Guide d'installation de NSX

Mise à jour 9
Modifié le 21 février 2020
VMware NSX Data Center for vSphere 6.3

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

Table des matières

Guide d'installation de NSX

Ce manuel, le *Guide d'installation de NSX*, explique comment installer le système VMware NSX® for vSphere® à l'aide de l'interface utilisateur de NSX Manager et de vSphere Web Client. Il contient des instructions de configuration pas à pas et des suggestions de meilleures pratiques.

Public visé

Ce manuel est destiné à tous ceux qui veulent installer ou utiliser NSX dans un environnement VMware vCenter. Les informations qu'il contient sont destinées aux administrateurs système expérimentés qui sont familiarisés avec la technologie des machines virtuelles et les opérations de centres de données virtuels. Ce guide suppose que vous connaissez VMware vSphere, notamment VMware ESXi vCenter Server et vSphere Web Client.

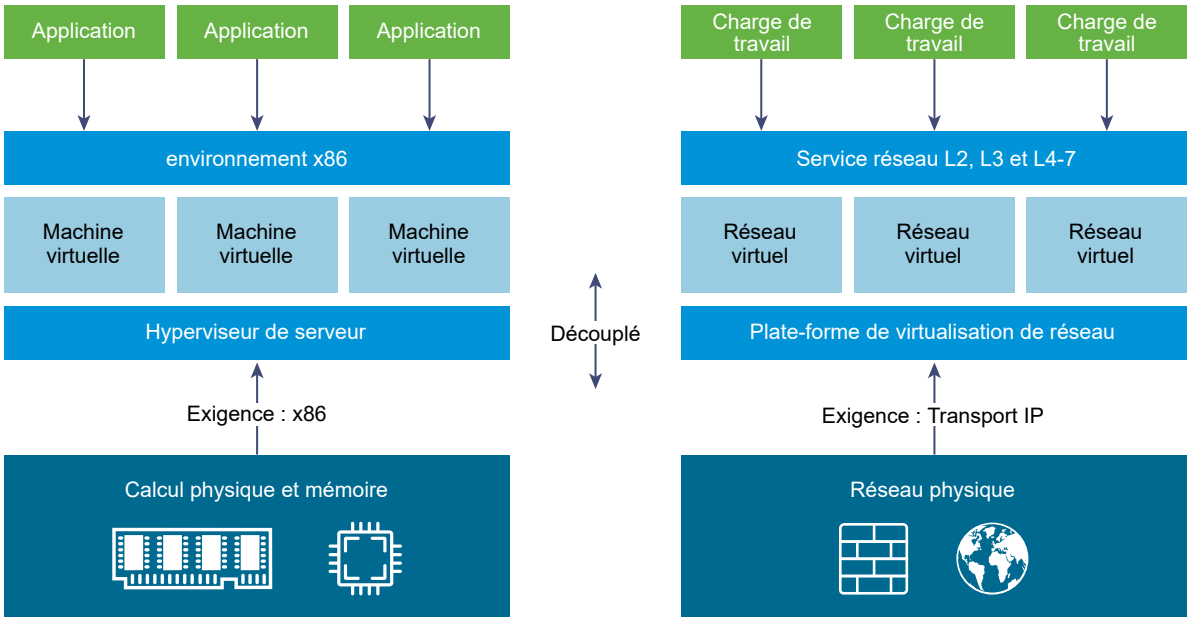
Glossaire VMware Technical Publications

VMware Technical Publications fournit un glossaire de termes pouvant ne pas vous être familiers. Pour consulter la définition des termes utilisés dans la documentation technique VMware, visitez le site Web http://www.vmware.com/support/pubs.

Présentation de NSX for vSphere 1

La virtualisation des serveurs s'est directement accompagnée d'avantages notables pour les entreprises informatiques. La consolidation des serveurs a réduit la complexité physique, accru l'efficacité opérationnelle et la capacité à réorienter dynamiquement les ressources sous-jacentes afin de répondre rapidement, et de façon optimale, aux besoins d'applications d'entreprise toujours plus dynamiques.

L'architecture SDDC (Software Defined Data Center) de VMware étend désormais les technologies de virtualisation dans l'ensemble de l'infrastructure de centre de données physique. NSX for vSphere est un produit clé de l'architecture SDDC. Avec NSX for vSphere, la virtualisation confère à la mise en réseau les mêmes avantages que ceux déjà assurés aux calculs et au stockage. Tout comme la virtualisation des serveurs crée, supprime et restaure des machines virtuelles basées sur des logiciels, et en crée des snapshots, de façon programmée, la virtualisation réseau NSX for vSphere crée, supprime et restaure des réseaux virtuels basés sur des logiciels, et en crée des snapshots, de façon programmée. Il en résulte une approche vouée à la transformation de la mise en réseau qui non seulement permet aux gestionnaires de centres de données d'atteindre des volumes, une agilité et des facteurs économiques améliorés, mais qui propose également un modèle opérationnel nettement simplifié pour le réseau physique sous-jacent. Grâce à sa capacité à être déployée sur n'importe quel réseau IP, y compris sur les modèles de mise en réseau traditionnels existants et sur les architectures matricielles de nouvelle génération de n'importe quel fournisseur, NSX for vSphere est une solution entièrement sans perturbation. En fait, avec NSX for vSphere, l'infrastructure du réseau physique dont vous disposez déjà est tout ce dont vous avez besoin pour déployer un centre de données SDDC.



L'illustration ci-dessus effectue une analogie entre la virtualisation des calculs et celle du réseau. Grâce à la virtualisation des serveurs, une couche d'abstraction logicielle (hyperviseur de serveur) reproduit les attributs habituels d'un serveur physique x86 (par exemple, unité centrale, mémoire RAM, disque, carte réseau virtuelle) dans le logiciel, ce qui permet de programmer leur assemblage dans n'importe quelle combinaison arbitraire pour produire une machine virtuelle unique en quelques secondes.

Avec la virtualisation réseau, l'équivalent fonctionnel d'un hyperviseur de réseau reproduit l'ensemble complet de services de mise en réseau de la couche 2 jusqu'à la couche 7 (par exemple commutation, routage, contrôle d'accès, création de pare-feu, qualité du service et équilibrage de charge) dans le logiciel. Par conséquent, ces services peuvent être assemblés de façon programmée dans n'importe quelle combinaison arbitraire afin de produit des réseaux virtuels isolés en quelques secondes.

La virtualisation réseau permet d'obtenir des avantages semblables à ceux offerts par la virtualisation des serveurs. Par exemple, tout comme les machines virtuelles sont indépendantes de la plate-forme x86 sous-jacente et permettent au service informatique de traiter les hôtes physiques comme un pool de capacités de calcul, les réseaux virtuels sont indépendants du matériel physique du réseau IP sous-jacent et permettent au service informatique de traiter le réseau physique comme un pool de capacités de transport pouvant être utilisées et réorientées à la demande. À la différence des architectures héritées, les réseaux virtuels peuvent être alloués, modifiés, stockés, supprimés et restaurés en fonction de la programmation sans qu'il soit nécessaire de reconfigurer le matériel physique ou la topologie sous-jacent(e). En égalant les capacités et les avantages découlant de solutions de virtualisation des serveurs et du stockage connues, cette approche de la mise en réseau favorisant la transformation laisse s'exprimer tout le potentiel du centre de données défini par le logiciel.

NSX for vSphere peut être configuré à l'aide de vSphere Web Client, d'une interface de ligne de commande (CLI) et d'une REST API.

Ce chapitre contient les rubriques suivantes :

- Composants de NSX for vSphere

- NSX Edge
- NSX Services

Composants de NSX for vSphere

Cette section décrit les composants de la solution NSX for vSphere.

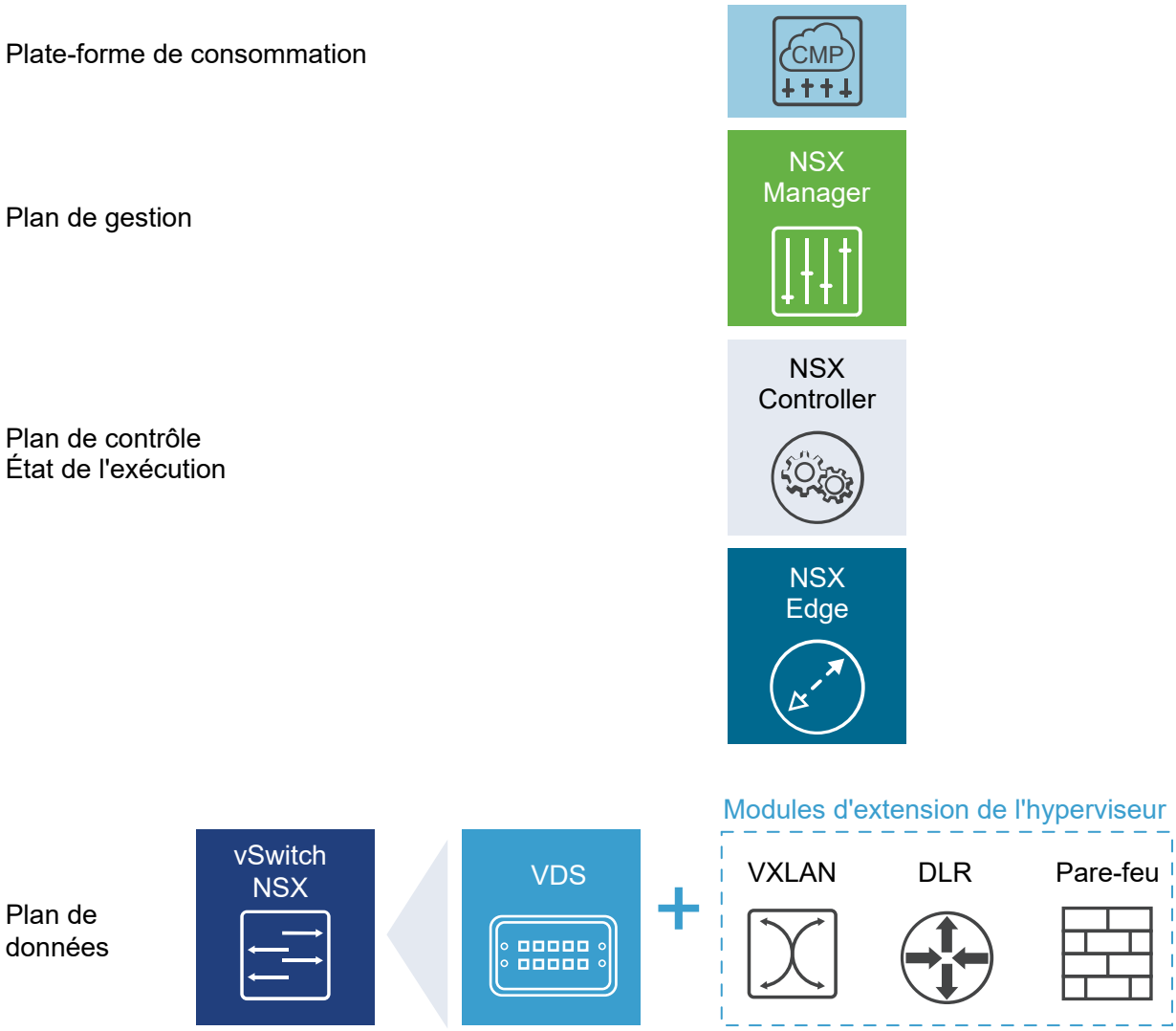


Plate-forme de consommation
CMP
Plan de gestion
NSX Manager
Plan de contrôle
État de l'exécution
NSX Controller
NSX Edge
Plan de données
vSwitch NSX
VDS
Modules d'extension de l'hyperviseur
VXLAN
DLR
Pare-feu

Sachez qu'une plate-forme de gestion du cloud (CMP) n'est pas un composant de NSX for vSphere. NSX for vSphere fournit cependant l'intégration à pratiquement toutes les CMP par le biais d'API REST, ainsi qu'une intégration directe aux plates-formes de gestion du cloud VMware.

Plan de données

Le plan de données NSX se compose du vSwitch NSX, lequel est basé sur le vSphere Distributed Switch (VDS) doté de composants supplémentaires pour activer les services. Les modules de noyau NSX, agents d'espace utilisateur, fichiers de configuration et scripts d'installation sont réunis dans des VIB afin de fournir des services tels que le routage distribué et les pare-feu logiques, ainsi que pour activer les capacités de pontage VXLAN.

Le NSX vSwitch (basé sur vDS) crée une abstraction du réseau physique et fournit une commutation de niveau d'accès dans l'hyperviseur. Il est essentiel à la virtualisation du réseau car il active des réseaux logiques indépendants des constructions physiques comme les VLAN. Parmi les avantages du vSwitch, on peut citer :

- La prise en charge de la création de réseaux superposés avec des protocoles (VXLAN, par exemple) et une configuration réseau centralisés. La création d'un réseau superposé active les capacités suivantes :
  - Réduction de l'utilisation des ID de VLAN dans le réseau physique.
  - Création d'une superposition de couche 2 (L2) logique flexible sur les réseaux IP existants sur l'infrastructure physique existante sans qu'il soit nécessaire de modifier l'architecture d'un réseau de centre de données quel qu'il soit.
  - Établissement de communications (horizontales et verticales) tout en maintenant l'isolation des locataires.
  - Charges de travail d'application et machines virtuelles ne connaissant pas le réseau superposé et fonctionnant comme si elles étaient connectées à un réseau de niveau 2 physique.
- Facilitation d'hyperviseurs d'immense envergure.
- De nombreuses fonctions (telles que la mise en miroir des ports, NetFlow/IPFIX, la sauvegarde et restauration de la configuration, le contrôle de santé du réseau, la qualité de service et le LACP) composent une trousse à outils exhaustive destinée à la gestion, à la surveillance et au dépannage du trafic dans un réseau virtuel.

Les routeurs logiques peuvent fournir un pontage de niveau 2 entre l'espace de mise en réseau logique (VXLAN) et le réseau physique (VLAN).

Le périphérique passerelle est généralement constitué d'un dispositif NSX Edge virtuel. NSX Edge offre des fonctions L2, L3, de pare-feu périmétrique et d'équilibrage de charge, ainsi que d'autres services tels que le VPN SSL et le DHCP.

Plan de contrôle

Le plan de contrôle NSX s'exécute dans le cluster NSX Controller. NSX Controller est un système avancé de gestion des états distribués qui fournit des fonctions de plan de contrôle pour les fonctions de

commutation et de routage logiques NSX. Il constitue le point de contrôle central de tous les commutateurs logiques figurant dans un réseau. Il gère également les informations de l'ensemble des hôtes, des commutateurs logiques (VXLAN) et des routeurs logiques distribués.

Le cluster du contrôleur est responsable de la gestion des modules de commutation distribuée et du routage dans les hyperviseurs. Le contrôleur n'est pas traversé par un trafic de plan de données. Des nœuds de contrôleur sont déployés dans un cluster de trois membres afin d'activer la haute disponibilité et l'échelle. Une défaillance des nœuds du contrôleur n'a aucune répercussion sur le trafic de plan de données.

Les instances de NSX Controller distribuent des informations sur le réseau aux hôtes. Pour atteindre un niveau élevé de résilience, NSX Controller est mis en cluster pour la montée en charge et le mode HA. Les instances de NSX Controller doivent être déployées dans un cluster à 3 nœuds. Les trois dispositifs virtuels fournissent, gèrent et mettent à jour l'état de l'ensemble du réseau fonctionnant dans le domaine NSX. NSX Manager permet de déployer des nœuds NSX Controller.

Les trois nœuds NSX Controller forment un cluster de contrôle. Le cluster de contrôleurs requiert un quorum (majorité) pour éviter qu'un scénario de « split brain » se produise. Dans un scénario de « split brain », les incohérences de données sont issues de la maintenance de deux ensembles de données distincts qui se chevauchent. Ces incohérences peuvent être dues à des défaillances et à des problèmes de synchronisation des données. La présence de trois nœuds de contrôleur permet d'assurer la redondance des données en cas de défaillance d'un nœud NSX Controller.

Un cluster de contrôleurs détient entre autres les rôles suivants :

- Fournisseur d'API
- Serveur de persistance
- Gestionnaire de commutateur
- Gestionnaire logique
- Serveur d'annuaire

Chaque rôle dispose d'un nœud de contrôleur maître. Si un nœud de contrôleur maître échoue pour un rôle, le cluster désigne un nouveau maître pour ce rôle parmi les nœuds NSX Controller disponibles. Le nouveau nœud NSX Controller maître détenant le rôle réattribue les portions de travail perdues entre les nœuds NSX Controller restants.

NSX prend en charge trois modes de plan de contrôle de commutateur logique : multidiffusion, monodiffusion et hybride. L'utilisation d'un cluster contrôlé pour gérer des commutateurs logiques basés sur VXLAN permet d'éliminer le besoin d'une prise en charge de la multidiffusion dans l'infrastructure réseau physique. Vous n'avez pas besoin de provisionner des adresses IP de groupe de multidiffusion, ni d'activer les fonctionnalités de routage PIM ou d'écoute IGMP sur des commutateurs physiques ou des routeurs. En conséquence, les modes monodiffusion ou hybrides dissocient NSX du réseau physique. Les réseaux VXLAN en mode de plan de contrôle de monodiffusion ne nécessitent plus que le réseau physique prenne en charge la multidiffusion pour gérer le trafic diffusion, monodiffusion inconnue et multidiffusion (BUM) au sein d'un commutateur logique. Le mode monodiffusion réplique tout le trafic

BUM localement sur l'hôte et ne nécessite aucune configuration du réseau physique. En mode hybride, une partie de la réplication du trafic BUM est déchargée sur le commutateur physique de premier saut pour obtenir de meilleures performances. Le mode hybride nécessite une écoute IGMP sur le commutateur de premier saut et un accès à une requête IGMP dans chaque sous-réseau VTEP.

Plan de gestion

Le plan de gestion NSX est créé par NSX Manager, le composant de gestion de réseau centralisé de NSX. Il fournit le point de configuration unique et les points d'entrée de l'API REST.

NSX Manager s'installe en tant que dispositif virtuel sur tout hôte ESX™ dans votre environnement vCenter Server. NSX Manager et vCenter entretiennent une relation de type un à un. À chaque instance de NSX Manager correspond un vCenter Server. Cela est vrai même dans un environnement cross-vCenter NSX.

Dans un environnement cross-vCenter NSX, il existe une instance principale de NSX Manager et une ou plusieurs instances secondaires de NSX Manager. L'instance principale de NSX Manager vous permet de créer et de gérer des commutateurs logiques universels, des routeurs logiques universels (distribués) et des règles de pare-feu universelles. Les instances secondaires de NSX Manager servent à gérer les services de mise en réseau qui sont locales pour cette instance spécifique de NSX Manager. Jusqu'à sept instances secondaires de NSX Manager peuvent être associées à l'instance principale de NSX Manager dans un environnement cross-vCenter NSX.

Plate-forme de consommation

La consommation de NSX peut s'effectuer directement par l'intermédiaire de l'interface utilisateur de NSX Manager qui est disponible dans vSphere Web Client. En général, les utilisateurs associent la virtualisation réseau à leur plate-forme de gestion de Cloud (CMP) pour déployer des applications. NSX fournit une forte intégration dans presque toutes les CMP par l'intermédiaire de l'API REST. L'intégration prédéfinie est également disponible dans VMware vCloud Automation Center, vCloud Director et OpenStack avec le plug-in Neutron pour NSX.

NSX Edge

Vous pouvez installer NSX Edge en tant que passerelle Edge Services Gateway (ESG) ou routeur logique distribué (DLR).

Edge Services Gateway

Edge Services Gateway vous donne accès à tous les services NSX Edge tels que le pare-feu, NAT, DHCP, VPN, l'équilibrage de charge et la haute disponibilité. Vous pouvez installer plusieurs dispositifs virtuels de passerelle ESG dans un centre de données. Chaque dispositif virtuel ESG peut comporter un total de dix interfaces réseau de liaison montante et internes. Avec une jonction, une passerelle ESG peut comporter jusqu'à 200 sous-interfaces. Les interfaces internes se connectent à des groupes de ports

sécurisés et font office de passerelle pour toutes les machines virtuelles protégées du groupe de ports. Le sous-réseau attribué à l'interface interne peut être un espace IP routé publiquement ou un espace privé NAT/routé défini par la RFC 1918. Les règles de pare-feu et les autres services NSX Edge sont appliqués au trafic entre les interfaces.

Les interfaces de liaison montante des passerelles ESG se connectent à des groupes de ports qui ont accès à un réseau d'entreprise partagé ou à un service fournissant un accès à la mise en réseau de la couche. Il est possible de configurer plusieurs adresses IP externes pour l'équilibreur de charge, le réseau privé virtuel (VPN) de site à site et les services de traduction des adresses réseau (NAT).

Routeur logique distribué

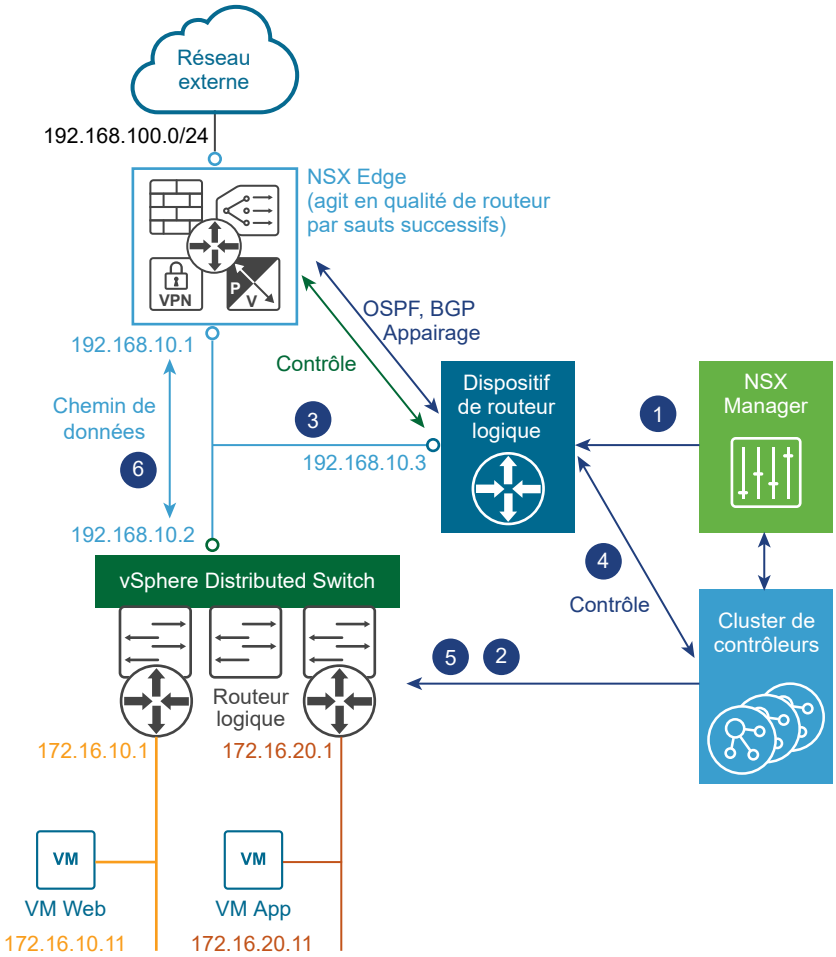
Le routeur logique distribué fournit un routage distribué horizontal avec un espace d'adressage IP de locataire et une isolation du chemin de données. Les machines ou les charges de travail virtuelles qui se trouvent surle même hôte sur différents sous-réseaux peuvent communiquer entre elles sans avoir à traverser une interface de routage traditionnelle.

Un routeur logique peut disposer de huit interfaces de liaison montante et jusqu'à un millier d'interfaces internes. Une interface de liaison montante sur un routeur distribué logique établit généralement une liaison homologue avec une interface ESG, avec un commutateur de transit logique de niveau 2 intervenant entre le routeur distribué logique et la passerelle ESG. Une interface interne sur un routeur distribué logique établit une liaison homologue avec une machine virtuelle hébergée sur un hyperviseur ESXi avec un commutateur logique intervenant entre la machine virtuelle et le routeur distribué logique.

Le routeur distribué logique possède deux composants principaux :

- Le plan de contrôle de routage est fourni par le dispositif virtuel du routeur distribué logique (aussi appelé machine virtuelle de contrôle). Cette machine virtuelle prend en charge les protocoles de routage dynamique (BGP et OSPF), échange des mises à jour de routage avec le périphérique de saut de couche 3 suivant (généralement la passerelle Edge Services Gateway) et communique avec NSX Manager et le cluster NSX Controller. La haute disponibilité pour le dispositif virtuel de routeur distribué logique est prise en charge au moyen d'une configuration en veille active : une paire de machines virtuelles fonctionnant en modes actif/veille est fournie lorsque vous créez le routeur distribué logique avec HA activé.
- Au niveau du plan de données, les modules de noyau de routeur distribué logique (VIB) sont installés sur des hôtes ESXi faisant partie du domaine NSX. Les modules de noyau sont similaires aux cartes de ligne dans un châssis modulaire prenant en charge le routage de couche 3. Les modules de noyau ont une base d'informations de routage (RIB), aussi appelée table de routage, envoyée depuis le cluster de controller. Au niveau du plan de données, les fonctionnalités de recherche de route et de recherche d'entrée ARP sont exécutées par les modules de noyau. Les modules de noyau sont équipés d'interfaces logiques (appelées LIF) établissant la connexion avec les différents commutateurs logiques et tout groupe de ports sauvegardés sur VLAN. Une adresse IP, représentant la passerelle IP par défaut pour le segment logique L2 auquel il se connecte, et une adresse vMAC sont attribuées à chaque LIF. L'adresse IP de chaque LIF est unique, alors que la même adresse vMAC est attribuée à tous les LIF définis.

Figure 1-1. Composants de routage logique



1 Une instance de routeur logique distribué est créée à partir de l'interface utilisateur de NSX Manager (ou au moyen d'appels d'API) et le routage est activé, à l'aide d'OSPF ou de BGP.

2 NSX Controller utilise le plan de contrôle avec les hôtes ESXi pour envoyer la nouvelle configuration de routeur logique distribué, y compris les LIF et leurs adresses IP et vMAC associées.

3 Considérant qu'un protocole de routage est aussi activé sur le périphérique de tronçon suivant (un NSX Edge [ESG] dans cet exemple), l'homologation OSPF ou BGP est établie entre l'ESG et la machine virtuelle de contrôle du routeur logique distribué. L'ESG et le routeur de logique distribué peuvent échanger des informations de routage :

   - La machine virtuelle de contrôle du routeur logique distribué peut être configurée pour redistribuer dans OSPF les préfixes IP pour tous les réseaux logiques connectés (172.16.10.0/24 et 172.16.20.0/24 dans cet exemple). Cela entraîne l'envoi des annonces de routes au NSX Edge. Notez que pour ces préfixes le prochain saut n'est pas l'adresse IP attribuée à la machine virtuelle de contrôle (192.168.10.3), mais l'adresse IP identifiant le composant du plan de données du routeur logique distribué (192.168.10.2). La première est appelée « adresse de protocole » du routeur logique distribué, alors que la seconde correspond à « l'adresse de transfert ».

- NSX Edge envoie les préfixes à la machine virtuelle de contrôle pour atteindre les réseaux IP du réseau externe. Dans la plupart des situations, il est probable qu'une seule route par défaut soit envoyée à NSX Edge, car elle représente le seul point de sortie vers l'infrastructure de réseau physique.

4 La machine virtuelle de contrôle de routeur logique distribué envoie les routes IP communiquées par NSX Edge au cluster de contrôleur.

5 Le cluster de contrôleur est responsable de la distribution aux hyperviseurs des routes communiquées par la machine virtuelle de contrôle de routeur logique distribué. Chaque nœud de contrôleur du cluster se charge de distribuer les informations pour une instance de routeur logique spécifique. Dans un déploiement comprenant plusieurs instances de routeur logique, la charge est répartie entre les nœuds de contrôleur. Une instance de routeur logique séparée est généralement associée à chaque locataire déployé.

6 Les modules de noyau de routage DLR de l'hôte gèrent le trafic du chemin de données pour communiquer avec le réseau externe au moyen de NSX Edge.

NSX Services

Les composants NSX œuvrent ensemble pour fournir les services fonctionnels suivants.

Commutateurs logiques

Un déploiement cloud ou un centre de données virtuel possède un grand nombre d'applications sur plusieurs locataires. Ces applications et ces locataires nécessitent d'être isolés les uns par rapport aux autres pour assurer la sécurité et la localisation des pannes, et pour éviter les chevauchements d'adresses IP. NSX permet de créer plusieurs commutateurs logiques dont chacun constitue un domaine de diffusion logique unique. Une application ou une machine virtuelle locataire peut être câblée de façon logique à un commutateur logique. Cela permet plus de flexibilité et de vitesse de déploiement tout en fournissant toutes les caractéristiques des domaines de diffusion des réseaux physiques (VLAN) sans les problèmes de prolifération ou de protocole Spanning Tree liés à la couche 2 physique.

Un commutateur logique est distribué et peut s'étendre à l'ensemble des hôtes de vCenter (ou d'un environnement cross-vCenter NSX). Cela permet d'assurer la mobilité des machines virtuelles (vMotion) au sein du centre de données, tout en s'affranchissant des limites de la couche 2 physique (VLAN). L'infrastructure physique n'est pas restreinte par les limites de la table MAC/FIB car le logiciel du commutateur logique contient le domaine de diffusion.

Routeurs logiques

Le routage fournit les informations de transfert nécessaires entre des domaines de diffusion de la couche 2, vous permettant ainsi de diminuer la taille des domaines de diffusion de la couche 2 et d'améliorer l'efficacité et l'échelle du réseau. NSX étend ces informations aux emplacements dans lesquels résident les charges de travail pour un routage horizontal. Cela permet une communication plus directe entre les machines virtuelles sans extension de sauts longue et coûteuse. En même temps, les routeurs logiques de NSX fournissent une connectivité verticale, permettant ainsi aux locataires d'accéder aux réseaux publics.

Pare-feu logique

Le pare-feu logique offre des mécanismes de sécurité pour les centres de données virtuels dynamiques. Le composant pare-feu distribué du pare-feu logique vous permet de segmenter les entités de centres de données virtuelles comme les machines virtuelles basées sur des noms et attributs de machine virtuelle, sur l'identité de l'utilisateur, sur des objets vCenter tels que des centres de données et sur des hôtes, ainsi que sur les attributs de mise en réseau traditionnels que sont les adresses IP, les réseaux VLAN, etc. Le composant Edge Firewall vous aide à respecter des exigences essentielles de sécurité du périmètre telles que la création des zones démilitarisées sur des constructions IP/VLAN et l'isolation entre locataires dans les centres de données virtuels à plusieurs locataires.

La fonction Flow Monitoring affiche l'activité réseau entre les machines virtuelles au niveau du protocole d'application. Vous pouvez utiliser ces informations pour contrôler le trafic réseau, définir et affiner les stratégies du pare-feu et identifier les menaces que court votre réseau.

Réseaux VPN (Virtual Private Network) logiques

VPN-Plus SSL permet à des utilisateurs distants d'accéder à des applications d'entreprise privées. VPN IPsec assure une connectivité de site à site entre une instance de NSX Edge et des sites distants avec NSX ou avec des routeurs matériels/passerelles VPN de fournisseurs tiers. VPN L2 permet d'étendre votre centre de données en autorisant les machines virtuelles à conserver la connectivité réseau tout en gardant la même adresse IP entre des limites géographiques.

Équilibrage de charge logique

L'équilibrage de charge de NSX Edge distribue les connexions clientes dirigées vers une adresse IP virtuelle unique (VIP) entre plusieurs destinations configurées en tant que membres d'un pool d'équilibrage de charge. Il distribue les demandes de service entrantes uniformément entre plusieurs serveurs de telle sorte que la distribution de la charge est transparente pour les utilisateurs. L'équilibrage de charge contribue donc à obtenir une utilisation optimale des ressources, à optimiser le débit, à réduire les temps de réponse et à éviter la surcharge.

Service Composer

Service Composer vous aide à provisionner et à attribuer des services de réseau et de sécurité à des applications dans une infrastructure virtuelle. Vous pouvez mapper ces services à un groupe de sécurité pour les appliquer aux machines virtuelles de ce groupe de sécurité en utilisant une règle de sécurité.

Extensibilité de NSX

Les fournisseurs de solutions tiers peuvent intégrer leur solutions à la plate-forme NSX, ce qui permet aux clients de bénéficier d'une expérience intégrée entre les produits VMware et les solutions des partenaires. Les opérateurs de centres de données peuvent provisionner des réseaux virtuels complexes et multiniveaux en quelques secondes, quels que soient la topologie du réseau et les composants sous-jacents.

Préparation à l'installation 2

Cette section décrit la configuration système requise pour NSX for vSphere, ainsi que les ports qui doivent être ouverts.

Ce chapitre contient les rubriques suivantes :

Configuration système requise pour NSX

Avant d'installer ou de mettre à niveau NSX, étudiez la configuration et les ressources de votre réseau. Vous pouvez installer une instance de NSX Manager par vCenter Server, une instance de Guest introspection par hôte ESXi™ et plusieurs instances de NSX Edge par centre de données.

Matériel

Ce tableau répertorie la configuration matérielle requise pour les dispositifs NSX.

Tableau 2-1. Configuration matérielle requise pour les dispositifs

Dispositif	Mémoire	vCPU	Espace disque
NSX Manager	16 Go (24 Go pour les grands déploiements de NSX)	4 (8 pour les grands déploiements de NSX)	60 Go
NSX Controller	4 Go	4	28 Go

Tableau 2-1. Configuration matérielle requise pour les dispositifs (suite)

Dispositif	Mémoire	vCPU	Espace disque
NSX Edge	Compacte : 512 Mo Grande : 1 Go Super grande : 2 Go Extra grande : 8 Go	Compacte : 1 Grande : 2 Super grande : 4 Extra grande : 6	Compacte, Grande : 1 disque de 584 Mo + 1 disque de 512 Mo Super grande : 1 disque de 584 Mo + 2 disques de 512 Mo Extra grande : 1 disque de 584 Mo + 1 disque de 2 Go + 1 disque de 512 Mo
Guest Introspection	2 Go	2	5 Go (l'espace provisionné est de 6,26 Go)

En règle générale, augmentez les ressources de NSX Manager à 8 vCPU et 24 Go de RAM si votre environnement géré par NSX contient plus de 256 hyperviseurs ou plus de 2 000 machines virtuelles.

Pour obtenir des détails concernant des tailles spécifiques, prenez contact avec le support VMware.

Pour obtenir des informations sur l'augmentation de la mémoire et l'allocation de vCPU pour vos dispositifs virtuels, consultez Allouer les ressources en mémoire et Modifier le nombre de cœurs de CPU virtuelles dans *Administration d'une machine virtuelle vSphere*.

L'espace provisionné d'un dispositif Guest Introspection indique 6,26 Go pour Guest Introspection. Cela s'explique par le fait que vSphere ESX Agent Manager crée un snapshot de la VM de service pour créer des clones rapides, lorsque plusieurs hôtes d'un cluster partagent un stockage. Pour plus d'informations sur la désactivation de cette option via ESX Agent Manager, consultez la documentation de *ESX Agent Manager*.

Latence du réseau

Vous devez vous assurer que la latence du réseau entre les composants est égale ou inférieure à la latence maximale décrite.

Tableau 2-2. Latence maximale du réseau entre les composants

Composants	Latence maximale
NSX Manager et NSX Controller	150 ms RTT
NSX Manager et hôtes ESXi	150 ms RTT
NSX Manager et système vCenter Server	150 ms RTT
NSX Manager et NSX Manager dans un environnement cross-vCenter NSX	150 ms RTT
NSX Controller et hôtes ESXi	150 ms RTT

Logiciels

Pour obtenir les informations d'interopérabilité les plus récentes, consultez le tableau d'interopérabilité du produit à l'adresse http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Pour connaître les versions recommandées de NSX, vCenter Server et ESXi, consultez les notes de mise à jour de la version de NSX vers laquelle vous mettez à niveau. Des notes de mise à jour sont disponibles sur le site de documentation de NSX for vSphere : https://docs.vmware.com/fr/VMware-NSX-for-vSphere/index.html.

Pour qu'une instance de NSX Manager participe à un déploiement cross-vCenter NSX, les conditions suivantes sont requises :

Composant	Version
NSX Manager	6.2 ou une version ultérieure
NSX Controller	6.2 ou une version ultérieure
vCenter Server	6.0 ou une version ultérieure
ESXi	■ ESXi 6.0 ou une version ultérieure ■ Clusters d'hôtes préparés avec des VIB NSX 6.2 ou version ultérieure

Pour gérer toutes les instances de NSX Manager sur un déploiement Cross-vCenter NSX depuis une seule instance de vSphere Web Client, vous devez connecter vos instances vCenter Server avec Enhanced Linked Mode. Consultez Utilisation de Enhanced Linked Mode dans *Gestion de vCenter Server et des hôtes* .

Pour vérifier la compatibilité des solutions de partenaires avec NSX, consultez le Guide de compatibilité de VMware pour Mise en réseau et sécurité à l'adresse http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security.

Accès client et utilisateur

Les éléments suivants sont requis pour gérer votre environnement NSX :

- Résolution de nom directe et inverse. Elle est nécessaire si vous avez ajouté des hôtes ESXi par nom à l'inventaire vSphere, sinon NSX Manager ne peut pas résoudre les adresses IP.
- Autorisations d'ajouter des machines virtuelles et de les mettre sous tension.
- Accès à la banque de données qui contient les fichiers de machine virtuelle et droits d'accès au compte pour copier les fichiers dans cette banque de données
- Les cookies doivent être activés dans votre navigateur Web pour accéder à l'interface utilisateur de NSX Manager.
- Le port 443 doit être ouvert entre NSX Manager et l'hôte ESXi, vCenter Server et les dispositifs NSX à déployer. Ce port est requis pour télécharger le fichier OVF sur l'hôte ESXi afin de le déployer.
- Un navigateur Web pris en charge pour la version de vSphere Web Client que vous utilisez. Consultez Utilisation de vSphere Web Client dans la documentation *Gestion de vCenter Server et des hôtes* pour obtenir des détails.

Ports et protocoles requis par NSX for vSphere

Les ports suivants doivent être ouverts pour que NSX for vSphere fonctionne correctement.

Note Si vous disposez d'un environnement cross-vCenter NSX et que vos systèmes vCenter Server sont en mode Enhanced Linked Mode, chaque dispositif NSX Manager doit disposer de la connectivité requise vers chaque système vCenter Server dans l'environnement pour gérer n'importe quel dispositif NSX Manager à partir de n'importe quel système vCenter Server.

Tableau 2-3. Ports et protocoles requis par NSX for vSphere

Source	Cible	Port	Protocole	Objectif	Données sensibles	TLS	Authentification
PC client	NSX Manager	443	TCP	Interface d'administration de NSX Manager	Non	Oui	Authentification PAM
PC client	NSX Manager	443	TCP	Accès au VIB de NSX Manager	Non	Non	Authentification PAM
Hôte ESXi	vCenter Server	443	TCP	Préparation d'hôtes ESXi	Non	Non	
vCenter Server	Hôte ESXi	443	TCP	Préparation d'hôtes ESXi	Non	Non	
Hôte ESXi	NSX Manager	5671	TCP	RabbitMQ	Non	Oui	Utilisateur/mot de passe de RabbitMQ
Hôte ESXi	NSX Controller	1234	TCP	Connexion de l'agent User World	Non	Oui	
NSX Controller	NSX Controller	2878, 2888, 3888	TCP	Cluster de contrôleurs - Synchronisation de l'état	Non	Oui	IPsec
NSX Controller	NSX Controller	7777	TCP	Port RPC inter-contrôleurs	Non	Oui	IPsec
NSX Controller	NSX Controller	30865	TCP	Cluster de contrôleurs - Synchronisation de l'état	Non	Oui	IPsec
NSX Manager	NSX Controller	443	TCP	Communication contrôleur-gestionnaire	Non	Oui	Utilisateur/Mot de passe
NSX Manager	vCenter Server	443	TCP	vSphere Web Access	Non	Oui	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	Non	Oui	
NSX Manager	Hôte ESXi	443	TCP	Connexion de gestion et de provisionnement	Non	Oui	

Tableau 2-3. Ports et protocoles requis par NSX for vSphere (suite)

Source	Cible	Port	Protocole	Objectif	Données sensibles	TLS	Authentification
NSX Manager	Hôte ESXi	902	TCP	Connexion de gestion et de provisionnement	Non	Oui	
NSX Manager	Serveur DNS	53	TCP	Connexion au client DNS	Non	Non	
NSX Manager	Serveur DNS	53	UDP	Connexion au client DNS	Non	Non	
NSX Manager	Serveur Syslog	514	TCP	Connexion Syslog	Non	Non	
NSX Manager	Serveur Syslog	514	UDP	Connexion Syslog	Non	Non	
NSX Manager	Serveur de temps NTP	123	TCP	Connexion au client NTP	Non	Oui	
NSX Manager	Serveur de temps NTP	123	UDP	Connexion au client NTP	Non	Oui	
vCenter Server	NSX Manager	80	TCP	Préparation de l'hôte	Non	Oui	
Client REST	NSX Manager	443	TCP	API REST de NSX Manager	Non	Oui	Utilisateur/Mot de passe
VXLAN Tunnel End Point (VTEP)	VXLAN Tunnel End Point (VTEP)	8472 (valeur par défaut avant NSX 6.2.3) ou 4789 (par défaut dans les nouvelles installations de NSX 6.2.3 et versions ultérieures)	UDP	Encapsulation du réseau de transport entre VTEP	Non	Oui	
Hôte ESXi	Hôte ESXi	6999	UDP	ARP sur LIF VLAN	Non	Oui	
Hôte ESXi	NSX Manager	8301, 8302	UDP	Synchronisation DVS	Non	Oui	

Tableau 2-3. Ports et protocoles requis par NSX for vSphere (suite)

Source	Cible	Port	Protocole	Objectif	Données sensibles	TLS	Authentification
NSX Manager	Hôte ESXi	8301, 8302	UDP	Synchronisation DVS	Non	Oui	
VM Guest Introspection	NSX Manager	5671	TCP	RabbitMQ	Non	Oui	Utilisateur/mot de passe de RabbitMQ
Instance principale de NSX Manager	Instance secondaire de NSX Manager	443	TCP	Service de synchronisation universelle de cross-vCenter NSX	Non	Oui	
Instance principale de NSX Manager	vCenter Server	443	TCP	vSphere API	Non	Oui	
Instance secondaire de NSX Manager	vCenter Server	443	TCP	vSphere API	Non	Oui	
Instance principale de NSX Manager	Cluster de contrôleur universel de NSX	443	TCP	API REST de NSX Controller	Non	Oui	Utilisateur/Mot de passe
Instance secondaire de NSX Manager	Cluster de contrôleur universel de NSX	443	TCP	API REST de NSX Controller	Non	Oui	Utilisateur/Mot de passe
Hôte ESXi	Cluster de contrôleur universel de NSX	1234	TCP	Protocole de plan de contrôle NSX	Non	Oui	
Hôte ESXi	Instance principale de NSX Manager	5671	TCP	RabbitMQ	Non	Oui	Utilisateur/mot de passe de RabbitMQ
Hôte ESXi	Instance secondaire de NSX Manager	5671	TCP	RabbitMQ	Non	Oui	Utilisateur/mot de passe de RabbitMQ

NSX et vSphere Distributed Switches

Dans un domaine NSX, NSX vSwitch est le logiciel qui fonctionne dans les hyperviseurs des serveurs pour former une couche d'abstraction logicielle entre des serveurs et le réseau physique.

NSX vSwitch est basé sur des vSphere Distributed Switches (VDS), qui fournissent des liaisons montantes assurant une connectivité hôte aux commutateurs physiques en haut de baie (Top-Of-Rack, TOR). Comme meilleure pratique, VMware recommande de planifier et de préparer vos vSphere Distributed Switches avant d'installer NSX for vSphere.

NSX Services n'est pas pris en charge sur vSphere Standard Switch. Les charges de travail VM doivent être connectées aux vSphere Distributed Switches pour utiliser les services et les fonctionnalités NSX.

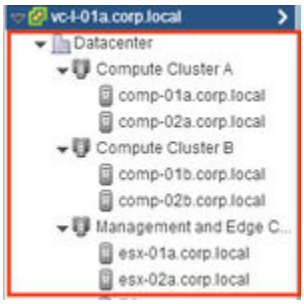
Un hôte spécifique peut être attaché à plusieurs VDS. Un seul VDS peut couvrir plusieurs hôtes dans plusieurs clusters. Pour chaque cluster d'hôtes qui participera à NSX, tous les hôtes du cluster doivent être attachés à un VDS commun.

Par exemple, supposons que vous disposiez d'un cluster incluant Hôte1 et Hôte2. Hôte1 est attaché à VDS1 et à VDS2. Hôte2 est attaché à VDS1 et à VDS3. Lorsque vous préparez un cluster pour NSX, vous pouvez uniquement associer NSX à VDS1 sur le cluster. Si vous ajoutez un autre hôte (Hôte3) au cluster et si Hôte3 n'est pas attaché à VDS1, cette configuration n'est pas valide et Hôte3 ne sera pas prêt pour la fonctionnalité NSX.

Souvent, pour simplifier un déploiement, chaque cluster d'hôtes est uniquement associé à un VDS, même si certains des VDS couvrent plusieurs clusters. Par exemple, supposons que vCenter contienne les cluster d'hôtes suivants :

- Cluster de calcul A pour les hôtes de la couche application
- Cluster de calcul B pour les hôtes de la couche Web
- Cluster de gestion et Edge pour les hôtes de gestion et Edge

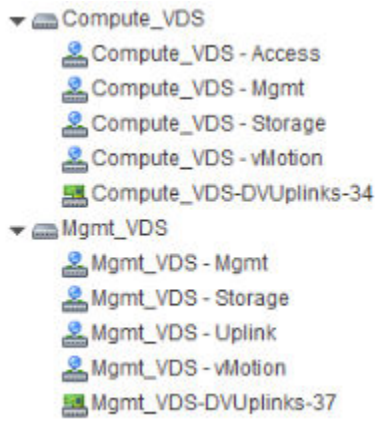
L'écran suivant montre comment ces clusters s'affichent dans vCenter.



Pour une telle conception de clusters, vous pouvez disposer de deux VDS nommés Compute_VDS et Mgmt_VDS. Compute_VDS couvre les deux clusters de calcul, et Mgmt_VDS est uniquement associé au cluster de gestion et Edge.

Chaque VDS contient des groupes de ports distribués pour les différents types de trafic à transporter. Les types de trafic courants incluent notamment gestion, stockage et vMotion. Des ports de liaison montante et d'accès sont aussi généralement requis. Normalement, un groupe de ports pour chaque type de trafic est créé sur chaque VDS.

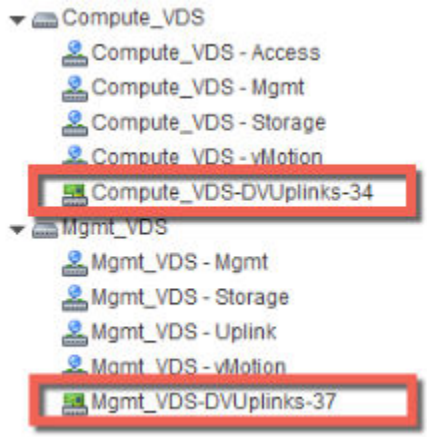
Par exemple, l'écran suivant montre comment ces Distributed Switches et ports s'affichent dans vCenter.



Chaque groupe de ports peut éventuellement être configuré avec un ID de VLAN. La liste suivante présente un exemple de l'association de VLAN avec les groupes de ports distribués pour fournir une isolation logique entre différents types de trafic :

- Compute_VDS - Access---VLAN 130
- Compute_VDS - Mgmt---VLAN 210
- Compute_VDS - Storage---VLAN 520
- Compute_VDS - vMotion---VLAN 530
- Mgmt_VDS - Uplink---VLAN 100
- Mgmt_VDS - Mgmt---VLAN 110
- Mgmt_VDS - Storage---VLAN 420
- Mgmt_VDS - vMotion---VLAN 430

Le groupe de ports DVUplinks est une jonction VLAN créée automatiquement lorsque vous créez un VDS. En tant que port de jonction, il envoie et reçoit des trames balisées. Par défaut, il transporte tous les ID de VLAN (0-4094). Cela signifie qu'un trafic incluant tout ID de VLAN peut être transmis via les adaptateurs réseau vmnic associés à l'emplacement DVUplink et filtré par les hôtes hyperviseurs lorsque le Distributed Switch détermine quel groupe de ports doit recevoir le trafic.



Si votre environnement vCenter existant contient des vSwitch standard plutôt que des Distributed Switches, vous pouvez migrer vos hôtes vers des Distributed Switches.

Exemple : utilisation d'un vSphere Distributed Switch

Cet exemple montre comment créer un nouveau vSphere Distributed Switch (VDS) ; ajouter des groupes de ports pour les types de trafic de gestion, de stockage et vMotion ; et migrer des hôtes d'un vSwitch standard vers le nouveau Distributed Switch.

Notez que cela n'est qu'un exemple servant à illustrer la procédure. Pour une analyse détaillée des liaisons montantes physiques et logiques VDS, reportez-vous au *Guide de conception de la virtualisation réseau de VMware NSX pour vSphere* à l'adresse https://communities.vmware.com/docs/DOC-27683.

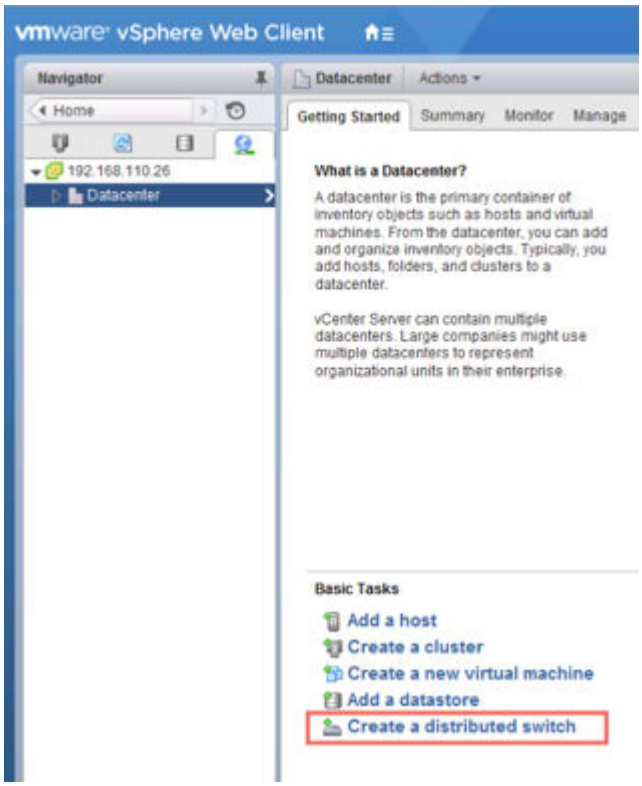
Conditions préalables

Cet exemple suppose que chaque hôte ESX à connecter au vSphere Distributed Switch dispose d'au moins une connexion à un commutateur physique (une liaison montante de vmnic). Cette liaison montante peut être utilisée pour le Distributed Switch et le trafic NSX VXLAN.

Procédure

1 Dans vSphere Web Client, accédez à un centre de données.

2 Cliquez sur **Créer un Distributed Switch (Create a Distributed Switch)**.



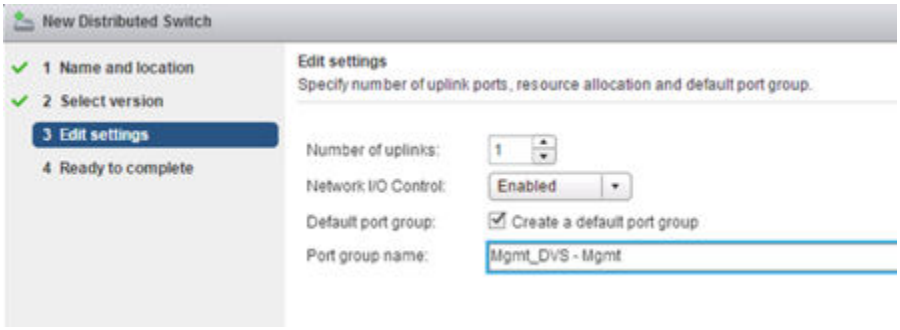
3 Donnez un nom significatif au commutateur basé sur le cluster d'hôtes qui lui sera associé.

Par exemple, si un Distributed Switch doit être associé à un cluster d'hôtes de gestion de centre de données, vous pouvez nommer le commutateur VDS_Mgmt.

4 Fournissez au moins une liaison montante au Distributed Switch, maintenez le contrôle d'E/S activé, puis donnez un nom significatif au groupe de ports par défaut. Notez qu'il n'est pas obligatoire de créer le groupe de ports par défaut. Vous pouvez le créer manuellement ultérieurement.

Par défaut, quatre liaisons montantes sont créées. Ajustez le nombre de liaisons montantes pour refléter votre conception de VDS. Le nombre de liaisons montantes requis est normalement égal au nombre de cartes réseau physiques que vous allouez au VDS.

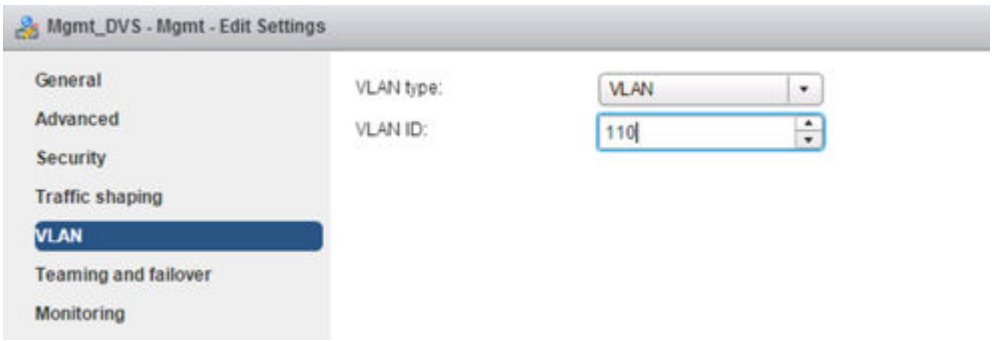
L'écran suivant montre un exemple de paramètres du trafic de gestion sur le cluster d'hôtes de gestion.



Le groupe de ports par défaut correspond simplement à l'un des groupes de ports que ce commutateur contiendra. Vous pourrez ajouter des groupes de ports pour différents types de trafic après la création du commutateur. Lors de la création d'un VDS, vous pouvez aussi décocher l'option **Créer un groupe de ports par défaut (Create a default port group)**. Cela peut constituer la meilleure pratique ; il est préférable d'être explicite lors de la création de groupes de ports.

5 (Facultatif) À la fin de l'assistant Nouveau Distributed Switch, modifiez les paramètres du groupe de ports par défaut pour le placer dans le VLAN approprié pour le trafic de gestion.

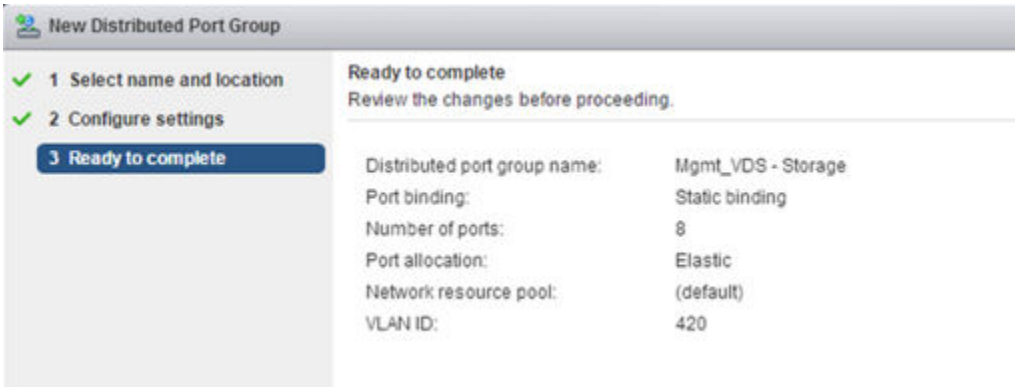
Par exemple, si vos interfaces de gestion d'hôtes se trouvent dans le VLAN 110, placez le groupe de ports par défaut dans le VLAN 110. Si vos interfaces de gestion d'hôtes ne se trouvent pas dans un VLAN, ignorez cette étape.



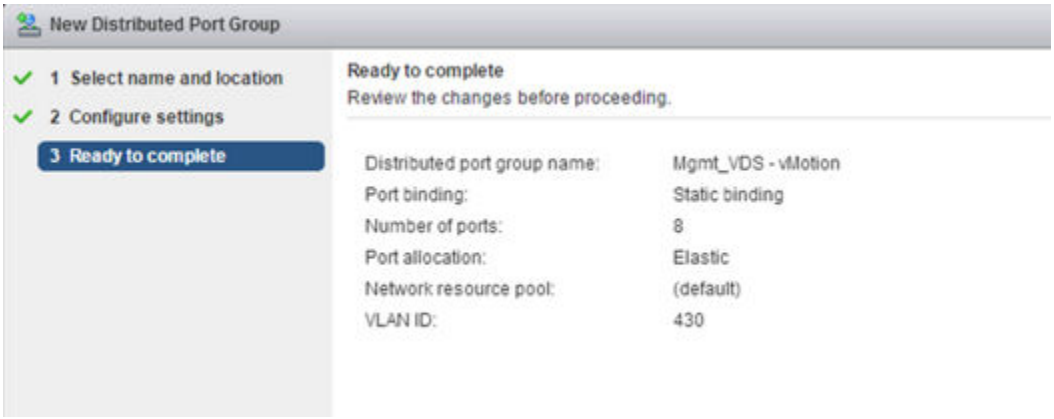
6 À la fin de l'assistant Nouveau Distributed Switch, cliquez avec le bouton droit sur le Distributed Switch et sélectionnez **Nouveau groupe de ports distribués (New Distributed Port Group)**.

Répétez cette étape pour chaque type de trafic, en veillant à fournir un nom significatif pour chaque groupe de ports et à configurer l'ID de VLAN approprié en fonction des exigences de séparation du trafic de votre déploiement.

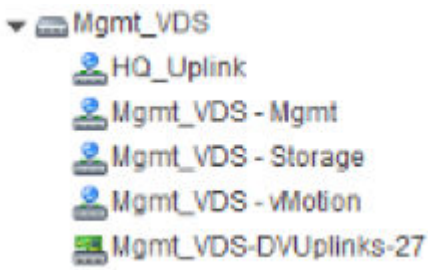
Exemple de paramètres de groupe pour le stockage.



Exemple de paramètres de groupe pour le trafic vMotion.

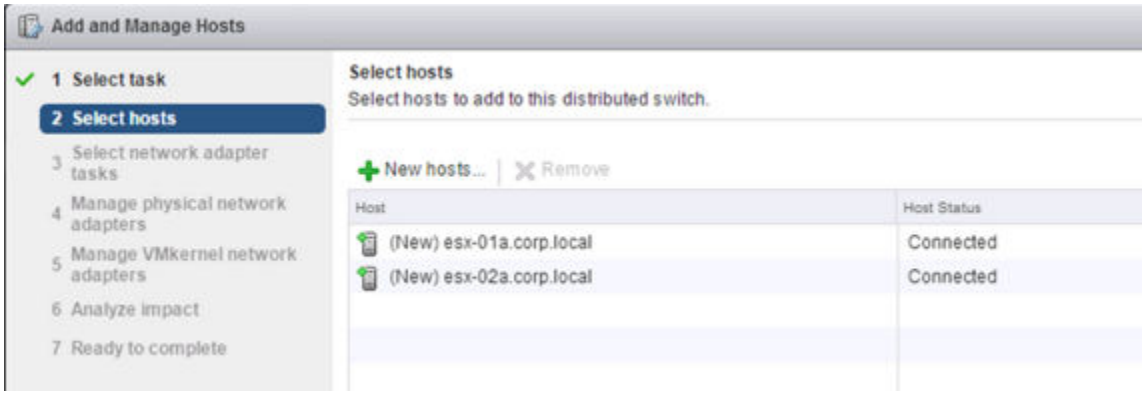


Le Distributed Switch et les groupes de ports résultants ont l'aspect suivant.

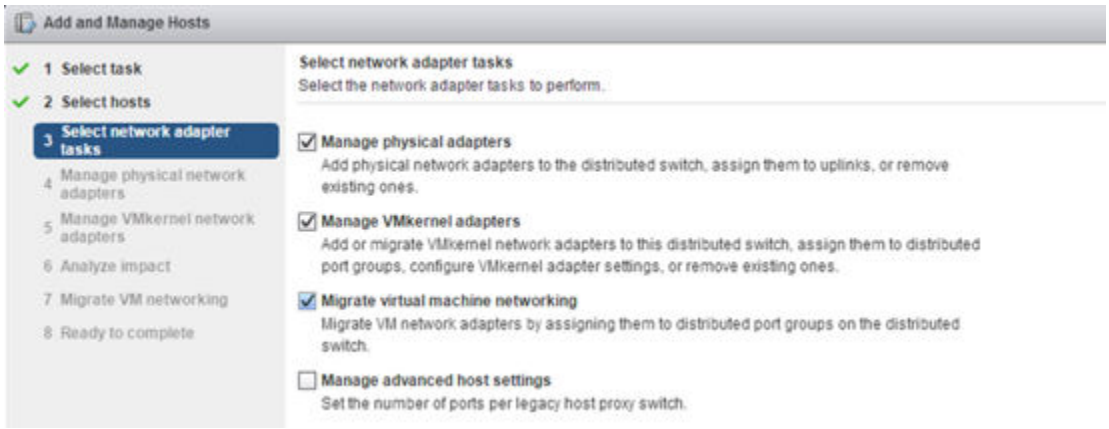


7 Cliquez avec le bouton droit sur le Distributed Switch, sélectionnez **Ajouter et gérer des hôtes (Add and Manage Hosts)**, puis **Ajouter des hôtes (Add Hosts)**.

Attachez tous les hôtes qui se trouvent dans le cluster associé. Par exemple, si le commutateur est destiné aux hôtes de gestion, sélectionnez tous les hôtes qui se trouvent dans le cluster de gestion.

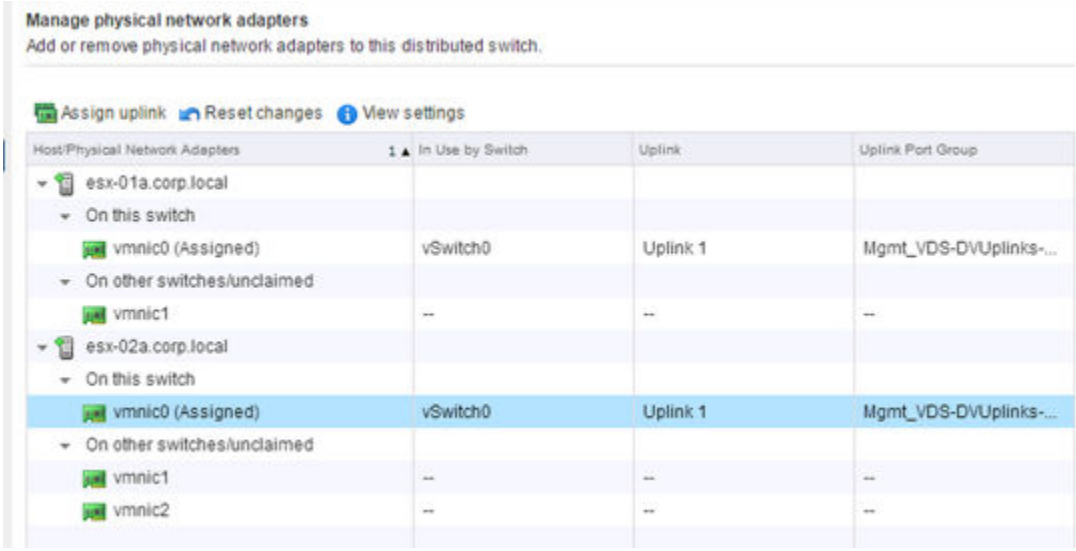


8 Sélectionnez les options pour migrer les adaptateurs physiques, les adaptateurs VMkernel et la mise en réseau de machines virtuelles.



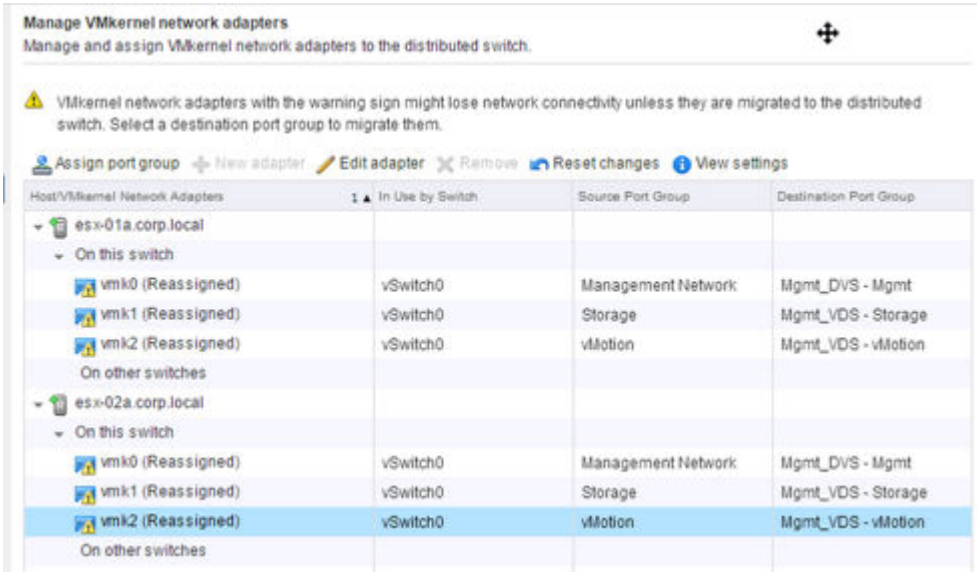
9 Sélectionnez une vmnic, puis cliquez sur **Attribuer une liaison montante (Assign uplink)** pour migrer la vmnic la vmnic à partir du vSwitch standard vers le Distributed Switch. Répétez cette étape pour chaque hôte que vous attachez au vSwitch distribué.

Par exemple, cet écran montre deux hôtes avec leurs liaisons montantes vmnic0 configurées pour une migration à partir de leur vSwitch standard respectif vers le groupe de ports distribués Mgmt_VDS-DVUplinks, qui est un port de jonction pouvant transporter n'importe quel ID de VLAN.



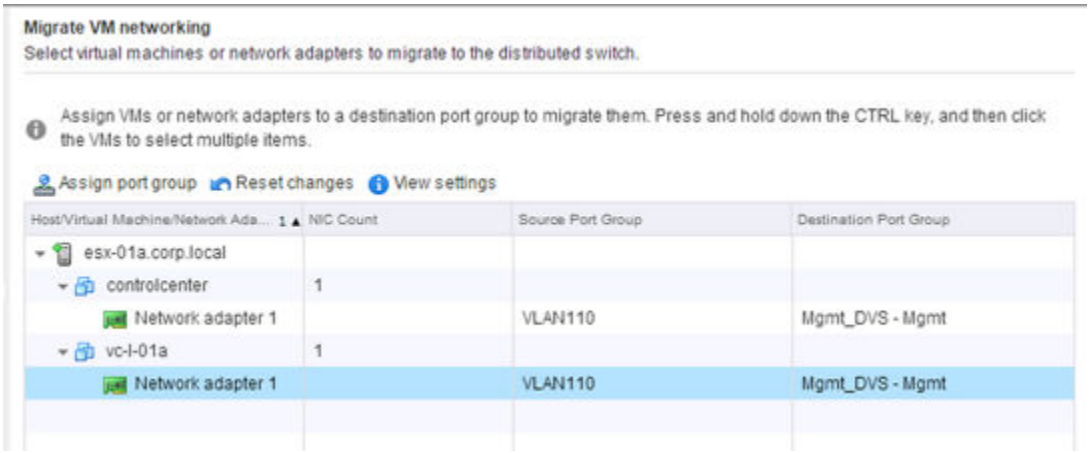
10 Sélectionnez un adaptateur réseau VMkernel, puis cliquez sur **Assigner un groupe de ports (Assign port group)**. Répétez cette étape pour tous les adaptateurs réseau sur tous les hôtes que vous attachez au vSwitch distribué.

Par exemple, cet écran montre trois adaptateurs réseau vmk sur deux hôtes configurés pour être migrés à partir des groupes de ports standard vers les nouveaux groupes de ports distribués.



11 Déplacez les machines virtuelles se trouvant sur les hôtes vers un groupe de ports distribués.

Par exemple, cet écran montre deux machines virtuelles sur un hôte spécifique à migrer à partir du groupe de ports standard vers le nouveau groupe de ports distribués.



Résultats

Une fois la procédure terminée, dans l'interface de ligne de commande de l'hôte, vous pouvez vérifier les résultats en exécutant les commandes suivantes :

- ```
  ~ # esxcli network vswitch dvs vmware list
  Mgmt_VDS
     Name: Mgmt_VDS
     VDS ID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
     Class: etherswitch
     Num Ports: 1862
     Used Ports: 5
     Configured Ports: 512
     MTU: 1600
     CDP Status: listen
     Beacon Timeout: -1
     Uplinks: vmnic0
     VMware Branded: true
     DVPort:
           Client: vmnic0
           DVPortgroup ID: dvportgroup-306
           In Use: true
           Port ID: 24

           Client: vmk0
           DVPortgroup ID: dvportgroup-307
           In Use: true
           Port ID: 0

           Client: vmk2
           DVPortgroup ID: dvportgroup-309
           In Use: true
           Port ID: 17

           Client: vmk1
           DVPortgroup ID: dvportgroup-308
           In Use: true
           Port ID: 9
  ```
  ```

- ```
  ~ # esxcli network ip interface list
  vmk2
     Name: vmk2
     MAC Address: 00:50:56:6f:2f:26
     Enabled: true
     Portset: DvsPortset-0
     Portgroup: N/A
     Netstack Instance: defaultTcpipStack
     VDS Name: Mgmt_VDS
     VDS UUID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
     VDS Port: 16
     VDS Connection: 1235399406
     MTU: 1500
     TSO MSS: 65535
     Port ID: 50331650

  vmk0
     Name: vmk0
     MAC Address: 54:9f:35:0b:dd:1a
     Enabled: true
     Portset: DvsPortset-0
     Portgroup: N/A
     Netstack Instance: defaultTcpipStack
     VDS Name: Mgmt_VDS
     VDS UUID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
     VDS Port: 2
     VDS Connection: 1235725173
     MTU: 1500
     TSO MSS: 65535
     Port ID: 50331651

  vmk1
     Name: vmk1
     MAC Address: 00:50:56:6e:a4:53
     Enabled: true
     Portset: DvsPortset-0
     Portgroup: N/A
     Netstack Instance: defaultTcpipStack
     VDS Name: Mgmt_VDS
     VDS UUID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
     VDS Port: 8
     VDS Connection: 1236595869
     MTU: 1500
     TSO MSS: 65535
     Port ID: 50331652
  ```

Étape suivante

Répétez le processus de migration pour tous les vSphere Distributed Switches.
  ```

Comprendre les modes de réplication

Lorsque vous créez une zone de transport ou un commutateur logique, vous devez sélectionner un mode de réplication. Comprendre les différents modes peut vous aider à déterminer celui qui est le plus adapté à votre environnement.

Chaque hôte ESXi préparé pour NSX est configuré avec un point de terminaison de tunnel VXLAN (VTEP). Chaque point de terminaison de tunnel VXLAN dispose d'une adresse IP. Ces adresses IP peuvent être dans le même sous-réseau ou dans des sous-réseaux différents.

Lorsque deux machines virtuelles sur des hôtes ESXi différents communiquent directement, le trafic de monodiffusion encapsulé est échangé entre les deux adresses IP de VTEP, sans saturation nécessaire. Cependant, comme avec n'importe quel réseau de couche 2, il arrive que le trafic en provenance d'une machine virtuelle doive être saturé ou envoyé à toutes les autres machines virtuelles appartenant au même commutateur logique. Le trafic de diffusion, de monodiffusion inconnue et de multidiffusion de couche 2 sont collectivement appelés trafic BUM. Le trafic BUM à partir d'une machine virtuelle sur un hôte donné doit être répliqué vers tous les autres hôtes sur lesquels des machines virtuelles sont connectées au même commutateur logique. NSX for vSphere prend en charge trois modes de réplication différents :

- Mode de réplication Monodiffusion
- Mode de réplication Multidiffusion
- Mode de réplication Hybride

Résumé des modes de réplication

Tableau 2-4. Résumé des modes de réplication

Mode de réplication	Méthode de réplication BUM vers les VTEP sur le même sous-réseau	Méthode de réplication BUM vers les VTEP sur un sous-réseau différent	Exigences en matière de réseau physique
Monodiffusion	Monodiffusion	Monodiffusion	■ Routage entre des sous-réseaux VTEP
Multidiffusion	Multidiffusion de couche 2	Multidiffusion de couche 3	■ Routage entre des sous-réseaux VTEP ■ Multidiffusion de couche 2, IGMP ■ Multidiffusion de couche 3, PIM ■ Attribution de groupes de multidiffusion à des commutateurs logiques
Hybride	Multidiffusion de couche 2	Monodiffusion	■ Routage entre des sous-réseaux VTEP ■ Multidiffusion de couche 2, IGMP

Mode de réplication Monodiffusion

Le mode de réplication monodiffusion ne nécessite pas de réseau physique pour prendre en charge la multidiffusion de couche 2 ou de couche 3 afin de gérer le trafic BUM au sein d'un commutateur logique. L'utilisation du mode Monodiffusion dissocie les réseaux logiques du réseau physique. Le mode Monodiffusion réplique tout le trafic BUM localement sur l'hôte source et transfère le trafic BUM aux hôtes distants dans un paquet de monodiffusion. En mode Monodiffusion, vous pouvez avoir tous les VTEP dans un sous-réseau ou dans plusieurs sous-réseaux.

Scénario d’un sous-réseau : si toutes les interfaces VTEP hôtes appartiennent à un seul sous-réseau, le VTEP source transfère le trafic BUM vers tous les VTEP distants. Cette action est appelée réplication de tête de réseau. La réplication de tête de réseau peut entraîner une capacité supplémentaire non souhaitée de l'hôte et une utilisation supérieure de bande passante. L'impact varie selon la quantité de trafic BUM et le nombre d'hôtes et de VTEP dans le sous-réseau.

Scénario de sous-réseau multiples : si les interfaces VTEP hôtes sont regroupées en plusieurs sous-réseaux IP, l'hôte source gère le trafic BUM en deux parties. Le VTEP source transfère le trafic BUM pour chaque VTEP dans le même sous-réseau (comme dans le scénario d’un sous-réseau). Pour les VTEP dans des sous-réseaux distants, le VTEP source transfère le trafic BUM vers un hôte dans chaque sous-réseau VTEP distant et définit le bit de réplication pour marquer ce paquet pour la réplication locale. Lorsqu'un hôte dans le sous-réseau distant reçoit ce paquet et détecte que le bit de réplication est défini, il envoie le paquet à tous les autres VTEP dans son sous-réseau sur lesquels le commutateur logique existe.

Par conséquent, le mode de réplication Monodiffusion évolue bien dans les architectures réseau ayant de nombreux sous-réseaux IP VTEP, car la charge est répartie entre plusieurs hôtes.

Mode de réplication Multidiffusion

Le mode de réplication Multidiffusion requiert que les multidiffusions de couche 2 et de couche 3 soient activées dans l'infrastructure physique. Pour configurer le mode Multidiffusion, l'administrateur réseau associe chaque commutateur logique à un groupe de multidiffusion IP. Pour les hôtes ESXi qui hébergent des machines virtuelles sur un commutateur logique spécifique, les VTEP associés rejoignent le groupe de multidiffusion à l'aide d'IGMP. Les routeurs suivent les jointures IGMP et créent une arborescence de distribution de multidiffusion entre eux à l'aide d'un protocole de routage de multidiffusion.

Lorsque les hôtes répliquent le trafic BUM vers des VTEP dans le même sous-réseau IP, ils utilisent la multidiffusion de couche 2. Lorsque les hôtes répliquent le trafic BUM vers des VTEP dans des sous-réseaux IP différents, ils utilisent la multidiffusion de couche 3. Dans les deux cas, la réplication du trafic BUM vers des VTEP distants est gérée par l'infrastructure physique.

Bien que la multidiffusion IP soit une technologie bien connue, le déploiement de la multidiffusion IP dans le centre de données est souvent considéré comme un obstacle, pour différentes raisons techniques, opérationnelles ou administratives. L'administrateur réseau doit faire preuve de prudence quant au nombre maximal d'états de multidiffusion pris en charge dans l'infrastructure physique pour activer le

mappage un à un entre le commutateur logique et le groupe de multidiffusion. L'un des avantages de la virtualisation est que celle-ci permet la mise à l'échelle de l'infrastructure virtuelle sans exposer l'infrastructure physique à des états supplémentaires. Le mappage de commutateurs logiques à des les groupes de multidiffusion « physiques » rompt ce modèle.

Note En mode de réplication Multidiffusion, le cluster NSX Controller n'est pas utilisé pour la commutation logique.

Mode de réplication Hybride

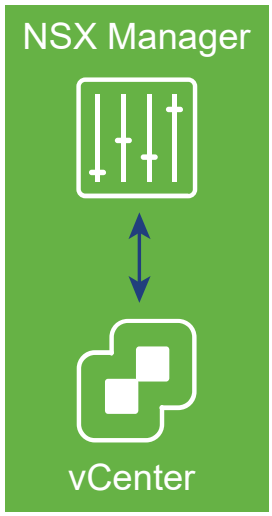
Le mode Hybride est un hybride entre les modes de réplication Multidiffusion et Monodiffusion. En mode de réplication Hybride, les VTEP hôtes utilisent la multidiffusion de couche 2 pour distribuer le trafic BUM aux VTEP homologue du même sous-réseau. Lorsque les VTEP hôtes répliquent le trafic BUM vers les VTEP de sous-réseaux différents, ils transfèrent le trafic sous forme de paquets de monodiffusion vers un seul hôte par sous-réseau VTEP. Cet hôte destinataire utilise à son tour la multidiffusion de couche 2 pour envoyer les paquets aux autres VTEP dans son sous-réseau.

La multidiffusion de couche 2 est plus courante dans les réseaux clients que la multidiffusion de couche 3, car elle est généralement plus facile à déployer. La réplication vers un VTEP différent du même sous-réseau est gérée dans le réseau physique. La réplication hybride peut représenter pour l'hôte source un soulagement significatif du trafic BUM s'il existe de nombreux VTEP homologues dans le même sous-réseau. Avec la réplication hybride, vous pouvez faire monter en puissance un environnement haute densité avec peu ou pas de segmentation.

Workflow d'installation de NSX et exemple de topologie

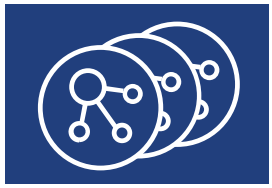
L'installation de NSX implique le déploiement de plusieurs dispositifs virtuels, la préparation des hôtes ESX et une configuration pour permettre la communication entre l'ensemble des périphériques physiques et virtuels.

1. Déployer NSX Manager



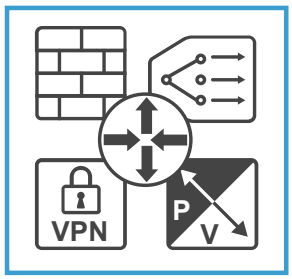
2. Enregistrer dans vCenter

3. Déployer des instances de NSX Controller



4. Préparer l'hôte

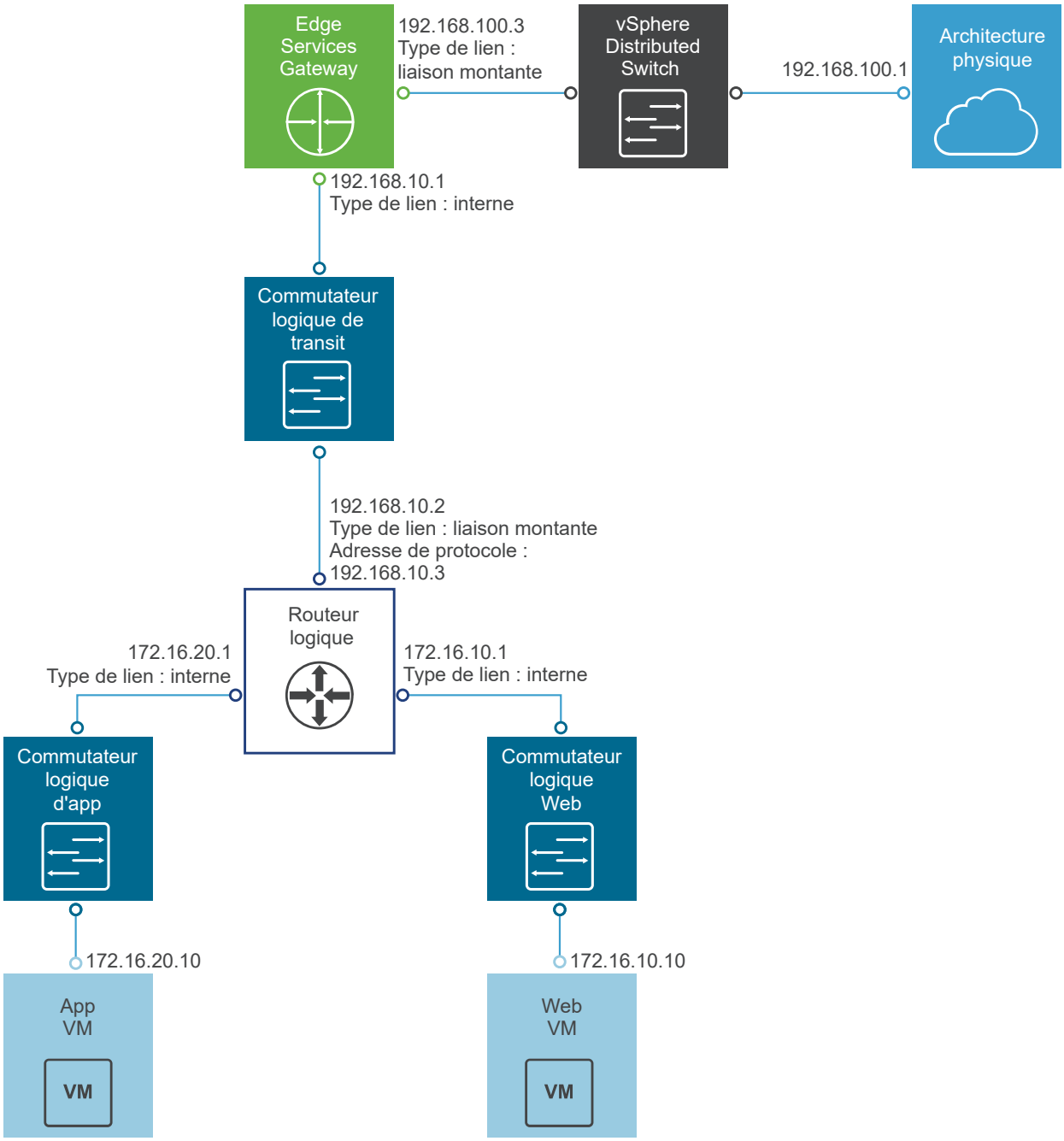
5. Configurer la mise en réseau logique, déployer et configurer la ou les passerelles NSX Edge Gateway et configurer les services réseau



Le processus commence par le déploiement d'un modèle NSX Manager OVF/OVA et la vérification que NSX Manager dispose d'une connectivité complète aux interfaces de gestion des hôtes ESX qu'il va gérer. Ensuite, NSX Manager et une instance vCenter doivent être liés réciproquement par un processus d'enregistrement. Cela permet ensuite le déploiement d'un cluster de contrôleurs NSX. Les contrôleurs NSX, à l'instar de NSX Manager, s'exécutent sous forme de dispositifs virtuels sur des hôtes ESX. L'étape suivante consiste à préparer les hôtes ESX pour NSX en y installant plusieurs VIB. Ces VIB activent la fonctionnalité VXLAN de couche 2, un routage distribué et la fonctionnalité du pare-feu distribué. Après la configuration de VXLAN, la spécification de plages d'interface réseau virtuelle (VNI) et la création de zones de transport, vous pouvez construire votre topologie de superposition NSX.

Ce guide d'installation décrit de façon détaillée chaque étape du processus.

Tout en étant applicable à n'importe quel déploiement NSX, ce guide présente les instructions de création d'un exemple de topologie de superposition NSX que vous pouvez utiliser à des fins d'exercice, d'assistance et de référence. L'exemple de superposition comporte un routeur logique distribué NSX (parfois nommé DLR), un dispositif ESG (Edge Services Gateway) et un commutateur de transit logique NSX connectant les deux périphériques de routage NSX. L'exemple de topologie inclut également les éléments d'une superposition, dont deux exemples de machines virtuelles. Ces machines virtuelles sont chacune connectées à un commutateur logique NSX distinct permettant la connectivité via le routeur logique NSX (DLR).


Edge Services Gateway
192.168.100.3
Type de lien : liaison montante
vSphere Distributed Switch
192.168.100.1
Architecture physique
192.168.10.1
Type de lien : interne
Commutateur logique de transit
192.168.10.2
Type de lien : liaison montante
Adresse de protocole : 192.168.10.3
Routeur logique
172.16.20.1
Type de lien : interne
172.16.10.1
Type de lien : interne
Commutateur logique d'app
Commutateur logique Web
172.16.20.10
172.16.10.10
App VM
VM
Web VM
VM

Cross-vCenter NSX et Enhanced Linked Mode

vSphere 6.0 introduit Enhanced Linked Mode, qui relie plusieurs systèmes vCenter Server en utilisant une ou plusieurs instances Platform Services Controller. Cela vous permet de consulter les inventaires de tous les systèmes vCenter Server liés dans vSphere Web Client et d'y effectuer des recherches. Dans un environnement cross-vCenter NSX, Enhanced Linked Mode vous permet de gérer toutes les instances de NSX Manager depuis une seule instance de vSphere Web Client.

Dans les grands déploiements qui comptent de nombreux serveurs vCenter, il peut être utile d'utiliser Cross-vCenter NSX avec Enhanced Linked Mode pour vCenter. Ces deux fonctionnalités sont complémentaires mais séparées.

Combinaison de Cross-vCenter NSX et Enhanced Linked Mode

Dans Cross-vCenter NSX, il y a une instance principale de NSX Manager et plusieurs instances secondaires. Chacune est liée à un vCenter Server séparé. Sur l'instance principale de NSX Manager, vous pouvez créer des composants NSX universels (tels que des commutateurs et des routeurs) consultables depuis les instances secondaires de NSX Manager.

Lorsque les systèmes vCenter Server individuels sont déployés avec Enhanced Linked Mode, ils peuvent tous être consultés et gérés depuis une seule instance vCenter Server de manière transparente.

Donc, lorsque Cross-vCenter NSX est combiné à Enhanced Linked Mode pour vCenter, vous pouvez consulter et gérer toutes les instances de NSX Manager et tous les composants NSX universels depuis n'importe quel système vCenter Server lié.

Utilisation de Cross-vCenter NSX sans Enhanced Linked Mode

L'utilisation de Enhanced Linked Mode n'est pas obligatoire ni exigée pour Cross-vCenter NSX. Sans Enhanced Linked Mode, vous pouvez toujours créer des zones de transport universelles, des commutateurs universels, des routeurs universels et des règles de pare-feu universelles Cross-vCenter. Toutefois, sans Enhanced Linked Mode, vous devez vous connecter aux instances vCenter Server individuelles pour accéder à chaque instance de NSX Manager.

Plus d'informations sur vSphere et Enhanced Linked Mode

Si vous décidez d'utiliser Enhanced Linked Mode, consultez le *Guide d'installation et de configuration vSphere* ou le *Guide de mise à niveau vSphere* pour connaître les dernières exigences concernant vSphere et Enhanced Linked Mode.

Installer le dispositif virtuel NSX Manager

3

NSX Manager est installé en tant que dispositif virtuel sur un hôte ESX de votre environnement vCenter.

NSX Manager fournit l'interface utilisateur graphique (GUI) et les API REST pour la création, la configuration et la surveillance de composants NSX, par exemple des contrôleurs, des commutateurs logiques et des dispositifs Edge Services Gateway. NSX Manager fournit une vue agrégée du système et constitue le composant de gestion réseau centralisée de NSX. La machine virtuelle NSX Manager est empaquetée dans un fichier OVA, ce qui vous permet d'utiliser vSphere Web Client pour importer NSX Manager dans la banque de données et l'inventaire de machines virtuelles.

Pour High Availability, VMware recommande de déployer NSX Manager dans un cluster configuré avec HA et DRS. Vous pouvez également installer NSX Manager dans un système vCenter différent de celui avec lequel NSX Manager va interopérer. Une instance unique de NSX Manager répond aux besoins d'un seul environnement vCenter Server.

Dans les installations de cross-vCenter NSX, assurez-vous que chaque instance de NSX Manager dispose d'un UUID unique. Les instances de NSX Manager déployées à partir de fichiers OVA ont des UUID uniques. Une instance de NSX Manager déployée à partir d'un modèle (comme lorsque vous convertissez une machine virtuelle en un modèle) aura le même UUID que l'instance d'origine de NSX Manager utilisée pour créer le modèle, et ces deux instances de NSX Manager ne peuvent pas être utilisées dans la même installation de cross-vCenter NSX. En d'autres termes, pour chaque instance de NSX Manager, vous devez installer un nouveau dispositif à partir de zéro de la manière décrite dans cette procédure.

L'installation d'une machine virtuelle NSX Manager inclut VMware Tools. Ne tentez pas de mettre à niveau ou d'installer VMware Tools sur l'instance de NSX Manager.

Lors de l'installation, vous pouvez choisir de participer au Programme d'amélioration du produit (CEIP) pour NSX. Consultez le Programme d'amélioration du produit dans le *Guide d'administration de NSX* pour plus d'informations sur le programme, y compris comment participer ou quitter le programme.

Conditions préalables

- Avant d'installer NSX Manager, assurez-vous que les ports requis sont ouverts. Reportez-vous à la section Ports et protocoles requis par NSX for vSphere.

- Assurez-vous qu'une banque de données est configurée et accessible sur l'hôte ESX cible. Un stockage partagé est recommandé. HA nécessite un stockage partagé afin que le dispositif NSX Manager puissent être redémarré sur un autre hôte si l'hôte d'origine est en panne.
- Assurez-vous de connaître l'adresse IP et la passerelle, les adresses IP du serveur DNS, la liste de recherche de domaines et les adresses IP du serveur NTP que NSX Manager utilisera.
- Décidez si NSX Manager disposera uniquement d'un adressage IPv4, uniquement d'un adressage IPv6 ou d'une configuration réseau à double pile. Le nom d'hôte de NSX Manager sera utilisé par d'autres entités. Il doit donc être mappé à l'adresse IP correcte dans les serveurs DNS utilisés dans ce réseau.
- Préparez un groupe de ports distribués de trafic de gestion sur lequel NSX Manager communiquera. Reportez-vous à la section Exemple : utilisation d'un vSphere Distributed Switch. L'interface de gestion de NSX Manager, vCenter Server et les interfaces de gestion d'hôtes ESXi doivent être accessibles par les instances de NSX Guest Introspection.
- Le plug-in d'intégration du client doit être installé. L'assistant Déployer un modèle OVF fonctionne mieux dans le navigateur Web Firefox. Parfois dans le navigateur Web Chrome, un message d'erreur sur l'installation du plug-in d'intégration de client s'affiche même si le plug-in est déjà installé. Pour installer le plug-in d'intégration du client :
  a Ouvrez un navigateur Web et tapez l'URL de vSphere Web Client.
  b Dans le bas de la page de connexion de vSphere Web Client, cliquez sur Télécharger le plug-in d'intégration du client.

  Si le plug-in d'intégration du client est déjà installé sur votre système, le lien de téléchargement ne s'affichera pas. Si vous désinstallez le plug-in d'intégration du client, le lien de téléchargement s'affichera sur la page de connexion de vSphere Web Client.

Procédure

1 Localisez le fichier OVA (Open Virtualization Appliance) de NSX Manager.

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

2 Dans Firefox, ouvrez vCenter.

3 Sélectionnez **VM et modèles (VMs and Templates)**, cliquez avec le bouton droit sur votre centre de données, puis sélectionnez **Déployer un modèle OVF (Deploy OVF Template)**.

4 Collez l'URL de téléchargement ou cliquez sur **Parcourir (Browse)** pour sélectionner le fichier sur votre ordinateur.

Note Si l'installation échoue avec un message d'erreur indiquant que l'`opération a expiré`, vérifiez les périphériques de stockage et de réseau pour voir s'il n'y a pas un problème de connectivité. Ce problème survient en effet en cas de problème au niveau de l'infrastructure physique, comme une perte de connectivité au niveau du périphérique de stockage ou un problème de connectivité avec la carte réseau ou le commutateur physique.

5 Cochez la case **Accepter les options de configuration supplémentaires (Accept extra configuration options)**.

Cela vous permet de définir les propriétés des adresses IPv4 et IPv6, de la passerelle par défaut ainsi que les propriétés DNS, NTP et SSH lors de l'installation, plutôt que de les configurer manuellement après l'installation.

6 Acceptez les contrats de licence VMware.

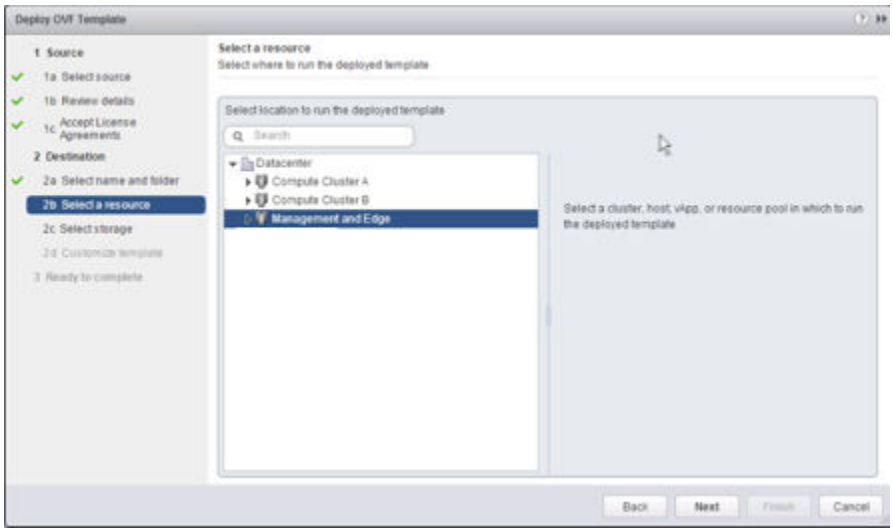
7 Modifiez le nom de NSX Manager (si nécessaire) et sélectionnez l'emplacement de l'instance déployée de NSX Manager

Le nom que vous tapez s'affiche dans l'inventaire vCenter.

Le dossier que vous sélectionnez sera utilisé pour appliquer des autorisations à l'instance de NSX Manager.

8 Sélectionnez un hôte ou un cluster sur lequel déployer le dispositif NSX Manager.

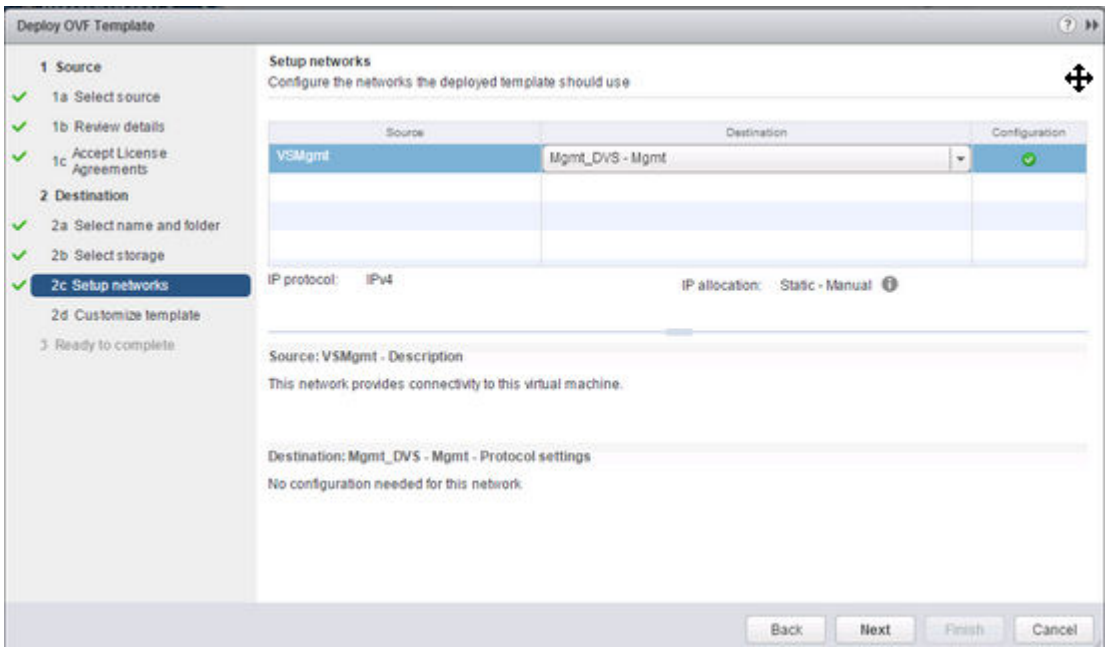
Par exemple :



9 modifiez le format du disque virtuel et utilisez **Provisionnement statique (Thick Provision)**, puis sélectionnez la banque de données pour les fichiers de configuration de la machine virtuelle et des disques virtuels.

10 Sélectionnez le groupe de ports pour l'instance de NSX Manager.

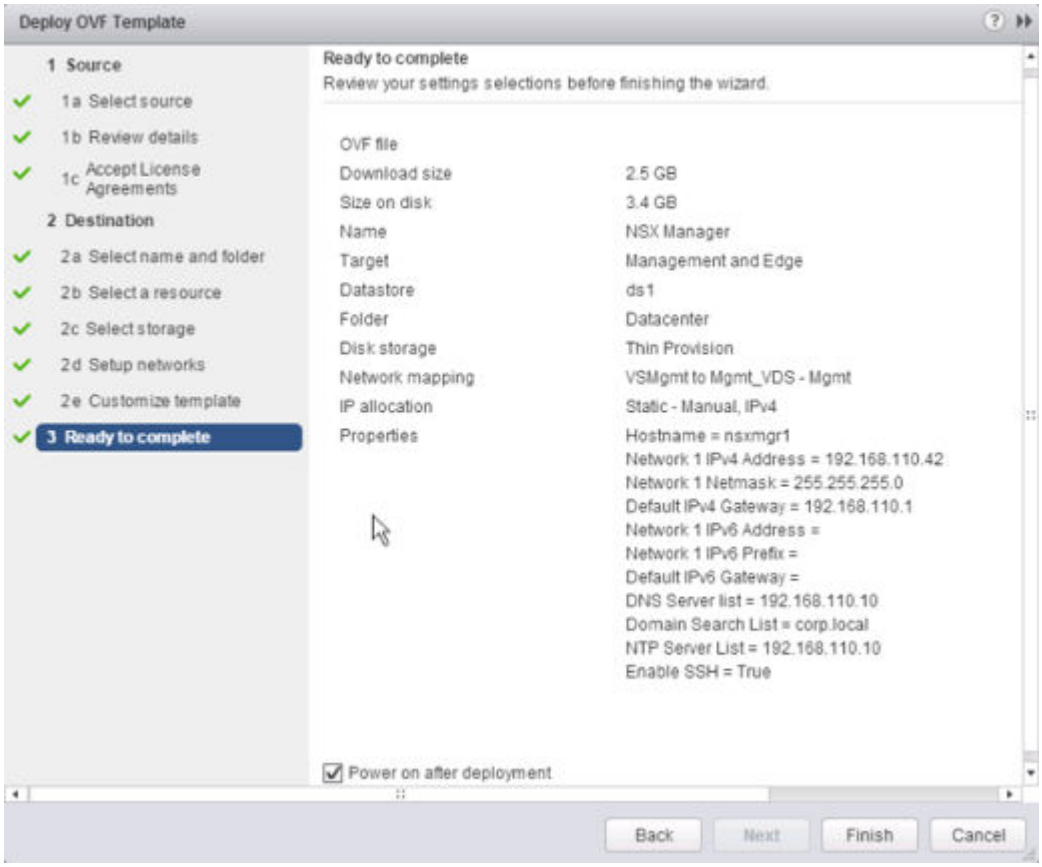
Par exemple, cette copie d'écran montre la sélection du groupe de ports Mgmt_DVS - Mgmt.



11 (Facultatif) Cochez la case **Participer au programme d'amélioration du produit (Join the Customer Experience Improvement Program)**.

12 Définissez les options de configuration supplémentaires de NSX Manager.

Par exemple, cet écran montre l'écran de révision finale après que toutes les options ont été configurées dans un déploiement exclusivement IPv4.



Résultats

Ouvrez la console de NSX Manager pour suivre le processus de démarrage.

Dès que NSX Manager a complètement démarré, connectez-vous à l'interface de ligne de commande et exécutez la commande `show interface` pour vérifier que l'adresse IP a été appliquée comme prévu.

```
nsxmgr1> show interface
Interface mgmt is up, line protocol is up
  index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:8e:c7:fa
  inet 192.168.110.42/24 broadcast 192.168.110.255
  inet6 fe80::250:56ff:fe8e:c7fa/64
  Full-duplex, 0Mb/s
    input packets 1370858, bytes 389455808, dropped 50, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 1309779, bytes 2205704550, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

Assurez-vous que NSX Manager peut effectuer un test ping sur sa passerelle par défaut, son serveur NTP, le serveur vCenter Server et l'adresse IP de l'interface de gestion de tous les hôtes hyperviseurs qu'il va gérer.

Connectez-vous à l'interface utilisateur graphique du dispositif NSX Manager en ouvrant un navigateur Web et en accédant à l'adresse IP ou au nom d'hôte de NSX Manager.

Après vous être connecté en tant qu'**administrateur (admin)** à l'aide du mot de passe défini durant l'installation, à partir de la page d'accueil, cliquez sur **Afficher le résumé (View Summary)** et assurez-vous que les services suivants sont en cours d'exécution :

- vPostgres
- RabbitMQ
- Services de gestion NSX

Pour bénéficier de performances optimales, VMware recommande de réserver de la mémoire pour le dispositif virtuel NSX Manager. Une réservation de mémoire est une limite inférieure garantie sur la quantité de mémoire physique que l'hôte réserve à une machine virtuelle, même lorsque la mémoire est surchargée. Définissez la réservation à un niveau qui garantit que NSX Manager dispose de suffisamment de mémoire pour s'exécuter efficacement.

Étape suivante

Enregistrez vCenter Server dans NSX Manager.

Enregistrer vCenter Server sur NSX Manager

4

NSX Manager et vCenter Server entretiennent une relation de type un à un. À chaque instance de NSX Manager correspond un serveur vCenter Server, y compris dans un environnement cross-vCenter NSX.

Vous ne pouvez enregistrer qu'une seule instance de NSX Manager dans un système vCenter Server. La modification de l'enregistrement de vCenter d'une instance de NSX Manager configurée n'est pas prise en charge.

Pour modifier l'enregistrement de vCenter d'une instance de NSX Manager existante, vous devez tout d'abord supprimer toutes les configurations de NSX for vSphere, puis supprimer le plug-in NSX Manager du système vCenter Server. Pour obtenir des instructions, reportez-vous à la section Supprimer une installation NSX en toute sécurité. Vous pouvez également déployer un nouveau dispositif NSX Manager pour l'enregistrer dans le nouveau système vCenter Server.

Si nécessaire, vous pouvez modifier le compte d'utilisateur de vCenter Server utilisé pour l'enregistrement dans NSX Manager. Le compte d'utilisateur de vCenter Server qui est utilisé pour l'enregistrement doit être membre du groupe **Administrateurs** de vCenter Single Sign-On.

Conditions préalables

- Le service de gestion NSX doit être en cours d'exécution. Dans l'interface Web de NSX Manager à l'adresse `https://<nsx-manager-ip>`, cliquez sur **Accueil (Home) > Afficher le résumé (View Summary)** pour afficher l'état du service.
- Vous devez utiliser un compte utilisateur vCenter Server qui est membre du groupe **Administrateurs** de vCenter Single Sign-On pour synchroniser NSX Manager avec le système vCenter Server. Si le mot de passe du compte comporte des caractères qui ne sont pas au format ASCII, vous devez le modifier avant de synchroniser NSX Manager avec le système vCenter Server. N'utilisez pas le compte racine.

  Pour plus d'informations sur l'ajout d'utilisateurs, reportez-vous à la section « Gestion des utilisateurs et des groupes vCenter Single Sign-On » dans la documentation *Administration de Platform Services Controller*.
- Vérifiez que la résolution de nom directe et inverse fonctionne et que les systèmes suivants peuvent résoudre mutuellement leurs noms DNS :
  - Dispositifs NSX Manager

- Systèmes vCenter Server
- Systèmes Platform Services Controller
- Hôtes ESXi

Procédure

1 Connectez-vous au dispositif virtuel NSX Manager.

Dans un navigateur Web, accédez à l'interface utilisateur graphique du dispositif NSX Manager à l'adresse https://<nsx-manager-ip> ou https://<nsx-manager-hostname> et connectez-vous en tant qu'**administrateur** ou avec un compte avec le rôle **Administrateur d'entreprise**.

2 Dans la page d'accueil, cliquez sur **Gérer l'enregistrement de vCenter (Manage vCenter Registration)**.

3 Modifiez l'élément vCenter Server afin qu'il pointe vers l'adresse IP ou le nom d'hôte du système vCenter Server, et entrez le nom d'utilisateur et le mot de passe du système vCenter Server.

4 Vérifiez que l'empreinte du certificat correspond au certificat du système vCenter Server.

Si vous avez installé un certificat signé par une autorité de certification sur le systèmevCenter Server , vous recevez l'empreinte de ce certificat. Sinon, vous recevez un certificat auto-signé.

5 Ne cochez pas **Modifier l'emplacement de téléchargement du script de plug-in (Modify plugin script download location)**, sauf si l'instance de NSX Manager se trouve derrière un pare-feu de type périphérique de masquage.

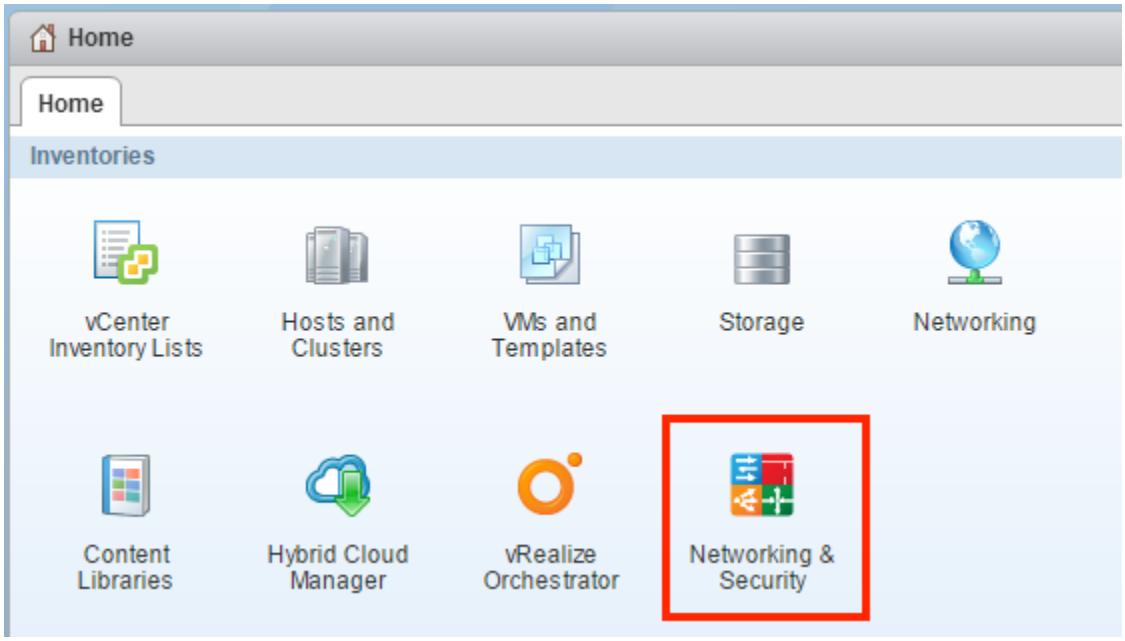
Cette option permet d'entrer une autre adresse IP pour NSX Manager. Il n'est pas recommandé de placer NSX Manager derrière un pare-feu de ce type.

6 Vérifiez que l'état du système vCenter Server est **Connecté (Connected)**.

7 Si vSphere Web Client est déjà ouvert, déconnectez-vous, puis reconnectez-vous avec le compte utilisé pour enregistrer NSX Manager avec vCenter Server.

Si vous ne vous déconnectez et reconnectez pas, vSphere Web Client n'affiche pas l'icône **Mise en réseau et sécurité (Networking & Security)** dans l'onglet **Accueil (Home)**.

Cliquez sur l'icône **Mise en réseau et sécurité (Networking & Security)** et vérifiez que la nouvelle instance déployée de NSX Manager est visible.



Étape suivante

Planifiez une sauvegarde des données de l'instance de NSX Manager immédiatement après l'installation de NSX Manager. Reportez-vous à la section Sauvegarde et restauration de NSX du *Guide d'administration de NSX*.

Si vous disposez d'une solution de partenaire NSX for vSphere, reportez-vous à la documentation du partenaire pour obtenir des informations sur l'enregistrement de la console du partenaire dans NSX Manager.

Vous pouvez maintenant installer et configurer les composants NSX for vSphere.

Configurer Single Sign-On

5

SSO renforce la sécurité de vSphere et NSX en autorisant les divers composants à communiquer entre eux par le biais d'un mécanisme sécurisé d'échange de jetons au lieu d'exiger que chaque composant authentifie un utilisateur séparément.

Vous pouvez configurer Lookup Service sur l'instance de NSX Manager et fournir les informations de connexion de l'administrateur SSO pour enregistrer le service de gestion NSX en tant qu'utilisateur SSO. L'intégration du service SSO (Single Sign-On) à NSX améliore la sécurité de l'authentification des utilisateurs vCenter et permet à NSX d'authentifier ces derniers à partir d'autres services d'identité tels qu'AD, NIS et LDAP. Avec SSO, NSX prend en charge l'authentification en utilisant des jetons SAML (Security Assertion Markup Language) authentifiés provenant d'une source approuvée via des appels API REST. NSX Manager peut également acquérir des jetons d'authentification SAML à utiliser avec d'autres solutions VMware.

NSX met en cache les informations de groupe pour les utilisateurs SSO. Les modifications apportées aux appartenances à un groupe se propagent en 60 minutes du fournisseur d'identité (par exemple Active Directory) à NSX.

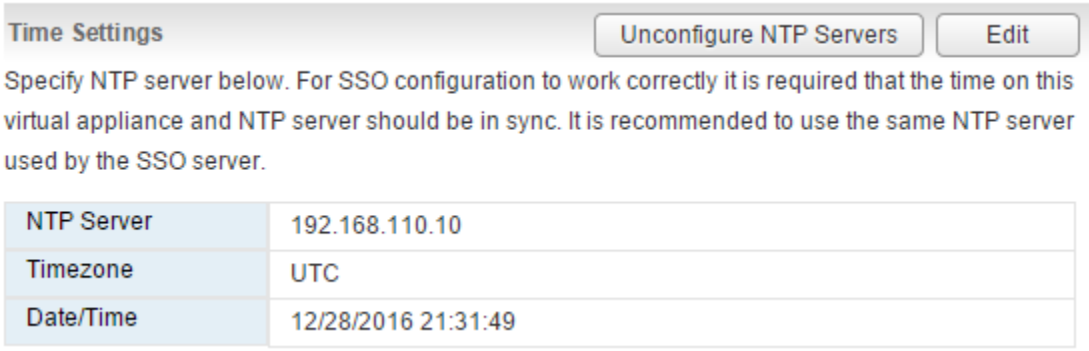
Conditions préalables

- Pour utiliser SSO sur NSX Manager, vous devez disposer de vCenter Server 5.5 ou d'une version ultérieure. En outre, le service d'authentification SSO doit être installé sur vCenter Server. Notez que cela s'applique à la version intégrée de SSO. À la place, votre déploiement peut utiliser un serveur SSO centralisé externe.

  Pour des informations relatives aux services SSO fournis par vSphere, consultez http://kb.vmware.com/kb/2072435 et http://kb.vmware.com/kb/2113115.

- Le serveur NTP doit être spécifié de sorte que l'heure du serveur SSO et l'heure de NSX Manager soient synchronisées.

  Par exemple :



Procédure

1 Connectez-vous au dispositif virtuel NSX Manager.

Dans un navigateur Web, accédez à l'interface utilisateur graphique du dispositif NSX Manager à l'adresse https://<nsx-manager-ip> ou https://<nsx-manager-hostname> et connectez-vous en tant qu'**administrateur** ou avec un compte avec le rôle **Administrateur d'entreprise**.

2 Connectez-vous au dispositif virtuel NSX Manager.

3 Dans la page d'accueil, cliquez sur **Gérer les paramètres des dispositifs (Manage Appliance Settings) > NSX Management Service**.

4 Cliquez sur **Modifier (Edit)** dans la section URL de Lookup Service.

5 Entrez le nom ou l'adresse IP de l'hôte qui dispose de Lookup Service.

6 Entrez le numéro de port.

Entrez le port 443 si vous utilisez vSphere 6.0. Pour vSphere 5.5, utilisez le numéro de port 7444.

L'URL de Lookup Service s'affiche en fonction de l'hôte et du port spécifiés.

7 Entrez le nom d'utilisateur et le mot de passe de l'administrateur SSO, puis cliquez sur **OK**.

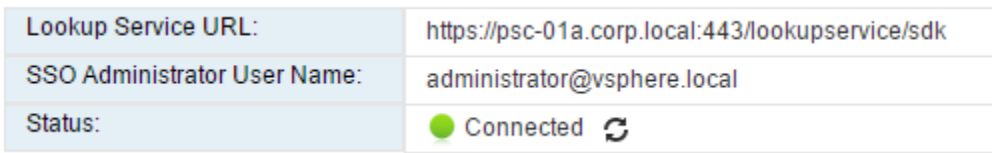
L'empreinte du certificat du serveur SSO s'affiche.

8 Vérifiez que l'empreinte du certificat correspond au certificat du serveur SSO.

Si vous avez installé un certificat signé par une autorité de certification sur le serveur d'autorité de certification, vous recevez l'empreinte de ce certificat. Sinon, vous recevez un certificat auto-signé.

9 Confirmez que l'état de Lookup Service est **Connecté (Connected)**.

Par exemple :



Étape suivante

Consultez la section Attribuer un rôle à un utilisateur vCenter dans le *Guide d'administration de NSX*.

Configurer un serveur Syslog pour NSX Manager

6

Si vous spécifiez un serveur Syslog, NSX Manager envoie l'ensemble de ses journaux d'audit et événements système au serveur Syslog.

Les données syslog sont particulièrement utiles pour la résolution des problèmes et la révision des données journalisées pendant l'installation et la configuration.

NSX Edge prend en charge deux serveurs Syslog. NSX Manager et NSX Controller prennent en charge un serveur Syslog.

Procédure

1 Connectez-vous au dispositif virtuel NSX Manager.

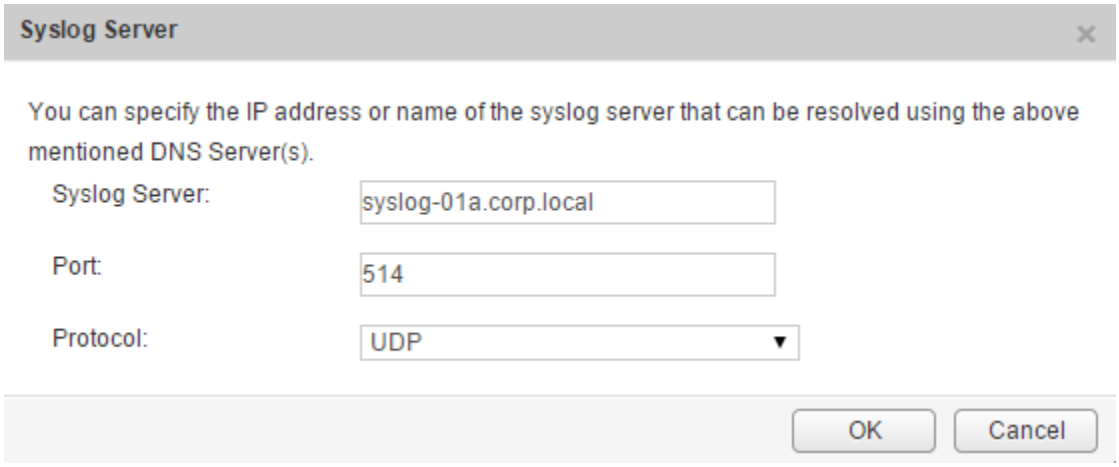
Dans un navigateur Web, accédez à l'interface utilisateur graphique du dispositif NSX Manager à l'adresse https://<nsx-manager-ip> ou https://<nsx-manager-hostname> et connectez-vous en tant qu'**administrateur** ou avec un compte avec le rôle **Administrateur d'entreprise**.

2 Dans la page d'accueil, cliquez sur **Gérer les paramètres des dispositifs (Manage Appliance Settings) > Général (General)**.

3 Cliquez sur **Modifier (Edit)** en regard de **Serveur syslog (Syslog Server)**.

4 Tapez l'adresse IP ou le nom d'hôte, le port et le protocole du serveur syslog.

Par exemple :



5 Cliquez sur **OK**.

Résultats

La journalisation à distance de NSX Manager est activée et les fichiers journaux sont stockés dans votre serveur Syslog autonome.

Installer et attribuer une licence NSX for vSphere

7

Vous pouvez installer et attribuer une licence NSX for vSphere après avoir installé NSX Manager à l'aide de vSphere Web Client.

À partir de NSX 6.2.3, la licence par défaut lors de l'installation sera NSX pour vShield Endpoint. Cette licence permet d'utiliser NSX pour déployer et gérer vShield Endpoint pour la capacité de déchargement d'antivirus uniquement. Elle dispose de la contrainte de mise en conformité inconditionnelle pour limiter l'utilisation de VXLAN, du pare-feu et des services Edge, en bloquant la préparation de l'hôte et la création de dispositifs NSX Edge.

Si vous avez besoin d'autres fonctionnalités de NSX, y compris des commutateurs logiques, des routeurs logiques, le pare-feu distribué ou NSX Edge, vous devez acheter une licence NSX pour utiliser ces fonctionnalités ou demander une licence d'évaluation pour en faire une évaluation à court terme.

Pour plus d'informations sur les éditions de licence NSX et les fonctionnalités associées, voir https://kb.vmware.com/kb/2145269.

Procédure

- Dans vSphere 5.5, effectuez les étapes suivantes pour ajouter une licence pour NSX.
  a. Connectez-vous à vSphere Web Client.
  b. Cliquez sur **Administration**, puis sur **Licences (Licenses)**.
  c. Cliquez sur l'onglet **Solutions**.
  d. Sélectionnez NSX for vSphere dans la liste Solutions. Cliquez sur **Attribuer une clé de licence (Assign a license key)**.
  e. Sélectionnez **Attribuer une nouvelle clé de licence (Assign a new license key)** dans le menu déroulant.
  f. Tapez la clé de licence, puis un libellé facultatif pour la nouvelle clé.
  g. Cliquez sur **Décoder (Decode)**.

     Décodez la clé de licence pour vérifier si son format est correct et si elle dispose d'une capacité suffisante pour attribuer une licence aux ressources.
  h. Cliquez sur **OK**.

- Dans vSphere 6.0, effectuez les étapes suivantes pour ajouter une licence pour NSX.
  a. Connectez-vous à vSphere Web Client.
  b. Cliquez sur **Administration**, puis sur **Licences (Licenses)**.
  c. Cliquez sur l'onglet **Actifs (Assets)**, puis sur l'onglet **Solutions**.
  d. Sélectionnez NSX for vSphere dans la liste Solutions. Dans le menu déroulant **Toutes les actions (All Actions)**, sélectionnez **Attribuer une licence... (Assign license...)**.
  e. Cliquez sur l'icône **Ajouter (Add) (** **)**. Entrez une clé de licence et cliquez sur **Suivant (Next)**. Ajoutez un nom pour la licence et cliquez sur **Suivant (Next)**. Cliquez sur **Terminer (Finish)** pour ajouter la licence.
  f. Sélectionnez la nouvelle licence.
  g. (Facultatif) Cliquez sur l'icône **Afficher les fonctionnalités (View Features)** pour voir quelles fonctionnalités sont activées avec cette licence. Affichez la colonne **Capacité (Capacity)** pour voir la capacité de la licence.
  h. Cliquez sur **OK** pour attribuer la nouvelle licence à NSX.

Étape suivante

Pour plus d'informations sur les licences de NSX, reportez-vous à http://www.vmware.com/files/pdf/vmware-product-guide.pdf.

Déployer le cluster NSX Controller

8

NSX Controller est un système avancé de gestion des états distribués qui fournit des fonctions de plan de contrôle pour les fonctions de commutation et de routage logiques NSX. C'est le point de contrôle central de tous les commutateurs logiques d'un réseau qui maintient des informations sur tous les hôtes, les commutateurs logiques (VXLAN) et les routeurs logiques distribués. Des instances de NSX Controller sont requises si vous prévoyez de déployer 1) des routeurs logiques distribués ou 2) VXLAN en mode monodiffusion ou hybride.

Quelle que soit la taille de votre déploiement NSX, VMware requiert que chaque cluster NSX Controller contienne trois nœuds de contrôleur. Les clusters qui ne respectent pas ce critère ne sont pas pris en charge.

Pour le cluster, il est impératif que le système de stockage sur disque de chaque contrôleur présente une latence d'écriture maximale inférieure à 300 ms et une latence d'écriture moyenne inférieure à 100 ms. Si le système de stockage ne respecte pas ces exigences, le cluster risque de devenir instable et d'entraîner l'interruption du système.

Attention Lorsque l'état d'un contrôleur est **Déploiement (Deploying)**, n'ajoutez pas ou ne modifiez pas des interrupteurs logiques ou le routage distribué dans votre environnement. De plus, ne poursuivez pas avec la procédure de préparation de l'hôte. Après l'ajout d'un nouveau contrôleur au cluster de contrôleur, tous les contrôleurs sont inactifs pour un court moment (pas plus de 5 minutes). Pendant cette interruption, toute opération relative aux contrôleurs (telle que la préparation d'un hôte) peut provoquer des résultats inattendus. Même si la préparation d'un hôte peut sembler avoir été réalisée avec succès, il est possible que la certification SSL ne soit pas correctement établie, entraînant des problèmes sur le réseau VXLAN.

Conditions préalables

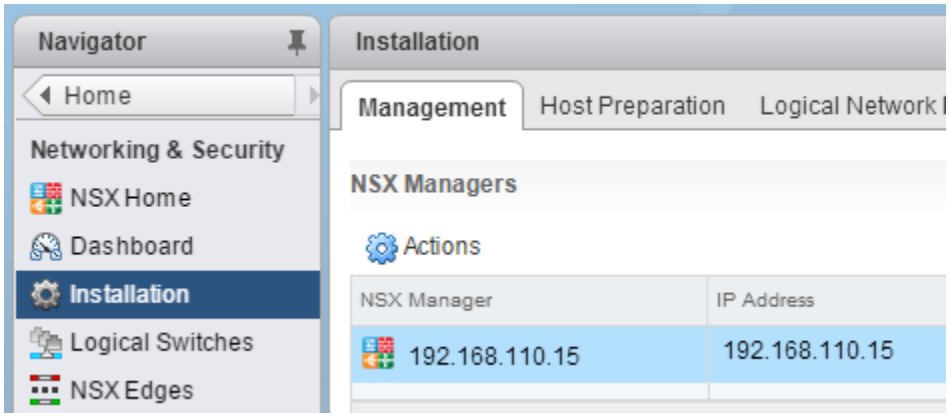
- Avant de déployer des instances de NSX Controller, vous devez déployer un dispositif NSX Manager et enregistrer vCenter dans NSX Manager.
- Déterminez les paramètres de pool IP de votre cluster de contrôleurs, notamment la passerelle et la plage d'adresses IP. Les paramètres DNS sont facultatifs. Le réseau IP de NSX Controller doit disposer d'une connectivité à NSX Manager et aux interfaces de gestion des hôtes ESXi.

Procédure

1 Connectez-vous à vSphere Web Client.

2 Accédez à **Accueil > Networking & Security > Installation (Home > Networking & Security > Installation)**, puis sélectionnez l'onglet **Gestion (Management)**.

Par exemple :

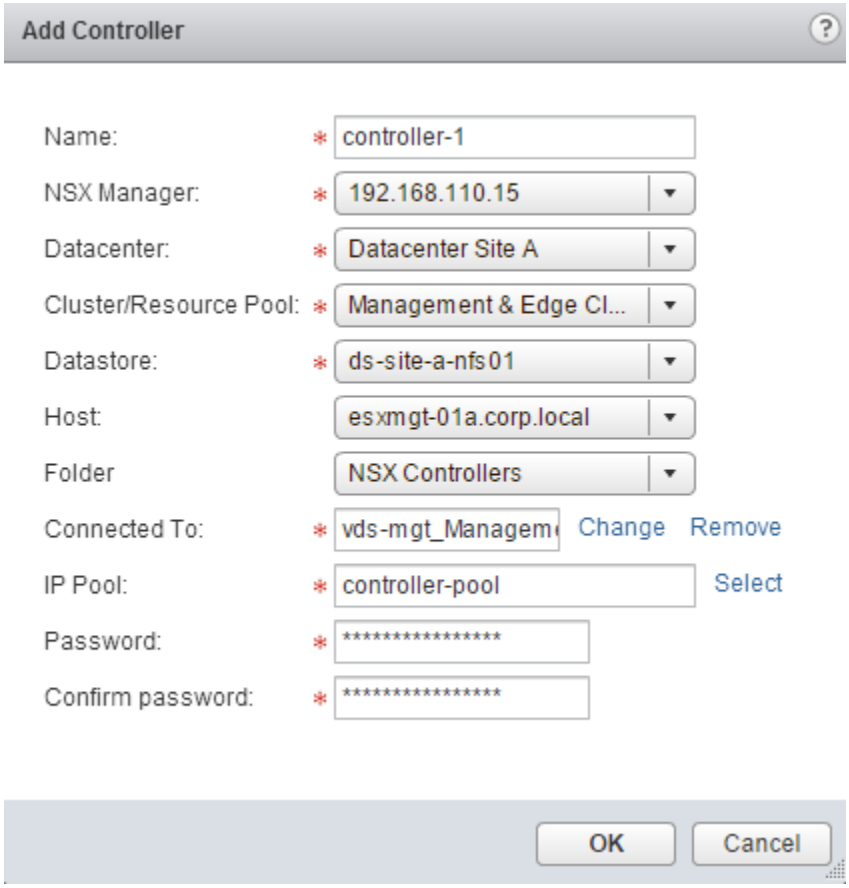


3 Dans la section Nœuds de NSX Controller, cliquez sur l'icône **Ajouter un nœud (Add Node)** ( ).

4 Entrez les paramètres de NSX Controller convenant à votre environnement.

Des instances de NSX Controller doivent être déployées sur un groupe de ports vSphere Standard Switch ou vSphere Distributed Switch qui ne repose pas sur VXLAN et qui dispose d'une connectivité avec NSX Manager, d'autres contrôleurs et des hôtes via IPv4.

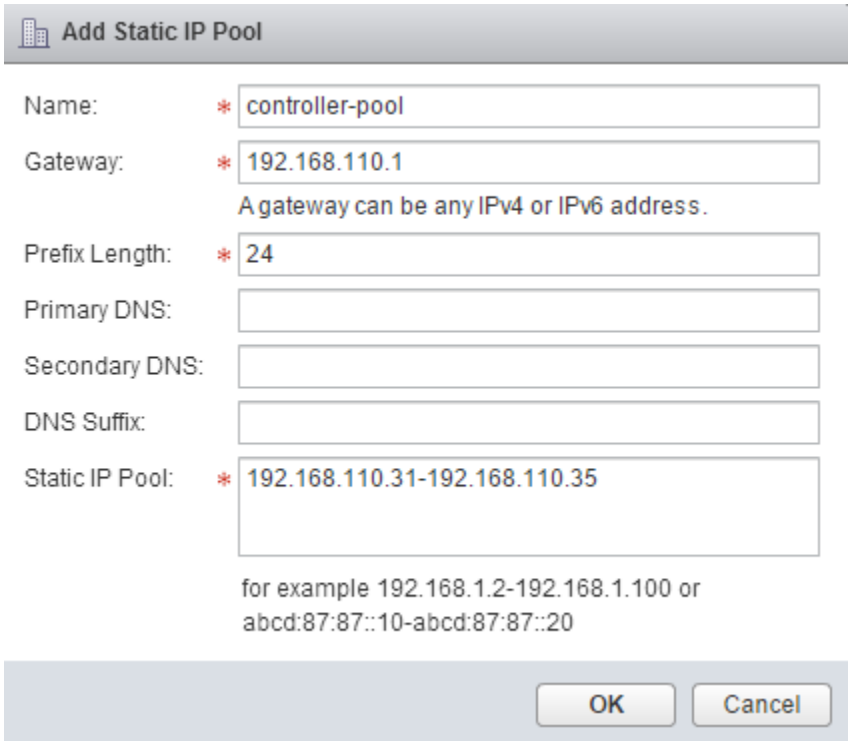
Par exemple :



5 Si vous n'avez pas encore configuré de pool IP pour votre cluster de contrôleurs, configurez-en un maintenant en cliquant sur **Nouveau pool IP (New IP Pool)**.

Des contrôleurs individuels peuvent se trouver dans des sous-réseaux IP distincts, si nécessaire.

Par exemple :



6 Tapez le mot de passe du contrôleur, puis retapez-le pour confirmer.

Note Le mot passe ne doit pas contenir le nom d'utilisateur comme sous-chaîne. Aucun caractère ne doit pas utilisé plus de 2 fois de manière consécutive.

Le mot de passe doit se composer d'au moins 12 caractères et doit respecter trois des quatre règles suivantes :

- Au moins une lettre en majuscule
- Au moins une lettre en minuscule
- Au moins un chiffre
- Au moins un caractère spécial

7 Après le déploiement complet du premier contrôleur, déployez deux autres contrôleurs.

Il est obligatoire de disposer de trois contrôleurs. Il est recommandé de configurer une règle d'anti-affinité du DRS pour éviter que les contrôleurs résident sur le même hôte.

Résultats

Une fois déployés, les contrôleurs présentent l'état **Connecté (Connected)** et affichent une coche verte.

Si le déploiement ne s'est pas correctement effectué, reportez-vous à la section Déploiement d'instances de NSX Controller du *Guide de dépannage de NSX*.

Sur les hôtes où les nœuds NSX Controller sont déployés en premier lieu, NSX permet le démarrage et l'arrêt automatique de machine virtuelle. Si les machines virtuelles du nœud de contrôleur sont migrées ultérieurement vers d'autres hôtes, il se peut que le démarrage et l'arrêt automatique de machine virtuelle ne soit pas activé sur les nouveaux hôtes. Pour cette raison, VMware vous recommande de vérifier tous les hôtes du cluster afin de vous assurer que le démarrage et l'arrêt de machine virtuelle soit activé. Reportez-vous à la section http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-5FE08AC7-4486-438E-AF88-80D6C7928810.html.

Exemple

Exclusion de machines virtuelles de la protection assurée par le pare-feu

9

Vous pouvez exclure un ensemble de machines virtuelles de la protection du pare-feu distribué NSX.

NSX Manager, les instances NSX Controller et les machines virtuelles NSX Edge sont automatiquement exclus de la protection assurée par le pare-feu distribué NSX. En outre, VMware vous recommande de placer les machines virtuelles de service suivantes dans la liste d'exclusion pour permettre au trafic de circuler sans entrave.

- vCenter Server. Il peut être déplacé vers un cluster protégé par pare-feu, mais il doit déjà exister dans la liste d'exclusion pour éviter tout problème de connectivité.

  Note Il est important d'ajouter vCenter Server à la liste d'exclusion avant de passer la règle par défaut « any any » de Autoriser à Bloquer. Le non-respect de cette instruction entraîne le blocage de l'accès à vCenter Server après la création d'une règle Refuser tout (ou après la modification de la règle par défaut sur l'action bloquer). Si cela se produit, restaurez DFW sur la règle de pare-feu par défaut définie en exécutant la commande d'API suivante : `https://NSX_Manager_IP/api/4.0/firewall/globalroot-0/config`. La demande doit renvoyer l'état 204. Cela restaure la stratégie par défaut (avec la règle par défaut Autoriser) pour DFW et réactive l'accès à vCenter Server et vSphere Web Client.

- Machines virtuelles de service partenaires.
- Machines virtuelles nécessitant un mode Promiscuité. Si ces machines virtuelles sont protégées par le pare-feu distribué NSX, leurs performances risquent d'en souffrir.
- Le serveur SQL utilisé par votre vCenter basé sur Windows.
- Serveur Web vCenter si vous l'exécutez séparément.

Procédure

1. Dans vSphere Web Client, cliquez sur **Mise en réseau et sécurité (Networking & Security)**.
2. Dans **Inventaire de mise en réseau et de sécurité (Networking & Security Inventory)**, cliquez sur **NSX Manager (NSX Managers)**.
3. Dans la colonne **Nom (Name)**, cliquez sur un dispositif NSX Manager.
4. Cliquez sur l'onglet **Gérer (Manage)**, puis sur l'onglet **Liste d'exclusion (Exclusion List)**.

5 Cliquez sur l'icône **Ajouter (Add)** ( ).

6 Sélectionnez les machines virtuelles à exclure et cliquez sur **Ajouter (Add)**.

7 Cliquez sur **OK**.

Résultats

Si une machine virtuelle dispose de plusieurs cartes réseau virtuelles (vNIC), toutes ces cartes virtuelles sont exclues de la protection. Si vous ajoutez des cartes réseau virtuelles (vNIC) à une machine virtuelle après son ajout à la liste d'exclusion, le pare-feu est automatiquement déployé sur les vNIC qui viennent d'être ajoutés. Pour exclure ces cartes réseau virtuelles (vNIC) de la protection assurée par le pare-feu, vous devez supprimer la machine virtuelle de la liste d'exclusion avant de l'ajouter à nouveau à cette liste. Une autre méthode consiste à appliquer un cycle d'alimentation (mettre hors tension, puis à nouveau sous tension) à la machine virtuelle, mais la première option entraîne moins de perturbations.

Préparer des clusters d'hôtes pour NSX

10

La préparation d'hôtes est le processus par lequel l'instance de NSX Manager 1) installe des modules du noyau NSX sur des hôtes ESXi membres de clusters vCenter et 2) construit le plan de contrôle NSX et la structure du plan de gestion. Les modules du noyau NSX for vSphere conditionnés dans des fichiers VIB s'exécutent dans le noyau de l'hyperviseur et fournissent des services tels que le routage distribué, le pare-feu distribué et les possibilités de pontage VXLAN.

Pour préparer votre environnement pour la virtualisation réseau, vous devez installer les composants de l'infrastructure réseau au niveau du cluster pour chaque vCenter Server sur lequel ils sont nécessaires. Cette opération déploie les logiciels requis sur tous les hôtes du cluster. Lorsqu'un hôte est ajouté au cluster, les logiciels requis sont automatiquement installés sur cet hôte.

Si vous utilisez ESXi en mode sans état (ce qui signifie qu'ESXi ne maintient pas son état entre redémarrages), vous devez télécharger manuellement les VIB de NSX et les inclure dans l'image de l'hôte. Vous trouverez les chemins de téléchargement des VIB de NSX sur la page : https://<NSX_MANAGER_IP>/bin/vdn/nwfabric.properties. Sachez que les chemins de téléchargement peuvent être modifiés pour chaque version de NSX. Consultez toujours la page https://<NSX_MANAGER_IP>/bin/vdn/nwfabric.properties pour obtenir les VIB appropriés. Pour plus d'informations, consultez Déploiement de VXLAN via Auto Deploy https://kb.vmware.com/kb/2041972.

Conditions préalables

- Enregistrez vCenter Server dans NSX Manager et déployez des contrôleurs NSX.
- Vérifiez que la recherche DNS inversée renvoie un nom de domaine complet lorsque vous l'interrogez sur l'adresse IP de NSX Manager. Par exemple :

```
C:\Users\Administrator>nslookup 192.168.110.42
Server:  localhost
Address:  127.0.0.1

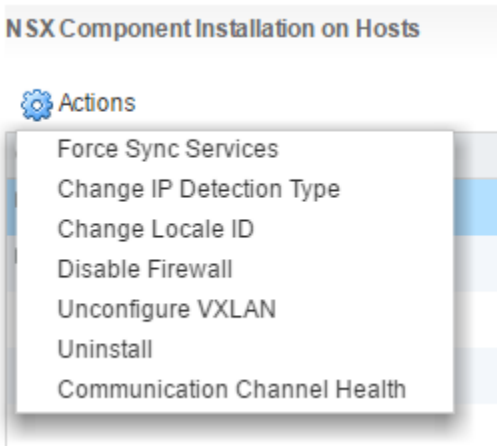
Name:    nsxmgr-l-01a.corp.local
Address:  192.168.110.42
```

- Vérifiez que les hôtes peuvent résoudre le nom DNS de vCenter Server.

- Vérifiez que les hôtes peuvent se connecter à vCenter Server sur le port 80.
- Vérifiez que l'heure du réseau sur vCenter Server et celle des hôtes ESXi sont synchronisées.
- Pour chaque cluster d'hôtes qui participera à NSX, vérifiez que les hôtes du cluster sont attachés à un commutateur vSphere Distributed Switch commun.

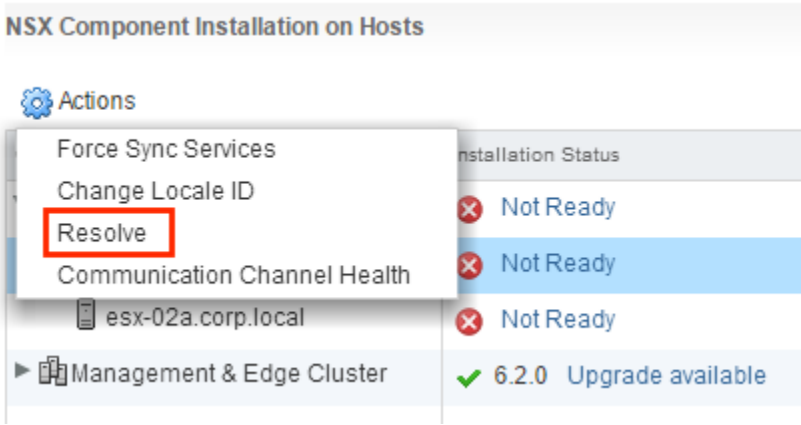
  Par exemple, supposons que vous disposiez d'un cluster incluant Hôte1 et Hôte2. Hôte1 est attaché à VDS1 et à VDS2. Hôte2 est attaché à VDS1 et à VDS3. Lorsque vous préparez un cluster pour NSX, vous pouvez uniquement associer NSX à VDS1 sur le cluster. Si vous ajoutez un autre hôte (Hôte3) au cluster et si Hôte3 n'est pas attaché à VDS1, cette configuration n'est pas valide et Hôte3 ne sera pas prêt pour la fonctionnalité NSX.
- Si votre environnement dispose de vSphere Update Manager (VUM), vous devez le désactiver avant de préparer des clusters pour la virtualisation réseau. Pour plus d'informations sur la vérification de l'activation de VUM et pour découvrir comment le désactiver si nécessaire, reportez-vous à http://kb.vmware.com/kb/2053782.
- Avant de commencer le processus de préparation d'hôtes NSX, assurez-vous toujours que le cluster se trouve dans l'état résolu, ce qui signifie que l'option **Résoudre (Resolve)** ne s'affiche pas dans la liste **Actions** du cluster.

  Par exemple :



  L'option **Résoudre (Resolve)** s'affiche parfois, car un ou plusieurs hôtes du cluster doivent être redémarrés.

  À d'autres occasions, l'option **Résoudre (Resolve)** s'affiche en présence d'une condition d'erreur à résoudre. Cliquez sur le lien **Non prêt (Not Ready)** pour voir l'erreur. Si vous le pouvez, effacez la condition d'erreur. Si vous ne pouvez pas effacer une condition d'erreur sur un cluster, une solution consiste à déplacer les hôtes vers un nouveau ou un autre cluster et à supprimer l'ancien cluster.



Si l'option **Résoudre (Resolve)** ne résout pas le problème, consultez le *Guide de dépannage de NSX*. Pour afficher la liste des problèmes résolus par l'option **Résoudre (Resolve)**, consultez *Journalisation et événements système dans NSX*.

Procédure

1 Connectez-vous à vSphere Web Client.

2 Accédez à **Accueil > Networking & Security > Installation (Home > Networking & Security > Installation)**, puis sélectionnez l'onglet **Préparation de l'hôte (Host Preparation)**.

3 Pour tous les clusters qui nécessitent une commutation logique NSX, un routage et des pare-feu, cliquez sur l'icône **Actions, (Actions) (** **)** puis sur **Installer (Install)**.

Un cluster de calcul (également appelé cluster de charge utile) est un cluster qui possède des VM d'application (Web, base de données, etc.). S'il est prévu qu'un cluster de calcul dispose d'une commutation NSX, d'un routage ou d'un pare-feu, cliquez sur **Installer (Install)** de ce cluster.

Dans un cluster « Gestion et Edge » partagé (comme illustré dans l'exemple), NSX Manager et les machines virtuelles de contrôleurs partagent un cluster avec des périphériques Edge, par exemple des routeurs logiques distribués (DLR) et des dispositifs Edge Services Gateway (ESG). Dans ce cas, il est important de cliquer sur **Installer (Install)** pour le cluster partagé.

Inversement, si Gestion et Edge disposent chacun d'un cluster dédié, non partagé (comme cela est recommandé dans un environnement de production), cliquez sur **Installer (Install)** pour le cluster Edge, mais pas pour le cluster Gestion.

Note En cours d'installation, vous ne devez ni déployer, ni mettre à niveau, ni désinstaller un service ou un composant.

4 Surveillez l'installation jusqu'à ce que la colonne **Statut de l'installation (Installation Status)** affiche une coche verte.

   Si la colonne **Statut de l'installation (Installation Status)** affiche une icône d'avertissement rouge et indique **Non prêt (Not Ready)**, cliquez sur **Résoudre (Resolve)**. Le fait de cliquer sur **Résoudre (Resolve)** peut entraîner le redémarrage de l'hôte. Si l'installation se termine encore avec des erreurs, cliquez sur l'icône d'avertissement. Toutes les erreurs sont affichées. Prenez les mesures nécessaires et cliquez de nouveau sur **Résoudre (Resolve)**.

   Une fois l'installation terminée, la colonne **État de l'installation (Installation Status)** affiche la version et la build de l'instance de NSX installée et la colonne **Pare-feu (Firewall)** indique **Activé (Enabled)**. Les deux colonnes comportent une coche verte. Si l'option Résoudre s'affiche dans la colonne **Statut de l'installation (Installation Status)**, cliquez dessus et actualisez la fenêtre de votre navigateur.

Résultats

Les VIB sont installés et enregistrés sur tous les hôtes dans le cluster préparé. Les VIB installés varient selon les versions de NSX et ESXi qui sont installées.

Version d'ESXi	Version de NSX	VIB installés
5.5	N'importe quelle version 6.3.x	■ esx-vsip ■ esx-vxlan
6.0 ou une version ultérieure	6.3.2 ou une version antérieure	■ esx-vsip ■ esx-vxlan
6.0 ou une version ultérieure	6.3.3 ou une version ultérieure	■ esx-nsxv

Pour vérifier, établissez une connexion SSH à chaque hôte et exécutez la commande `esxcli software vib list`, puis recherchez les VIB correspondants. Outre l'affichage des VIB, cette commande affiche la version des VIB installés.

```
[root@host:~] esxcli software vib list | grep esx
esx-XXXX      6.0.0-0.0.XXXXXXX    VMware  VMwareCertified   2016-12-29
```

Si vous ajoutez un hôte à un cluster préparé, les VIB NSX sont automatiquement installés sur l'hôte.

Si vous déplacez un hôte vers un cluster non préparé, les VIB NSX sont automatiquement désinstallés de cet hôte.

Ajouter un hôte à un cluster préparé

11

Cette section décrit comment ajouter un hôte à un cluster préparé pour la virtualisation réseau.

Procédure

1. Ajoutez l'hôte à vCenter Server comme hôte autonome.

   Consultez la *Documentation ESXi et vCenter Server*.

2. Ajoutez l'hôte à l'instance de vSphere Distributed Switch mappée au cluster dans lequel vous souhaitez l'ajouter.

   Tous les hôtes du cluster doivent se trouver dans l'instance de vSphere Distributed Switch exploitée par NSX.

3. Cliquez avec le bouton droit sur l'hôte cible et sélectionnez **Mode de maintenance (Maintenance Mode)** > **Entrer en mode de maintenance (Enter Maintenance Mode)**.

4. Faites glisser et déposez l'hôte cible dans le cluster NSX activé existant.

   Comme il s'agit d'un cluster préparé, le logiciel requis est automatiquement installé sur l'hôte récemment ajouté.

5. Cliquez avec le bouton droit sur l'hôte et sélectionnez **Mode de maintenance (Maintenance Mode)** > **Quitter le mode de maintenance (Exit Maintenance Mode)**.

   DRS équilibre les machines virtuelles sur l'hôte.

Retirer un hôte d'un cluster NSX préparé

12

Cette section décrit comment retirer un hôte d'un cluster préparé pour la virtualisation réseau. Par exemple, cette intervention est nécessaire si vous décidez que l'hôte ne doit pas participer à NSX.

Important Si NSX 6.3.0 ou version ultérieure et ESXi 6.0 ou version ultérieure sont installés sur l'hôte, vous ne devez pas redémarrer ce dernier pour désinstaller des VIB. Si des versions antérieures de NSX et d'ESXi sont installées, vous devez redémarrer l'hôte pour finaliser la désinstallation des VIB.

Procédure

1. Placez l'hôte en mode de maintenance et attendez que DRS évacue l'hôte, ou retirez-le de l'hôte manuellement avec vMotion des machines virtuelles en cours d'exécution.
2. Retirez l'hôte du cluster préparé en le déplaçant vers un cluster non préparé ou en le transformant en un hôte autonome à l'extérieur de tout cluster.

   NSX désinstalle les composants de la virtualisation de réseau et les machines virtuelles de service de l'hôte.
3. Si NSX 6.2.x ou version antérieure ou ESXi 5.5 est installé sur l'hôte, redémarrez ce dernier.
4. Vérifiez que la désinstallation des VIB est terminée.
   a. Consultez le volet Tâches récentes de vSphere Web Client.
   b. Sous l'onglet **Préparation de l'hôte (Host Preparation)**, vérifiez la présence d'une coche verte en regard du Statut de l'installation du cluster dont l'hôte a été supprimé.

      Si le Statut de l'installation est `Installation en cours`, la désinstallation n'est pas terminée.
5. À la fin de la désinstallation, faites quitter l'hôte du mode de maintenance.

Résultats

Les VIB NSX sont retirés de l'hôte. Pour vérifier, établissez une connexion SSH à l'hôte et exécutez la commande `esxcli software vib list | grep esx`. Assurez-vous que les VIB suivants ne sont pas présents sur l'hôte :

- esx-vsip
- esx-vxlan

Si les VIB sont toujours présents sur l'hôte, vous pouvez consulter les journaux pour déterminer pourquoi le retrait automatique des VIB n'a pas fonctionné.

Vous pouvez retirer les VIB manuellement en exécutant les commandes suivantes :

- `esxcli software vib remove --vibname=esx-vxlan`
- `esxcli software vib remove --vibname=esx-vsip`

Configurer les paramètres de transport VXLAN

13

Le réseau VXLAN est utilisé pour la commutation logique de couche 2 entre hôtes, couvrant potentiellement plusieurs domaines de couche 3 sous-jacents. Vous configurez VXLAN par cluster, c'est-à-dire que vous mappez chaque cluster devant participer à NSX à un vSphere Distributed Switch (VDS). Lorsque vous mappez un cluster à un commutateur distribué, chaque hôte de ce cluster est activé pour les commutateurs logiques. Les paramètres choisis ici seront utilisés lors de la création de l'interface VMkernel.

Si vous avez besoin d'un routage et d'une commutation logiques, des paramètres de transport VXLAN doivent être configurés sur tous les clusters dans lesquels des NSX VIB sont installés sur les hôtes. Si vous prévoyez de déployer uniquement un pare-feu distribué, vous n'avez pas besoin de configurer les paramètres du transport VXLAN..

Lorsque vous configurez la mise en réseau VXLAN, vous devez fournir un commutateur vSphere Distributed Switch, un ID de VLAN, une taille de MTU, un mécanisme d'adressage IP (DHCP ou pool d'adresses IP) et une stratégie d'association de cartes réseau.

Le MTU de chaque commutateur doit être défini sur 1 550 ou une valeur supérieure. Par défaut, il est défini sur 1 600. Si la taille de MTU du commutateur vSphere Distributed Switch est supérieure à celle du MTU de VXLAN, le MTU du commutateur vSphere Distributed Switch n'est pas ajusté à une valeur inférieure. S'il est défini sur une valeur inférieure, Il sera ajusté pour correspondre au MTU de VXLAN. Par exemple, si le MTU du commutateur vSphere Distributed Switch est défini sur 2 000 et que vous acceptez la valeur par défaut (1 600) du MTU de VXLAN, aucune modification n'est apportée au MTU du commutateur vSphere Distributed Switch. Si le MTU du commutateur vSphere Distributed Switch est de 1 500 et que le MTU de VXLAN est de 1 600, le MTU du commutateur vSphere Distributed Switch est modifié pour prendre la valeur 1 600.

Les VTEP sont associés à un ID de VLAN. Cependant, vous pouvez spécifier ID de VLAN = 0 pour les VTEP, ce qui signifie que les trames ne seront pas balisées.

Vous pouvez utiliser des paramètres d'adresse IP différents pour vos clusters de gestion et vos clusters de calcul. Cela dépend de la conception du réseau physique et ce ne sera probablement pas le cas dans les petits déploiements.

Conditions préalables

- Tous les hôtes du cluster doivent être attachés à un commutateur vSphere Distributed Switch commun.

- NSX Manager doit être installé.
- Les contrôleurs NSX doivent être installés, sauf si vous utilisez le mode de réplication multidiffusion pour le plan de contrôle.
- Planifiez votre stratégie d'association NIC. La stratégie d'association de cartes réseau détermine les paramètres d'équilibrage de charge et de basculement du commutateur vSphere Distributed Switch.

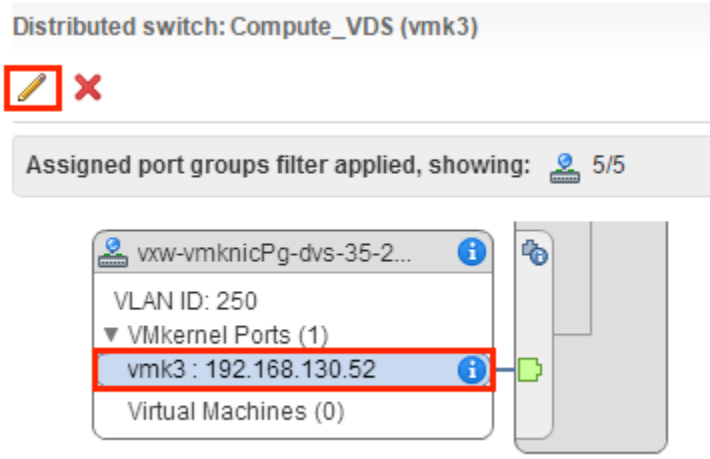
  N'utilisez pas différentes stratégies d'association pour différents groupes de ports d'un commutateur vSphere Distributed Switch où certains d'entre eux utilisent EtherChannel, LACPv1 ou LACPv2 et d'autres utilisent une autre stratégie d'association. Si des liaisons montantes sont partagées dans ces différentes stratégies d'association, le trafic sera interrompu. Des problèmes de routage peuvent survenir si des routeurs logiques sont présents. Ce type de configuration n'est pas pris en charge et doit être évité.

  Pour l'association basée sur le hachage IP (EtherChannel, LACPv1 ou LACPv2), il est recommandé d'utiliser toutes les liaisons montantes du commutateur vSphere Distributed Switch de l'équipe et que les groupes de ports de ce commutaeur utilisent les mêmes stratégies d'association. Pour plus d'informations et une aide supplémentaire, reportez-vous au *Guide de conception de virtualisation réseau de VMware® NSX for vSphere* à l'adresse https://communities.vmware.com/docs/DOC-27683.
- Planifiez le schéma d'adressage IP des points de terminaison du tunnel VXLAN (VTEP). Les VTEP sont les adresses source et destination utilisées dans l'en-tête IP externe pour identifier de façon unique les hôtes ESX à l'origine et à la conclusion de l'encapsulation VXLAN des trames. Vous pouvez utiliser DHCP ou configurer manuellement des pools IP pour les adresses IP VTEP.

  Si vous souhaitez attribuer une adresse IP spécifique à un VTEP, vous pouvez 1) utiliser une adresse fixe DHCP ou une réservation qui mappe une adresse MAC à une adresse IP spécifique sur le serveur DHCP ou 2) utiliser un pool d'adresses IP et modifier manuellement l'adresse IP VTEP attribuée à la vmknic dans **Hôtes et clusters (Hosts and Clusters) > *hôte* (*host*) > Gérer (Manage) > Mise en réseau (Networking) > Commutateurs virtuels (Virtual Switches)**.

  Note Si vous modifiez manuellement l'adresse IP, assurez-vous qu'elle n'est pas similaire à la plage de pool d'adresses IP d'origine.

  Par exemple :



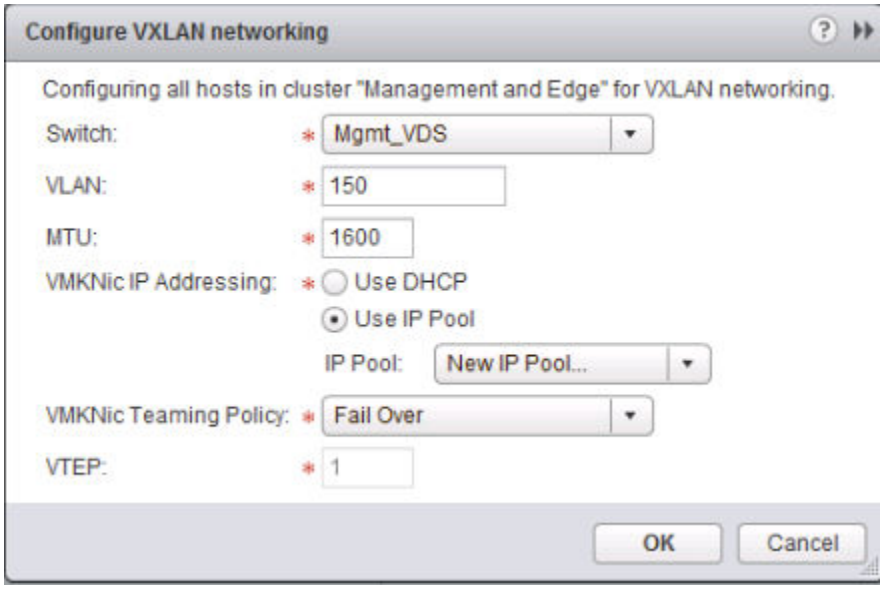
- Pour les clusters membres du même VDS, l'ID de VLAN des VTEP et de l'association de NIC doivent être identiques.
- Il est recommandé d'exporter la configuration de vSphere Distributed Switch avant de préparer le cluster pour le protocole VXLAN. Reportez-vous à la section http://kb.vmware.com/kb/2034602.

Procédure

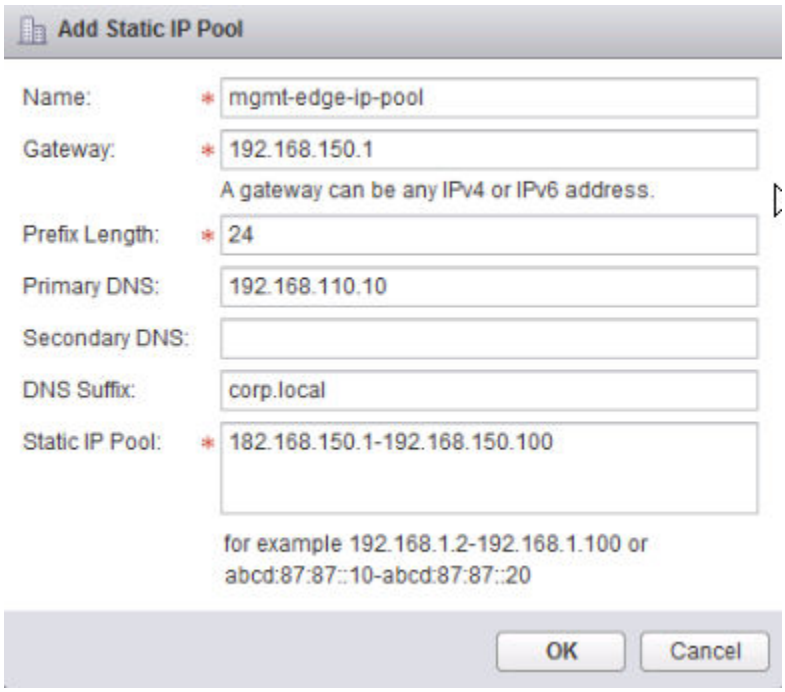
1. Connectez-vous à vSphere Web Client.
2. Accédez à **Accueil > Networking & Security > Installation (Home > Networking & Security > Installation)**, puis sélectionnez l'onglet **Préparation de l'hôte (Host Preparation)**.
3. Cliquez sur **Non configuré (Not Configured)** dans la colonne **VXLAN**.
4. Configurez la mise en réseau logique.

   Cela implique la sélection d'un commutateur vSphere Distributed Switch, d'un ID de VLAN, d'une taille de MTU, d'un mécanisme d'adressage IP et d'une stratégie d'association de cartes réseau.

   Ces exemples d'écrans montrent une configuration d'un cluster de gestion disposant de la plage d'adresses de pool IP 182.168.150.1-192.168.150.100, sauvegardée par VLAN 150 et avec une stratégie d'association NIC de basculement.



Le nombre de VTEP n'est pas modifiable dans l'interface utilisateur. Le nombre de VTEP est défini pour correspondre au nombre de dvUplinks sur le vSphere Distributed Switch en cours de préparation.

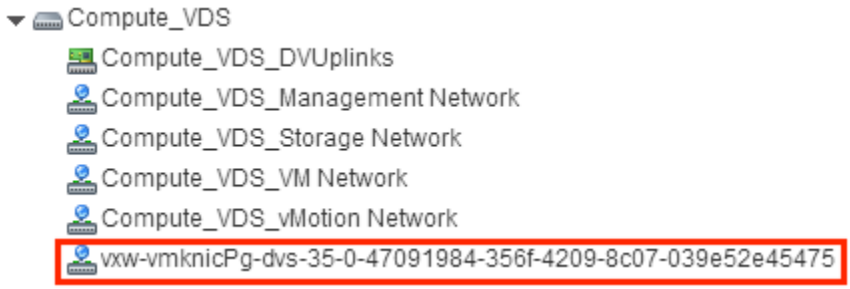


Pour les clusters de calcul, vous pouvez utiliser d'autres paramètres d'adresse IP, tels que 192.168.250.0/24 avec un VLAN de 250. Cela dépend de la conception du réseau physique et ce ne sera probablement pas le cas dans les petits déploiements.

Résultats

La configuration d'un VXLAN entraîne la création d'un nouveau groupe de ports distribués dans le commutateur vSphere Distributed Switch spécifié.

Par exemple :



Pour plus d'informations sur le dépannage de VXLAN, consultez le *Guide de dépannage de NSX*.

Attribuer un pool d'ID de segments et une plage d'adresses de multidiffusion

14

Les segments VXLAN sont construits entre des points de terminaison de tunnel VXLAN (VTEP). Un hôte d'hyperviseur est un exemple standard de VTEP. Chaque tunnel VXLAN possède un ID de segment. Vous devez spécifier un pool d'ID de segments pour chaque NSX Manager afin d'isoler le trafic de votre réseau. Si un contrôleur NSX n'est pas déployé dans votre environnement, vous devez également ajouter une plage d'adresses de multidiffusion pour répartir le trafic dans votre réseau sans surcharger une adresse de multidiffusion spécifique.

Lors de la détermination de la taille de chaque pool d'ID de segments, gardez à l'esprit que la plage d'ID de segments contrôle le nombre de commutateurs logiques pouvant être créés. Choisissez un sous-ensemble réduit des 16 millions d'identifiants VNI potentiels. Vous ne devez pas configurer plus de 10 000 VNI dans un vCenter, car vCenter limite le nombre de dvPortgroups à 10 000.

Si VXLAN est en place dans un autre déploiement NSX, déterminez quels VNI sont déjà en cours d'utilisation et évitez le chevauchement de VNI. Les VNI sans chevauchement sont automatiquement placés dans une seule et même instance de NSX Manager et dans l'environnement vCenter. Les plages VNI locales ne peuvent pas se chevaucher. Il est toutefois important de vous assurer que les VNI ne se chevauchent pas dans vos déploiements NSX distincts. Les VNI sans chevauchement sont pratiques pour le suivi et contribuent à garantir que vos déploiements sont prêts pour un environnement cross-vCenter.

Si l'une de vos zones de transport utilise le mode de réplication multidiffusion ou hybride, vous devez ajouter une adresse multidiffusion ou une plage d'adresses multidiffusion.

L'utilisation d'une plage d'adresses de multidiffusion répartit le trafic à l'échelle de votre réseau, empêche la surcharge d'une adresse de multidiffusion spécifique et optimise la réplication BUM.

N'utilisez ni 239.0.0.0/24 ni 239.128.0.0/24 comme plage d'adresses de multidiffusion, car ces réseaux sont utilisés pour le contrôle de sous-réseau locaux, ce qui signifie que les commutateurs physiques envoient tout le trafic qui utilise ces adresses. Pour plus d'informations sur les adresses de multidiffusion non utilisables, reportez-vous à https://tools.ietf.org/html/draft-ietf-mboned-ipv4-mcast-unusable-01.

Lorsque les modes de multidiffusion VXLAN et de réplication hybride sont configurés et fonctionnent correctement, une copie du trafic multidiffusion est livrée uniquement aux hôtes ayant envoyé des messages de jonction IGMP. Sinon, le réseau physique envoie tout le trafic multidiffusion à tous les hôtes au sein du même domaine de diffusion. Pour éviter une telle saturation, vous devez prendre les mesures suivantes :

- Assurez-vous que le commutateur physique sous-jacent est configuré avec un MTU supérieur ou égal à 1 600.
- Assurez-vous que le commutateur physique sous-jacent est correctement configuré avec l'écoute IGMP et un interrogateur IGMP dans les segments réseau qui transportent du trafic VTEP.
- Assurez-vous que la zone de transport est configurée avec la plage d'adresses de multidiffusion recommandée. La plage d'adresses de multidiffusion recommandée commence à 239.0.1.0/24 et exclut 239.128.0.0/24.

L'interface de vSphere Web Client vous permet de configurer une seule plage d'ID de segments et une seule adresse multidiffusion ou plage d'adresses multidiffusion. Pour configurer plusieurs plages d'ID de segments ou plusieurs valeurs d'adresses multidiffusion, vous pouvez utiliser NSX API. Reportez-vous à *Guide de NSX API* pour plus de détails.

Procédure

1. Connectez-vous à vSphere Web Client.
2. Accédez à **Accueil > Networking & Security > Installation (Home > Networking & Security > Installation)**, puis sélectionnez l'onglet **Préparation du réseau logique (Logical Network Preparation)**.
3. Cliquez sur **ID de segment > Modifier (Segment ID > Edit)**.
4. Entrez une plage pour les ID de segments, par exemple `5000–5999`.
5. (Facultatif) Si l'une de vos zones de transport utilise le mode de réplication multidiffusion ou hybride, vous devez ajouter une adresse multidiffusion ou une plage d'adresses multidiffusion.
   a. Cochez la case **Activer l'adressage multidiffusion (Enable Multicast addressing)**.
   b. Entrez une adresse multidiffusion ou une plage d'adresses multidiffusion, par exemple `239.0.0.0–239.255.255.255`.

Résultats

Lorsque vous configurez des commutateurs logiques, chaque commutateur logique reçoit un ID de segment du pool.

Ajouter une zone de transport

15

Une zone de transport contrôle quels hôtes un commutateur logique peut atteindre. Elle peut couvrir un ou plusieurs clusters vSphere. Les zones de transport dictent quels clusters et, en conséquence, quelles machines virtuelles peuvent participer à l'utilisation d'un réseau donné.

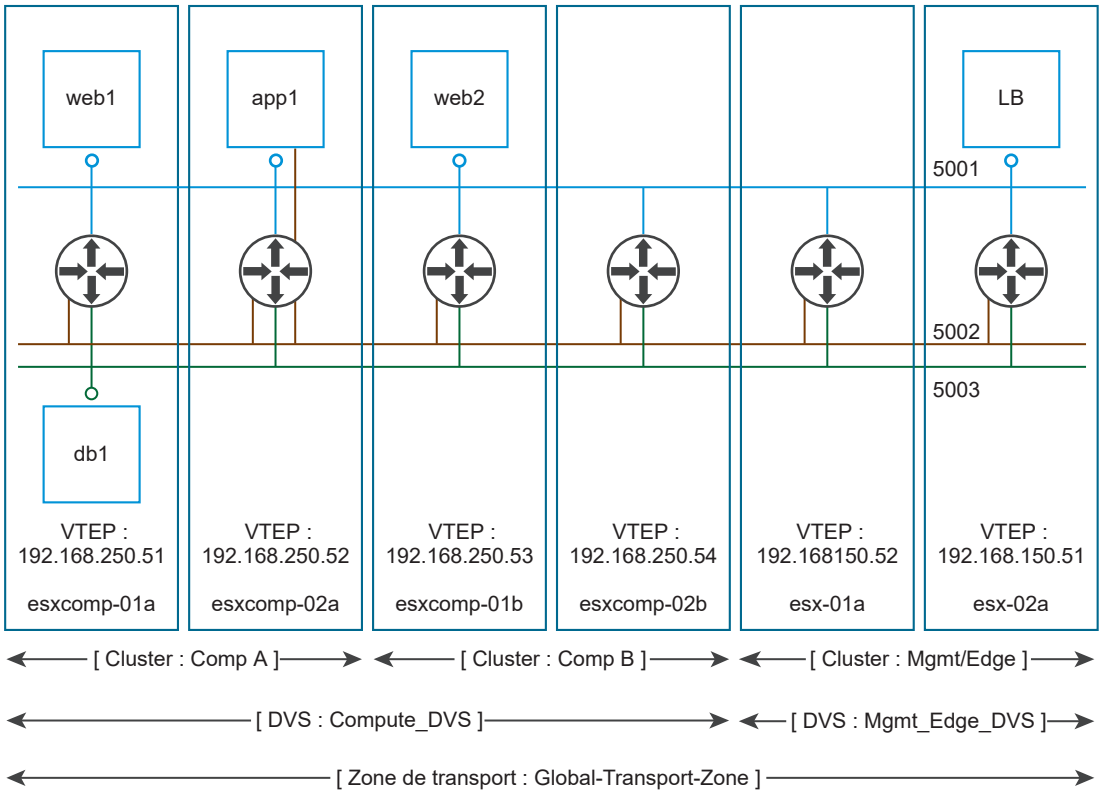
Un environnement NSX peut comporter une ou plusieurs zones de transport en fonction de vos conditions requises. Un cluster d'hôtes peut faire partie de plusieurs zones de transport. Un commutateur logique ne peut faire partie que d'une zone de transport.

NSX n'autorise pas la connexion de machines virtuelles se trouvant dans des zones de transport distinctes. L'étendue d'un commutateur logique est limitée à une zone de transport, de sorte que des machines virtuelles situées dans des zones de transport distinctes ne puissent pas se trouver sur le même réseau de couche 2. Un routeur logique distribué ne peut pas se connecter à des commutateurs logiques se trouvant dans des zones de transport distinctes. Après avoir connecté le premier commutateur logique, la sélection d'autres commutateurs logiques est limitée aux commutateurs se trouvant dans la même zone de transport.

Les directives suivantes sont destinées à vous aider à concevoir vos zones de transport :

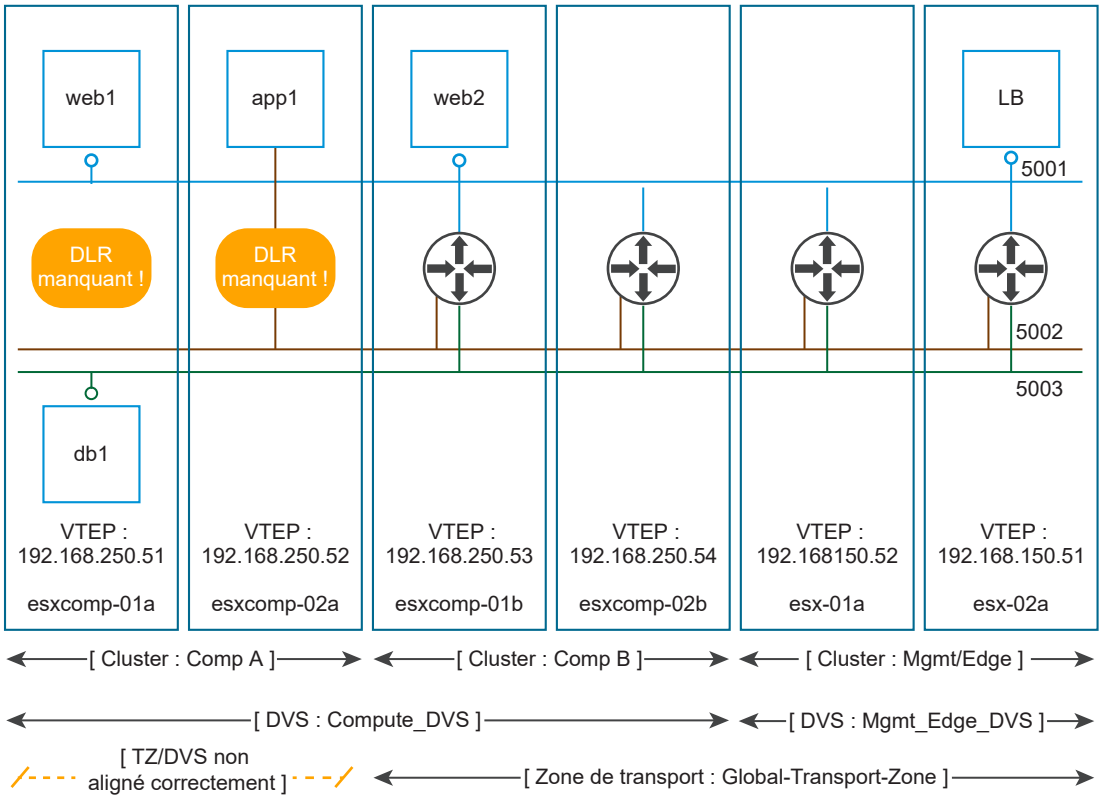
- Si un cluster nécessite une connectivité de couche 3, il doit se trouver dans une zone de transport contenant également un cluster Edge, c'est-à-dire un cluster contenant des périphériques Edge de couche 3 (des routeurs logiques distribués et des passerelles Edge Services Gateway).
- Supposons que vous ayez deux clusters, l'un pour des services Web et l'autre pour des services d'application. Pour avoir une connectivité VXLAN entre les machines virtuelles dans ces deux clusters, ceux-ci doivent être inclus dans la zone de transport.
- N'oubliez pas que tous les commutateurs logiques inclus dans la zone de transport seront disponibles et visibles de toutes les machines virtuelles des clusters inclus dans la zone de transport. Si un cluster comprend des environnements sécurisés, vous pouvez ne pas vouloir le rendre disponible à toutes les machines virtuelles d'autres clusters. Au contraire, vous pouvez placer votre cluster sécurisé dans une zone de transport plus isolée.
- L'étendue de vSphere Distributed Switch (VDS ou DVS) doit correspondre à celle de la zone de transport. Lorsque vous créez des zones de transport dans des configurations VDS avec plusieurs clusters, vérifiez que tous les clusters du VDS sélectionné sont inclus dans la zone de transport. Cela permet de s'assurer que le DLR est disponible sur tous les clusters dans lesquels des dvPortgroups VDS sont disponibles.

Le diagramme suivant présente une zone de transport alignée correctement sur la limite du VDS.



Si vous ne suivez pas cette recommandation, n'oubliez pas que si un VDS s'étend au-delà d'un cluster d'hôtes et que la zone de transport inclut uniquement l'un de ces clusters (ou un sous-ensemble), tous les commutateurs logiques compris dans cette zone de transport peuvent accéder aux machines virtuelles situées dans tous les clusters reliés par le VDS. Autrement dit, la zone de transport ne sera pas en mesure de limiter l'étendue du commutateur logique à un sous-ensemble des clusters. Si ce commutateur logique est ensuite connecté à un DLR, vous devez vous assurer que les instances du routeur sont créées uniquement dans le cluster inclus dans la zone de transport pour éviter des problèmes de couche 3.

Par exemple, lorsqu'une zone de transport n'est pas alignée sur la limite du VDS, l'étendue des commutateurs logiques (5001, 5002 et 5003) et des instances du DLR auxquels ces commutateurs logiques sont connectés se retrouve disjointe, ce qui a pour conséquence d'interrompre l'accès des machines virtuelles du cluster Comp A aux interfaces logiques du DLR (LIF).



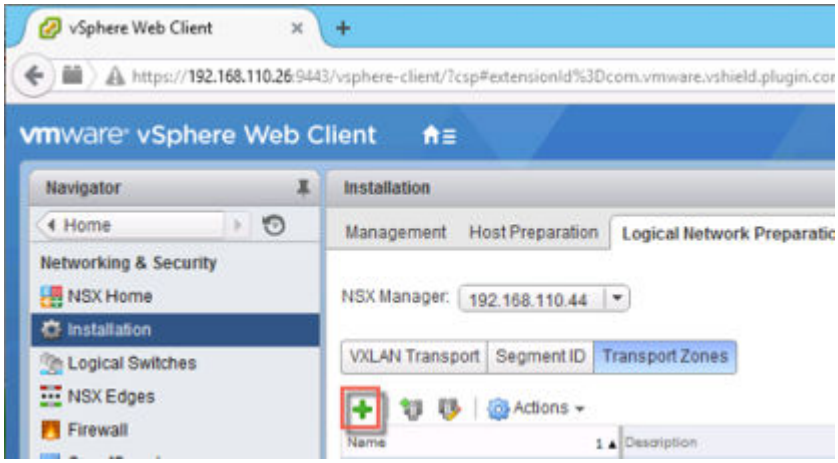
Procédure

1 Connectez-vous à vSphere Web Client.

2 Accédez à **Accueil > Networking & Security > Installation (Home > Networking & Security > Installation)**, puis sélectionnez l'onglet **Préparation du réseau logique (Logical Network Preparation)**.

3 Cliquez sur **Zones de transport (Transport Zones)**, puis sur l'icône **Nouvelle zone de transport (New Transport Zone) (+)**.

Par exemple :



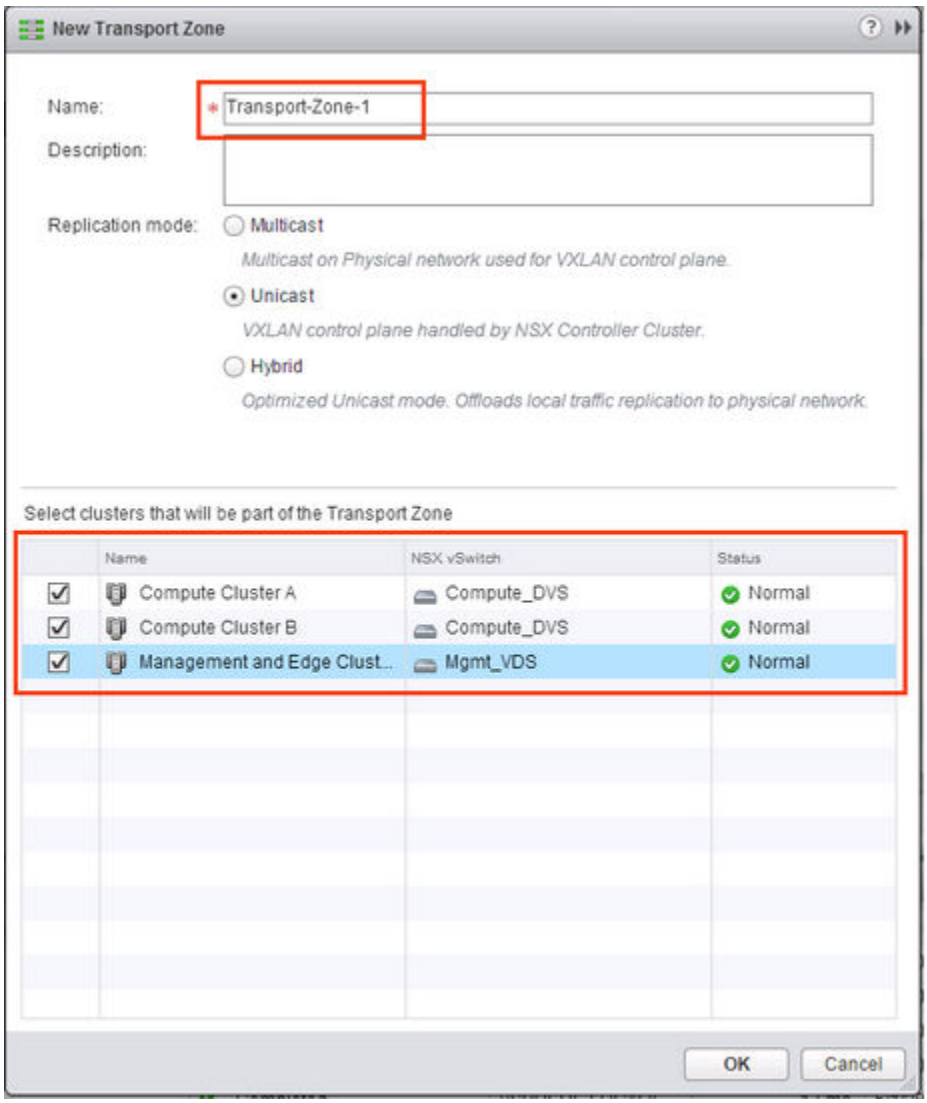
4 Dans la boîte de dialogue Nouvelle zone de transport, tapez un nom et une description (facultative) pour la zone de transport.

5 Selon que vous disposez d'un nœud de contrôleur dans votre environnement ou que vous souhaitez utiliser des adresses multidiffusion, sélectionnez le mode de plan de contrôle.

- **Multidiffusion (Multicast)** : la multidiffusion des adresses IP sur le réseau physique est utilisée pour le plan de contrôle. Ce mode est uniquement recommandé lors de la mise à niveau à partir d'anciens déploiements VXLAN. Nécessite PIM/IGMP sur le réseau physique.
- **Monodiffusion (Unicast)** : le plan de contrôle est géré par un NSX Controller. Tout le trafic de monodiffusion exploite la réplication de tête de réseau optimisée. Aucune adresse IP multidiffusion ni aucune configuration réseau spéciale n'est requise.
- **Hybride (Hybrid)** : décharge la réplication du trafic local vers un réseau physique (multidiffusion de niveau 2). Ce mode nécessite une surveillance IGMP sur le commutateur de premier saut et un accès à une requête IGMP dans chaque sous-réseau VTEP, mais n'a pas besoin de PIM. Le commutateur de premier saut gère la réplication du trafic du sous-réseau.

6 Sélectionnez les clusters à ajouter à la zone de transport.

Par exemple :



Étape suivante

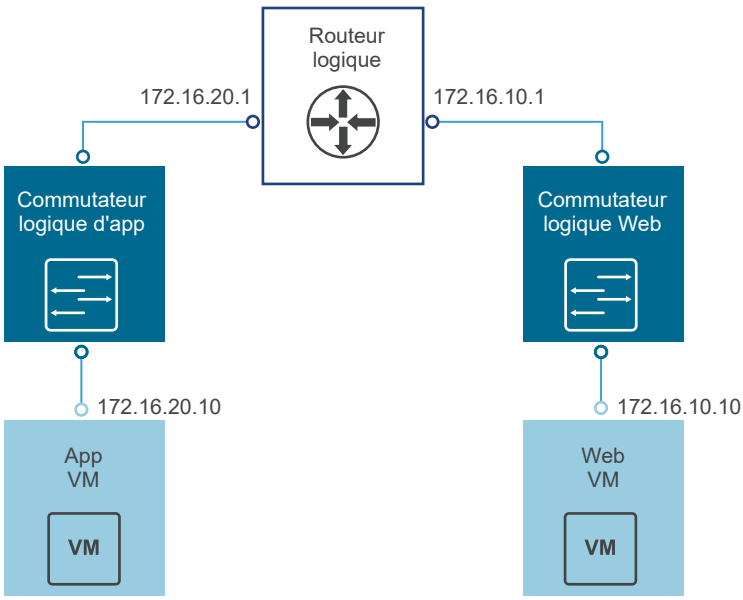
À présent que vous disposez d'une zone de transport, vous pouvez ajouter des commutateurs logiques.

Ajouter un commutateur logique

16

Un commutateur logique NSX for vSphere reproduit la fonctionnalité de commutation (monodiffusion, multidiffusion et diffusion) dans un environnement virtuel complètement dissocié du matériel sous-jacent. Les commutateurs logiques sont semblables aux VLAN en ce qu'ils fournissent des connexions réseau auxquelles vous pouvez associer des machines virtuelles. Les VM peuvent ainsi communiquer entre elles par le VLAN si elles sont connectées au même commutateur logique. Chaque commutateur logique possède un ID de segment, comme un ID de VLAN. Cependant, contrairement aux ID de VLAN, il est possible d'avoir jusqu'à 16 millions d'ID de segment.

Lorsque vous ajoutez des commutateurs logiques, il est important que vous réfléchissiez à la topologie particulière que vous créez. Par exemple, la simple topologie suivante présente deux commutateurs logiques connectés à un seul routeur logique distribué (DLR). Dans ce diagramme, chaque commutateur logique est connecté à une seule machine virtuelle. Les deux machines virtuelles peuvent être situées sur des hôtes distincts ou un seul et même hôte, dans différents clusters d'hôtes ou le même cluster d'hôtes. Si aucun DLR ne sépare les machines virtuelles, les adresses IP sous-jacentes configurées sur les machines virtuelles peuvent être sur le même sous-réseau. Si un DLR les sépare, les adresses IP sur les machines virtuelles doivent se trouver sur des sous-réseaux distincts (comme présenté dans l'exemple).



Lorsque vous créez un commutateur logique, en plus de sélectionner une zone de transport et un mode de réplication, vous configurez deux options : la découverte d'adresses IP et l'apprentissage MAC.

La découverte d'adresses IP permet de limiter la saturation du trafic ARP dans les segments VXLAN individuels, c'est-à-dire entre les machines virtuelles connectées au même commutateur logique. La découverte d'adresses IP est activée par défaut.

L'apprentissage MAC construit une table d'apprentissage VLAN/MAC sur chaque vNIC. Cette table est stockée avec les données dvfilter. Dans vMotion, dvfilter enregistre et restaure la table au nouvel emplacement. Puis, le commutateur génère des RARP pour toutes les entrées VLAN/MAC de la table. Vous voudrez peut-être activer l'apprentissage MAC si vous utilisez des cartes réseau virtuelles effectuant la jonction VLAN.

Conditions préalables

- vSphere Distributed Switches doivent être configurés.
- NSX Manager doit être installé.
- Les contrôleurs doivent être déployés.
- Les clusters d'hôtes doivent être préparés pour NSX.
- VXLAN doit être configuré.
- Un pool d'ID de segments doit être configuré.
- Une zone de transport doit être créée.

Procédure

1. Connectez-vous à vSphere Web Client.
2. Accédez à **Accueil > Mise en réseau et sécurité > Commutateurs logiques (Home > Networking & Security > Logical Switches)**.
3. Cliquez sur l'icône **Nouveau commutateur logique (New Logical Switch) (**  **)**.
4. Tapez un nom et une description (facultative) pour le commutateur logique.
5. Sélectionnez la zone de transport dans laquelle vous voulez créer le commutateur logique.

   Par défaut, le commutateur logique hérite du mode de réplication du plan de contrôle de la zone de transport.
6. (Facultatif) Remplacez le mode de réplication déterminé par la zone de transport.

   Vous pouvez changer cela et choisir l'un des autres modes disponibles. Les modes disponibles sont monodiffusion, hybride et multidiffusion.

   Pour remplacer le mode de réplication du plan de contrôle hérité de la zone de transport d'un commutateur logique individuel, il faut que le commutateur logique que vous créez ait des caractéristiques très différentes en termes de volume de trafic BUM à transporter. Dans ce cas, vous pouvez créer une zone de transport utilisant un mode de monodiffusion et utiliser un mode hybride ou de multidiffusion pour le commutateur logique individuel.

7 (Facultatif) Cliquez sur **Activer la découverte d'adresses IP (Enable IP Discovery)** pour activer la suppression d'ARP.

8 (Facultatif) Cliquez sur **Activer l'apprentissage MAC (Enable MAC learning)**

9 Attachez une machine virtuelle au commutateur logique en sélectionnant le commutateur et en cliquant sur l'icône **Ajouter une machine virtuelle (Add Virtual Machine) (**  **)**.

10 Sélectionnez une ou plusieurs machines virtuelles, puis cliquez sur le bouton représentant une flèche vers la droite **()(**  **)**.

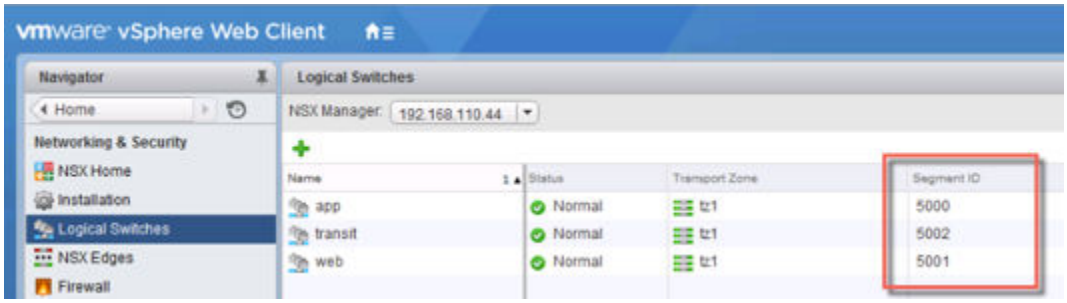
Les machines virtuelles passent de la liste des objets disponibles à la liste des objets sélectionnés.

11 Cliquez sur **Suivant (Next)**, puis sélectionnez une vNIC pour chaque machine virtuelle. Cliquez sur **Terminer (Finish)**.

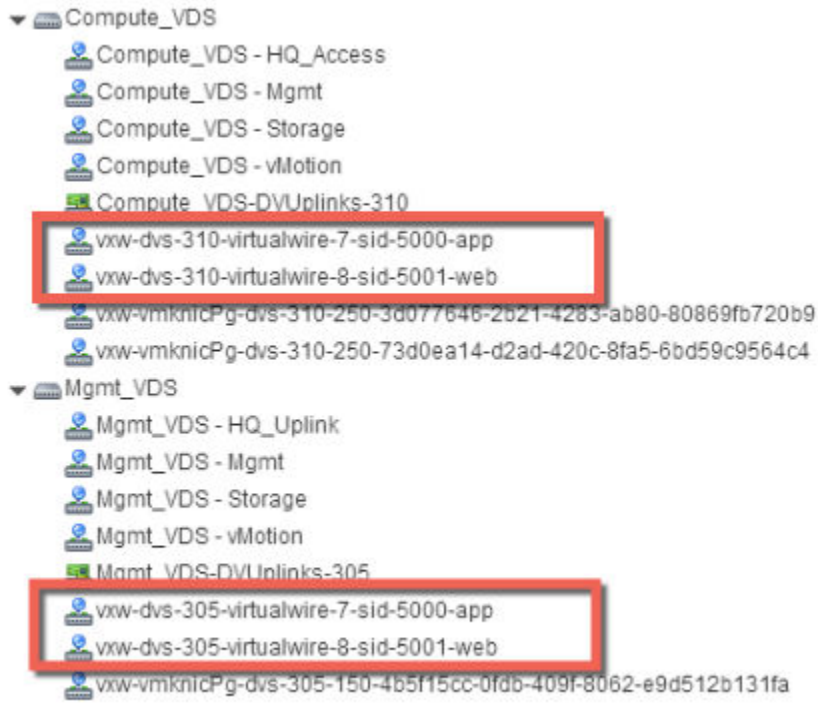
Résultats

Chaque commutateur logique que vous créez reçoit un ID du pool d'ID de segments et un câble virtuel est créé. Un câble virtuel est un dvPortgroup créé sur chaque vSphere Distributed Switch. Le descripteur de câble virtuel contient le nom du commutateur logique et l'ID de segment du commutateur logique. Des ID de segments attribués s'affichent à différents endroits, comme le montrent les exemples suivants.

Dans **Accueil > Mise en réseau et sécurité > Commutateurs logiques (Home > Networking & Security > Logical Switches)** :

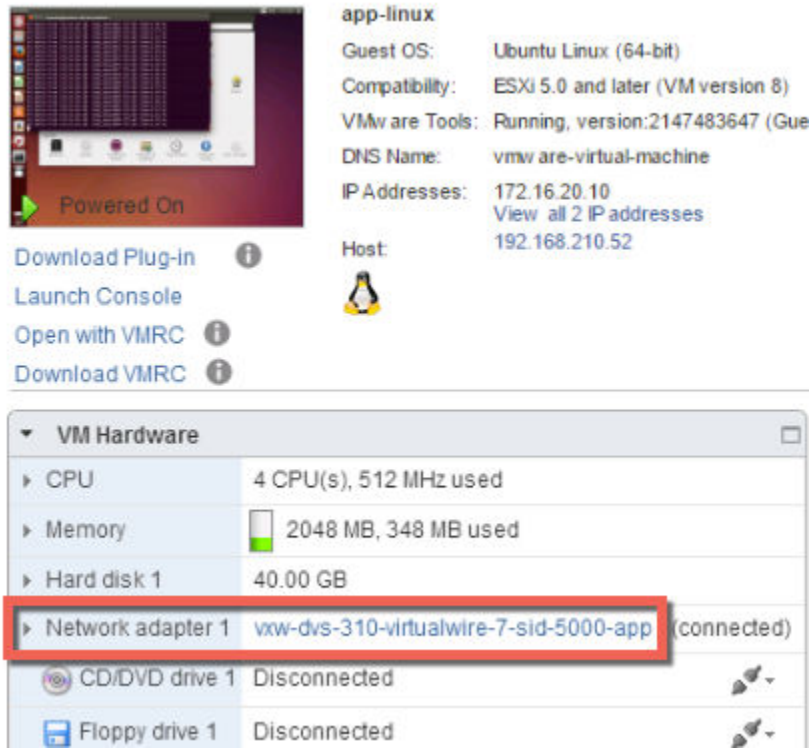


Dans **Accueil > Mise en réseau (Home > Networking)** :



Notez que les câbles virtuels sont créés à la fois sur les vSphere Distributed Switches, Compute_VDS et Mgmt_VDS. Cela est dû au fait que ces deux vSphere Distributed Switches font partie de la zone de transport associée aux commutateurs logiques Web et d'application.

Dans **Accueil > Hôtes et clusters > Machine virtuelle > Résumé (Home > Hosts and Clusters > VM > Summary)** :



Connectez-vous aux hôtes exécutant les machines virtuelles associées au commutateur logique et exécutez les commandes suivantes pour afficher la configuration de VXLAN locale et des informations sur l'état.

- Affiche des détails sur le VXLAN spécifique à l'hôte.

```
~ # esxcli network vswitch dvs vmware vxlan list
VDS ID                                          VDS Name      MTU  Segment ID     Gateway IP
Gateway MAC        Network Count  Vmknic Count
-----------------------------------------------  ------------  ----  -------------  -------------
-----------------  -------------  ------------
88 eb 0e 50 96 af 1d f1-36 fe c1 ef a1 51 51 49  Compute_VDS  1600  192.168.250.0  192.168.250.1
ff:ff:ff:ff:ff:ff              0             1
```

Note Si la commande `esxcli network vswitch dvs vmware vxlan` renvoie le message d'erreur « Commande ou espace de nom inconnu », exécutez la commande `/etc/init.d/hostd restart` sur l'hôte, puis réessayez.

Le nom VDS affiche vSphere Distributed Switch auquel l'hôte est associé.

L'ID de segment correspond au réseau IP utilisé par VXLAN.

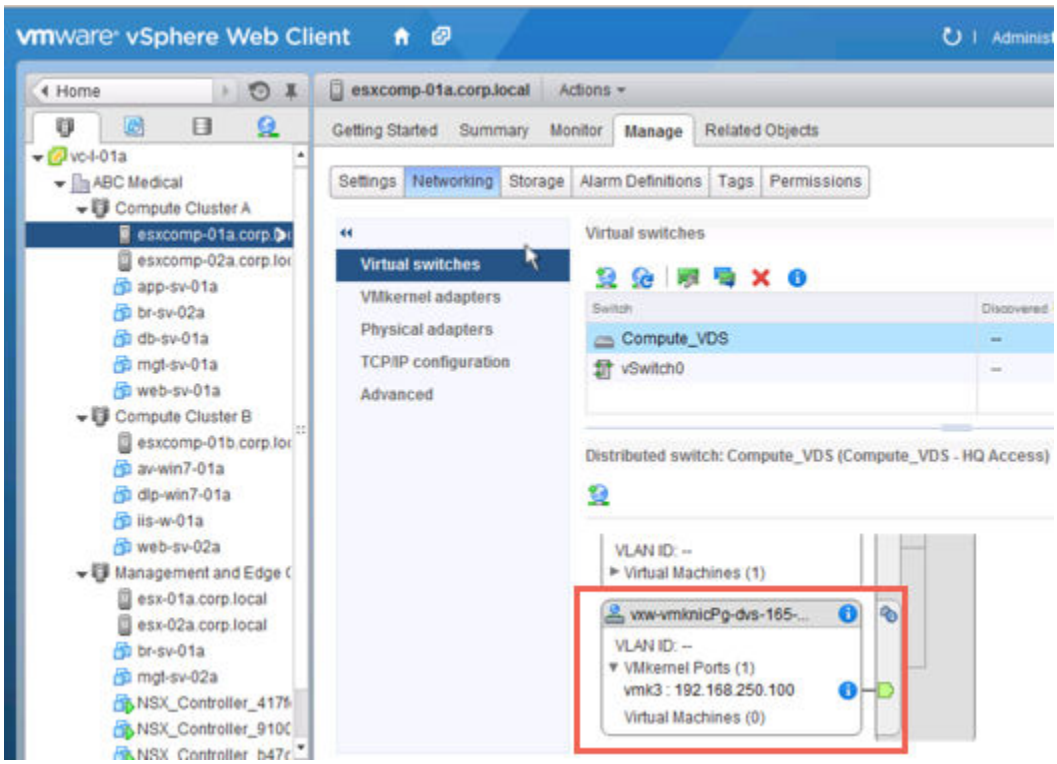
L'ID de passerelle correspond à l'adresse IP de passerelle utilisée par VXLAN.

L'adresse MAC de la passerelle reste ff:ff:ff:ff:ff:ff.

Le nombre de réseaux reste à 0, sauf si un DLR est associé au commutateur logique.

Le nombre de Vmknic doit correspondre au nombre de machines virtuelles associées au commutateur logique.

- Testez la connectivité de l'interface VTEP IP et vérifiez que la valeur de MTU a été augmentée pour prendre en charge l'encapsulation de VXLAN. Exécutez la commande ping à l'adresse IP de l'interface vmknic que vous pouvez trouver sur la page **Gérer > Mise en réseau > Commutateurs virtuels (Manage > Networking > Virtual switches)** de l'hôte dans vCenter Web Client.



L'indicateur -d définit le bit DF (ne pas fragmenter) sur les paquets IPv4. L'indicateur -s définit la taille du paquet.

```
root@esxcomp-02a ~ # vmkping ++netstack=vxlan -d -s 1570 192.168.250.100
PING 192.168.250.100 (192.168.250.100): 1570 data bytes
1578 bytes from 192.168.250.100: icmp_seq=0 ttl=64 time=1.294 ms
1578 bytes from 192.168.250.100: icmp_seq=1 ttl=64 time=0.686 ms
1578 bytes from 192.168.250.100: icmp_seq=2 ttl=64 time=0.758 ms

--- 192.168.250.100 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.686/0.913/1.294 ms
~ #
```

```
root@esxcomp-01a ~ # vmkping ++netstack=vxlan -d -s 1570 192.168.250.101
PING 192.168.250.101 (192.168.250.101): 1570 data bytes
1578 bytes from 192.168.250.101: icmp_seq=0 ttl=64 time=0.065 ms
1578 bytes from 192.168.250.101: icmp_seq=1 ttl=64 time=0.118 ms
```

```
--- 192.168.250.101 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.065/0.091/0.118 ms
```

Étape suivante

Créez un routeur logique (distribué) et associez-le à vos commutateurs logiques pour activer la connectivité entre les machines virtuelles connectées à différents commutateurs logiques.

Ajouter un routeur logique distribué

17

Un routeur logique distribué (DLR) est un dispositif virtuel contenant le plan de contrôle du routage distribuant le plan de données dans les modules noyaux de chaque hôte hyperviseur. La fonction de plan de contrôle de DLR s'appuie sur le cluster de NSX Controller pour transférer les mises à jour de routage dans les modules noyaux.

Lors du déploiement d'un nouveau routeur logique, prenez en compte les points suivants :

- Dans NSX 6.2 et les versions ultérieures, les interfaces logiques acheminées par un routeur logique peuvent être connectées à un VXLAN relié à un VLAN.
- Les interfaces de routeur logique et les interfaces de pontage ne peuvent pas être connectées à un dvPortgroup avec l'ID de VLAN définie sur 0.
- Une instance de routeur logique donnée ne peut pas être connectée aux commutateurs logiques se trouvant dans des zones de transport distinctes. Cela permet de s'assurer que tous les commutateurs logiques et instances de routeur logique sont alignés.
- Un routeur logique ne peut pas être connecté à des groupes de ports reposant sur VLAN si ce routeur logique est connecté à des commutateurs logiques s'étendant sur plusieurs VDS (vSphere Distributed Switch). Cela permet d'assurer un alignement correct des instances de routeur logique avec des dvPortgroups de commutateur logique entre les hôtes.
- Les interfaces de routeur logique ne doivent pas être créées sur deux groupes de ports distribués distincts (dvPortgroups) portant le même ID de VLAN si ces deux réseaux se trouvent dans le même commutateur vSphere Distributed Switch.
- Les interfaces de routeur logique ne doivent pas être créées sur deux dvPortgroups distincts portant le même ID de VLAN si ces deux réseaux se trouvent dans différents vSphere Distributed Switches partageant les mêmes hôtes. Autrement dit, les interfaces de routeur logique peuvent être créées sur deux réseaux distincts avec le même ID de VLAN si les deux dvPortgroups sont dans deux vSphere Distributed Switches distincts, tant que ceux-ci ne partagent pas d'hôte.
- Si VXLAN est configuré, les interfaces de routeur logique doivent être connectées à des groupes de ports distribués sur le commutateur vSphere Distributed Switch sur lequel VXLAN est configuré. Ne connectez pas les interfaces de routeur logique à des groupes de ports sur d'autres commutateurs vSphere Distributed Switch.

La liste suivante décrit la prise en charge de fonctionnalités par type d'interface (liaison montante et interne) sur le routeur logique :

- Les protocoles de routage dynamique (BGP et OSPF) sont pris en charge uniquement par des interfaces de liaison montante.
- Les règles de pare-feu s'appliquent uniquement aux interfaces de liaison montante et sont limitées au trafic de contrôle et de gestion destiné au dispositif virtuel Edge.
- Pour plus d'informations sur l'interface de gestion du DLR, consultez l'article de la base de connaissances « Management Interface Guide: DLR Control VM - NSX » (Guide d'interface de gestion : VM de contrôle du DLR - NSX) http://kb.vmware.com/kb/2122060.

Conditions préalables

- Le rôle **Administrateur d'entreprise** ou **Administrateur NSX** doit vous avoir été attribué.
- Vous devez créer un pool local d'ID de segments, même si vous ne prévoyez pas de créer des commutateurs logiques NSX.
- Avant de créer ou de modifier une configuration de routeur logique, vérifiez que le cluster de contrôleurs est actif et disponible. Un routeur logique ne peut pas distribuer les informations de routage aux hôtes sans l'aide des instances de NSX Controller. Un routeur logique s'appuie sur les instances de NSX Controller pour fonctionner, au contraire des passerelles Edge Services Gateway.
- Si un routeur logique doit être connecté à des dvportGroups VLAN, vérifiez que tous les hôtes hyperviseurs avec un dispositif de routeur logique installé peuvent communiquer entre eux sur le port UDP 6999. La communication sur ce port est requise pour que le proxy ARP basé sur VLAN du routeur logique fonctionne.
- Déterminez l'emplacement où déployer le dispositif de routeur logique.
  - L'hôte de destination doit appartenir à la même zone de transport que les commutateurs logiques connectés aux interfaces du nouveau routeur logique.
  - Évitez de le placer sur le même hôte en tant que passerelle ESG en amont si vous utilisez ESG dans une configuration ECMP. Vous pouvez utiliser les règles anti-affinité de DRS pour le mettre en application, ce qui permet de limiter l'impact d'une défaillance de l'hôte sur le transfert du routeur logique. Cette directive ne s'applique pas si vous avez une seule ESG en amont ou en mode HA. Pour plus d'informations, reportez-vous au *Guide de conception de virtualisation réseau de VMware NSX for vSphere* à l'adresse https://communities.vmware.com/docs/DOC-27683.
- Vérifiez que le cluster d'hôtes sur lequel vous installez le dispositif de routeur logique est préparé pour NSX. Consultez « Préparer des clusters d'hôtes pour NSX » dans le *Guide d'installation de NSX*.

Procédure

1. Dans vSphere Web Client, accédez à **Page d'accueil > Mise en réseau et sécurité > Dispositifs NSX Edge (Home > Networking & Security > NSX Edges)**.

2 Cliquez sur l'icône **Ajouter (Add)** ( ).

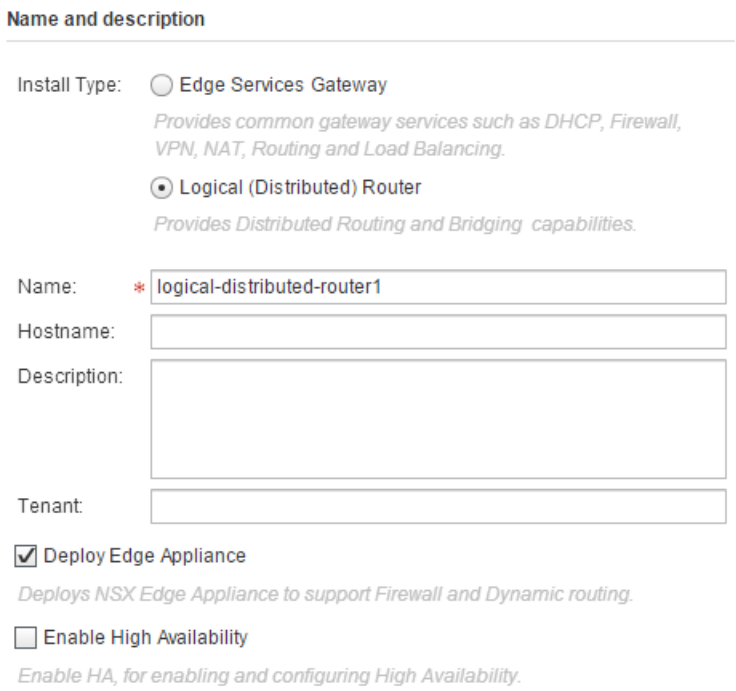
3 Sélectionnez **Routeur (distribué) logique (Logical (Distributed) Router)** et tapez le nom du périphérique.

Ce nom apparaît dans l'inventaire vCenter. Utilisez un nom unique au sein de tous les routeurs logiques d'un même locataire.

Sinon, vous pouvez entrer également un nom d'hôte (en option). Ce nom apparaît dans l'interface de ligne de commande. Si vous n'entrez aucun nom d'hôte, l'ID du dispositif Edge, créé automatiquement, s'affiche dans l'interface de ligne de commande.

Sinon, vous pouvez entrer une description et un locataire (en option).

Par exemple :



4 (Facultatif) Déployez un dispositif Edge.

Déployer un dispositif Edge (Deploy Edge Appliance) est sélectionné par défaut. Un dispositif Edge (également appelé dispositif virtuel de routeur logique) est requis pour le routage dynamique et le pare-feu du dispositif de routeur logique qui s'applique aux pings du routeur logique, à l'accès SSH et au trafic de routage dynamique.

Vous pouvez décocher l'option du dispositif Edge si vous avez besoin d'itinéraires statiques uniquement et que vous ne souhaitez pas déployer de dispositif Edge. Une fois le routeur logique créé, vous ne pouvez pas y ajouter de dispositif Edge.

5 (Facultatif) Activez la haute disponibilité.

Activer la haute disponibilité (Enable High Availability) n'est pas coché par défaut. Cochez la case **Activer la haute disponibilité (Enable High Availability)** pour activer et configurer la haute disponibilité. La haute disponibilité est requise si vous prévoyez d'effectuer du routage dynamique.

6 Composez et confirmez un mot de passe pour le routeur logique.

Le mot de passe doit se composer de 12 à 255 caractères et doit contenir ce qui suit :

- Au moins une lettre majuscule
- Au moins une lettre minuscule
- Au moins un chiffre
- Au moins un caractère spécial

7 (Facultatif) Activez SSH.

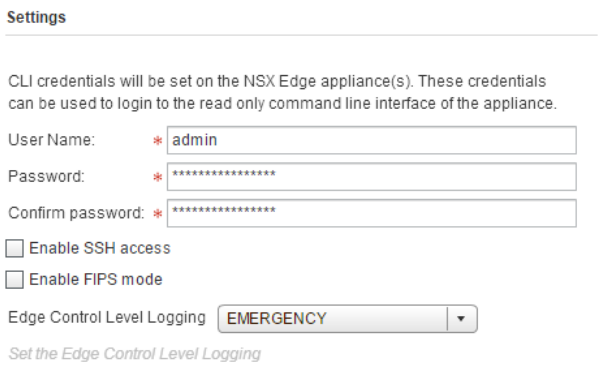
Par défaut, l'accès SSH est désactivé. Si vous n'activez pas l'accès SSH, vous pouvez toujours accéder au routeur logique en ouvrant la console du dispositif virtuel. L'activation de SSH ici entraîne l'exécution du processus SSH sur le dispositif virtuel de routeur logique. Vous devez ajuster la configuration du pare-feu de routeur logique manuellement afin d'autoriser l'accès SSH à l'adresse du protocole du routeur logique. L'adresse du protocole est configurée au moment de la configuration du routage dynamique sur le routeur logique.

8 (Facultatif) Activez le mode FIPS et définissez le niveau de journal.

Par défaut, le mode FIPS est désactivé. Cochez la case **Activer le mode FIPS (Enable FIPS mode)** pour activer le mode FIPS. Lorsque le mode FIPS est activé, toutes les communications sécurisées en provenance ou à destination du dispositif NSX Edge utilisent des protocoles ou des algorithmes cryptographiques qui sont autorisés par FIPS.

Par défaut, le niveau de journal est le niveau d'urgence.

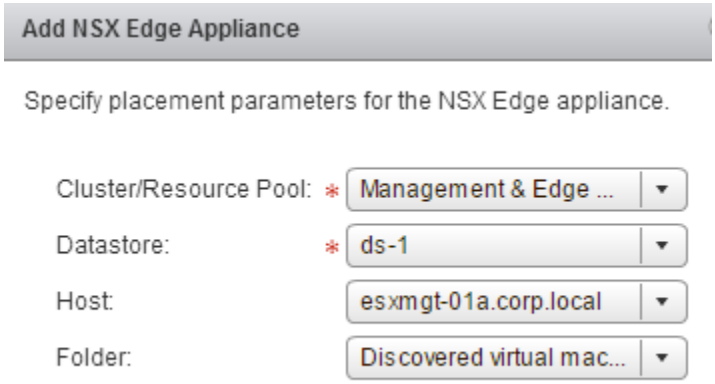
Par exemple :



9 Configurez le déploiement.

- Si vous n'avez pas sélectionné **Déployer un dispositif Edge (Deploy Edge Appliance)**, l'icône **Ajouter (Add) (+)** est grisée. Cliquez sur **Suivant (Next)** pour poursuivre la configuration.
- Si vous avez sélectionné **Déployer un dispositif Edge (Deploy Edge Appliance)**, entrez les paramètres du dispositif virtuel de routeur logique.

Par exemple :



10 Configurez des interfaces. sur les routeurs logiques, seul l'adressage IPv4 est pris en charge.

a Configurez la connexion à l'interface HA et éventuellement une adresse IP.

Si vous avez sélectionné **Déployer un dispositif Edge (Deploy Edge Appliance)**, vous devez connecter l'interface HA à un commutateur logique ou un groupe de ports distribués. Si vous utilisez cette interface comme une interface haute disponibilité uniquement, utilisez un commutateur logique. Un sous-réseau /30 est alloué à partir de la plage locale de lien 169.254.0.0/16 et il est utilisé pour fournir une adresse IP à chacun des deux dispositifs NSX Edge.

Si vous souhaitez utiliser cette interface pour vous connecter à NSX Edge, vous pouvez définir une adresse IP et un préfixe supplémentaires pour l'interface HA.

Note Dans les versions antérieures à NSX 6.2, l'interface HA était appelée interface de gestion. Vous ne pouvez pas utiliser l'accès SSH pour vous connecter à l'interface HA si vous ne vous trouvez pas sur le même sous-réseau IP que l'interface. Vous ne pouvez pas configurer d'itinéraire statique pointant vers l'interface HA, ce qui signifie que RPF refusera le trafic entrant. En théorie, vous pouvez désactiver RPF, mais cela est contre-productif pour la haute disponibilité. Pour l'accès SSH, vous pouvez aussi utiliser l'adresse du protocole du routeur logique qui est configurée ultérieurement lors de la configuration du routage dynamique.

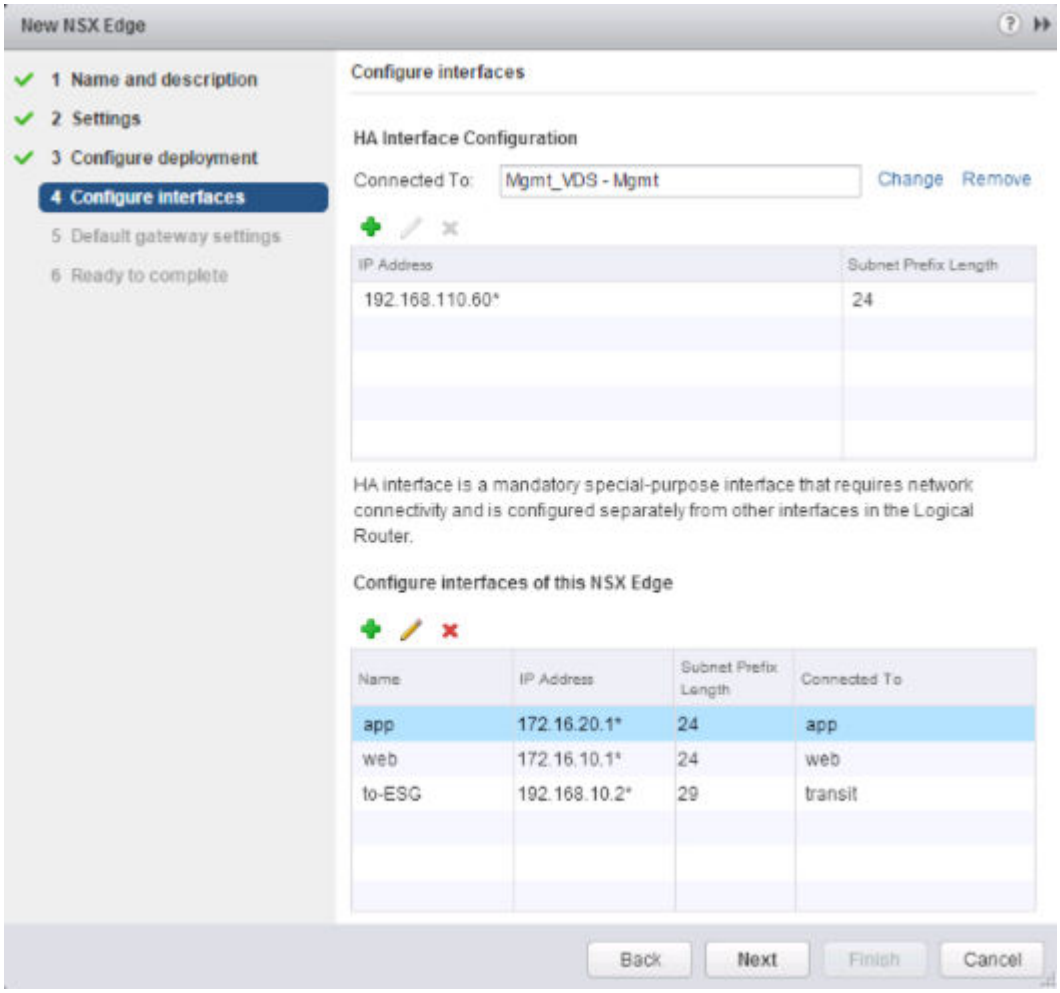
Dans NSX 6.2 et les versions ultérieures, l'interface HA d'un routeur logique est automatiquement exclue de la redistribution d'itinéraire.

b Configurer les interfaces de ce dispositif NSX Edge.

Dans **Configurer les interfaces de ce dispositif NSX Edge (Configure interfaces of this NSX Edge)**, les interfaces internes sont conçues pour les connexions aux commutateurs autorisant la communication de machine virtuelle à machine virtuelle (parfois appelée communication horizontale). Les interfaces internes sont créées en tant que pseudo vNIC sur le dispositif virtuel de routeur logique. Les interfaces de liaison montante concernent les communications verticales. Une interface de liaison montante de routeur logique peut se connecter à une passerelle Edge Services Gateway ou à une machine virtuelle de routeur tierce. Pour que le routage dynamique fonctionne, vous devez disposer d'au moins une interface de liaison montante . Les interfaces de liaison montante sont créées en tant que vNIC sur le dispositif virtuel de routeur logique.

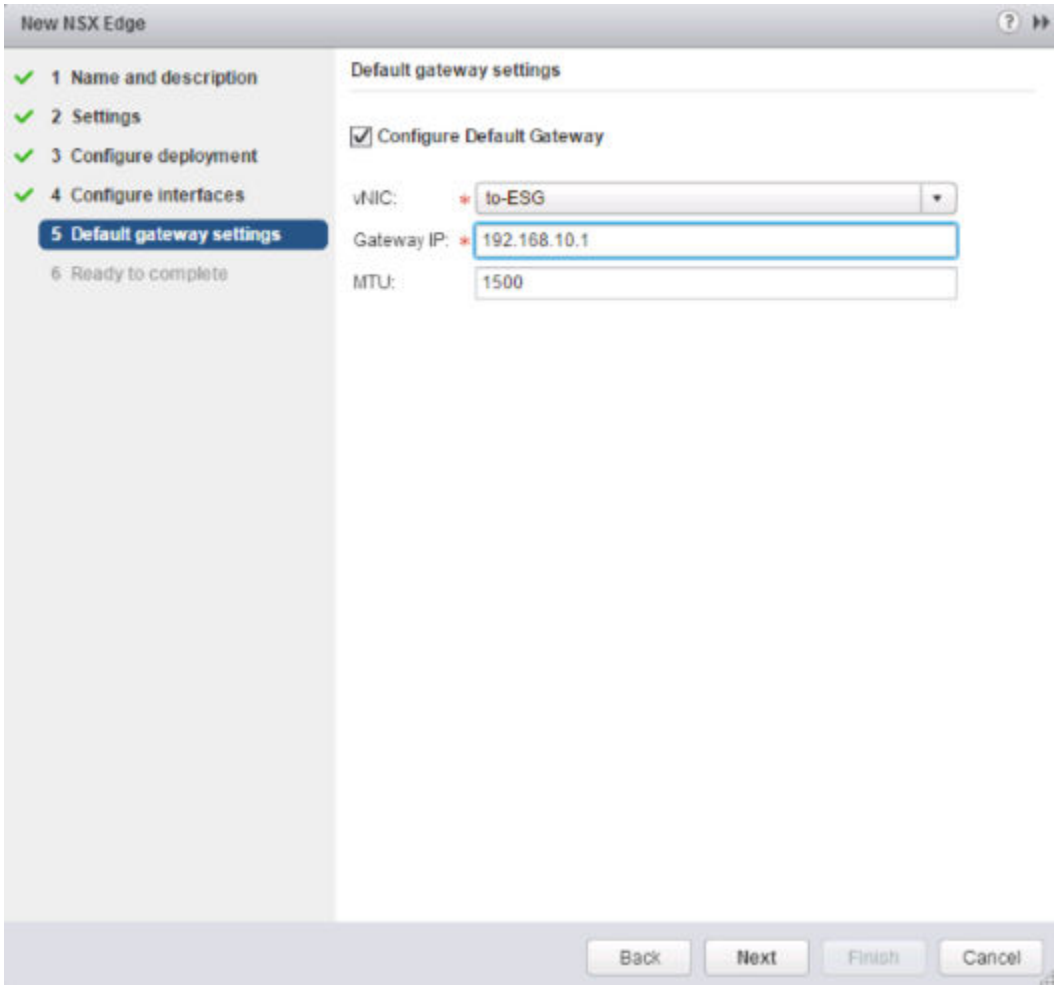
La configuration de l'interface que vous entrez ici peut être modifiée ultérieurement. Vous pouvez ajouter, supprimer et modifier les interfaces une fois qu'un routeur logique est déployé.

L'exemple suivant présente une interface HA connectée au groupe de port distribué de gestion. Il présente également deux interfaces internes (application et Web) et une interface de liaison montante (vers ESG).


New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Ready to complete
Configure interfaces
HA Interface Configuration
Connected To: Mgmt_VDS - Mgmt
Change
Remove
IP Address
Subnet Prefix Length
192.168.110.60*
24
HA interface is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.
Configure interfaces of this NSX Edge
Name
IP Address
Subnet Prefix Length
Connected To
app
172.16.20.1*
24
app
web
172.16.10.1*
24
web
to-ESG
192.168.10.2*
29
transit
Back
Next
Finish
Cancel

11 Configurez une passerelle par défaut.

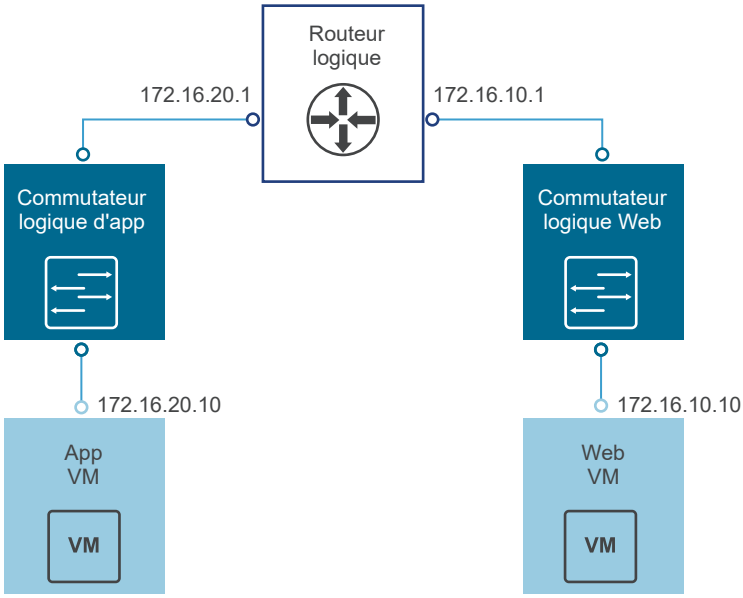
Par exemple :



12 Vérifiez que les passerelles par défaut des machines virtuelles associées aux commutateurs logiques sont définies correctement sur les adresses IP de l'interface du routeur logique.

Résultats

Dans l'exemple de topologie suivant, la passerelle par défaut de la machine virtuelle d'application est 172.16.20.1. la passerelle par défaut de la machine virtuelle Web est 172.16.10.1. Vérifiez que les machines virtuelles peuvent exécuter une commande ping sur leurs passerelles par défaut et entre elles.



Connectez-vous à NSX Manager à l'aide de SSH ou de la console, puis exécutez les commandes suivantes :

- Répertoriez toutes les informations de l'instance de routeur logique.

```
nsxmgr-l-01a> show logical-router list all
Edge-id             Vdr Name                    Vdr id              #Lifs
edge-1              default+edge-1              0x00001388          3
```

- Répertoriez les hôtes ayant reçu les informations de routage du routeur logique de la part du cluster de contrôleurs.

```
nsxmgr-l-01a> show logical-router list dlr edge-1 host
ID                   HostName
host-25              192.168.210.52
host-26              192.168.210.53
host-24              192.168.110.53
```

  La sortie inclut tous les hôtes de tous les clusters d'hôtes configurés en tant que membres de la zone de transport dont fait partie le commutateur logique connecté au routeur logique spécifié (edge-1 dans cet exemple).

- Répertoriez les informations de la table de routage communiquées aux hôtes par le routeur logique. Les entrées de la table de routage doivent être homogènes sur tous les hôtes.

```
nsx-mgr-l-01a> show logical-router host host-25 dlr edge-1 route

VDR default+edge-1 Route Table
Legend: [U: Up], [G: Gateway], [C: Connected], [I: Interface]
Legend: [H: Host], [F: Soft Flush] [!: Reject] [E: ECMP]

Destination     GenMask         Gateway         Flags   Ref Origin   UpTime    Interface
-----------     -------         -------         -----   --- ------   ------    ---------
0.0.0.0         0.0.0.0         192.168.10.1    UG      1   AUTO     4101      138800000002
```

```
172.16.10.0     255.255.255.0    0.0.0.0         UCI     1   MANUAL   10195     13880000000b
172.16.20.0     255.255.255.0    0.0.0.0         UCI     1   MANUAL   10196     13880000000a
192.168.10.0    255.255.255.248  0.0.0.0         UCI     1   MANUAL   10196     138800000002
192.168.100.0   255.255.255.0    192.168.10.1    UG      1   AUTO     3802      138800000002
```

- Répertoriez les informations sur le routeur du point de vue de l'un des hôtes. Cela permet d'apprendre quel contrôleur communique avec l'hôte.

```
nsx-mgr-l-01a> show logical-router host host-25 dlr edge-1 verbose

VDR Instance Information :
---------------------------

Vdr Name:                   default+edge-1
Vdr Id:                     0x00001388
Number of Lifs:             3
Number of Routes:           5
State:                      Enabled
Controller IP:              192.168.110.203
Control Plane IP:           192.168.210.52
Control Plane Active:       Yes
Num unique nexthops:        1
Generation Number:          0
Edge Active:                No
```

Vérifiez le champ Adresse IP du contrôleur dans les résultats de la commande `show logical-router host host-25 dlr edge-1 verbose`.

Connectez-vous via SSH à un contrôleur et exécutez les commandes suivantes pour afficher les informations sur l'état que vous avez apprises sur le contrôleur (VNI, VTEP, MAC et ARP).

- ```
  192.168.110.202 # show control-cluster logical-switches vni 5000
  VNI      Controller      BUM-Replication ARP-Proxy Connections
  5000     192.168.110.201 Enabled         Enabled   0
  ```

  Les résultats sur VNI 5000 n'affichent aucune connexion et répertorient le contrôleur 192.168.110.201 comme propriétaire de VNI 5000. Connectez-vous à ce contrôleur pour réunir des informations supplémentaires pour VNI 5000.

  ```
  192.168.110.201 # show control-cluster logical-switches vni 5000
  VNI      Controller      BUM-Replication ARP-Proxy Connections
  5000     192.168.110.201 Enabled         Enabled   3
  ```

  Les résultats sur 192.168.110.201 affichent trois connexions. Vérifiez les VNI supplémentaires.

  ```
  192.168.110.201 # show control-cluster logical-switches vni 5001
  VNI      Controller      BUM-Replication ARP-Proxy Connections
  5001     192.168.110.201 Enabled         Enabled   3
  ```

  ```
  192.168.110.201 # show control-cluster logical-switches vni 5002
  VNI      Controller      BUM-Replication ARP-Proxy Connections
  5002     192.168.110.201 Enabled         Enabled   3
  ```
  ```

Du fait que 192.168.110.201 possède les trois connexions VNI, nous nous attendons à ce que l'autre contrôleur, 192.168.110.203, n'ait aucune connexion.

```
192.168.110.203 # show control-cluster logical-switches vni 5000
VNI      Controller      BUM-Replication ARP-Proxy Connections
5000     192.168.110.201 Enabled         Enabled   0
```

- Avant de vérifier les tables MAC et ARP, exécutez une commande ping de l'une des machines virtuelles à l'autre.

  De la machine virtuelle d'application à la machine virtuelle Web :

  ```
  vmware@app-vm$ ping 172.16.10.10
  PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
  64 bytes from 172.16.10.10: icmp_req=1 ttl=64 time=2.605 ms
  64 bytes from 172.16.10.10: icmp_req=2 ttl=64 time=1.490 ms
  64 bytes from 172.16.10.10: icmp_req=3 ttl=64 time=2.422 ms
  ```

  Vérifiez les tables MAC.

  ```
  192.168.110.201 # show control-cluster logical-switches mac-table 5000
  VNI      MAC               VTEP-IP         Connection-ID
  5000     00:50:56:a6:23:ae 192.168.250.52  7
  ```

  ```
  192.168.110.201 # show control-cluster logical-switches mac-table 5001
  VNI      MAC               VTEP-IP         Connection-ID
  5001     00:50:56:a6:8d:72 192.168.250.51  23
  ```

  Vérifiez les tables ARP.

  ```
  192.168.110.201 # show control-cluster logical-switches arp-table 5000
  VNI      IP              MAC               Connection-ID
  5000     172.16.20.10    00:50:56:a6:23:ae 7
  ```

  ```
  192.168.110.201 # show control-cluster logical-switches arp-table 5001
  VNI      IP              MAC               Connection-ID
  5001     172.16.10.10    00:50:56:a6:8d:72 23
  ```

Vérifiez les informations sur le routeur logique. Chaque instance de routeur logique est desservie par l'un des nœuds de contrôleur.

La sous-commande `instance` de la commande `show control-cluster logical-routers` affiche une liste de routeurs logiques connectés à ce contrôleur.

La sous-commande `interface-summary` affiche les LIF apprises par le contrôleur auprès de l'instance de NSX Manager. Ces informations sont envoyées aux hôtes situés dans les clusters d'hôtes gérés dans la zone de transport.

La sous-commande `routes` affiche la table de routage envoyée à ce contrôleur par le dispositif virtuel du routeur logique (également appelé machine virtuelle de contrôle). Contrairement aux hôtes ESXi, la table de routage n'inclut pas les sous-réseaux connectés directement, car ces informations sont fournies par la configuration de LIF. Les informations d'itinéraires sur les hôtes ESXi incluent les sous-réseaux connectés directement, car dans ce cas, il s'agit d'une table de transfert utilisée par le chemin d'accès aux données de l'hôte ESXi.

- Répertoriez tous les routeurs logiques connectés à ce contrôleur.

```
controller # show control-cluster logical-routers instance all
LR-Id      LR-Name            Universal Service-Controller Egress-Locale
0x1388     default+edge-1     false     192.168.110.201    local
```

  Prenez note de l'ID du routeur logique et utilisez-le dans la commande suivante.

-
```
controller # show control-cluster logical-routers interface-summary 0x1388
Interface                       Type   Id           IP[]
13880000000b                    vxlan  0x1389       172.16.10.1/24
13880000000a                    vxlan  0x1388       172.16.20.1/24
138800000002                    vxlan  0x138a       192.168.10.2/29
```

-
```
controller # show control-cluster logical-routers routes 0x1388
Destination        Next-Hop[]      Preference Locale-Id                            Source
192.168.100.0/24   192.168.10.1    110        00000000-0000-0000-0000-000000000000 CONTROL_VM
0.0.0.0/0          192.168.10.1    0          00000000-0000-0000-0000-000000000000 CONTROL_VM
```

```
[root@comp02a:~] esxcfg-route -l
VMkernel Routes:
Network          Netmask          Gateway          Interface
10.20.20.0       255.255.255.0    Local Subnet     vmk1
192.168.210.0    255.255.255.0    Local Subnet     vmk0
default          0.0.0.0          192.168.210.1    vmk0
```

- Affichez les connexions du contrôleur au VNI spécifique.

```
192.168.110.203 # show control-cluster logical-switches connection-table 5000
Host-IP         Port  ID
192.168.110.53  26167 4
192.168.210.52  27645 5
192.168.210.53  40895 6
```

```
192.168.110.202 # show control-cluster logical-switches connection-table 5001
Host-IP         Port  ID
192.168.110.53  26167 4
192.168.210.52  27645 5
192.168.210.53  40895 6
```

  Les adresses IP d'hôtes sont des interfaces vmk0, pas des VTEP. Les connexions entre hôtes ESXi et contrôleurs sont créées sur le réseau de gestion. Les numéros de port sont des ports TCP éphémères alloués par ma pile d'adresses IP de l'hôte ESXi lorsque l'hôte établit une connexion avec le contrôleur.

- Sur l'hôte, vous pouvez afficher la connexion réseau du contrôleur associée au numéro de port.

```
[root@192.168.110.53:~] #esxcli network ip connection list | grep 26167
tcp         0       0  192.168.110.53:26167             192.168.110.101:1234  ESTABLISHED
96416  newreno  netcpa-worker
```

- Affichez les VNI actifs sur l'hôte. Observez les différences de résultat entre les hôtes. Tous les VNI ne sont pas actifs sur tous les hôtes. Un VNI est actif sur un hôte si celui-ci a une machine virtuelle connectée au commutateur logique.

```
[root@192.168.210.52:~] # esxcli network vswitch dvs vmware vxlan network list --vds-name
Compute_VDS
VXLAN ID  Multicast IP               Control Plane                        Controller Connection
Port Count  MAC Entry Count  ARP Entry Count  VTEP Count
--------  -------------------------  -----------------------------------  ---------------------
----------  ---------------  ---------------  ----------
    5000  N/A (headend replication)  Enabled (multicast proxy,ARP proxy)  192.168.110.203
(up)            1                0                0           0
    5001  N/A (headend replication)  Enabled (multicast proxy,ARP proxy)  192.168.110.202
(up)            1                0                0           0
```

Note Pour activer l'espace de nom vxlan dans vSphere 6.0 et versions ultérieures, exécutez la commande `/etc/init.d/hostd restart`.

Pour les commutateurs logiques en mode hybride ou monodiffusion, la commande `esxcli network vswitch dvs vmware vxlan network list --vds-name <vds-name>` contient la sortie suivante :

- Le plan de contrôle est activé.
- Le proxy de multidiffusion et le proxy ARP sont répertoriés. Le proxy AARP est répertorié, même si vous avez désactivé la découverte d'adresses IP.
- Une adresse IP de contrôleur valide est répertoriée et la connexion est active.
- Si un routeur logique est connecté à l'hôte ESXi, le nombre de ports est d'au moins 1, même s'il n'y a aucune machine virtuelle sur l'hôte connecté au commutateur logique. Ce port est me vdrPort, qui est un dvPort spécial connecté au module de noyau du routeur logique sur l'hôte ESXi.

- Exécutez d'abord la commande ping d'une machine virtuelle à une autre sur un sous-réseau différent, puis affichez la table des adresses MAC. Notez que l'adresse MAC interne correspond à l'entrée de la machine virtuelle, tandis que les adresses IP et MAC externes renvoient au VTEP.

```
~ # esxcli network vswitch dvs vmware vxlan network mac list --vds-name=Compute_VDS --vxlan-
id=5000
Inner MAC          Outer MAC          Outer IP        Flags
-----------------  -----------------  --------------  --------
00:50:56:a6:23:ae  00:50:56:6a:65:c2  192.168.250.52  00000111
```

```
~ # esxcli network vswitch dvs vmware vxlan network mac list --vds-name=Compute_VDS --vxlan-
id=5001
Inner MAC          Outer MAC          Outer IP        Flags
-----------------  -----------------  --------------  --------
02:50:56:56:44:52  00:50:56:6a:65:c2  192.168.250.52  00000101
00:50:56:f0:d7:e4  00:50:56:6a:65:c2  192.168.250.52  00000111
```

Étape suivante

Lorsque vous installez un dispositif NSX Edge, NSX permet le démarrage/arrêt automatique des VM sur l'hôte si vSphere HA est désactivé sur le cluster. Si les VM du dispositif sont par la suite migrées vers d'autres hôtes du cluster, le mécanisme de démarrage/arrêt automatique des VM peut ne pas être activé sur ces nouveaux hôtes. C'est la raison pour laquelle VMware vous recommande, lorsque vous installez des dispositifs NSX Edge sur des clusters où vSphere HA est désactivé, de vérifier tous les hôtes du cluster pour vous assurer que le démarrage/arrêt automatique des machines virtuelles est activé. Dans *Administration d'une machine virtuelle vSphere*, consultez la section « Modifier les paramètres de démarrage et d'arrêt d'une machine virtuelle ».

Une fois le routeur logique déployé, double-cliquez sur l'ID du routeur logique pour configurer des paramètres supplémentaires, comme les interfaces, le routage, le pare-feu, le pontage et le relais DHCP.

Ajouter un dispositif Edge Services Gateway (ESG)

18

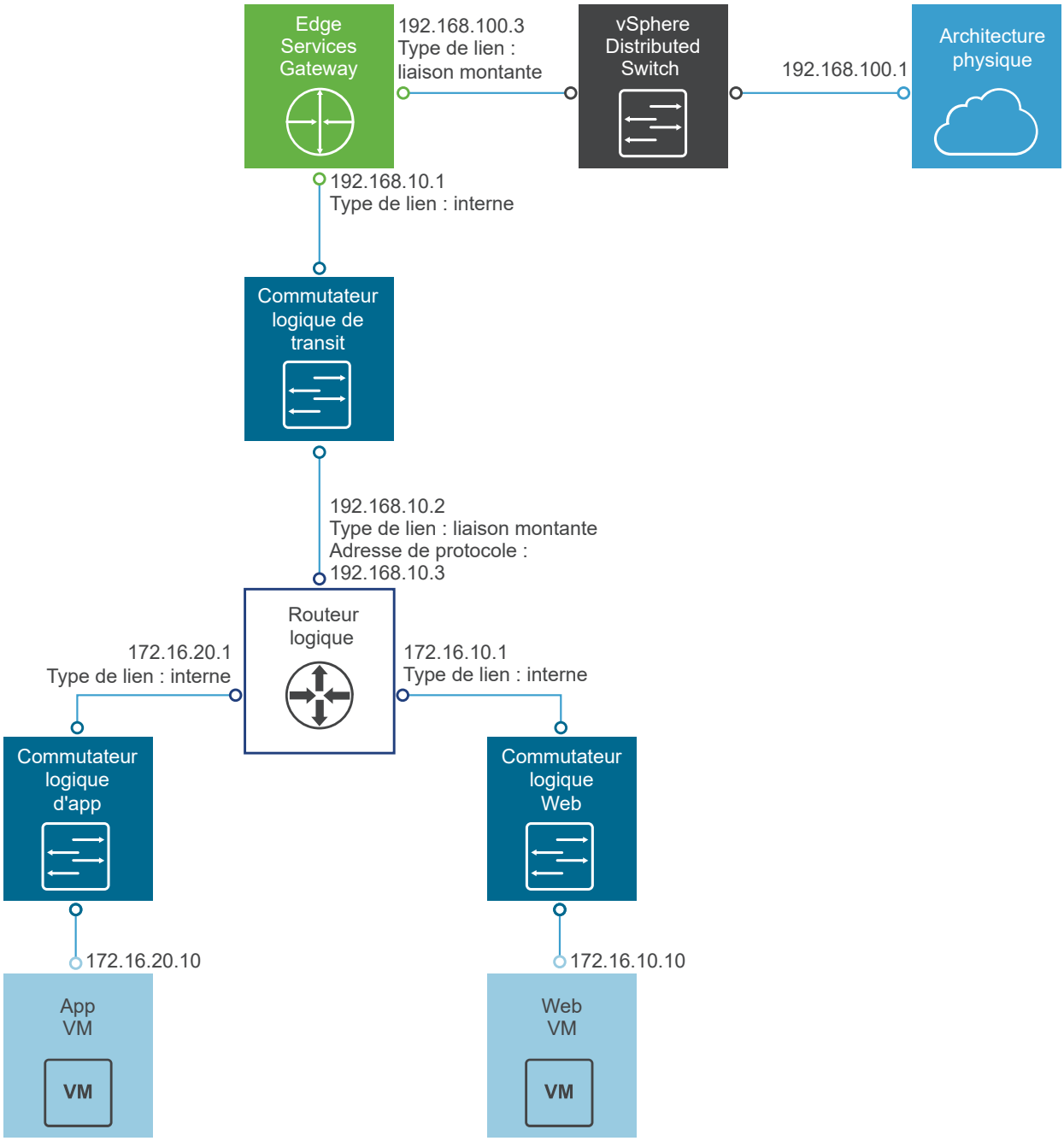
Vous pouvez installer plusieurs dispositifs virtuels Services Gateway NSX Edge dans un centre de données. Chaque dispositif virtuel NSX Edge peut disposer d'un total de dix interfaces réseau internes et de liaison montante. Les interfaces internes se connectent à des groupes de ports sécurisés et font office de passerelle pour toutes les machines virtuelles protégées du groupe de ports. Le sous-réseau attribué à l'interface interne peut être un espace d'adresses IP routé publiquement ou un espace privé NAT/routé défini par la RFC 1918. Les règles de pare-feu et les autres services NSX Edge sont appliqués au trafic entre les interfaces.

Les interfaces de liaison montante d'une ESG se connectent à des groupes de ports de liaison montante ayant accès à un réseau d'entreprise partagé ou à un service qui propose la mise en réseau avec couche d'accès.

La liste suivante décrit la prise en charge de fonctionnalités par type d'interface (liaison montante et interne) sur une passerelle ESG.

- DHCP : non pris en charge sur l'interface de liaison montante.
- Redirecteur DNS : non pris en charge sur l'interface de liaison montante.
- HA : non prise en charge sur l'interface de liaison montante, nécessite au moins une interface interne.
- VPN SSL : l'adresse IP de l'écouteur doit faire partie de l'interface de liaison montante.
- VPN IPSec : l'adresse IP locale doit faire partie de l'interface de liaison montante.
- VPN de niveau 2 : seuls des réseaux internes peuvent être étendus.

L'illustration suivante présente un exemple de topologie avec une interface de liaison montante de passerelle ESG connectée à une infrastructure physique par l'intermédiaire de vSphere Distributed Switch et l'interface interne de la passerelle ESG se connecte à un routeur logique NSX par l'intermédiaire d'un commutateur logique NSX.


Edge Services Gateway
192.168.100.3
Type de lien : liaison montante
vSphere Distributed Switch
192.168.100.1
Architecture physique
192.168.10.1
Type de lien : interne
Commutateur logique de transit
192.168.10.2
Type de lien : liaison montante
Adresse de protocole : 192.168.10.3
Routeur logique
172.16.20.1
Type de lien : interne
172.16.10.1
Type de lien : interne
Commutateur logique d'app
Commutateur logique Web
172.16.20.10
172.16.10.10
App VM
VM
Web VM
VM

Il est possible de configurer plusieurs adresses IP externes pour les services d'équilibrage de charge, de VPN d'un site à l'autre et NAT.

Conditions préalables

- Le rôle Administrateur d'entreprise ou Administrateur NSX doit vous avoir été attribué.
- Vérifiez que la capacité du pool de ressources est suffisante pour que le dispositif virtuel de la passerelle ESG (Edge Services Gateway) puisse être déployé. Reportez-vous à la section Configuration système requise pour NSX.
- Vérifiez que les clusters d'hôtes sur lesquels le dispositif NSX Edge sera installé sont préparés pour NSX. Consultez Préparer des clusters d'hôtes pour NSX dans le *Guide d'installation de NSX*.

Procédure

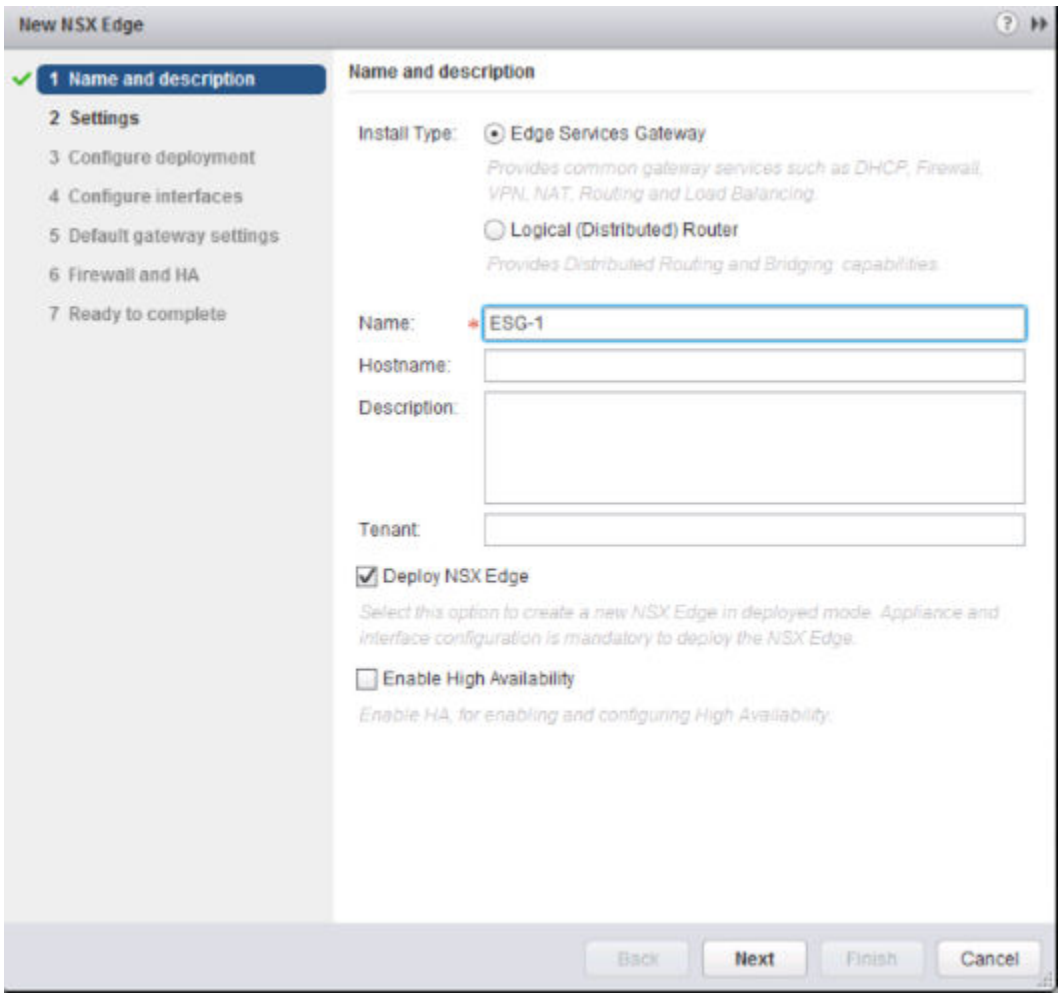
1. Dans vCenter, accédez à **Accueil > Mise en réseau et sécurité > Dispositifs NSX Edge (Home > Networking & Security > NSX Edges)** et cliquez sur l'icône **Ajouter (Add)** ( ).
2. Sélectionnez **Edge Services Gateway** et tapez le nom du périphérique.

   Ce nom apparaît dans l'inventaire vCenter. Ce nom doit être unique au sein des passerelles ESG d'un même locataire.

   Sinon, vous pouvez entrer également un nom d'hôte (en option). Ce nom apparaît dans l'interface de ligne de commande. Si vous ne spécifiez pas le nom d'hôte, l'ID du dispositif Edge, créé automatiquement, s'affiche dans l'interface de ligne de commande.

   Sinon, vous pouvez entrer une description et un locataire et activer la haute disponibilité (facultatif).

   Par exemple :



3 Composez et confirmez un mot de passe pour la passerelle ESG.

Le mot de passe doit se composer d'au moins 12 caractères et doit respecter trois des quatre règles suivantes :

- Au moins une lettre en majuscule
- Au moins une lettre en minuscule
- Au moins un chiffre
- Au moins un caractère spécial

4 (Facultatif) Activez SSH, la haute disponibilité, la génération automatique de règles et le mode FIPS, puis définissez le niveau de journal.

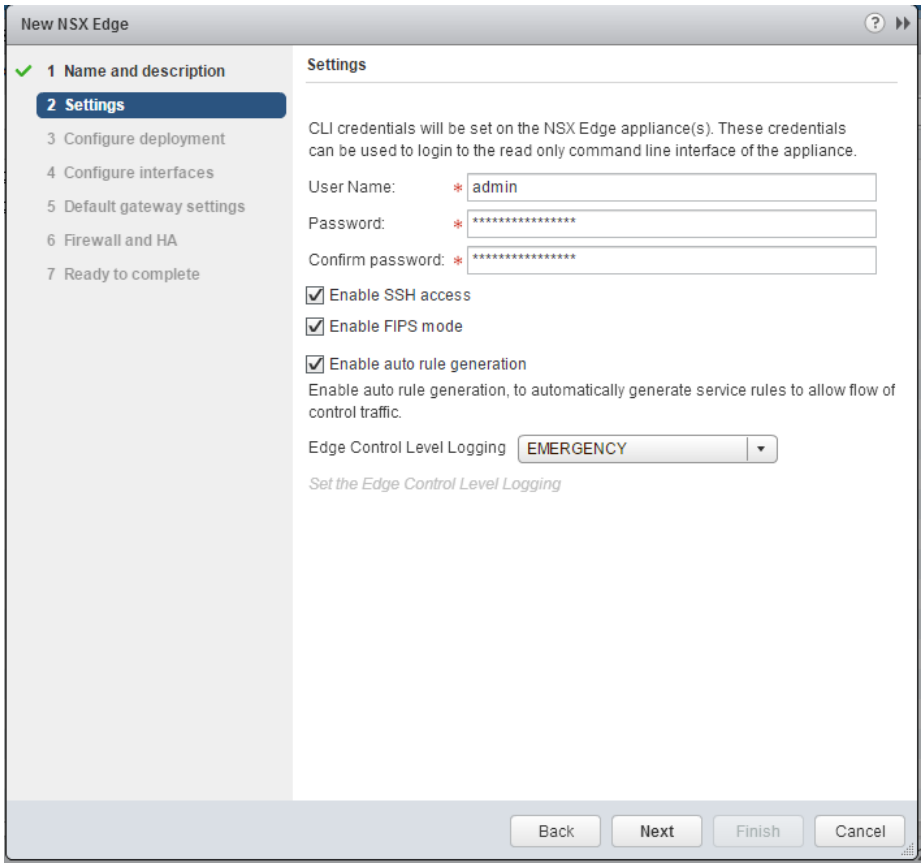
Si vous n'activez pas la génération automatique de règles, vous devez ajouter manuellement une configuration de pare-feu, de NAT et de routage afin d'autoriser le trafic de contrôle pour certains services NSX Edge, notamment l'équilibrage de charge et le VPN. La génération automatique de règles ne crée pas de règles pour le trafic du canal de données.

Par défaut, SSH et la haute disponibilité sont désactivés et la génération automatique de règles est activée.

Par défaut, le mode FIPS est désactivé.

Par défaut, le niveau de journal est le niveau d'urgence.

Par exemple :



5 Sélectionnez la taille de l'instance de NSX Edge en fonction de vos ressources système.

La taille **Grande (Large)** de NSX Edge dispose d'une ressource de CPU plus puissante, d'une plus grande capacité mémoire et d'un plus grand espace disque que la taille **Compacte (Compact)** de NSX Edge, et elle prend en charge un plus grand nombre d'utilisateurs VPN-Plus SSL simultanés. La taille **Extra grande (X-Large)** de NSX Edge convient aux environnements bénéficiant de l'équilibrage de charge gérant des millions de sessions simultanées. La taille Super grande de NSX Edge est recommandée pour un débit élevé et nécessite une vitesse de connexion élevée.

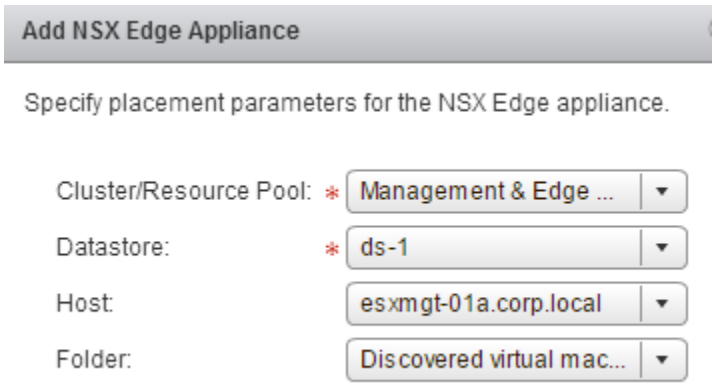
Reportez-vous à la section Configuration système requise pour NSX.

6 Créez un dispositif Edge.

Entrez les paramètres du dispositif virtuel de la passerelle ESG qui sera ajoutée à votre inventaire vCenter. Si vous n'ajoutez pas de dispositif lors de l'installation de NSX Edge, NSX Edge reste en mode hors ligne jusqu'à ce que vous ajoutiez un dispositif.

Si vous avez activé HA, vous pouvez ajouter deux dispositifs. Si vous ajoutez un dispositif unique, NSX Edge réplique sa configuration pour le dispositif en veille et fait en sorte que les deux machines virtuelles NSX Edge HA ne se trouvent pas sur le même hôte ESX, même après avoir utilisé DRS et vMotion (sauf si vous les migrez manuellement à l'aide de vMotion vers le même hôte). Pour que HA fonctionne correctement, vous devez déployer les deux dispositifs sur une banque de données partagée.

Par exemple :



7 Sélectionnez **Déployer le dispositif NSX Edge (Deploy NSX Edge)** pour ajouter le dispositif Edge en mode déployé. Vous devez configurer des dispositifs et des interfaces pour le dispositif Edge avant qu'il puisse être déployé.

8 Configurez des interfaces.

Sur les passerelles ESG (Edge Services Gateway), les adresses IPv4 et IPv6 sont prises en charge.

Pour que HA fonctionne, vous devez ajouter au moins une interface interne.

Une interface peut avoir plusieurs sous-réseaux qui ne se chevauchent pas.

Si vous entrez plusieurs adresses IP pour une interface, vous pouvez sélectionner l'adresse IP principale. Une interface peut être dotée d'une adresse IP principale et de plusieurs adresses IP secondaires. NSX Edge considère l'adresse IP principale comme l'adresse source du trafic généré localement, par exemple les pings du serveur syslog distant et ceux initiés par l'opérateur.

Vous devez ajouter une adresse IP à une interface avant de l'utiliser sur une configuration des fonctionnalités.

Sinon, vous pouvez entrer l'adresse MAC de l'interface (facultatif).

Si vous modifiez l'adresse MAC à l'aide d'un appel API ultérieurement, vous devez redéployer le dispositif Edge après la modification de l'adresse MAC.

Si HA est activée, vous pouvez entrer deux adresses IP de gestion au format CIDR (facultatif). Les pulsations des deux machines virtuelles NSX Edge HA sont communiquées via ces adresses IP de gestion. Les adresses IP de gestion doivent se trouver dans le même sous-réseau L2 et doivent pouvoir communiquer entre elles.

Vous pouvez également modifier le MTU (facultatif).

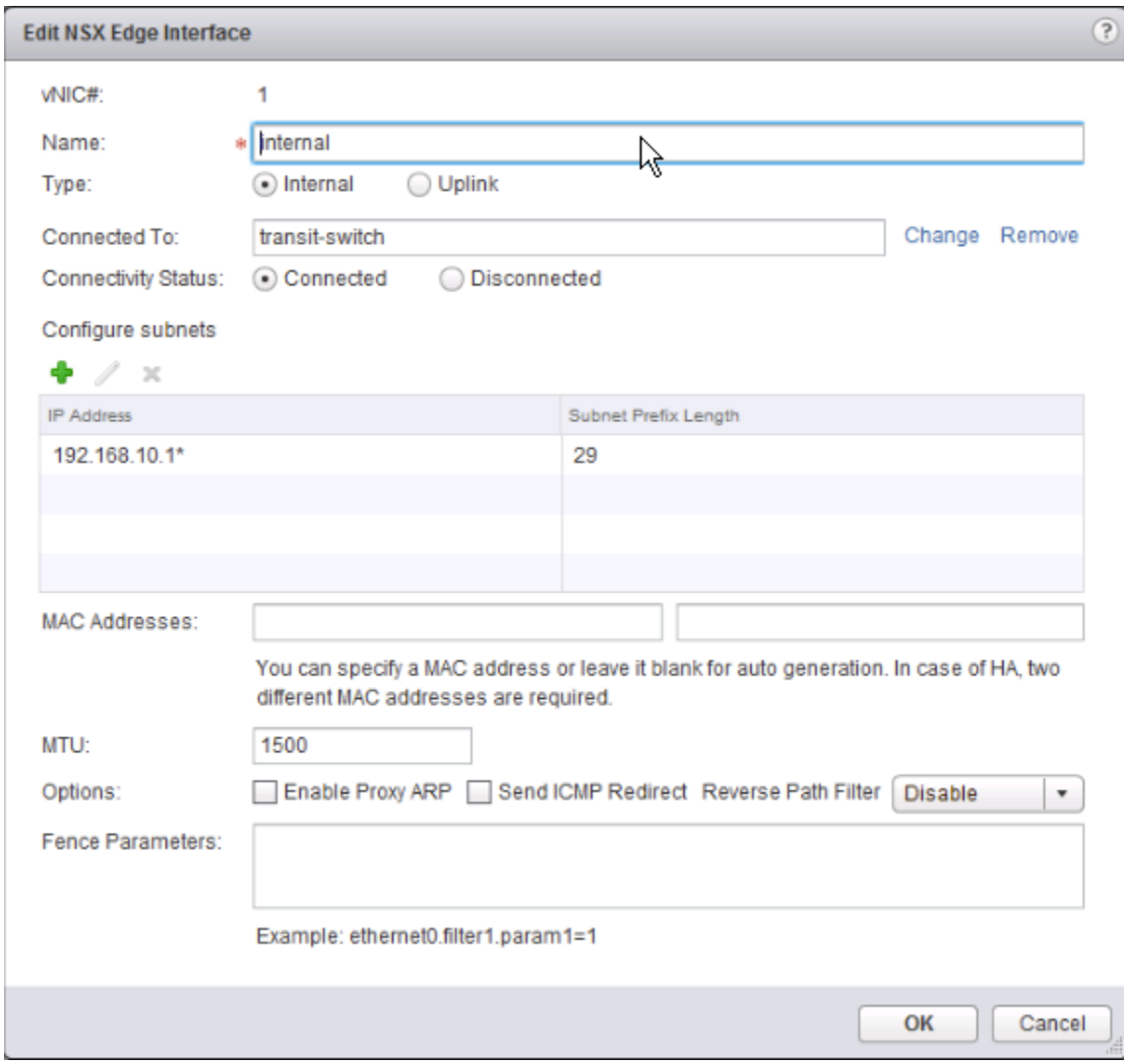
Activez l'ARP de proxy si vous souhaitez autoriser la passerelle ESG à répondre aux demandes ARP destinées aux autres machines. C'est utile notamment lorsque vous disposez du même sous-réseau de part et d'autre d'une connexion WAN.

Activez la redirection ICMP pour acheminer les informations de routage aux hôtes.

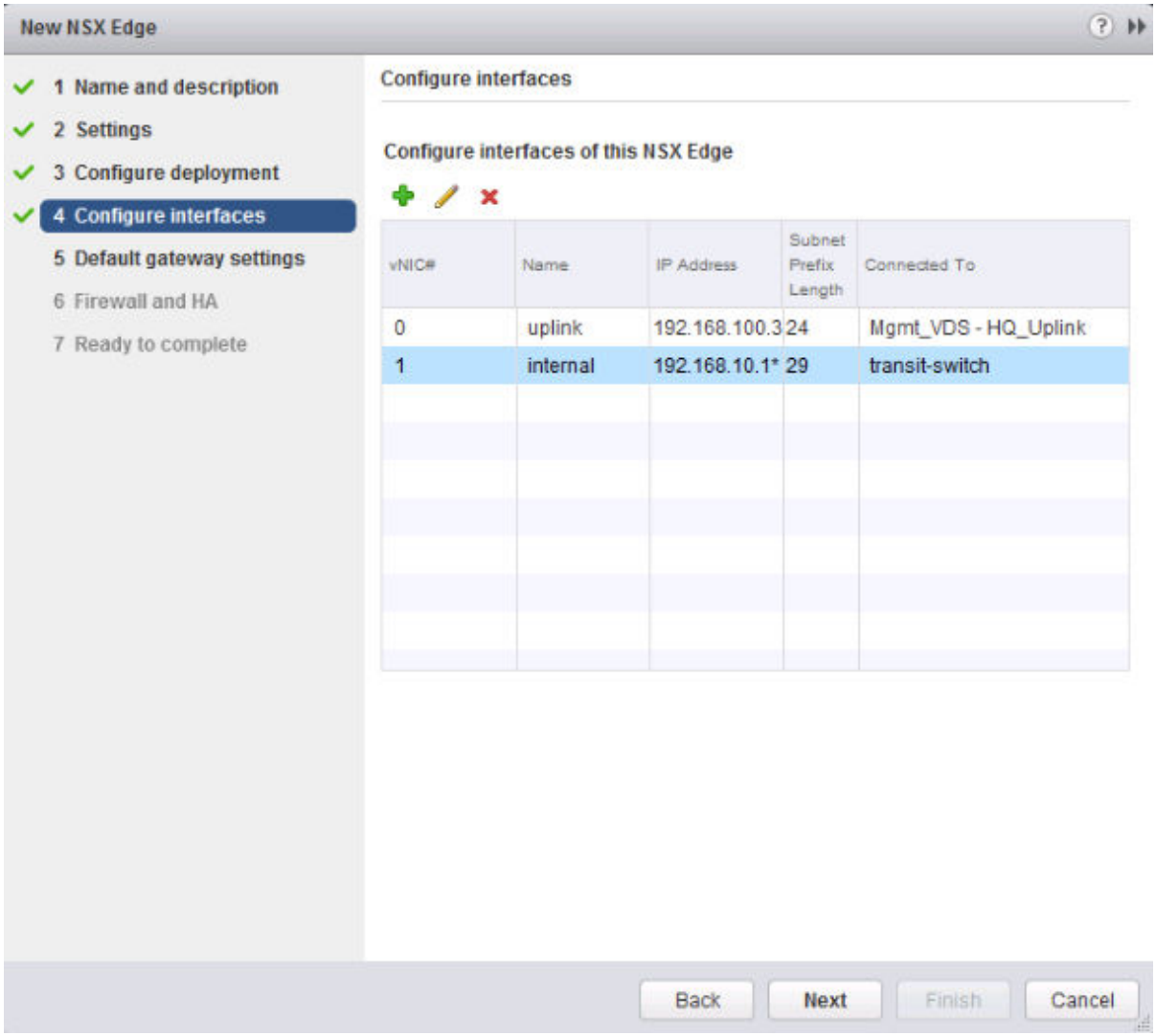
Activez le filtrage inversé des chemins pour vérifier l'accessibilité de l'adresse source dans les paquets transférés. En mode activé, le paquet doit être reçu sur l'interface que le routeur utiliserait pour transférer le paquet de retour. En mode Loose, l'adresse source doit apparaître sur la table de routage.

Configurez des paramètres de délimitation si vous souhaitez réutiliser des adresses IP et MAC dans différents environnements délimités. Par exemple, sur une plate-forme de gestion de Cloud (CMP), la délimitation vous permet d'exécuter plusieurs instances de Cloud simultanément avec les mêmes adresses IP et MAC entièrement isolées ou « délimitées ».

Par exemple :



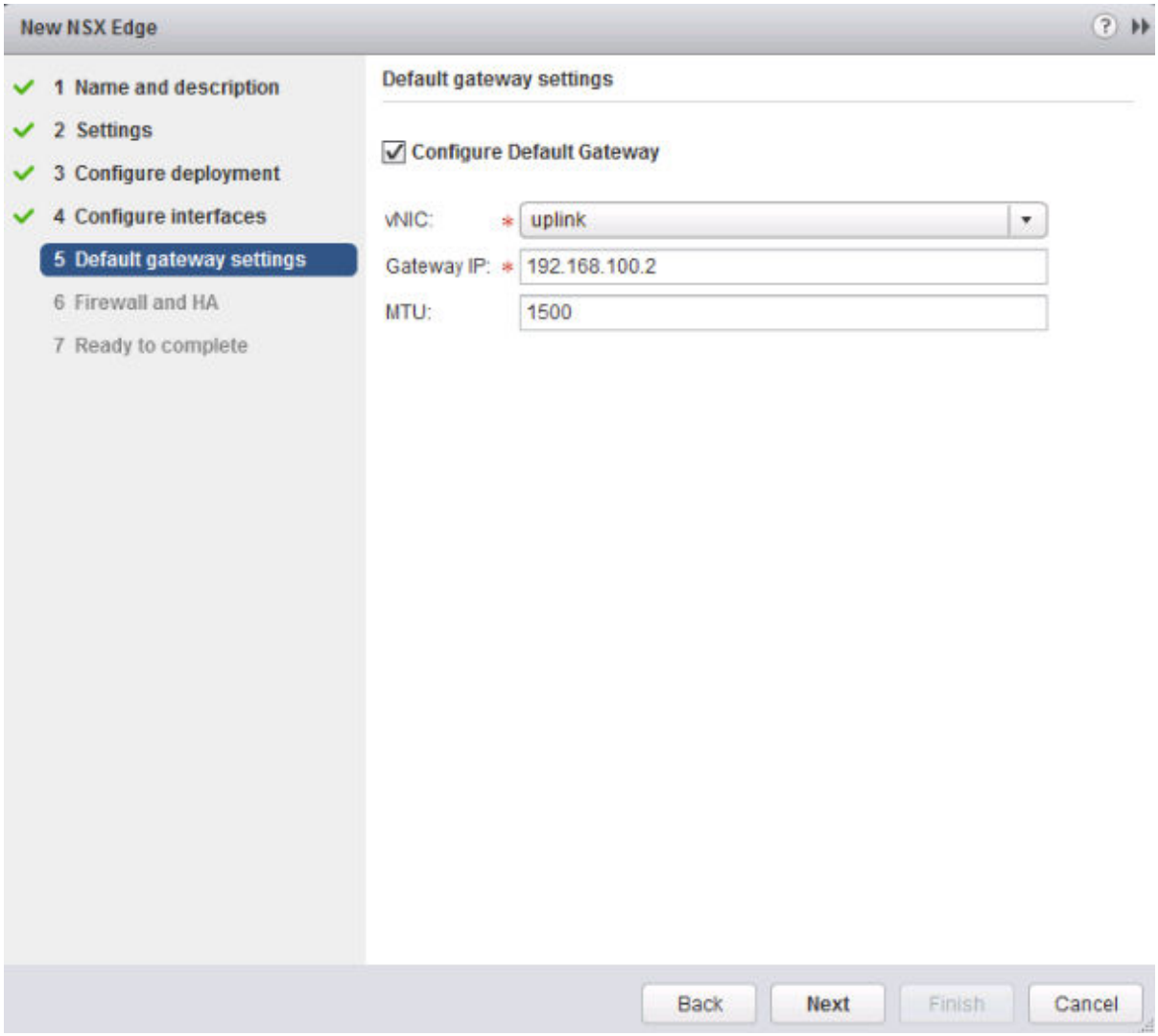
L'exemple suivant présente deux interfaces, l'une associant la passerelle ESG au monde extérieur par l'intermédiaire d'un groupe de ports de liaison montante sur un vSphere Distributed Switch et l'autre associant la passerelle ESG à un commutateur de transit logique auquel un routeur logique distribué est également associé.



9 Configurez une passerelle par défaut.

Vous pouvez modifier la valeur MTU, mais elle ne peut pas être supérieure à la valeur MTU configurée sur l'interface.

Par exemple :



10 Configurez tous les paramètres de stratégie de pare-feu, de journalisation et HA.

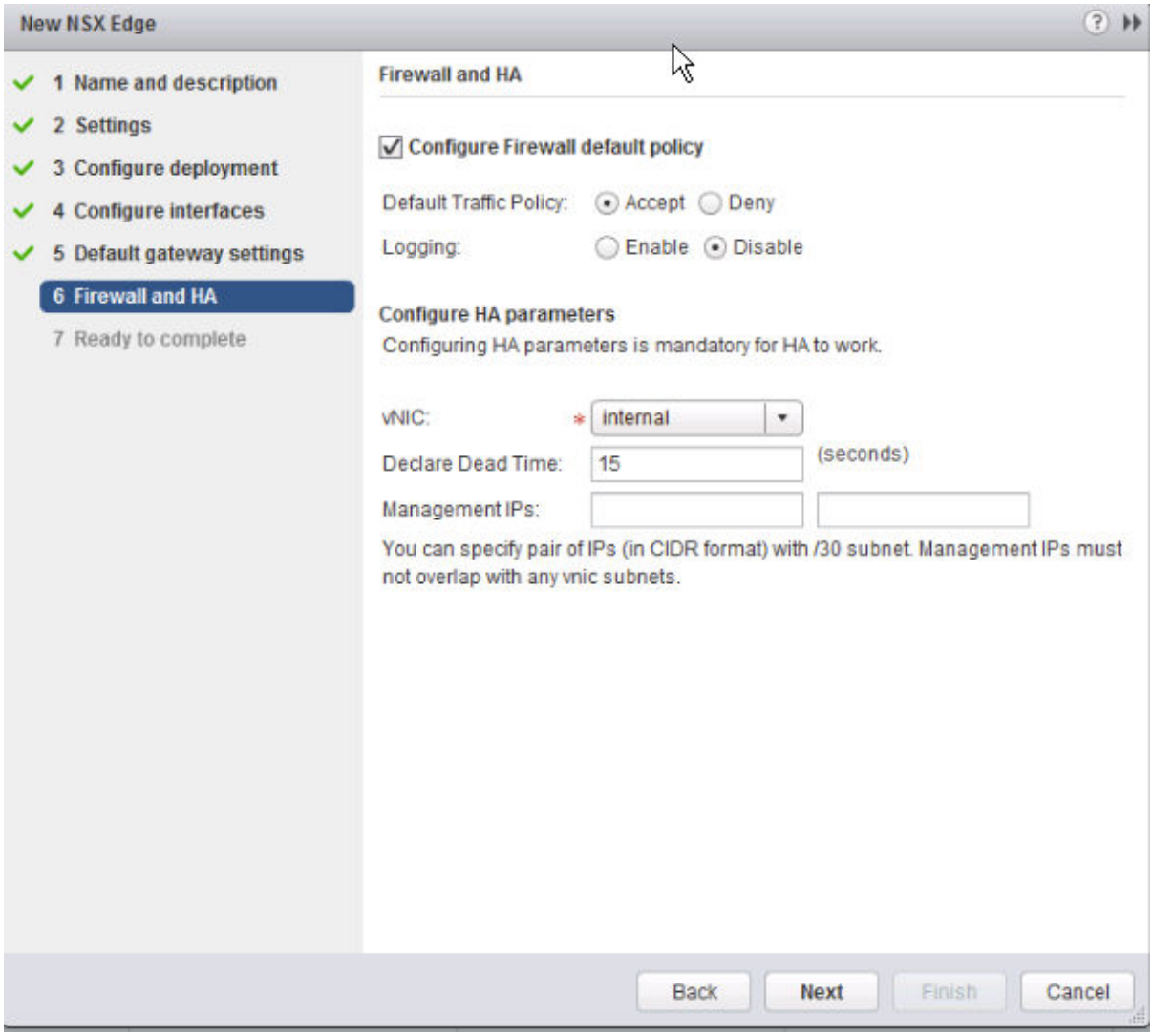
Attention Si vous ne configurez pas la stratégie de pare-feu, la stratégie par défaut est définie pour refuser l'ensemble du trafic.

Par défaut, les journaux sont activés sur tous les nouveaux dispositifs NSX Edge. Le niveau de journalisation par défaut est REMARQUE. Si des journaux sont stockés localement sur la passerelle ESG, la journalisation peut générer un volume trop important de journaux, ce qui a une incidence sur les performances de votre dispositif NSX Edge. Pour cette raison, il vous est recommandé de configurer des serveurs Syslog distants et de transférer tous les journaux à un collecteur centralisé à des fins d'analyse et de surveillance.

Si vous avez activé la haute disponibilité, renseignez la section HA. Par défaut, HA choisit automatiquement une interface interne et attribue automatiquement des adresses IP de liens locaux. NSX Edge prend en charge deux machines virtuelles pour la haute disponibilité, toutes deux étant actualisées avec les configurations utilisateur. En cas d'échec des pulsations sur la machine virtuelle principale, l'état de la machine virtuelle secondaire devient actif. Ainsi, une machine virtuelle NSX

Edge est en permanence active sur le réseau. NSX Edge réplique la configuration du dispositif principal pour le dispositif en veille et s'assure que deux machines virtuelles NSX Edge HA ne se trouvent pas sur le même hôte ESX, même après avoir utilisé DRS et vMotion. Deux machines virtuelles sont déployées sur vCenter dans le même pool de ressources et la même banque de données que le dispositif que vous avez configuré. Des adresses IP de liens locaux sont attribuées aux machines virtuelles HA dans NSX Edge HA pour que ces dernières puissent communiquer ensemble. Sélectionnez l'interface interne dont les paramètres HA doivent être configurés. Si vous sélectionnez TOUTES pour l'interface, mais qu'aucune interface interne n'est configurée, l'interface utilisateur affiche une erreur. Deux dispositifs Edge sont créés, mais du fait qu'aucune interface interne n'est configurée, le nouveau dispositif Edge reste en veille et HA est désactivée. Une fois qu'une interface interne est configurée, HA est activée sur le dispositif Edge. Tapez la période, exprimée en secondes, au cours de laquelle si le dispositif de sauvegarde ne reçoit pas de signal de pulsation du dispositif principal, ce dernier est considéré comme étant inactif et le dispositif de sauvegarde prend le relais. L'intervalle par défaut est de 15 secondes. Tapez deux adresses IP de gestion au format CIDR pour remplacer les adresses IP de liens locaux attribuées aux machines virtuelles HA. Assurez-vous que les adresses IP de gestion ne se chevauchent pas avec les adresses IP utilisées pour toute autre interface et n'interfèrent pas avec le routage du trafic. Vous ne devez pas utiliser l'une des adresses IP de votre réseau, même si ce réseau n'est pas directement rattaché au dispositif NSX Edge.

Par exemple :



Résultats

Une fois la passerelle ESG déployée, accédez à la vue Hôtes et clusters et ouvrez la console du dispositif virtuel Edge. Dans la console, assurez-vous de pouvoir exécuter une commande ping sur les interfaces connectées.

Étape suivante

Lorsque vous installez un dispositif NSX Edge, NSX permet le démarrage/arrêt automatique des VM sur l'hôte si vSphere HA est désactivé sur le cluster. Si les VM du dispositif sont par la suite migrées vers d'autres hôtes du cluster, le mécanisme de démarrage/arrêt automatique des VM peut ne pas être activé sur ces nouveaux hôtes. C'est la raison pour laquelle VMware vous recommande, lorsque vous installez des dispositifs NSX Edge sur des clusters où vSphere HA est désactivé, de vérifier tous les hôtes du cluster pour vous assurer que le démarrage/arrêt automatique des machines virtuelles est activé. Dans *Administration d'une machine virtuelle vSphere*, consultez la section « Modifier les paramètres de démarrage et d'arrêt d'une machine virtuelle ».

Vous pouvez à présent configurer le routage afin d'autoriser la connectivité entre des périphériques externes et vos machines virtuelles.

Configurer le protocole OSPF sur un routeur logique (distribué) universel

19

La configuration d'un protocole OSPF sur un routeur logique permet d'activer la connectivité d'une machine virtuelle entre les routeurs logiques ainsi qu'entre les routeurs logiques et les passerelles ESG (Edge Services Gateway).

Les stratégies de routage OSPF mettent en œuvre un processus dynamique d'équilibrage de charge du trafic entre des itinéraires à coût égal.

Un réseau OSPF est divisé en zones de routage afin d'optimiser le flux de trafic et de limiter la taille des tables de routage. Une zone est une collection logique de réseaux, de routeurs et de liaisons OSPF qui disposent tous de la même identification de zone.

Les zones sont identifiées par un ID de zone.

Conditions préalables

L'ID du routeur doit être configuré comme décrit dans Protocole OSPF configuré sur le routeur (distribué) logique.

Lorsque vous activez un ID de routeur, le champ est renseigné par défaut avec l'interface de liaison montante du routeur logique.

Procédure

1. Connectez-vous à vSphere Web Client.
2. Cliquez sur **Mise en réseau et sécurité (Networking & Security)**, puis sur **Dispositifs NSX Edge (NSX Edges)**.
3. Double-cliquez sur un routeur logique.
4. Cliquez sur **Routage (Routing)**, puis sur **OSPF**.

5 Activez OSPF.

a Cliquez sur **Modifier (Edit)** dans le coin supérieur droit de la fenêtre, puis sur **Activer OSPF (Enable OSPF)**

b Dans **Adresse de transfert (Forwarding Address)**, tapez une adresse IP devant être utilisée par le module du chemin d'accès aux données du routeur dans les hôtes afin de transférer des paquets de chemins d'accès aux données.

c Dans **Adresse de protocole (Protocol Address)**, tapez une adresse IP unique au sein du même sous-réseau que l'**Adresse de transfert (Forwarding Address)**. L'adresse du protocole est utilisée par le protocole pour former des combinaisons avec ses homologues.

6 Configurez les zones OSPF.

a Sinon, supprimez la zone 51 NSSA (not-so-stubby area) configurée par défaut.///

b Dans **Définitions de zone (Area Definitions)**, cliquez sur l'icône **Ajouter (Add)**.

c Entrez un ID de zone. NSX Edge prend en charge un ID de zone sous la forme d'un nombre décimal. Les valeurs valides sont comprises entre 0 et 4294967295.

d Dans **Type**, sélectionnez **Normal** ou **NSSA**.

Les NSSA empêchent la saturation des annonces d'états de liens externes à l'AS (LSA) dans les NSSA. Elles reposent sur du routage par défaut vers des destinations externes. En conséquence, les NSSA doivent être placées en périphérie d'un domaine de routage OSPF. Une NSSA peut importer des itinéraires externes dans le domaine de routage OSPF, ce qui leur permet de fournir un service de transit à de petits domaines de routage ne faisant pas partie du domaine de routage OSPF.

7 (Facultatif) Sélectionnez le type d'**authentification (Authentication)**. OSPF effectue une authentification au niveau de la zone.

Tous les routeurs de la zone doivent avoir la même authentification et le mot de passe correspondant configuré. Pour garantir le fonctionnement de l'authentification MD5, les routeurs de réception et de transmission doivent avoir la même clé MD5.

a **Aucune (None)** : aucune authentification n'est requise (valeur par défaut).

b **Mot de passe (Password)** : dans cette méthode d'authentification, un mot de passe est inclus dans le paquet transmis.

c **MD5** : Cette méthode d'authentification utilise le chiffrement MD5 (Message Digest type 5). Un total de contrôle MD5 est inclus dans le paquet transmis.

d Dans **Mot de passe (Password)** ou le type d'authentification**MD5**, tapez le mot de passe ou la clé MD5.

Important

- Si NSX Edge est configuré pour la haute disponibilité avec le redémarrage normal d'OSPF activé et que MD5 est utilisé pour l'authentification, OSPF ne parvient pas à redémarrer normalement. Des contiguïtés sont formées uniquement après l'expiration du délai de grâce sur les nœuds auxiliaires d'OSPF.
- Vous ne pouvez pas configurer l'authentification **MD5** lorsque le mode FIPS est activé.
- NSX for vSphere utilise toujours une valeur d'ID de clé égale à 1. Tout dispositif non géré par NSX for vSphere homologue avec une passerelle Edge Services Gateway ou un routeur logique distribué doit être configuré pour utiliser un ID de clé de valeur 1 lorsque l'authentification MD5 est utilisée. Sinon, une session OSPF ne peut pas être établie.

8 Mappez des interfaces sur les zones.

a Dans **Zone de mappage d'interface (Area to Interface Mapping)**, cliquez sur l'icône **Ajouter (Add)** pour mapper l'interface appartenant sur la zone OSPF.

b Sélectionnez l'interface que vous souhaitez mapper et la zone OSPF sur laquelle vous souhaitez la mapper.

9 (Facultatif) Au besoin, vous pouvez modifier les paramètres OSPF par défaut.

Dans la plupart des cas, il est recommandé de conserver les paramètres OSPF par défaut. Si vous modifiez les paramètres, assurez-vous que les homologues OSPF ont les mêmes paramètres.

a **Intervalle de salutation (Hello Interval)** affiche l'intervalle par défaut entre les paquets de salutation qui sont envoyés sur l'interface.

b **Intervalle d'inactivité (Dead Interval)** affiche l'intervalle par défaut pendant lequel au moins un paquet de salutation doit être reçu d'un voisin avant que le routeur ne déclare ce voisin inactif.

c **Priorité (Priority)** affiche la priorité par défaut de l'interface. L'interface disposant de la priorité la plus élevée est le routeur désigné.

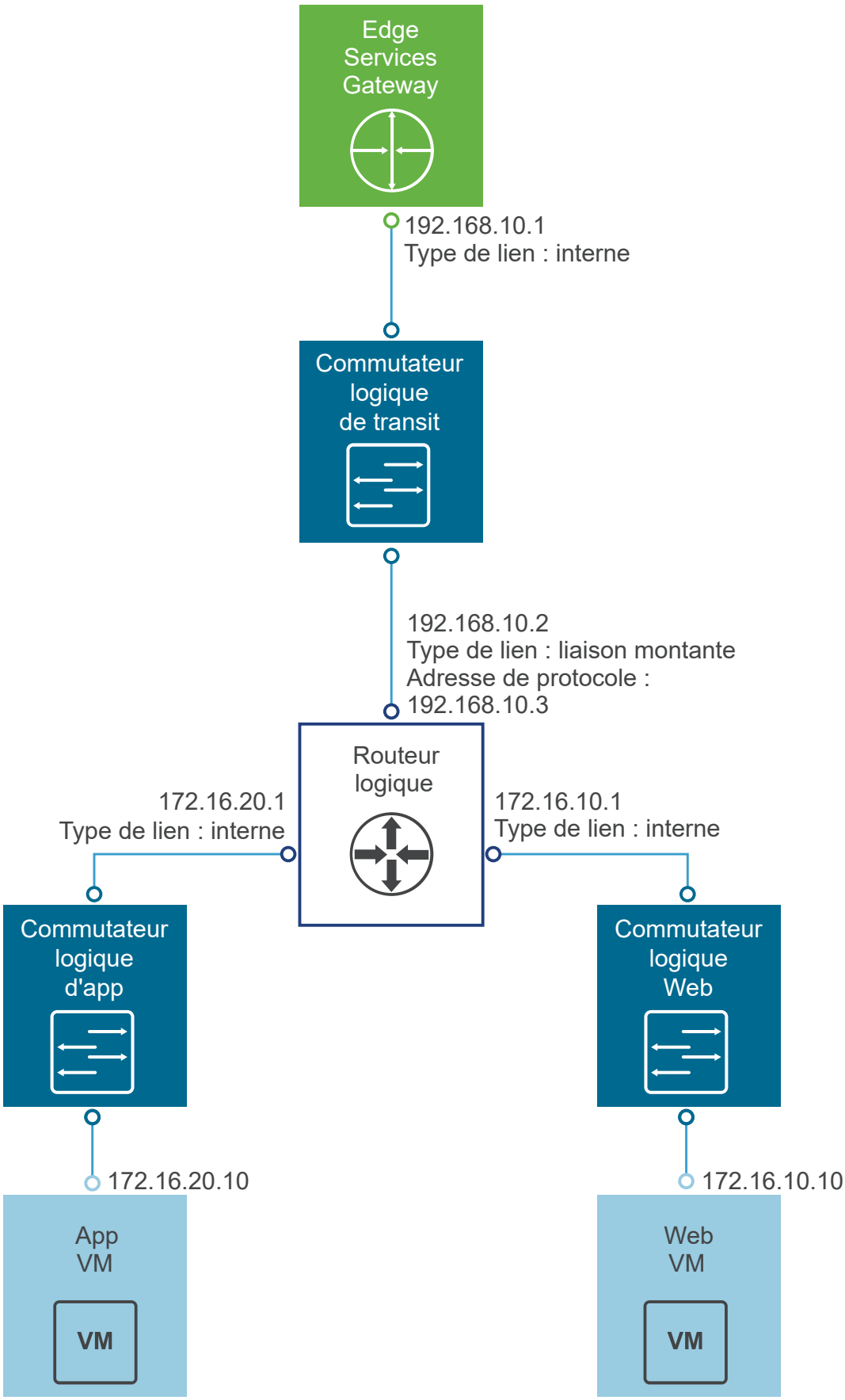
d **Coût (Cost)** d'une interface affiche la charge supplémentaire par défaut requise pour envoyer des paquets sur cette interface. Le coût d'une interface est inversement proportionnel à la bande passante de cette interface. Plus la bande passante est grande, moins le coût est élevé.

10 Cliquez sur **Publier les modifications (Publish Changes)**.

Exemple : Protocole OSPF configuré sur le routeur (distribué) logique

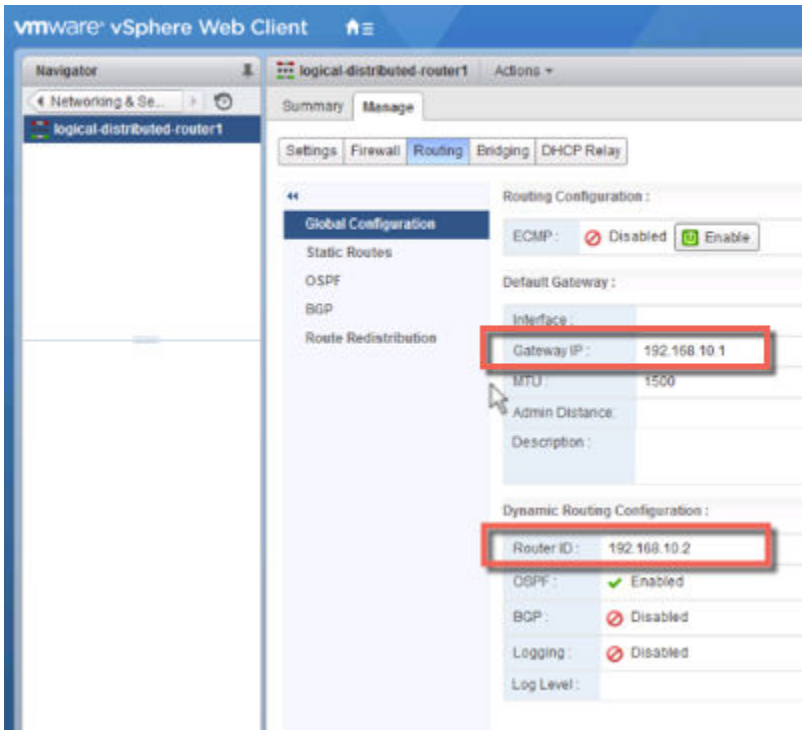
L'illustration suivante présente un scénario NSX for vSphere simple utilisant OSPF dans lequel un routeur logique (DLR) et une passerelle ESG (Edge Services Gateway) sont voisins de protocole OSPF.

Figure 19-1. Topologie NSX for vSphere

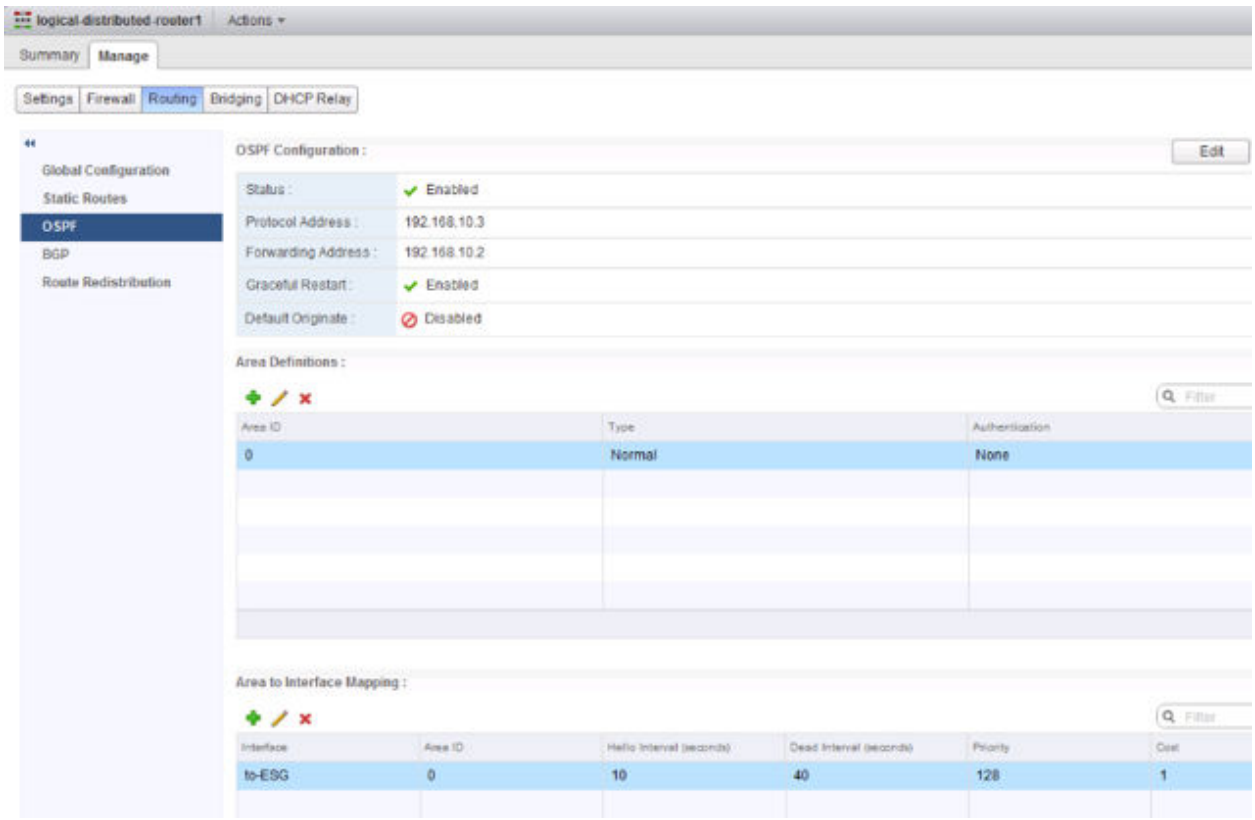


Sur l'écran suivant, la passerelle par défaut du routeur logique est l'adresse IP de l'interface interne de l'ESG (192.168.10.1).

L'ID du routeur est l'interface de liaison montante du routeur logique, c'est-à-dire l'adresse IP soumise à l'ESG (192.168.10.2).



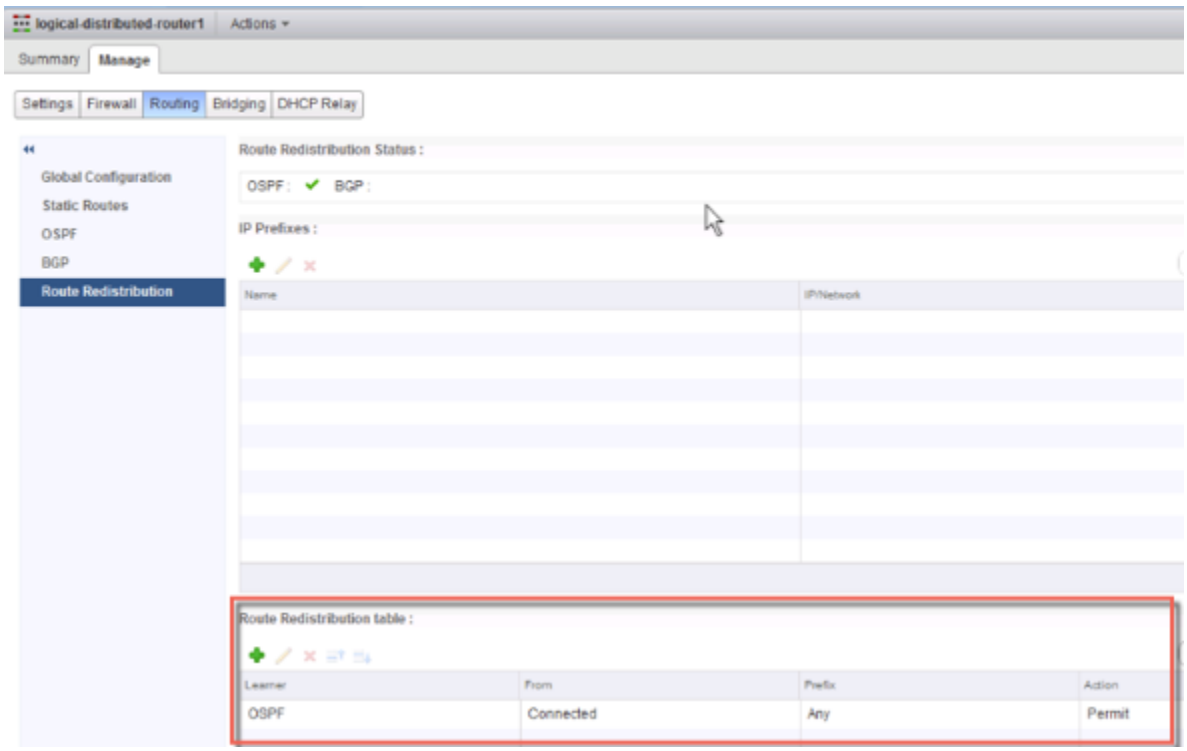
La configuration du routeur logique utilise 192.168.10.2 comme adresse de transfert. L'adresse de protocole peut être n'importe quelle adresse IP se trouvant sur le même sous-réseau et qui n'est utilisée nulle part ailleurs. Dans le cas présent, 192.168.10.3 est configuré. L'ID de zone configuré est 0 et l'interface de liaison montante (l'interface soumise à l'ESG) est mappée sur la zone.



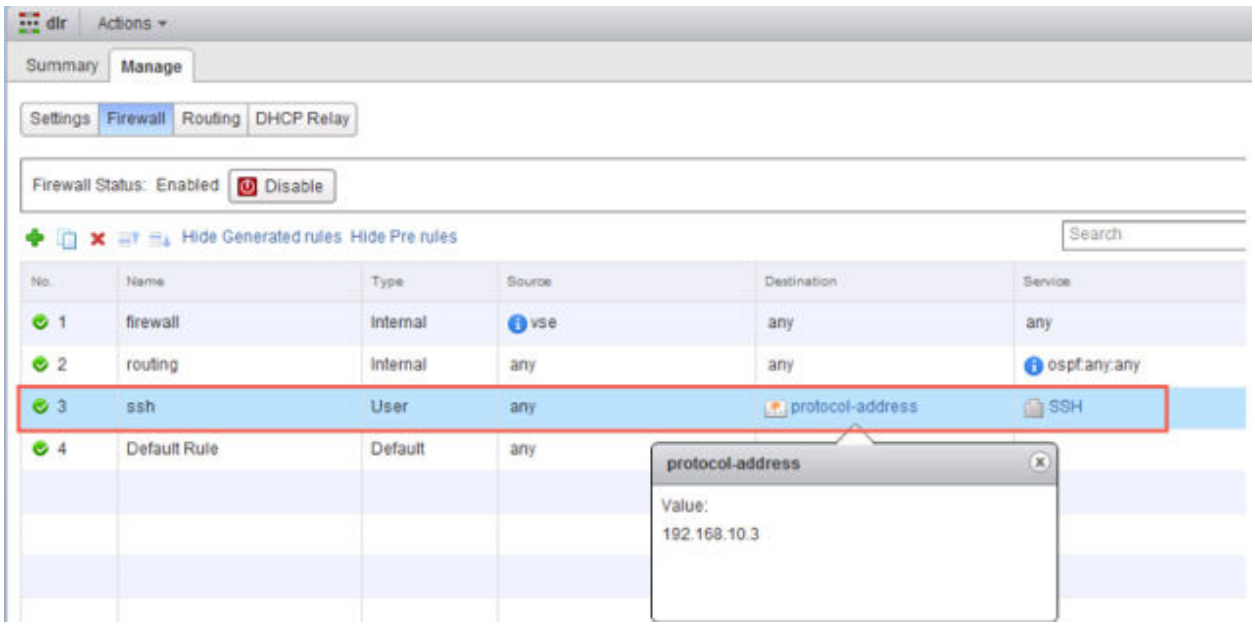
Étape suivante

Vérifiez que la redistribution d'itinéraire et la configuration du pare-feu permettent l'annonce d'itinéraires corrects.

Dans cet exemple, les itinéraires connectés du routeur logique (172.16.10.0/24 et 172.16.20.0/24) sont annoncés dans OSPF.



Si vous avez activé SSH quand vous avez créé le routeur logique, vous devez également configurer un filtre de pare-feu autorisant l'accès SSH à l'adresse du protocole du routeur logique. Par exemple :



Configurer un protocole OSPF sur une passerelle Edge Services Gateway

20

La configuration d'un protocole OSPF sur une passerelle ESG (Edge Services Gateway) active l'apprentissage et l'annonce d'itinéraires dans la passerelle ESG. L'application la plus courante du protocole OSPF sur une passerelle ESG se situe sur le lien entre la passerelle ESG et un routeur (distribué) logique. Cela permet à la passerelle ESG d'enregistrer des informations sur les interfaces logiques (LIF) connectées au routeur logique. Cet objectif peut être atteint avec les protocoles OSPF, IS-IS, BGP ou un routage statique.

Les stratégies de routage OSPF mettent en œuvre un processus dynamique d'équilibrage de charge du trafic entre des itinéraires à coût égal.

Un réseau OSPF est divisé en zones de routage afin d'optimiser le flux de trafic et de limiter la taille des tables de routage. Une zone est une collection logique de réseaux, de routeurs et de liaisons OSPF qui disposent tous de la même identification de zone.

Les zones sont identifiées par un ID de zone.

Conditions préalables

L'ID du routeur doit être configuré comme décrit dans Protocole OSPF configuré sur la passerelle Edge Services Gateway.

Lorsque vous activez un ID de routeur, le champ est renseigné par défaut avec l'adresse IP de l'interface de liaison montante de la passerelle ESG.

Procédure

1. Connectez-vous à vSphere Web Client.
2. Cliquez sur **Mise en réseau et sécurité (Networking & Security)**, puis sur **Dispositifs NSX Edge (NSX Edges)**.
3. Double-cliquez sur une passerelle ESG.
4. Cliquez sur **Routage (Routing)**, puis sur **OSPF**.

5 Activez OSPF.

   a Cliquez sur **Modifier (Edit)** dans le coin supérieur droit de la fenêtre, puis sur **Activer OSPF (Enable OSPF)**

   b (Facultatif) Cliquez sur **Activer le redémarrage normal (Enable Graceful Restart)** pour que le transfert de paquets soit ininterrompu pendant le redémarrage des services OSPF.

   c (Facultatif) Cliquez sur **Activer la provenance par défaut (Enable Default Originate)** pour autoriser la passerelle ESG à s'annoncer en tant que passerelle par défaut à ses homologues.

6 Configurez les zones OSPF.

   a (Facultatif) Supprimez la zone 51 NSSA (not-so-stubby area) configurée par défaut.///

   b Dans **Définitions de zone (Area Definitions)**, cliquez sur l'icône **Ajouter (Add)**.

   c Tapez un ID de zone. NSX Edge prend en charge un ID de zone sous la forme d'une adresse IP ou d'un nombre décimal.

   d Dans **Type**, sélectionnez **Normal** ou **NSSA**.

      Les NSSA empêchent la saturation des annonces d'états de liens externes à l'AS (LSA) dans les NSSA. Elles reposent sur du routage par défaut vers des destinations externes. En conséquence, les NSSA doivent être placées en périphérie d'un domaine de routage OSPF. Une NSSA peut importer des itinéraires externes dans le domaine de routage OSPF, ce qui leur permet de fournir un service de transit à de petits domaines de routage ne faisant pas partie du domaine de routage OSPF.

7 (Facultatif) Si vous sélectionnez le type **NSSA**, le champ **Rôle Traducteur NSSA (NSSA Translator Role)** s'affiche. Cochez la case **Toujours (Always)** pour traduire des LSA de type 7 en LSA de type 5. Tous les LSA de type 7 sont traduits en LSA de type 5 par la NSSA.

8 (Facultatif) Sélectionnez le type d'**authentification (Authentication)**. OSPF effectue une authentification au niveau de la zone.

   Tous les routeurs de la zone doivent avoir la même authentification et le mot de passe correspondant configuré. Pour garantir le fonctionnement de l'authentification MD5, les routeurs de réception et de transmission doivent avoir la même clé MD5.

   a **Aucune (None)** : aucune authentification n'est requise (valeur par défaut).

   b **Mot de passe (Password)** : dans cette méthode d'authentification, un mot de passe est inclus dans le paquet transmis.

c **MD5** : Cette méthode d'authentification utilise le chiffrement MD5 (Message Digest type 5). Un total de contrôle MD5 est inclus dans le paquet transmis.

d Dans **Mot de passe (Password)** ou le type d'authentification**MD5**, tapez le mot de passe ou la clé MD5.

Note

- Vous ne pouvez pas configurer l'authentification **MD5** lorsque le mode FIPS est activé.
- NSX utilise toujours une valeur d'ID de clé égale à 1. Tous les périphériques non-NSX qui se lient à un dispositif NSX Edge ou à un routeur distribué logique doivent être configurés pour utiliser une valeur de clé de 1 pour l'authentification MD5, sinon il sera impossible d'établir une session OSPF.

9 Mappez des interfaces sur les zones.

a Dans **Zone de mappage d'interface (Area to Interface Mapping)**, cliquez sur l'icône **Ajouter (Add)** pour mapper l'interface appartenant sur la zone OSPF.

b Sélectionnez l'interface que vous souhaitez mapper et la zone OSPF sur laquelle vous souhaitez la mapper.

10 (Facultatif) Modifiez les paramètres OSPF par défaut.

Dans la plupart des cas, il est recommandé de conserver les paramètres OSPF par défaut. Si vous modifiez les paramètres, assurez-vous que les homologues OSPF ont les mêmes paramètres.

a **Intervalle de salutation (Hello Interval)** affiche l'intervalle par défaut entre les paquets de salutation qui sont envoyés sur l'interface.

b **Intervalle d'inactivité (Dead Interval)** affiche l'intervalle par défaut pendant lequel au moins un paquet de salutation doit être reçu d'un voisin avant que le routeur ne déclare ce voisin inactif.

c **Priorité (Priority)** affiche la priorité par défaut de l'interface. L'interface disposant de la priorité la plus élevée est le routeur désigné.

d **Coût (Cost)** d'une interface affiche la charge supplémentaire par défaut requise pour envoyer des paquets sur cette interface. Le coût d'une interface est inversement proportionnel à la bande passante de cette interface. Plus la bande passante est grande, moins le coût est élevé.

11 Cliquez sur **Publier les modifications (Publish Changes)**.

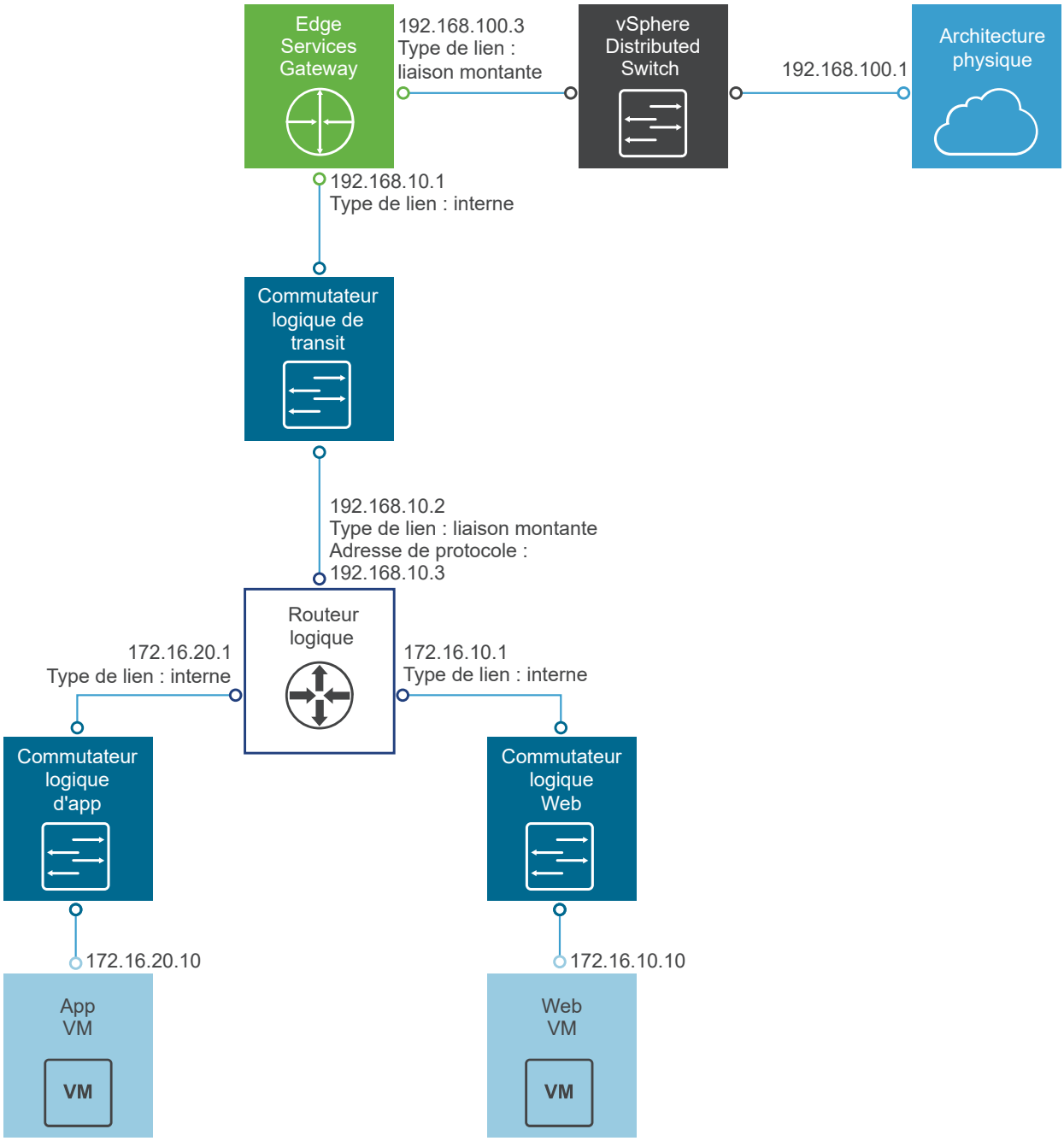
12 Vérifiez que la redistribution d'itinéraire et la configuration du pare-feu permettent l'annonce d'itinéraires corrects.

Exemple : Protocole OSPF configuré sur la passerelle Edge Services Gateway

L'illustration suivante présente un scénario NSX simple utilisant OSPF dans lequel un routeur logique et une passerelle Edge Services Gateway sont voisins OSPF.

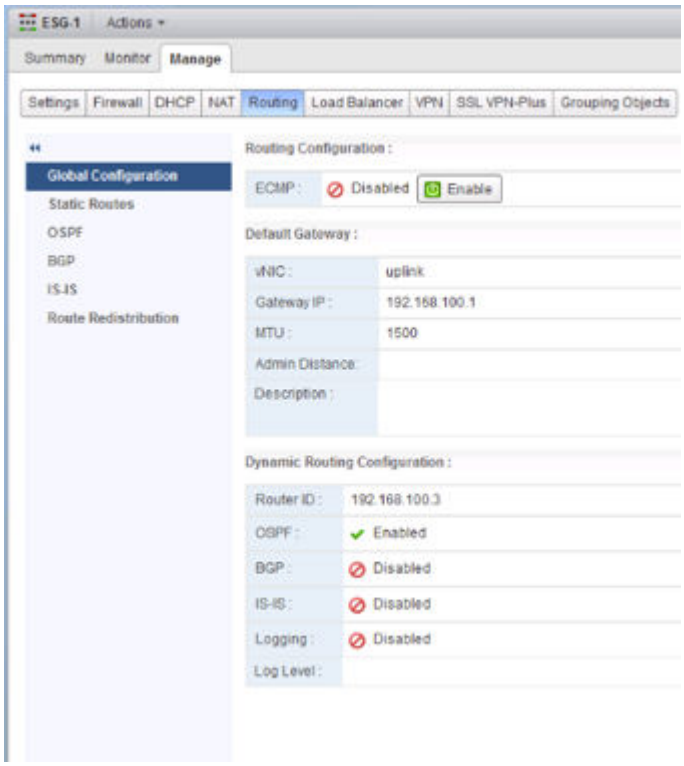
La passerelle ESG peut être connectée au monde extérieur par un pont, un routeur physique (ou comme présenté ici) par l'intermédiaire d'un groupe de ports de liaison montante sur un vSphere Distributed Switch.

Figure 20-1. Topologie NSX

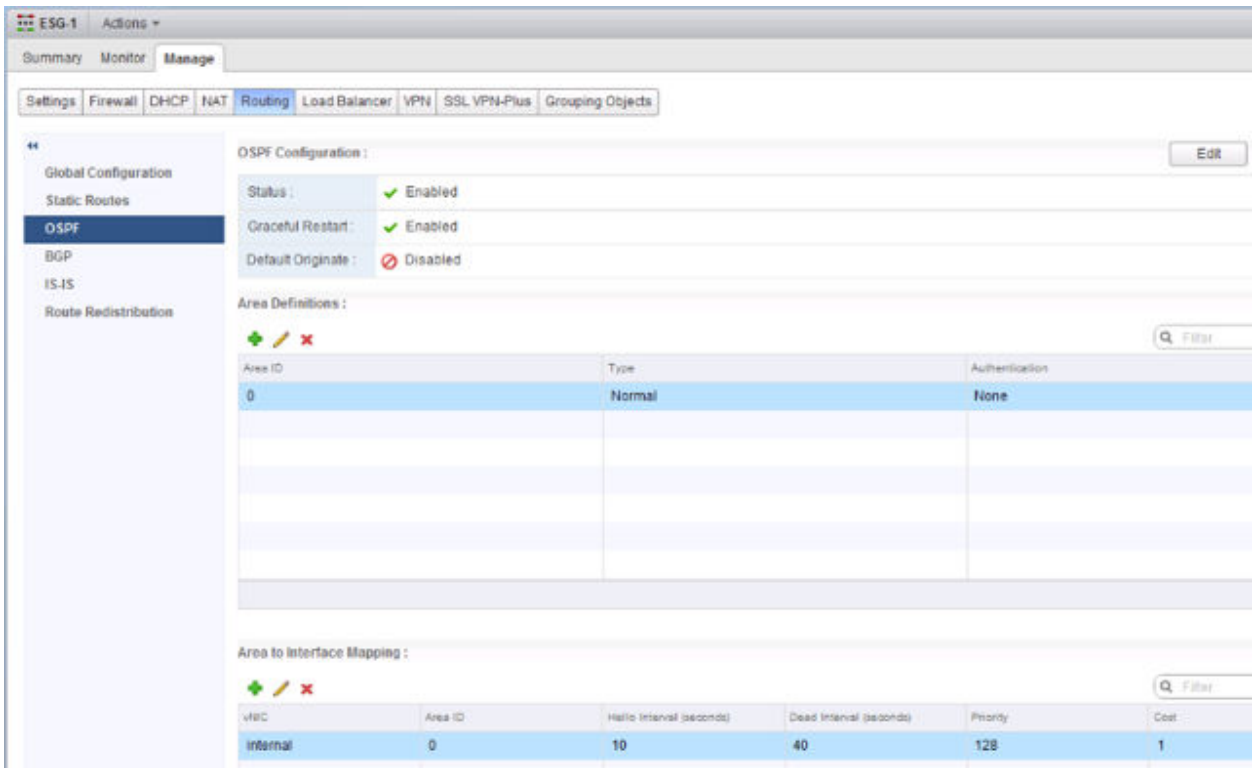


Sur l'écran suivant, la passerelle par défaut de la passerelle ESG est l'interface interne de liaison montante de l'ESG à son homologue externe.

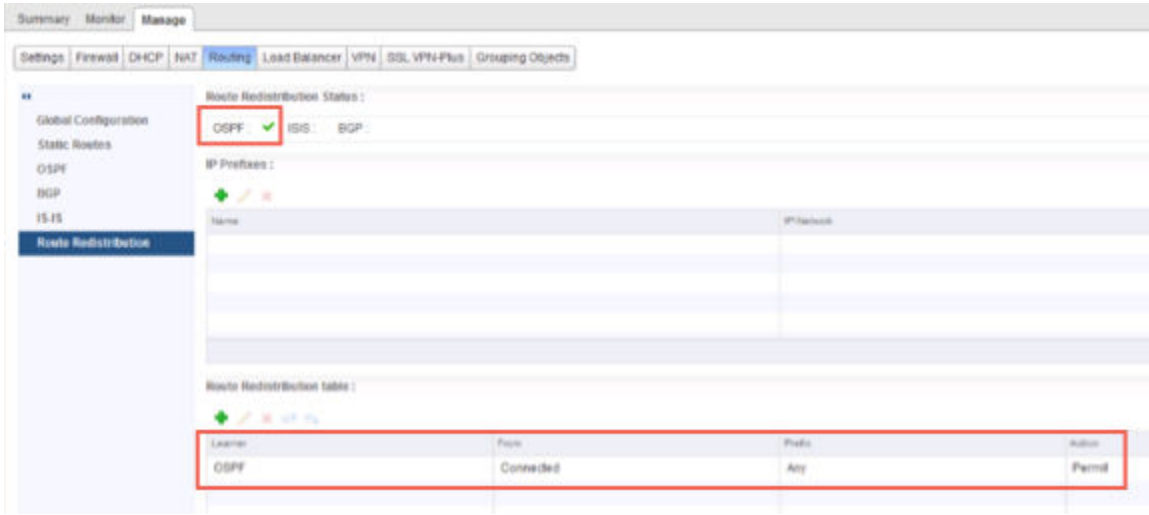
L'ID du routeur est l'adresse IP de l'interface de liaison montante de la passerelle ESG, c'est-à-dire l'adresse IP soumise à son homologue externe.



L'ID de zone configuré est 0 et l'interface interne (l'interface soumise au routeur logique) est mappée sur la zone.

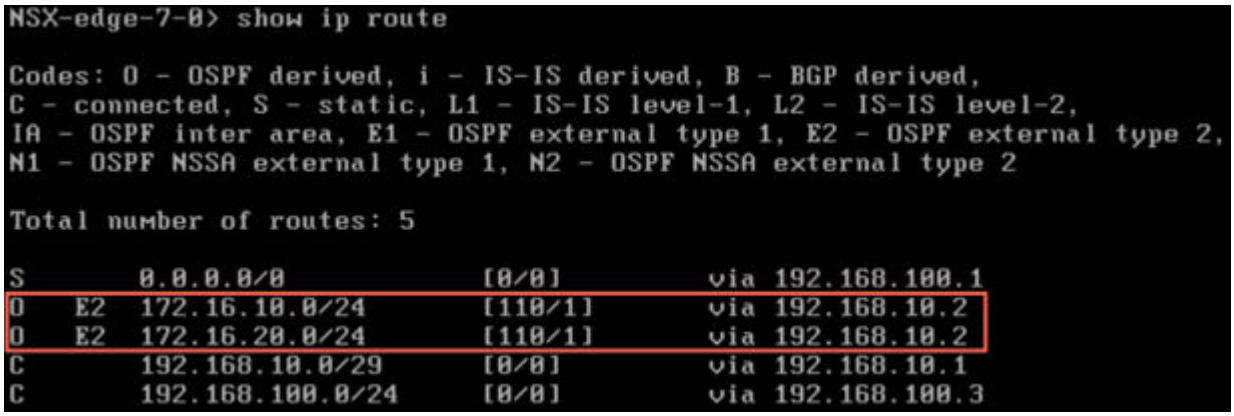


Les itinéraires connectés sont redistribués dans OSPF de sorte le voisin OSPF (le routeur logique) peut en savoir plus sur le réseau de liaison montante de la passerelle ESG.


Summary
Monitor
Manage
Settings
Firewall
DHCP
NAT
Routing
Load Balancer
VPN
SSL VPN-Plus
Grouping Objects
Global Configuration
Static Routes
OSPF
BGP
IS-IS
Route Redistribution
Route Redistribution Status :
OSPF
ISIS
BGP
IP Prefixes :
Route Redistribution table :
OSPF
Connected
Any
Permit

Note De plus, OSPF peut être configuré entre la passerelle ESG et son routeur homologue externe, mais plus généralement, ce lien utilise BGP pour l'annonce d'itinéraire.

Vérifiez que la passerelle ESG apprend les itinéraires externes PSPF auprès du routeur logique.



Pour vérifier la connectivité, assurez-vous qu'un périphérique externe situé dans l'architecture physique peut exécuter une commande ping sur les machines virtuelles.

Par exemple :

```
PS C:\Users\Administrator> ping 172.16.10.10

Pinging 172.16.10.10 with 32 bytes of data:
Reply from 172.16.10.10: bytes=32 time=5ms TTL=61
Reply from 172.16.10.10: bytes=32 time=1ms TTL=61

Ping statistics for 172.16.10.10:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 3ms
```

```
PS C:\Users\Administrator> ping 172.16.20.10

Pinging 172.16.20.10 with 32 bytes of data:
Reply from 172.16.20.10: bytes=32 time=2ms TTL=61
Reply from 172.16.20.10: bytes=32 time=1ms TTL=61

Ping statistics for 172.16.20.10:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Installer Guest introspection sur les clusters d'hôtes

21

L'installation de Guest introspection installe automatique un nouveau VIB et une machine virtuelle de service sur chaque hôte du cluster. Guest introspection est requis pour Activity Monitoring et plusieurs solutions de sécurité de tiers.

Note Vous ne pouvez pas migrer une VM de service (SVM) avec vMotion/SvMotion. Les SVM doivent rester sur l'hôte sur lequel elles ont été déployées pour un fonctionnement correct.

Conditions préalables

Les instructions d'installation qui suivent supposent que vous disposez du système suivant :

- un centre de données avec les versions prises en charge de vCenter Server et ESXi installées sur chaque hôte du cluster.
- Si les hôtes de vos clusters ont été mis à niveau à partir de vCenter Server version 5.0 à 5.5, vous devez ouvrir les ports 80 et 443 sur ces hôtes.
- Les hôtes dans le cluster sur lequel vous voulez installer Guest introspection ont été préparés pour NSX. Consultez Préparer des clusters d'hôtes pour NSX dans le *Guide d'installation de NSX*. Guest introspection ne peut pas être installé sur des hôtes autonomes. Si vous utilisez NSX pour déployer et gérer Guest introspection pour la capacité de déchargement d'antivirus uniquement, vous n'avez pas besoin de préparer les hôtes pour NSX, et la licence NSX for vShield Endpoint ne l'autorise pas.
- NSX Manager doit être installé et en cours d'exécution.
- Assurez-vous que NSX Manager et les hôtes préparés qui exécutent les services Guest Introspection sont reliés au même serveur NTP et que l'heure est synchronisée. Si ce n'est pas le cas, il se peut que les machines virtuelles ne soient pas protégées par des services antivirus, même si l'état du cluster est vert pour Guest introspection et tout service tiers.

  Si vous ajoutez un serveur NTP, VMware recommande que vous redéployiez Guest introspection et tout service tiers.

Si vous souhaitez attribuer une adresse IP à la machine virtuelle de service NSX Guest introspection à partir d'un pool d'adresses IP, créez le pool d'adresses IP avant d'installer NSX Guest introspection. Consultez la section Utilisation des pools d'adresses IP dans le *Guide d'administration de NSX*.

Attention Guest introspection utilise le sous-réseau 169.254.x.x pour attribuer des adresses IP en interne au service GI. Si vous attribuez l'adresse IP 169.254.1.1 à une interface VMkernel d'un hôte ESXi, l'installation de Guest introspection échouera. Le service GI utilise cette adresse IP pour la communication interne.

vSphere Fault Tolerance ne fonctionne pas avec Guest introspection.

Procédure

1. Dans l'onglet **Installation**, cliquez sur **Déploiements de services (Service Deployments)**.
2. Cliquez sur l'icône **Nouveau déploiement de services (New Service Deployment)** ( ).
3. Dans la boîte de dialogue Déployer les services Réseau et sécurité, sélectionnez **Guest Introspection**.
4. Dans **Spécifier la planification (Specify schedule)** (en bas de la boîte de dialogue), sélectionnez **Déployer maintenant (Deploy now)** pour déployer Guest Introspection dès qu'il est installé ou sélectionnez une date et une heure de déploiement.
5. Cliquez sur **Suivant (Next)**.
6. Sélectionnez le centre de données et le ou les clusters dans lesquels vous souhaitez installer Guest Introspection, puis cliquez sur **Suivant (Next)**.
7. Sur la page Sélectionner le réseau de stockage et de gestion, sélectionnez la banque de données à laquelle ajouter le stockage des machines virtuelles de service ou sélectionnez **Spécifié sur l'hôte (Specified on host)**. Nous vous conseillons d'utiliser des banques de données et réseaux partagés plutôt que « spécifiés sur l'hôte » afin d'automatiser les workflows du déploiement.

   La banque de données doit être disponible sur tous les hôtes dans le cluster sélectionné.

   Si vous avez sélectionné **Spécifié sur l'hôte (Specified on host)**, suivez les étapes ci-dessous pour chaque hôte du cluster.

   a Sur la page d'accueil de vSphere Web Client, cliquez sur **vCenter**, puis sur **Hôtes (Hosts)**.

   b Cliquez sur un hôte dans la colonne **Nom (Name)**, puis cliquez sur l'onglet **Gérer (Manage)**.

   c Cliquez sur **VM d'agent (Agent VMs)**, puis cliquez sur **Modifier (Edit)**.

   d Sélectionnez la banque de données et cliquez sur **OK**.
8. Sélectionnez le groupe de ports virtuels distribués devant héberger l'interface de gestion. Si la banque de données est définie sur **Spécifié sur l'hôte (Specified on host)**, le réseau doit également être défini sur **Spécifié sur l'hôte (Specified on host)**.

   Le groupe de ports sélectionné doit pouvoir atteindre le groupe de ports de NSX Manager et être disponible sur tous les hôtes du cluster sélectionné.

Si vous avez sélectionné **Spécifié sur l'hôte (Specified on host)**, suivez les sous-étapes de l'étape 7 pour sélectionner un réseau sur l'hôte. Lorsque vous ajoutez un ou plusieurs hôtes à un cluster, la banque de données et le réseau doivent être définis avant l'ajout de chaque hôte au cluster.

9 Dans la section Attribution IP, sélectionnez l'une des options suivantes :

Sélectionner	Vers
DHCP	Attribuez une adresse IP à la machine virtuelle de serviceNSX Guest Introspection via le protocole DHCP (Dynamic Host Configuration Protocol). Sélectionnez cette option si vos hôtes se trouvent sur des sous-réseaux différents.
Un pool IP	Attribuez une adresse IP à la machine virtuelle de service NSX Guest Introspection à partir du pool d'adresses IP sélectionné.

10 Cliquez sur **Suivant (Next)**, puis sur **Terminer (Finish)** sur la page Prêt à terminer.

11 Surveillez le déploiement jusqu'à ce que la colonne **Statut de l'installation (Installation Status)** affiche **Réussi (Succeeded)**.

12 Si la colonne **Installation Status** affiche **Échec (Failed)**, cliquez sur l'icône en regard d'Échec. Toutes les erreurs de déploiement sont affichées. Cliquez sur **Résoudre (Resolve)** pour corriger les erreurs. Dans certains cas, la résolution des erreurs affiche d'autres erreurs. Prenez les mesures nécessaires et cliquez de nouveau sur **Résoudre (Resolve)**.

Désinstallation des composants NSX

22

Ce chapitre décrit en détail la procédure de désinstallation des composants NSX de l'inventaire vCenter.

Note Ne supprimez aucun dispositif déployé par NSX (par exemple, un contrôleur ou un dispositif Edge) directement depuis vCenter. Pour gérer et supprimer des dispositifs NSX, utilisez toujours l'onglet **Mise en réseau et sécurité (Networking & Security)** de vSphere Web Client.

Ce chapitre contient les rubriques suivantes :

Désinstallation d'un module Guest Introspection

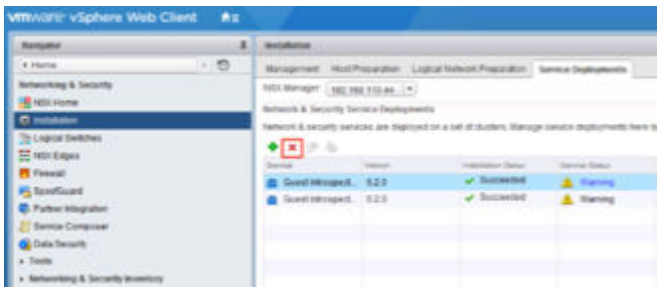
La désinstallation d'un module Guest Introspection supprime un VIB des hôtes du cluster et supprime la machine virtuelle de service de chaque hôte du cluster. Guest Introspection est requis pour Identity Firewall, la surveillance des points de terminaison et plusieurs solutions de sécurité tierces. La désinstallation de Guest Introspection peut avoir des conséquences de grande ampleur.

Attention Avant de désinstaller un module Guest Introspection d'un cluster, vous devez désinstaller tous les produits tiers qui utilisent Guest Introspection des hôtes de ce cluster. Suivez les instructions du fournisseur de la solution.

Il existe une perte de protection pour les VM dans le cluster NSX. Vous devez migrer les VM par vMotion hors du cluster avant de les désinstaller.

Pour désinstaller Guest Introspection :

1. Dans vCenter, accédez à **Accueil > Réseau et sécurité > Installation (Home > Networking & Security > Installation)** et sélectionnez l'onglet **Déploiements de services (Service Deployments)**.
2. Sélectionnez une instance Guest Introspection, puis cliquez sur l'icône Supprimer.
3. Supprimez maintenant ou prévoyez de supprimer ultérieurement.



Désinstaller un dispositif NSX Edge Services Gateway ou un routeur logique distribué

Vous pouvez désinstaller un dispositif NSX Edge à l'aide de vSphere Web Client.

Conditions préalables

Le rôle Administrateur d'entreprise ou Administrateur NSX doit vous avoir été attribué.

Procédure

1. Connectez-vous à vSphere Web Client.
2. Cliquez sur **Mise en réseau et sécurité (Networking & Security)**, puis sur **Dispositifs NSX Edge (NSX Edges)**.
3. Sélectionnez un dispositif NSX Edge et cliquez sur l'icône **Supprimer (Delete)** ( ).

Désinstaller un commutateur logique

Avant de désinstaller un commutateur logique, vous devez supprimer toutes les machines virtuelles qui y sont attachées.

Conditions préalables

Le rôle Administrateur d'entreprise ou Administrateur NSX doit vous avoir été attribué.

Procédure

1. Dans vSphere Web Client, accédez à **Page d'accueil > Mise en réseau et sécurité > Commutateurs logiques (Home > Networking & Security > Logical Switches)**.
2. Supprimez toutes les machines virtuelles d'un commutateur logique.
   a. Sélectionnez un commutateur logique et cliquez sur l'icône de suppression des machines virtuelles **()(** **)**.
   b. Déplacez toutes les machines virtuelles de la liste des objets disponibles vers la liste des objets sélectionnés, puis cliquez sur **OK**.
3. Le commutateur logique étant sélectionné, cliquez sur l'icône **Supprimer (Delete)** ( ).

Désinstaller NSX des clusters d'hôtes

Vous pouvez désinstaller NSX à partir de tous les hôtes dans un cluster.

Pour supprimer NSX de chaque hôte au lieu de procéder par cluster entier, reportez-vous au Chapitre 12 Retirer un hôte d'un cluster NSX préparé.

Conditions préalables

- Déconnectez les VM du cluster des commutateurs logiques.

Procédure

1. Supprimez le cluster de sa zone de transport.

   Accédez à **Préparation du réseau logique > Zones de transport (Logical Network Preparation > Transport Zones)** et déconnectez le cluster de la zone de transport.

   Si le cluster est grisé et que vous ne pouvez pas le déconnecter, cela peut être dû au fait que 1) un hôte du cluster est déconnecté ou est hors tension ou 2) le cluster peut contenir une ou plusieurs machines virtuelles, ou des dispositifs connectés à la zone de transport. Par exemple, si l'hôte se trouve dans un cluster de gestion et si des instances de NSX Controller y sont installées, commencez par supprimer ou déplacer les contrôleurs.

2. Désinstallez les VIB NSX. Dans vCenter Web Client, accédez à **Networking & Security > Installation > Préparation de l'hôte (Networking & Security > Installation > Host Preparation)**.

   Sélectionnez un cluster et cliquez sur **Actions (Actions) (** **)**, puis sélectionnez **Désinstaller (Uninstall)**.

   Le Statut de l'installation indique **Non prêt (Not Ready)**. Si vous cliquez sur **Non prêt (Not Ready)**, la boîte de dialogue affiche ce message : `L'hôte doit passer en mode de maintenance pour terminer l'installation du VIB agent`.

3. Sélectionnez le cluster et cliquez sur l'action **Résoudre (Resolve)** pour terminer la désinstallation.

   - Si NSX 6.2.x ou version antérieure, ou ESXi version 5.5 est installé sur l'hôte, un redémarrage est nécessaire pour terminer la désinstallation. Si DRS est activé sur le cluster, DRS tente de redémarrer les hôtes d'une manière contrôlée permettant aux machines virtuelles de continuer à fonctionner. Si DRS échoue pour une raison quelconque, l'action **Résoudre (Resolve)** s'arrête. Dans ce cas, vous devrez éventuellement déplacer les machines virtuelles manuellement, puis tenter de nouveau l'action **Résoudre (Resolve)** ou redémarrer les hôtes manuellement.
   - Si NSX 6.3.0 ou version ultérieure et ESXi 6.0 ou version ultérieure sont installés sur l'hôte, ce dernier doit être mis en mode maintenance pour terminer la désinstallation. Si DRS est activé sur le cluster, DRS tente de placer les hôtes en mode de maintenance d'une manière contrôlée

permettant aux machines virtuelles de continuer à fonctionner. Si DRS échoue pour une raison quelconque, l'action **Résoudre (Resolve)** s'arrête. Dans ce cas, vous devrez éventuellement déplacer les machines virtuelles manuellement, puis tenter de nouveau l'action **Résoudre (Resolve)** ou placer manuellement les hôtes en mode de maintenance.

Important Si vous placez manuellement les hôtes en mode de maintenance, vérifiez que la désinstallation de VIB hôte est terminée avant de sortir l'hôte de ce mode.

a Consultez le volet Tâches récentes de vSphere Web Client.

b Sous l'onglet **Préparation de l'hôte (Host Preparation)**, vérifiez la présence d'une coche verte en regard du Statut de l'installation du cluster dont l'hôte a été supprimé.

Si le Statut de l'installation est `Installation en cours`, la désinstallation n'est pas terminée.

Supprimer une installation NSX en toute sécurité

La désinstallation complète de NSX entraîne la suppression des VIB de l'hôte, de l'instance de NSX Manager, des contrôleurs, de toutes les configurations de VXLAN, des commutateurs logiques, des routeurs logiques, du pare-feu NSX, Guest Introspection et du plug-in vCenter NSX. Veillez à bien suivre ces étapes pour tous les hôtes du cluster. VMware recommande de commencer par désinstaller les composants de virtualisation de réseau d'un cluster avant de supprimer le plug-in NSX de vCenter Server.

Note Ne supprimez aucun dispositif déployé par NSX (par exemple, des contrôleurs et des dispositifs Edge) directement depuis vCenter. Pour gérer et supprimer des dispositifs NSX, utilisez toujours l'onglet **Mise en réseau et sécurité (Networking & Security)** de vSphere Web Client.

Conditions préalables

- Le rôle Administrateur d'entreprise ou Administrateur NSX doit vous avoir été attribué.
- Avant d'inverser la préparation de l'hôte afin de supprimer normalement les VM de service du cluster, supprimez toutes les solutions des partenaires enregistrées, ainsi que les services Endpoint.
- Supprimez tous les dispositifs NSX Edge. Reportez-vous à la section Désinstaller un dispositif NSX Edge Services Gateway ou un routeur logique distribué.
- Détachez les machines virtuelles se trouvant dans la zone de transport des commutateurs logiques et supprimez les commutateurs logiques. Reportez-vous à la section Désinstaller un commutateur logique.
- Désinstallez NSX des clusters d'hôtes. Reportez-vous à la section Désinstaller NSX des clusters d'hôtes.

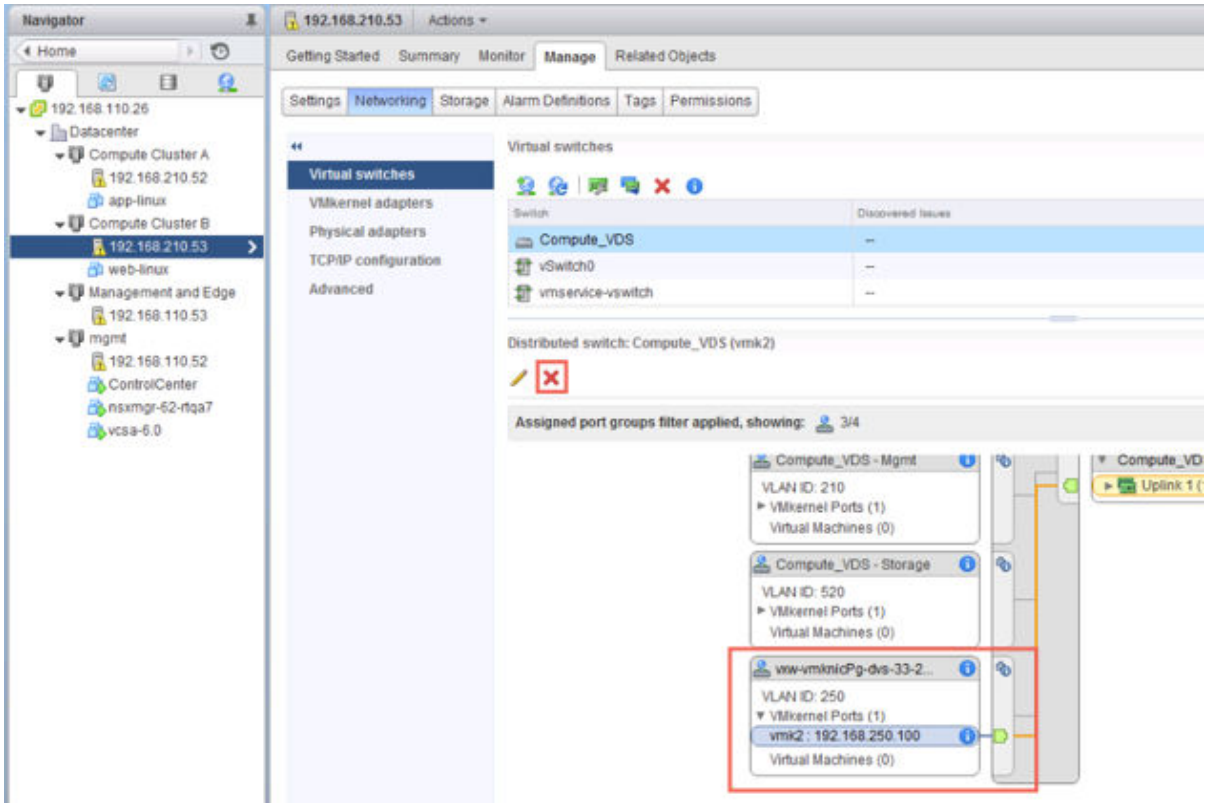
Procédure

1 Supprimez la zone de transport.

2 Supprimez le dispositif NSX Manager et toutes les machines virtuelles du dispositif NSX Controller du disque.

3 Supprimez toute interface VTEP vmkernel restante.

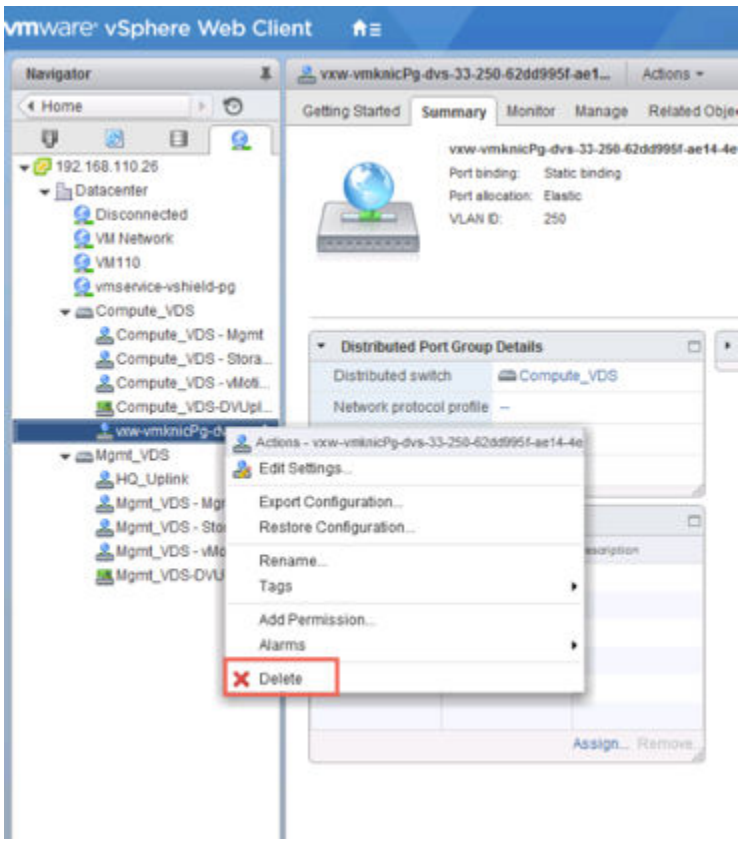
Par exemple :



Généralement, les interfaces vmkernel de VTEP sont déjà supprimées suite aux précédentes opérations de désinstallation.

4 Supprimez tout dvPortgroup restant utilisé pour les VTEP.

Par exemple :



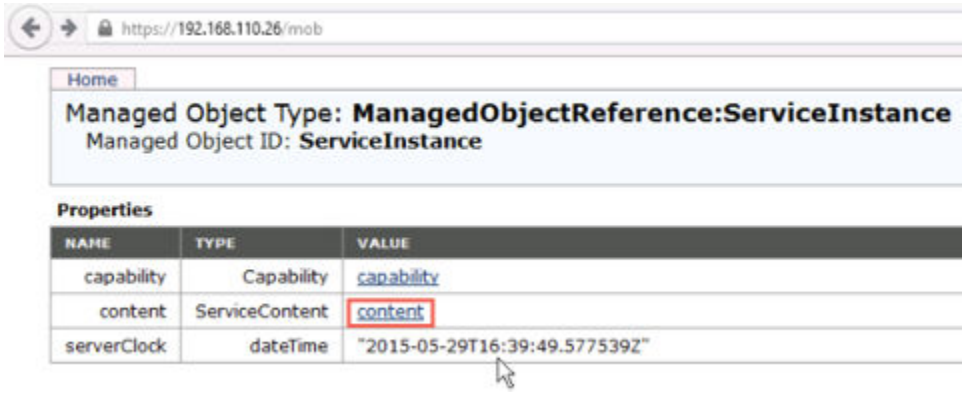
Généralement, les dvPortgroups utilisés pour les VTEP sont déjà supprimés suite aux précédentes opérations de désinstallation.

5 Si vous avez supprimé les interfaces vmkernel ou dvPortgroups de VTEP, redémarrez les hôtes.

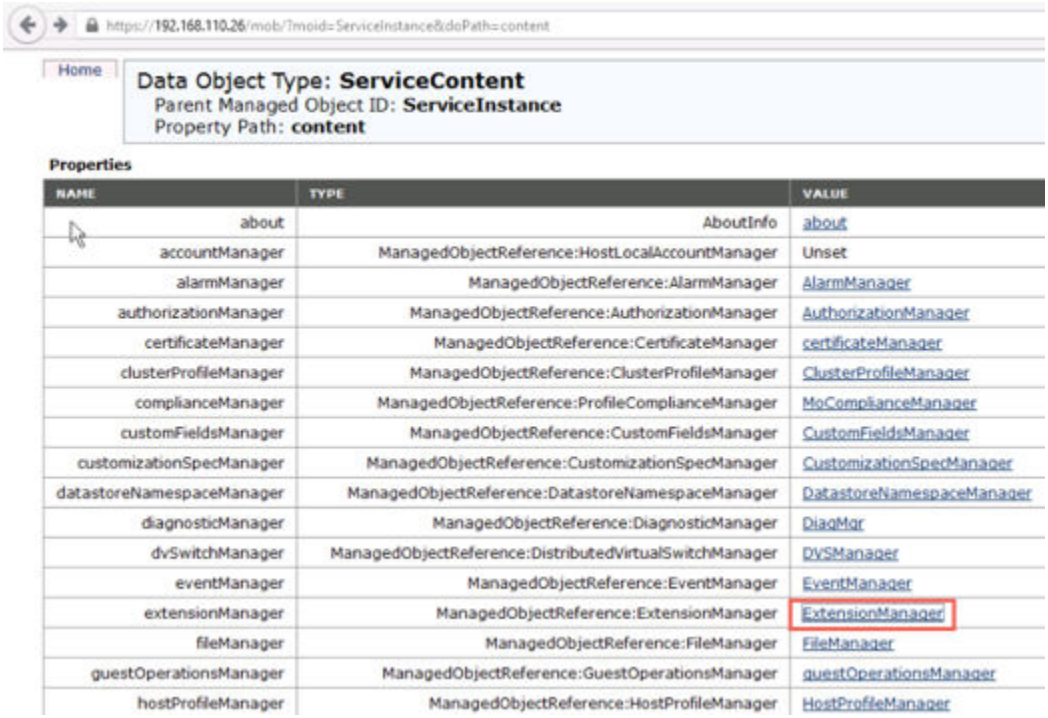
6 Pour l'instance de vCenter de laquelle vous souhaitez supprimer le plug-in NSX Manager, connectez-vous au navigateur de l'objet géré à l'adresse https://your_vc_server/mob.

7 Cliquez sur **Contenu (Content)**.

Par exemple :



8 Cliquez sur **ExtensionManager**.



https://192.168.110.26/mob/?moid=ServiceInstance&doPath=content

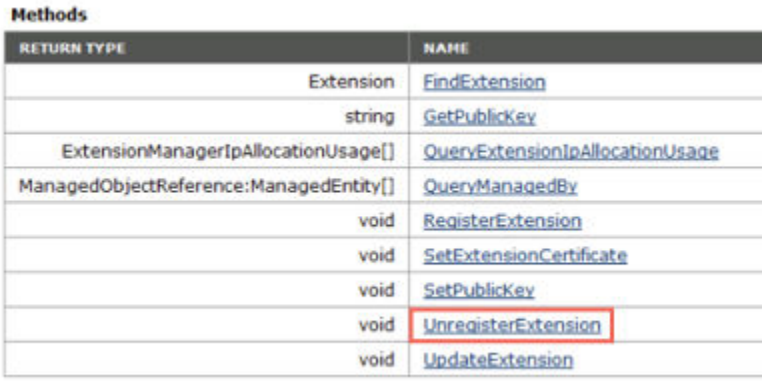
Home

Data Object Type: ServiceContent
Parent Managed Object ID: **ServiceInstance**
Property Path: **content**

Properties

NAME	TYPE	VALUE
about	AboutInfo	about
accountManager	ManagedObjectReference:HostLocalAccountManager	Unset
alarmManager	ManagedObjectReference:AlarmManager	AlarmManager
authorizationManager	ManagedObjectReference:AuthorizationManager	AuthorizationManager
certificateManager	ManagedObjectReference:CertificateManager	certificateManager
clusterProfileManager	ManagedObjectReference:ClusterProfileManager	ClusterProfileManager
complianceManager	ManagedObjectReference:ProfileComplianceManager	MoComplianceManager
customFieldsManager	ManagedObjectReference:CustomFieldsManager	CustomFieldsManager
customizationSpecManager	ManagedObjectReference:CustomizationSpecManager	CustomizationSpecManager
datastoreNamespaceManager	ManagedObjectReference:DatastoreNamespaceManager	DatastoreNamespaceManager
diagnosticManager	ManagedObjectReference:DiagnosticManager	DiagMgr
dvSwitchManager	ManagedObjectReference:DistributedVirtualSwitchManager	DVSManager
eventManager	ManagedObjectReference:EventManager	EventManager
extensionManager	ManagedObjectReference:ExtensionManager	ExtensionManager
fileManager	ManagedObjectReference:FileManager	FileManager
guestOperationsManager	ManagedObjectReference:GuestOperationsManager	guestOperationsManager
hostProfileManager	ManagedObjectReference:HostProfileManager	HostProfileManager

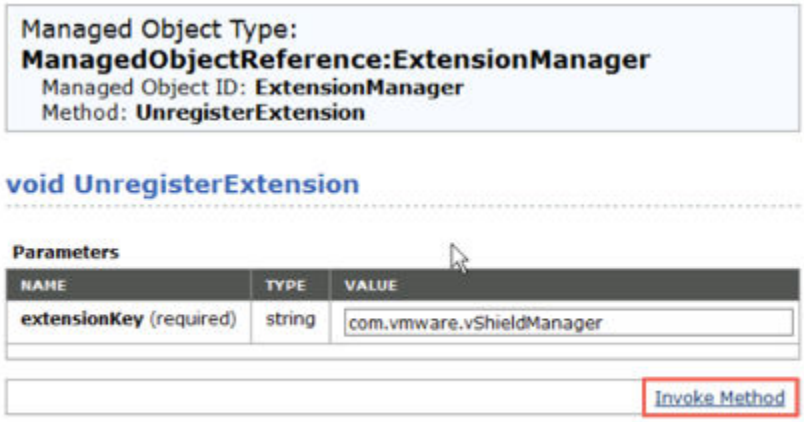
9 Cliquez sur **UnregisterExtension**.



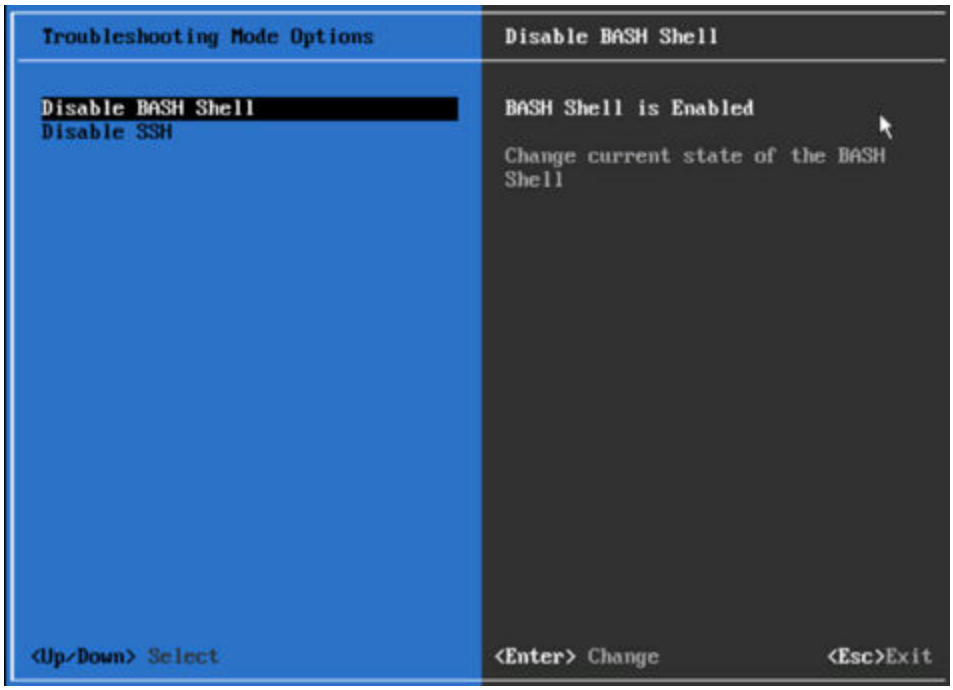
Methods

RETURN TYPE	NAME
Extension	FindExtension
string	GetPublicKey
ExtensionManagerIpAllocationUsage[]	QueryExtensionIpAllocationUsage
ManagedObjectReference:ManagedEntity[]	QueryManagedBy
void	RegisterExtension
void	SetExtensionCertificate
void	SetPublicKey
void	UnregisterExtension
void	UpdateExtension

10 Entrez la chaîne **com.vmware.vShieldManager**, puis cliquez sur **Invoquer la méthode (Invoke Method)**.



11 Si vous exécutez le dispositif vSphere 6 vCenter, lancez la console et activez l'interpréteur de commandes de dépistage sous **Options de mode de dépannage (Troubleshooting Mode Options)**.



Il est également possible d'activer l'interpréteur de commandes de dépistage en se connectant en tant qu'utilisateur racine et en exécutant la commande `shell.set --enabled true`.

12 Supprimez les répertoires de vSphere Web Client pour NSX, puis redémarrez le service Web Client.

Les répertoires de vSphere Web Client pour NSX se nomment com.vmware.vShieldManager.** et se trouvent aux emplacements suivants :

- VMware vCenter Server pour Windows : C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity\
- VMware vCenter Server Appliance : /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/

Redémarrez vCenter Server Appliance :

- Dans vCenter Server Appliance 6.0, connectez-vous au shell vCenter Server en tant qu'utilisateur racine et exécutez les commandes suivantes :

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

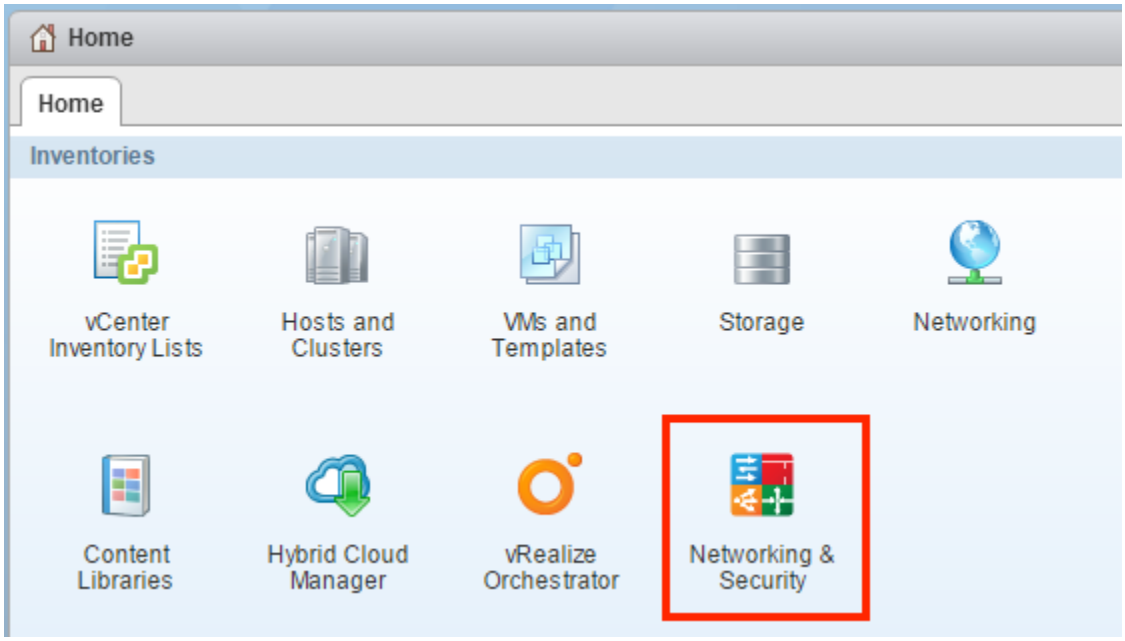
- Dans vCenter Server 6.0 sous Windows, vous pouvez exécuter les commandes suivantes.

```
cd C:\Program Files\VMware\vCenter Server\binservice-control --stop
vspherewebclientsvcservice-control --start vspherewebclientsvc
```

Résultats

Le plug-in NSX Manager est supprimé de vCenter. Pour confirmer, déconnectez-vous de vCenter, puis reconnectez-vous.

L'icône **Mise en réseau et sécurité (Networking & Security)** du plug-in NSX Manager n'apparaît plus sur l'écran d'accueil de vCenter Web Client.



Accédez à **Administration > Plug-ins des clients (Administration > Client Plug-Ins)** et vérifiez que la liste des plug-ins n'inclut pas **Plug-in de l'interface utilisateur de NSX (NSX User Interface plugin)**.