses IP.
- 4 (Facultatif) Entrez une description.
- 5 Cliquez sur **Ajouter**.
- 6 Cliquez sur la cellule Plages d'adresses IP et entrez les plages d'adresses IP.
Passez le curseur de la souris sur le coin supérieur droit de chaque cellule et cliquez sur l'icône de crayon pour la modifier.
- 7 (Facultatif) Entrez une passerelle.
- 8 Entrez une adresse IP CIDR avec un suffixe.
- 9 (Facultatif) Entrez des serveurs DNS.
- 10 (Facultatif) Entrez un suffixe DNS.
- 11 Cliquez sur **Enregistrer**.

Préparer la migration d'un environnement NSX Data Center for vSphere

Vous devez vérifier l'état de l'environnement de NSX Data Center for vSphere et corriger les problèmes rencontrés. En outre, selon votre environnement, vous devrez modifier votre configuration de NSX Data Center for vSphere avant que vous puissiez migrer vers NSX-T Data Center.

État du système

Vérifier les états système suivants :

- Vérifiez que les composants de NSX for vSphere sont dans un état vert sur le tableau de bord de NSX.
- Vérifiez que tous les hôtes ESXi sont dans un état opérationnel. Réolvez les problèmes impliquant des hôtes, y compris les états déconnectés. Aucun redémarrage ni aucune tâche ne doit être en attente pour passer en mode de maintenance.
- Vérifiez l'état de publication du Pare-feu distribué et Service Composer pour vous assurer qu'il n'y a pas de modifications non publiées.

Configuration générale

- Sauvegardez les environnements NSX for vSphere et vSphere. Reportez-vous à la section « Sauvegarde et restauration de NSX » du *Guide d'administration de NSX*.
- Le port VXLAN doit être défini sur 4789. Si votre environnement NSX for vSphere utilise un port différent, vous devez le modifier avant de pouvoir migrer. Reportez-vous à la section « Modifier le port VXLAN » du *Guide d'administration de NSX NSX for vSphere*.

Configuration du contrôleur

- Le coordinateur de migration ne prend pas en charge les zones de transport de NSX for vSphere avec le mode de réplication multidiffusion ou hybride. Un cluster NSX Controller est obligatoire si VXLAN est en cours d'utilisation. Les topologies de micro-segmentation reposant sur VLAN n'utilisent pas VXLAN et n'ont donc pas besoin d'un cluster NSX Controller.

Configuration d'hôte

- Sur tous les clusters d'hôtes de l'environnement NSX for vSphere, vérifiez ces paramètres et mettez-les à jour si nécessaire :
 - Définissez le vSphere DRS sur manuel
 - Désactivez la Haute disponibilité vSphere.
 - Définissez la version d'exportation du filtre du pare-feu distribué sur 1 000. Reportez-vous à la section [Configurer la version d'exportation du filtre du pare-feu distribué sur des hôtes](#).
- Si vous avez des hôtes sur lesquels NSX for vSphere est installé mais ne sont pas ajoutés à un vSphere Distributed Switch, vous devez les ajouter à des commutateurs distribués si vous souhaitez les migrer vers NSX-T. Pour plus d'informations, reportez-vous à la section [Configurer les hôtes non attachés aux vSphere Distributed Switches](#).
- Sur chaque cluster sur lequel NSX for vSphere est installé, vérifiez si le Pare-feu distribué est activé. Vous pouvez afficher l'état activé dans **Installation et mise à niveau > Préparation de l'hôte**.
Si le Pare-feu distribué est activé sur les clusters de NSX for vSphere avant la migration, le Pare-feu distribué est activé sur tous les clusters lorsqu'ils migrent vers le dispositif NSX-T. Déterminez l'impact de l'activation du Pare-feu distribué sur tous les clusters et modifiez la configuration du Pare-feu distribué, si nécessaire.
- Vérifiez que tous les hôtes possèdent une seule interface VTEP configurée. Vérifiez chaque hôte dans **Hôtes et Clusters > Hôte > Configurer > Adaptateurs VMKernel**. Vérifiez qu'il n'existe qu'une seule interface avec la pile TCP/IP vxlan par hôte. La migration d'hôtes avec plusieurs VTEP n'est pas prise en charge.

Configuration de la passerelle Edge Services Gateway

- Les passerelles Edge Services Gateway doivent utiliser BGP pour le routage ascendant. Si OSPF est utilisé, vous devez le reconfigurer pour utiliser BGP avant de commencer la migration.

- Vous devrez éventuellement apporter des modifications à votre configuration de redistribution d'itinéraire NSX for vSphere avant le début de la migration.
 - Les filtres préfixes configurés au niveau de la redistribution n'ont pas migré. Ajoutez tous les filtres dont vous avez besoin en tant que filtres BGP dans la configuration du voisin BGP de la passerelle de service Edge.
 - Après la migration, les routes apprises dynamiquement entre le routeur logique distribué et la passerelle de service Edge sont converties en routes statiques et toutes les routes statiques sont redistribuées dans BGP. Si vous devez filtrer l'une de ces routes, avant de démarrer la migration, configurez les filtres voisins BGP pour refuser ces préfixes tout en autorisant d'autres.
- NSX for vSphere prend en charge les sessions de VPN IPsec basé sur les stratégies dans lequel les sous-réseaux locaux et homologues de deux ou plusieurs sessions se chevauchent mutuellement. Ce comportement n'est pas pris en charge sur NSX-T. Vous devez reconfigurer les sous-réseaux afin qu'ils ne se chevauchent pas avant de commencer la migration. Si ce problème de configuration n'est pas résolu, l'étape **Migrer la configuration** échoue.
- Si vous disposez d'une passerelle Edge Services effectuant la fonction d'équilibrage de charge à un bras, vous devez modifier les configurations suivantes si elle est présente avant d'importer la configuration :
 - Si la passerelle Edge Services dispose d'une interface configurée pour la gestion, vous devez la supprimer avant la migration. Vous ne pouvez avoir qu'une seule interface connectée à une passerelle Edge Services fournissant une fonction d'équilibrage de charge à un bras. Si elle contient plusieurs interfaces, l'étape **Migrer la configuration** échoue.
 - Si le pare-feu de passerelle Edge Services est désactivé et que la règle par défaut est définie sur Refuser, vous devez activer le pare-feu et modifier la règle par défaut sur accepter. Après la migration, le pare-feu est activé sur la passerelle de niveau 1, et la règle par défaut Accepter prend effet. Modifier la règle par défaut à accepter avant la migration empêche le trafic entrant vers l'équilibrage de charge d'être bloqué.
- Vérifiez que les passerelles Edge Services Gateways sont toutes correctement connectées à la topologie en cours de migration. Si les passerelles Edge Services font partie de l'environnement de NSX for vSphere, mais ne sont pas correctement attachées au reste de l'environnement, elles ne sont pas migrées.

Par exemple, si une passerelle Edge Services est configurée comme un équilibrage de charge à un bras, mais a une des configurations suivantes, elle n'est pas migrée :

- La passerelle Edge Services dispose d'une interface de liaison montante connectée à un commutateur logique.
- La passerelle Edge Services dispose d'une interface de liaison montante connectée à un commutateur logique, mais l'adresse IP de liaison montante ne correspond pas au sous-réseau associé au routeur logique distribué qui se connecte au commutateur logique.

Configurer les hôtes non attachés aux vSphere Distributed Switches

Un environnement de NSX for vSphere peut contenir des hôtes sur lesquels NSX for vSphere est installé, mais ne sont pas ajoutés à un vSphere Distributed Switch. Vous devez ajouter les hôtes à un vSphere Distributed Switch avant de pouvoir les migrer.

Vous pouvez utiliser un commutateur distribué dont vous disposez déjà dans votre environnement ou en créez un nouveau à cet effet. Effectuez un clic droit sur le commutateur distribué et sélectionnez **Ajouter et gérer les hôtes** afin d'ajouter les hôtes au commutateur distribué. Vous n'avez pas besoin d'attribuer des liaisons montantes physiques ou des adaptateurs réseau VMkernel au commutateur distribué.

Reportez-vous à la section « Ajouter des hôtes à un vSphere Distributed Switch » dans le *Guide de mise en réseau vSphere* pour plus d'informations.

Si vous importez la configuration avant d'effectuer cette modification, vous devez redémarrer la migration pour importer la configuration mise à jour. Reportez-vous à la section [Apporter des modifications à l'environnement NSX for vSphere](#).

Une fois la migration terminée, les hôtes n'ont plus besoin d'être connectés au commutateur distribué.

- Si vous avez ajouté les hôtes à un commutateur distribué existant, vous pouvez les en supprimer.
- Si vous avez ajouté les hôtes à un nouveau commutateur distribué que vous n'utilisez pas à d'autres fins, vous pouvez supprimer le commutateur distribué.

Configurer la version d'exportation du filtre du pare-feu distribué sur des hôtes

La version d'exportation du pare-feu distribué doit être définie sur 1 000 sur les hôtes pour que ces derniers puissent être migrés vers NSX-T Data Center. Vous devez vérifier la version d'exportation et effectuer une mise à jour si nécessaire.

Procédure

- ◆ Pour chaque hôte, effectuez les étapes suivantes.
 - a Connectez-vous à l'interface de ligne de commande.
 - b Récupérez le filtre du pare-feu distribué correspondant à l'hôte.

```
[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 Utilisez les informations de filtrage pour récupérer la version d'exportation de l'hôte.

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

- d Si la version d'exportation n'est pas 1 000, définissez-la. Utilisez l'une des méthodes suivantes.
 - Utilisez la commande `vsipioctl setexportversion` pour définir la version d'exportation.

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

- Désactivez, puis activez le pare-feu distribué sur l'hôte.
- e Vérifiez que la version d'exportation est à jour.

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

Migration de NSX Data Center for vSphere vers NSX-T Data Center

Utiliser le coordinateur de migration pour importer votre configuration, résoudre les problèmes de configuration et migrer des dispositifs Edge et des hôtes vers votre environnement NSX-T Data Center.

Conditions préalables

Vérifiez que vous avez effectué toutes les étapes de préparation appropriées avant de démarrer la migration. Reportez-vous à la section [Préparation de la migration d'un environnement NSX Data Center for vSphere](#).

Importer la configuration de NSX Data Center for vSphere

Pour migrer votre environnement NSX Data Center de NSX for vSphere vers NSX-T, vous devez fournir les détails de votre environnement NSX for vSphere.

Le service de coordinateur de migration s'exécute sur un seul nœud du dispositif NSX Manager. Effectuez toutes les opérations de migration à partir du nœud qui exécute le service de coordinateur de migration.

Attention Déployez un nouvel environnement NSX-T en tant que destination pour la migration de NSX for vSphere.

Pendant l'étape **Importer une configuration**, toutes les interfaces de nœud Edge dans l'environnement NSX-T de destination sont arrêtées. Si l'environnement NSX-T de destination est déjà configuré et est en cours d'utilisation, le démarrage de l'importation de la configuration entraînera l'interruption du trafic.

Conditions préalables

- Vérifiez que le système vCenter Server associé à l'environnement NSX for vSphere est enregistré en tant que gestionnaire de calcul. Reportez-vous à la section [Ajouter un gestionnaire de calcul](#).
- Vérifiez que vous avez créé un pool d'adresses IP à utiliser pour les TEP Edge. Reportez-vous à la section [Créer un pool d'adresses IP pour les points de terminaison de tunnel Edge](#).

Procédure

- 1 Connectez-vous à l'interface de ligne de commande NSX Manager en tant qu'**administrateur** et démarrez le service de coordinateur de migration.

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

- 2 À partir d'un navigateur, connectez-vous au nœud du dispositif NSX Manager sur lequel vous avez lancé le service de coordinateur de migration. Connectez-vous en tant qu'**administrateur**.
- 3 Accédez à **Système > Migrer**.
- 4 Dans le volet **Migrer NSX for vSphere**, cliquez sur **Démarrer**.
- 5 Sur la page **Importer une configuration**, cliquez sur **Sélectionner NSX** et fournissez les informations d'identification pour vCenter et NSX for vSphere.

Note Le menu déroulant de vCenter affiche tous les systèmes de vCenter Server qui sont enregistrés comme gestionnaires de calcul. Cliquez sur **Ajouter nouveau** si vous avez besoin d'ajouter un gestionnaire de calcul.

- 6 Cliquez sur **Démarrer** pour importer la configuration.
- 7 Une fois l'importation terminée, cliquez sur **Continuer** pour passer à la page **Résoudre les problèmes**.

Annuler ou redémarrer la migration de NSX for vSphere

Vous pouvez annuler le processus de migration. Vous devrez peut-être effectuer cette opération, car vous avez effectué des modifications dans l'environnement NSX for vSphere et vous devez redémarrer la migration.

Un bouton **Annuler** se trouve sur chaque page de la migration. L'annulation d'une migration supprime tous les états de migration à partir du système.

Attention N'annulez pas une migration si la migration d'un dispositif Edge ou de l'hôte a démarré. L'annulation de la migration supprime tous les états de migration et vous empêche d'afficher les progrès antérieurs.

Si vous avez importé votre configuration, mais que vous n'avez pas encore migré la configuration, vous pouvez cliquer sur **Annuler** pour recommencer.

Si vous avez migré la configuration, vous devez effectuer les étapes suivantes pour redémarrer la migration :

- 1 Annulez la migration.
- 2 Déployez un nouvel environnement NSX-T avec des dispositifs NSX Manager et NSX Edge.

3 Démarrez une nouvelle migration.

Attention Dans NSX-T Data Center 2.4.0, il existe un bouton **Restauration** pour certaines étapes de la migration. L'utilisation du bouton **Restauration** peut entraîner un comportement inattendu. Au lieu de cela, utilisez le bouton **Annuler** pour annuler la migration à l'étape **Importer une configuration** ou **Migrer la configuration**. Si vous avez migré des nœuds Edge et que vous devez les restaurer, contactez le support VMware.

Résoudre les problèmes de configuration et déployer des nœuds Edge

Après avoir importé la configuration de l'environnement NSX Data Center for vSphere, vous devez examiner et résoudre les problèmes de configuration signalés avant de poursuivre la migration.

Examiner les informations de migration

Si vous devez apporter des modifications dans votre environnement de NSX for vSphere, vous devez redémarrer la migration afin de récupérer la nouvelle configuration. Passez en revue tous les commentaires sur la migration avant de commencer à fournir des données afin d'éviter la duplication du travail.

Note Pour certaines fonctionnalités de NSX for vSphere, il peut y avoir des configurations automatiques telles que des certificats présents. Si ces configurations sont destinées à des fonctionnalités qui ne sont pas prises en charge pour la topologie spécifique, ces configurations automatiques sont signalées comme des problèmes qui doivent être ignorés lors de la migration. Par exemple, dans les topologies qui ne prennent pas en charge les services L4-L7 sur les passerelles de services Edge, les certificats présents pour VPN et DNS déclenchent des problèmes pour ignorer ces configurations de la migration.

Procédure

- 1 À partir de la page **Résoudre la configuration**, cliquez sur **Messages** pour afficher des informations sur la migration.

La fenêtre de **Messages** inclut des informations sur les nœuds Edge du dispositif NSX-T requises pour remplacer les passerelles NSX for vSphere Edge Services Gateways. La configuration requise inclut la taille et le nombre de nœuds Edge. Vous devez déployer les nœuds Edge pour pouvoir terminer l'étape **Résoudre la configuration**. Pour plus d'informations, reportez-vous à [Déployer des nœuds NSX Edge](#).

- 2 Passez en revue les problèmes signalés dans chaque catégorie afin d'identifier les problèmes de blocage ou d'autres problèmes qui nécessitent des modifications dans votre environnement de NSX for vSphere.

Étape suivante

Si vous trouvez des problèmes de blocage ou d'autres configurations qui nécessitent une modification dans l'environnement de NSX for vSphere, effectuez ces configurations avant de continuer. Vous devez annuler la migration en cours et importer la nouvelle configuration. Reportez-vous à la section [Apporter des modifications à l'environnement NSX for vSphere](#).

Si vous n'avez pas trouvé de problèmes de blocage ou d'autres configurations qui nécessitent une modification dans l'environnement de NSX for vSphere, vous pouvez poursuivre la migration. Reportez-vous à la section [Déployer des nœuds NSX Edge](#).

Apporter des modifications à l'environnement NSX for vSphere

Vous devrez peut-être apporter des modifications à votre environnement de NSX for vSphere pour poursuivre la migration, par exemple, si des problèmes de blocage sont constatés. Si vous apportez des modifications, vous devez importer à nouveau la configuration afin que le coordinateur de migration soit informé de ces modifications.

Conditions préalables

Vérifiez que la migration d'un hôte ou d'un dispositif Edge n'a pas démarré. Reportez-vous à la section [Annuler ou redémarrer la migration de NSX for vSphere](#) pour plus d'informations sur le redémarrage de la migration.

Procédure

1 Effectuez les modifications nécessaires dans l'environnement de NSX for vSphere.

2 Accédez à la page **Importer la configuration** et cliquez sur **Annuler**.

L'annulation efface le processus de migration en cours. Toute entrée fournie précédemment est supprimée.

3 Cliquez sur **Démarrer** pour importer la configuration mise à jour.

La migration recommence avec la nouvelle configuration de NSX for vSphere.

Étape suivante

Poursuivre le processus de migration. Reportez-vous à la section [Résoudre les problèmes de configuration et déployer des nœuds Edge](#).

Déployer des nœuds NSX Edge

Avant de pouvoir terminer la migration, vous devez déployer un nombre approprié de nœuds Edge de taille adéquate.

Dans un nouvel environnement NSX-T, de nombreuses options sont disponibles pour le déploiement de NSX Edge. Cependant, si vous effectuez la migration à l'aide du coordinateur de migration, vous devez déployer NSX Edge comme machine virtuelle sur ESXi. Procédez au déploiement à l'aide d'un fichier OVA ou OVF. Ne déployez pas sur un dispositif bare metal. N'effectuez pas le déploiement à partir de l'interface de NSX Manager.

Vous devez déployer les nœuds NSX Edge sur des hôtes ESXi qui ne font pas partie de l'environnement NSX for vSphere.

Pour plus d'informations sur la mise en réseau Edge, reportez-vous à la section « Configuration de la mise en réseau NSX Edge » du *Guide d'installation de NSX-T Data Center*.

Conditions préalables

- Vous devez disposer d'un nombre suffisant d'hôtes ESXi avec les ressources appropriées disponibles pour héberger les dispositifs NSX Edge.

Procédure

- 1 Localisez le fichier OVA du dispositif NSX Edge sur le portail de téléchargement de VMware.
Copiez l'URL de téléchargement ou téléchargez le fichier OVA sur votre ordinateur.
- 2 Dans vSphere Client, sélectionnez l'hôte sur lequel installer le dispositif NSX Edge.
- 3 Cliquez avec le bouton droit et sélectionnez **Déployer un modèle OVF** pour démarrer l'Assistant d'installation.
- 4 Entrez l'URL de téléchargement de l'OVA ou accédez au fichier OVA enregistré.
- 5 Entrez un nom pour la machine virtuelle NSX Edge.
Le nom saisi s'affiche dans l'inventaire.
- 6 Sélectionnez une ressource de calcul pour le dispositif NSX Edge.
- 7 Pour des performances optimales, réservez de la mémoire pour le dispositif NSX Edge.
Définissez la réservation de manière à garantir que NSX Edge dispose de suffisamment de mémoire pour s'exécuter efficacement. Reportez-vous à la section « Configuration système requise pour les machines virtuelles NSX Edge » du *Guide d'installation de NSX-T Data Center*.
- 8 Vérifiez les informations du modèle OVF.
- 9 Sélectionnez une banque de données pour stocker les fichiers du dispositif NSX Edge.
- 10 Acceptez l'interface réseau source et de destination par défaut.
Vous pouvez accepter la destination réseau par défaut pour le reste des réseaux et modifier la configuration du réseau une fois NSX Edgedéployé.
- 11 Sélectionnez l'allocation d'adresse IP dans le menu déroulant.
- 12 Entrez les mots de passe de racine système de NSX Edge, d'administrateur de l'interface de ligne de commande et d'audit.
Vos mots de passe doivent respecter les indications relatives au niveau de sécurité du mot de passe.
 - Au moins 12 caractères
 - Au moins une lettre minuscule
 - Au moins une lettre majuscule
 - Au moins un chiffre
 - Au moins un caractère spécial
 - Au moins cinq caractères différents
 - Aucun mot issu du dictionnaire

- Aucun palindrome
- Une séquence de plus de quatre caractères monotones n'est pas autorisée

13 Entrez la passerelle par défaut, l'adresse IPv4 du réseau de gestion, le masque du réseau de gestion, le DNS et l'adresse IP NTP.

14 Entrez le nom d'hôte de la machine virtuelle NSX Edge.

15 Activez SSH et, si nécessaire, autorisez une connexion SSH racine à la ligne de commande NSX Edge.

Par défaut, ces options sont désactivées pour des raisons de sécurité.

16 Vérifiez que l'ensemble des spécifications de votre modèle OVA personnalisé sont correctes et cliquez sur **Terminer** pour lancer l'installation.

L'installation peut prendre 7 à 8 minutes.

17 Ouvrez la console de NSX Edge pour suivre le processus de démarrage.

Si la fenêtre de console ne s'ouvre pas, vérifiez que les fenêtres contextuelles sont autorisées.

18 Une fois que NSX Edge a démarré, connectez-vous à l'interface de ligne de commande avec des informations d'identification d'administrateur.

Note Après le démarrage de NSX Edge, si vous ne vous connectez pas avec les informations d'identification de l'administrateur pour la première fois, le service de plan de données ne démarre pas automatiquement sur NSX Edge.

19 Exécutez la commande `get interface eth0.<vlan_ID>` pour vérifier que l'adresse IP a été appliquée comme il convient

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

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

Note Lors de l'activation de VM NSX Edge sur un hôte géré non-NSX, vérifiez que le paramètre MTU est défini sur 1600 (au lieu de 1500) sur le commutateur hôte physique pour la carte réseau de données.

20 Vérifiez que le dispositif NSX Edge dispose de la connectivité requise.

Si vous avez activé le protocole SSH, assurez-vous de pouvoir l'utiliser avec votre dispositif NSX Edge.

- Vous pouvez effectuer un test ping de votre dispositif NSX Edge.
- NSX Edge peut effectuer un test ping de sa passerelle par défaut.

- NSX Edge peut effectuer un test ping des hôtes d'hyperviseur qui se trouvent sur le même réseau que le dispositif NSX Edge.
- NSX Edge peut effectuer un test ping de son serveur DNS et de son serveur NTP.

21 Résolvez les problèmes de connectivité.

Note Si la connectivité n'est pas établie, vérifiez que l'adaptateur réseau de la machine virtuelle se trouve sur le réseau ou VLAN adéquat.

Par défaut, le chemin de données du dispositif NSX Edge réclame toutes les cartes réseau des machines virtuelles à l'exception de la carte réseau de gestion (celle qui possède une adresse IP et un itinéraire par défaut). Si vous avez attribué de manière incorrecte une carte réseau comme interface de gestion, suivez ces étapes pour utiliser DHCP afin d'attribuer l'adresse IP de gestion à la carte réseau appropriée.

- a Connectez-vous à l'interface de ligne de commande et tapez la commande **stop service dataplane**.
- b Tapez la commande **set interface *interface* dhcp plane mgmt**.
- c Placez *interface* dans le réseau DHCP et attendez qu'une adresse IP soit attribuée à *interface*.
- d Tapez la commande **start service dataplane**.

Les ports fp-ethX de chemin de données utilisés pour la liaison montante VLAN et la superposition du tunnel sont indiqués dans les commandes **get interfaces** et **get physical-port** sur le dispositif NSX Edge.

Joindre NSX Edge au plan de gestion

Vous devez joindre les nœuds Edge que vous avez créés au plan de gestion.

Ne joignez pas les nœuds Edge au plan de gestion en utilisant une autre méthode. Ne créez pas de nœuds de transport à partir des nœuds Edge.

Procédure

- 1 Ouvrez une session SSH vers le dispositif NSX Manager.
- 2 Ouvrez une session SSH vers le dispositif NSX Edge.
- 3 Sur le dispositif NSX Manager, exécutez la commande `get certificate api thumbprint`.

La sortie de la commande est une chaîne alphanumérique propre à ce dispositif NSX Manager.

Par exemple :

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

- 4 Sur le dispositif NSX Edge, exécutez la commande **join management-plane**.

Fournissez les informations suivantes :

- Nom d'hôte ou adresse IP du dispositif NSX Manager avec numéro de port facultatif

- Nom du dispositif NSX Manager
- Empreinte numérique de certificat du dispositif NSX Manager
- Mot de passe du dispositif NSX Manager

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

Répétez cette commande sur chaque nœud NSX Edge.

- 5 Vérifiez le résultat en exécutant la commande `get managers` sur vos dispositifs NSX Edge.

```
nsx-edge-1> get managers  
- 10.172.165.163 Connected  
  
- 10.172.165.164 Standby  
  
- 10.172.165.165 Standby
```

- 6 Dans l'interface utilisateur de NSX Manager, sélectionnez la page **Système > Nœuds d'infrastructure > Clusters Edge > Nœuds**.

La connectivité doit être activée. Si la connectivité n'est pas activée, essayez d'actualiser l'écran du navigateur.

Fournir des données pour les problèmes de configuration

Une fois que vous avez vérifié les informations de migration et que vous êtes prêt à procéder à la migration, vous pouvez fournir des données pour les problèmes de configuration signalés. Les données que vous fournissez déterminent la façon dont l'environnement de NSX-T est configuré.

Pour consulter des exemples de problèmes de configuration et les données requises, y compris l'installation du nœud Edge, reportez-vous à la section [Exemple de problèmes de configuration](#).

Note Pour certaines fonctionnalités de NSX for vSphere, il peut y avoir des configurations automatiques telles que des certificats présents. Si ces configurations sont destinées à des fonctionnalités qui ne sont pas prises en charge pour la topologie spécifique, ces configurations automatiques sont signalées comme des problèmes qui doivent être ignorés lors de la migration. Par exemple, dans les topologies qui ne prennent pas en charge les services L4-L7 sur les passerelles de services Edge, les certificats présents pour VPN et DNS déclenchent des problèmes pour ignorer ces configurations de la migration.

Conditions préalables

- Vérifiez que vous avez examiné tous les problèmes et les messages de migration, et que vous êtes prêt à poursuivre la migration.

- Tous les problèmes de blocage et autres problèmes nécessitant une modification du NSX for vSphere doivent être résolus.

Important Si, pour une raison quelconque, vous avez apporté une modification à l'environnement NSX for vSphere depuis la dernière importation de la configuration, vous devez relancer la migration. C'est le cas, par exemple, si vous avez connecté une nouvelle machine virtuelle à un commutateur logique, modifié une règle de pare-feu ou installé NSX for vSphere sur de nouveaux hôtes. Reportez-vous à la section [Apporter des modifications à l'environnement NSX for vSphere](#) pour plus d'informations sur le redémarrage de la migration.

Procédure

- 1 Dans la page **Résoudre la configuration**, cliquez sur chaque problème et fournir les données.

Chaque problème peut concerner plusieurs éléments de configuration. Pour chaque élément, il peut exister une ou plusieurs résolutions possibles au problème (ignorer, configurer ou sélectionner une valeur spécifique, par exemple).

Lorsqu'un problème s'applique à plusieurs éléments de configuration, vous pouvez fournir des données pour chaque élément individuellement, ou bien les sélectionner tous et fournir une réponse pour tous les éléments.

Plusieurs personnes peuvent fournir les données via différentes sessions. Vous pouvez revenir sur un commentaire envoyé pour le modifier.

- 2 Une fois les données fournies, le bouton **Envoyer** s'affiche sur la page **Résoudre la configuration**. Cliquez sur **Envoyer** pour enregistrer votre progression.
- 3 Une fois que vous avez fourni les données pour tous les problèmes de configuration, cliquez sur **Envoyer**.

L'entrée est validée. Si certaines données ne sont pas valides, vous êtes invité à les mettre à jour. Vous devrez peut-être fournir des données supplémentaires pour certains éléments de configuration.

- 4 Après avoir envoyé tous les données demandées, cliquez sur **Continuer** pour passer à l'étape de migration de la configuration.

Exemple de problèmes de configuration

Vous devez fournir des données sur un grand nombre de problèmes, y compris les détails de configuration pour les nouveaux nœuds Edge de NSX-T.

Lors de l'étape **Résoudre la configuration**, vous fournissez des informations sur les nœuds Edge que vous avez créés pour remplacer vos passerelles Edge Services Gateways NSX for vSphere. La configuration peut être modifiée pour fonctionner correctement sur NSX-T. Vous devrez utiliser une autre adresse IP et VLAN que celle utilisée dans NSX for vSphere.

Migration de la passerelle Edge Services Gateway avec les services L4-L7

L'utilisation de la même interface pour la liaison montante du routeur et des services tels que VPN est prise en charge dans NSX for vSphere. Cette configuration n'est pas prise en charge dans NSX-T. Vous pouvez attribuer de nouvelles adresses IP pour les liaisons montantes des nœuds Edge pour ne pas avoir à modifier l'adresse IP pour les services en cours d'exécution sur le nœud Edge.

Migration de la passerelle Edge Services Gateway dans une configuration à haute disponibilité

La topologie de NSX for vSphere qui contient des passerelles Edge Services Gateway dans une configuration à haute disponibilité peut comporter une passerelle Edge Services Gateway avec deux liaisons montantes connectées à deux groupes de ports distribués différents sur différents réseaux.

Dans NSX-T, cette configuration est remplacée par deux nœuds Edge, tous deux doivent disposer de leurs liaisons montantes sur le même réseau.

Par exemple, une passerelle Edge Services Gateway avec HA peut avoir cette configuration :

- vnic1 a l'adresse IP 192.178.14.2/24 et est associé à un groupe de ports Public-DVPG qui utilise le VLAN 11.
- vnic4 a l'adresse IP 192.178.44.2/24 et est associé à un groupe de ports Public-DVPG-2 qui utilise le VLAN 15.

Pour fonctionner après la migration, au moins une de ces adresses IP doit être modifiée, car elles doivent toutes les deux être sur le même réseau.

Voici un exemple des informations qui peuvent être fournies lors de l'étape Résoudre la configuration.

Pour le premier nœud Edge :

- L'ID d'infrastructure est fa3346d8-2502-11e9-8013-000c2936d594.
- L'adresse IP est 192.178.14.2/24.
- Le VLAN est à 11.

Pour le second nœud Edge :

- L'ID d'infrastructure est fa2de198-2502-11e9-9d7a-000c295cfc6.
- L'adresse IP est 192.178.14.4/24.
- Vous n'avez pas besoin de fournir le VLAN étant donné que le VLAN utilisé pour le premier nœud est supposé.

Les deux nœuds Edge doivent avoir une connectivité à ce réseau.

Migrer la configuration de NSX Data Center for vSphere

Une fois que vous avez résolu tous les problèmes de configuration, vous pouvez migrer la configuration. Lorsque la configuration est migrée, les modifications de configuration sont effectuées dans

l'environnement du dispositif NSX-T pour répliquer la configuration de NSX for vSphere. Aucune modification de configuration n'est effectuée dans l'environnement de NSX for vSphere.

Attention Dans NSX-T Data Center 2.4.0, il existe un bouton **Restauration** pour certaines étapes de la migration. L'utilisation du bouton **Restauration** peut entraîner un comportement inattendu. Au lieu de cela, utilisez le bouton **Annuler** pour annuler la migration à l'étape **Importer une configuration** ou **Migrer la configuration**. Si vous avez migré des nœuds Edge et que vous devez les restaurer, contactez le support VMware.

Pour plus d'informations, reportez-vous à la section [Annuler ou redémarrer la migration de NSX for vSphere](#).

Conditions préalables

Vérifiez que vous avez effectué l'étape **Résoudre les problèmes**.

Procédure

- 1 Dans la page **Migrer la configuration**, cliquez sur **Démarrer**.
La configuration de NSX for vSphere est migrée vers le dispositif NSX-T.
- 2 Vérifiez que toutes les configurations de NSX for vSphere sont affichées sur l'interface de NSX Manager du dispositif NSX-T ou sur l'API.

Important Lorsque la configuration est migrée vers le dispositif NSX-T, les modifications de configuration sont effectuées dans la base de données NSX Manager du dispositif NSX-T, mais cela peut prendre un certain temps avant que la configuration ne prenne effet. Vous devez vérifier que toutes les configurations prévues de NSX for vSphere s'affichent dans l'interface NSX Manager du dispositif NSX-T ou dans l'API avant de procéder à l'étape **Migrer les dispositifs Edge**. Par exemple, la configuration du pare-feu, les commutateurs logiques et les zones de transport.

Modifier la configuration du dispositif Edge avant la migration des dispositifs Edge

Lorsque les passerelles Edge Services de NSX for vSphere sont migrées vers NSX-T, une configuration par défaut est utilisée pour les paramètres MTU d'interface. Si vous souhaitez modifier cette valeur par défaut, vous pouvez le faire avant de démarrer l'étape **Migrer les dispositifs Edge**.

Les paramètres personnalisés de la MTU dans les interfaces de routage des passerelles Edge Services ne sont pas migrées vers NSX-T. Les interfaces de routeur logique créées dans NSX-T utilisent le paramètre de la MTU globale par défaut, qui est 1500. Si vous souhaitez vous assurer que toutes les interfaces de routeur logique ont une MTU supérieure, vous pouvez modifier le paramètre de la MTU globale par défaut. Vous pouvez également modifier les MTU d'interface au cas par cas.

Procédure

- 1 Utilisez GET `/api/v1/global-configs/RoutingGlobalConfig` pour récupérer la configuration actuelle.
- 2 Modifiez la valeur de la MTU globale par défaut : `logical_uplink_mtu`

- 3 Utilisez PUT `/api/v1/global-configs/RoutingGlobalConfig` pour effectuer la modification de la configuration.

Migrer les dispositifs Edge NSX Data Center for vSphere

Après la migration de la configuration, vous pouvez migrer les services Edge de NSX for vSphere vers NSX-T. Il s'agit de la première étape de la migration qui modifie votre environnement de production.

Si vous migrez une topologie de microsegmentation supportée par VLAN, vous n'avez aucun dispositif Edge Service Gateway à migrer. Vous devez toujours cliquer sur **Démarrer** afin de procéder à l'étape **Migrer les hôtes**.

Attention Dans NSX-T Data Center 2.4.0, il existe un bouton **Restauration** pour certaines étapes de la migration. L'utilisation du bouton **Restauration** peut entraîner un comportement inattendu. Au lieu de cela, utilisez le bouton **Annuler** pour annuler la migration à l'étape **Importer une configuration** ou **Migrer la configuration**. Si vous avez migré des nœuds Edge et que vous devez les restaurer, contactez le support VMware.

Pour plus d'informations, reportez-vous à la section [Annuler ou redémarrer la migration de NSX for vSphere](#).

Conditions préalables

- Tous les problèmes de configuration doivent être résolus.
- La configuration doit être migrée.
- Vérifiez que vous disposez d'une sauvegarde de NSX for vSphere et de vSphere, car les modifications de configuration les plus récentes ont été apportées.
- Vérifiez que toutes les configurations de NSX for vSphere que vous vous attendiez à migrer s'affichent sur l'interface du dispositif NSX Manager NSX-T ou sur l'API.
- Si vous utilisez des nouvelles adresses IP pour les liaisons montantes de NSX-T Edge nœud, vous devez configurer les routeurs ascendants avec ces nouvelles adresses IP BGP voisines.

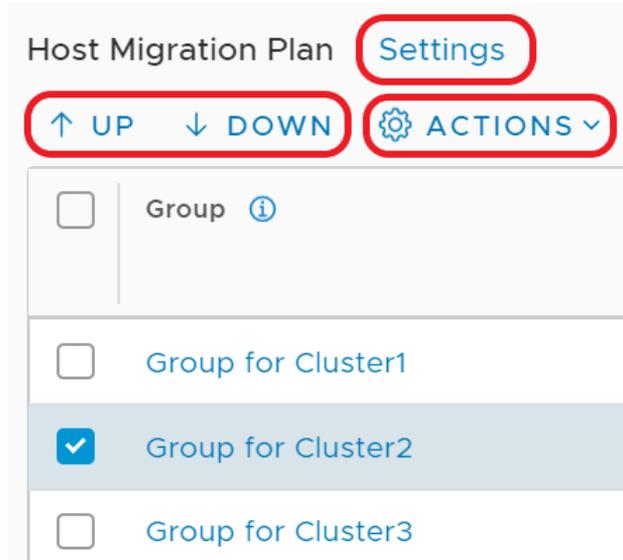
Procédure

- ◆ Dans la page **Migrer les dispositifs Edge**, cliquez sur **Démarrer**.

Tous les dispositifs Edge sont migrés. Les liaisons montantes sur les passerelles NSX for vSphere Edge Services Gateway sont désactivées, et les liaisons montantes sur les nœuds Edge NSX-T sont mises en ligne.

Configuration de la migration d'hôtes

Les clusters de l'environnement NSX for vSphere s'affichent sur la page **Migrer les hôtes**. Les clusters sont organisés en groupes de migration, chaque groupe de migration contenant un cluster d'hôtes vSphere. Plusieurs paramètres contrôlent la migration de l'hôte.



- Cliquez sur **Paramètres** pour modifier les paramètres globaux : **Pause entre les groupes** et **Ordre de migration entre les groupes**.
- Sélectionnez un seul groupe d'hôtes (cluster) et utilisez les flèches pour le déplacer vers le haut ou vers le bas dans la séquence de migration.
- Sélectionnez un ou plusieurs groupes d'hôtes (clusters) et cliquez sur **Actions** pour modifier les paramètres de ces groupes d'hôtes : **Ordre de migration au sein des groupes** et **État de migration**.

Pause entre les groupes

Pause entre les groupes est un paramètre global qui s'applique à tous les groupes d'hôtes. Si la suspension est activée, le coordinateur de migration migre un groupe d'hôtes, puis attend une entrée. Vous devez cliquer sur **Continuer** pour passer au groupe d'hôtes suivant. Si vous souhaitez vérifier l'état de chaque cluster avant de passer au suivant, activez **Pause entre les groupes**.

Pause entre les groupes est désactivé par défaut.

Ordre de migration séquentiel ou parallèle

Vous pouvez définir si la migration s'effectue dans un ordre séquentiel ou parallèle. Il existe deux paramètres de commande :

- **Ordre de migration entre les groupes**

Ordre de migration entre les groupes est un paramètre global qui s'applique à tous les groupes d'hôtes.

- **Série** : un groupe d'hôtes (cluster) est migré à la fois.
- **Parallèle** : jusqu'à cinq groupes d'hôtes sont migrés à la fois. Après la migration de ces cinq groupes d'hôtes, le lot suivant de cinq groupes d'hôtes maximum est migré.

- **Ordre de migration au sein du groupe**

Ordre de migration au sein du groupe est un paramètre spécifique à un groupe d'hôtes (cluster) qui peut donc être configuré séparément sur chaque groupe d'hôtes.

- **Série** : un hôte au sein du groupe d'hôtes (cluster) est migré à la fois.
- **Parallèle** : jusqu'à cinq hôtes dans le groupe d'hôtes sont migrés à la fois. Une fois ces hôtes migrés, le lot suivant de cinq hôtes maximum est migré.

Par défaut, les deux paramètres sont définis sur **Série**. Ensemble, les paramètres déterminent le nombre d'hôtes migrés à la fois.

Tableau 1-11. Effets des paramètres de migration sur le nombre d'hôtes tentant de migrer simultanément

Ordre de migration entre les groupes (Clusters)	Ordre de migration au sein des groupes (clusters)	Nombre maximal d'hôtes tentant la migration simultanément
Série	Série	1 Un hôte d'un groupe d'hôtes
Série	Parallèle	5 Cinq hôtes d'un groupe d'hôtes
Parallèle	Série	5 Un hôte de cinq groupes d'hôtes
Parallèle	Parallèle	25 Cinq hôtes à partir de cinq groupes d'hôtes

Important En cas d'échec de migration d'un hôte, le processus de migration s'interrompt une fois toutes les migrations d'hôtes en cours terminées. Si **Parallèle** est sélectionné pour la migration entre les groupes et la migration au sein des groupes, il peut y avoir une longue interruption de l'hôte ayant échoué avant de pouvoir effectuer une nouvelle tentative de migration. Dans un environnement de production, ne sélectionnez pas l'ordre de migration parallèle au sein des groupes.

Séquence de groupes de migration

Vous pouvez sélectionner un groupe d'hôtes (cluster) et utiliser les flèches pour le déplacer vers le haut ou vers le bas dans la liste des groupes.

Si la migration d'un hôte échoue, vous pouvez déplacer son groupe d'hôtes en bas de la liste des groupes. La migration d'autres groupes d'hôtes peut continuer pendant que vous résolvez le problème de l'hôte posant problème.

Activer ou désactiver les groupes

Les groupes d'hôtes (clusters) peuvent avoir l'un des trois états suivants :

- **Activé**

Les hôtes de ces groupes sont migrés vers NSX-T lorsque vous cliquez sur **Démarrer** sur la page **Migrer les hôtes**.
- **Désactivé**

Les hôtes de ces groupes ne sont pas migrés vers NSX-T lorsque vous cliquez sur **Démarrer** sur la page **Migrer les hôtes**. Cependant, si vous n'avez pas encore cliqué sur **Terminer** pour la migration, vous pouvez revenir à la page **Migrer les hôtes** pour les activer et redémarrer la migration de l'hôte. Terminez toutes les tâches de migration d'hôte et cliquez sur **Terminer** dans la même fenêtre de maintenance.

■ **Ne pas migrer**

Les hôtes de ces groupes ont été identifiés pendant l'étape **Résoudre la configuration** comme n'étant pas éligibles pour la migration.

Par exemple, les hôtes sur lesquels NSX for vSphere n'est pas installé ont l'état **Ne pas migrer**.

Si vous souhaitez éviter la migration des machines virtuelles d'infrastructure comme NSX Manager, NSX Controller, la passerelle Edge Services Gateway ou le routeur logique distribué, vous pouvez désactiver la migration de leurs clusters.

Migrer les hôtes NSX Data Center for vSphere

Une fois que vous avez migré des dispositifs Edge vers NSX-T et vérifié que le routage et les services fonctionnent correctement, vous pouvez migrer vos hôtes NSX for vSphere aux nœuds de transport hôtes NSX-T.

Vous pouvez configurer plusieurs paramètres relatifs à la migration d'hôtes, y compris l'ordre de migration et l'activation des hôtes. Avant de changer les paramètres par défaut, assurez-vous de comprendre les effets de ces paramètres. Pour plus d'informations, reportez-vous à la section [Configuration de la migration d'hôtes](#).

Pendant la migration de l'hôte, les modifications suivantes sont effectuées :

- Le logiciel NSX for vSphere est désinstallé.
- Le logiciel NSX-T est installé.
- Les hôtes sont configurés avec un N-VDS pour remplacer les commutateurs distribués (Distributed Switch) vSphere :
 - Chaque N-VDS est créé avec un nom qui fait référence au nom de Distributed Switch. Par exemple, Distributed Switch ComputeSwitchA est créé en tant que N-VDS `nvds.ComputeSwitchA`.
 - Si différents clusters utilisent des commutateurs distribués (Distributed Switch) différents pour soutenir des commutateurs logiques, un N-VDS est créé avec un nom qui associe tous les noms de Distributed Switch. Par exemple, si `ComputeCluster1` et `ComputeCluster2` utilisent Distributed Switch `ComputeSwitchA` pour soutenir des commutateurs logiques et que `ComputeCluster3` utilise `ComputeSwitchB` pour soutenir des commutateurs logiques, le N-VDS est créé sous la forme `nvds.ComputeSwitchA.ComputeSwitchB`.
- Les PNIC, vmk et VTEP de Distributed Switch sont migrés vers N-VDS.

- Les machines virtuelles connectées aux commutateurs distribués (Distributed Switch) sont connectés au N-VDS.

Attention Pendant la migration de l'hôte, il existe une interruption du trafic. La migration d'hôtes doit être terminée dans la même fenêtre de maintenance que la migration Edge.

Si vous avez des règles de pare-feu distribué qui sont appliquées à une machine virtuelle, ces règles ne sont pas poussées vers l'hôte tant que l'hôte et toutes ses machines virtuelles n'ont pas migré. Jusqu'à ce que les règles soient poussées vers l'hôte, les points suivants s'appliquent :

- Si vous utilisez la mise en liste verte (la règle par défaut est deny), votre application est hors ligne.
- Si vous utilisez la mise en liste noire (la règle par défaut est accept), la machine virtuelle n'est pas protégée par les règles Appliqué à.

Si la migration d'un hôte échoue, elle s'interrompt une fois toutes les migrations d'hôte en cours terminées. Une fois le problème avec l'hôte résolu, cliquez sur **Réessayer** pour retenter la migration de l'hôte échouée.

Si la migration d'un hôte échoue, vous pouvez déplacer son groupe d'hôtes en bas de la liste des groupes. La migration d'autres groupes d'hôtes peut continuer pendant que vous résolvez le problème de l'hôte posant problème.

Après que l'hôte a migré vers NSX-T, il est possible que vous aperceviez une alarme avec le message **Connectivité réseau perdue**. Cette alarme se produit, car l'hôte ne possède plus de carte réseau/NIC connectée au vSphere Distributed Switch auquel il était précédemment connecté.

Conditions préalables

- Vérifiez que la migration Edge est terminée et que tous les services de routage fonctionnent correctement.
- Vérifiez que tous les hôtes ESXi sont dans un état opérationnel. Résolvez les problèmes impliquant des hôtes, y compris les états déconnectés. Aucun redémarrage ni aucune tâche ne doit être en attente pour passer en mode de maintenance.

Note Les hôtes ne passent en mode de maintenance pendant la migration.

Procédure

- ◆ Cliquez sur **Démarrer** pour démarrer la migration de l'hôte.

Les hôtes NSX for vSphere sont convertis en nœuds de transport hôtes NSX-T. Les interfaces réseau des machines virtuelles sur les hôtes sont déconnectées des commutateurs logiques NSX for vSphere et connectées aux segments NSX-T.

Terminer la migration NSX Data Center for vSphere

Après avoir migré tous les dispositifs Edge et les hôtes vers l'environnement NSX-T Data Center, vérifiez que le nouvel environnement fonctionne correctement. Si tout fonctionne correctement, vous pouvez terminer la migration.

Important Vérifiez que tout fonctionne et cliquez sur **Terminer** dans la fenêtre de maintenance. Lorsque vous cliquez sur **Terminer**, un nettoyage post-migration est opéré. Ne laissez pas le coordinateur de migration dans un état inachevé au-delà de la fenêtre de la migration.

Après la migration, des erreurs apparaîtront sur les hôtes. Le message d'erreur est le suivant :
'UserVars.RmqHostId' est non valide ou dépasse le nombre maximum de caractères autorisés. Cette erreur indique que l'hôte appartient encore à l'inventaire de NSX Data Center for vSphere.

Conditions préalables

- Vérifiez que tous les éléments prévus ont été migrés vers l'environnement NSX-T Data Center.
- Vérifiez que l'environnement NSX-T Data Center fonctionne correctement.

Procédure

- 1 Accédez à la page **Migrer les hôtes** du coordinateur de migration.
- 2 Cliquez sur **Terminer**.

Une boîte de dialogue s'affiche pour vous permettre de confirmer que vous souhaitez terminer la migration. Si vous terminez la migration, tous les détails de celle-ci s'effaceront. Vous ne pourrez plus réviser ses paramètres, tels que les données entrées à la page **Résoudre les problèmes**, ou encore les hôtes exclus de la migration.

Étape suivante

Si vous avez migré depuis NSX for vSphere 6.4.4, effectuez un redémarrage de tous les hôtes ayant migré vers NSX-T. Cette opération doit être effectuée avant de procéder à la mise à niveau vers une version ultérieure de NSX-T.

Désinstallation de NSX for vSphere après la migration

Après avoir vérifié que la migration a réussi et cliqué sur **Terminer** pour terminer la migration, vous pouvez désinstaller votre environnement NSX for vSphere.

Le processus de désinstallation de NSX for vSphere après la migration vers NSX-T est différent de la désinstallation standard de NSX for vSphere.

Conditions préalables

- Vérifiez que la migration est réussie et que toutes les fonctionnalités fonctionnent dans l'environnement NSX-T.
- Vérifiez que vous avez cliqué sur **Terminer** sur la page **Migrer les hôtes**.

Procédure

- 1 Supprimez les agences ESX Agent Manager associées à l'environnement NSX for vSphere.
 - a Dans vSphere Client, accédez à **Menu > Administration**. Sous **Solutions**, cliquez sur **Extensions vCenter Server**. Double-cliquez sur **vSphere ESX Agent Manager** puis cliquez sur l'onglet **Configurer**.
 - b Pour chaque agence dont le nom commence par `_NSX_`, sélectionnez l'agence, puis cliquez sur le menu à trois points (⋮) et sélectionnez **Supprimer l'agence**.
- 2 Supprimez le plug-in NSX de vCenter.
 - a Accédez au gestionnaire d'extensions depuis le navigateur d'objets gérés à l'adresse `https://<vcenter-ip>/mob/?moid=ExtensionManager`.
 - b Cliquez sur **UnregisterExtension**.
 - c Dans la boîte de dialogue **UnregisterExtension**, entrez `com.vmware.vShieldManager` dans la zone de texte **Valeur** et cliquez sur **Appeler la méthode**.
 - d Dans la boîte de dialogue **UnregisterExtension**, entrez `com.vmware.nsx.ui.h5` dans la zone de texte **Valeur** et cliquez sur **Appeler la méthode**.
 - e Vous pouvez vérifier que vous avez annulé l'enregistrement des extensions en accédant à la page du gestionnaire d'extensions à l'adresse `https://<vcenter-ip>/mob/?moid=ExtensionManager` et en affichant les valeurs de la propriété **extensionList**.

3 Supprimez les répertoires vSphere Web Client et vSphere Client (HTML5) pour NSX for vSphere, puis redémarrez les services du client.

a Connectez-vous à la ligne de commande du système vCenter Server.

- Si vous utilisez un dispositif vCenter Server, connectez-vous en tant qu'utilisateur racine à l'aide de la console ou de SSH. Vous devez vous connecter en tant qu'utilisateur racine et exécuter les commandes à partir de l'interpréteur en ligne de commande Bash. Vous pouvez démarrer l'interpréteur en ligne de commande Bash à l'aide de la commande suivante :

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

- Si vous utilisez vCenter Server pour Windows, connectez-vous en tant qu'administrateur à l'aide de la console ou de RDP.

b Supprimez tous les répertoires du plug-in NSX for vSphere.

Note Un répertoire de plug-in peut ne pas être présent si vous n'avez jamais lancé le client associé.

Sur le dispositif vCenter Server, supprimez les répertoires suivants :

- Pour supprimer le plug-in vSphere Web Client, supprimez le répertoire `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/com.vmware.vShieldManager-<version>-<build>`.
- Pour supprimer le plug-in vSphere Client, supprimez le répertoire `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/com.vmware.nsx.ui.h5-<version>-<build>`.

Sur vCenter Server pour Windows, supprimez les répertoires suivants :

- Pour supprimer le plug-in vSphere Web Client, supprimez le répertoire `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity\com.vmware.vShieldManager-<version>-<build>`.
- Pour supprimer le plug-in vSphere Client, supprimez le répertoire `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity\com.vmware.nsx.ui.h5-<version>-<build>`.

c Redémarrez les services du client sur le dispositif vCenter Server ou vCenter Server sous Windows.

Tableau 1-12. Commandes du service client

Service client	vCenter Server Appliance	vCenter Server pour Windows
Redémarrer vSphere Web Client	<pre># service-control --stop vsphere-client # service-control --start vsphere-client</pre>	<pre>> cd C:\Program Files\VMware \vCenter Server\bin</pre>

Tableau 1-12. Commandes du service client (suite)

Service client	vCenter Server Appliance	vCenter Server pour Windows
		<pre>> service-control --stop vspherewebclientsvc > service-control --start vspherewebclientsvc</pre>
Redémarrer vSphere Client	<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 Mettez les dispositifs NSX for vSphere hors tension et supprimez-les.

- a Accédez à **Accueil > Hôtes et clusters**.
- b Localisez les machines virtuelles du dispositif NSX for vSphere suivantes. Sur chaque machine virtuelle, cliquez avec le bouton droit et sélectionnez **Mettre hors tension**, puis cliquez avec le bouton droit et sélectionnez **Supprimer du disque**.
 - Machines virtuelles NSX Edge.
 - Machines virtuelles NSX Controller.
 - Machine virtuelle NSX Manager.

Dépannage de la migration NSX Data Center for vSphere

Vous pouvez voir des erreurs lors de l'exécution de la migration de NSX Data Center for vSphere. Ces informations de dépannage peuvent aider à résoudre les problèmes.

Accéder au coordinateur de migration

Problème	Solution
<p>Le coordinateur de migration n'est pas visible à Système > Migrer.</p>	<p>Vérifiez si le service de coordinateur de migration est en cours d'exécution sur NSX Manager.</p> <pre data-bbox="810 359 1428 489">manager> get service migration-coordinator Service name: migration-coordinator Service state: running</pre> <p>Si le service n'est pas en cours d'exécution, démarrez-le avec <code>start service migration-coordinator</code>.</p>
<p>Lors du retour au coordinateur de migration, la migration en cours n'est pas visible.</p>	<p>Le coordinateur de migration ne stocke pas les informations d'identification de vCenter Server ou NSX Manager. Si le service de coordinateur de migration est redémarré lorsqu'une migration est en cours, la page Système > Migrer peut afficher des informations de configuration périmées ou aucune information sur le programme d'installation. Pour afficher le dernier état de migration si le service de coordinateur de migration est redémarré, procédez comme suit :</p> <ol style="list-style-type: none"> 1 Actualisez la page Système > Migrer. 2 Cliquez sur Démarrer et entrez les informations d'identification de vCenter Server et NSX Manager.

Importer les problèmes de configuration

Problème	Solution
<p>La configuration de l'importation échoue.</p>	<ol style="list-style-type: none"> 1 Cliquez sur Réessayer pour essayer à nouveau d'importer. Seules les étapes d'importation ayant échoué sont réessayées.

Problèmes de migration de l'hôte

Problème	Solution
<p>La migration vers un hôte échoue en raison d'une configuration du gestionnaire de calcul manquante.</p>	<p>La configuration du gestionnaire de calcul est une condition préalable pour la migration. Cependant, si la configuration du gestionnaire de calcul est supprimée du dispositif NSX Manager après le démarrage de la migration, le coordinateur de migration conserve le paramètre. La migration se poursuit jusqu'à ce l'étape de migration de l'hôte, qui échoue.</p> <p>Ajoutez un gestionnaire de calcul à NSX Manager et entrez les mêmes détails de vCenter Server utilisés pour l'importation de la configuration initiale de NSX for vSphere.</p>
<p>La migration de l'hôte échoue en raison de dvFilters périmés présents.</p> <p>Exemple de message d'erreur : Stale dvFilters present: ['port 33554463 (disconnected)', 'port 33554464 (disconnected)'] Stale dvfilters present. Aborting]</p>	<p>Connectez-vous à l'hôte qui n'a pas pu migrer, identifiez les ports déconnectés, et redémarrez la machine virtuelle appropriée ou connectez les ports déconnectés. Recommencez l'étape de la Migration de l'hôte.</p> <ol style="list-style-type: none"> 1 Connectez-vous à l'interface de ligne de commande de l'hôte qui n'a pas pu migrer. 2 Exécutez <code>summarize-dvfilter</code> et recherchez les ports signalés dans le message d'erreur. <pre style="background-color: #f0f0f0; padding: 10px;">world 1000057161 vmm0:2-vm_RHEL- srv5.6.0.9-32-local-258-963adcb8-ab56-41d6- bd9e-2d1c329e7745 vcluid:'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 Localisez la machine virtuelle et le port concernés. <p>Par exemple, le message d'erreur indique que le port 33554463 est déconnecté.</p> <ol style="list-style-type: none"> a Recherchez la section de la sortie de <code>summarize-dvfilter</code> qui correspond à ce port. Le nom de la machine virtuelle est répertorié ici. Dans ce cas, il s'agit de <code>2-vm_RHEL-srv5.6.0.9-32-local-258-963adcb8-ab56-41d6-bd9e-2d1c329e7745</code>. b Recherchez l'entrée de <code>name</code> déterminer quelle interface de machine virtuelle est déconnectée. Dans ce cas, il s'agit de <code>eth1</code>. Par conséquent, la seconde interface de <code>2-vm_RHEL-srv5.6.0.9-32-local-258-963adcb8-ab56-41d6-bd9e-2d1c329e7745</code> est déconnectée. <ol style="list-style-type: none"> 4 Résolez le problème avec ce port. Effectuez l'une des étapes suivantes : <ul style="list-style-type: none"> ■ Redémarrez la machine virtuelle affectée. ■ Connectez le port vnic déconnecté à n'importe quel réseau.

Problème	Solution
	5 Sur la page Migrer les hôtes , cliquez sur Réessayer .

Migration de la mise en réseau vSphere

2

Vous pouvez utiliser le coordinateur de migration pour migrer la configuration d'un vSphere Distributed Switch existant vers un environnement NSX-T Data Center.

Le coordinateur de migration déplace les dispositifs de renforcement de vSphere Distributed Switch, des hôtes de calcul, des PNIC, des vmkNIC et des vNIC vers le N-VDS.

Note Vous pouvez utiliser le coordinateur de migration pour migrer les configurations de vSphere Distributed Switch vers NSX-T uniquement si NSX for vSphere n'est pas installé sur l'hôte.

Ce chapitre contient les rubriques suivantes :

- [Présentation de la migration de la Mise en réseau vSphere](#)
- [Préparation de la migration de la Mise en réseau vSphere](#)
- [Migrer la mise en réseau vSphere vers NSX-T Data Center](#)

Présentation de la migration de la Mise en réseau vSphere

Vous pouvez migrer un Distributed Switch vSphere à la fois vers NSX-T.

Présentation du processus de migration

Lors de la migration, vous allez effectuer les étapes suivantes :

- Préparez votre environnement NSX-T.
 - Configurez un gestionnaire de calcul dans l'environnement NSX-T. Ajoutez le système de vCenter Server qui gère le vSphere Distributed Switch que vous souhaitez migrer.
 - Démarrez le service de coordinateur de migration.
- Importez la configuration à partir de vSphere.
 - Entrez les détails de votre environnement vSphere.
 - La configuration est récupérée et les vérifications préalables sont exécutées.
- Sélectionnez le vSphere Distributed Switch que vous souhaitez migrer.
- Résolvez les problèmes liés à la configuration.

Avant de pouvoir migrer votre environnement vSphere vers NSX-T, fournissez des réponses aux questions de configuration à résoudre. La résolution des problèmes peut être effectuée en plusieurs passes et par plusieurs personnes.

- Migrez la configuration.
 - Une fois tous les problèmes de configuration résolus, vous pouvez importer la configuration vers NSX-T. Les modifications de configuration sont effectuées sur NSX-T, mais à ce stade, aucune modification n'est apportée à l'environnement vSphere.
- Migrez les hôtes.
 - Le logiciel du dispositif NSX-T est installé sur les hôtes. Les interfaces des machines virtuelles sont déconnectées des groupes de ports des vSphere Distributed Switch et connectées aux nouveaux segments NSX-T.

Attention Pendant la migration de chaque hôte, il existe une interruption du trafic.

- Terminez la migration.
 - Après avoir vérifié que la mise en réseau migrée fonctionne correctement, vous pouvez cliquer sur **Terminer** pour effacer l'état de migration. Vous pouvez maintenant migrer un autre vSphere Distributed Switch vers le dispositif NSX-T.

Préparation de la migration de la Mise en réseau vSphere

Vous pouvez migrer des vSphere Distributed Switches qui ne font pas partie d'un environnement NSX Data Center for vSphere.

Logiciels et versions requises

- Reportez-vous aux *matrices d'interopérabilité de VMware* pour connaître les versions de vCenter Server et d' ESXi : http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php#interop&175=&1=&2=
- Les versions 6.5.0 et 6.6.0 de vSphere Distributed Switch sont prises en charge.

Ajouter un gestionnaire de calcul

Pour migrer un vSphere Distributed Switch, vous devez configurer le système vCenter Server associé en tant que gestionnaire de calcul dans NSX-T avant de pouvoir démarrer le processus de migration.

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Système > Infrastructure > Gestionnaires de calcul > Ajouter**.

3 Indiquez les détails des gestionnaires de calcul.

Option	Description
Nom et description	Tapez le nom pour identifier l'instance de vCenter Server. Vous pouvez éventuellement indiquer des détails, tels que le nombre de clusters dans l'instance de vCenter Server.
Nom de domaine/adresse IP	Tapez l'adresse IP de l'instance de vCenter Server.
Type	Conservez l'option par défaut.
Nom d'utilisateur et mot de passe	Tapez les informations d'identification de connexion de vCenter Server.
Empreinte numérique	Tapez la valeur de l'algorithme d'empreinte numérique SHA-256 de vCenter Server.

Si la valeur d'empreinte est vide, vous êtes invité à accepter l'empreinte numérique du serveur fournie.

Une fois que vous acceptez l'empreinte numérique, quelques secondes sont nécessaires pour que NSX-T Data Center découvre et enregistre les ressources de vCenter Server.

4 Si l'icône de progression passe de **En cours** à **Non enregistré**, suivez les étapes décrites ci-dessous pour résoudre l'erreur.

- a Sélectionnez le message d'erreur et cliquez sur **Résoudre**. Un message d'erreur possible est le suivant :

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

- b Entrez les informations d'identification de vCenter Server et cliquez sur **Résoudre**.
S'il existe déjà un enregistrement, il sera remplacé.

Migrer la mise en réseau vSphere vers NSX-T Data Center

Utilisez le coordinateur de migration pour importer votre configuration, résoudre les problèmes de configuration et migrer des hôtes vers votre environnement NSX-T Data Center.

Importer la configuration de la mise en réseau vSphere

Pour migrer la mise en réseau et les hôtes vSphere vers NSX-T Data Center, vous devez fournir les détails de votre environnement vSphere.

Le service de coordinateur de migration s'exécute sur un seul nœud du dispositif NSX Manager. Effectuez toutes les opérations de migration à partir du nœud qui exécute le service de coordinateur de migration.

Conditions préalables

- Vérifiez que le système vCenter Server associé au vSphere Distributed Switch que vous voulez migrer est enregistré en tant que gestionnaire de calcul. Reportez-vous à la section [Ajouter un gestionnaire de calcul](#).

Procédure

- 1 Connectez-vous à une interface de ligne de commande NSX Manager en tant qu'**administrateur** et démarrez le service de coordinateur de migration.

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

- 2 À partir d'un navigateur, connectez-vous au nœud du dispositif NSX Manager qui exécute le service de coordinateur de migration. Connectez-vous en utilisant un compte doté de privilèges admin.
- 3 Accédez à **Système > Migrer**.
- 4 Dans le volet **Migrer la mise en réseau vSphere**, cliquez sur **Démarrer**.
- 5 Sur la page **Importer une configuration**, cliquez sur **Sélectionner vSphere** et fournissez les informations demandées sur votre environnement vSphere.

Note Le menu déroulant de vCenter affiche tous les systèmes de vCenter Server qui sont enregistrés comme gestionnaires de calcul. Cliquez sur **Ajouter nouveau** si vous avez besoin d'ajouter un gestionnaire de calcul.

- 6 Cliquez sur **Démarrer** pour importer la configuration.
- 7 Une fois l'importation terminée, cliquez sur **Continuer** pour passer à la page **Résoudre les problèmes**.

Annuler ou redémarrer la migration de la mise en réseau vSphere

Un bouton **Annuler** se trouve sur chaque page de la migration. L'annulation d'une migration supprime tous les états de migration à partir du système.

Attention N'annulez pas une migration si la migration de l'hôte a démarré. L'annulation de la migration supprime tous les états de migration et vous empêche d'afficher les progrès antérieurs.

Si vous avez importé votre configuration, mais que vous n'avez pas encore migré la configuration, vous pouvez cliquer sur **Annuler** pour recommencer.

Si vous avez migré la configuration, vous devez effectuer les étapes suivantes pour redémarrer la migration :

- 1 Annulez la migration.
- 2 Déployez un nouvel environnement NSX-T avec des dispositifs NSX Manager et NSX Edge.
- 3 Démarrez une nouvelle migration.

Attention Dans NSX-T Data Center 2.4.0, il existe un bouton **Restauration** pour certaines étapes de la migration. L'utilisation du bouton **Restauration** peut entraîner un comportement inattendu. Au lieu de cela, utilisez le bouton **Annuler** pour annuler la migration à l'étape **Importer une configuration** ou **Migrer la configuration**.

Résoudre les problèmes de la configuration de la Mise en réseau vSphere

Après avoir importé la configuration de la mise en réseau de l'environnement vSphere, vous devez examiner et résoudre les problèmes de configuration signalés avant de poursuivre la migration.

Vous ne pourrez poursuivre la migration qu'après avoir fourni des commentaires pour tous les problèmes de configuration à résoudre. Plusieurs personnes peuvent fournir les commentaires via différentes sessions. Après avoir commenté un problème donné, vous pouvez cliquer sur **Envoyer** pour enregistrer le commentaire. Vous pouvez revenir sur un commentaire envoyé pour le modifier.

Une fois que tous les problèmes ont été commentés, les commentaires sont validés. La validation peut générer des demandes de commentaires supplémentaires, que vous devrez fournir avant de poursuivre la migration.

Procédure

- 1 Sur la page **Résoudre la configuration**, cliquez sur **Sélectionnez le commutateur** pour sélectionner quel Distributed Switch vSphere migrer.

Une fois qu'un commutateur distribué est sélectionné, les problèmes de configuration sont affichés.

- 2 Passez en revue les problèmes signalés.

Les problèmes sont classés en plusieurs groupes. Chaque problème peut concerner plusieurs éléments de configuration. Pour chaque élément, il peut exister une ou plusieurs résolutions possibles au problème (ignorer, configurer ou sélectionner une valeur spécifique, par exemple).

- 3 Cliquez sur chaque problème et fournissez vos commentaires.

Lorsqu'un problème s'applique à plusieurs éléments de configuration, vous pouvez fournir des commentaires pour chacun d'eux individuellement, ou bien les sélectionner tous et fournir une réponse pour tous les éléments.

Plusieurs personnes peuvent fournir les données via différentes sessions. Vous pouvez revenir sur un commentaire envoyé pour le modifier.

- 4 Une fois les commentaires fournis, le bouton **Envoyer** s'affiche sur la page **Résoudre les problèmes**. Cliquez sur **Envoyer** pour enregistrer votre progression.

- 5 Une fois que tous les problèmes de configuration sont commentés, cliquez sur **Envoyer**.

L'entrée est validée. Si certaines données ne sont pas valides, vous êtes invité à les mettre à jour. Vous devrez peut-être fournir des données supplémentaires pour certains éléments de configuration.

- 6 Après avoir envoyé tous les commentaires demandés, cliquez sur **Continuer** pour passer à l'étape de migration de la configuration.

Migrer la configuration de la mise en réseau vSphere

Une fois que vous avez résolu tous les problèmes de configuration, vous pouvez migrer la configuration de la mise en réseau de vSphere. Les modifications de configuration sont effectuées dans

l'environnement de NSX-T pour répliquer la configuration vSphere traduite. Aucune modification de configuration n'est effectuée dans vSphere.

Attention Dans NSX-T Data Center 2.4.0, il existe un bouton **Restauration** pour certaines étapes de la migration. L'utilisation du bouton **Restauration** peut entraîner un comportement inattendu. Au lieu de cela, utilisez le bouton **Annuler** pour annuler la migration à l'étape **Importer une configuration** ou **Migrer la configuration**.

Pour plus d'informations, reportez-vous à [Annuler ou redémarrer la migration de la mise en réseau vSphere](#).

Conditions préalables

Vérifiez que vous avez effectué l'étape **Résoudre la configuration**.

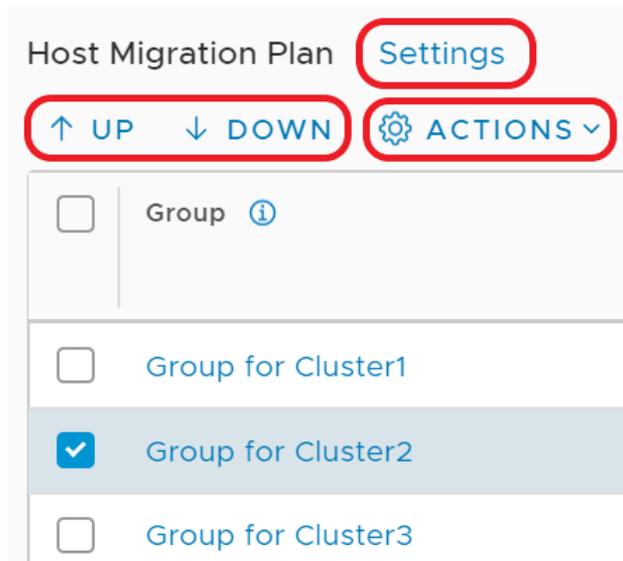
Procédure

- ◆ Dans la page **Migrer la configuration**, cliquez sur **Démarrer**.

La configuration du commutateur distribué est migrée vers NSX-T.

Configuration de la migration d'hôte

Les clusters de l'environnement vSphere s'affichent sur la page **Migrer les hôtes**. Les clusters sont organisés en groupes de migration, chaque groupe de migration contient un cluster d'hôtes vSphere. Plusieurs paramètres contrôlent la manière dont la migration de l'hôte est effectuée.



- Cliquez sur **Paramètres** pour modifier les paramètres globaux : **Pause entre les groupes** et **Ordre de migration entre les groupes**.
- Sélectionnez un seul groupe d'hôtes (cluster) et utilisez les flèches pour le déplacer vers le haut ou vers le bas dans la séquence de migration.

- Sélectionnez un ou plusieurs groupes d'hôtes (clusters) et cliquez sur **Actions** pour modifier les paramètres de ces groupes d'hôtes : **Ordre de migration au sein des groupes** et **État de migration**.

Pause entre les groupes

Pause entre les groupes est un paramètre global qui s'applique à tous les groupes d'hôtes. Si la suspension est activée, le coordinateur de migration migre un groupe d'hôtes, puis attend une entrée. Vous devez cliquer sur **Continuer** pour passer au groupe d'hôtes suivant. Si vous souhaitez vérifier l'état de chaque cluster avant de passer au suivant, activez **Pause entre les groupes**.

Pause entre les groupes est désactivé par défaut.

Ordre de migration séquentiel ou parallèle

Vous pouvez définir si la migration s'effectue dans un ordre séquentiel ou parallèle. Il existe deux paramètres de commande :

■ Ordre de migration entre les groupes

Ordre de migration entre les groupes est un paramètre global qui s'applique à tous les groupes d'hôtes.

- **Série** : un groupe d'hôtes (cluster) est migré à la fois.
- **Parallèle** : jusqu'à cinq groupes d'hôtes sont migrés à la fois. Après la migration de ces cinq groupes d'hôtes, le lot suivant de cinq groupes d'hôtes maximum est migré.

■ Ordre de migration au sein du groupe

Ordre de migration au sein du groupe est un paramètre spécifique à un groupe d'hôtes (cluster) qui peut donc être configuré séparément sur chaque groupe d'hôtes.

- **Série** : un hôte au sein du groupe d'hôtes (cluster) est migré à la fois.
- **Parallèle** : jusqu'à cinq hôtes dans le groupe d'hôtes sont migrés à la fois. Une fois ces hôtes migrés, le lot suivant de cinq hôtes maximum est migré.

Par défaut, les deux paramètres sont définis sur **Série**. Ensemble, les paramètres déterminent le nombre d'hôtes migrés à la fois.

Tableau 2-1. Effets des paramètres de migration sur le nombre d'hôtes tentant de migrer simultanément

Ordre de migration entre les groupes (Clusters)	Ordre de migration au sein des groupes (clusters)	Nombre maximal d'hôtes tentant la migration simultanément
Série	Série	1 Un hôte d'un groupe d'hôtes
Série	Parallèle	5 Cinq hôtes d'un groupe d'hôtes

Tableau 2-1. Effets des paramètres de migration sur le nombre d'hôtes tentant de migrer simultanément (suite)

Ordre de migration entre les groupes (Clusters)	Ordre de migration au sein des groupes (clusters)	Nombre maximal d'hôtes tentant la migration simultanément
Parallèle	Série	5 Un hôte de cinq groupes d'hôtes
Parallèle	Parallèle	25 Cinq hôtes à partir de cinq groupes d'hôtes

Important En cas d'échec de migration d'un hôte, le processus de migration s'interrompt une fois toutes les migrations d'hôtes en cours terminées. Si **Parallèle** est sélectionné pour la migration entre les groupes et la migration au sein des groupes, il peut y avoir une longue interruption de l'hôte ayant échoué avant de pouvoir effectuer une nouvelle tentative de migration. Dans un environnement de production, ne sélectionnez pas l'ordre de migration parallèle au sein des groupes.

Séquence de groupes de migration

Vous pouvez sélectionner un groupe d'hôtes (cluster) et utiliser les flèches pour le déplacer vers le haut ou vers le bas dans la liste des groupes.

Si la migration d'un hôte échoue, vous pouvez déplacer son groupe d'hôtes en bas de la liste des groupes. La migration d'autres groupes d'hôtes peut continuer pendant que vous résolvez le problème de l'hôte posant problème.

Activer ou désactiver les groupes

Les groupes d'hôtes (clusters) peuvent avoir l'un des trois états suivants :

- **Activé**

Les hôtes de ces groupes sont migrés vers NSX-T lorsque vous cliquez sur **Démarrer** sur la page **Migrer les hôtes**.

- **Désactivé**

Les hôtes de ces groupes ne sont pas migrés vers NSX-T lorsque vous cliquez sur **Démarrer** sur la page **Migrer les hôtes**. Cependant, si vous n'avez pas encore cliqué sur **Terminer** pour la migration, vous pouvez revenir à la page **Migrer les hôtes** pour les activer et redémarrer la migration de l'hôte. Terminez toutes les tâches de migration d'hôte et cliquez sur **Terminer** dans la même fenêtre de maintenance.

- **Ne pas migrer**

Les hôtes de ces groupes ont été identifiés pendant l'étape **Résoudre la configuration** comme n'étant pas éligibles pour la migration.

Migrer les hôtes vSphere

Après la migration de la configuration, vous pouvez migrer les hôtes vSphere vers NSX-T Data Center.

Vous pouvez configurer plusieurs paramètres relatifs à la migration d'hôte, y compris l'ordre de migration et l'activation des hôtes. Avant de changer les paramètres par défaut, assurez-vous de comprendre les effets de ces paramètres. Pour plus d'informations, reportez-vous à la section [Configuration de la migration d'hôte](#).

Attention Pendant la migration de l'hôte, il existe une interruption du trafic. Effectuez cette étape au cours d'une fenêtre de maintenance.

Si la migration d'un hôte échoue, elle s'interrompt une fois toutes les migrations d'hôte en cours terminées. Une fois le problème avec l'hôte résolu, cliquez sur **Réessayer** pour retenter la migration de l'hôte échouée.

Si la migration d'un hôte échoue, vous pouvez déplacer son groupe d'hôtes en bas de la liste des groupes. La migration d'autres groupes d'hôtes peut continuer pendant que vous résolvez le problème de l'hôte posant problème.

Après que l'hôte a migré vers NSX-T, il est possible que vous aperceviez une alarme avec le message **Connectivité réseau perdue**. Cette alarme se produit, car l'hôte ne possède plus de carte réseau/NIC connectée au vSphere Distributed Switch auquel il était précédemment connecté.

Conditions préalables

- Vérifiez que tous les hôtes ESXi sont dans un état opérationnel. Résolvez les problèmes impliquant des hôtes, y compris les états déconnectés. Aucun redémarrage ni aucune tâche ne doit être en attente pour passer en mode de maintenance.

Note Les hôtes ne passent en mode de maintenance pendant la migration.

Procédure

- ◆ Cliquez sur **Démarrer** pour démarrer la migration de l'hôte.

Les hôtes vSphere sont convertis en nœuds de transport hôtes NSX-T. Les interfaces réseau des machines virtuelles sur les hôtes sont déconnectées des groupes de ports vSphere Distributed Switch et connectées aux segments NSX-T.

Terminer la migration

Après avoir migré les hôtes vers l'environnement NSX-T Data Center, vérifiez que le nouvel environnement fonctionne correctement. Si tout fonctionne correctement, vous pouvez terminer la migration.

Important Vérifiez que tout fonctionne et cliquez sur **Terminer** dans la fenêtre de maintenance. Lorsque vous cliquez sur **Terminer**, un nettoyage post-migration est opéré. Ne laissez pas le coordinateur de migration dans un état inachevé au-delà de la fenêtre de la migration.

Conditions préalables

Vérifiez que l'environnement NSX-T Data Center fonctionne correctement.

Procédure

- 1 Accédez à la page **Migrer les hôtes** du coordinateur de migration.
- 2 Cliquez sur **Terminer**.

Une boîte de dialogue s'affiche pour vous permettre de confirmer que vous souhaitez terminer la migration. Si vous terminez la migration, tous les détails de celle-ci s'effaceront. Vous ne pourrez plus réviser ses paramètres, Par exemple, quelles entrées ont été effectuées sur la page **Résoudre les problèmes**.