

Guide d'installation de NSX-T Data Center

Modifié le 23 avril 2019

VMware NSX-T Data Center 2.3



vmware®

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

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

Les dernières mises à jour produit se trouvent également sur le site Web de VMware.

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

docfeedback@vmware.com

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

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

Copyright © 2018, 2019 VMware, Inc. Tous droits réservés. [Informations sur le copyright et les marques commerciales.](#)

Table des matières

Guide d'installation de NSX-T Data Center 5

1 Présentation de NSX-T Data Center 6

- Plan de gestion 7
- Plan de contrôle 9
- Plan de données 10
- Commutateurs logiques 11
- Routeurs logiques 12
- Concepts clés 13

2 Préparation à l'installation 17

- Configuration système requise 17
- Ports et protocoles 22
- Tâches de haut niveau de l'installation de NSX-T Data Center 28

3 Utilisation de KVM 30

- Configurer KVM 30
- Gérer vos machines virtuelles invitées dans l'interface de ligne de commande de KVM 35

4 Installation de NSX Manager 37

- Installer NSX Manager et les dispositifs disponibles 39
- Installer NSX Manager sur ESXi à l'aide de l'outil OVF de ligne de commande 41
- Installer NSX Manager sur KVM 44
- Se connecter à l'instance de NSX Manager qui vient d'être créée 47

5 Installation et mise en cluster de NSX Controller 48

- Installation automatisée d'un contrôleur et d'un cluster à partir de NSX Manager 50
- Installer NSX Controller sur ESXi à l'aide d'une interface utilisateur graphique 57
- Installer NSX Controller sur ESXi à l'aide de l'outil OVF de ligne de commande 60
- Installer NSX Controller sur KVM 62
- Joindre des dispositifs NSX Controller à NSX Manager 65
- Initialiser le cluster de contrôle pour créer un maître de cluster de contrôle 66
- Relier les dispositifs NSX Controller au maître de cluster 68

6 Installation de NSX Edge 72

- Configuration réseau de NSX Edge 74
- Déploiement automatique de machines virtuelles NSX Edge à partir de NSX Manager 80
- Installer un dispositif NSX Edge sur ESXi à l'aide d'une interface utilisateur graphique vSphere 81

- Installer NSX Edge sur ESXi à l'aide de l'outil OVF de ligne de commande 84
- Installer NSX Edge à l'aide d'un fichier ISO avec un serveur PXE 88
- Relier NSX Edge au plan de gestion 101

7 Préparation de l'hôte 103

- Installer les modules tiers sur un hôte KVM ou un serveur bare metal 103
- Vérifier la version Open vSwitch sur les hôtes RHEL KVM 106
- Ajouter un hôte d'hyperviseur ou un serveur bare metal à l'infrastructure NSX-T Data Center 107
- Installation manuelle de modules de noyau NSX-T Data Center 111
- Relier les hôtes d'hyperviseur au plan de gestion 116

8 Zones de transport et nœuds de transport 119

- À propos des zones de transport 119
- Chemin de données optimisé 121
- Créer un pool d'adresses IP pour les adresses IP des points de terminaison de tunnel 123
- Créer un profil de liaison montante 125
- Créer des zones de transport 129
- Créer un nœud de transport hôte 132
- Créer une interface d'application pour les charges de travail de serveur Bare Metal 150
- Configurer des profils Network I/O Control 151
- Créer un nœud de transport NSX Edge 160
- Créer un cluster NSX Edge 164

9 Installation des composants NSX Cloud 166

- Architecture et composants de NSX Cloud 166
- Présentation de l'installation de composants NSX Cloud 167
- Installer CSM et se connecter à NSX Manager 169
- Connecter le cloud public avec déploiement sur site 172
- Ajouter votre compte de cloud public 176
- Déployer PCG 181
- Annuler le déploiement de PCG 187

10 Désinstallation de NSX-T Data Center 192

- Annuler la configuration d'une superposition NSX-T Data Center 192
- Supprimer un hôte de NSX-T Data Center ou désinstaller complètement NSX-T Data Center 193

Guide d'installation de NSX-T Data Center

Le *Guide d'installation de NSX-T Data Center* décrit comment installer le produit VMware NSX-T™ Data Center. Il contient des instructions de configuration pas à pas et des suggestions de meilleures pratiques.

Public visé

Ces informations s'adressent aux personnes qui veulent installer ou utiliser NSX-T Data Center. Les informations sont destinées aux administrateurs système expérimentés qui maîtrisent la technologie des machines virtuelles et les concepts de virtualisation du réseau.

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-T Data Center

1

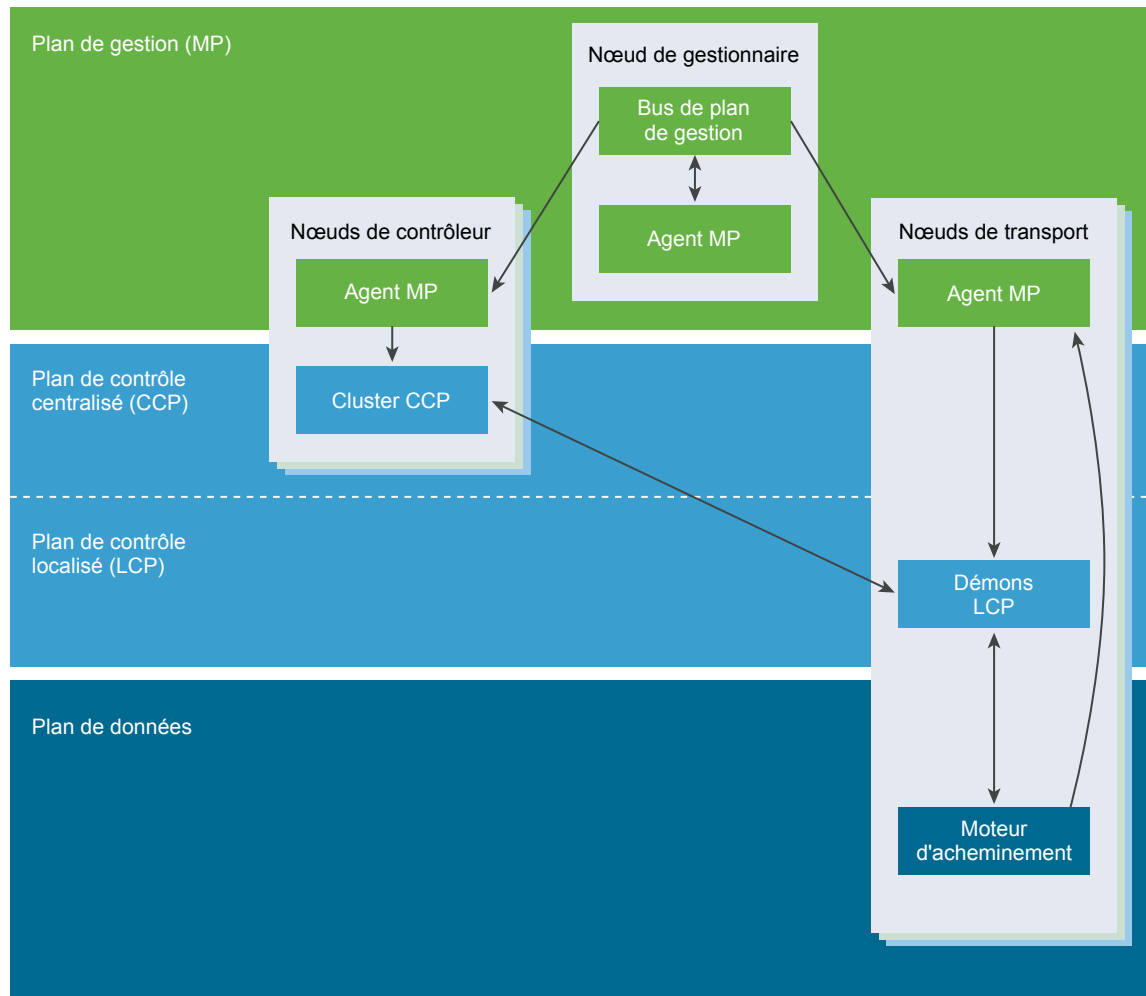
Tout comme la virtualisation des serveurs crée, supprime et restaure des machines virtuelles basées sur des logiciels, et en crée des snapshots, de façon programmée, la virtualisation réseau NSX-T Data Center crée, supprime et restaure des réseaux virtuels basés sur des logiciels de façon programmée.

Avec la virtualisation réseau, l'équivalent fonctionnel d'un hyperviseur de réseau reproduit l'ensemble complet des 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 et qualité de service) dans le logiciel. Par conséquent, ces services peuvent être assemblés de façon programmée dans n'importe quelle combinaison arbitraire afin de produire des réseaux virtuels isolés en quelques secondes.

NSX-T Data Center travaille en mettant en œuvre trois plans distincts mais intégrés : gestion, contrôle et données. Les trois plans sont implémentés sous la forme d'un ensemble de processus, de modules et d'agents résidant sur trois types de nœuds : gestionnaire, contrôleur et transport.

- Chaque nœud héberge un agent du plan de gestion.
- Le nœud NSX Manager héberge des services API. Chaque installation NSX-T Data Center prend en charge un unique nœud NSX Manager.
- Les nœuds NSX Controller hébergent les démons de cluster du plan de contrôle central.
- Les nœuds NSX Manager et NSX Controller peuvent être co-hébergés sur le même serveur physique.

- Les nœuds de transport hébergent des démons du plan de contrôle local et des moteurs d'acheminement.



Ce chapitre contient les rubriques suivantes :

- [Plan de gestion](#)
- [Plan de contrôle](#)
- [Plan de données](#)
- [Commutateurs logiques](#)
- [Routeurs logiques](#)
- [Concepts clés](#)

Plan de gestion

Le plan de gestion fournit un point d'entrée API unique au système, enregistre la configuration de l'utilisateur, gère les requêtes des utilisateurs et exécute des tâches opérationnelles sur tous les nœuds des plans de gestion, de contrôle et de données du système.

Concernant NSX-T Data Center, le plan de gestion est chargé de l'interrogation, la modification et la persistance de la configuration utilisateur, alors que la diffusion de cette configuration vers le sous-ensemble approprié des éléments du plan de données incombe au plan de contrôle. Cela signifie que certaines données appartiennent à plusieurs plans selon le stade de leur cycle de vie. Le plan de gestion gère également l'interrogation des états récents et des statistiques à partir du plan de contrôle, et parfois directement à partir du plan de données.

Le plan de gestion est la seule source fiable pour le système configuré (logique), tel qu'il est géré par l'utilisateur via la configuration. Les modifications sont apportées par le biais d'une API RESTful ou de l'interface utilisateur de NSX-T Data Center.

NSX possède également un agent de plan de gestion (MPA) qui s'exécute sur tous les nœuds de cluster de contrôleurs et de transport. L'agent MPA est accessible localement et à distance. Sur les nœuds de transport, il peut également effectuer des tâches liées au plan de données.

Les tâches qui ont lieu sur le plan de gestion incluent ce qui suit :

- Persistance de la configuration (état logique souhaité)
- Validation des entrées
- Gestion des utilisateurs (attributions de rôles)
- Gestion des stratégies
- Suivi des tâches d'arrière-plan

NSX Manager

NSX Manager est un dispositif virtuel qui fournit l'interface utilisateur graphique (GUI) et les API REST pour la création, la configuration et la surveillance des composants NSX-T Data Center, tels que les commutateurs logiques et les passerelles de services NSX Edge.

NSX Manager est le plan de gestion de l'écosystème NSX-T Data Center. NSX Manager fournit une vue agrégée du système et constitue le composant de gestion réseau centralisée de NSX-T Data Center. Il permet la configuration et l'orchestration des éléments suivants :

- Composants de mise en réseau logique (commutation et routage logique)
- Mise en réseau et services Edge
- Services de sécurité et pare-feu distribué

NSX Manager fournit une méthode pour surveiller et dépanner les charges de travail rattachées aux réseaux virtuels créés par NSX-T Data Center. Il permet une orchestration transparente des services intégrés et externes. Tous les services de sécurité, intégrés ou tiers, sont déployés et configurés par le plan de gestion NSX-T Data Center. Le plan de gestion fournit une fenêtre unique pour visualiser la disponibilité des services. Il facilite également le chaînage des services basés sur des stratégies, le partage de contexte et la gestion des événements inter-services. Cela simplifie l'audit du dispositif de sécurité, en rationalisant la mise en application des contrôles basés sur l'identité (par exemple, les profils AD et de mobilité).

NSX Manager fournit également des points d'entrée REST API pour automatiser la consommation. Cette architecture flexible permet l'automatisation de tous les aspects liés à la configuration et la surveillance quel que soit la plate-forme de gestion cloud, la plate-forme de fournisseur de sécurité ou le cadre d'automatisation.

L'agent MPA NSX-T Data Center est un composant NSX Manager qui réside sur chaque nœud (hyperviseur). L'agent MPA est responsable de la persistance de l'état souhaité du système et de la communication de messages sans contrôle de flux (NFC) tels que la configuration, les statistiques, l'état et les données en temps réel entre les nœuds de transport et le plan de gestion.

NSX Policy Manager

NSX Policy Manager est un dispositif virtuel qui fournit un système basé sur l'intention pour simplifier la consommation de services NSX-T Data Center.

NSX Policy Manager fournit une interface utilisateur graphique (GUI) et des API REST pour spécifier l'intention liée à la mise en réseau, à la sécurité et à la disponibilité.

NSX Policy Manager accepte l'intention de l'utilisateur sous la forme d'un modèle de données basé sur l'arborescence et configure NSX Manager pour réaliser cette intention. NSX Policy Manager prend en charge la spécification de l'intention de communication qui configure un pare-feu distribué sur NSX Manager.

Cloud Service Manager

Cloud Service Manager (CSM) fournit un point de terminaison de gestion à panneau de contrôle unique, écran unique pour toutes les constructions de votre cloud public.

CSM est un dispositif virtuel qui fournit l'interface utilisateur (GUI) et les API REST pour l'intégration, configuration et la surveillance de votre inventaire de cloud public.

Plan de contrôle

Calcule tous les états d'exécution éphémères en fonction de la configuration du plan de gestion, diffuse les informations sur la topologie indiquées par les éléments du plan de données et transfère la configuration sans état aux moteurs d'acheminement.

Le plan de contrôle est divisé en deux parties dans NSX-T Data Center, le plan de contrôle central (CCP), qui s'exécute sur les nœuds du cluster NSX Controller, et le plan de contrôle local (LCP), qui s'exécute sur les nœuds de transport adjacents au plan de données qu'il contrôle. Le plan de contrôle central calcule des états d'exécution éphémères en fonction de la configuration du plan de gestion et diffuse les informations indiquées par les éléments du plan de données via le plan de contrôle local. Le plan de contrôle local surveille l'état des liens locaux, calcule la plupart des états d'exécution éphémères en fonction des mises à jour du plan de données et du plan de contrôle central, et transfère la configuration sans état aux moteurs d'acheminement. Le plan de contrôle local est solidaire de l'élément de plan de données qui l'héberge.

NSX Controller

NSX Controller, appelé « plan de contrôle central » (Central Control Plane, CCP) est un système de gestion des états distribués avancé qui contrôle les réseaux virtuels et les tunnels de transport de superposition.

NSX Controller est déployé en tant que cluster de dispositifs virtuels hautement disponibles qui sont chargés du déploiement programmatique des réseaux virtuels sur l'ensemble de l'architecture NSX-T Data Center. Le CCP de NSX-T Data Center est logiquement séparé de tout le trafic du plan de données, ce qui signifie que toute défaillance dans le plan de contrôle n'affecte pas les opérations en cours dans le plan de données. Le trafic ne passe pas par le contrôleur. Celui-ci est chargé de fournir la configuration à d'autres composants NSX Controller, tels que les commutateurs logiques, les routeurs logiques et la configuration Edge. La stabilité et la fiabilité du transport de données sont cruciales en matière de gestion réseau. Pour améliorer encore la haute disponibilité et l'évolutivité, NSX Controller est déployé dans un cluster de trois instances.

Plan de données

Effectue l'acheminement/la transformation sans état des paquets en fonction de tables remplies par le plan de contrôle, fournit les informations sur la topologie au plan de contrôle et réalise des statistiques au niveau des paquets.

Le plan de données est une source d'informations fiable pour les états et la topologie physiques, par exemple, l'emplacement des cartes virtuelles, l'état du tunnel, etc. Si vous déplacez des paquets d'un emplacement à un autre, vous êtes dans le plan de données. Le plan de données maintient également l'état de basculement et gère le basculement entre plusieurs liens/tunnels. Les performances par paquet sont capitales, avec des exigences strictes en matière de latence ou de gigue. Le plan de données n'est pas nécessairement totalement contenu dans le noyau, les pilotes, l'espace utilisateur ou même des processus d'espace utilisateur spécifiques. Le plan de données est limité à des acheminements entièrement sans état basés sur des tables/règles renseignées par le plan de contrôle.

Le plan de données peut aussi avoir des composants qui conservent un certain degré d'état pour des fonctionnalités telles que les déconnexions TCP. L'état géré du plan de données est différent de l'état géré du plan de contrôle, tel que le mappage de tunnels MAC:IP. Le second vise en effet à acheminer les paquets, tandis que le premier est limité à la manière de manipuler la charge utile.

NSX Edge

NSX Edge fournit des services de routage et la connectivité aux réseaux qui sont externes au déploiement NSX-T Data Center.

NSX Edge peut être déployé comme un nœud de système nu ou comme une machine virtuelle.

NSX Edge est nécessaire à l'établissement de la connectivité externe à partir du domaine NSX-T Data Center par le biais d'un routeur de niveau 0 via BGP ou routage statique. De plus, un système NSX Edge doit être déployé si vous avez besoin des services de traduction d'adresses réseau (NAT) sur les routeurs logiques de niveau 0 ou de niveau 1.

La passerelle NSX Edge permet de connecter des réseaux isolés ou réseaux d'extrémité à des réseaux partagés (liaison montante) en fournissant des services courants de passerelle tels que NAT et le routage dynamique. NSX Edge est couramment déployé dans la DMZ et les environnements cloud à locataires multiples dans lesquels NSX Edge crée des limites virtuelles pour chaque locataire.

Zones de transport

Une zone de transport est une construction logique qui contrôle les hôtes qu'un commutateur logique peut atteindre. Elle peut s'étendre sur un ou plusieurs clusters d'hôtes. Les zones de transport dictent quels hôtes et, en conséquence, quelles machines virtuelles peuvent participer à l'utilisation d'un réseau donné.

Une zone de transport définit une collection d'hôtes qui peuvent communiquer les uns avec les autres sur une infrastructure de réseau physique. Cette communication intervient sur une ou plusieurs interfaces définies en tant que VTEP (Virtual Tunnel Endpoints).

Les nœuds de transport sont les hôtes exécutant les démons du plan de contrôle local et les moteurs d'acheminement appliquant le plan de données NSX-T Data Center. Les nœuds de transport se composent d'un commutateur virtuel distribué NSX-T Data Center (N-VDS), qui est responsable de la commutation de paquets en fonction de la configuration des services réseau disponibles.

Si deux nœuds de transport se trouvent dans la même zone de transport, les machines virtuelles hébergées sur ces nœuds de transport peuvent « voir » les commutateurs logiques NSX-T Data Center de cette zone de transport et y être attachées. Ce rattachement permet aux machines virtuelles de communiquer entre elles, en admettant que celles-ci soient accessibles via la couche 2/couche 3. Si les machines virtuelles sont attachées à des commutateurs qui sont dans des zones de transport différentes, elles ne peuvent pas communiquer entre elles. Les zones de transport ne remplacent pas les exigences en matière d'accessibilité de la couche 2/couche 3, mais elles limitent l'accessibilité. En d'autres termes, l'appartenance à une même zone de transport est une condition préalable à la connectivité. Une fois que cette condition préalable est remplie, l'accessibilité est possible, mais elle n'est pas automatique. Pour que l'accessibilité soit effective, la couche 2 et (pour d'autres sous-réseaux) la couche 3 doivent être opérationnelles.

Un hôte peut servir de nœud de transport s'il contient au moins un commutateur virtuel distribué géré par NSX (N-VDS, anciennement appelé commutateur hôte). Lorsque vous créez un nœud de transport hôte, puis ajoutez le nœud à une zone de transport, NSX-T Data Center installe un N-VDS sur l'hôte. Pour chaque zone de transport à laquelle appartient l'hôte, un N-VDS distinct est installé. Le N-VDS est utilisé pour relier des machines virtuelles à des commutateurs logiques NSX-T Data Center et pour créer des liaisons montantes et des liaisons descendantes de routeurs logiques NSX-T Data Center.

Commutateurs logiques

La capacité de commutation logique de la plate-forme NSX-T Data Center permet d'exploiter des réseaux de couche 2 logiques isolés avec autant de souplesse et d'agilité qu'une machine virtuelle.

Un commutateur logique fournit une représentation de la connectivité de couche 2 entre plusieurs hôtes accessibles via la couche IP 3. Si vous envisagez de limiter l'accès à certains réseaux logiques à un nombre restreint d'hôtes ou si vous avez des exigences de connectivité personnalisées, il peut s'avérer nécessaire de créer des commutateurs logiques supplémentaires.

Ces applications et ces locataires nécessitent d'être isolés les uns des autres pour assurer la sécurité et l'isolement des pannes, et pour éviter les problèmes de chevauchement des adresses IP. Les points de terminaison, tant virtuels que physiques, peuvent se connecter à des segments logiques et établir une connectivité indépendamment de leur emplacement physique sur le réseau du centre de données. La virtualisation du réseau NSX-T Data Center permet en effet de dissocier l'infrastructure réseau du réseau logique (c'est-à-dire de séparer le réseau sous-jacent du réseau de superposition).

Routeurs logiques

Les routeurs logiques NSX-T Data Center fournissent la connectivité nord-sud, permettant ainsi aux locataires d'accéder aux réseaux publics, et la connectivité est-ouest entre différents réseaux au sein des mêmes locataires. Dans le cas d'une connectivité est-ouest, les routeurs logiques sont répartis sur le noyau des hôtes.

Avec NSX-T Data Center, il est possible de créer une topologie de routeurs logiques à deux niveaux : le routeur logique de niveau supérieur s'appelle routeur de niveau 0 tandis que le routeur logique de niveau inférieur est le routeur de niveau 1. Cette structure permet aux administrateurs fournisseurs et aux administrateurs locataires d'avoir le contrôle complet de leurs services et stratégies. Les administrateurs contrôlent et configurent le routage et les services de niveau 0, et les administrateurs locataires contrôlent et configurent le niveau 1. L'extrémité nord du routeur de niveau 0 communique avec le réseau physique et c'est à cet endroit qu'il est possible de configurer les protocoles de routage dynamique afin d'échanger des informations de routage avec les routeurs physiques. L'extrémité sud du routeur de niveau 0 se connecte à plusieurs couches de routage de niveau 1 et reçoit des informations de routage de celles-ci. Pour optimiser l'utilisation des ressources, la couche de niveau 0 ne transfère pas tous les itinéraires provenant du réseau physique vers le niveau 1, mais fournit des informations par défaut.

En direction du sud, la couche de routage de niveau 1 communique avec les commutateurs logiques définis par les administrateurs locataires, et fournit une fonction de routage à tronçon unique entre eux. Pour que les sous-réseaux attachés au niveau 1 soient accessibles depuis le réseau physique, il est nécessaire que la redistribution d'itinéraires soit activée vers la couche de niveau 0. Cependant, il n'existe pas de protocole de routage classique (tel que OSPF ou BGP) entre la couche de niveau 1 et la couche de niveau 0 et tous les itinéraires passent par le plan de contrôle NSX-T Data Center. Notez que, s'il n'est pas nécessaire de séparer le fournisseur et le locataire, la topologie de routage à deux niveaux n'est pas obligatoire. Une topologie à un seul niveau peut être créée et, dans ce scénario, les commutateurs logiques sont directement connectés à la couche de niveau 0 et il n'existe pas de couche de niveau 1.

Un routeur logique se compose de deux éléments facultatifs : un routeur distribué (DR) et un ou plusieurs routeurs de services (SR).

Un DR s'étend sur les hyperviseurs dont les machines virtuelles sont connectées à ce routeur logique, ainsi qu'aux nœuds Edge auxquels le routeur logique est lié. Du point de vue fonctionnel, le DR est chargé du routage distribué à tronçon unique entre les commutateurs logiques et/ou routeurs logiques connectés à ce routeur logique. Le SR est chargé de la livraison de services qui ne sont pas actuellement mis en œuvre de manière distribuée, tels que la traduction d'adresses réseau (NAT) avec état.

Un routeur logique possède toujours un DR et il possède des SR si l'une des conditions suivantes est remplie :

- Le routeur logique est un routeur de niveau 0 même si aucun service avec état n'est configuré
- Le routeur logique est un routeur de niveau 1 lié à un routeur de niveau 0 et possède des services configurés sans implémentation distribuée (telle que NAT, LB ou DHCP)

Le plan de gestion (MP) NSX-T Data Center est chargé de créer automatiquement la structure qui connecte le routeur de services au routeur distribué. Le MP crée un commutateur logique de transit et lui attribue un VNI, puis crée un port sur chaque SR et DR, les connecte au commutateur logique de transit et alloue des adresses IP pour le SR et le DR.

Concepts clés

Concepts NSX-T Data Center courants utilisés dans la documentation et l'interface utilisateur.

Gestionnaire de calcul	Un gestionnaire de calcul est une application qui gère les ressources, telles que des hôtes et des machines virtuelles. Par exemple, vCenter Server.
Plan de contrôle	Calcule l'état d'exécution en fonction de la configuration à partir du plan de gestion. Le plan de contrôle diffuse les informations de topologie signalées par les éléments du plan de données et transfère la configuration sans état aux moteurs d'acheminement.
Plan de données	Effectue l'acheminement ou la transformation sans état des paquets sur la base de tables remplies par le plan de contrôle. Le plan de données rapporte les informations de topologie au plan de contrôle et gère les statistiques au niveau des paquets.
Mise en réseau externe	Réseau physique ou réseau local virtuel non géré par NSX-T Data Center. Vous pouvez lier votre réseau logique ou votre réseau de superposition à un réseau externe par le biais d'un dispositif NSX Edge. Par exemple, un réseau physique dans un centre de données client ou un réseau local virtuel dans un environnement physique.
Nœud d'infrastructure	Hôte enregistré auprès du plan de gestion NSX-T Data Center et dont les modules NSX-T Data Center sont installés. Pour qu'un hôte d'hyperviseur ou un dispositif NSX Edge appartienne à une superposition NSX-T Data Center, il doit être ajouté à l'infrastructure NSX-T Data Center.

Sortie de port logique	Le trafic réseau sortant quittant la machine virtuelle ou le réseau logique est appelé « sortie », car le trafic quitte le réseau virtuel et pénètre dans le centre de données.
Entrée de port logique	Le trafic réseau entrant quittant le centre de données et pénétrant dans la machine virtuelle est un trafic d'entrée.
Routeur logique	Entité de routage NSX-T Data Center.
Port de routeur logique	Port réseau logique auquel vous pouvez connecter un port de commutateur logique ou un port de liaison montante vers un réseau physique.
Commutateur logique	<p>Entité qui fournit une commutation virtuelle de couche 2 pour les interfaces de machine virtuelle et les interfaces de passerelle. Un commutateur logique offre aux administrateurs réseau locataire l'équivalent logique d'un commutateur physique de couche 2, leur permettant ainsi de connecter un ensemble de machines virtuelles à un domaine de diffusion commun. Un commutateur logique est une entité logique indépendante de l'infrastructure de l'hyperviseur physique et s'étend sur de nombreux hyperviseurs, connectant les machines virtuelles indépendamment de leur emplacement physique.</p> <p>Dans un cloud à locataires multiples, de nombreux commutateurs logiques peuvent exister côte à côte sur le même hyperviseur physique, les segments de couche 2 étant isolés les uns des autres. Les commutateurs logiques peuvent être connectés à l'aide de routeurs logiques, et les routeurs logiques peuvent fournir des ports de liaison montante connectés au réseau physique externe.</p>
Port de commutateur logique	Point d'attache de commutateur logique permettant d'établir une connexion à une interface de réseau de machine virtuelle ou à une interface de routeur logique. Le port du commutateur logique indique le profil de commutation appliqué, l'état du port et l'état du lien.
Plan de gestion	Fournit un point d'entrée API unique au système, enregistre la configuration de l'utilisateur, gère les requêtes des utilisateurs et exécute des tâches opérationnelles sur tous les nœuds des plans de gestion, de contrôle et de données du système. Le plan de gestion est également chargé de l'interrogation, de la modification et de la persistance de la configuration d'utilisation.
Cluster NSX Controller	Déployé en tant que cluster de dispositifs virtuels hautement disponibles qui sont chargés du déploiement programmatique des réseaux virtuels sur l'ensemble de l'architecture NSX-T Data Center.
Cluster NSX Edge	Ensemble de dispositifs de nœud NSX Edge qui possèdent les mêmes paramètres que les protocoles impliqués dans la surveillance haute disponibilité.

Nœud NSX Edge	Composant dont l'objectif fonctionnel est de fournir la puissance de calcul nécessaire au routage IP et aux fonctions de services IP.
Commutateur virtuel distribué géré par NSX ou KVM Open vSwitch	<p>Logiciel qui s'exécute sur l'hyperviseur et assure l'acheminement du trafic. Le commutateur virtuel distribué géré par NSX (N-VDS, anciennement appelé commutateur hôte) ou OVS est invisible pour l'administrateur réseau locataire et fournit le service d'acheminement sous-jacent sur lequel repose chaque commutateur logique. Pour effectuer la virtualisation du réseau, un contrôleur réseau doit configurer les commutateurs virtuels d'hyperviseur avec les tables de flux réseau qui forment les domaines de diffusion logiques que les administrateurs locataires ont définis lorsqu'ils ont créé et configuré leurs commutateurs logiques.</p> <p>Chaque domaine de diffusion logique est implémenté en tunnellant le trafic entre machines virtuelles et le trafic entre machine virtuelle et routeur logique à l'aide du mécanisme d'encapsulation de tunnel Geneve. Le contrôleur réseau dispose de la vue globale du centre de données et s'assure que les tables de flux des commutateurs virtuels d'hyperviseur sont mises à jour lorsque des machines virtuelles sont créées, déplacées ou supprimées.</p> <p>Un N-VDS dispose de deux modes : chemin de données standard et amélioré. Les performances d'un chemin de données amélioré N-VDS permettent de prendre en charge les charges de travail NFV (virtualisation des fonctions réseau).</p>
NSX Manager	Nœud qui héberge les services d'API, le plan de gestion et les services d'agent.
NSX-T Data Center Unified Appliance	NSX-T Data Center Unified Appliance est un dispositif inclus dans le module d'installation de NSX-T Data Center. Vous pouvez déployer le dispositif dans le rôle de NSX Manager, de Gestionnaire de stratégie ou de Cloud Service Manager. Actuellement, le dispositif prend uniquement en charge un seul rôle à la fois.
Open vSwitch (OVS)	Commutateur logiciel Open Source qui agit comme un commutateur virtuel dans XenServer, Xen, KVM et d'autres hyperviseurs basés sur Linux.
Réseau logique de superposition	Réseau logique implémenté à l'aide de la tunnellation de couche 2 dans la couche 3, de sorte que la topologie vue par les machines virtuelles est dissociée de celle du réseau physique.
Interface physique (pNIC)	Interface réseau d'un serveur physique sur lequel un hyperviseur est installé.

Routeur logique de niveau 0

Le routeur logique fournisseur est également connu sous le nom de routeur logique de niveau 0 connecté au réseau physique. Le routeur logique de niveau 0 est un routeur de niveau supérieur et peut être considéré comme un cluster de services actif-actif ou actif-en veille. Le routeur logique exécute BGP et des homologues avec des routeurs physiques. Dans le mode actif-en veille, le routeur logique peut également fournir des services avec état.

Routeur logique de niveau 1

Le routeur logique de niveau 1 est le routeur de niveau inférieur qui se connecte à un routeur logique de niveau 0 pour assurer la connectivité vers le nord et à un ou plusieurs réseaux de superposition pour la connectivité vers le sud. Le routeur logique de niveau 1 peut être un cluster actif-en veille de services fournissant des services avec état.

Zone de transport

Ensemble de nœuds de transport qui définit la portée maximale des commutateurs logiques. Une zone de transport représente un ensemble d'hyperviseurs provisionnés de manière similaire et les commutateurs logiques qui connectent les machines virtuelles de ces hyperviseurs.

Nœud de transport

Nœud capable de participer à une mise en réseau de superposition NSX-T Data Center ou VLAN NSX-T Data Center. Pour un hôte KVM, vous pouvez préconfigurer le N-VDS ou laisser à NSX Manager le soin d'effectuer la configuration. Pour un hôte ESXi, NSX Manager configure toujours le N-VDS.

Profil de liaison montante

Définit des stratégies pour les liens des hôtes d'hyperviseur vers les commutateurs logiques NSX-T Data Center ou des nœuds NSX Edge vers les commutateurs ToR (Top-of-Rack). Les paramètres définis par les profils de liaison montante peuvent inclure des règles d'association, des liens actifs/en veille, l'ID du VLAN de transport et le paramètre MTU.

Interface de machine virtuelle (vNIC)

Interface réseau sur une machine virtuelle fournissant une connectivité entre le système d'exploitation invité virtuel et le commutateur standard vSwitch ou vSphere Distributed Switch. La vNIC peut être attachée à un port logique. Vous pouvez identifier une vNIC à l'aide de son identificateur unique (UUID).

Point de terminaison de tunnel virtuel

Permet aux hôtes d'hyperviseur de participer à une superposition NSX-T Data Center. La superposition NSX-T Data Center déploie un réseau de couche 2 au-dessus d'une infrastructure réseau de couche 3 existante en encapsulant des trames à l'intérieur des paquets et en transférant les paquets sur un réseau de transport sous-jacent. Le réseau de transport sous-jacent peut être un autre réseau de couche 2 ou il peut traverser les limites de couche 3. Le VTEP est le point de connexion où l'encapsulation et la décapsulation ont lieu.

Préparation à l'installation

Avant d'installer NSX-T Data Center, assurez-vous que votre environnement est préparé.

Ce chapitre contient les rubriques suivantes :

- [Configuration système requise](#)
- [Ports et protocoles](#)
- [Tâches de haut niveau de l'installation de NSX-T Data Center](#)

Configuration système requise

NSX-T Data Center a des exigences spécifiques concernant les ressources matérielles et les versions logicielles.

Configuration requise pour l'hyperviseur

Hyperviseur	Version	Cœurs de CPU	Mémoire
vSphere	Version de vSphere prise en charge	4	16 Go
RHEL KVM	7.5 et 7.4	4	16 Go
ubuntu KVM	16.04.2 LTS	4	16 Go
CentOS KVM	7.4	4	16 Go

NSX-T Data Center prend en charge la préparation d'hôte sur RHEL 7.5, RHEL 7.4, Ubuntu 16.04 et CentOS 7.4. Le déploiement de NSX Manager et de NSX Controller n'est pas pris en charge sur RHEL 7.5 et CentOS 7.4. Le déploiement de nœud NSX Edge n'est pris en charge que sur vSphere.

Pour les hôtes ESXi, NSX-T Data Center prend en charge les fonctionnalités de profils d'hôte et de déploiement automatique sur vSphere 6.7 U1 ou version supérieure.



Attention Sous RHEL, la commande `yum update` peut mettre à jour la version de noyau et rompre la compatibilité avec NSX-T Data Center. Désactivez la mise à jour de noyau automatique lorsque vous exécutez `yum update`. En outre, après avoir exécuté `yum install`, vérifiez que NSX-T Data Center prend en charge la version du noyau.

Configuration requise du serveur bare metal

Système d'exploitation	Version	Cœurs de CPU	Mémoire
RHEL	7.5 et 7.4	4	16 Go
Ubuntu	16.04.2 LTS	4	16 Go
CentOS	7.4	4	16 Go

Configuration requise pour les ressources NSX Manager

La taille du disque virtuel dynamique est 3.1 Go et celle du disque virtuel statique est 200 Go.

Dispositif	Mémoire	vCPU	Stockage	Version matérielle de machine virtuelle
Petite machine virtuelle NSX Manager	8 Go	2	200 Go	10 ou une version ultérieure
Machine virtuelle moyenne NSX Manager	16 Go	4	200 Go	10 ou une version ultérieure
Machine virtuelle moyenne-grande NSX Manager	24 Go	6	200 Go	10 ou une version ultérieure
Grande machine virtuelle NSX Manager	32 Go	8	200 Go	10 ou une version ultérieure
Machine virtuelle très grande NSX Manager	48 Go	12	200 Go	10 ou une version ultérieure

Note Une petite machine virtuelle NSX Manager doit être utilisée dans les déploiements de laboratoire et de preuve de concept.

Les besoins en ressources NSX Manager s'appliquent au NSX Policy Manager et au Cloud Service Manager.

Configuration requise pour les ressources NSX Controller

Dispositif	Mémoire	vCPU	Espace disque	Type de déploiement
Petite machine virtuelle NSX Controller	8 Go	2	120 Go	Déploiements de laboratoire et de preuve de concept
Machine virtuelle moyenne NSX Controller	16 Go	4	120 Go	Recommandé pour les déploiements de taille moyenne
Grande machine virtuelle NSX Controller	32 Go	8	120 Go	Requis pour les déploiements à grande échelle

Note Déployez trois instances de NSX Controller pour garantir une haute disponibilité et éviter toute interruption du plan de contrôle NSX-T Data Center.

Chaque cluster NSX Controller doit occuper trois hôtes d'hyperviseur physique distincts afin d'éviter qu'une panne d'hôte d'hyperviseur physique ne compromette le bon fonctionnement du plan de contrôle NSX-T Data Center. Consultez le guide *Conception de référence de NSX-T Data Center*.

Pour les déploiements de laboratoire et de preuve de concept sans charge de travail de production, vous pouvez utiliser un seul NSX Controller pour économiser des ressources.

Vous ne pouvez déployer que des machines virtuelles de petites et grandes tailles à partir de l'interface de déploiement OVF de vSphere.

Configuration requise des ressources de machine virtuelle NSX Edge

Taille du déploiement	Mémoire	vCPU	Espace disque	Version matérielle de machine virtuelle
Petite	4 Go	2	120 Go	10 ou version ultérieure (vSphere 5.5 ou version ultérieure)
Moyenne	8 Go	4	120 Go	10 ou version ultérieure (vSphere 5.5 ou version ultérieure)
Grande	16 Go	8	120 Go	10 ou version ultérieure (vSphere 5.5 ou version ultérieure)

Note Pour NSX Manager et NSX Edge, le petit dispositif est destiné aux déploiements de validation technique. Le dispositif moyen est adapté à un environnement de production normal et peut prendre en charge jusqu'à 64 hyperviseurs. Le grand dispositif est destiné aux déploiements à grande échelle avec plus de 64 hyperviseurs.

Note La vNIC VMXNET 3 est prise en charge uniquement pour la machine virtuelle NSX Edge.

Configuration requise de la machine virtuelle NSX Edge et du CPU NSX Edge sans système d'exploitation

Note Les nœuds NSX Edge sont pris en charge uniquement sur les hôtes basés sur ESXi avec des chipsets basés sur Intel. Sinon, le mode EVC de vSphere peut empêcher le démarrage des nœuds Edge, affichant un message d'erreur dans la console.

Pour la prise en charge DPDK, la plate-forme sous-jacente doit disposer de la configuration requise suivante :

- Le CPU doit disposer de la fonctionnalité AES-NI.
- Le CPU doit disposer de la prise en charge d'énormes pages de 1 Go.

Note Comme le plan de données de NSX-T Data Center utilise les fonctions réseau du DPDK (Data Plane Development Kit) d'Intel, seuls les CPU basés sur Intel sont pris en charge.

Matériel	Type
CPU	<ul style="list-style-type: none">■ Xeon 56xx (Westmere-EP)■ Xeon E7-xxxx (Westmere-EX et CPU de génération ultérieure)■ Xeon E5-xxxx (Sandy Bridge et CPU de génération ultérieure)

Exigences matérielles d'un dispositif NSX Edge bare metal

Vérifiez que le matériel du dispositif NSX Edge bare metal est répertorié dans cette URL

<https://certification.ubuntu.com/server/models/?release=16.04%20LTS&category=Server>. Si le matériel n'est pas répertorié, le stockage, l'adaptateur vidéo ou les composants de la carte mère risquent de ne pas fonctionner sur le dispositif NSX Edge.

Configuration requise de la carte réseau spécifique à NSX Edge sans système d'exploitation

Type de carte réseau	Description	ID du périphérique PCI
Intel X520/Intel 82599	IXGBE_DEV_ID_82599_KX4	0x10F7
	IXGBE_DEV_ID_82599_KX4_MEZZ	0x1514
	IXGBE_DEV_ID_82599_KR	0x1517
	IXGBE_DEV_ID_82599_COMBO_BACK PLANE	0x10F8
	IXGBE_DEV_ID_82599_COMBO_BACK PLANE	0x000C
	IXGBE_SUBDEV_ID_82599_KX4_KR_MEZZ	0x10F9
	IXGBE_SUBDEV_ID_82599_KX4_KR_MEZZ	0x10FB
	IXGBE_DEV_ID_82599_CX4	0x11A9
	IXGBE_DEV_ID_82599_SFP	0x1F72
	IXGBE_SUBDEV_ID_82599_SFP	0x17D0
	IXGBE_SUBDEV_ID_82599_RNDC	0x0470
	IXGBE_SUBDEV_ID_82599_560FLR	0x1507
	IXGBE_SUBDEV_ID_82599_ECNA_DP	0x154D
	IXGBE_DEV_ID_82599_SFP_EM	0x154A
	IXGBE_DEV_ID_82599_SFP_SF2	0x1558
	IXGBE_DEV_ID_82599_SFP_SF_QP	0x1557
	IXGBE_DEV_ID_82599_QSFP_SF_QP	0x10FC
	IXGBE_DEV_ID_82599EN_SFP	0x151C
	IXGBE_DEV_ID_82599_XAUI_LOM	
	IXGBE_DEV_ID_82599_T3_LOM	
Intel X540	IXGBE_DEV_ID_X540T	0x1528
	IXGBE_DEV_ID_X540T1	0x1560
Intel X550	IXGBE_DEV_ID_X550T	0x1563
	IXGBE_DEV_ID_X550T1	0x15D1
Intel X710	I40E_DEV_ID_SFP_X710	0x1572
	I40E_DEV_ID_KX_C	0x1581
	I40E_DEV_ID_10G_BASE_T	0x1586
Intel XL710	I40E_DEV_ID_KX_B	0x1580
	I40E_DEV_ID_QSFP_A	0x1583
	I40E_DEV_ID_QSFP_B	0x1584
	I40E_DEV_ID_QSFP_C	0x1585
Cisco VIC 1387	Carte d'interface virtuelle Cisco UCS 1387	0x0043

Configuration requise de mémoire, CPU et disque NSX Edge sans système d'exploitation

Mémoire	Cœurs de CPU	Espace disque
32 Go	8	200 Go

Pilotes de carte réseau de chemin d'accès aux données améliorés

Téléchargez les pilotes de carte réseau pris en charge depuis la page [My VMware](#).

Carte réseau	Pilote de carte réseau
Intel 82599	ixgben 1.1.0.26-1OEM.670.0.0.7535516
Contrôleur Ethernet Intel(R) X710 pour 10GbE SFP+	i40en 1.1.3-1OEM.670.0.0.8169922
Contrôleur Ethernet Intel(R) XL710 pour 40GbE QSFP+	

Prise en charge du navigateur NSX Manager

Navigateur	Windows 10	Windows 8.1	Ubuntu 14.04	Mac OS X 10.11 et 10.12
Internet Explorer 11	Oui	Oui		
Firefox 55			Oui	Oui
Chrome 60	Oui	Oui		Oui
Safari 10				Oui
Microsoft Edge 40	Oui			

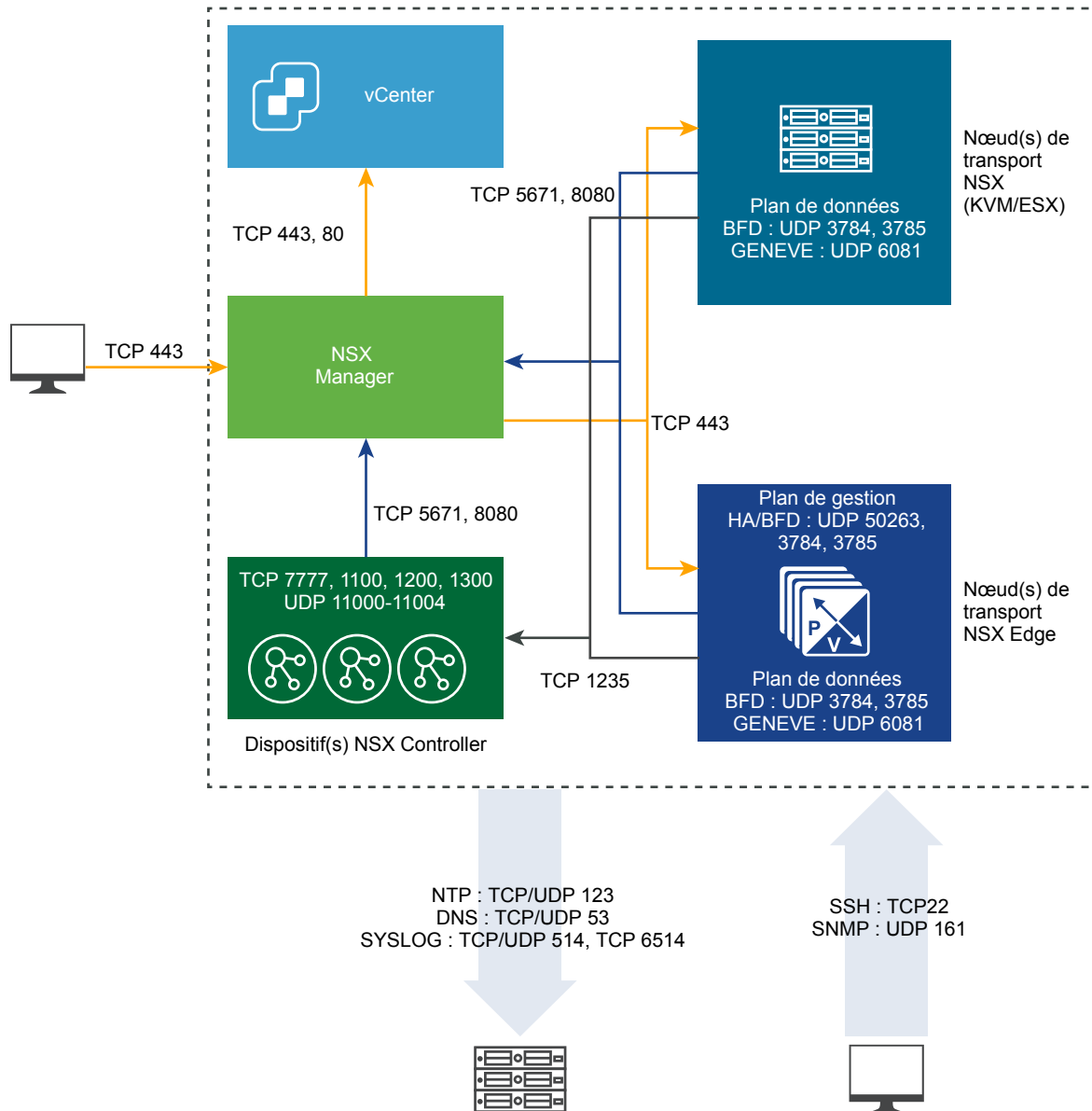
Note Le mode de compatibilité d'Internet Explorer 11 n'est pas pris en charge.

La résolution minimale du navigateur prise en charge est 1 280x800 pixels.

Ports et protocoles

Les ports et les protocoles autorisent les chemins de communication de nœud à nœud dans NSX-T Data Center, les chemins d'accès doivent être sécurisés et authentifiés, et un emplacement de stockage des informations d'identification est utilisé pour établir l'authentification mutuelle.

Chiffre 2-1. Ports et protocoles NSX-T Data Center



Par défaut, tous les certificats sont auto-signés. Les certificats d'interface utilisateur et d'API et les clés privées ascendants peuvent être remplacés par des certificats signés par une autorité de certification.

Il existe des démons internes qui communiquent sur les sockets de bouclage ou de domaine UNIX :

- KVM : MPA, netcpa, nsx-agent, OVS
- ESX : netcpa, ESX-DP (dans le noyau)


Dans la base de données d'utilisateurs RMQ (db), les mots de passe sont hachés avec une fonction de hachage non réversible. $h(p1)$ est la valeur de hachage du mot de passe $p1$.

CCP Plan de contrôle central

LCP Plan de contrôle local

MP	plan de gestion
MPA	Agent du plan de gestion

Note Pour obtenir l'accès aux nœuds NSX-T Data Center, vous devez activer SSH sur ces nœuds.

 **Remarque concernant NSX Cloud** Reportez-vous à la section [Activer l'accès aux ports et protocoles sur CSM pour la connectivité hybride](#) pour obtenir la liste des ports requis pour déployer NSX Cloud.

Ports TCP et UDP utilisés par NSX Manager

NSX Manager utilise certains ports TCP et UDP pour communiquer avec d'autres composants et produits. Ces ports doivent être ouverts dans le pare-feu.

Vous pouvez utiliser un appel d'API ou une commande d'interface de ligne de commande pour spécifier des ports personnalisés pour le transfert de fichiers (la valeur par défaut est 22) et pour l'exportation de données Syslog (les valeurs par défaut sont 514 et 6514). Si vous le faites, vous devez configurer le pare-feu en conséquence.

Tableau 2-1. Ports TCP et UDP utilisés par NSX Manager

Source	Cible	Port	Protocole	Description
Clients de gestion	NSX Manager	22	TCP	SSH (désactivé par défaut)
Serveurs NTP	NSX Manager	123	UDP	NTP
Clients de gestion	NSX Manager	443	TCP	Serveur NSX API
Serveurs SNMP	NSX Manager	161	UDP	SNMP
NSX Controller, nœuds NSX Edge, nœuds de transport, vCenter Server	NSX Manager	8080	TCP	Référentiel HTTP d'installation-mise à niveau
NSX Controller, nœuds NSX Edge, nœuds de transport	NSX Manager	5671	TCP	Messagerie NSX
NSX Manager	Serveurs SCP de gestion	22	TCP	SSH (télécharger le bundle de support, sauvegardes, etc.)
NSX Manager	Serveurs DNS	53	TCP	DNS
NSX Manager	Serveurs DNS	53	UDP	DNS
NSX Manager	Serveurs NTP	123	UDP	NTP
NSX Manager	Serveurs SNMP	161, 162	TCP	SNMP
NSX Manager	Serveurs SNMP	161, 162	UDP	SNMP
NSX Manager	Serveurs Syslog	514	TCP	Syslog
NSX Manager	Serveurs Syslog	514	UDP	Syslog
NSX Manager	Serveurs Syslog	6514	TCP	Syslog

Tableau 2-1. Ports TCP et UDP utilisés par NSX Manager (Suite)

Source	Cible	Port	Protocole	Description
NSX Manager	Serveurs Syslog	6514	UDP	Syslog
NSX Manager	Serveur LogInsight	9000	TCP	Agent Log Insight
NSX Manager	Destination Traceroute	3343 4 - 3352 3	UDP	Traceroute
NSX Manager	vCenter Server	80	TCP	NSX Manager avec les communications du gestionnaire de calcul (vCenter Server), lorsque configuré.
NSX Manager	vCenter Server	443	TCP	NSX Manager avec les communications du gestionnaire de calcul (vCenter Server), lorsque configuré.

Ports TCP et UDP utilisés par NSX Controller

NSX Controller utilise certains ports TCP et UDP pour communiquer avec d'autres composants et produits. Ces ports doivent être ouverts dans le pare-feu.

Vous pouvez utiliser un appel d'API ou une commande d'interface de ligne de commande pour spécifier des ports personnalisés pour le transfert de fichiers (la valeur par défaut est 22) et pour l'exportation de données Syslog (les valeurs par défaut sont 514 et 6514). Si vous le faites, vous devez configurer le pare-feu en conséquence.

Tableau 2-2. Ports TCP et UDP utilisés par NSX Controller

Source	Cible	Port	Protocole	Description
Clients de gestion	NSX Controller	22	TCP	SSH (désactivé par défaut)
Serveurs DNS	NSX Controller	53	UDP	DNS
Serveurs NTP	NSX Controller	123	UDP	NTP
Serveurs SNMP	NSX Controller	161	UDP	SNMP
NSX Controller	NSX Controller	1100	TCP	Quorum Zookeeper
NSX Controller	NSX Controller	1200	TCP	Élection d'un leader Zookeeper
NSX Controller	NSX Controller	1300	TCP	Serveur Zookeeper
Nœuds NSX Edge, nœuds de transport	NSX Controller	1235	TCP	Communication CCP-netcpa
NSX Controller	NSX Controller	7777	TCP	Moot RPC
NSX Controller	NSX Controller	11000 - 11004	UDP	Tunnels vers d'autres nœuds de cluster. Vous devez ouvrir plus de ports si le cluster contient plus de 5 nœuds.
Destination Traceroute	NSX Controller	33434 - 33523	UDP	Traceroute

Tableau 2-2. Ports TCP et UDP utilisés par NSX Controller (Suite)

Source	Cible	Port	Protocole	Description
NSX Controller	Destination SSH	22	TCP	SSH (désactivé par défaut)
NSX Controller	Serveurs DNS	53	UDP	DNS
NSX Controller	Serveurs DNS	53	TCP	DNS
NSX Controller	Serveurs NTP	123	UDP	NTP
NSX Controller	NSX Manager	5671	TCP	Messagerie NSX
NSX Controller	Serveur LogInsight	9000	TCP	Agent Log Insight
NSX Controller	NSX Controller	11000 - 11004	TCP	Tunnels vers d'autres nœuds de cluster. Vous devez ouvrir plus de ports si le cluster contient plus de 5 nœuds.
NSX Controller	NSX Manager	8080	TCP	Mise à niveau de NSX
NSX Controller	Destination Traceroute	33434 - 33523	UDP	Traceroute
NSX Controller	Serveurs Syslog	514	UDP	Syslog
NSX Controller	Serveurs Syslog	514	TCP	Syslog
NSX Controller	Serveurs Syslog	6514	TCP	Syslog

Ports TCP et UDP utilisés par NSX Edge

NSX Edge utilise certains ports TCP et UDP pour communiquer avec d'autres composants et produits. Ces ports doivent être ouverts dans le pare-feu.

Vous pouvez utiliser un appel d'API ou une commande d'interface de ligne de commande pour spécifier des ports personnalisés pour le transfert de fichiers (la valeur par défaut est 22) et pour l'exportation de données Syslog (les valeurs par défaut sont 514 et 6514). Si vous le faites, vous devez configurer le pare-feu en conséquence.

Tableau 2-3. Ports TCP et UDP utilisés par NSX Edge

Source	Cible	Port	Protocole	Description
Clients de gestion	Nœuds NSX Edge	22	TCP	SSH (désactivé par défaut)
Serveurs NTP	Nœuds NSX Edge	123	UDP	NTP
Serveurs SNMP	Nœuds NSX Edge	161	UDP	SNMP
Nœuds NSX Edge	Nœuds NSX Edge	1167	TCP	DHCP principal
Nœuds NSX Edge, nœuds de transport	Nœuds NSX Edge	3784, 3785	UDP	BFD entre l'adresse IP TEP du nœud de Transport dans les données.
Agent NSX	Nœuds NSX Edge	5555	TCP	NSX Cloud - Agent sur l'instance communique avec la passerelle de NSX Cloud.

Tableau 2-3. Ports TCP et UDP utilisés par NSX Edge (Suite)

Source	Cible	Port	Protocole	Description
Nœuds NSX Edge	Nœuds NSX Edge	6666	TCP	NSX Cloud - communications locales NSX Edge.
Nœuds NSX Edge	NSX Manager	8080	TCP	NAPI, mise à niveau de NSX-T Data Center
Nœuds NSX Edge	Nœuds NSX Edge	2480	TCP	Nestdb
Nœuds NSX Edge	Serveurs SCP ou SSH de gestion	22	TCP	SSH
Nœuds NSX Edge	Serveurs DNS	53	UDP	DNS
Nœuds NSX Edge	Serveurs NTP	123	UDP	NTP
Nœuds NSX Edge	Serveurs SNMP	161, 162	UDP	SNMP
Nœuds NSX Edge	Serveurs SNMP	161, 162	TCP	SNMP
Nœuds NSX Edge	NSX Manager	443	TCP	HTTPS
Nœuds NSX Edge	Serveurs Syslog	514	TCP	Syslog
Nœuds NSX Edge	Serveurs Syslog	514	UDP	Syslog
Nœuds NSX Edge	Nœuds NSX Edge	1167	TCP	DHCP principal
Nœuds NSX Edge	NSX Controller	1235	TCP	netcpa
Nœuds NSX Edge	Serveur d'API OpenStack Nova	3000 - 9000	TCP	Proxy de métadonnées
Nœuds NSX Edge	NSX Manager	5671	TCP	Messagerie NSX
Nœuds NSX Edge	Serveurs Syslog	6514	TCP	Syslog sur TLS
Nœuds NSX Edge	Destination Traceroute	33434 - 33523	UDP	Traceroute
Nœuds NSX Edge	Nœuds NSX Edge	50263	UDP	Haute disponibilité

Ports TCP et UDP utilisés par vSphere ESXi , les hôtes KVM et le serveur Bare Metal

Lorsque vSphere ESXi, les hôtes KVM et le serveur Bare Metal servent de nœuds de transport, certains ports TCP et UDP doivent être disponibles.

Tableau 2-4. Ports TCP et UDP utilisés par les hôtes vSphere ESXi et KVM

Source	Cible	Port	Protocole	Description
NSX Manager	Hôte vSphere ESXi	443	TCP	Connexion de gestion et de provisionnement
NSX Manager	Hôte KVM	443	TCP	Connexion de gestion et de provisionnement
Hôte vSphere ESXi	NSX Manager	567 1	TCP	Canal de communication AMQP vers NSX Manager
Hôte vSphere ESXi	NSX Controller	123 5	TCP	Plan de contrôle - Communication LCP à CCP
Hôte KVM	NSX Manager	567 1	TCP	Canal de communication AMQP vers NSX Manager
Hôte KVM	NSX Controller	123 5	TCP	Plan de contrôle - Communication LCP à CCP
Hôte vSphere ESXi	NSX Manager	808 0	TCP	Installer et mettre à niveau le référentiel HTTP
Hôte KVM	NSX Manager	808 0	TCP	Installer et mettre à niveau le référentiel HTTP
Point de terminaison de résiliation (Termination End Point, TEP) GENEVE	Point de terminaison de résiliation (Termination End Point, TEP) GENEVE	608 1	UDP	Réseau de transport
Nœud de transport NSX-T Data Center	Nœud de transport NSX-T Data Center	378 4, 378 5	UDP	Session BFD entre les TEP, dans le chemin de données, à l'aide de l'interface TEP

Tâches de haut niveau de l'installation de NSX-T Data Center

Utilisez la liste de contrôle pour suivre l'avancée de l'installation.

Suivez l'ordre des procédures recommandé.

- 1 Installez NSX Manager, reportez-vous à [Chapitre 4 Installation de NSX Manager](#).
- 2 Installez des NSX Controller, reportez-vous à [Chapitre 5 Installation et mise en cluster de NSX Controller](#).
- 3 Reliez les dispositifs NSX Controller au plan de gestion, reportez-vous à [Joindre des dispositifs NSX Controller à NSX Manager](#).
- 4 Créez un NSX Controller maître pour initialiser le cluster de contrôle, reportez-vous à [Initialiser le cluster de contrôle pour créer un maître de cluster de contrôle](#).
- 5 Associez les dispositifs NSX Controller à un cluster de contrôle, reportez-vous à [Relier les dispositifs NSX Controller au maître de cluster](#).

NSX Manager installe des modules NSX-T Data Center après avoir ajouté les hôtes d'hyperviseur.

Note Des certificats sont créés sur les hôtes d'hyperviseur lors de la création de modules NSX-T Data Center.

- 6 Reliez les hôtes d'hyperviseur au plan de gestion, reportez-vous à [Relier les hôtes d'hyperviseur au plan de gestion](#).

L'hôte envoie alors son certificat d'hôte au plan de gestion.

- 7 Installez des dispositifs NSX Edge, reportez-vous à la section [Chapitre 6 Installation de NSX Edge](#).
- 8 Reliez les dispositifs NSX Edge au plan de gestion, reportez-vous à [Relier NSX Edge au plan de gestion](#).
- 9 Créez des zones de transport et des nœuds de transport, reportez-vous à [Chapitre 8 Zones de transport et nœuds de transport](#).

Un commutateur virtuel est créé sur chaque hôte. Le plan de gestion envoie les certificats d'hôte au plan de contrôle et le plan de gestion transfère les informations du plan de contrôle aux hôtes. Chaque hôte se connecte au plan de contrôle à l'aide de SSL en présentant son certificat. Le plan de contrôle valide le certificat en le comparant au certificat d'hôte fourni par le plan de gestion. Les contrôleurs acceptent la connexion lorsque la validation est effective.

L'ordre d'installation normal est le suivant :

- 1 NSX Manager est installé en premier.
- 2 NSX Controller peut être installé et joindre le plan de gestion.
- 3 Les modules NSX-T Data Center peuvent être installés sur un hôte d'hyperviseur avant de relier celui-ci au plan de gestion. Vous pouvez également effectuer les deux procédures simultanément à l'aide des options de menu **Infrastructure > Hôtes > Ajouter**.
- 4 Les dispositifs NSX Controller, NSX Edge et les hôtes dotés de modules NSX-T Data Center peuvent joindre le plan de gestion à tout moment.

Post-installation

Lorsque les hôtes sont des nœuds de transport, vous pouvez créer des zones de transport, des commutateurs logiques, des routeurs logiques et d'autres composants réseau par le biais de l'interface utilisateur ou de l'API NSX Manager à tout moment. Lorsque des dispositifs NSX Controller, NSX Edge et des hôtes se joignent au plan de gestion, les entités logiques NSX-T Data Center et l'état de configuration sont transférés automatiquement vers ces dispositifs NSX Controller, NSX Edge et hôtes.

Pour plus d'informations, reportez-vous à *Guide d'administration de NSX-T Data Center*.

Utilisation de KVM

NSX-T Data Center prend en charge KVM de deux façons : 1) en tant que nœud de transport hôte et 2) en tant qu'hôte pour NSX Manager et NSX Controller.

Tableau 3-1. Versions de KVM prises en charge

Exigences	Description
Plates-formes prises en charge	<ul style="list-style-type: none">■ RHEL 7.5■ RHEL 7.4■ Ubuntu 16.04.2 LTS■ CentOS 7.4

Ce chapitre contient les rubriques suivantes :

- [Configurer KVM](#)
- [Gérer vos machines virtuelles invitées dans l'interface de ligne de commande de KVM](#)

Configurer KVM

Si vous souhaitez utiliser KVM en tant que nœud de transport ou en tant qu'hôte pour les machines virtuelles invitées NSX Manager et NSX Controller, mais que vous n'avez pas encore configuré KVM, vous pouvez utiliser la procédure ci-dessous.

Note Le protocole d'encapsulation Geneve utilise le port UDP 6081. Vous devez autoriser cet accès de port dans le pare-feu sur l'hôte KVM.

Procédure

- 1 (Red Hat uniquement) Ouvrez le fichier `/etc/yum.conf`.
- 2 Recherchez la ligne `exclude`.
- 3 Ajoutez la ligne `"kernel* redhat-release"` pour configurer yum afin d'éviter les mises à niveau RHEL non prises en charge.
`exclude=[existing list] kernel* redhat-release*`

Si vous prévoyez d'exécuter NSX-T Container Plug-in, qui a des exigences de compatibilité spécifiques, excluez les modules associés aux conteneurs.

```
exclude=[existing list] kernel* redhat-release* kubelet-* kubeadm-* kubectl-*
docker-*
```

La version prise en charge est RHEL 7.4.

4 Installez KVM et les utilitaires de pont.

Distribution Linux	Commandes
Ubuntu	<pre>apt-get install -y qemu-kvm libvirt-bin ubuntu-vm-builder bridge-utils virtinst virt-manager virt-viewer libguestfs-tools</pre>
RHEL	<pre>yum groupinstall "Virtualization Hypervisor" yum groupinstall "Virtualization Client" yum groupinstall "Virtualization Platform" yum groupinstall "Virtualization Tools"</pre>

5 Vérifiez la capacité de virtualisation matérielle.

```
cat /proc/cpuinfo | egrep "vmx|svm"
```

La sortie doit contenir vmx.

6 Vérifiez que le module KVM est installé.

Distribution Linux	Commandes
Ubuntu	<pre>kvm-ok</pre> <p>INFO: /dev/kvm exists KVM acceleration can be used</p>
RHEL	<pre>lsmod grep kvm</pre> <pre>kvm_intel 53484 6 kvm 316506 1 kvm_intel</pre>

- 7 Pour que KVM soit utilisé en tant qu'hôte pour NSX Manager ou NSX Controller, préparez le réseau de pont, l'interface de gestion et les interfaces de carte réseau.

Dans l'exemple suivant, la première interface Ethernet (eth0 ou ens32) est utilisée pour la connectivité vers la machine Linux elle-même. Selon votre environnement de déploiement, cette interface peut utiliser des paramètres DHCP ou IP statiques. Avant d'attribuer des interfaces de liaison montante aux hôtes NSX-T, assurez-vous que les scripts d'interface utilisés par ces liaisons montantes sont déjà configurés. Sans ces fichiers d'interface sur le système, vous ne pouvez pas réussir à créer un nœud de transport hôte.

Note Les noms d'interface peuvent varier selon les environnements.

Distribution	Configuration réseau
Linux	
Ubuntu	<p>Modifiez /etc/network/interfaces :</p> <pre> auto lo iface lo inet loopback auto eth0 iface eth0 inet manual auto br0 iface br0 inet static address 192.168.110.51 netmask 255.255.255.0 network 192.168.110.0 broadcast 192.168.110.255 gateway 192.168.110.1 dns-nameservers 192.168.3.45 dns-search example.com bridge_ports eth0 bridge_stp off bridge_fd 0 bridge_maxwait 0 </pre> <p>Créez un fichier xml de définition de réseau pour le pont. Par exemple, créez /tmp/bridge.xml avec les lignes suivantes :</p> <pre> <network> <name>bridge</name> <forward mode='bridge' /> <bridge name='br0' /> </network> </pre> <p>Définissez et démarrez le réseau de pont avec les commandes suivantes :</p> <pre> virsh net-define bridge.xml virsh net-start bridge virsh net-autostart bridge </pre>

Distribution

Linux

Configuration réseau

Vous pouvez vérifier l'état du réseau de pont avec la commande suivante :

```
virsh net-list --all
```

Name	State	Autostart	Persistent
bridge	active	yes	yes
default	active	yes	yes

RHEL

Modifiez /etc/sysconfig/network-scripts/ifcfg-management_interface :

```
DEVICE="ens32"
TYPE="Ethernet"
NAME="ens32"
UUID="<UUID>"
BOOTPROTO="none"
HWADDR="<HWADDR>"
ONBOOT="yes"
NM_CONTROLLED="no"
BRIDGE="br0"
```

Modifiez /etc/sysconfig/network-scripts/ifcfg-eth1 :

```
DEVICE="eth1"
TYPE="Ethernet"
NAME="eth1"
UUID="<UUID>"
BOOTPROTO="none"
HWADDR="<HWADDR>"
ONBOOT="yes"
NM_CONTROLLED="no"
```

Modifiez /etc/sysconfig/network-scripts/ifcfg-eth2 :

```
DEVICE="eth2"
TYPE="Ethernet"
NAME="eth2"
UUID="<UUID>"
BOOTPROTO="none"
HWADDR="<HWADDR>"
ONBOOT="yes"
NM_CONTROLLED="no"
```

Modifiez /etc/sysconfig/network-scripts/ifcfg-br0 :

```
DEVICE="br0"
BOOTPROTO="dhcp"
NM_CONTROLLED="no"
ONBOOT="yes"
TYPE="Bridge"
```

8 Pour utiliser KVM en tant que nœud de transport, préparez le pont réseau.

Dans l'exemple suivant, la première interface Ethernet (eth0 ou ens32) est utilisée pour la connectivité vers la machine Linux elle-même. Selon votre environnement de déploiement, cette interface peut utiliser des paramètres DHCP ou IP statiques.

Note Les noms d'interface peuvent varier selon les environnements.

Distribution Linux	Configuration réseau
Ubuntu	<p>Modifiez /etc/network/interfaces :</p> <pre> auto lo iface lo inet loopback auto eth0 iface eth0 inet manual auto eth1 iface eth1 inet manual auto br0 iface br0 inet dhcp bridge_ports eth0 </pre>
RHEL	<p>Modifiez /etc/sysconfig/network-scripts/ifcfg-ens32 :</p> <pre> DEVICE="ens32" TYPE="Ethernet" NAME="ens32" UUID="<something>" BOOTPROTO="none" HWADDR="<something>" ONBOOT="yes" NM_CONTROLLED="no" BRIDGE="br0" </pre> <p>Modifiez /etc/sysconfig/network-scripts/ifcfg-ens33 :</p> <pre> DEVICE="ens33" TYPE="Ethernet" NAME="ens33" UUID="<something>" BOOTPROTO="none" HWADDR="<something>" ONBOOT="yes" NM_CONTROLLED="no" </pre> <p>Modifiez /etc/sysconfig/network-scripts/ifcfg-br0 :</p> <pre> DEVICE="br0" BOOTPROTO="dhcp" NM_CONTROLLED="no" ONBOOT="yes" TYPE="Bridge" </pre>

Important Pour Ubuntu, toutes les configurations réseau doivent figurer dans `/etc/network/interfaces`. Ne créez pas de fichiers de configuration réseau individuels, tels que `/etc/network/ifcfg-eth1`, car cela pourrait entraîner l'échec de la création du nœud de transport.

Après cette étape, une fois que l'hôte KVM est configuré comme nœud de transport, l'interface de pont « `nsx-vtep0.0` » est créée. Dans Ubuntu, `/etc/network/interfaces` possède des entrées similaires à celles-ci :

```
iface nsx-vtep0.0 inet static
pre-up ip addr flush dev nsx-vtep0.0
address <IP_pool_address>
netmask <subnet_mask>
mtu 1600
down ifconfig nsx-vtep0.0 down
up ifconfig nsx-vtep0.0 up
```

Dans RHEL, l'agent NSX hôte (nsxa) crée un fichier de configuration appelé `ifcfg-nsx-vtep0.0`, qui contient des entrées similaires à celles-ci :

```
DEVICE=nsx-vtep0.0
BOOTPROTO=static
NETMASK=<IP address>
IPADDR=<subnet mask>
MTU=1600
ONBOOT=yes
USERCTL=no
NM_CONTROLLED=no
```

- 9 Pour que les modifications réseau prennent effet, redémarrez le service de mise en réseau `systemctl restart network` ou redémarrez le serveur Linux.

Gérer vos machines virtuelles invitées dans l'interface de ligne de commande de KVM

NSX Manager et NSX Controller peuvent être installés en tant que machines virtuelles KVM. En outre, KVM peut être utilisé comme hyperviseur des nœuds de transport NSX-T Data Center.

La gestion des machines virtuelles invitées KVM n'est pas traitée dans ce guide. Cependant, voici quelques commandes simples de l'interface de ligne de commande de KVM pour commencer.

Pour gérer vos machines virtuelles invitées dans l'interface de ligne de commande de KVM, vous pouvez utiliser les commandes `virsh`. Voici quelques commandes `virsh` courantes. Reportez-vous à la documentation de KVM pour plus d'informations.

```
# List running
virsh list

# List all
virsh list --all
```

```
# Control instances
virsh start <instance>
virsh shutdown <instance>
virsh destroy <instance>
virsh undefine <instance>
virsh suspend <instance>
virsh resume <instance>

# Access an instance's CLI
virsh console <instance>
```

Dans l'interface de ligne de commande Linux, la commande `ifconfig` affiche l'interface `vnetX`, qui représente l'interface créée pour la machine virtuelle invitée. Si vous ajoutez des machines virtuelles invitées supplémentaires, ajoutez des interfaces `vnetX`.

```
ifconfig
...

vnet0    Link encap:Ethernet  HWaddr fe:54:00:b0:a0:6d
          inet6 addr: fe80::fc54:ff:feb0:a06d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13183 errors:0 dropped:0 overruns:0 frame:0
          TX packets:181524 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:4984832 (4.9 MB)  TX bytes:29498709 (29.4 MB)
```

Installation de NSX Manager

NSX Manager fournit l'interface utilisateur graphique (GUI) et les API REST pour la création, la configuration et la surveillance de composants NSX-T Data Center, par exemple, des commutateurs logiques, des routeurs logiques et des pare-feu.

NSX Manager fournit une vue du système et constitue le composant de gestion de NSX-T Data Center.

Un déploiement de NSX-T Data Center ne peut avoir qu'une seule instance de NSX Manager. Si NSX Manager est déployé sur un hôte ESXi, vous pouvez utiliser la fonctionnalité de haute disponibilité (HA) vSphere pour garantir la disponibilité de NSX Manager.

Tableau 4-1. Exigences du déploiement, de la plate-forme et de l'installation de NSX Manager

Exigences	Description
Méthodes de déploiement prises en charge	<ul style="list-style-type: none"> ■ OVA/OVF ■ QCOW2
Plates-formes prises en charge	<p>Reportez-vous à la section Configuration système requise.</p> <p>Sous ESXi, il est recommandé d'installer le dispositif NSX Manager sur un stockage partagé. vSphere HA nécessite un stockage partagé afin que les machines virtuelles puissent être redémarrées sur un autre hôte si l'hôte d'origine est en panne.</p>
Adresse IP	Un système NSX Manager doit posséder une adresse IP statique. Vous ne pouvez pas modifier l'adresse IP après l'installation.
Mot de passe du dispositif NSX-T Data Center	<ul style="list-style-type: none"> ■ Au moins huit caractères ■ Au moins une lettre minuscule ■ Au moins une lettre majuscule ■ Au moins un chiffre ■ Au moins un caractère spécial ■ Au moins cinq caractères différents ■ Aucun mot issu du dictionnaire ■ Aucun palindrome
Nom d'hôte	<p>Lorsque vous installez NSX Manager, spécifiez un nom d'hôte qui ne contient pas de caractères non valides comme un caractère de soulignement. Si le nom d'hôte contient un caractère non valide, après le déploiement, le nom d'hôte sera défini sur nsx-manager. Pour plus d'informations sur les restrictions de nom d'hôte, reportez-vous à https://tools.ietf.org/html/rfc952 et https://tools.ietf.org/html/rfc1123.</p>
VMware Tools	VMTools est installé sur la machine virtuelle NSX Manager exécutée sur ESXi. Ne supprimez pas ou ne mettez pas VMTools à niveau.

Tableau 4-1. Exigences du déploiement, de la plate-forme et de l'installation de NSX Manager (Suite)

Exigences	Description
Système	<ul style="list-style-type: none"> ■ Vérifiez que la configuration requise est respectée. Reportez-vous à la section Configuration système requise. ■ Vérifiez que les ports requis sont ouverts. Reportez-vous à la section Ports et protocoles. ■ Créez le réseau du groupe de ports de machines virtuelles cible, si celui-ci n'existe pas déjà. Il est recommandé de placer les dispositifs NSX-T Data Center sur un réseau de machines virtuelles de gestion. <p>Si vous disposez de plusieurs réseaux de gestion, vous pouvez ajouter des itinéraires statiques aux autres réseaux à partir du dispositif NSX-T Data Center.</p> <ul style="list-style-type: none"> ■ Planifiez votre schéma d'adresses IP IPv4. Dans cette version de NSX-T Data Center, IPv6 n'est pas pris en charge.
Privilèges OVF	<p>Vérifiez que vous disposez des privilèges appropriés pour déployer un modèle OVF sur l'hôte ESXi.</p> <p>Un outil de gestion pouvant déployer des modèles OVF, tels que vCenter Server ou vSphere Client. L'outil de déploiement de modèles OVF doit prendre en charge des options de configuration qui permettent la configuration manuelle.</p> <p>La version de l'outil OVF doit être la 4.0 ou une version ultérieure.</p>
Plug-in client	Le plug-in d'intégration du client doit être installé.

Note Lors d'une nouvelle installation de NSX Manager, d'un redémarrage ou après la modification du mot de passe **admin** à la première connexion, le démarrage de NSX Manager peut prendre plusieurs minutes.

Scénarios d'installation de NSX Manager

Important Lorsque vous installez NSX Manager à partir d'un fichier OVA ou OVF, depuis vSphere Web Client ou depuis la ligne de commande, les valeurs de propriété OVA/OVF, telles que les noms d'utilisateur, les mots de passe ou les adresses IP, ne sont pas validées avant la mise sous tension de la machine virtuelle.

- Si vous spécifiez un nom d'utilisateur pour l'utilisateur **admin** ou **audit**, le nom doit être unique. Si vous spécifiez le même nom, il est ignoré et les noms par défaut (**admin** et **audit**) sont utilisés.
- Si le mot de passe de l'utilisateur **admin** ne répond pas aux exigences de complexité, vous devez vous connecter à NSX Manager via SSH ou à la console en tant qu'utilisateur **admin**. Vous êtes invité à modifier le mot de passe.
- Si le mot de passe de l'utilisateur **audit** ne respecte pas les exigences de complexité, le compte d'utilisateur est désactivé. Pour activer le compte, connectez-vous à NSX Manager via SSH ou à la console en tant qu'utilisateur **admin** et exécutez la commande **set user audit** pour définir le mot de passe de l'utilisateur **audit** (le mot de passe actuel est une chaîne vide).

- Si le mot de passe de l'utilisateur **racine** ne respecte pas les exigences de complexité, vous devez vous connecter à NSX Manager via SSH ou à la console en tant que **racine** avec le mot de passe **vmware**. Vous êtes invité à modifier le mot de passe.



Attention Les modifications apportées à NSX-T Data Center tout en étant connecté avec les informations d'identification de l'utilisateur **racine** peuvent provoquer la défaillance du système et avoir éventuellement un impact sur votre réseau. Vous pouvez uniquement apporter des modifications à l'aide des informations d'identification de l'utilisateur **racine** en suivant les instructions de l'équipe de support de VMware.

Note Sur le dispositif, les services de base ne démarrent pas tant qu'un mot de passe suffisamment complexe n'est pas défini.

Après avoir déployé NSX Manager à partir d'un fichier OVA, vous ne pouvez pas modifier les paramètres IP de la machine virtuelle en mettant la machine virtuelle hors tension, puis en modifiant les paramètres OVA de vCenter Server.

Ce chapitre contient les rubriques suivantes :

- [Installer NSX Manager et les dispositifs disponibles](#)
- [Installer NSX Manager sur ESXi à l'aide de l'outil OVF de ligne de commande](#)
- [Installer NSX Manager sur KVM](#)
- [Se connecter à l'instance de NSX Manager qui vient d'être créée](#)

Installer NSX Manager et les dispositifs disponibles

Vous pouvez utiliser vSphere Web Client pour déployer NSX Manager, NSX Policy Manager ou Cloud Service Manager en tant que dispositif virtuel.

NSX Policy Manager est un dispositif virtuel qui vous permet de gérer des stratégies. Vous pouvez configurer des stratégies pour spécifier des règles pour les composants de NSX-T Data Center, tels que des ports logiques, des adresses IP et des machines virtuelles. Les règles NSX Policy Manager vous autorisent à définir des règles d'utilisation et d'accès aux ressources de niveau supérieur qui sont appliquées sans spécifier de détails exacts.

Cloud Service Manager est un dispositif virtuel qui utilise les composants NSX-T Data Center et les intègre dans votre Cloud public.

Note Il est recommandé d'utiliser vSphere Web Client plutôt que vSphere Client. Si votre environnement n'est pas doté de vCenter Server, utilisez la commande `ovftool` pour déployer NSX Manager. Reportez-vous à la section [Installer NSX Manager sur ESXi à l'aide de l'outil OVF de ligne de commande](#).

Procédure

- 1 Localisez le fichier OVA ou OVF de NSX-T Data Center Unified Appliance.

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

- 2 Dans vSphere Web Client, lancez l'assistant **Déployer un modèle OVF**, puis accédez au fichier .ova ou à un lien vers ce fichier.

- 3 Entrez un nom pour le dispositif NSX Manager, puis sélectionnez un dossier ou un centre de données.

Le nom saisi s'affiche dans l'inventaire.

Le dossier que vous sélectionnez sera utilisé pour appliquer des autorisations au dispositif NSX Manager.

- 4 Sélectionnez une banque de données pour stocker les fichiers du dispositif virtuel NSX Manager.
- 5 Si vous effectuez une installation dans vCenter, sélectionnez un hôte ou un cluster sur lequel déployer le dispositif NSX Manager.
- 6 Sélectionnez le groupe de ports ou le réseau de destination du dispositif NSX Manager.
- 7 Spécifiez les mots de passe et les paramètres IP du dispositif NSX Manager.
- 8 Acceptez le rôle **nsx-manager**.

- Sélectionnez le rôle **nsx-policy-manager** dans le menu déroulant pour installer le dispositif NSX Policy Manager.
- Sélectionnez le rôle **nsx-cloud-service-manager** dans le menu déroulant pour installer le dispositif NSX Cloud.

Note Le rôle **nsx-manager nsx-cloud-service-manager (rôles multiples)** n'est pas pris en charge.

- 9 (Facultatif) Pour des performances optimales, réservez de la mémoire pour le composant NSX-T Data Center.

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 sur un niveau qui garantit que le composant NSX-T Data Center dispose de suffisamment de mémoire pour s'exécuter efficacement. Reportez-vous à la section [Configuration système requise](#).

- 10 Ouvrez la console du composant NSX-T Data Center pour suivre le processus de démarrage.
- 11 Dès que le composant NSX-T Data Center a démarré, connectez-vous à l'interface de ligne de commande en tant qu'administrateur et exécutez la commande `get interface eth0` pour vérifier que l'adresse IP a été appliquée comme prévu.

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```


12 Vérifiez que votre composant NSX-T Data Center dispose de la connectivité requise.

Assurez-vous que vous pouvez effectuer les tâches suivantes.

- Effectuer un test ping de votre composant NSX-T Data Center à partir d'une autre machine.
- Le composant NSX-T Data Center peut effectuer un test ping de sa passerelle par défaut.
- Le composant NSX-T Data Center peut effectuer un test ping des hôtes d'hyperviseur qui se trouvent dans le même réseau que le composant NSX-T Data Center à l'aide de l'interface de gestion.
- Le composant NSX-T Data Center peut effectuer un test ping de son serveur DNS et de son serveur NTP.
- Si vous avez activé le protocole SSH, assurez-vous de pouvoir l'utiliser avec votre composant NSX-T Data Center.

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

Étape suivante

Connectez-vous à l'interface graphique utilisateur NSX Manager à partir d'un navigateur Web pris en charge.

L'URL est `https://<adresse IP de NSX Manager>`. Par exemple, `https://10.16.176.10`.

Note Vous devez utiliser HTTPS. HTTP n'est pas pris en charge.

Installer NSX Manager sur ESXi à l'aide de l'outil OVF de ligne de commande

Si vous préférez automatiser ou utiliser l'interface de ligne de commande pour l'installation de NSX Manager, vous pouvez utiliser l'outil OVF de VMware, qui est un utilitaire de ligne de commande.

Par défaut, `nsx_isSSHEnabled` et `nsx_allowSSHRootLogin` sont tous deux désactivés pour des raisons de sécurité. Lorsqu'ils sont désactivés, vous ne pouvez pas utiliser SSH ou vous connecter à la ligne de commande NSX Manager. Si vous activez `nsx_isSSHEnabled` mais pas `nsx_allowSSHRootLogin`, vous pouvez utiliser SSH avec NSX Manager, mais ne pouvez pas vous connecter en tant qu'utilisateur racine.

Conditions préalables

- Vérifiez que la configuration requise est respectée. Reportez-vous à la section [Configuration système requise](#).
- Vérifiez que les ports requis sont ouverts. Reportez-vous à la section [Ports et protocoles](#).
- Créez le réseau du groupe de ports de machines virtuelles cible, si celui-ci n'existe pas déjà. Il est recommandé de placer les dispositifs NSX-T Data Center sur un réseau de machines virtuelles de gestion.

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

- Planifiez votre schéma d'adresses IP IPv4. Dans cette version de NSX-T Data Center, IPv6 n'est pas pris en charge.

Procédure

- Pour un hôte autonome, exécutez la commande `ovftool` avec les paramètres appropriés.

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-manager
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--net="management"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_role=nsx-manager
--prop:nsx_ip_0=192.168.110.75
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=<True|False>
--prop:nsx_allowSSHRootLogin=<True|False>
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-manager
nsx-<component>.ova
vi://root:<password>@192.168.110.51
```

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://root:<password>@192.168.110.51
Deploying to VI: vi://root:<password>@192.168.110.51
Transfer Completed
Powering on VM: nsx-manager
Task Completed
Completed successfully
```

- Pour un hôte géré par vCenter Server, exécutez la commande `ovftool` avec les paramètres appropriés. Par exemple,

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-manager
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--network="management"
```

```

--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_role=nsx-manager
--prop:nsx_ip_0=192.168.110.75
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=<True|False>
--prop:nsx_allowSSHRootLogin=<True|False>
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-manager
nsx-<component>.ova
vi://administrator@vsphere.local:<password>@192.168.110.24/?ip=192.168.110.51

```

```

Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://administrator@vsphere.local@192.168.110.24:443/
Deploying to VI: vi://administrator@vsphere.local@192.168.110.24:443/
Transfer Completed
Powering on VM: nsx-manager
Task Completed
Completed successfully

```

- (Facultatif) Pour des performances optimales, réservez de la mémoire pour le composant NSX-T Data Center.

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 sur un niveau qui garantit que le composant NSX-T Data Center dispose de suffisamment de mémoire pour s'exécuter efficacement. Reportez-vous à la section [Configuration système requise](#).

- Ouvrez la console du composant NSX-T Data Center pour suivre le processus de démarrage.
- Dès que le composant NSX-T Data Center a démarré, connectez-vous à l'interface de ligne de commande en tant qu'administrateur et exécutez la commande `get interface eth0` pour vérifier que l'adresse IP a été appliquée comme prévu.

```

nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...

```

- Vérifiez que votre composant NSX-T Data Center dispose de la connectivité requise.

Assurez-vous que vous pouvez effectuer les tâches suivantes.

- Effectuer un test ping de votre composant NSX-T Data Center à partir d'une autre machine.
- Le composant NSX-T Data Center peut effectuer un test ping de sa passerelle par défaut.
- Le composant NSX-T Data Center peut effectuer un test ping des hôtes d'hyperviseur qui se trouvent dans le même réseau que le composant NSX-T Data Center à l'aide de l'interface de gestion.
- Le composant NSX-T Data Center peut effectuer un test ping de son serveur DNS et de son serveur NTP.
- Si vous avez activé le protocole SSH, assurez-vous de pouvoir l'utiliser avec votre composant NSX-T Data Center.

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

Étape suivante

Connectez-vous à l'interface graphique utilisateur NSX Manager à partir d'un navigateur Web pris en charge.

L'URL est `https://<adresse IP de NSX Manager>`. Par exemple, `https://10.16.176.10`.

Note Vous devez utiliser HTTPS. HTTP n'est pas pris en charge.

Installer NSX Manager sur KVM

NSX Manager peut être installé en tant que dispositif virtuel sur un hôte KVM.

La procédure d'installation de QCOW2 utilise `guestfish`, un outil de ligne de commande Linux qui permet d'écrire des paramètres de machine virtuelle dans le fichier QCOW2.

Conditions préalables

- KVM configuré. Reportez-vous à la section [Configurer KVM](#).
- Privilèges pour le déploiement d'une image QCOW2 sur l'hôte KVM.
- Vérifiez que le mot de passe dans le fichier `guestinfo` respecte les exigences de complexité du mot de passe afin de pouvoir vous connecter après l'installation. Reportez-vous à la section [Chapitre 4 Installation de NSX Manager](#).

Procédure

- 1 Téléchargez l'image QCOW2 de NSX Manager et copiez-la sur la machine KVM qui exécute NSX Manager à l'aide de SCP ou de la synchronisation.

- 2 (Ubuntu uniquement) Ajoutez l'utilisateur connecté en tant qu'utilisateur libvirt :

```
adduser $USER libvirt
```

- 3 Dans le répertoire où vous avez enregistré l'image QCOW2, créez un fichier appelé guestinfo (sans extension de fichier) et remplissez-le avec les propriétés de la machine virtuelle NSX Manager.

Par exemple :

```
<?xml version="1.0" encoding="UTF-8"?>
<Environment
  xmlns="http://schemas.dmtf.org/ovf/environment/1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:oe="http://schemas.dmtf.org/ovf/environment/1">
  <PropertySection>
    <Property oe:key="nsx_role" oe:value="nsx-manager"/>
    <Property oe:key="nsx_allowSSHRootLogin" oe:value="True"/>
    <Property oe:key="nsx_cli_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_dns1_0" oe:value="192.168.110.10"/>
    <Property oe:key="nsx_domain_0" oe:value="corp.local"/>
    <Property oe:key="nsx_gateway_0" oe:value="192.168.110.1"/>
    <Property oe:key="nsx_hostname" oe:value="nsx-manager1"/>
    <Property oe:key="nsx_ip_0" oe:value="192.168.110.19"/>
    <Property oe:key="nsx_isSSHEnabled" oe:value="True"/>
    <Property oe:key="nsx_netmask_0" oe:value="255.255.255.0"/>
    <Property oe:key="nsx_ntp_0" oe:value="192.168.110.10"/>
    <Property oe:key="nsx_passwd_0" oe:value="<password>"/>
  </PropertySection>
</Environment>
```

Dans cet exemple, `nsx_isSSHEnabled` et `nsx_allowSSHRootLogin` sont tous deux activés. Lorsqu'ils sont désactivés, vous ne pouvez pas utiliser SSH ou vous connecter à la ligne de commande NSX Manager. Si vous activez `nsx_isSSHEnabled` mais pas `nsx_allowSSHRootLogin`, vous pouvez utiliser SSH avec NSX Manager, mais ne pouvez pas vous connecter en tant qu'utilisateur racine.

- 4 Utilisez `guestfish` pour écrire le fichier `guestinfo` dans l'image QCOW2.

Une fois que les informations `guestinfo` sont écrites dans une image QCOW2, elles ne peuvent pas être écrasées.

```
sudo guestfish --rw -i -a nsx-manager1-build.qcow2 upload guestinfo /config/guestinfo
```

- 5 Déployez l'image QCOW2 avec la commande `virt-install`.

```
user@ubuntu1604:/var/lib/libvirt/images$ sudo virt-install --import --name nsx-manager1 --ram
16348 --vcpus 4 --network=bridge:br0,model=e1000 --disk path=/var/lib/libvirt/images/nsx-
manager-1.1.0.0.4446302.qcow2,format=qcow2 --nographics

Starting install...
```

```

Creating domain... | 0 B 00:01
Connected to domain nsx-manager1
Escape character is ^]

nsx-manager1 login:

```

À l'issue du démarrage du dispositif NSX Manager, la console NSX Manager s'affiche.

- 6 (Facultatif) Pour des performances optimales, réservez de la mémoire pour le composant NSX-T Data Center.

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 sur un niveau qui garantit que le composant NSX-T Data Center dispose de suffisamment de mémoire pour s'exécuter efficacement. Reportez-vous à la section [Configuration système requise](#).

- 7 Ouvrez la console du composant NSX-T Data Center pour suivre le processus de démarrage.
- 8 Dès que le composant NSX-T Data Center a démarré, connectez-vous à l'interface de ligne de commande en tant qu'administrateur et exécutez la commande `get interface eth0` pour vérifier que l'adresse IP a été appliquée comme prévu.

```

nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...

```

- 9 Vérifiez que votre composant NSX-T Data Center dispose de la connectivité requise.

Assurez-vous que vous pouvez effectuer les tâches suivantes.

- Effectuer un test ping de votre composant NSX-T Data Center à partir d'une autre machine.
- Le composant NSX-T Data Center peut effectuer un test ping de sa passerelle par défaut.
- Le composant NSX-T Data Center peut effectuer un test ping des hôtes d'hyperviseur qui se trouvent dans le même réseau que le composant NSX-T Data Center à l'aide de l'interface de gestion.
- Le composant NSX-T Data Center peut effectuer un test ping de son serveur DNS et de son serveur NTP.
- Si vous avez activé le protocole SSH, assurez-vous de pouvoir l'utiliser avec votre composant NSX-T Data Center.

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

10 Quittez la console KVM.

```
control-]
```

Étape suivante

Connectez-vous à l'interface graphique utilisateur NSX Manager à partir d'un navigateur Web pris en charge.

L'URL est `https://<adresse IP de NSX Manager>`. Par exemple, `https://10.16.176.10`.

Note Vous devez utiliser HTTPS. HTTP n'est pas pris en charge.

Se connecter à l'instance de NSX Manager qui vient d'être créée

Après avoir installé NSX Manager, vous pouvez utiliser l'interface utilisateur pour effectuer d'autres tâches d'installation.

Après avoir installé NSX Manager, vous pouvez rejoindre le Programme d'amélioration du produit pour NSX-T Data Center. Consultez le Programme d'amélioration du produit dans le *Guide d'administration de NSX-T Data Center* pour plus d'informations sur le programme, y compris comment participer ou quitter le programme.

Conditions préalables

Vérifiez que NSX Manager est installé.

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
Le CLUF apparaît.
- 2 Faites défiler l'écran jusqu'au bas du CLUF et acceptez-en les conditions.
- 3 Indiquez si vous voulez rejoindre le Programme d'amélioration du produit de VMware.
- 4 Cliquez sur **Enregistrer**

Installation et mise en cluster de NSX Controller

5

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-T Data Center.

NSX Controller 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 et les routeurs logiques. Les dispositifs NSX Controller contrôlent les appareils qui acheminent des paquets. Ces appareils d'acheminement sont plus connus sous le nom de commutateurs virtuels.

Des commutateurs virtuels, tels que des commutateurs virtuels distribués gérés par NSX (N-VDS, anciennement appelés commutateurs hôtes) et des Open vSwitch (OVS), se trouvent sur ESXi et d'autres hyperviseurs tels que KVM.

Dans un environnement de production, vous devez disposer d'un cluster NSX Controller avec trois membres afin d'éviter toute interruption du plan de contrôle NSX. Chaque contrôleur doit être placé sur un hôte d'hyperviseur unique pour un total de trois hôtes d'hyperviseur physiques, afin d'éviter un échec d'un hôte d'hyperviseur physique, ce qui affecterait le plan de contrôle NSX. Pour les déploiements de laboratoire et de validation technique pour lesquels il n'y a aucune charge de travail de production, un seul contrôleur peut être exécuté afin d'économiser des ressources.

Tableau 5-1. Exigences du déploiement, de la plate-forme et de l'installation de NSX Controller

Exigences	Description
Méthodes de déploiement prises en charge	<ul style="list-style-type: none">■ OVA/OVF■ QCOW2 <p>Note La méthode de déploiement de démarrage de l'environnement d'exécution de pré-amorçage n'est pas prise en charge.</p>
Plates-formes prises en charge	<p>Reportez-vous à la section Configuration système requise. NSX Controller est pris en charge sur ESXi en tant que machine virtuelle et KVM.</p> <p>Note La méthode de déploiement de démarrage de l'environnement d'exécution de pré-amorçage n'est pas prise en charge.</p>

Tableau 5-1. Exigences du déploiement, de la plate-forme et de l'installation de NSX Controller (Suite)

Exigences	Description
Adresse IP	<p>Un système NSX Controller doit posséder une adresse IP statique. Vous ne pouvez pas modifier l'adresse IP après l'installation.</p> <p>Planifiez votre schéma d'adresses IP IPv4. Dans cette version de NSX-T Data Center, IPv6 n'est pas pris en charge.</p>
Mot de passe du dispositif NSX-T Data Center	<ul style="list-style-type: none"> ■ Au moins huit caractères ■ Au moins une lettre minuscule ■ Au moins une lettre majuscule ■ Au moins un chiffre ■ Au moins un caractère spécial ■ Au moins cinq caractères différents ■ Aucun mot issu du dictionnaire ■ Aucun palindrome
Nom d'hôte	<p>Lorsque vous installez NSX Controller, spécifiez un nom d'hôte qui ne contient pas de caractères non valides comme un caractère de soulignement. Si le nom d'hôte contient un caractère non valide, après le déploiement, le nom d'hôte sera défini sur localhost. Pour plus d'informations sur les restrictions de nom d'hôte, reportez-vous à https://tools.ietf.org/html/rfc952 et https://tools.ietf.org/html/rfc1123.</p>
VMware Tools	<p>VMTools est installé sur la machine virtuelle NSX Controller exécutée sur ESXi. Ne supprimez pas ou ne mettez pas VMTools à niveau.</p>
Système	<p>Vérifiez que la configuration requise est respectée. Reportez-vous à la section Configuration système requise.</p>
Ports	<p>Vérifiez que les ports requis sont ouverts. Reportez-vous à la section Ports et protocoles.</p>

Scénarios d'installation de NSX Controller

Important Lorsque vous installez NSX Controller à partir d'un fichier OVA ou OVF, depuis vSphere Web Client ou depuis la ligne de commande, les valeurs de propriété OVA/OVF, telles que les noms d'utilisateur, les mots de passe ou les adresses IP, ne sont pas validées avant la mise sous tension de la machine virtuelle.

- Si vous spécifiez un nom d'utilisateur pour l'utilisateur **admin** ou **audit**, le nom doit être unique. Si vous spécifiez le même nom, il est ignoré et les noms par défaut (**admin** et **audit**) sont utilisés.
- Si le mot de passe de l'utilisateur **admin** ne répond pas aux exigences de complexité, vous devez vous connecter à NSX Controller via SSH ou à la console en tant qu'utilisateur **admin**. Vous êtes invité à modifier le mot de passe.

- Si le mot de passe de l'utilisateur **audit** ne respecte pas les exigences de complexité, le compte d'utilisateur est désactivé. Pour activer le compte, connectez-vous à NSX Controller via SSH ou à la console en tant qu'utilisateur **admin** et exécutez la commande **set user audit** pour définir le mot de passe de l'utilisateur **audit** (le mot de passe actuel est une chaîne vide).
- Si le mot de passe de l'utilisateur **racine** ne respecte pas les exigences de complexité, vous devez vous connecter à NSX Controller via SSH ou à la console en tant que **racine** avec le mot de passe **vmware**. Vous êtes invité à modifier le mot de passe.



Attention Les modifications apportées à NSX-T Data Center tout en étant connecté avec les informations d'identification de l'utilisateur **racine** peuvent provoquer la défaillance du système et avoir éventuellement un impact sur votre réseau. Vous pouvez uniquement apporter des modifications à l'aide des informations d'identification de l'utilisateur **racine** en suivant les instructions de l'équipe de support de VMware.

Note

- N'utilisez pas des privilèges racines pour installer des démons ou des applications. L'utilisation de privilèges racines pour installer des démons ou des applications peut rendre votre contrat de support nul. Utilisez des privilèges racines uniquement si l'équipe du support VMware le demande.
- Sur le dispositif, les services de base ne démarrent pas tant qu'un mot de passe suffisamment complexe n'a pas été défini.

Après avoir déployé un dispositif NSX Controller à partir d'un fichier OVA, vous ne pouvez pas modifier les paramètres IP de la machine virtuelle en mettant la machine virtuelle hors tension, puis en modifiant les paramètres OVA de vCenter Server.

Ce chapitre contient les rubriques suivantes :

- [Installation automatisée d'un contrôleur et d'un cluster à partir de NSX Manager](#)
- [Installer NSX Controller sur ESXi à l'aide d'une interface utilisateur graphique](#)
- [Installer NSX Controller sur ESXi à l'aide de l'outil OVF de ligne de commande](#)
- [Installer NSX Controller sur KVM](#)
- [Joindre des dispositifs NSX Controller à NSX Manager](#)
- [Initialiser le cluster de contrôle pour créer un maître de cluster de contrôle](#)
- [Relier les dispositifs NSX Controller au maître de cluster](#)

Installation automatisée d'un contrôleur et d'un cluster à partir de NSX Manager

Vous pouvez configurer NSX Manager pour installer des contrôleurs automatiquement sur des hôtes vSphere ESXi. Après le déploiement, ces contrôleurs sont automatiquement ajoutés à un cluster de contrôleurs sur cet hôte vSphere ESXi géré par un serveur vCenter Server. Vous pouvez également utiliser des REST API NSX Manager pour installer automatiquement des clusters de contrôleurs.

NSX Manager vous permet de déployer des contrôleurs supplémentaires automatiquement sur un cluster existant qui est déployé manuellement. Toutefois, si un contrôleur a été ajouté manuellement, il doit également être supprimé manuellement du cluster.

Cas d'utilisation pris en charge

- Création d'un cluster à nœud unique
- Création d'un cluster à nœuds multiples
- Ajout de nœuds à un cluster existant
- Suppression d'un contrôleur déployé automatiquement à partir d'un cluster fonctionnel

Configurer l'installation automatisée d'un contrôleur et d'un cluster à l'aide de l'interface utilisateur de NSX Manager

Configurez NSX Manager pour installer automatiquement des contrôleurs sur les hôtes vSphere ESXi gérés par un serveur vCenter Server. Après l'installation, ces contrôleurs sont automatiquement ajoutés à un cluster de contrôleurs sur un hôte vSphere ESXi.

Conditions préalables

- Déployer NSX Manager.
- Déployer des hôtes vCenter Server et vSphere ESXi.
- Enregistrer un hôte vSphere ESXi sur le vCenter Server.
- L'hôte vSphere ESXi doit disposer de suffisamment de ressources CPU, mémoire et disque dur pour prendre en charge 12 vCPU, 48 Go de RAM et 360 Go de stockage.

Procédure

- 1 Connectez-vous au NSX Manager, <https://<adresseIPnsxmanager>/>.
- 2 Dans l'interface utilisateur NSX Manager, en l'absence de vCenter enregistré, accédez au panneau **Infrastructure**, cliquez sur **Gestionnaires de calcul**, puis ajoutez un gestionnaire de calcul.
- 3 Sur la page système, cliquez sur **Ajouter des contrôleurs**.
- 4 Sur la page Attributs communs, entrez les valeurs requises sur la page.
- 5 Sélectionnez **Gestionnaire de calcul**.
- 6 (Facultatif) Vous pouvez activer SSH.
- 7 (Facultatif) Vous pouvez activer l'accès racine.
- 8 (Facultatif) Si vous ajoutez un nœud à un cluster existant, activez Joindre un cluster existant.
- 9 Entrez et confirmez la clé Secret partagé requise pour initialiser et former le cluster.

Note Tous les nœuds de contrôleur ajoutés à ce cluster doivent utiliser la même clé Secret partagé.

- 10 Entrez les informations d'identification du contrôleur.

- 11 Cliquez sur **Suivant**.
- 12 Sur la page Contrôleurs, cliquez sur **Ajouter un contrôleur**.
- 13 Entrez un nom d'hôte valide ou un nom de domaine complet pour le nœud du contrôleur.
- 14 Sélectionnez le cluster.
- 15 (Facultatif) Sélectionnez le pool de ressources. Le pool de ressources fournit uniquement un pool de ressources de calcul pour déployer les nœuds de contrôleur. Attribuez des ressources de stockage spécifiques.
- 16 (Facultatif) Sélectionnez l'hôte.
- 17 Sélectionnez la banque de données.
- 18 Sélectionnez l'interface de gestion utilisée par l'hôte pour communiquer avec les différents composants au sein de l'hôte lui-même.
- 19 Entrez une adresse IP statique avec les détails du port (*<AdresseIP>/<NuméroPort>*) et le masque de réseau.
- 20 Vous pouvez ajouter plusieurs contrôleurs. Cliquez sur le bouton **+** et entrez les détails de contrôleur avant de lancer le déploiement.
- 21 Cliquez sur **Terminer**.

L'installation automatisée du contrôleur commence. Les contrôleurs sont tout d'abord enregistrés auprès de NSX Manager avant de former le cluster ou de joindre un cluster existant.

- 22 Vérifiez si les contrôleurs sont enregistrés avec NSX Manager.
 - a Connectez-vous à la console NSX Manager.
 - b Entrez `# get management-cluster status`
L'état du cluster de gestion doit être STABLE.
 - c Vous pouvez également, à partir de l'interface utilisateur NSX Manager, vérifier que la connectivité de Manager est active.
- 23 Vérifiez l'état du cluster de contrôle.
 - a Connectez-vous à la console d'interface de ligne de commande du contrôleur.
 - b Entrez `# get control-cluster status`.
L'état du cluster de contrôle doit être STABLE.
 - c Vous pouvez également, à partir de l'interface utilisateur NSX Manager, vérifier que la connectivité du cluster est active.

Étape suivante

Configurez NSX Manager pour installer automatiquement des contrôleurs et des clusters à l'aide d'API. Reportez-vous à la section [Configurer l'installation automatisée d'un contrôleur et d'un cluster à l'aide d'API](#).

Configurer l'installation automatisée d'un contrôleur et d'un cluster à l'aide d'API

À l'aide d'API, configurez NSX Manager pour installer automatiquement des contrôleurs sur les hôtes vSphere ESXi gérés par un serveur vCenter Server. Une fois les contrôleurs installés, ils sont automatiquement ajoutés à un cluster de contrôleurs sur des hôtes vSphere ESXi.

Procédure

- 1 Avant de déclencher la création automatique du cluster de contrôleurs, vous devez extraire l'ID de vCenter Server, l'ID de calcul, l'ID de stockage et l'ID réseau requis en tant que charge utile de l'API POST.
- 2 Connectez-vous à vCenter Server.
`https://<vCenterServer_IPAddress>/mob.`
- 3 Dans la colonne Valeur, cliquez sur **Contenu**.
- 4 Sur la page Propriétés du contenu, accédez à la fonction de recherche de la colonne Valeur pour rechercher le centre de données et cliquez sur le lien du groupe.
- 5 Sur la page Propriétés du groupe, accédez à la colonne Valeur et cliquez sur le lien du centre de données.
- 6 Sur la page Propriétés du centre de données, copiez la valeur de banque de données et la valeur de réseau que vous souhaitez utiliser pour créer le cluster de contrôleurs.
- 7 Cliquez sur le lien **HostFolder**.
- 8 Sur la page Propriétés du groupe, copiez la valeur de cluster que vous souhaitez utiliser pour créer le cluster de contrôleurs.
- 9 Pour extraire l'ID vCenter Server, accédez à l'interface utilisateur NSX Manager et copiez son ID à partir de la page Gestionnaire de calcul.
- 10 POST `https://<nsx-manager>/api/v1/cluster/nodes/deployments`

```
REQUEST
{
  "deployment_requests": [
    {
      "roles": ["CONTROLLER"],
      "user_settings": {
        "cli_password": "CLIp4$$w4rd",
        "root_password": "ROOTp4$$w4rd"
      },
      "deployment_config": {
        "placement_type": "VsphereClusterNodeVMDeploymentConfig",
        "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
        "management_network_id": "network-13",
        "hostname": "controller-0",
        "compute_id": "domain-s9",
        "storage_id": "datastore-12",
```

```

    "default_gateway_addresses": [
      "10.33.79.253"
    ],
    "management_port_subnets": [
      {
        "ip_addresses": [
          "10.33.79.64"
        ],
        "prefix_length": "22"
      }
    ]
  },
  {
    "roles": ["CONTROLLER"],
    "user_settings": {
      "cli_password": "VMware$123",
      "root_password": "VMware$123"
    },
    "deployment_config": {
      "placement_type": "VsphereClusterNodeVMDeploymentConfig",
      "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
      "management_network_id": "network-13",
      "hostname": "controller-1",
      "compute_id": "domain-s9",
      "storage_id": "datastore-12",
      "default_gateway_addresses": [
        "10.33.79.253"
      ],
      "management_port_subnets": [
        {
          "ip_addresses": [
            "10.33.79.65"
          ],
          "prefix_length": "22"
        }
      ]
    }
  }
],
    "deployment_config": {
      "placement_type": "VsphereClusterNodeVMDeploymentConfig",
      "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
      "management_network_id": "network-13",
      "hostname": "controller-0",
      "compute_id": "domain-s9",
      "storage_id": "datastore-12",
      "default_gateway_addresses": [
        "10.33.79.253"
      ],
      "management_port_subnets": [
        {
          "ip_addresses": [
            "10.33.79.66"
          ]
        }
      ]
    }
  }
],

```

```

    ],
    "prefix_length": "22"
  }
]
}
},

  "clustering_config": {
    "clustering_type": "ControlClusteringConfig",
    "shared_secret": "123456",
    "join_to_existing_cluster": false
  }
}

Response
{
  "result_count": 2,
  "results": [
    {
      "user_settings": {
        "cli_password": "[redacted]",
        "root_password": "[redacted]",
        "cli_username": "admin"
      },
      "vm_id": "71f02260-644f-4482-aa9a-ab8570bb49a3",
      "roles": [
        "CONTROLLER"
      ],
      "deployment_config": {
        "placement_type": "VsphereClusterNodeVMDeploymentConfig",
        "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
        "management_network_id": "network-13",
        "default_gateway_addresses": [
          "10.33.79.253"
        ],
        "hostname": "controller-0",
        "compute_id": "domain-s9",
        "storage_id": "datastore-12",
        "management_port_subnets": [
          {
            "ip_addresses": [
              "10.33.79.64"
            ],
            "prefix_length": 22
          }
        ]
      }
    },
    {
      "form_factor": "SMALL"
    }
  ],
  {
    "user_settings": {
      "cli_password": "[redacted]",
      "root_password": "[redacted]",

```

```

    "cli_username": "admin"
  },

  "vm_id": "38029a2b-b9bc-467f-8138-aef784e802cc",
  "roles": [
    "CONTROLLER"
  ],
  "deployment_config": {
    "placement_type": "VsphereClusterNodeVMDeploymentConfig",
    "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
    "management_network_id": "network-13",
    "hostname": "controller-1",
    "compute_id": "domain-s9",
    "storage_id": "datastore-12"
  },
  "form_factor": "MEDIUM"
}
]
}

```

- 11** Vous pouvez afficher l'état du déploiement à l'aide de l'appel d'API. GET <https://<nsx-manager>/api/v1/cluster/nodes/deployments>

```

{

  "result_count": 2,
  "results": [
    {
      "user_settings": {
        "cli_password": "[redacted]",
        "root_password": "[redacted]"
      },
      "vm_id": "12f563af-af9f-48f3-848e-e9257c8740b0",
      "roles": [
        "CONTROLLER"
      ],

      "deployment_config": {
        "placement_type": "VsphereClusterNodeVMDeploymentConfig",
        "vc_id": "15145422-47a1-4c55-81da-01d953151d1f",
        "management_network_id": "network-158",
        "hostname": "controller-0",
        "compute_id": "domain-c154",
        "storage_id": "datastore-157"
      },
      "form_factor": "SMALL",
    },
    {
      "user_settings": {
        "cli_password": "[redacted]",
        "root_password": "[redacted]"
      },
      "vm_id": "cc21854c-265b-42de-af5f-05448c00777a",
      "roles": [

```



```

    "CONTROLLER"
  ],
  "deployment_config": {
    "placement_type": "VsphereClusterNodeVMDeploymentConfig",
    "vc_id": "feb17651-49a7-4ce6-88b4-41d3f624e53b",
    "management_network_id": "network-158",
    "hostname": "controller-0",
    "compute_id": "domain-c154",
    "storage_id": "datastore-157"
  },
  "form_factor": "MEDIUM",
}
]
}

```

Étape suivante

Supprimez un cluster. Reportez-vous à la section [Supprimer NSX Controller](#).

Supprimer NSX Controller

Supprimez des NSX Controller du cluster.

Procédure

- 1 Connectez-vous au site **<https://<adresse-ip-nsx-manager>/>**.
- 2 Cliquez sur **Système > Composants**.
- 3 Sous Cluster de contrôleurs, identifiez les NSX Controller.
- 4 Cliquez sur l'icône **Paramètres**, puis sur **Supprimer**.
- 5 Cliquez sur **Confirmer**.

NSX-T Data Center détache les NSX Controller du cluster, en annule l'inscription auprès de NSX Manager, le met hors tension et supprime le NSX Controller.

Étape suivante

Installez un NSX Controller sur un hôte vSphere ESXi à l'aide de l'interface utilisateur graphique. Reportez-vous à la section [Installer NSX Controller sur ESXi à l'aide d'une interface utilisateur graphique](#).

Installer NSX Controller sur ESXi à l'aide d'une interface utilisateur graphique

Si vous préférez une installation interactive de NSX Controller, vous pouvez utiliser un outil de gestion de machine virtuelle doté d'une interface utilisateur, tel que vSphere Client connecté à vCenter Server.

L'installation réussit même si le mot de passe ne répond pas aux exigences. Toutefois, lorsque vous vous connectez pour la première fois, vous êtes invité à modifier le mot de passe.

Important Sur le dispositif, les services de base ne démarrent pas tant qu'un mot de passe suffisamment complexe n'a pas été défini.

Important Les installations de machine virtuelle de composant NSX-T Data Center incluent VMware Tools. La suppression ou la mise à niveau de VMware Tools n'est pas prise en charge sur les dispositifs NSX-T Data Center.

Conditions préalables

- Vérifiez que la configuration requise est respectée. Reportez-vous à la section [Configuration système requise](#).
- Vérifiez que les ports requis sont ouverts. Reportez-vous à la section [Ports et protocoles](#).
- Créez le réseau du groupe de ports de machines virtuelles cible, si celui-ci n'existe pas déjà. Il est recommandé de placer les dispositifs NSX-T Data Center sur un réseau de machines virtuelles de gestion.

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

- Planifiez votre schéma d'adresses IP IPv4. Dans cette version de NSX-T Data Center, IPv6 n'est pas pris en charge.
- Vérifiez que vous disposez des privilèges appropriés pour déployer un modèle OVF sur l'hôte ESXi.
- Vérifiez que les noms d'hôte n'incluent pas de traits de soulignement. Autrement, le nom d'hôte est défini sur *nsx-controller*.
- Un outil de gestion pouvant déployer des modèles OVF, tels que vCenter Server ou vSphere Client.
L'outil de déploiement de modèles OVF doit prendre en charge des options de configuration qui permettent la configuration manuelle.
- Le plug-in d'intégration du client doit être installé.

Procédure

- 1 Localisez le fichier OVA ou OVF de NSX Controller.
Copiez l'URL de téléchargement ou téléchargez le fichier OVA sur votre ordinateur.
- 2 Dans l'outil de gestion, lancez l'assistant **Déployer un modèle OVF**, puis accédez au fichier .ova ou à un lien vers ce fichier.

- 3 Entrez un nom pour le dispositif NSX Controller, puis sélectionnez un dossier ou un centre de données.

Le nom saisi s'affichera dans l'inventaire.

Le dossier que vous sélectionnez sera utilisé pour appliquer des autorisations au dispositif NSX Controller.

- 4 Sélectionnez une banque de données pour stocker les fichiers du dispositif virtuel NSX Controller.
- 5 Si vous utilisez vCenter, sélectionnez un hôte ou un cluster sur lequel déployer le dispositif NSX Controller.
- 6 Sélectionnez le groupe de ports ou le réseau de destination du dispositif NSX Controller.
- 7 Spécifiez les mots de passe et les paramètres IP du dispositif NSX Controller.
- 8 (Facultatif) Pour des performances optimales, réservez de la mémoire pour le composant NSX-T Data Center.

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 sur un niveau qui garantit que le composant NSX-T Data Center dispose de suffisamment de mémoire pour s'exécuter efficacement. Reportez-vous à la section [Configuration système requise](#).

- 9 Ouvrez la console du composant NSX-T Data Center pour suivre le processus de démarrage.
- 10 Dès que le composant NSX-T Data Center a démarré, connectez-vous à l'interface de ligne de commande en tant qu'administrateur et exécutez la commande `get interface eth0` pour vérifier que l'adresse IP a été appliquée comme prévu.

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

- 11 Vérifiez que votre composant NSX-T Data Center dispose de la connectivité requise.

Assurez-vous que vous pouvez effectuer les tâches suivantes.

- Effectuer un test ping de votre composant NSX-T Data Center à partir d'une autre machine.
- Le composant NSX-T Data Center peut effectuer un test ping de sa passerelle par défaut.
- Le composant NSX-T Data Center peut effectuer un test ping des hôtes d'hyperviseur qui se trouvent dans le même réseau que le composant NSX-T Data Center à l'aide de l'interface de gestion.
- Le composant NSX-T Data Center peut effectuer un test ping de son serveur DNS et de son serveur NTP.

- Si vous avez activé le protocole SSH, assurez-vous de pouvoir l'utiliser avec votre composant NSX-T Data Center.

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

Étape suivante

Reliez le dispositif NSX Controller au plan de gestion. Reportez-vous à la section [Joindre des dispositifs NSX Controller à NSX Manager](#).

Installer NSX Controller sur ESXi à l'aide de l'outil OVF de ligne de commande

Si vous préférez automatiser l'installation de NSX Controller, vous pouvez utiliser l'outil OVF de VMware, qui est un utilitaire de ligne de commande.

Par défaut, `nsx_isSSHEnabled` et `nsx_allowSSHRootLogin` sont tous deux désactivés pour des raisons de sécurité. Lorsqu'ils sont désactivés, vous ne pouvez pas utiliser SSH ou vous connecter à la ligne de commande NSX Controller. Si vous activez `nsx_isSSHEnabled` mais pas `nsx_allowSSHRootLogin`, vous pouvez utiliser SSH avec NSX Controller, mais ne pouvez pas vous connecter en tant qu'utilisateur racine.

Conditions préalables

- Vérifiez que la configuration requise est respectée. Reportez-vous à la section [Configuration système requise](#).
- Vérifiez que les ports requis sont ouverts. Reportez-vous à la section [Ports et protocoles](#).
- Créez le réseau du groupe de ports de machines virtuelles cible, si celui-ci n'existe pas déjà. Il est recommandé de placer les dispositifs NSX-T Data Center sur un réseau de machines virtuelles de gestion.

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

- Planifiez votre schéma d'adresses IP IPv4. Dans cette version de NSX-T Data Center, IPv6 n'est pas pris en charge.
- OVF Tool version 4.0 ou ultérieure.

Procédure

- Pour un hôte autonome, exécutez la commande `ovftool` avec les paramètres appropriés.

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-controller
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--network="management"
```

```

--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.210
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=<True|False>
--prop:nsx_allowSSHRootLogin=<True|False>
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_cli_audit_passwd_0=<password>
--prop:nsx_hostname=nsx-controller
<path/url to nsx component ova>
vi://root:<password>@192.168.110.51

```

- Pour un hôte géré par vCenter Server, exécutez la commande `ovftool` avec les paramètres appropriés.

```

C:\Users\Administrator\Downloads>ovftool
--name=nsx-controller
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--network="management"
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.210
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=<True|False>
--prop:nsx_allowSSHRootLogin=<True|False>
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_cli_audit_passwd_0=<password>
--prop:nsx_hostname=nsx-controller
<path/url to nsx component ova>
vi://administrator@vsphere.local:<vcenter_password>@192.168.110.24/?ip=192.168.110.51

```

- (Facultatif) Pour des performances optimales, réservez de la mémoire pour le composant NSX-T Data Center.

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 sur un niveau qui garantit que le composant NSX-T Data Center dispose de suffisamment de mémoire pour s'exécuter efficacement. Reportez-vous à la section [Configuration système requise](#).

- Ouvrez la console du composant NSX-T Data Center pour suivre le processus de démarrage.
- Dès que le composant NSX-T Data Center a démarré, connectez-vous à l'interface de ligne de commande en tant qu'administrateur et exécutez la commande `get interface eth0` pour vérifier que l'adresse IP a été appliquée comme prévu.

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

- Vérifiez que votre composant NSX-T Data Center dispose de la connectivité requise.

Assurez-vous que vous pouvez effectuer les tâches suivantes.

- Effectuer un test ping de votre composant NSX-T Data Center à partir d'une autre machine.
- Le composant NSX-T Data Center peut effectuer un test ping de sa passerelle par défaut.
- Le composant NSX-T Data Center peut effectuer un test ping des hôtes d'hyperviseur qui se trouvent dans le même réseau que le composant NSX-T Data Center à l'aide de l'interface de gestion.
- Le composant NSX-T Data Center peut effectuer un test ping de son serveur DNS et de son serveur NTP.
- Si vous avez activé le protocole SSH, assurez-vous de pouvoir l'utiliser avec votre composant NSX-T Data Center.

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

Étape suivante

Reliez le dispositif NSX Controller au plan de gestion. Reportez-vous à la section [Joindre des dispositifs NSX Controller à NSX Manager](#).

Installer NSX Controller sur KVM

NSX Controller est le point de contrôle central de tous les commutateurs logiques d'un réseau. Il stocke des informations sur tous les hôtes, commutateurs logiques et routeurs logiques distribués.

La procédure d'installation de QCOW2 utilise guestfish, un outil de ligne de commande Linux qui permet d'écrire des paramètres de machine virtuelle dans le fichier QCOW2.

Conditions préalables

- KVM configuré. Reportez-vous à la section [Configurer KVM](#).
- Privilèges pour le déploiement d'une image QCOW2 sur l'hôte KVM.

Procédure

- 1 Téléchargez l'image QCOW2 de NSX Controller dans le répertoire `/var/lib/libvirt/images`.
- 2 (Ubuntu uniquement) Ajoutez l'utilisateur connecté en tant qu'utilisateur libvirt :

```
adduser $USER libvirt
```

- 3 Dans le répertoire où vous avez enregistré l'image QCOW2, créez un fichier appelé `guestinfo` (sans extension de fichier) et remplissez-le avec les propriétés de la machine virtuelle NSX Controller.

Par exemple :

```
<?xml version="1.0" encoding="UTF-8"?>
<Environment
  xmlns="http://schemas.dmtf.org/ovf/environment/1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:oe="http://schemas.dmtf.org/ovf/environment/1">
  <PropertySection>
    <Property oe:key="nsx_allowSSHRootLogin" oe:value="True"/>
    <Property oe:key="nsx_cli_audit_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_cli_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_dns1_0" oe:value="192.168.110.10"/>
    <Property oe:key="nsx_domain_0" oe:value="corp.local"/>
    <Property oe:key="nsx_gateway_0" oe:value="192.168.110.1"/>
    <Property oe:key="nsx_hostname" oe:value="nsx-Controller1"/>
    <Property oe:key="nsx_ip_0" oe:value="192.168.110.34"/>
    <Property oe:key="nsx_isSSHEnabled" oe:value="True"/>
    <Property oe:key="nsx_netmask_0" oe:value="255.255.255.0"/>
    <Property oe:key="nsx_ntp_0" oe:value="192.168.110.10"/>
    <Property oe:key="nsx_passwd_0" oe:value="<password>"/>
  </PropertySection>
</Environment>
```

Dans cet exemple, `nsx_isSSHEnabled` et `nsx_allowSSHRootLogin` sont tous deux activés. Lorsqu'ils sont désactivés, vous ne pouvez pas utiliser SSH ou vous connecter à la ligne de commande NSX Controller. Si vous activez `nsx_isSSHEnabled` mais pas `nsx_allowSSHRootLogin`, vous pouvez utiliser SSH avec NSX Controller, mais ne pouvez pas vous connecter en tant qu'utilisateur racine.

- 4 Utilisez `guestfish` pour écrire le fichier `guestinfo` dans l'image QCOW2.

Si vous créez plusieurs dispositifs NSX Controller, créez une copie distincte de l'image QCOW2 pour chaque contrôleur. Une fois que les informations `guestinfo` sont écrites dans une image QCOW2, elles ne peuvent pas être écrasées.

```
sudo guestfish --rw -i -a nsx-controller1-build.qcow2 upload guestinfo /config/guestinfo
```

5 Déployez l'image QCOW2 avec la commande `virt-install`.

```
user@ubuntu1604:/var/lib/libvirt/images$ sudo virt-install --import --name nsx-controller1 --ram
16384 --vcpus 2 --network=bridge:br0,model=e1000 --disk path=/var/lib/libvirt/images/nsx-
controller-release_version_number.qcow2,format=qcow2 --nographics --noautoconsole
```

À l'issue du démarrage du dispositif NSX Controller, la console NSX Controller s'affiche.

6 (Facultatif) Pour des performances optimales, réservez de la mémoire pour le composant NSX-T Data Center.

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 sur un niveau qui garantit que le composant NSX-T Data Center dispose de suffisamment de mémoire pour s'exécuter efficacement. Reportez-vous à la section [Configuration système requise](#).

7 Ouvrez la console du composant NSX-T Data Center pour suivre le processus de démarrage.

8 Dès que le composant NSX-T Data Center a démarré, connectez-vous à l'interface de ligne de commande en tant qu'administrateur et exécutez la commande `get interface eth0` pour vérifier que l'adresse IP a été appliquée comme prévu.

```
nsx-component> get interface eth0
Interface: eth0
Address: 192.168.110.25/24
MAC address: 00:50:56:86:7b:1b
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

9 Vérifiez que votre composant NSX-T Data Center dispose de la connectivité requise.

Assurez-vous que vous pouvez effectuer les tâches suivantes.

- Effectuer un test ping de votre composant NSX-T Data Center à partir d'une autre machine.
- Le composant NSX-T Data Center peut effectuer un test ping de sa passerelle par défaut.
- Le composant NSX-T Data Center peut effectuer un test ping des hôtes d'hyperviseur qui se trouvent dans le même réseau que le composant NSX-T Data Center à l'aide de l'interface de gestion.
- Le composant NSX-T Data Center peut effectuer un test ping de son serveur DNS et de son serveur NTP.
- Si vous avez activé le protocole SSH, assurez-vous de pouvoir l'utiliser avec votre composant NSX-T Data Center.

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

Étape suivante

Reliez le dispositif NSX Controller au plan de gestion. Reportez-vous à la section [Joindre des dispositifs NSX Controller à NSX Manager](#).

Joindre des dispositifs NSX Controller à NSX Manager

La jonction des dispositifs NSX Controller à NSX Manager garantit que les dispositifs NSX Manager et NSX Controller peuvent communiquer les uns avec les autres.

Conditions préalables

- Vérifiez que NSX Manager est installé.
- Vérifiez que vous disposez des privilèges d'administrateur pour vous connecter aux dispositifs NSX Manager et NSX Controller.

Procédure

- 1 Ouvrez une session SSH vers NSX Manager.
- 2 Ouvrez une session SSH vers chaque dispositif NSX Controller.
Par exemple, NSX-Controller1, NSX-Controller2 et NSX-Controller3.
- 3 Sur NSX Manager, exécutez la commande `get certificate api thumbprint`.

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

- 4 Sur chaque dispositif NSX Controller, exécutez la commande **join management-plane**.

```
NSX-Controller1> join management-plane NSX-Manager-IP-address username admin thumbprint <NSX-Manager-thumbprint>

Password for API user: <NSX-Manager-password>
Node successfully registered and controller restarted
```

Exécutez cette commande sur chaque nœud NSX Controller déployé.

Fournissez les informations suivantes :

- Adresse IP du dispositif NSX Manager avec numéro de port facultatif
 - Nom du dispositif NSX Manager
 - Empreinte numérique de certificat du dispositif NSX Manager
 - Mot de passe du dispositif NSX Manager
- 5 Vérifiez le résultat en exécutant la commande `get managers` sur vos dispositifs NSX Controller.

```
NSX-Controller1> get managers
- 192.168.110.47 Connected
```

- 6 Sur le dispositif NSX Manager, exécutez la commande `get management-cluster status` et assurez-vous que les dispositifs NSX Controller sont répertoriés.

```
NSX-Manager> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.47 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.201 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
- 192.168.110.202 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
- 192.168.110.203 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
```

Étape suivante

Initialisez le cluster de contrôle. Reportez-vous à la section [Initialiser le cluster de contrôle pour créer un maître de cluster de contrôle](#).

Initialiser le cluster de contrôle pour créer un maître de cluster de contrôle

Après l'installation du premier dispositif NSX Controller dans votre déploiement NSX-T Data Center, vous pouvez initialiser le cluster de contrôle. L'initialisation du cluster de contrôle est obligatoire, même si vous définissez un petit environnement de démonstration de faisabilité ne comportant qu'un nœud de contrôleur. Si vous n'initialisez pas le cluster de contrôle, le contrôleur ne peut pas communiquer avec les hôtes d'hyperviseur. Dans le cluster, il vous suffit d'initialiser un seul contrôleur.

Conditions préalables

- Installez au moins un dispositif NSX Controller.
- Reliez le dispositif NSX Controller au plan de gestion.
- Vérifiez que vous disposez des privilèges d'administrateur pour vous connecter au dispositif NSX Controller.
- Attribuez un mot de passe secret partagé. Un mot de passe secret partagé est un mot de passe secret partagé défini par l'utilisateur (par exemple, « secret123 »).

Procédure

- 1 Ouvrez une session SSH pour votre dispositif NSX Controller.
- 2 Exécutez la commande `set control-cluster security-model shared-secret secret <secret>` et entrez un secret partagé lorsque vous y êtes invité.

3 Exécutez la commande `initialize control-cluster`.

Cette commande fait de ce contrôleur le maître de cluster de contrôle.

Par exemple :

```
NSX-Controller1> initialize control-cluster
Control cluster initialization successful.
```

4 Exécutez la commande `get control-cluster status verbose`.

Assurez-vous que les attributs `is master` et `in majority` sont définis sur `true`, que l'état est `active` et que `Zookeeper Server IP` est défini sur `reachable, ok`.

```
nsx-controller1> get control-cluster status verbose
NSX Controller Status:

uuid: 78d5b561-4f66-488d-9e53-089735eac1c1
is master: true
in majority: true
uuid                address                status
78d5b561-4f66-488d-9e53-089735eac1c1 192.168.110.34    active

Cluster Management Server Status:

uuid                rpc address                rpc port                global
id                vpn address                status
557a911f-41fd-4977-9c58-f3ef55b3efe7 192.168.110.34    7777
1                169.254.1.1                connected

Zookeeper Ensemble Status:

Zookeeper Server IP: 10.0.0.1, reachable, ok
Zookeeper version: 3.5.1-alpha--1, built on 03/08/2016 01:18 GMT
Latency min/avg/max: 0/0/1841
Received: 212095
Sent: 212125
Connections: 5
Outstanding: 0
Zxid: 0x10000017a
Mode: leader
Node count: 33
Connections: /10.0.0.1:51726[1]
(queueued=0,recved=60324,sent=60324,sid=0x100000f14a10003,lop=PING,est=1459376913497,to=30000,lcid=0
x8,lzid=0x10000017a,lresp=604617273,llat=0,minlat=0,avglat=0,maxlat=1088)
/10.0.0.1:35462[0](queueued=0,recved=1,sent=0)
/10.0.0.1:51724[1]
(queueued=0,recved=45786,sent=45803,sid=0x100000f14a10001,lop=GETC,est=1459376911226,to=40000,lcid=0
x21e,lzid=0x10000017a,lresp=604620658,llat=0,minlat=0,avglat=0,maxlat=1841)
/10.0.0.1:51725[1]
(queueued=0,recved=60328,sent=60333,sid=0x100000f14a10002,lop=PING,est=1459376913455,to=30000,lcid=0
```

```
xc,lzxid=0x10000017a,lresp=604618294,llat=0,minlat=0,avglat=0,maxlat=1356)
/10.0.0.1:51730[1]
(queued=0,recved=45315,sent=45324,sid=0x100000f14a10006,lop=PING,est=1459376914516,to=40000,lcxid=0
x49,lzxid=0x10000017a,lresp=604623243,llat=0,minlat=0,avglat=0,maxlat=1630)
```

Étape suivante

Ajoutez d'autres dispositifs NSX Controller au cluster de contrôle. Reportez-vous à la section [Relier les dispositifs NSX Controller au maître de cluster](#).

Relier les dispositifs NSX Controller au maître de cluster

Un cluster multinœud de dispositifs NSX Controller contribue à garantir qu'au moins un dispositif NSX Controller est toujours disponible.

Conditions préalables

- Installez un minimum de trois dispositifs NSX Controller.
- Vérifiez que vous disposez des privilèges d'administrateur pour vous connecter aux dispositifs NSX Controller.
- Assurez-vous que les nœuds NSX Controller sont reliés au plan de gestion. Reportez-vous à la section [Joindre des dispositifs NSX Controller à NSX Manager](#).
- Initialisez le cluster de contrôle pour créer un maître de cluster de contrôle. Vous devez initialiser le premier contrôleur uniquement.
- Dans la commande `join control-cluster`, vous devez utiliser une adresse IP, pas un nom de domaine.
- Si vous utilisez vCenter et que vous déployiez des contrôleurs NSX-T Data Center vers le même cluster, veillez à configurer des règles anti-affinité DRS. Les règles anti-affinité empêchent DRS de migrer plusieurs nœuds vers un même hôte.

Procédure

- 1 Ouvrez une session SSH pour chacun de vos dispositifs NSX Controller.

Par exemple, NSX-Controller1, NSX-Controller2 et NSX-Controller3. Dans cet exemple, NSX-Controller1 a déjà initialisé le cluster de contrôle et est déjà maître de cluster de contrôle.

- 2 Sur les dispositifs NSX Controller non maîtres, exécutez la commande `set control-cluster security-model` avec un mot de passe secret partagé. Le mot de passe secret partagé saisi pour NSX-Controller2 et NSX-Controller3 doit correspondre à celui qui a été saisi sur NSX-Controller1.

Par exemple :

```
NSX-Controller2> set control-cluster security-model shared-secret secret <NSX-Controller1's-shared-secret-password>
```

```
Security secret successfully set on the node.
```

```
NSX-Controller3> set control-cluster security-model shared-secret secret <NSX-Controller1's-shared-secret-password>
```

```
Security secret successfully set on the node.
```

- 3 Sur les dispositifs NSX Controller non maîtres, exécutez la commande `get control-cluster certificate thumbprint`.

La sortie de la commande est une chaîne numérique qui est unique pour chaque dispositif NSX Controller.

Par exemple :

```
NSX-Controller2> get control-cluster certificate thumbprint
...
```

```
NSX-Controller3> get control-cluster certificate thumbprint
...
```

- 4 Sur le dispositif NSX Controller maître, exécutez la commande **`join control-cluster`**;

Fournissez les informations suivantes :

- Adresse IP avec numéro de port facultatif des dispositifs NSX Controller non maîtres (NSX-Controller2 et NSX-Controller3 dans l'exemple)
- Empreinte numérique de certificat des dispositifs NSX Controller non maîtres

N'exécutez pas les commandes `join` parallèlement sur plusieurs contrôleurs. Assurez-vous que chaque jonction est terminée avant de relier un autre contrôleur.

```
NSX-Controller1> join control-cluster <NSX-Controller2-IP> thumbprint <nsx-controller2's-thumbprint>
Node 192.168.210.48 has successfully joined the control cluster.
Please run 'activate control-cluster' command on the new node.
```

Assurez-vous que NSX-Controller2 est relié au cluster en exécutant la commande `get control-cluster status`.

```
NSX-Controller1> join control-cluster <NSX-Controller3-IP> thumbprint <nsx-controller3's-
thumbprint>
Node 192.168.210.49 has successfully joined the control cluster.
Please run 'activate control-cluster' command on the new node.
```

Assurez-vous que NSX-Controller3 est relié au cluster en exécutant la commande `get control-cluster status`.

- 5 Sur les deux nœuds NSX Controller s'étant reliés au maître du cluster de contrôle, exécutez la commande `activate control-cluster`.

Note N'exécutez pas les commandes `activate` parallèlement sur plusieurs dispositifs NSX Controller. Assurez-vous que chaque activation est complète avant d'activer un autre contrôleur.

Par exemple :

```
NSX-Controller2> activate control-cluster
Control cluster activation successful.
```

Sur NSX-Controller2, exécutez la commande `get control-cluster status verbose` et assurez-vous que Zookeeper Server IP indique `reachable, ok`.

```
NSX-Controller3> activate control-cluster
Control cluster activation successful.
```

Sur NSX-Controller3, exécutez la commande `get control-cluster status verbose` et assurez-vous que Zookeeper Server IP indique `reachable, ok`.

- 6 Vérifiez le résultat en exécutant la commande `get control-cluster status`.

```
NSX-Controller1> get control-cluster status
uuid: db4aa77a-4397-4d65-ad33-9fde79ac3c5c
is master: true
in majority: true
  uuid                                address                status
  0cfe232e-6c28-4fea-8aa4-b3518baef00d 192.168.210.47         active
  bd257108-b94e-4e6d-8b19-7fa6c012961d 192.168.210.48         active
  538be554-1240-40e4-8e94-1497e963a2aa 192.168.210.49         active
```

Les premiers UUID répertoriés concernent le cluster de contrôle dans son ensemble. Chaque nœud NSX Controller possède également un UUID.

Si vous tentez de relier un contrôleur à un cluster et que la commande `set control-cluster security-model` ou `join control-cluster` échoue, les fichiers de configuration du cluster risquent de se trouver dans un état incohérent.

Pour résoudre ce problème, procédez comme suit :

- Sur le dispositif NSX Controller que vous tentez de relier au cluster, exécutez la commande `deactivate control-cluster`.
- Si la commande `get control-cluster status` ou `get control-cluster status verbose` affiche des informations relatives au contrôleur en échec sur le contrôleur maître, exécutez la commande `detach control-cluster <IP address of failed controller>`.

Étape suivante

Déployez NSX Edge. Reportez-vous à la section [Chapitre 6 Installation de NSX Edge](#).

Installation de NSX Edge

NSX Edge fournit des services de routage et la connectivité aux réseaux qui sont externes au déploiement NSX-T Data Center. Un NSX Edge est requis si vous souhaitez déployer un routeur de niveau 0 ou un routeur de niveau 1 avec des services avec état, comme la traduction d'adresse réseau (Network Address Translation, NAT), un VPN, etc.

Tableau 6-1. Exigences du déploiement, des plates-formes et de l'installation de NSX Edge

Exigences	Description
Méthodes de déploiement prises en charge	<ul style="list-style-type: none"> ■ OVA/OVF ■ ISO avec PXE ■ ISO sans PXE
Plates-formes prises en charge	<p>NSX Edge est pris en charge uniquement sur ESXi ou sur un système nu.</p> <p>NSX Edge n'est pas pris en charge sur KVM.</p>
installation PXE	La chaîne Mot de passe doit être chiffrée avec l'algorithme sha-512 pour le mot de passe de l'utilisateur racine et Admin.
Mot de passe du dispositif NSX-T Data Center	<ul style="list-style-type: none"> ■ Au moins huit caractères ■ Au moins une lettre minuscule ■ Au moins une lettre majuscule ■ Au moins un chiffre ■ Au moins un caractère spécial ■ Au moins cinq caractères différents ■ Aucun mot issu du dictionnaire ■ Aucun palindrome
Nom d'hôte	<p>Lorsque vous installez NSX Edge, spécifiez un nom d'hôte qui ne contient pas de caractères non valides comme un caractère de soulignement. Si le nom d'hôte contient un caractère non valide, après le déploiement, le nom d'hôte sera défini sur localhost. Pour plus d'informations sur les restrictions de nom d'hôte, reportez-vous à https://tools.ietf.org/html/rfc952 et https://tools.ietf.org/html/rfc1123.</p>
VMware Tools	VMTools est installé sur la machine virtuelle NSX Edge exécutée sur ESXi. Ne supprimez pas ou ne mettez pas VMTools à niveau.
Système	Vérifiez que la configuration requise est respectée. Reportez-vous à la section Configuration système requise .

Tableau 6-1. Exigences du déploiement, des plates-formes et de l'installation de NSX Edge (Suite)

Exigences	Description
Ports NSX	<p>Vérifiez que les ports requis sont ouverts. Reportez-vous à la section Ports et protocoles.</p> <p>Créez le réseau du groupe de ports de machines virtuelles cible, si celui-ci n'existe pas déjà. Il est recommandé de placer les dispositifs NSX-T Data Center sur un réseau de machines virtuelles de gestion.</p>
Adresses IP	<p>Si vous disposez de plusieurs réseaux de gestion, vous pouvez ajouter des itinéraires statiques aux autres réseaux à partir du dispositif NSX-T Data Center.</p> <p>Planifiez votre schéma d'adresses IP IPv4. Dans cette version de NSX-T Data Center, IPv6 n'est pas pris en charge.</p> <p>Le format IPv6 n'est pas pris en charge.</p>
Modèle OVF	<ul style="list-style-type: none"> ■ Vérifiez que vous disposez des privilèges appropriés pour déployer un modèle OVF sur l'hôte ESXi. ■ Vérifiez que les noms d'hôte n'incluent pas de traits de soulignement. Autrement, le nom d'hôte est défini sur <i>nsx-manager</i>. ■ Un outil de gestion pouvant déployer des modèles OVF, tels que vCenter Server ou vSphere Client. <p>L'outil de déploiement de modèles OVF doit prendre en charge des options de configuration qui permettent la configuration manuelle.</p> <ul style="list-style-type: none"> ■ Le plug-in d'intégration du client doit être installé.
Serveur NTP	Le même serveur NTP doit être configuré sur tous les serveurs NSX Edge dans un cluster Edge.

Scénarios d'installation de NSX Edge

Important Lorsque vous installez NSX Edge à partir d'un fichier OVA ou OVF, depuis vSphere Web Client ou depuis la ligne de commande, les valeurs de propriété OVA/OVF, telles que les noms d'utilisateur, les mots de passe ou les adresses IP, ne sont pas validées avant la mise sous tension de la machine virtuelle.

- Si vous spécifiez un nom d'utilisateur pour l'utilisateur **admin** ou **audit**, le nom doit être unique. Si vous spécifiez le même nom, il est ignoré et les noms par défaut (**admin** et **audit**) sont utilisés.
- Si le mot de passe de l'utilisateur **admin** ne respecte pas les conditions requises de complexité, vous devez vous connecter à NSX Edge via SSH ou à la console en tant qu'utilisateur **admin** avec le mot de passe **vmware**. Vous êtes invité à modifier le mot de passe.
- Si le mot de passe de l'utilisateur **audit** ne respecte pas les exigences de complexité, le compte d'utilisateur est désactivé. Pour activer le compte, connectez-vous à NSX Edge via SSH ou à la console en tant qu'utilisateur **admin** et exécutez la commande **set user audit** pour définir le mot de passe de l'utilisateur **audit** (le mot de passe actuel est une chaîne vide).

- Si le mot de passe de l'utilisateur **racine** ne respecte pas les exigences de complexité, vous devez vous connecter à NSX Edge via SSH ou à la console en tant que **racine** avec le mot de passe **vmware**. Vous êtes invité à modifier le mot de passe.



Attention Les modifications apportées à NSX-T Data Center tout en étant connecté avec les informations d'identification de l'utilisateur **racine** peuvent provoquer la défaillance du système et avoir éventuellement un impact sur votre réseau. Vous pouvez uniquement apporter des modifications à l'aide des informations d'identification de l'utilisateur **racine** en suivant les instructions de l'équipe de support de VMware.

Note Sur le dispositif, les services de base ne démarrent pas tant qu'un mot de passe suffisamment complexe n'a pas été défini.

Après avoir déployé NSX Edge à partir d'un fichier OVA, vous ne pouvez pas modifier les paramètres IP de la machine virtuelle en mettant la machine virtuelle hors tension, puis en modifiant les paramètres OVA de vCenter Server.

Ce chapitre contient les rubriques suivantes :

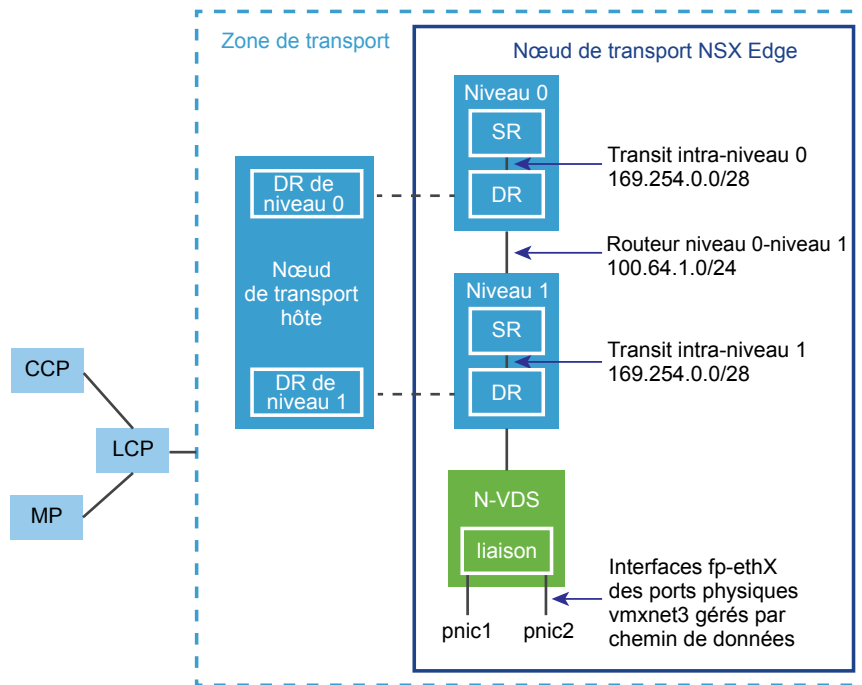
- [Configuration réseau de NSX Edge](#)
- [Déploiement automatique de machines virtuelles NSX Edge à partir de NSX Manager](#)
- [Installer un dispositif NSX Edge sur ESXi à l'aide d'une interface utilisateur graphique vSphere](#)
- [Installer NSX Edge sur ESXi à l'aide de l'outil OVF de ligne de commande](#)
- [Installer NSX Edge à l'aide d'un fichier ISO avec un serveur PXE](#)
- [Relier NSX Edge au plan de gestion](#)

Configuration réseau de NSX Edge

NSX Edge peut être installé en utilisant ISO, OVA/OVF ou le démarrage PXE. Quelle que soit la méthode d'installation, assurez-vous que la mise en réseau de l'hôte est préparée avant d'installer NSX Edge.

Vue générale de NSX Edge dans une zone de transport

Les nœuds NSX Edge sont des dispositifs de service avec des pools de capacité, dédiés aux services réseau en cours d'exécution qui ne peuvent pas être distribués aux hyperviseurs. Les nœuds Edge peuvent être considérés comme des conteneurs vides lorsqu'ils sont déployés pour la première fois.

Chiffre 6-1. Présentation générale de NSX Edge

Un nœud NSX Edge est le dispositif qui fournit des cartes réseau physiques pour se connecter à l'infrastructure physique. Ces fonctionnalités incluent :

- Connectivité à l'infrastructure physique
- NAT
- Serveur DHCP
- Proxy de métadonnées
- Edge Firewall

Lorsque l'un de ces services est configuré ou qu'une liaison montante est définie sur le routeur logique pour se connecter à l'infrastructure physique, un SR est instancié sur le nœud NSX Edge. Le nœud NSX Edge est également un nœud de transport comme les nœuds de calcul dans NSX-T Data Center et similaire au nœud de calcul que NSX Edge peut connecter à plusieurs zones de transport : un pour la superposition et l'autre pour l'homologation nord-sud avec des périphériques externes. Il existe deux zones de transport sur NSX Edge :

Zone de transport de superposition : tout le trafic provenant d'une VM participant au domaine NSX-T Data Center peut nécessiter une accessibilité à des périphériques ou des réseaux externes. Cela est généralement décrit comme un trafic externe nord-sud. Le nœud NSX Edge est responsable de la décapsulation du trafic de superposition reçu depuis les nœuds de calcul, ainsi que de l'encapsulation du trafic envoyé aux nœuds de calcul.

Zone de transport VLAN : en plus de la fonction d'encapsulation ou de décapsulation du trafic, les nœuds NSX Edge ont également besoin d'une zone de transport VLAN pour fournir une connectivité de liaison montante à l'infrastructure physique.

Par défaut, les liens entre le SR et le DR utilisent le sous-réseau 169.254.0.0/28. Ces liens de transit intra-routeur sont créés automatiquement lorsque vous déployez un routeur logique de niveau 0 ou de niveau 1. Vous n'avez pas besoin de configurer ou de modifier la configuration du lien sauf si le sous-réseau 169.254.0.0/28 est déjà utilisé dans votre déploiement. Sur un routeur logique de niveau 1, le SR est présent uniquement si vous sélectionnez un dispositif NSX Edge lors de la création du routeur logique de niveau 1.

L'espace d'adressage par défaut attribué aux connexions de niveau 0 à niveau 1 est l'espace 100.64.0.0/10. Chaque connexion homologue de niveau 0 à niveau 1 reçoit un sous-réseau /31 dans l'espace d'adressage 100.64.0.0/10. Ce lien est créé automatiquement lorsque vous créez un routeur de niveau 1 et que vous le connectez à un routeur de niveau 0. Vous n'avez pas besoin de configurer ou de modifier les interfaces sur ce lien sauf si le sous-réseau 100.64.0.0/10 est déjà utilisé dans votre déploiement.

Chaque déploiement NSX-T Data Center comporte un cluster de plan de gestion (MP) et un cluster de plan de contrôle (CCP). Le MP et le CCP transfèrent les configurations vers le plan de contrôle local (LCP) de chaque zone de transport. Lorsqu'un hôte ou un dispositif NSX Edge rejoint le plan de gestion, l'agent du plan de gestion (MPA) établit la connectivité avec l'hôte ou le dispositif NSX Edge, et ce dernier NSX Edge devient un nœud d'infrastructure NSX-T Data Center. Lorsque le nœud d'infrastructure est ensuite ajouté en tant que nœud de transport, la connectivité LCP est établie avec l'hôte ou le dispositif NSX Edge.

Le schéma Présentation générale de NSX Edge montre un exemple de deux cartes réseau physiques (pNIC1 et pNIC2) qui sont liées pour fournir une haute disponibilité. Le chemin des données gère les cartes réseau physiques. Elles peuvent servir soit de liaisons montantes VLAN vers un réseau externe, soit de liens de point de terminaison de tunnel vers des réseaux de machines virtuelles internes gérés par NSX-T Data Center.

Il est recommandé d'allouer au moins deux liens physiques à chaque dispositif NSX Edge qui est déployé en tant que VM. Vous pouvez éventuellement faire chevaucher les groupes de ports sur la même pNIC en utilisant différents ID de VLAN. Le premier lien réseau trouvé est utilisé pour la gestion. Par exemple, sur une VM NSX Edge, le premier lien trouvé pourrait être vnic1.

Pour une installation bare metal, le premier lien trouvé pourrait être eth0 ou em0. Les liens restants sont utilisés pour les liaisons montantes et les tunnels. Par exemple, l'un d'eux pourrait être destiné à un point de terminaison de tunnel utilisé par les VM gérées par NSX-T Data Center. L'autre pourrait être destiné à une liaison montante TOR NSX Edge dirigée vers l'extérieur.

Vous pouvez afficher les informations de lien physique de NSX Edge, vous connecter à l'interface de ligne de commande en tant qu'administrateur et exécuter les commandes `get interfaces` et `get physical-ports`. Dans l'API, vous pouvez utiliser l'appel d'API `GET fabric/nodes/<edge-node-id>/network/interfaces`.

Que vous installiez NSX Edge sur un système nu ou en tant que machine virtuelle, vous disposez de plusieurs options pour la configuration réseau, en fonction de votre déploiement.

Zones de transport et N-VDS

Les zones de transport contrôlent l'accessibilité des réseaux de couche 2 dans NSX-T Data Center. Un N-VDS est un commutateur logiciel qui est créé sur un nœud de transport. Le composant principal impliqué dans le plan de données des nœuds de transport est le N-VDS. Le N-VDS transfère le trafic entre les composants exécutés sur le nœud de transport par exemple, entre des machines virtuelles ou entre des composants internes et le réseau physique. Dans ce dernier cas, le N-VDS doit posséder une ou plusieurs interfaces physiques (pNIC) sur le nœud de transport. Comme avec les autres commutateurs virtuels, un N-VDS ne peut pas partager une interface physique avec un autre N-VDS. Il peut coexister avec un autre N-VDS lors de l'utilisation d'un ensemble distinct de pNIC.

Il existe deux types de zones de transport :

- Superposition pour la tunnellation NSX-T Data Center interne entre les nœuds de transport.
- VLAN pour les liaisons montantes externes à NSX-T Data Center.

Cette opération se justifie si vous souhaitez que chaque dispositif NSX Edge n'ait qu'un seul N-VDS. Il est également possible d'intégrer NSX Edge à plusieurs zones de transport VLAN, à raison d'une pour chaque liaison montante.

Le choix de conception le plus courant consiste à définir trois zones de transport : une superposition et deux zones de transport VLAN pour les liaisons montantes redondantes.

Pour plus d'informations sur les zones de transport, reportez-vous à [À propos des zones de transport](#).

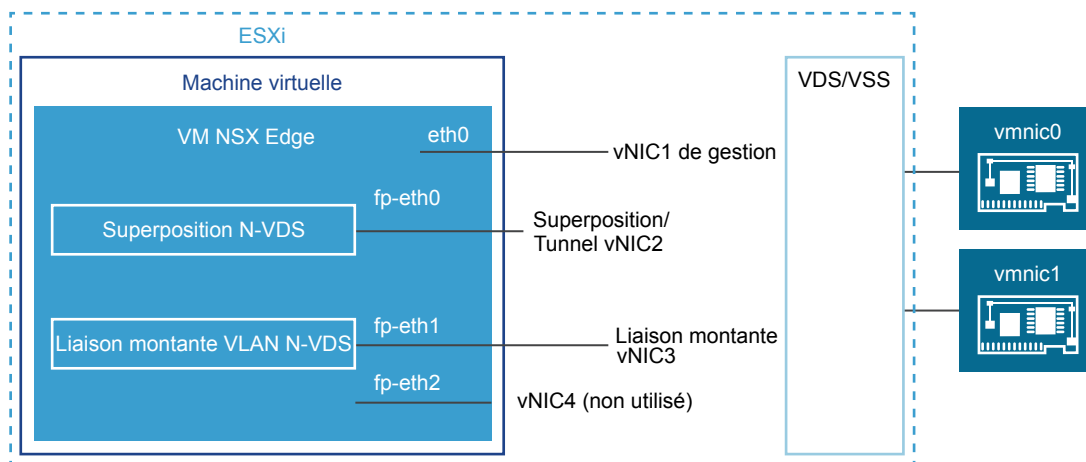
Mise en réseau NSX Edge de dispositifs virtuels/machines virtuelles

Une VM NSX Edge dispose de quatre interfaces internes : eth0, fp-eth0, fp-eth1 et fp-eth2. Eth0 est réservé à la gestion et les autres interfaces sont attribuées au chemin d'accès rapide DPDK. Ces interfaces sont allouées pour des liaisons montantes vers des commutateurs ToR et pour la tunnellation de superposition NSX-T Data Center. L'attribution d'interface est flexible pour la liaison montante ou la superposition. Par exemple, fp-eth0 peut être attribué pour le trafic de superposition avec fp-eth1, fp-eth2 ou les deux pour le trafic de liaison montante.

Sur le commutateur distribué vSphere ou le commutateur standard vSphere, vous devez allouer au moins deux vmnic au dispositif NSX Edge pour la redondance.

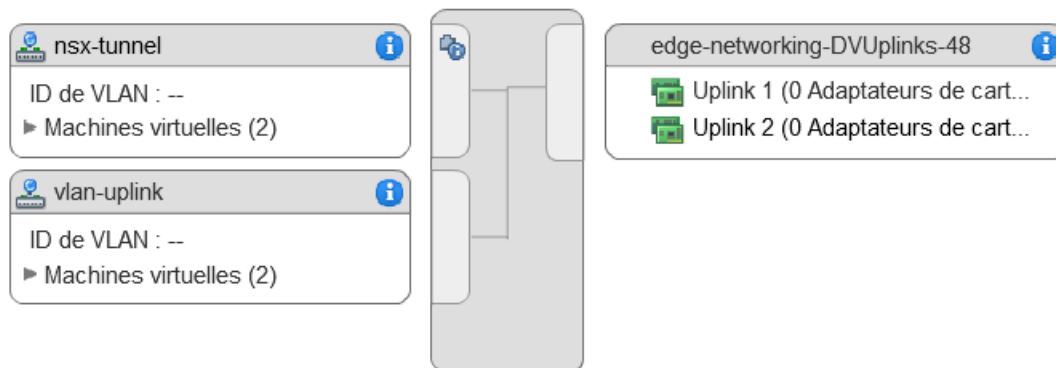
Dans l'exemple de topologie physique suivant, eth0 est utilisé pour le réseau de gestion, fp-eth0 est utilisé pour le trafic de superposition NSX-T Data Center, fp-eth1 est utilisé pour la liaison montante VLAN et fp-eth2 n'est pas utilisé. Si fp-eth2 n'est pas utilisé, vous devez le déconnecter.

Chiffre 6-2. Configuration de lien suggérée pour la mise en réseau de machines virtuelles NSX Edge



Le dispositif NSX Edge représenté dans cet exemple appartient à deux zones de transport (une superposition et un réseau local virtuel) et possède donc deux N-VDS, un pour le tunnel et l'autre pour le trafic de liaison montante.

Cette capture d'écran montre les groupes de ports de machine virtuelle, nsx-tunnel et vlan-uplink.



Pendant le déploiement, vous devez spécifier les noms de réseau correspondant aux noms configurés sur vos groupes de ports de machine virtuelle. Ainsi, pour faire correspondre les groupes de ports de machine virtuelle dans notre exemple, les paramètres ovftool du réseau peuvent être les suivants si vous utilisez la commande ovftool pour déployer NSX Edge :

```
--net:"Network 0-Mgmt" --net:"Network 1-nsx-tunnel" --net:"Network 2=vlan-uplink"
```

L'exemple illustré ici utilise les noms de groupe de ports de machine virtuelle Mgmt, nsx-tunnel et vlan-uplink. Vous pouvez utiliser n'importe quel nom pour vos groupes de ports de machine virtuelle.

Par exemple, sur un vSwitch standard, vous configurez les ports de jonction comme suit : **Hôte > Configuration > Mise en réseau > Ajouter une mise en réseau > Machine virtuelle > ID VLAN Tous (4095).**

La VM NSX Edge peut être installée sur un commutateur distribué vSphere ou sur des commutateurs standard vSphere.

Une machine virtuelle NSX Edge peut être installée sur un hôte NSX-T Data Center préparé et configurée comme un nœud de transport. Il existe deux types de déploiement :

- Une machine virtuelle NSX Edge peut être déployée à l'aide de groupes de ports VSS/VDS où VSS/VDS consomment des pNIC(s) distincts sur l'hôte. Le nœud de transport d'hôte consomme une ou des pNIC distinctes pour l'instance de N-VDS installée sur l'hôte. L'instance de N-VDS du nœud de transport d'hôte coexiste avec VSS ou VDS, les deux consommant des pNIC distinctes. Le TEP (point de terminaison de tunnel) de l'hôte et le TEP de NSX Edge peuvent se trouver dans le même sous-réseau ou des sous-réseaux distincts.
- Une machine virtuelle NSX Edge peut être déployée à l'aide de commutateurs logiques soutenus par VLAN sur le N-VDS du nœud de transport d'hôte. Le TEP de l'hôte et le TEP de NSX Edge doivent se trouver dans des sous-réseaux distincts.

Plusieurs VM NSX Edge peuvent être installées sur un hôte unique, en utilisant les mêmes groupes de ports de gestion, VLAN et de superposition.

Pour une VM NSX Edge déployée sur un hôte ESXi disposant de vSphere et non de N-VDS, vous devez procéder comme suit :

- Activez la fausse transmission pour le serveur DHCP en cours d'exécution sur ce dispositif NSX Edge.
- Activez le mode promiscuité pour que la VM NSX Edge reçoive des paquets de monodiffusion inconnus, l'apprentissage MAC étant désactivé par défaut. Cela n'est pas nécessaire pour vDS 6.6 ou version ultérieure, l'apprentissage MAC étant activé par défaut.

Mise en réseau de NSX Edge sur un système nu

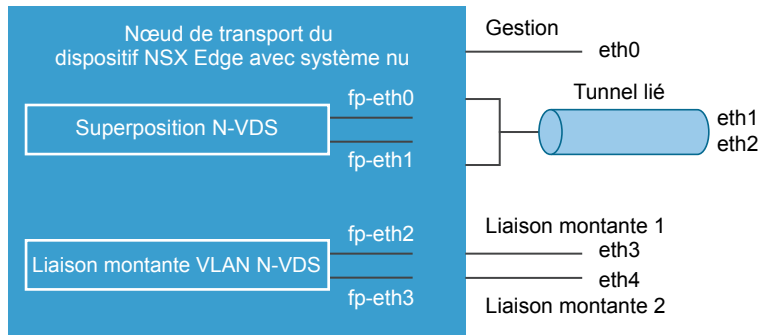
Le dispositif NSX Edge bare metal NSX-T Data Center s'exécute sur un serveur physique et est installé à l'aide d'un fichier ISO ou d'un démarrage PXE. Le dispositif NSX Edge bare metal est recommandé pour les environnements de production où des services comme NAT, pare-feu et équilibrage de charge sont nécessaires en plus du transfert de monodiffusion de couche 3. Un dispositif NSX Edge bare metal diffère du format de la VM NSX Edge en termes de performances. Il fournit une convergence quasi instantanée, un basculement plus rapide et un débit plus élevé.

Lorsqu'un nœud NSX Edge bare metal est installé, une interface dédiée est conservée pour la gestion. Si la redondance est souhaitée, deux cartes réseau peuvent être utilisées pour la haute disponibilité du plan de gestion. Ces interfaces de gestion peuvent également être 1G.

Le nœud NSX Edge bare metal prend en charge un maximum de 8 cartes réseau physiques pour le trafic de superposition et le trafic de liaison montante vers les commutateurs ToR (Top-of-Rack). Pour chacune de ces 8 cartes réseau physiques sur le serveur, une interface interne est créée en respectant le schéma de dénomination « fp-ethX ». Ces interfaces internes sont attribuées au chemin d'accès rapide DPDK. L'attribution d'interfaces fp-eth pour la connectivité de superposition ou de liaison montante est entièrement flexible.

Dans l'exemple de topologie physique suivant, fp-eth0 et fp-eth1 sont liés et utilisés pour le tunnel de superposition NSX-T Data Center. fp-eth2 et fp-eth3 sont utilisés en tant que liaisons montantes VLAN redondantes vers des appareils TOR.

Chiffre 6-3. Configuration de lien suggérée pour la mise en réseau de NSX Edge sur système nu



Déploiement automatique de machines virtuelles NSX Edge à partir de NSX Manager

Vous pouvez configurer un dispositif NSX Edge dans l'interface utilisateur de NSX Manager et déployer automatiquement le dispositif NSX Edge dans vCenter Server.

Conditions préalables

- Consultez les conditions de réseau de NSX Edge dans [Configuration réseau de NSX Edge](#).
- Si un vCenter Server est enregistré en tant que gestionnaire de calcul dans NSX-T Data Center, vous pouvez utiliser l'interface utilisateur NSX Manager pour configurer un hôte comme nœud NSX Edge et le déployer automatiquement sur vCenter Server.
- Vérifiez que la banque de données vCenter Server sur laquelle le dispositif NSX Edge est installé possède un minimum de 120 Go disponibles.
- Vérifiez que le cluster ou l'hôte vCenter Server a accès à la banque de données et aux réseaux spécifiés dans la configuration.

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Infrastructure > Nœuds > Dispositifs Edge > Ajouter une VM Edge**.
- 3 Tapez un nom pour le dispositif NSX Edge.
- 4 Tapez le nom d'hôte ou le nom de domaine complet de vCenter Server.
- 5 Sélectionnez une taille de configuration : petite, moyenne ou grande.

La configuration requise varie selon la taille de la configuration.

- 6 Spécifiez les mots de passe d'interface de ligne de commande et racine pour les systèmes.

Les restrictions sur les mots de passe d'administrateur racine et d'interface de ligne de commande s'appliquent également pour le déploiement automatique.

- 7 Sélectionnez le gestionnaire de calcul dans le menu déroulant.

Le gestionnaire de calcul est le dispositif vCenter Server enregistré dans le plan de gestion.

- 8 Pour le gestionnaire de calcul, sélectionnez un cluster dans le menu déroulant ou attribuez un pool de ressources.

- 9 Sélectionnez une banque de données pour le stockage des fichiers des machines virtuelles de NSX Edge.

- 10 Sélectionnez le cluster sur lequel vous voulez déployer la machine virtuelle NSX Edge.

Il est recommandé d'ajouter le dispositif NSX Edge dans un cluster qui fournit des utilitaires de gestion de réseau.

- 11 Sélectionnez l'hôte ou un pool de ressources. Un seul hôte peut être ajouté à la fois.

- 12 Sélectionnez l'adresse IP et tapez les adresses IP de réseau de gestion et les chemins d'accès sur lesquels vous voulez placer les interfaces de NSX Edge. L'adresse IP saisie doit être au format CIDR.

Le réseau de gestion doit être capable d'accéder au dispositif NSX Manager. Il doit recevoir son adresse IP à partir d'un serveur DHCP. Vous pouvez changer ces réseaux après le déploiement du dispositif NSX Edge.

- 13 Ajoutez une passerelle par défaut si l'adresse IP de réseau de gestion n'appartient pas à la même couche 2 que le réseau NSX Manager.

Vérifiez que la connectivité de couche 3 est disponible entre NSX Manager et le réseau de gestion NSX Edge.

Le déploiement de NSX Edge dure entre 1 et 2 minutes. Vous pouvez suivre l'état du déploiement en temps réel dans l'interface utilisateur.

Étape suivante

Si le déploiement de NSX Edge échoue, accédez aux fichiers `/var/log/cm-inventory/cm-inventory.log` et `/var/log/proton/nsxapi.log` pour résoudre le problème.

Avant d'ajouter le dispositif NSX Edge à un cluster NSX Edge ou de le configurer comme nœud de transport, assurez-vous que le nœud NSX Edge que vous venez de créer s'affiche en tant que nœud prêt.

Installer un dispositif NSX Edge sur ESXi à l'aide d'une interface utilisateur graphique vSphere

Si vous préférez une installation interactive de NSX Edge, vous pouvez utiliser un outil de gestion de machine virtuelle doté d'une interface utilisateur, tel que vSphere Client connecté à vCenter Server.

Dans cette version de NSX-T Data Center, IPv6 n'est pas pris en charge.

Conditions préalables

- Consultez les conditions de réseau de NSX Edge dans [Configuration réseau de NSX Edge](#).

Procédure

- 1 Localisez le fichier OVA ou OVF de NSX Edge.

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

- 2 Dans l'outil de gestion, lancez l'assistant **Déployer un modèle OVF**, puis accédez au fichier .ova ou à un lien vers ce fichier.

- 3 Entrez un nom pour le dispositif NSX Edge, puis sélectionnez un dossier ou un centre de données de vCenter Server.

Le nom saisi s'affiche dans l'inventaire.

Le dossier que vous sélectionnez est utilisé pour appliquer des autorisations au dispositif NSX Edge.

- 4 Sélectionnez une taille de configuration : petite, moyenne ou grande.

La configuration système requise varie selon la taille du déploiement de NSX Edge. Reportez-vous à la section [Configuration système requise](#).

- 5 Sélectionnez une banque de données pour stocker les fichiers du dispositif virtuel NSX Edge.

- 6 Si vous effectuez une installation dans vCenter Server, sélectionnez un hôte ou un cluster sur lequel déployer le dispositif NSX Edge.

- 7 Sélectionnez les réseaux sur lesquels placer les interfaces NSX Edge.

Vous pouvez changer ces réseaux après le déploiement du dispositif NSX Edge.

- 8 Spécifiez le mot de passe et les paramètres IP du dispositif NSX Edge.

- 9 (Facultatif) Pour des performances optimales, réservez de la mémoire pour le composant NSX-T Data Center.

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 sur un niveau qui garantit que le composant NSX-T Data Center dispose de suffisamment de mémoire pour s'exécuter efficacement. Reportez-vous à la section [Configuration système requise](#).

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

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

- 11 Après le démarrage de NSX Edge, connectez-vous avec des privilèges d'administrateur à l'interface de ligne de commande. Le nom d'utilisateur est **admin** et le mot de passe est **default**.

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

- 12 Après le redémarrage, vous pouvez vous connecter avec les informations d'identification de l'administrateur ou de l'utilisateur racine. Le mot de passe par défaut de l'utilisateur racine est **vmware**.
- 13 Exécutez la commande `get interface eth0` pour vérifier que l'adresse IP a été appliquée comme il convient

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

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

Si nécessaire, exécutez la commande `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` pour mettre à jour l'interface de gestion. Vous pouvez éventuellement démarrer le service SSH à l'aide de la commande `start service ssh`.

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

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

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

- 15 Résolvez les problèmes de connectivité.

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

Par défaut, le chemin de données du dispositif NSX Edge réclame toutes les cartes réseau des machines virtuelles à l'exception de la carte réseau de gestion (celle qui possède une adresse IP et un itinéraire par défaut). Si DHCP attribue la mauvaise carte réseau comme solution de gestion, effectuez les tâches pour corriger le problème.

- a Connectez-vous à l'interface de ligne de commande et tapez la commande **stop service dataplane**.
- b Tapez la commande **set interface eth0 dhcp plane mgmt**.

- c Placez eth0 dans le réseau DHCP et attendez qu'une adresse IP soit attribuée à eth0.
- d Tapez la commande **start service dataplane**.

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

Étape suivante

Reliez le dispositif NSX Edge au plan de gestion. Reportez-vous à la section [Relier NSX Edge au plan de gestion](#).

Installer NSX Edge sur ESXi à l'aide de l'outil OVF de ligne de commande

Si vous préférez automatiser l'installation de NSX Edge, vous pouvez utiliser l'outil OVF de VMware, qui est un utilitaire de ligne de commande.

Dans cette version de NSX-T Data Center, IPv6 n'est pas pris en charge.

Conditions préalables

- Vérifiez que la configuration requise est respectée. Reportez-vous à la section [Configuration système requise](#).
- Vérifiez que les ports requis sont ouverts. Reportez-vous à la section [Ports et protocoles](#).
- Créez le réseau du groupe de ports de machines virtuelles cible, si celui-ci n'existe pas déjà. Il est recommandé de placer les dispositifs NSX-T Data Center sur un réseau de machines virtuelles de gestion.

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

- Planifiez votre schéma d'adresses IP IPv4. Dans cette version de NSX-T Data Center, IPv6 n'est pas pris en charge.
- Consultez les conditions de réseau de NSX Edge dans [Configuration réseau de NSX Edge](#).
- Vérifiez que vous disposez des privilèges appropriés pour déployer un modèle OVF sur l'hôte ESXi.
- Vérifiez que les noms d'hôte n'incluent pas de traits de soulignement. Autrement, le nom d'hôte est défini sur *localhost*.
- OVF Tool version 4.0 ou ultérieure.

Procédure

- Pour un hôte autonome, exécutez la commande `ovftool` avec les paramètres appropriés.

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-edge-1
--deploymentOption=medium
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--net:"Network 0=Mgmt"
--net:"Network 1=nsx-tunnel"
--net:"Network 2=vlan-uplink"
--net:"Network 3=vlan-uplink"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.37
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=True
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-edge
<path/url to nsx component ova>
vi://root:<password>@192.168.110.51
```

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://root@192.168.110.24
Deploying to VI: vi://root@192.168.110.24
Transfer Completed
Powering on VM: nsx-edge-1
Task Completed
Completed successfully
```

- Pour un hôte géré par vCenter Server, exécutez la commande `ovftool` avec les paramètres appropriés.

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-edge-1
--deploymentOption=medium
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
```

```

--datastore=ds1
--net:"Network 0=Mgmt"
--net:"Network 1=nsx-tunnel"
--net:"Network 2=vlan-uplink"
--net:"Network 3=vlan-uplink"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.37
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=True
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-edge
<path/url to nsx component ova>
vi://administrator@vsphere.local:<password>@192.168.110.24/?ip=192.168.210.53

```

```

Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://administrator@vsphere.local@192.168.110.24:443/
Deploying to VI: vi://administrator@vsphere.local@192.168.110.24:443/
Transfer Completed
Powering on VM: nsx-edge-1
Task Completed
Completed successfully

```

- (Facultatif) Pour des performances optimales, réservez de la mémoire pour le composant NSX-T Data Center.

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 sur un niveau qui garantit que le composant NSX-T Data Center dispose de suffisamment de mémoire pour s'exécuter efficacement. Reportez-vous à la section [Configuration système requise](#).

- Ouvrez la console de NSX Edge pour suivre le processus de démarrage.
- Après le démarrage de NSX Edge, connectez-vous avec des privilèges d'administrateur à l'interface de ligne de commande. Le nom d'utilisateur est **admin** et le mot de passe est **default**.

- Exécutez la commande `get interface eth0` pour vérifier que l'adresse IP a été appliquée comme il convient

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

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

Si nécessaire, exécutez la commande `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` pour mettre à jour l'interface de gestion. Vous pouvez éventuellement démarrer le service SSH à l'aide de la commande `start service ssh`.

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

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

- Vous pouvez effectuer un test ping de votre dispositif NSX Edge.
- NSX Edge peut effectuer un test ping de sa passerelle par défaut.
- NSX Edge peut effectuer un test ping des hôtes d'hyperviseur qui se trouvent sur le même réseau que le dispositif NSX Edge.
- NSX Edge peut effectuer un test ping de son serveur DNS et de son serveur NTP.
- Résolvez les problèmes de connectivité.

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

Par défaut, le chemin de données du dispositif NSX Edge réclame toutes les cartes réseau des machines virtuelles à l'exception de la carte réseau de gestion (celle qui possède une adresse IP et un itinéraire par défaut). Si DHCP attribue la mauvaise carte réseau comme solution de gestion, effectuez les tâches pour corriger le problème.

- Connectez-vous à l'interface de ligne de commande et tapez la commande **stop service dataplane**.
- Tapez la commande **set interface eth0 dhcp plane mgmt**.
- Placez eth0 dans le réseau DHCP et attendez qu'une adresse IP soit attribuée à eth0.
- Tapez la commande **start service dataplane**.

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

Étape suivante

Reliez le dispositif NSX Edge au plan de gestion. Reportez-vous à la section [Relier NSX Edge au plan de gestion](#).

Installer NSX Edge à l'aide d'un fichier ISO avec un serveur PXE

Vous pouvez installer des dispositifs NSX Edge automatiquement sur un système nu ou en tant que machine virtuelle à l'aide de PXE.

Note L'installation via l'environnement de démarrage PXE n'est pas prise en charge pour NSX Manager et NSX Controller. Vous ne pouvez pas non plus configurer des paramètres de mise en réseau, tels que l'adresse IP, la passerelle, le masque réseau, NTP et DNS.

Préparer le serveur PXE pour une installation de NSX Edge

PXE comprend plusieurs composants : DHCP, HTTP et TFTP. Cette procédure illustre la configuration d'un serveur PXE sous Ubuntu.

DHCP distribue dynamiquement les paramètres IP aux composants NSX-T Data Center, tels que NSX Edge. Dans un environnement PXE, le serveur DHCP autorise NSX Edge à demander et à recevoir automatiquement une adresse IP.

TFTP est un protocole de transfert de fichier. Le serveur TFTP écoute toujours les clients PXE sur le réseau. Lorsqu'il détecte un client PXE demandant des services PXE, il fournit le fichier ISO de composants NSX-T Data Center et les paramètres d'installation contenus dans un fichier présélectionné.

Conditions préalables

- Un serveur PXE doit être disponible dans votre environnement de déploiement. Le serveur PXE peut être défini dans n'importe quelle distribution Linux. Le serveur PXE doit posséder deux interfaces, l'une pour les communications externes, l'autre pour les services IP DHCP et TFTP.

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

- Dans le fichier de configuration prédéfini, vérifiez que les paramètres `net.ifnames=0` et `biosdevname=0` sont définis après `--` afin de persister après le redémarrage.
- Consultez les conditions de réseau de NSX Edge dans [Configuration réseau de NSX Edge](#).

Procédure

- 1 (Facultatif) Utilisez un fichier kickstart pour configurer un nouveau service TFTP ou DHCP sur un serveur Ubuntu.

Un fichier kickstart est un fichier texte contenant des commandes CLI que vous exécutez sur le dispositif après le premier démarrage.

Nommez le fichier kickstart en fonction du serveur PXE sur lequel il pointe. Par exemple :

```
nsxcli.install
```

Le fichier doit être copié sur votre serveur Web, par exemple, à l'adresse `/var/www/html/nsx-edge/nsxcli.install`.

Dans le fichier kickstart, vous pouvez ajouter des commandes CLI. Par exemple, pour configurer l'adresse IP de l'interface de gestion :

```
stop dataplane
set interface eth0 <ip-cidr-format> plane mgmt
start dataplane
```

Pour modifier le mot de passe de l'utilisateur Admin :

```
set user admin password <new_password> old-password <old-password>
```

Si vous spécifiez un mot de passe dans le fichier `preseed.cfg`, vous devez utiliser le même mot de passe dans le fichier kickstart. Autrement, utilisez le mot de passe par défaut (« default »).

Pour relier le dispositif NSX Edge au plan de gestion :

```
join management-plane <mgr-ip> thumbprint <mgr-thumbprint> username <mgr-username> password <mgr-password>
```

2 Créez deux interfaces, l'une pour la gestion et l'autre pour les services DHCP et TFTP.

Assurez-vous que l'interface DHCP/TFTP réside sur le même sous-réseau que celui où le dispositif NSX Edge se trouve.

Par exemple, si les interfaces de gestion NSX Edge doivent résider sur le sous-réseau 192.168.210.0/24, placez `eth1` sur ce même sous-réseau.

```
# The loopback network interface
auto lo
iface lo inet loopback

# PXE server's management interface
auto eth0
iface eth0 inet static
    address 192.168.110.81
    gateway 192.168.110.1
    netmask 255.255.255.0
    dns-nameservers 192.168.110.10

# PXE server's DHCP/TFTP interface
auto eth1
iface eth1 inet static
```

```
address 192.168.210.82
gateway 192.168.210.1
netmask 255.255.255.0
dns-nameservers 192.168.110.10
```

3 Installez le logiciel serveur DHCP.

```
sudo apt-get install isc-dhcp-server -y
```

4 Modifiez le fichier /etc/default/isc-dhcp-server, puis ajoutez l'interface qui fournit le service DHCP.

```
INTERFACES="eth1"
```

5 (Facultatif) Si vous voulez que ce serveur DHCP soit le serveur DHCP officiel du réseau local, supprimez le commentaire de la ligne **authoritative**; du fichier /etc/dhcp/dhcpd.conf.

```
...
authoritative;
...
```

6 Dans le fichier /etc/dhcp/dhcpd.conf, définissez les paramètres DHCP pour le réseau PXE.

Par exemple :

```
subnet 192.168.210.0 netmask 255.255.255.0 {
    range 192.168.210.90 192.168.210.95;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 192.168.110.10;
    option routers 192.168.210.1;
    option broadcast-address 192.168.210.255;
    default-lease-time 600;
    max-lease-time 7200;
}
```

7 Démarrez le service DHCP.

```
sudo service isc-dhcp-server start
```

8 Vérifiez que le service DHCP est en cours d'exécution.

```
service --status-all | grep dhcp
```

9 Installez Apache, TFTP et d'autres composants requis pour l'amorçage PXE.

```
sudo apt-get install apache2 tftpd-hpa inetutils-inetd
```

10 Vérifiez que TFTP et Apache sont en cours d'exécution.

```
service --status-all | grep tftpd-hpa
service --status-all | grep apache2
```

11 Ajoutez les lignes suivantes au fichier `/etc/default/tftpd-hpa`.

```
RUN_DAEMON="yes"
OPTIONS="-l -s /var/lib/tftpboot"
```

12 Ajoutez la ligne suivante au fichier `/etc/inetd.conf`.

```
tftp      dgram    udp       wait      root      /usr/sbin/in.tftpd /usr/sbin/in.tftpd -s /var/lib/tftpboot
```

13 Redémarrez le service TFTP.

```
sudo /etc/init.d/tftpd-hpa restart
```

14 Copiez ou téléchargez le fichier ISO du programme d'installation NSX Edge dans un dossier temporaire.**15** Montez le fichier ISO et copiez les fichiers d'installation sur le serveur TFTP et le serveur Apache.

```
sudo mount -o loop ~/nsx-edge.<build>.iso /mnt
cd /mnt
sudo cp -fr install/netboot/* /var/lib/tftpboot/
sudo mkdir /var/www/html/nsx-edge
sudo cp -fr /mnt/* /var/www/html/nsx-edge/
```

- 16** (Facultatif) Éditez le fichier `/var/www/html/nsx-edge/preseed.cfg` pour modifier les mots de passe chiffrés.

Vous pouvez utiliser un outil Linux, tel que `mkpasswd`, pour créer un hachage de mot de passe.

```
sudo apt-get install whois
sudo mkpasswd -m sha-512

Password:
$6$SUFGqs[...]FcoHLijOuFD
```

- a Modifiez le mot de passe racine, modifiez `/var/www/html/nsx-edge/preseed.cfg` et recherchez la ligne suivante :

```
d-i passwd/root-password-crypted password $6$tgmLNLmp$9BuAHhN...
```

- b Remplacez la chaîne de hachage.

Vous n'avez pas besoin d'échapper les caractères spéciaux tels que `$`, `'`, `"` ou `\`.

- c Ajoutez la commande `usermod` à `preseed.cfg` pour définir le mot de passe de l'utilisateur racine, de l'utilisateur Admin ou des deux.

Par exemple, recherchez la ligne `echo 'VMware NSX Edge'` et ajoutez la commande suivante.

```
usermod --password '$6\$VS3exId0aKmzW\$U3g0V7BF0DXlmRI.LR0v/VgloxVotEDp00b02hUF8u/' root; \
usermod --password '$6\$VS3exId0aKmzW\$U3g0V7BF0DXlmRI.LR0v/VgloxVotEDp00b02hUF8u/' admin; \
```

La chaîne de hachage est un exemple. Vous devez échapper tous les caractères spéciaux. Le mot de passe racine dans la première commande `usermod` remplace le mot de passe qui est défini dans `d-i passwd/root-password-crypted password 6tgm...`

Si vous utilisez la commande `usermod` pour définir le mot de passe, l'utilisateur n'est pas invité à le modifier lors de la première connexion. Dans les autres cas, l'utilisateur doit changer le mot de passe lors de la première connexion.

- 17** Ajoutez les lignes suivantes au fichier `/var/lib/tftpboot/pxelinux.cfg/default`.

Remplacez `192.168.210.82` par l'adresse IP de votre serveur TFTP.

```
label nsxedge
    kernel ubuntu-installer/amd64/linux
    ipappend 2
    append netcfg/dhcp_timeout=60 auto=true priority=critical vga=normal partman-
lvm/device_remove_lvm=true netcfg/choose_interface=auto debian-
installer/allow_unauthenticated=true preseed/url=http://192.168.210.82/nsx-edge/preseed.cfg
mirror/country=manual mirror/http/hostname=192.168.210.82 nsx-
kickstart/url=http://192.168.210.82/nsx-edge/nsxcli.install mirror/http/directory=/nsx-edge
initrd=ubuntu-installer/amd64/initrd.gz mirror/suite=xenial --
```

18 Ajoutez la ligne suivante au fichier `/etc/dhcp/dhcpd.conf`.

Remplacez 192.168.210.82 par l'adresse IP de votre serveur DHCP.

```
allow booting;
allow bootp;

next-server 192.168.210.82; #Replace this IP address
filename "pxelinux.0";
```

19 Redémarrez le service DHCP.

```
sudo service isc-dhcp-server restart
```

Note Si un message d'erreur apparaît, par exemple « arrêt : Instance inconnue : démarrage : Échec du démarrage du travail », exécutez `sudo /etc/init.d/isc-dhcp-server stop`, puis `sudo /etc/init.d/isc-dhcp-server start`. La commande `sudo /etc/init.d/isc-dhcp-server start` renvoie des informations sur la source de l'erreur.

Étape suivante

Installez NSX Edge à l'aide du système bare-metal ou du fichier ISO. Reportez-vous à la section [Installer un dispositif NSX Edge sur un système nu](#) ou [Installer NSX Edge par le biais d'un fichier ISO en tant que dispositif virtuel](#).

Installer un dispositif NSX Edge sur un système nu

Vous pouvez installer des dispositifs NSX Edge manuellement sur un système nu à l'aide d'un fichier ISO. Cela comprend la configuration des paramètres du réseau, tels que l'adresse IP, la passerelle, le masque de réseau, NTP et DNS.

Conditions préalables

- Vérifiez que le mode BIOS système est défini sur BIOS hérité.
- Consultez les conditions de réseau de NSX Edge dans [Configuration réseau de NSX Edge](#).

Procédure

- 1 Créez un disque amorçable sur lequel réside le fichier ISO NSX Edge.
- 2 Démarrez la machine physique à partir du disque.

3 Choisissez **Installation automatique**.

Lorsque vous appuyez sur Entrée, la procédure peut se figer pendant 10 secondes.

Au cours de la mise sous tension, le programme d'installation demande une configuration réseau par le biais de DHCP. Si DHCP n'est pas disponible dans votre environnement, le programme d'installation vous invite à fournir les paramètres IP.

Par défaut, le mot de passe de connexion est **vmware** pour l'utilisateur racine et **default** pour l'administrateur.

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

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

5 Après le démarrage de NSX Edge, connectez-vous avec des privilèges d'administrateur à l'interface de ligne de commande. Le nom d'utilisateur est **admin** et le mot de passe est **default**.

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

6 Après le redémarrage, vous pouvez vous connecter avec les informations d'identification de l'administrateur ou de l'utilisateur racine. Le mot de passe par défaut de l'utilisateur racine est **vmware**.

7 Exécutez la commande `get interface eth0` pour vérifier que l'adresse IP a été appliquée comme il convient

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

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

Si nécessaire, exécutez la commande `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` pour mettre à jour l'interface de gestion. Vous pouvez éventuellement démarrer le service SSH à l'aide de la commande `start service ssh`.

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

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

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

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

9 Résolvez les problèmes de connectivité.

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

Par défaut, le chemin de données du dispositif NSX Edge réclame toutes les cartes réseau des machines virtuelles à l'exception de la carte réseau de gestion (celle qui possède une adresse IP et un itinéraire par défaut). Si DHCP attribue la mauvaise carte réseau comme solution de gestion, effectuez les tâches pour corriger le problème.

- Connectez-vous à l'interface de ligne de commande et tapez la commande **stop service dataplane**.
- Tapez la commande **set interface eth0 dhcp plane mgmt**.
- Placez eth0 dans le réseau DHCP et attendez qu'une adresse IP soit attribuée à eth0.
- Tapez la commande **start service dataplane**.

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

Étape suivante

Reliez le dispositif NSX Edge au plan de gestion. Reportez-vous à la section [Relier NSX Edge au plan de gestion](#).

Installer NSX Edge par le biais d'un fichier ISO en tant que dispositif virtuel

Vous pouvez installer des machines virtuelles NSX Edge manuellement à l'aide d'un fichier ISO.

Important Les installations de machine virtuelle de composant NSX-T Data Center incluent VMware Tools. La suppression ou la mise à niveau de VMware Tools n'est pas prise en charge sur les dispositifs NSX-T Data Center.

Conditions préalables

- Consultez les conditions de réseau de NSX Edge dans [Configuration réseau de NSX Edge](#).

Procédure

- 1 Sur un hôte autonome ou dans le client Web vCenter, créez une machine virtuelle et allouez les ressources suivantes :
 - Système d'exploitation invité : Autre (64 bits).

- 3 cartes réseau VMXNET3. NSX Edge ne prend pas en charge le pilote de carte réseau e1000.
- Ressources système appropriées requises pour votre déploiement NSX-T Data Center.

2 Liez le fichier ISO de NSX Edge à la machine virtuelle.

Assurez-vous que l'état du lecteur de CD/DVD est défini sur **Connecter à la mise sous tension**.

edge-from-iso - Einstellungen bearbeiten

Matériel virtuel Options VM Règles SDRS Options vApp

CPU	1	
Mémoire	2048	Mo
Festplatte 1	16	GB
SCSI-Controller 0	Paravirtuel VMware	
Netzwerkadapter 1	VM Network	<input checked="" type="checkbox"/> Connecté
CD-/DVD-Laufwerk 1	Fichier ISO de la bibliothèque de conte	<input type="checkbox"/> Connecté
Statut	<input checked="" type="checkbox"/> Connecter lors de la mise sous tension	
Support CD/DVD	[datastore (2)]/nsx-edge-2.3	Parcourir...
Mode Périphérique	Émuler CD-ROM	
Noeud de périphérique virtuel	SATA-Controller 0	SATA(0:0)
Diskettenlaufwerk 1	Périphérique client	<input type="checkbox"/> Connecté
Grafikkarte	Spécifier les paramètres personnalisé	
SATA-Controller 0		
VMCI-Gerät		
Autres périphériques		

3 Durant l'amorçage ISO, ouvrez la console de la machine virtuelle et choisissez **Installation automatique**.

Lorsque vous appuyez sur Entrée, la procédure peut se figer pendant 10 secondes.

Au cours de la mise sous tension, la machine virtuelle demande une configuration réseau par le biais de DHCP. Si DHCP n'est pas disponible dans votre environnement, le programme d'installation vous invite à fournir les paramètres IP.

Par défaut, le mot de passe de connexion est **vmware** pour l'utilisateur racine et **default** pour l'administrateur.

Lorsque vous vous connectez pour la première fois, vous êtes invité à modifier le mot de passe. Pour modifier ce mot de passe, vous devez obéir à des règles de complexité strictes, notamment les suivantes :

- Au moins huit caractères
- Au moins une lettre minuscule
- Au moins une lettre majuscule
- Au moins un chiffre
- Au moins un caractère spécial
- Au moins cinq caractères différents
- Aucun mot issu du dictionnaire
- Aucun palindrome

Important Sur le dispositif, les services de base ne démarrent pas tant qu'un mot de passe suffisamment complexe n'a pas été défini.

- 4 (Facultatif) Pour des performances optimales, réservez de la mémoire pour le composant NSX-T Data Center.

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 sur un niveau qui garantit que le composant NSX-T Data Center dispose de suffisamment de mémoire pour s'exécuter efficacement. Reportez-vous à la section [Configuration système requise](#).

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

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

- 6 Après le démarrage de NSX Edge, connectez-vous avec des privilèges d'administrateur à l'interface de ligne de commande. Le nom d'utilisateur est **admin** et le mot de passe est **default**.

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

- 7 Après le redémarrage, vous pouvez vous connecter avec les informations d'identification de l'administrateur ou de l'utilisateur racine. Le mot de passe par défaut de l'utilisateur racine est **vmware**.
- 8 Exécutez la commande `get interface eth0` pour vérifier que l'adresse IP a été appliquée comme il convient

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

Interface: eth0
Address: 192.168.110.37/24
MAC address: 00:50:56:86:62:4d
```

```
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

Si nécessaire, exécutez la commande `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` pour mettre à jour l'interface de gestion. Vous pouvez éventuellement démarrer le service SSH à l'aide de la commande `start service ssh`.

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

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

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

10 Résolvez les problèmes de connectivité.

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

Par défaut, le chemin de données du dispositif NSX Edge réclame toutes les cartes réseau des machines virtuelles à l'exception de la carte réseau de gestion (celle qui possède une adresse IP et un itinéraire par défaut). Si DHCP attribue la mauvaise carte réseau comme solution de gestion, effectuez les tâches pour corriger le problème.

- a Connectez-vous à l'interface de ligne de commande et tapez la commande **stop service dataplane**.
- b Tapez la commande **set interface eth0 dhcp plane mgmt**.
- c Placez eth0 dans le réseau DHCP et attendez qu'une adresse IP soit attribuée à eth0.
- d Tapez la commande **start service dataplane**.

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

Étape suivante

Reliez le dispositif NSX Edge au plan de gestion. Reportez-vous à la section [Relier NSX Edge au plan de gestion](#).

Accéder à l'installation de NSX Edge et la vérifier

Vous pouvez vous connecter à la machine virtuelle NSX-T Data Center ou à l'hôte bare-metal NSX-T Data Center, vérifiez que l'installation a réussi et résolvez les problèmes le cas échéant.

Conditions préalables

- Vérifiez que votre serveur PXE est configuré pour l'installation. Reportez-vous à la section [Préparer le serveur PXE pour une installation de NSX Edge](#).
- Vérifiez que NSX Edge est installé à l'aide du système bare-metal ou du fichier ISO. Reportez-vous à la section [Installer un dispositif NSX Edge sur un système nu](#) ou [Installer NSX Edge par le biais d'un fichier ISO en tant que dispositif virtuel](#).

Procédure

- 1 Mettez sous tension la machine virtuelle NSX-T Data Center ou l'hôte NSX-T Data Center bare-metal.
- 2 Dans le menu de démarrage, sélectionnez **nsxedge**.

Le réseau est configuré, les partitions sont créées et les composants NSX Edge sont installés.

Lorsque l'invite de connexion de NSX Edge s'affiche, vous pouvez vous connecter en tant qu'utilisateur Admin ou racine.

Par défaut, le mot de passe de connexion est **vmware** pour l'utilisateur racine et **default** pour l'administrateur.

- 3 (Facultatif) Pour des performances optimales, réservez de la mémoire pour le composant NSX-T Data Center.

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 sur un niveau qui garantit que le composant NSX-T Data Center dispose de suffisamment de mémoire pour s'exécuter efficacement. Reportez-vous à la section [Configuration système requise](#).

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

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

- 5 Après le démarrage de NSX Edge, connectez-vous avec des privilèges d'administrateur à l'interface de ligne de commande. Le nom d'utilisateur est **admin** et le mot de passe est **default**.

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

- 6 Après le redémarrage, vous pouvez vous connecter avec les informations d'identification de l'administrateur ou de l'utilisateur racine. Le mot de passe par défaut de l'utilisateur racine est **vmware**.

- 7 Exécutez la commande `get interface eth0` pour vérifier que l'adresse IP a été appliquée comme il convient

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

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

Si nécessaire, exécutez la commande `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` pour mettre à jour l'interface de gestion. Vous pouvez éventuellement démarrer le service SSH à l'aide de la commande `start service ssh`.

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

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

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

- 9 Résolvez les problèmes de connectivité.

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

Par défaut, le chemin de données du dispositif NSX Edge réclame toutes les cartes réseau des machines virtuelles à l'exception de la carte réseau de gestion (celle qui possède une adresse IP et un itinéraire par défaut). Si DHCP attribue la mauvaise carte réseau comme solution de gestion, effectuez les tâches pour corriger le problème.

- a Connectez-vous à l'interface de ligne de commande et tapez la commande **stop service dataplane**.
- b Tapez la commande **set interface eth0 dhcp plane mgmt**.
- c Placez eth0 dans le réseau DHCP et attendez qu'une adresse IP soit attribuée à eth0.
- d Tapez la commande **start service dataplane**.

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

Étape suivante

Reliez le dispositif NSX Edge au plan de gestion. Reportez-vous à la section [Relier NSX Edge au plan de gestion](#).

Relier NSX Edge au plan de gestion

Relier les dispositifs NSX Edge au plan de gestion garantit que les dispositifs NSX Manager et NSX Edge peuvent communiquer les uns avec les autres.

Conditions préalables

Vérifiez que vous disposez des privilèges d'administrateur pour vous connecter aux dispositifs NSX Edge et au dispositif NSX Manager.

Procédure

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

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

Par exemple :

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

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

Fournissez les informations suivantes :

- Nom d'hôte ou adresse IP du dispositif NSX Manager avec numéro de port facultatif
- Nom du dispositif NSX Manager
- Empreinte numérique de certificat du dispositif NSX Manager
- Mot de passe du dispositif NSX Manager

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

Répétez cette commande sur chaque nœud NSX Edge.

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

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

Dans l'interface utilisateur de NSX Manager, le dispositif NSX Edge s'affiche sur la page **Infrastructure > Nœuds > Dispositifs Edge**. La connectivité de NSX Manager doit être activée. Si la connectivité de NSX Manager n'est pas activée, essayez d'actualiser la fenêtre du navigateur.

Étape suivante

Ajoutez le dispositif NSX Edge en tant que nœud de transfert. Reportez-vous à la section [Créer un nœud de transport NSX Edge](#).

Préparation de l'hôte

Une fois prêts à fonctionner avec NSX-T Data Center, les hôtes d'hyperviseurs sont alors appelés « nœuds d'infrastructure ». Des modules NSX-T Data Center sont installés sur ces hôtes ou nœuds d'infrastructure et ces derniers sont enregistrés dans le plan de gestion de NSX-T Data Center.

Ce chapitre contient les rubriques suivantes :

- [Installer les modules tiers sur un hôte KVM ou un serveur bare metal](#)
- [Vérifier la version Open vSwitch sur les hôtes RHEL KVM](#)
- [Ajouter un hôte d'hyperviseur ou un serveur bare metal à l'infrastructure NSX-T Data Center](#)
- [Installation manuelle de modules de noyau NSX-T Data Center](#)
- [Relier les hôtes d'hyperviseur au plan de gestion](#)

Installer les modules tiers sur un hôte KVM ou un serveur bare metal

Pour préparer un hôte KVM ou un serveur bare metal à devenir un nœud d'infrastructure, vous devez installer des modules tiers.

Conditions préalables

- (Red Hat et CentOS) Avant d'installer les modules tiers, installez les modules de virtualisation. Sur l'hôte, exécutez les commandes suivantes :

```
yum groupinstall "Virtualization Hypervisor"  
yum groupinstall "Virtualization Client"  
yum groupinstall "Virtualization Platform"  
yum groupinstall "Virtualization Tools"
```

Si vous n'êtes pas en mesure d'installer les modules, vous pouvez les installer manuellement avec la commande `yum install glibc.i686 nspr` sur une nouvelle installation.

- (Ubuntu) Avant d'installer les modules tiers, installez les modules de virtualisation. Sur l'hôte Ubuntu, exécutez les commandes suivantes :

```
apt-get install qemu-kvm
apt-get install libvirt-bin
apt-get install virtinst
apt-get install virt-manager
apt-get install virt-viewer
apt-get install ubuntu-vm-builder
apt-get install bridge-utils
```

- (Serveur bare metal) Il n'existe aucune condition préalable de virtualisation pour l'installation de modules tiers.

Procédure

- Sous Ubuntu 16.04.2 LTS, assurez-vous que les modules tiers suivants sont installés sur l'hôte.

```
libunwind8
libgflags2v5
libgoogle-perftools4
traceroute
python-mako
python-simplejson
python-unittest2
python-yaml
python-netaddr
libprotobuf9v5
libboost-chrono1.58.0
libgoogle-glog0v5
dkms
libboost-date-time1.58.0
libleveldb1v5
libsnapylv5
python-gevent
python-protobuf
ieee-data
libyaml-0-2
python-linecache2
python-traceback2
libtcmalloc-minimal4
python-greenlet
python-markupsafe
libboost-program-options1.58.0
```

Si les modules de dépendance ne sont pas installés sur Ubuntu 16.04.2 LTS, exécutez `apt-get install <package>` pour installer manuellement les modules.

- Vérifiez que les hôtes Red Hat et CentOS sont inscrits et que les référentiels respectifs sont accessibles.

Note Si vous préparez l'hôte en utilisant l'interface utilisateur NSX-T Data Center, vous devez installer les dépendances suivantes sur l'hôte.

Installez des modules tiers sur RHEL 7.4 et CentOS 7.4.

```
yum-utils
wget
redhat-lsb-core
tcpdump
boost-filesystem
PyYAML
boost-iostreams
boost-chrono
python-mako
python-netaddr
python-six
gperftools-libs
libunwind
snappy
boost-date-time
c-ares
libev
python-gevent
python-greenlet
```

Installez des modules tiers sur RHEL 7.5.

```
PyYAML
c-ares
libev
libunwind
libyaml
python-beaker
python-gevent
python-greenlet
python-mako
python-markupsafe
python-netaddr
python-paste
python-tempita
```

- Si vous préparez manuellement l'hôte qui est déjà enregistré sur RHEL ou CentOS, vous n'avez pas besoin d'installer les dépendances sur celui-ci. Si l'hôte n'est pas enregistré, installez manuellement les dépendances répertoriées en utilisant `yum install <package>`.

- Installez les modules tiers sur un serveur bare metal.
 - a Selon votre environnement, installez les modules Ubuntu, RHEL ou CentOS tiers répertoriés dans cette rubrique.
 - b Installez des modules tiers spécifiques du serveur bare metal.
 - Ubuntu - `apt-get install libvirt-libs`
 - RHEL ou CentOS - `yum install libvirt-libs`

Vérifier la version Open vSwitch sur les hôtes RHEL KVM

Si des modules OVS existent sur l'hôte, vous devez supprimer les modules existants et installer les modules pris en charge.

La version prise en charge d'Open vSwitch est la version 2.9.1.8614397-1.

Procédure

- 1 Vérifiez la version actuelle de l'Open vSwitch installé sur l'hôte.

```
ovs-vswitchd --version
```

Si vous disposez d'une version ultérieure ou antérieure d'Open vSwitch, vous devez remplacer cette version Open vSwitch par celle prise en charge.

- a Supprimez les modules Open vSwitch suivants.
 - `kmod-openvswitch`
 - `openvswitch`
 - `openvswitch-selinux-policy`
 - b Installez NSX-T Data Center à partir de NSX Manager ou suivez la procédure d'installation manuelle.
- 2 Vous pouvez également mettre à niveau les modules Open vSwitch requis par NSX-T Data Center.
 - a Connectez-vous à l'hôte en tant qu'administrateur.
 - b Téléchargez le fichier `nsx-lcp`, puis copiez-le dans le répertoire `/tmp`.
 - c Décompressez le module.


```
tar -zxvf nsx-lcp-<release>-rhel74_x86_64.tar.gz
```

- d Naviguez jusqu'au répertoire du module.

```
cd nsx-lcp-rhel74_x86_64/
```

- e Remplacez la version existante d'Open vSwitch par celle prise en charge.

- Pour une version ultérieure d'Open vSwitch, utilisez la commande `--nodeps`.

Par exemple, `rpm -Uvh kmod-openvswitch-<new version>.e17.x86_64.rpm --nodeps`

```
rpm -Uvh openvswitch-*.rpm --nodeps
```

- Pour une version antérieure d'Open vSwitch, utilisez la commande `--force`.

Par exemple, `rpm -Uvh kmod-openvswitch-<new version>.e17.x86_64.rpm --nodeps --force`

```
rpm -Uvh openvswitch-*.rpm --nodeps --force
```

Étape suivante

Ajouter un hôte d'hyperviseur à l'infrastructure NSX-T Data Center. Reportez-vous à la section [Ajouter un hôte d'hyperviseur ou un serveur bare metal à l'infrastructure NSX-T Data Center](#).

Ajouter un hôte d'hyperviseur ou un serveur bare metal à l'infrastructure NSX-T Data Center

Un nœud d'infrastructure est un nœud qui a été enregistré avec le plan de gestion NSX-T Data Center et sur lequel des modules NSX-T Data Center sont installés. Pour pouvoir faire partie de la superposition NSX-T Data Center, un hôte d'hyperviseur ou un serveur bare metal doit d'abord être ajouté à l'infrastructure NSX-T Data Center.

Vous pouvez ignorer cette procédure si vous avez installé les modules sur les hôtes manuellement et relié les hôtes au plan de gestion à l'aide de l'interface de ligne de commande.

Note Pour un hôte KVM sous RHEL, vous pouvez utiliser les informations d'identification **sudo** pour effectuer des activités de préparation de l'hôte.

Conditions préalables

- Pour chaque hôte à ajouter à l'infrastructure NSX-T Data Center, il convient d'abord de rassembler les informations suivantes :
 - Nom d'hôte
 - Adresse IP de gestion
 - Nom d'utilisateur
 - Mot de passe
 - (Facultatif) (KVM) Empreinte numérique SHA-256 SSL
 - (Facultatif) (ESXi) Empreinte numérique SHA-256 SSL

- Pour Ubuntu, vérifiez que les modules tiers requis sont installés. Reportez-vous à la section [Installer les modules tiers sur un hôte KVM ou un serveur bare metal](#).

Procédure

- 1 (Facultatif) Récupérez l'empreinte numérique de l'hyperviseur de manière à pouvoir la fournir lors de l'ajout de l'hôte à l'infrastructure.

- a Rassemblez les informations d'empreinte numérique de l'hyperviseur.

Utilisez un shell Linux.

```
# echo -n | openssl s_client -connect <esxi-ip-address>:443 2>/dev/null | openssl x509 -noout -fingerprint -sha256
```

Utilisez l'interface de ligne de commande vSphere ESXi de l'hôte.

```
[root@host:~] openssl x509 -in /etc/vmware/ssl/rui.crt -fingerprint -sha256 -noout
SHA256 Fingerprint=49:73:F9:A6:0B:EA:51:2A:15:57:90:DE:C0:89:CA:7F:46:8E:30:15:CA:4D:5C:
95:28:0A:9E:A2:4E:3C:C4:F4
```

- b Récupérez l'empreinte numérique SHA-256 d'un hyperviseur KVM ; pour cela, exécutez la commande dans l'hôte KVM.

```
# awk '{print $2}' /etc/ssh/ssh_host_rsa_key.pub | base64 -d | sha256sum -b | sed 's/ .*$//' | xxd -r -p | base64
```

- 2 Dans l'interface de ligne de commande de NSX Manager, vérifiez que le service d'installation-mise à niveau est en cours d'exécution.

```
nsx-manager-1> get service install-upgrade
```

```
Service name: install-upgrade
Service state: running
Enabled: True
```

- 3 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 4 Sélectionnez **Infrastructure > Nœuds > Hôtes** et cliquez sur **Ajouter**.
- 5 Entrez le nom d'hôte, l'adresse IP, le nom d'utilisateur, le mot de passe et l'empreinte numérique facultative.

Par exemple :

Ajouter un hôte



Nom*	comp-02b
Adresses IP*	<div>192.168.210.54 x</div>
Système d'exploitation*	ESXi ▼
Nom d'utilisateur*	root
Mot de passe*	●●●●●●●●
Empreinte numérique SHA-256	

[ANNULER](#)[AJOUTER](#)

Pour le serveur bare metal, vous pouvez sélectionner le **Serveur RHEL**, le **Serveur Ubuntu** ou le **Serveur CentOS** dans le menu déroulant Système d'exploitation.

Si vous n'entrez pas l'empreinte numérique de l'hôte, l'interface utilisateur de NSX-T Data Center vous invite à utiliser l'empreinte par défaut récupérée à partir de l'hôte en texte brut.

Par exemple :

Empreinte numérique non valide



L'empreinte numérique saisie n'était pas valide.

Voulez-vous utiliser cette empreinte numérique fournie par le serveur ?

fa984ff00d4856c1e8db1be005ff908a3f2335bcd67776447e926aba71a006b8

NON

AJOUTER

Lorsqu'un hôte a été ajouté à l'infrastructure NSX-T Data Center, la page de NSX Manager **Hôtes** affiche **État du déploiement : Installation terminée** et **Connectivité MPA : Active**.

Connectivité LCP demeure non disponible tant que vous n'avez pas transformé le nœud d'infrastructure en nœud de transport.

- 6 Vérifiez que les modules de NSX-T Data Center sont installés sur votre hôte ou votre serveur bare metal.

Suite à l'ajout d'un hôte ou d'un serveur bare metal à l'infrastructure de NSX-T Data Center, une collection de modules NSX-T Data Center est installée sur l'hôte ou sur le serveur bare metal.

Sur vSphere ESXi, les modules sont regroupés sous forme de fichiers VIB. Pour KVM ou le serveur bare metal sur RHEL, ils sont regroupés sous forme de fichiers RPM. Pour KVM ou le serveur bare metal sur Ubuntu, ils sont regroupés sous forme de fichiers DEB.

- Sur ESXi, tapez la commande `esxcli software vib list | grep nsx`.

La date est le jour où vous avez effectué l'installation.

- Sur RHEL, tapez la commande `yum list installed` ou `rpm -qa`.

- Sur Ubuntu, tapez la commande `dpkg --get-selections`.

- 7 (Facultatif) Affichez les nœuds d'infrastructure à l'aide de l'appel d'API GET `https://<nsx-mgr>/api/v1/fabric/nodes/<node-id>`.

- 8 (Facultatif) Surveillez l'état dans l'API à l'aide de l'appel d'API GET `https://<nsx-mgr>/api/v1/fabric/nodes/<node-id>/status`.

- 9 (Facultatif) Modifiez les intervalles d'interrogation de certains processus, si vous disposez de 500 hyperviseurs ou plus.

NSX Manager peut rencontrer des problèmes de performances et d'utilisation élevée de CPU s'il y a plus de 500 hyperviseurs.

- a Utilisez la commande CLI NSX-T Data Center `copy file` ou l'API `POST /api/v1/node/file-store/<file-name>?action=copy_to_remote_file` pour copier le script `aggsvc_change_intervals.py` sur un hôte.
- b Exécutez le script, qui se trouve dans le magasin de fichiers NSX-T Data Center.

```
python aggsvc_change_intervals.py -m '<NSX Manager IP address>' -u 'admin' -p '<password>' -i 900
```

- c (Facultatif) Rétablissez les valeurs par défaut des intervalles d'interrogation.

```
python aggsvc_change_intervals.py -m '<NSX Manager IP address>' -u 'admin' -p '<password>' -r
```

Étape suivante

Créez une zone de transport. Reportez-vous à la section [À propos des zones de transport](#).

Installation manuelle de modules de noyau NSX-T Data Center

Comme alternative à l'utilisation de l'interface utilisateur de NSX-T Data Center **Infrastructure > Nœuds > Hôtes > Ajouter** ou de l'API `POST /api/v1/fabric/nodes`, vous pouvez installer les modules du noyau NSX-T Data Center manuellement à partir de la ligne de commande de l'hyperviseur.

Note Vous ne pouvez pas installer manuellement des modules de noyau NSX-T Data Center sur un serveur Bare Metal.

Installer manuellement les modules de noyau NSX-T Data Center sur les hyperviseurs ESXi

Pour préparer l'intégration des hôtes dans NSX-T Data Center, vous devez installer les modules du noyau NSX-T Data Center sur les hôtes ESXi. Cela permet de créer l'infrastructure du plan de contrôle et du plan de gestion de NSX-T Data Center. Les modules du noyau NSX-T Data Center conditionnés dans des fichiers VIB s'exécutent dans le noyau de l'hyperviseur et fournissent des services tels que le routage distribué, Distributed Firewall et les possibilités de pontage.

Vous pouvez télécharger les VIB NSX-T Data Center manuellement et les intégrer à l'image hôte. Les chemins de téléchargement peuvent être modifiés pour chaque version de NSX-T Data Center. Consultez toujours la page des téléchargements NSX-T Data Center pour obtenir les VIB appropriés.

Procédure

- 1 Connectez-vous à l'hôte en tant qu'utilisateur racine ou utilisateur disposant des privilèges d'administrateur.
- 2 Accédez au répertoire /tmp.

```
[root@host:~]: cd /tmp
```

- 3 Téléchargez le fichier nsx-lcp, puis copiez-le dans le répertoire /tmp.
- 4 Exécutez la commande d'installation.

```
[root@host:/tmp]: esxcli software vib install -d /tmp/nsx-lcp-<release>.zip
Installation Result
  Message: Operation finished successfully.
  Reboot Required: false
  VIBs Installed: VMware_bootbank_nsx-aggsservice_<release>, VMware_bootbank_nsx-da_<release>,
VMware_bootbank_nsx-esx-datapath_<release>, VMware_bootbank_nsx-exporter_<release>,
VMware_bootbank_nsx-host_<release>, VMware_bootbank_nsx-lldp_<release>, VMware_bootbank_nsx-
mpa_<release>, VMware_bootbank_nsx-netcpa_<release>, VMware_bootbank_nsx-python-
protobuf_<release>, VMware_bootbank_nsx-sfhc_<release>, VMware_bootbank_nsxa_<release>,
VMware_bootbank_nsxcli_<release>
  VIBs Removed:
  VIBs Skipped:
```

Selon ce qui a déjà été installé sur l'hôte, certains fichiers VIB peuvent être supprimés et certains peuvent être ignorés. Il n'est pas nécessaire d'effectuer un redémarrage sauf si la sortie de commande indique Reboot Required: true.

L'ajout d'un hôte ESXi à la infrastructure NSX-T Data Center a pour effet d'installer les VIB suivants sur l'hôte.

- nsx-aggsservice : fournit des bibliothèques côté hôte pour le service d'agrégation de NSX-T Data Center. Le service d'agrégation de NSX-T Data Center est un service qui s'exécute dans les nœuds du plan de gestion et extrait l'état d'exécution des composants NSX-T Data Center.
- nsx-da : collecte les données de l'agent de découverte (DA) sur la version du système d'exploitation de l'hyperviseur, les machines virtuelles et les interfaces réseau. Fournit au plan de gestion les données à utiliser dans les outils de dépannage.
- nsx-esx-datapath : fournit la fonctionnalité de traitement du plan de données NSX-T Data Center.
- nsx-exporter : fournit des agents d'hôte qui rapportent l'état d'exécution au service d'agrégation qui s'exécute dans le plan de gestion.
- nsx-host : fournit les métadonnées du bundle VIB installé sur l'hôte.
- nsx-lldp : fournit la prise en charge du protocole LLDP (Link Layer Discovery Protocol), qui est un protocole de couche de liaison utilisé par les périphériques réseau pour indiquer leur identité, leurs fonctionnalités et l'identité de leurs voisins sur un réseau local.

- `nsx-mpa` : fournit des communications entre NSX Manager et les hôtes d'hyperviseur.
- `nsx-netcpa` : fournit des communication entre le plan de contrôle central et les hyperviseurs. Reçoit l'état de réseau logique du plan de contrôle central et programme cet état dans le plan de données.
- `nsx-python-protobuf` : fournit des liaisons Python pour les zones tampons de protocole.
- `nsx-sfhc` : composant hôte de l'infrastructure de services (SFHC). Fournit un agent hôte pour gérer le cycle de vie de l'hyperviseur en tant qu'hôte d'infrastructure dans l'inventaire du plan de gestion. Cela fournit un canal pour les opérations telles que la mise à niveau et la désinstallation de NSX-T Data Center ainsi que la surveillance des modules NSX-T Data Center sur les hyperviseurs.
- `nsxa` : effectue des configurations de niveau hôte, telles que la création de N-VDS et la configuration de liaisons montantes.
- `nsxcli` : fournit l'interface de ligne de commande NSX-T Data Center sur les hôtes d'hyperviseur.
- `nsx-support-bundle-client` : permet de collecter des bundles de prise en charge.

Pour le vérifier, vous pouvez exécuter la commande **`esxcli software vib list | grep nsx`** ou la commande **`esxcli software vib list | grep <aaaa-mm-jj>`** sur l'hôte ESXi, dans laquelle la date correspond à la date d'installation.

Étape suivante

Ajoutez l'hôte au plan de gestion NSX-T Data Center. Reportez-vous à la section [Relier les hôtes d'hyperviseur au plan de gestion](#).

Installer manuellement les modules de noyau NSX-T Data Center sur des hyperviseurs Ubuntu KVM

Pour préparer l'intégration des hôtes dans NSX-T Data Center, vous pouvez installer manuellement les modules du noyau NSX-T Data Center sur les hôtes Ubuntu KVM. Cela permet de créer l'infrastructure du plan de contrôle et du plan de gestion de NSX-T Data Center. Les modules du noyau NSX-T Data Center conditionnés dans des fichiers DEB s'exécutent dans le noyau de l'hyperviseur et fournissent des services tels que le routage distribué, Distributed Firewall et les possibilités de pontage.

Vous pouvez télécharger les DEB NSX-T Data Center manuellement et les intégrer à l'image hôte. Sachez que les chemins de téléchargement peuvent être modifiés pour chaque version de NSX-T Data Center. Consultez toujours la page des téléchargements NSX-T Data Center pour obtenir les DEB appropriés.

Conditions préalables

- Vérifiez que les modules tiers requis sont installés. Reportez-vous à la section [Installer les modules tiers sur un hôte KVM ou un serveur bare metal](#).

Procédure

- 1 Connectez-vous à l'hôte en tant qu'utilisateur disposant des privilèges d'administrateur.

- 2 (Facultatif) Accédez au répertoire /tmp.

```
cd /tmp
```

- 3 Téléchargez le fichier nsx-lcp, puis copiez-le dans le répertoire /tmp.

- 4 Décompressez le module.

```
tar -xvf nsx-lcp-<release>-ubuntu-trusty-amd64.tar.gz
```

- 5 Naviguez jusqu'au répertoire du module.

```
cd nsx-lcp-trusty-amd64/
```

- 6 Installez les modules.

```
sudo dpkg -i *.deb
```

- 7 Rechargez le module de noyau OVS.

```
/etc/init.d/openvswitch-switch force-reload-kmod
```

Si l'hyperviseur utilise DHCP sur les interfaces OVS, redémarrez l'interface réseau sur laquelle DHCP est configuré. Vous pouvez arrêter manuellement l'ancien processus dhclient sur l'interface réseau et redémarrer un nouveau processus dhclient sur cette interface.

- 8 Pour effectuer une vérification, vous pouvez exécuter la commande `dpkg -l | grep nsx`.

```
user@host:~$ dpkg -l | grep nsx
```

ii	nsx-agent	<release>	amd64	NSX Agent
ii	nsx-aggservice	<release>	all	NSX Aggregation Service Lib
ii	nsx-cli	<release>	all	NSX CLI
ii	nsx-da	<release>	amd64	NSX Inventory Discovery Agent
ii	nsx-host	<release>	all	NSX host meta package
ii	nsx-host-node-status-reporter	<release>	amd64	NSX Host Status Reporter for
	Aggregation Service			
ii	nsx-lldp	<release>	amd64	NSX LLDP Daemon
ii	nsx-logical-exporter	<release>	amd64	NSX Logical Exporter
ii	nsx-mpa	<release>	amd64	NSX Management Plane Agent Core
ii	nsx-netcpa	<release>	amd64	NSX Netcpa
ii	nsx-sfhc	<release>	amd64	NSX Service Fabric Host
	Component			
ii	nsx-transport-node-status-reporter	<release>	amd64	NSX Transport Node Status
	Reporter			
ii	nsxa	<release>	amd64	NSX L2 Agent

Les erreurs sont généralement dues à des dépendances incomplètes. La commande `apt-get install -f` peut tenter de résoudre les dépendances et de réexécuter l'installation de NSX-T Data Center.

Étape suivante

Ajoutez l'hôte au plan de gestion NSX-T Data Center. Reportez-vous à la section [Relier les hôtes d'hyperviseur au plan de gestion](#).

Installer manuellement des modules de noyau NSX-T Data Center sur des hyperviseurs KVM RHEL et CentOS

Pour préparer l'intégration des hôtes dans NSX-T Data Center, vous pouvez installer manuellement les modules du noyau NSX-T Data Center sur les hôtes KVM RHEL ou CentOS.

Cela permet de créer l'infrastructure du plan de contrôle et du plan de gestion de NSX-T Data Center. Les modules du noyau NSX-T Data Center conditionnés dans des fichiers VIB s'exécutent dans le noyau de l'hyperviseur et fournissent des services tels que le routage distribué, Distributed Firewall et les possibilités de pontage.

Vous pouvez télécharger les RPM NSX-T Data Center manuellement et les intégrer à l'image hôte. Sachez que les chemins de téléchargement peuvent être modifiés pour chaque version de NSX-T Data Center. Consultez toujours la page des téléchargements NSX-T Data Center pour obtenir les RPM appropriés.

Conditions préalables

Capacité d'accéder à un référentiel RHEL ou CentOS.

Procédure

- 1 Connectez-vous à l'hôte en tant qu'administrateur.
- 2 Téléchargez le fichier nsx-lcp, puis copiez-le dans le répertoire /tmp.
- 3 Décompressez le module.

```
tar -zxvf nsx-lcp-<release>-rhel7.4_x86_64.tar.gz
```

- 4 Naviguez jusqu'au répertoire du module.

```
cd nsx-lcp-rhel74_x86_64/
```

- 5 Installez les modules.

```
sudo yum install *.rpm
```

Lorsque vous exécutez la commande d'installation yum, toutes les dépendances NSX-T Data Center sont résolues, en partant du principe que les hôtes RHEL ou CentOS peuvent accéder à leurs référentiels respectifs.

- 6 Rechargez le module de noyau OVS.

```
/etc/init.d/openvswitch force-reload-kmod
```

Si l'hyperviseur utilise DHCP sur les interfaces OVS, redémarrez l'interface réseau sur laquelle DHCP est configuré. Vous pouvez arrêter manuellement l'ancien processus dhclient sur l'interface réseau et redémarrer un nouveau processus dhclient sur cette interface.

- 7 Pour effectuer une vérification, vous pouvez exécuter la commande `rpm -qa | egrep 'nsx|openvswitch|nicira'`.

Les modules installés dans la sortie doivent correspondre aux modules présents dans le répertoire `nsx-rhel74` ou `nsx-centos74`.

Étape suivante

Ajoutez l'hôte au plan de gestion NSX-T Data Center. Reportez-vous à la section [Relier les hôtes d'hyperviseur au plan de gestion](#).

Relier les hôtes d'hyperviseur au plan de gestion

Cette procédure garantit que NSX Manager et les hôtes peuvent communiquer les uns avec les autres.

Conditions préalables

L'installation des modules NSX-T Data Center doit être terminée.

Procédure

- 1 Ouvrez une session SSH vers le dispositif NSX Manager.
- 2 Connectez-vous avec les informations d'identification d'administrateur.
- 3 Ouvrez une session SSH vers l'hôte d'hyperviseur.
- 4 Sur le dispositif NSX Manager, exécutez la commande d'interface de ligne de commande `get certificate api thumbprint`.

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

Par exemple :

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

- 5 Sur l'hôte d'hyperviseur, exécutez la commande **nsxcli** pour ouvrir l'interface de ligne de commande NSX-T Data Center.

Note Pour KVM, exécutez la commande en tant que superutilisateur (sudo).

```
[user@host:~] nsxcli
host>
```

L'invite change.

6 Sur l'hôte d'hyperviseur, exécutez la commande **join management-plane**.

Fournissez les informations suivantes :

- Nom d'hôte ou adresse IP du dispositif NSX Manager avec numéro de port facultatif
- Nom du dispositif NSX Manager
- Empreinte numérique de certificat du dispositif NSX Manager
- Mot de passe du dispositif NSX Manager

```
host> join management-plane NSX-Manager1 username admin thumbprint <NSX-Manager1's-thumbprint>
Password for API user: <NSX-Manager1's-password>
Node successfully joined
```

Vérifiez le résultat en exécutant la commande `get managers` sur vos hôtes.

```
host> get managers
- 192.168.110.47 Connected
```

Dans l'interface utilisateur de NSX Manager, dans **Infrastructure > Nœud > Hôtes**, vérifiez que la connectivité de l'agent MPA de l'hôte est **Active**.

Pour visualiser également l'état de l'hôte d'infrastructure, vous pouvez exécuter l'appel d'API **GET** <https://<nsx-mgr>/api/v1/fabric/nodes/<id-noeud-infrastructure>/state> :

```
{
  "details": [],
  "state": "success"
}
```

Le plan de gestion envoie les certificats d'hôte au plan de contrôle et le plan de contrôle transfère les informations du plan de contrôle aux hôtes.

Vous devez voir les adresses NSX Controller dans `/etc/vmware/nsx/controller-info.xml` sur chaque hôte ESXi ou accéder à l'interface CLI à l'aide de `get controllers`.

```
[root@host:~] cat /etc/vmware/nsx/controller-info.xml
<?xml version="1.0" encoding="utf-8"?>
<config>
  <connectionList>
    <connection id="0">
      <server>10.143.1.47</server>
      <port>1234</port>
      <sslEnabled>true</sslEnabled>
      <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
    <connection id="1">
      <server>10.143.1.45</server>
      <port>1234</port>
      <sslEnabled>true</sslEnabled>
      <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
```

```

<connection id="2">
  <server>10.143.1.46</server>
  <port>1234</port>
  <sslEnabled>true</sslEnabled>
  <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
</connection>
</connectionList>
</config>

```

La connexion de l'hôte aux dispositifs NSX-T Data Center est établie mais elle conserve l'état « CLOSE_WAIT » jusqu'à ce que l'hôte devienne un nœud de transport. Pour le vérifier, exécutez la commande **esxcli network ip connection list | grep 1234**.

```

# esxcli network ip connection list | grep 1234
tcp          0      0 192.168.210.53:45823      192.168.110.34:1234  CLOSE_WAIT    37256  newreno
netcpa

```

Pour KVM, la commande est **netstat -anp --tcp | grep 1234**.

```

user@host:~$ netstat -anp --tcp | grep 1234
tcp  0  0 192.168.210.54:57794  192.168.110.34:1234  CLOSE_WAIT -

```

Étape suivante

Créez une zone de transport. Reportez-vous à la section [À propos des zones de transport](#).

Zones de transport et nœuds de transport

8

Les zones de transport et nœuds de transport sont des concepts importants dans NSX-T Data Center.

Ce chapitre contient les rubriques suivantes :

- [À propos des zones de transport](#)
- [Chemin de données optimisé](#)
- [Créer un pool d'adresses IP pour les adresses IP des points de terminaison de tunnel](#)
- [Créer un profil de liaison montante](#)
- [Créer des zones de transport](#)
- [Créer un nœud de transport hôte](#)
- [Créer une interface d'application pour les charges de travail de serveur Bare Metal](#)
- [Configurer des profils Network I/O Control](#)
- [Créer un nœud de transport NSX Edge](#)
- [Créer un cluster NSX Edge](#)

À propos des zones de transport

Une zone de transport est un conteneur qui définit la portée potentielle des nœuds de transport. Les nœuds de transport sont des hôtes d'hyperviseur et des dispositifs NSX Edge qui participent à une superposition NSX-T Data Center. Pour un hôte d'hyperviseur, cela signifie héberger les machines virtuelles qui communiquent sur les commutateurs logiques NSX-T Data Center. Pour un dispositif NSX Edge, cela signifie détenir toutes les liaisons montantes et descendantes du routeur logique.

Lorsque vous créez une zone de transport, vous devez spécifier un mode N-VDS, soit **Standard**, soit **Chemin de données amélioré**. Lorsque vous ajoutez un nœud de transport à une zone de transport, le N-VDS associé à la zone de transport est installé sur le nœud de transport. Chaque zone de transport prend en charge un seul N-VDS. Un chemin de données N-VDS amélioré dispose des performances nécessaires pour prendre en charge les charges de travail NFV (Network Functions Virtualization, réseau de fonctions de virtualisation), ainsi que les réseaux VLAN et de superposition, et requiert un hôte ESXi prenant en charge le N-VDS à chemin de données amélioré.

Un nœud de transport peut appartenir à :

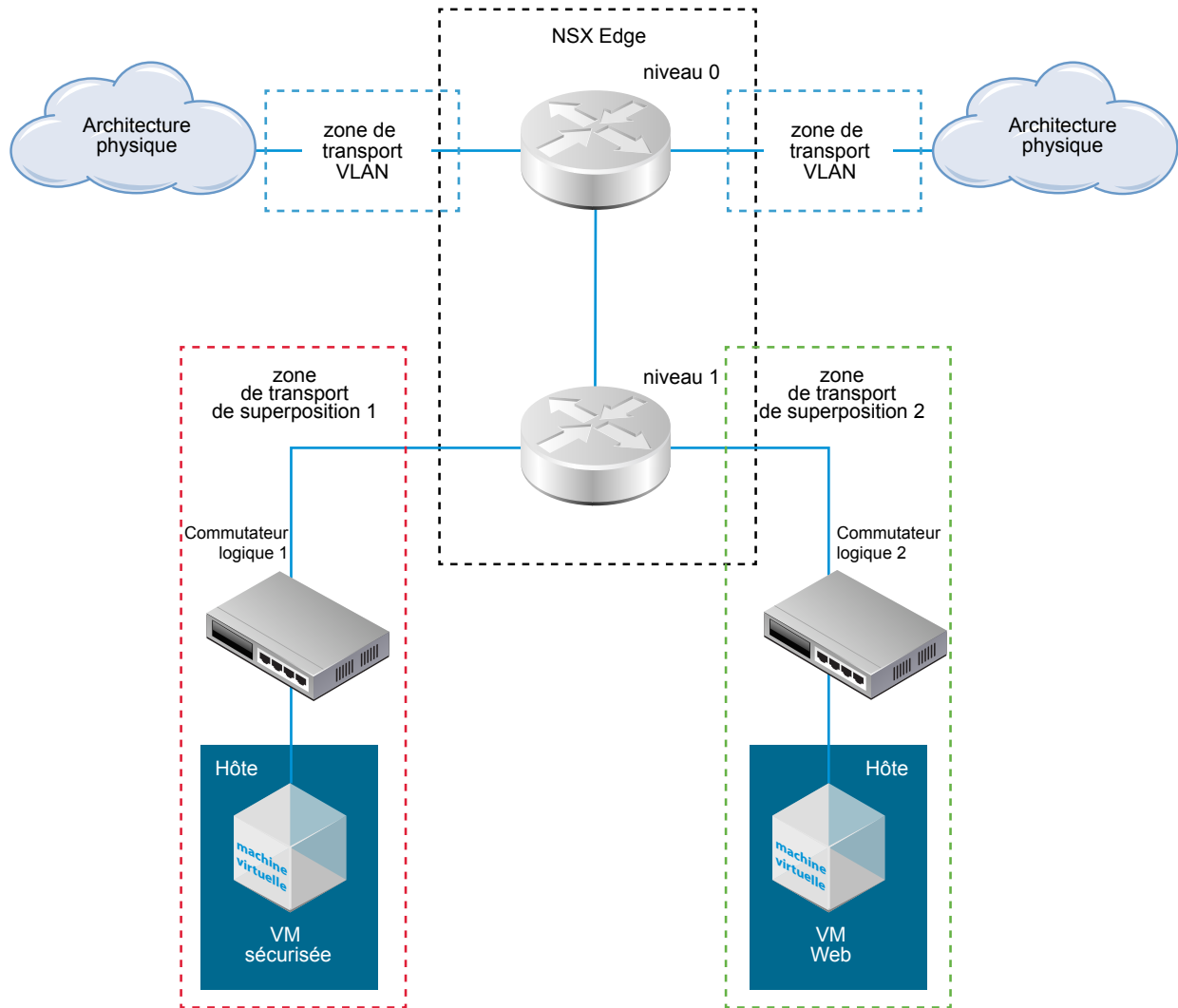
- Plusieurs zones de transport VLAN.
- Au maximum une zone de transport de superposition avec un N-VDS standard.
- Plusieurs zones de transport de superposition avec un N-VDS à chemin de données avancé si le nœud de transport est exécuté sur un hôte ESXi.

Si deux nœuds de transport se trouvent dans la même zone de transport, les machines virtuelles hébergées sur ces nœuds de transport peuvent être attachées aux commutateurs logiques NSX-T Data Center de cette zone de transport. Ce rattachement permet aux machines virtuelles de communiquer entre elles, en admettant que celles-ci soient accessibles via la couche 2/couche 3. Si les machines virtuelles sont attachées à des commutateurs qui sont dans des zones de transport différentes, elles ne peuvent pas communiquer entre elles. Les zones de transport ne remplacent pas les exigences en matière d'accessibilité de sous-couche de la couche 2/couche 3, mais elles limitent l'accessibilité. En d'autres termes, l'appartenance à une même zone de transport est une condition préalable à la connectivité. Une fois que cette condition préalable est remplie, l'accessibilité est possible, mais elle n'est pas automatique. Pour que l'accessibilité soit effective, la mise en réseau de sous-couche de la couche 2 et (pour d'autres sous-réseaux) de la couche 3 doit être opérationnelle.

Supposons qu'un nœud de transport contient à la fois des machines virtuelles classiques et des machines virtuelles hautement sécurisées. Dans votre architecture réseau, les machines virtuelles classiques doivent pouvoir communiquer entre elles sans toutefois être en mesure d'atteindre les machines virtuelles hautement sécurisées. Pour ce faire, vous pouvez placer les machines virtuelles sécurisées sur les hôtes qui appartiennent à une même zone de transport nommée *secure-tz*. Les machines virtuelles standard et sécurisées ne peuvent pas être sur le même nœud de transport. Les machines virtuelles sont alors placées sur une zone de transport différente nommée *general-tz*. Les machines virtuelles classiques sont attachées à un commutateur logique NSX-T Data Center qui se trouve également dans la zone *general-tz*. Les machines virtuelles hautement sécurisées sont attachées à un commutateur logique NSX-T Data Center qui se trouve dans la zone *secure-tz*. Les machines virtuelles qui se trouvent dans des zones de transport différentes ne peuvent pas communiquer entre elles, même si elles sont sur le même sous-réseau. Finalement, c'est la connexion machine virtuelle vers commutateur logique qui contrôle l'accessibilité des machines virtuelles. Ainsi, les deux commutateurs logiques étant dans des zones de transport distinctes, les « machines virtuelles Web » et les « machines virtuelles sécurisées » ne peuvent pas communiquer entre elles.

Par exemple, le schéma suivant présente un dispositif NSX Edge qui appartient à trois zones de transport : deux zones de transport VLAN et une zone de transport de superposition 2. La zone de transport de superposition 1 contient un hôte, un commutateur logique NSX-T Data Center et une machine virtuelle sécurisée. Le dispositif NSX Edge n'appartenant pas à la zone de transport de superposition 1, la machine virtuelle sécurisée n'a pas accès à l'architecture physique. En revanche, la machine virtuelle Web qui se trouve dans la zone de transport de superposition 2 peut communiquer avec l'architecture physique parce que le dispositif NSX Edge appartient à la zone de transport de superposition 2.

Chiffre 8-1. Zones de transport NSX-T Data Center



Chemin de données optimisé

Le mode Chemin de données optimisé est un mode de pile de mise en réseau qui, lorsqu'il est configuré, améliore les performances réseau. Il est principalement conçu pour les charges de travail NFV, car elles nécessitent les performances avantageuses fournies par ce mode.

Le commutateur N-VDS ne peut être configuré dans le mode de chemin de données optimisé que sur un hôte ESXi.

En mode de chemin de données optimisé, vous pouvez configurer les trafics suivants :

- Trafic de superposition
- Trafic VLAN

Processus détaillé de configuration du chemin de données optimisé

En tant qu'administrateur réseau, avant de créer des zones de transport prenant en charge N-VDS en mode de chemin de données optimisé, vous devez préparer le réseau avec les cartes et les pilotes réseau pris en charge. Pour améliorer les performances réseau, vous pouvez permettre à la stratégie d'association de source d'équilibrage de charge de reconnaître le nœud NUMA.

Les étapes de haut niveau sont les suivantes :

- 1 Utilisez des cartes réseau qui prennent en charge le mode de chemin de données optimisé.
Reportez-vous au [Guide de compatibilité VMware](#) pour savoir quelles cartes réseau prennent en charge le mode de chemin de données optimisé.
Sur la page Guide de compatibilité VMware, sous la catégorie de **Périphériques d'E/S**, sélectionnez **ESXi 6.7**, Type de périphérique d'E/S comme **Réseau** et Fonctionnalité comme **Chemin de données optimisé N-VDS**.
- 2 Téléchargez et installez les pilotes de carte réseau depuis la [page My VMware](#).
- 3 Créez une stratégie de liaison montante.
Reportez-vous à la section [Créer un profil de liaison montante](#).
- 4 Créez une zone de transport avec N-VDS en mode de chemin de données optimisé.
Reportez-vous à la section [Créer des zones de transport](#).
- 5 Créez un nœud de transport d'hôte. Configurez le N-VDS en mode de chemin de données optimisé avec des cœurs logiques et des nœuds NUMA.
Reportez-vous à la section [Créer un nœud de transport hôte](#).

Mode de stratégie d'association de source d'équilibrage de charge prenant en charge NUMA

Le mode de stratégie d'association d'équilibrage de charge défini pour un chemin de données optimisé N-VDS prend en charge NUMA lorsque les conditions suivantes sont réunies :

- La **Sensibilité de latence** sur les machines virtuelles est **Élevée**.
- Le type d'adaptateur réseau utilisé est VMXNET3.

Si l'emplacement de nœud NUMA de la machine virtuelle ou de la carte réseau physique n'est pas disponible, la stratégie d'association de source d'équilibrage de charge ne tient pas compte pas de la prise en charge de NUMA pour aligner des machines virtuelles et des cartes réseau.

La stratégie d'association fonctionne sans prise en charge de NUMA dans les conditions suivantes :

- La liaison montante LAG est configurée avec des liens physiques de plusieurs nœuds NUMA.
- La machine virtuelle bénéficie d'une affinité à plusieurs nœuds NUMA.

- L'hôte ESXi n'a pas pu définir les informations NUMA pour une machine virtuelle ou des liens physiques.

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

Vous pouvez utiliser un pool d'adresses IP pour les points de terminaison de tunnel. Les points de terminaison de tunnel sont les adresses IP source et de destination utilisées dans l'en-tête IP externe pour identifier de façon univoque les hôtes d'hyperviseur qui débutent et terminent l'encapsulation NSX-T Data Center des trames de superposition. Vous pouvez également utiliser DHCP ou configurer manuellement des pools d'adresses IP pour les adresses IP des points de terminaison de tunnel.

Si vous utilisez à la fois des hôtes ESXi et KVM, vous pouvez opter pour une architecture qui utilise deux sous-réseaux différents pour le pool d'adresses IP des points de terminaison de tunnel ESXi (sub_a) et le pool d'adresses IP des points de terminaison de tunnel KVM (sub_b). Dans ce cas, il est nécessaire d'ajouter sur les hôtes KVM un itinéraire statique vers sub_a avec une passerelle par défaut dédiée.

Voici un exemple de la table de routage obtenue sur un hôte Ubuntu où sub_a = 192.168.140.0 et sub_b = 192.168.150.0. (Le sous-réseau de gestion peut, par exemple, être 192.168.130.0.)

Table de routage IP du noyau :

Destination	Gateway	Genmask	Iface
0.0.0.0	192.168.130.1	0.0.0.0	eth0
192.168.122.0	0.0.0.0	255.255.255.0	virbr0
192.168.130.0	0.0.0.0	255.255.255.0	eth0
192.168.140.0	192.168.150.1	255.255.255.0	nsx-vtep0.0
192.168.150.0	0.0.0.0	255.255.255.0	nsx-vtep0.0

Il existe au moins deux façons d'ajouter la route. De ces deux méthodes, la route persiste après le redémarrage de l'hôte uniquement si vous ajoutez celle-ci en modifiant l'interface. L'ajout d'une route au moyen de la commande `route add` ne persiste pas après le redémarrage d'un hôte.

```
route add -net 192.168.140.0 netmask 255.255.255.0 gw 192.168.150.1 dev nsx-vtep0.0
```

Dans `/etc/network/interfaces` avant « `up ifconfig nsx-vtep0.0 up` », ajoutez cet itinéraire statique :

```
post-up route add -net 192.168.140.0 netmask 255.255.255.0 gw 192.168.150.1
```

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Inventaire > Groupes > Pools IP**, puis cliquez sur **Ajouter**.

3 Entrez le nom du pool d'adresses IP, une description (facultatif) et les paramètres du réseau.

Ces derniers incluent :

- Plage d'adresses IP
- Passerelle
- Adresse réseau au format CIDR
- (Facultatif) Liste des serveurs DNS séparés par une virgule
- (Facultatif) Suffixe DNS

Par exemple :

Ajouter un nouveau pool d'adresses IP



Nom *

Description

Sous-réseaux

[+ AJOUTER](#) [SUPPRIMER](#)

<input checked="" type="checkbox"/> Plages d'adresses IP *	Passerelle	CIDR *	Serveurs DNS	Suffixe DNS
<input checked="" type="checkbox"/> 192.168.250.100 - 192.168.250.200	192.168.210.1	192.168.250.0/24		

[ANNULER](#) [AJOUTER](#)

Vous pouvez également afficher les pools d'adresses IP à l'aide de l'appel d'API GET <https://<nsx-mgr>/api/v1/pools/ip-pools> :

```
{
  "cursor": "0036e2d8c2e8-f6d7-498e-821b-b7e44d2650a9ip-pool-1",
  "sort_by": "displayName",
  "sort_ascending": true,
  "result_count": 1,
  "results": [
    {
      "id": "e2d8c2e8-f6d7-498e-821b-b7e44d2650a9",
      "display_name": "comp-tep",
      "resource_type": "IpPool",
      "subnets": [
        {
          "dns_nameservers": [
            "192.168.110.10"
          ]
        }
      ]
    }
  ]
}
```

```

    ],
    "allocation_ranges": [
      {
        "start": "192.168.250.100",
        "end": "192.168.250.200"
      }
    ],
    "gateway_ip": "192.168.250.1",
    "cidr": "192.168.250.0/24",
    "dns_suffix": "corp.local"
  }
],
"_last_modified_user": "admin",
"_last_modified_time": 1443649891178,
"_create_time": 1443649891178,
"_system_owned": false,
"_create_user": "admin",
"_revision": 0
}
]
}

```

Étape suivante

Créez un profil de liaison montante. Reportez-vous à la section [Créer un profil de liaison montante](#).

Créer un profil de liaison montante

Un profil de liaison montante définit des stratégies pour les liens des hôtes d'hyperviseur vers les commutateurs logiques NSX-T Data Center ou des nœuds NSX Edge vers les commutateurs ToR (Top-of-Rack).

Les paramètres définis par les profils de liaison montante peuvent inclure des règles d'association, des liens actifs/en veille, l'ID du VLAN de transport et le paramètre MTU.

Les profils de liaison montante vous permettent de configurer des fonctionnalités identiques pour tous les adaptateurs réseau au sein de plusieurs hôtes ou nœuds. Les profils de liaison montante sont des conteneurs pour les propriétés ou les fonctionnalités que vous souhaitez attribuer à vos adaptateurs réseau. Plutôt que de configurer des propriétés ou des fonctionnalités de manière individuelle pour chaque adaptateur réseau, vous pouvez spécifier les fonctionnalités dans les profils de liaison montante, puis les appliquer au moment de la création des nœuds de transport NSX-T Data Center.

Les liaisons montantes à l'état de veille ne sont pas prises en charge sur les dispositifs NSX Edge basés sur une machine/un dispositif virtuel. Lorsque vous installez NSX Edge comme un dispositif virtuel, utilisez le profil de liaison montante par défaut. Chaque profil de liaison montante créé pour un dispositif NSX Edge basé sur une machine virtuelle doit uniquement spécifier une liaison montante active, pas de liaison montante à l'état de veille.

Note Les machines virtuelles NSX Edge permettent l'utilisation de plusieurs liaisons montantes, si vous créez un N-VDS distinct pour chaque liaison montante, en utilisant un VLAN différent pour chacun. Chaque liaison montante a besoin d'une zone de transport VLAN distincte. Ceci permet de prendre en charge un nœud NSX Edge qui se connecte à plusieurs commutateurs ToR.

Conditions préalables

- Familiarisez-vous avec la mise en réseau de NSX Edge. Reportez-vous à la section [Configuration réseau de NSX Edge](#).
- Chaque liaison montante du profil de liaison montante doit correspondre à un lien physique actif et disponible sur votre hôte d'hyperviseur ou sur le nœud NSX Edge.

Par exemple, supposons que votre hôte d'hyperviseur dispose de deux liens physiques actifs : vmnic0 et vmnic1. Supposons que vmnic0 soit utilisé pour les réseaux de gestion et de stockage, tandis que vmnic1 n'est pas utilisé. Cela peut signifier que vmnic1 peut être utilisé comme liaison montante de NSX-T Data Center, mais que vmnic0 ne le peut pas. Pour effectuer une association de liens, vous devez disposer de deux liens physiques non utilisés, tels que vmnic1 et vmnic2.

Pour un dispositif NSX Edge, les liaisons montantes VLAN et celles des points de terminaison de tunnel peuvent utiliser le même lien physique. Par exemple, vmnic0/eth0/em0 peut être utilisé pour votre réseau de gestion et vmnic1/eth1/em1 peut être utilisé pour vos liens fp-ethX.

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Infrastructure > Profils > Profils de liaison montante** et cliquez sur **Ajouter**.
- 3 Renseignez les détails du profil de liaison montante.

Option	Description
Nom	Entrez un nom de profil de liaison montante.
Description	Ajoutez une description de profil de liaison montante facultative.

Option	Description
LAG	<p>(Facultatif) Groupes d'agrégation de liens (LAG) utilisant le protocole LACP (Link Aggregation Control Protocol) pour le réseau de transport</p> <p>Note Pour le protocole LACP, plusieurs LAG ne sont pas pris en charge sur les hôtes KVM.</p> <p>Ajoutez une liste séparée par des virgules de noms de liaisons montantes actives.</p> <p>Ajoutez une liste séparée par des virgules de noms de liaisons montantes en veille. Les noms de liaisons montantes actives et à l'état de veille créés peuvent être un texte de votre choix qui représente les liens physiques. Ces noms de liaisons montantes seront utilisés plus tard lors de la création des nœuds de transport. L'interface utilisateur/API des nœuds de transport vous permet de spécifier le lien physique qui correspond à chaque liaison montante nommée.</p> <p>Options de mécanisme de hachage LAG possibles.</p> <ul style="list-style-type: none"> ■ Adresse MAC source ■ Adresse MAC de destination ■ Adresse MAC source et de destination ■ Adresse IP source/destination et VLAN ■ Adresse MAC source et de destination, adresse IP et port TCP/UDP
Associations	<p>Dans la section Association, cliquez sur Ajouter et entrez les détails. La stratégie d'association définit la manière dont le N-VDS utilise sa liaison montante pour la redondance et l'équilibrage de charge du trafic. Il existe deux modes de stratégie d'association pour configurer la stratégie d'association :</p> <ul style="list-style-type: none"> ■ Ordre de basculement : une liaison montante active est spécifiée, ainsi qu'une liste facultative de liaisons montantes en veille. En cas d'échec de la liaison montante active, la liaison montante suivante dans la liste en veille remplace la liaison montante active. Aucun équilibrage de charge n'est réellement effectué avec cette option. ■ Source avec équilibrage de charge : une liste de liaisons montantes actives est spécifiée et chaque interface sur le nœud de transport est liée à une liaison montante active. Cette configuration permet l'utilisation de plusieurs liaisons montantes actives en même temps. <p>Note Sur les hôtes KVM, une seule stratégie d'association d'ordre de basculement est prise en charge. La stratégie d'association de source d'équilibrage de charge n'est pas prise en charge.</p> <p>(Uniquement pour les hôtes ESXi) Vous pouvez définir les stratégies suivantes pour une zone de transport :</p> <ul style="list-style-type: none"> ■ Une stratégie d'association nommée pour chaque commutateur logique configuré sur le commutateur. ■ Une stratégie d'association par défaut pour l'ensemble du commutateur. <p>Stratégie d'association nommée : avec une stratégie d'association nommée, pour chaque commutateur logique vous pouvez définir un mode spécifique de stratégie d'association et des liaisons montantes. Ce type de stratégie vous donne la possibilité de sélectionner des liaisons montantes en fonction des besoins de bande passante.</p> <ul style="list-style-type: none"> ■ Si vous définissez une stratégie d'association nommée, le N-VDS l'utilise si elle est spécifiée par la zone de transport et le commutateur logique liés dans l'hôte.

Option	Description
	<ul style="list-style-type: none"> ■ Si vous ne définissez pas de stratégies d'association nommées, le N-VDS utilise la stratégie d'association par défaut.

4 Entrez une valeur du VLAN de transport.

5 Entrez la valeur de MTU.

La valeur par défaut est 1600.

Outre l'interface utilisateur, vous pouvez également afficher les profils de liaison montante avec l'appel d'API GET `/api/v1/host-switch-profiles` :

```
{
  "result_count": 2,
  "results": [
    {
      "resource_type": "UplinkHostSwitchProfile",
      "id": "16146a24-122b-4274-b5dd-98b635e4d52d",
      "display_name": "comp-uplink",
      "transport_vlan": 250,
      "teaming": {
        "active_list": [
          {
            "uplink_type": "PNIC",
            "uplink_name": "uplink-1"
          }
        ],
        "standby_list": [ {
          "uplink_name": "uplink-2",
          "uplink_type": "PNIC"
        } ],
        "policy": "FAILOVER_ORDER"
      },
      "mtu": 1600,
      "_last_modified_time": 1457984399526,
      "_create_time": 1457984399526,
      "_last_modified_user": "admin",
      "_system_owned": false,
      "_create_user": "admin",
      "_revision": 0
    },
    {
      "resource_type": "UplinkHostSwitchProfile",
      "id": "c9e35cec-e9d9-4c51-b52e-17a5c1bd9a38",
      "display_name": "vlan-uplink",
      "transport_vlan": 100,
      "teaming": {
        "active_list": [
          {
            "uplink_type": "PNIC",
            "uplink_name": "uplink-1"
          }
        ],

```



```

        "standby_list": [],
        "policy": "FAILOVER_ORDER"
    },
    "named_teamings": [
        {
            "active_list": [
                {
                    "uplink_type": "PNIC",
                    "uplink_name": "uplink-2"
                }
            ],
            "standby_list": [
                {
                    "uplink_type": "PNIC",
                    "uplink_name": "uplink-1"
                }
            ],
            "policy": "FAILOVER_ORDER",
            "name": "named teaming policy"
        }
    ],
    "mtu": 1600,
    "_last_modified_time": 1457984399574,
    "_create_time": 1457984399574,
    "_last_modified_user": "admin",
    "_system_owned": false,
    "_create_user": "admin",
    "_revision": 0
}
]
}

```

Étape suivante

Créez une zone de transport. Reportez-vous à la section [Créer des zones de transport](#).

Créer des zones de transport

Les zones de transport dictent quels hôtes et, en conséquence, quelles machines virtuelles peuvent participer à l'utilisation d'un réseau donné. En limitant le nombre d'hôtes pouvant « voir » un commutateur logique, la zone de transport limite les machines virtuelles pouvant être attachées à ce dernier. Une zone de transport peut s'étendre sur un ou plusieurs clusters d'hôtes.

Un environnement NSX-T Data Center peut comporter une ou plusieurs zones de transport en fonction de vos besoins. Un hôte peut faire partie de plusieurs zones de transport. Un commutateur logique ne peut faire partie que d'une zone de transport.

NSX-T Data Center n'autorise pas la connexion de machines virtuelles qui se trouvent dans des zones de transport différentes dans le réseau de couche 2. 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.

La zone de transport de superposition est à la fois utilisée par les nœuds de transport hôte et les dispositifs NSX Edge. Lorsqu'un hôte ou un nœud de transport NSX Edge est ajouté à une zone de transport de superposition, un N-VDS est installé sur l'hôte ou sur le dispositif NSX Edge.

La zone de transport VLAN est utilisée par le dispositif NSX Edge pour ses liaisons montantes VLAN. Lorsqu'un dispositif NSX Edge est ajouté à une zone de transport VLAN, un N-VDS VLAN est installé sur le dispositif NSX Edge.

Le N-VDS permet aux paquets de faire circuler des dispositifs virtuels vers les dispositifs physiques en liant les liaisons montantes et descendantes des routeurs logiques aux cartes réseau physiques.

Lorsque vous créez une zone de transport, vous devez donner un nom au N-VDS qui sera installé sur les nœuds de transport lorsque ceux-ci seront ajoutés à la zone de transport. Vous avez toute liberté quant au choix du nom du N-VDS.

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Infrastructure > Zones de transport > Ajouter**.
- 3 Entrez un nom pour la zone de transport et éventuellement une description.
- 4 Entrez un nom pour le N-VDS.
- 5 Sélectionnez un mode N-VDS.

Les options sont **Standard** et **Chemin de données amélioré**.

- 6 Si le mode N-VDS est Standard, sélectionnez un type de trafic.

Les options sont **Superposition** et **VLAN**.

- 7 Si le mode N-VDS est Chemin de données optimisé, sélectionnez un type de trafic.

Les options sont **Superposition** et **VLAN**.

Note Dans le mode de chemin de données optimisé, seules les configurations de carte réseau spécifiques sont prises en charge. Assurez-vous de configurer les cartes réseau prises en charge.

- 8 Entrez un ou plusieurs noms de stratégie d'association de liaisons montantes. Ces stratégies d'association nommées peuvent être utilisées par les commutateurs logiques attachés à la zone de transport. Si les commutateurs logiques ne trouvent pas de stratégie d'association nommée correspondante, la stratégie d'association de liaison montante par défaut est utilisée.
- 9 Sur la page **Zones de Transport**, affichez la nouvelle zone de transport.
- 10 (Facultatif) Vous pouvez également afficher la nouvelle zone de transport à l'aide de l'appel d'API GET `https://<nsx-mgr>/api/v1/transport-zones`.

```
{
  "cursor": "00369b661aed-1eaa-4567-9408-ccbfcfe50b416tz-vlan",
  "result_count": 2,
```

```

"results": [
  {
    "resource_type": "TransportZone",
    "description": "comp overlay transport zone",
    "id": "efd7f38f-c5da-437d-af03-ac598f82a9ec",
    "display_name": "tz-overlay",
    "host_switch_name": "overlay-hostswitch",
    "transport_type": "OVERLAY",
    "transport_zone_profile_ids": [
      {
        "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
        "resource_type": "BfdHealthMonitoringProfile"
      }
    ],
    "_create_time": 1459547126454,
    "_last_modified_user": "admin",
    "_system_owned": false,
    "_last_modified_time": 1459547126454,
    "_create_user": "admin",
    "_revision": 0,
    "_schema": "/v1/schema/TransportZone"
  },
  {
    "resource_type": "TransportZone",
    "description": "comp vlan transport zone",
    "id": "9b661aed-1eaa-4567-9408-ccbcbfe50b416",
    "display_name": "tz-vlan",
    "host_switch_name": "vlan-uplink-hostswitch",
    "transport_type": "VLAN",
    "transport_zone_profile_ids": [
      {
        "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
        "resource_type": "BfdHealthMonitoringProfile"
      }
    ],
    "_create_time": 1459547126505,
    "_last_modified_user": "admin",
    "_system_owned": false,
    "_last_modified_time": 1459547126505,
    "_create_user": "admin",
    "_revision": 0,
    "_schema": "/v1/schema/TransportZone"
  }
]
}

```

Étape suivante

Vous pouvez également créer un profil de zone de transport personnalisé et le lier à la zone de transport. Les profils de zone de transport personnalisés peuvent être créés à l'aide de l'API `POST /api/v1/transportzone-profiles`. Il n'existe pas de workflow pour la création d'un profil de zone de transport via l'interface utilisateur. Une fois créé, le profil de zone de transport peut être recherché dans la zone de transport à l'aide de l'API `PUT /api/v1/transport-zones/<transport-zone-id>`.

Créez un nœud de transport. Reportez-vous à la section [Créer un nœud de transport hôte](#).

Créer un nœud de transport hôte

Un nœud de transport est un nœud qui participe à une superposition NSX-T Data Center ou à une mise en réseau VLAN NSX-T Data Center.

Pour un hôte KVM, vous pouvez préconfigurer le N-VDS ou laisser à NSX Manager le soin d'effectuer la configuration. Pour un hôte ESXi, NSX Manager configure toujours le N-VDS.

Note Si vous prévoyez de créer des nœuds de transport à partir d'une machine virtuelle modèle, assurez-vous qu'il n'existe aucun certificat sur l'hôte dans `/etc/vmware/nsx/`. L'agent netcpa ne crée pas de certificat s'il en existe déjà un.

Le serveur bare metal prend en charge une zone de transport de superposition et VLAN. Vous pouvez utiliser l'interface de gestion pour gérer le serveur bare metal. L'interface d'application vous permet d'accéder aux applications sur le serveur bare metal.

Les cartes réseau physiques uniques fournissent une adresse IP pour les interfaces IP de gestion et d'application.

Les doubles cartes réseau physiques fournissent une carte réseau physique et une adresse IP unique pour l'interface de gestion. Les doubles cartes réseau physiques fournissent également une carte réseau physique et une adresse IP unique pour l'interface d'application.

Plusieurs cartes réseau physiques dans une configuration liée fournissent deux cartes réseau physiques et une adresse IP unique pour l'interface de gestion. Plusieurs cartes réseau physiques dans une configuration liée fournissent également deux cartes réseau physiques et une adresse IP unique pour l'interface d'application.

Conditions préalables

- L'hôte doit être relié au plan de gestion et la connectivité MPA doit être activée sur la page **Infrastructure > Hôtes**.
- Une zone de transport doit être configurée.
- Un profil de liaison montante doit être configuré ou vous pouvez utiliser le profil de liaison montante par défaut.
- Un pool d'adresses IP doit être configuré, ou un serveur DHCP doit être disponible dans le déploiement de réseau.

- Au moins une carte réseau physique non utilisée doit être disponible sur le nœud hôte.

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Infrastructure > Nœuds > Nœuds de transport > Ajouter**.
- 3 Entrez un nom pour le nœud de transport.
- 4 Sélectionnez un nœud dans le menu déroulant.
- 5 Sélectionnez les zones de transport appartenant à ce nœud de transport.
- 6 Cliquez sur l'onglet **N-VDS**.
- 7 Pour un nœud KVM, sélectionnez le type de N-VDS.

Option	Description
Standard	NSX Manager crée le N-VDS. Cette option est sélectionnée par défaut.
Préconfiguré	Le N-VDS est déjà configuré.

Pour un nœud non-KVM, le type N-VDS est toujours **Standard** ou **Chemin de données optimisé**.

- 8 Pour un N-VDS standard, indiquez les informations suivantes.

Option	Description
Nom du N-VDS	Il doit être identique à celui du N-VDS de la zone de transport à laquelle ce nœud appartient.
Profil NIOC	Sélectionnez le profil NIOC dans le menu déroulant.
Profil de liaison montante	Sélectionnez le profil de liaison montante dans le menu déroulant.
Attribution IP	Sélectionnez Utiliser DHCP , Utiliser le pool IP ou Utiliser la liste d'adresses IP statiques . Si vous sélectionnez Utiliser la liste d'adresses IP statiques , vous devez spécifier une liste d'adresses IP séparées par des virgules, une passerelle et un masque de sous-réseau.
Pool IP	Si vous avez sélectionné l'option Utiliser le pool IP pour l'attribution d'adresse IP, spécifiez le nom du pool d'adresses IP.
Cartes réseau physiques	Assurez-vous que la carte réseau physique est déjà utilisée (par exemple, par un commutateur virtuel standard ou par un commutateur distribué vSphere). Sinon, le nœud de transport reste à l'état réussite partielle et l'établissement de la connectivité LCP du nœud d'infrastructure échoue. Pour le serveur bare metal, sélectionnez la carte réseau physique qui peut être configurée en tant que port de liaison montante 1. Le port de liaison montante 1 est défini dans le profil de liaison montante. Si vous ne disposez que d'un seul adaptateur réseau dans votre serveur bare metal, sélectionnez cette carte réseau physique pour que le port de liaison montante 1 soit attribué à l'interface de gestion et à l'interface d'application.

9 Pour un chemin de données optimisé N-VDS, fournissez les informations suivantes.

Option	Description
Nom du N-VDS	Il doit être identique à celui du N-VDS de la zone de transport à laquelle ce nœud appartient.
Attribution IP	<p>Sélectionnez Utiliser DHCP, Utiliser le pool IP ou Utiliser la liste d'adresses IP statiques.</p> <p>Si vous sélectionnez Utiliser la liste d'adresses IP statiques, vous devez spécifier une liste d'adresses IP séparées par des virgules, une passerelle et un masque de sous-réseau.</p>
Pool IP	Si vous avez sélectionné l'option Utiliser le pool IP pour l'attribution d'adresses IP, spécifiez le nom du pool d'adresses IP.
Cartes réseau physiques	Sélectionnez une carte réseau physique pouvant mettre en œuvre un chemin de données optimisé. Assurez-vous que la carte réseau physique est déjà utilisée (par exemple, par un commutateur virtuel standard ou par un commutateur distribué vSphere). Sinon, le nœud de transport reste à l'état réussite partielle , et la connectivité LCP du nœud d'infrastructure est impossible à établir.
Liaison montante	Sélectionnez le profil de liaison montante dans le menu déroulant.
Configuration du CPU	<p>Dans le menu déroulant Index de nœud NUMA, sélectionnez le nœud NUMA que vous souhaitez attribuer à un commutateur N-VDS. Le premier nœud NUMA présent sur le nœud est représenté par la valeur 0.</p> <p>Vous pouvez déterminer le nombre de nœuds NUMA sur votre hôte en exécutant la commande <code>esxcli hardware memory get</code>.</p> <p>Note Si vous souhaitez modifier le nombre de nœuds NUMA qui ont une affinité avec un commutateur N-VDS, vous pouvez mettre à jour la valeur d'index du nœud NUMA.</p> <p>Dans le menu déroulant Nombre de fichiers Lcore par nœud NUMA, sélectionnez le nombre de cœurs logiques qui doivent être utilisés par le chemin de données optimisé.</p> <p>Vous pouvez déterminer le nombre maximal de cœurs logiques pouvant être créés sur le nœud NUMA en exécutant la commande <code>esxcli network ens maxLcores get</code>.</p> <p>Note Si vous avez épuisé les nœuds et les cœurs logiques NUMA disponibles, tout nouveau commutateur ajouté au nœud de transport ne peut pas être activé pour le trafic ENS.</p>

10 Pour un N-VDS préconfiguré, indiquez les informations suivantes.

Option	Description
ID externe du N-VDS	Il doit être identique à celui du N-VDS de la zone de transport à laquelle ce nœud appartient.
VTEP	Nom du point de terminaison de tunnel virtuel.

Après l'ajout de l'hôte en tant que nœud de transport, la connexion d'hôte à NSX Controller passe à l'état actif.

11 Observez l'état de connexion sur la page **Nœuds de Transport**.

12 Vous pouvez également afficher l'état de connexion à l'aide des commandes CLI.

- ◆ Pour ESXi, tapez la commande `esxcli network ip connection list | grep 1234`.

```
# esxcli network ip connection list | grep 1234
tcp    0    0 192.168.210.53:20514 192.168.110.34:1234 ESTABLISHED 1000144459 newreno
netcpa
```

- ◆ Pour KVM, tapez la commande `netstat -anp --tcp | grep 1234`.

```
user@host:~$ netstat -anp --tcp | grep 1234
tcp    0    0 192.168.210.54:57794 192.168.110.34:1234 ESTABLISHED -
```

13 (Facultatif) Affichez le nœud de transport à l'aide de l'appel d'API GET `https://<nsx-mgr>/api/v1/transport-nodes/<node-id>`.

```
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "95c8ce77-f895-43de-adc4-03a3ae2565e2",
  "display_name": "node-comp-01b",
  "tags": [],
  "transport_zone_endpoints": [
    {
      "transport_zone_id": "efd7f38f-c5da-437d-af03-ac598f82a9ec",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ]
    }
  ],
  "host_switches": [
    {
      "host_switch_profile_ids": [
        {
          "value": "8abdb6c0-db83-4e69-8b99-6cd85bfcc61d",
          "key": "UplinkHostSwitchProfile"
        },
        {
          "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
          "key": "LldpHostSwitchProfile"
        }
      ]
    },
    {
      "host_switch_name": "overlay-hostswitch",
      "pnics": [
        {
          "device_name": "vmnic1",
          "uplink_name": "uplink-1"
        }
      ]
    }
  ],
}
```

```

        "static_ip_pool_id": "c78ac522-2a50-43fe-816a-c459a210127e"
    }
],
"node_id": "c551290a-f682-11e5-ae84-9f8726e1de65",
"_create_time": 1460051753373,
"_last_modified_user": "admin",
"_system_owned": false,
"_last_modified_time": 1460051753373,
"_create_user": "admin",
"_revision": 0
}

```

14 Ajoutez le nœud de transport qui vient d'être créé à une zone de transport.

- a Sélectionnez le nœud de transport.
- b Sélectionnez **Actions > Ajouter à la zone de transport**.
- c Sélectionnez la zone de transport dans le menu déroulant.

Tous les autres champs sont remplis.

Note Pour un N-VDS standard, une fois le nœud de transport créé, si vous souhaitez modifier la configuration, telle que l'attribution IP sur le point de terminaison de tunnel, vous devez le faire via l'interface utilisateur graphique de NSX Manager et non via l'interface de ligne de commande de l'hôte.

Étape suivante

Migrez les interfaces réseau à partir d'un commutateur vSphere standard vers un commutateur virtuel distribué NSX-T. Reportez-vous à la section [Migration de VMkernel vers un commutateur N-VDS](#).

Configurer la création de nœuds de transport automatisée

Si vous disposez d'un cluster vCenter Server, vous pouvez automatiser l'installation et la création des nœuds de transport sur tous les hôtes NSX-T Data Center dans un ou plusieurs clusters au lieu de les configurer manuellement.

Note La création de nœuds de transport NSX-T Data Center automatisée est prise en charge uniquement sur vCenter Server 6.5 Update 1, 6.5 Update 2 et 6.7.

Si le nœud de transport est déjà configuré, la création de nœuds de transport automatisée n'est pas applicable pour ce nœud.

Conditions préalables

- L'hôte doit faire partie d'un cluster vCenter Server.
- Une zone de transport doit être configurée.
- Un profil de liaison montante doit être configuré ou vous pouvez utiliser le profil de liaison montante par défaut.

- Un pool d'adresses IP doit être configuré, ou un serveur DHCP doit être disponible dans le déploiement de réseau.
- Au moins une carte réseau physique non utilisée doit être disponible sur le nœud hôte.
- vCenter Server doit disposer d'au moins un cluster.
- Un gestionnaire de calcul doit être configuré.

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Infrastructure > Nœuds > Hôtes**.
- 3 Dans le menu déroulant Géré par, sélectionnez un gestionnaire de calcul existant.
- 4 Sélectionnez un cluster et cliquez sur **Configurer le cluster**.
- 5 Indiquez les détails du cluster de configuration.

Option	Description
Installer automatiquement NSX	Basculez le bouton pour activer l'installation de NSX-T Data Center sur tous les hôtes du cluster vCenter Server.
Créer automatiquement des nœuds de transport	<p>Basculez le bouton pour activer la création de nœuds de transport sur tous les hôtes du cluster vCenter Server. Il s'agit d'un paramètre obligatoire.</p> <p>Note Si un nœud de transport préconfiguré existe dans le cluster ou est déplacé vers un autre cluster, NSX-T Data Center ne met pas à jour le nœud de transport préalablement configuré avec la configuration définie dans le modèle de nœud de transport du cluster. Pour vous assurer que tous les nœuds ont la même configuration, supprimez le nœud de transport préconfiguré et ajoutez cet hôte au cluster.</p>
Zone de transport	Sélectionnez un nœud de transport existant dans le menu déroulant.
Profil de liaison montante	<p>Sélectionnez un profil de liaison montante existant dans le menu déroulant ou créez un profil de liaison montante personnalisé.</p> <p>Note Les hôtes d'un cluster doivent avoir le même profil de liaison montante.</p> <p>Vous pouvez également utiliser le profil de liaison montante par défaut.</p>
Attribution IP	<p>Dans le menu déroulant, sélectionnez Utiliser DHCP ou Utiliser le pool d'adresses IP.</p> <p>Si vous sélectionnez Utiliser le pool d'adresses IP, vous devez allouer un pool d'adresses IP existant dans le réseau dans le menu déroulant.</p>
Cartes réseau physiques	<p>Assurez-vous que la carte réseau physique est déjà utilisée, par exemple par un commutateur virtuel standard ou par un commutateur distribué vSphere. Sinon, le nœud de transport est à l'état réussite partielle, et la connectivité LCP du nœud d'infrastructure est impossible à établir.</p> <p>Vous pouvez utiliser la liaison montante par défaut ou attribuer une liaison montante existante dans le menu déroulant.</p> <p>Cliquez sur Ajouter une PNIC pour augmenter le nombre de cartes réseau dans la configuration.</p>

La création de nœuds d'installation et de transport de NSX-T Data Center sur chaque hôte du cluster démarre en parallèle. L'intégralité du processus dépend du nombre d'hôtes dans le cluster.

Lorsqu'un nouvel hôte est ajouté au cluster vCenter Server, la création de nœuds d'installation et de transport de NSX-T Data Center s'effectue automatiquement.

6 (Facultatif) Affichez l'état de connexion ESXi.

```
# esxcli network ip connection list | grep 1234
tcp    0    0  192.168.210.53:20514  192.168.110.34:1234  ESTABLISHED  1000144459  newreno  netcpa
```

7 (Facultatif) Supprimez un nœud d'installation et de transport de NSX-T Data Center d'un hôte du cluster.

- a Sélectionnez un cluster et cliquez sur **Configurer le cluster**.
- b Basculez le bouton Installer automatiquement NSX pour désactiver l'option.
- c Sélectionnez un ou plusieurs hôtes et cliquez sur **Désinstaller NSX**.

La désinstallation prend jusqu'à 3 minutes.

Configurer un nœud de transport d'hôte ESXi avec agrégation de liens

Cette procédure décrit comment créer un profil de liaison montante qui dispose d'un groupe d'agrégation de liens configuré et comment configurer un nœud de transport d'hôte ESXi pour utiliser ce profil de liaison montante.

Conditions préalables

- Familiarisez-vous avec les étapes de création d'un profil de liaison montante. Reportez-vous à la section [Créer un profil de liaison montante](#).
- Familiarisez-vous avec les étapes de création d'un nœud de transport hôte. Reportez-vous à la section [Créer un nœud de transport hôte](#).

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Infrastructure > Profils > Profils de liaison montante** et cliquez sur **Ajouter**.
- 3 Entrez un nom et éventuellement une description.
Par exemple, vous entrez le nom **uplink-profile1**.
- 4 Sous **LAG**, cliquez sur **Ajouter** pour ajouter un groupe d'agrégation de liens.
Par exemple, vous ajoutez un LAG appelé **lag1** avec 2 liaisons montantes.
- 5 Sous **Associations**, sélectionnez l'entrée **Association par défaut**.

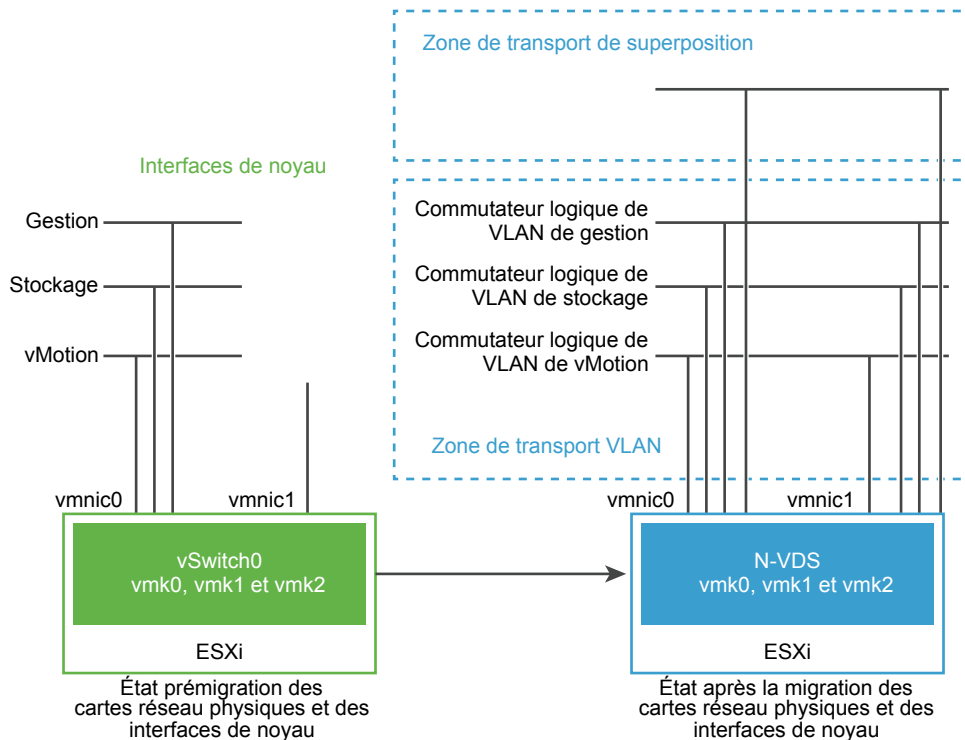
- 6 Dans le champ **Liaisons montantes actives**, entrer le nom du groupe d'agrégation de liens que vous avez ajouté à l'étape 4. Dans cet exemple, le nom est **lag1**.
- 7 Cliquez sur **Ajouter** en bas de la boîte de dialogue.
- 8 Entrez une valeur pour **Transport VLAN** et **MTU**.
- 9 Cliquez sur **Ajouter** en bas de la fenêtre.
- 10 Sélectionnez **Infrastructure > Nœuds > Nœuds de transport > Ajouter**.
- 11 Renseignez l'onglet **Général**.
- 12 Dans l'onglet **N-VDS**, sélectionnez le profil de liaison montante **uplink-profile1** qui a été créé à l'étape 3.
- 13 Dans le champ **Cartes réseau physiques**, vous verrez une liste déroulante de cartes réseau physiques et une liste déroulante des liaisons montantes que vous avez spécifiées lorsque vous avez créé le profil de liaison montante. Vous verrez notamment les liaisons montantes **lag1-0** et **lag1-1**, correspondant au groupe d'agrégation de liens **lag1** qui a été créé à l'étape 4. Sélectionnez une carte réseau physique pour **lag1-0** et une carte réseau physique pour **lag1-1**.
- 14 Renseignez les autres champs.

Migration de VMkernel vers un commutateur N-VDS

Lorsque vous créez un nœud de transport, il peut être nécessaire de migrer les cartes réseau physiques et les interfaces de noyau d'un commutateur vSphere standard (VSS) ou VDS vers un commutateur virtuel distribué NSX-T Data Center (N-VDS). Après la migration, N-VDS gère le trafic sur le réseau VLAN.

Les cartes réseau physiques et leurs interfaces VMkernel sont initialement associées à un commutateur VSS ou VDS sur un hôte vSphere ESXi. Ces interfaces de noyau sont définies sur ces hôtes pour fournir de la connectivité à l'interface de gestion, de stockage et à d'autres interfaces. Après la migration, les interfaces VMkernel et leurs cartes réseau physiques associées se connectent au N-VDS et gèrent le trafic sur le réseau VLAN et les zones de transport de superposition.

Dans la figure suivante, si un hôte possède seulement deux cartes réseau physiques, vous pouvez souhaiter attribuer ces deux cartes réseau au N-VDS à des fins de redondance.

Chiffre 8-2. Prémigration et post-migration des interfaces réseau vers un N-VDS

Avant la migration, l'hôte vSphere ESXi dispose de deux liaisons montantes dérivées de deux ports physiques : vmnic0 et vmnic1. Ici, vmnic0 est configurée pour être dans un état actif, attachée à un VSS ou VDS, tandis que vmnic1 n'est pas utilisée. En outre, il existe trois interfaces VMkernel : vmk0, vmk1 et vmk2.

Vous migrez les interfaces VMkernel en utilisant l'interface utilisateur de NSX-T Data Center Manager ou des API de NSX-T Data Center. Reportez-vous à la section *Guide de l'API de NSX-T Data Center*.

Après la migration, vmnic0, vmnic1 et leurs interfaces VMkernel sont migrées vers le commutateur N-VDS. La vmnic0 et la vmnic1 sont connectées sur le VLAN et les zones de transport de superposition.

Migrer les interfaces VMkernel vers un commutateur N-VDS à l'aide de l'interface utilisateur de NSX-T Data Center Manager

L'interface utilisateur de NSX-T Data Center Manager vous permet de migrer toutes les interfaces de noyau, notamment l'interface de gestion depuis un VSS ou un VDS vers un commutateur N-VDS.

Dans cet exemple, envisagez d'utiliser un hôte vSphere ESXi avec deux adaptateurs physiques, vmnic0 et vmnic1. Le commutateur VSS ou VDS par défaut sur l'hôte est configuré avec une seule liaison montante mappée à vmnic0. L'interface VMkernel, vmk0, est également configurée sur VSS ou VDS pour exécuter le trafic de gestion sur le nœud. L'objectif est de migrer vmnic0 et vmk0 vers le commutateur N-VDS.

Dans le cadre de la préparation de l'hôte, VLAN et les zones de transport de superposition sont créés pour exécuter le trafic de gestion et de VM, respectivement. Un commutateur N-VDS est également créé et configuré avec une liaison montante mappée à vmnic1. Après la migration, NSX-T Data Center migre vmnic0 et vmk0 depuis le commutateur VSS ou VDS vers le commutateur N-VDS sur le nœud.

Conditions préalables

- Vérifiez que l'infrastructure réseau physique fournit la même connectivité de réseau local à vmnic1 et à vmnic0.
- Vérifiez que la carte réseau physique inutilisée, vmnic1, dispose d'une connectivité de couche 2 avec vmnic0.
- Assurez-vous que toutes interfaces VMkernel impliquées dans cette migration appartiennent au même réseau. Si vous migrez des interfaces VMkernel vers une liaison montante connectée à un autre réseau, l'hôte peut devenir inaccessible ou ne plus fonctionner.

Procédure

- 1 Dans l'interface utilisateur de NSX Manager, accédez à **Infrastructure -> Profil -> Profils de liaison montante**.
- 2 Créez un profil de liaison montante en utilisant vmnic0 en tant que liaison montante active et vmnic1 en tant que la liaison montante passive.
- 3 Accédez à **Infrastructure -> Zones de transport -> Ajouter**.
- 4 Créez une superposition et des zones de transport VLAN pour gérer le trafic de machine virtuelle et le trafic de gestion, respectivement.

Note Le nom du N-VDS utilisé dans la zone de transport VLAN et la zone de transport de SUPERPOSITION doit être le même.

- 5 Accédez à **Infrastructure -> Nœud -> Nœud de transport**.
- 6 Ajoutez les deux zones de transport au nœud de transport.
- 7 Dans l'onglet N-VDS, ajoutez un N-VDS en définissant des liaisons montantes, des adaptateurs physiques à utiliser par N-VDS.

Le nœud de transport est connecté aux zones de transport via une seule liaison montante.
- 8 Pour vous assurer que vmk0 et vmnic0 obtiennent une connectivité à la zone de transport VLAN après la migration, créez un commutateur logique pour la zone de transport VLAN appropriée.
- 9 Sélectionnez le nœud de transport, cliquez sur **Actions -> Migrer les adaptateurs physiques et VMkernel ESX**.
- 10 Sélectionnez **Migrer vers des commutateurs logiques**.
- 11 Sélectionnez le commutateur N-VDS.
- 12 Ajoutez les adaptateurs VMkernel et les commutateurs logiques associés.
- 13 Ajoutez l'adaptateur physique correspondant à l'interface VMkernel. Assurez-vous qu'il reste au moins un adaptateur physique sur le commutateur VSS ou VDS.
- 14 Cliquez sur **Enregistrer**.
- 15 Cliquez sur **Continuer** pour commencer la migration.

- 16 Testez la connectivité vers vmnic0 et vmk0 depuis NSX Manager.
- 17 En outre, dans vCenter Server, vérifiez que l'adaptateur VMkernel est associé au commutateur NSX-T Data Center.

Les interfaces VMkernel et leurs adaptateurs physiques correspondants sont migrés vers N-VDS.

Étape suivante

Vous pouvez restaurer la migration VMkernel vers un commutateur VSS ou VDS.

Restaurer la migration d'interfaces VMkernel vers un commutateur VSS ou VDS en utilisant l'interface utilisateur de NSX-T Data Center Manager

Pour restaurer la migration d'interfaces VMkernel vers un commutateur VSS ou VDS, assurez-vous qu'il existe un groupe de ports sur l'hôte ESXi.

NSX-T Data Center doit être un groupe de ports pour migrer les interfaces VMkernel depuis le commutateur N-VDS vers le commutateur VSS ou VDS. Le groupe de ports accepte la demande du réseau de migrer ces interfaces vers le commutateur VSS ou VDS. Le membre de port qui participe à cette migration est déterminé en fonction de sa configuration de bande passante et de stratégie.

Avant de commencer la migration de VMkernel vers le commutateur VSS ou VDS, assurez-vous que les interfaces VMkernel sont opérationnelles et que la connectivité est établie sur le commutateur N-VDS.

Conditions préalables

- Un groupe de ports existe sur le serveur vSphere ESXi.

Procédure

- 1 Dans l'interface utilisateur de NSX Manager, accédez à **Infrastructure** -> **Nœuds** -> **Nœuds de transport**.
- 2 Sélectionnez le nœud de transport, cliquez sur **Actions** -> **Migrer les adaptateurs physiques et VMkernel ESX**.
- 3 Sélectionnez **Migrer vers des groupes de ports**.
- 4 Sélectionnez le commutateur N-VDS.
- 5 Ajoutez les adaptateurs VMkernel et les commutateurs logiques associés.
- 6 Ajoutez l'adaptateur physique correspondant à l'interface VMkernel. Assurez-vous qu'au moins un adaptateur physique reste connecté au commutateur VSS ou VDS.
- 7 Cliquez sur **Enregistrer**.
- 8 Cliquez sur **Continuer** pour commencer la migration.
- 9 Testez la connectivité vers vmnic0 et vmk0 depuis NSX Manager.
- 10 Dans vCenter Server, vous pouvez également vérifier que l'adaptateur VMkernel est associé au commutateur VSS ou VDS.

Les interfaces VMkernel et leurs adaptateurs physiques correspondants sont migrés vers N-VDS.

Étape suivante

Vous pouvez souhaiter migrer des interfaces VMkernel à l'aide d'API. Reportez-vous à la section [Migrer les interfaces du noyau vers N-VDS en utilisant des API](#).

Migrer les interfaces du noyau vers N-VDS en utilisant des API

Lorsque vous utilisez des API NSX-T Data Center, assurez-vous de d'abord migrer toutes les interfaces de noyau avant de migrer l'interface de gestion.

Envisagez d'utiliser l'hôte disposant de deux liaisons montantes connectées aux cartes réseau physiques respectifs. Dans cette procédure, vous pouvez commencer par une migration de l'interface du noyau de stockage, vmk1, vers N-VDS. Une fois que cette interface de noyau a migré vers N-VDS, vous pouvez migrer l'interface de gestion du noyau.

Reportez-vous à la section *Guide de l'API de NSX-T Data Center*.

Conditions préalables

- Vérifiez que l'infrastructure réseau physique fournit la même connectivité de réseau local à vmnic1 et à vmnic0.
- Vérifiez que la carte réseau physique inutilisée, vmnic1, dispose d'une connectivité de couche 2 avec vmnic0.
- Assurez-vous que toutes interfaces VMkernel impliquées dans cette migration appartiennent au même réseau. Si vous migrez des interfaces VMkernel vers une liaison montante connectée à un autre réseau, l'hôte peut devenir inaccessible ou ne plus fonctionner.

Procédure

- 1 Créez une zone de transport VLAN avec le host_switch_name du N-VDS utilisé par la zone de transport de superposition.
- 2 Créez un commutateur logique sauvegardé sur le VLAN dans la zone de transport VLAN avec un ID de VLAN qui correspond à celui utilisé par vmk1 sur le VSS ou VDS.
- 3 Ajoutez le nœud de transport vSphere ESXi à la zone de transport VLAN.

- 4 Récupérez la configuration du nœud de transport vSphere ESXi.

```
GET /api/v1/transport-nodes/<transportnode-id>
```

Où *<transportnode-id>* est l'UUID du nœud de transport.

- 5 Migrez vmk1 vers N-VDS.

```
PUT https://<NSXmgr>/api/v1/transport-nodes/<transportnode-id> ?
if_id=<vmk>&esx_mgmt_if_migration_dest=<network>
```

Où le *<transportnode-id>* est l'UUID du nœud de transport. *<vmk>* est le nom de l'interface VMkernel, vmk1. Le *<network>* est l'UUID du commutateur logique cible.

6 Vérifiez que la migration a réussi.

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```

Attendez que l'état de migration s'affiche comme SUCCESS. Vous pouvez également vérifier l'état de la migration de l'interface VMkernel dans vCenter Server.

L'interface VMkernel est migrée depuis un VSS ou un VDS vers le commutateur N-VDS.

Étape suivante

Vous pouvez migrer les interfaces VMkernel restantes et l'interface du noyau de gestion depuis le VSS ou le VDS vers le N-VDS.

Migrer l'interface du noyau de gestion depuis VSS ou VDS vers un N-VDS en utilisant des API

Après la migration de toutes les autres interfaces de noyau, procédez à la migration de l'interface du noyau de gestion. Lorsque vous migrez l'interface du noyau de gestion, vous déplacez vmnic0 et vmk0 d'un VSS ou VDS vers un N-VDS.

Ensuite, vous pouvez migrer la liaison montante physique vmnic0 et vmk0 vers le N-VDS en une seule étape. Modifiez la configuration de nœud de transport afin que la vmnic0 soit à présent configurée en tant qu'une de ses liaisons montantes.

Note Si vous souhaitez migrer la liaison montante vmnic0 et l'interface du noyau vmk0 séparément, migrez tout d'abord vmk0, puis migrez vmnic0. Si vous migrez vmnic0 d'abord, vmk0 reste sur le service VSS ou VDS sans aucune liaison montante de sauvegarde et vous perdez la connectivité à l'hôte.

Conditions préalables

- Vérifiez la connectivité aux vmknics déjà migrées. Reportez-vous à la section [Migrer les interfaces du noyau vers N-VDS en utilisant des API](#).
- Si vmk0 et vmk1 utilisent des VLAN différents, VLAN trunk doit être configuré sur le commutateur physique connecté aux PNIC vmnic0 et vmnic1 pour prendre en charge les deux réseaux VLAN.
- Vérifiez qu'un périphérique externe peut atteindre l'interface vmk1 sur le commutateur logique sauvegardé sur le VLAN de stockage et l'interface vmk2 sur le commutateur logique reposant sur le VLAN vMotion.

Procédure

- 1 (Facultatif) Créez une seconde interface de noyau de gestion sur VSS ou VDS et migrez cette interface nouvellement créée vers N-VDS.
- 2 (Facultatif) Depuis un périphérique externe, vérifiez la connectivité à l'interface de gestion de test.
- 3 Si vmk0 (interface de gestion) utilise un VLAN autre que vmk1 (interface de stockage), créez un commutateur logique sauvegardé sur le VLAN dans la zone de transport VLAN avec un ID de VLAN qui correspond à l'ID de VLAN utilisé par vmk0 sur le VSS ou VDS.

- Récupérez la configuration du nœud de transport vSphere ESXi.

```
GET /api/v1/transport-nodes/<transportnode-id>
```

Où *<transportnode-id>* est l'UUID du nœud de transport.

- Dans l'élément `host_switch_spec:host_switches` de la configuration, ajoutez la `vmnic0` à la table de `pnics` et attribuez-la à une liaison montante dédiée, `uplink-2`.

Note Lors de la migration des interfaces de VMkernel, nous avons attribué `vmnic1` à `uplink-1`. Il est nécessaire d'attribuer `vmnic0`, l'interface de gestion, à une liaison montante dédiée pour la réussite de la migration et pour l'accessibilité de l'hôte après la migration.

```
"pnics": [
  {
    "device_name": "vmnic0",
    "uplink_name": "uplink-2"
  },
  {
    "device_name": "vmnic1",
    "uplink_name": "uplink-1"
  }
],
```

- Migrez l'interface du noyau de gestion, de `vmk0` vers N-VDS à l'aide de la configuration mise à jour.

```
PUT api/v1/transport-nodes/<transportnode-  
id>?if_id=<vmk>&esx_mgmt_if_migration_dest=<network>
```

Où *<transportnode-id>* est l'UUID du nœud de transport. Le *<vmk>* est le nom de l'interface de gestion VMkernel `vmk0`. Le *<network>* est l'UUID du commutateur logique cible.

- Vérifiez que la migration a réussi.

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```

Attendez que l'état de migration s'affiche comme `SUCCESS`. Dans vCenter Server, vous pouvez vérifier si les adaptateurs de noyau sont configurés pour afficher le nouveau nom du commutateur logique.

Étape suivante

Vous pouvez choisir de rétablir la migration des interfaces de noyau et l'interface de gestion depuis N-VDS vers un commutateur VSS ou VDS.

Restaurer la migration d'interfaces VMkernel depuis un commutateur N-VDS vers un commutateur VSS ou VDS en utilisant des API

Lorsque vous restaurez des interfaces VMkernel, vous devez commencer par la migration de l'interface du noyau de gestion. Migrez ensuite les autres interfaces de noyau d'un N-VDS vers un commutateur VSS ou VDS.

Procédure

- 1 Vérifiez que l'état du nœud de transport indique une réussite.

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```

- 2 Récupérez la configuration du nœud de transport vSphere ESXi pour trouver les cartes réseau physiques définies à l'intérieur de l'élément "host_switch_spec":"host_switches".

```
GET /api/v1/transport-nodes/<transportnode-id>
```

```
"pnics": [
  { "device_name": "vmnic0",
    "uplink_name": "uplink-2"
  },
  { "device_name": "vmnic1",
    "uplink_name": "uplink-1"
  }
],
```

- 3 Supprimez vmnic0 de l'élément "host_switch_spec":"host_switches" de la configuration de nœud de transport pour préparer l'interface de gestion à la migration.

```
"pnics": [
  { "device_name": "vmnic1",
    "uplink_name": "uplink-1"
  }
],
```

- 4 Migrez l'interface de gestion, vmnic0 et vmk0, depuis N-VDS vers VSS ou VDS, à l'aide de la configuration modifiée.

```
PUT api/v1/transport-nodes/< transportnode-id>?
if_id=vmk0&esx_mgmt_if_migration_dest=<vmk0_port_group_name>
```

Où, <groupe_ports_vmk0> est le nom de groupe de ports qui a été affecté à vmk0 avant la migration vers le commutateur logique.

- 5 Vérifiez l'état de la migration.

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```

Attendez que l'état s'affiche comme « SUCCESS ».

- 6 Récupérez la configuration du nœud de transport vSphere ESXi.

```
GET /api/v1/transport-nodes/<transportnode-id>
```

- 7 Migrez vmk1 depuis N-VDS vers VSS ou VDS, à l'aide de la configuration de nœud de transport précédente.

```
PUT api/v1/transport-nodes/< transportnode-id>?
if_id=vmk1&esx_mgmt_if_migration_dest=<vmk1_port_group>
```

Où, `<groupe_ports_vmk1>` est le nom de groupe de ports qui a été affecté à vmk1 avant la migration vers le commutateur logique.

Note vmk0 ou vmk1 doit être migré vers le VSS ou le VDS avec au moins une carte réseau physique, le VSS ou le VDS ne disposant pas de carte réseau physique associée.

- 8 Vérifiez que l'état du nœud de transport indique une réussite.

GET /api/v1/transport-nodes/<transportnode-id>/state.

- 9 Effectuez la vérification post-migration pour éviter tout problème.
 - a L'interface du noyau de gestion vmk0 ne doit pas être migrée avant l'association d'une interface de liaison montante à VSS ou VDS.
 - b Assurez-vous que vmk0 reçoit son adresse IP de vmnic0. Dans le cas contraire, l'adresse IP peut changer, et les autres composants, comme VC, peuvent perdre la connectivité à l'hôte via l'ancienne adresse IP.

Vérifier l'état des nœuds de transport

Assurez-vous que le processus de création des nœuds de transport fonctionne correctement.

Après avoir créé un nœud de transport hôte, le N-VDS est installé sur l'hôte.

Procédure

- 1 Connectez-vous à NSX-T Data Center.
- 2 Accédez à la page Nœud de transport et affichez l'état VDS-N.
- 3 Vous pouvez également visualiser le N-VDS sur ESXi à l'aide de la commande `esxcli network ip interface list`.

Sous ESXi, la sortie de commande doit comporter une interface vmk (par exemple, vmk10) avec un nom de VDS correspondant au nom que vous avez utilisé lors de la configuration de la zone de transport et du nœud de transport.

```
# esxcli network ip interface list
...

vmk10
  Name: vmk10
  MAC Address: 00:50:56:64:63:4c
  Enabled: true
  Portset: DvsPortset-1
  Portgroup: N/A
  Netstack Instance: vxlan
  VDS Name: overlay-hostswitch
  VDS UUID: 18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2
  VDS Port: 10
  VDS Connection: 10
  Opaque Network ID: N/A
  Opaque Network Type: N/A
```

```

External ID: N/A
MTU: 1600
TSO MSS: 65535
Port ID: 67108895

```

```
...
```

Si vous utilisez le vSphere Client, vous pouvez afficher le N-VDS installé via l'interface utilisateur en sélectionnant l'hôte **Configuration > Adaptateurs réseau**.

La commande KVM qui permet de vérifier l'installation du N-VDS est la commande `ovs-vsctl show`. Notez que sur KVM, le nom du N-VDS est `nsx-switch.0`. Il ne correspond pas au nom utilisé dans la configuration du nœud de transport. La conception ne permet pas de faire autrement.

```

# ovs-vsctl show
...
    Bridge "nsx-switch.0"
        Port "nsx-uplink.0"
            Interface "em2"
        Port "nsx-vtep0.0"
            tag: 0
            Interface "nsx-vtep0.0"
                type: internal
        Port "nsx-switch.0"
            Interface "nsx-switch.0"
                type: internal
    ovs_version: "2.4.1.3340774"

```

4 Vérifiez qu'une adresse de point de terminaison est attribuée au nœud de transport.

L'interface `vmk10` reçoit une adresse IP du pool d'adresses IP NSX-T Data Center ou de DHCP, comme illustré ici :

```

# esxcli network ip interface ipv4 get

```

Name	IPv4 Address	IPv4 Netmask	IPv4 Broadcast	Address Type	DHCP	DNS
vmk0	192.168.210.53	255.255.255.0	192.168.210.255	STATIC		false
vmk1	10.20.20.53	255.255.255.0	10.20.20.255	STATIC		false
vmk10	192.168.250.3	255.255.255.0	192.168.250.255	STATIC		false

Dans KVM, vous pouvez vérifier le point de terminaison de tunnel et l'allocation IP à l'aide de la commande `ifconfig`.

```

# ifconfig
...
nsx-vtep0.0 Link encap:Ethernet HWaddr ba:30:ae:aa:26:53
    inet addr:192.168.250.4 Bcast:192.168.250.255 Mask:255.255.255.0
...

```

5 Vérifiez les informations d'état à l'aide de l'API.

Utilisez l'appel d'API GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state`. Par exemple :

```
{
  "state": "success",
  "host_switch_states": [
    {
      "endpoints": [
        {
          "default_gateway": "192.168.250.1",
          "device_name": "vmk10",
          "ip": "192.168.250.104",
          "subnet_mask": "255.255.255.0",
          "label": 69633
        }
      ],
      "transport_zone_ids": [
        "efd7f38f-c5da-437d-af03-ac598f82a9ec"
      ],
      "host_switch_name": "overlay-hostswitch",
      "host_switch_id": "18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2"
    }
  ],
  "transport_node_id": "2d030569-5769-4a13-8918-0c309c63fdb9"
}
```

Ajouter un gestionnaire de calcul

Un gestionnaire de calcul, par exemple, vCenter Server, est une application qui gère les ressources, telles que des hôtes et des machines virtuelles. NSX-T Data Center interroge les gestionnaires de calcul pour connaître les modifications, telles que l'ajout ou la suppression d'hôtes ou de machines virtuelles, et met à jour son inventaire en conséquence. L'ajout d'un gestionnaire de calcul est facultatif, NSX-T obtenant des informations d'inventaire, même sans gestionnaire de calcul, comme des machines virtuelles et des hôtes autonomes.

Dans cette version, cette fonctionnalité prend en charge :

- vCenter Server versions 6.5 Update 1, 6.5 Update 2 et 6.7.
- Les communications IPv6 et IPv4 avec vCenter Server.
- Un maximum de 5 gestionnaires de calcul.

Note NSX-T Data Center ne prend pas en charge la même instance de vCenter Server à enregistrer avec plusieurs instances de NSX Manager.

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.

- 2 Sélectionnez **Infrastructure > Gestionnaires de calcul** dans le panneau de navigation.
- 3 Cliquez sur **Ajouter**.
- 4 Indiquez les détails des gestionnaires de calcul.

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

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

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

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

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

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

Le panneau Gestionnaires de calcul affiche une liste de gestionnaires de calcul. Vous pouvez cliquer sur le nom du gestionnaire pour voir ou modifier ses détails ou pour gérer les balises qui s'appliquent au gestionnaire.

Créer une interface d'application pour les charges de travail de serveur Bare Metal

Avant de créer ou de migrer une interface d'application pour les charges de travail de serveur Bare Metal, vous devez configurer les modules de noyau NSX-T Data Center et installer des modules tiers Linux.

Procédure

- 1 Installez les modules tiers requis.

Reportez-vous à la section [Installer les modules tiers sur un hôte KVM ou un serveur bare metal](#).

2 Configurez les ports TCP et UDP.

Reportez-vous à la section [Ports TCP et UDP utilisés par vSphere ESXi, les hôtes KVM et le serveur Bare Metal](#).

3 Ajoutez un serveur Bare Metal à l'infrastructure NSX-T Data Center.

Reportez-vous à la section [Ajouter un hôte d'hyperviseur ou un serveur bare metal à l'infrastructure NSX-T Data Center](#).

4 Créez un nœud de transport hôte KVM.

Reportez-vous à la section [Créer un nœud de transport hôte](#).

5 Utilisez le playbook Ansible pour créer une interface d'application.

Reportez-vous à la section <https://github.com/vmware/bare-metal-server-integration-with-nsxt>.

Configurer des profils Network I/O Control

Utilisez le profil Network I/O Control (NIOC) pour allouer de la bande passante réseau aux applications stratégiques et pour résoudre les problèmes issus de l'utilisation de ressources communes par différents types de trafic.

Le profil NIOC présente une méthode de réservation de la bande passante pour le trafic système qui se fonde sur la capacité des adaptateurs physiques d'un hôte. Avec la version 3 de la fonctionnalité Network I/O Control, l'allocation et la réservation des ressources réseau sont améliorées sur l'ensemble du commutateur.

Network I/O Control version 3 pour NSX-T Data Center prend en charge la gestion des ressources de trafic système associée aux machines virtuelles et aux services d'infrastructure, comme vSphere Fault Tolerance. Le trafic système est exclusivement associé à un hôte vSphere ESXi.

Garantie de bande passante pour le trafic système

Network I/O Control version 3 provisionne les adaptateurs réseau des machines virtuelles en bande passante en utilisant les parts et les valeurs de réservation et de limite définis. Ces constructions peuvent être définies dans l'interface utilisateur NSX-T Data Center Manager. La réservation de bande passante du trafic de machine virtuelle s'utilise également dans le contrôle d'admission. Lorsque vous mettez sous tension une machine virtuelle, l'utilitaire de contrôle d'admission vérifie que suffisamment de bande passante est disponible avant de placer une machine virtuelle sur un hôte capable de fournir la capacité nécessaire en ressources.

Allocation de bande passante pour le trafic système

Vous pouvez configurer Network I/O Control de manière à allouer une certaine quantité de bande passante au trafic généré par vSphere Fault Tolerance, vSphere vMotion, des machines virtuelles, etc.

- Trafic de gestion : trafic correspondant à la gestion de l'hôte
- Trafic Fault Tolerance (FT) : trafic correspondant au basculement et à la récupération.

- Trafic NFS : trafic lié à un transfert de fichier dans le système de fichiers du réseau.
- Trafic vSAN : trafic généré par le réseau de zone de stockage virtuel.
- Trafic vMotion : trafic correspondant à la migration des ressources de calcul.
- Trafic vSphere Replication : trafic correspondant à la réplication.
- Trafic de sauvegarde vSphere Data Protection : trafic généré par la sauvegarde des données.
- Trafic de machine virtuelle : trafic généré par les machines virtuelles.
- Trafic iSCSI : trafic correspondant à Internet Small Computer System Interface.

Le serveur vCenter Server propage l'allocation à partir du Distributed Switch vers chaque adaptateur physique des hôtes qui y sont connectés.

Paramètres d'allocation de bande passante pour le trafic système

Le service Network I/O Control alloue la bande passante au trafic provenant des fonctionnalités du système vSphere de base à l'aide de plusieurs paramètres de configuration. Paramètres d'allocation pour le trafic système.

Paramètres d'allocation pour le trafic système

- **Parts** : les parts (valeur de 1 à 100) désignent la priorité relative d'un type de trafic système par rapport aux autres types actifs sur le même adaptateur physique. Les parts relatives attribuées à un type de trafic système et la quantité de données transmises par d'autres fonctionnalités du système déterminent la bande passante disponible pour ce type de trafic système.
- **Réservation** : quantité minimale de bande passante (en Mo/s) garantie sur chaque adaptateur physique. La quantité totale de bande passante réservée sur tous les types de trafic système ne peut pas dépasser 75 % de la bande passante que peut fournir l'adaptateur réseau physique de plus faible capacité. La bande passante non utilisée est mise à disposition des autres types de trafic système. Toutefois, Network I/O Control ne redistribue pas la capacité non utilisée par le trafic système au placement des machines virtuelles.
- **Limite** : quantité maximale de bande passante (en Mo/s ou Go/s) qu'un type de trafic système peut consommer sur chaque adaptateur physique.

Note Vous ne pouvez pas réserver plus de 75 pour cent de la bande passante d'un adaptateur réseau physique. Par exemple, si les adaptateurs réseau connectés à un hôte ESXi sont des adaptateurs 10 GbE, vous pouvez allouer uniquement 7,5 Gbits/s de bande passante aux différents types de trafic. Vous pouvez conserver davantage de capacité non utilisée. L'hôte peut allouer la bande passante non utilisée dynamiquement en fonction des parts, des limites et de l'utilisation. L'hôte ne réserve que la bande passante suffisante pour l'opération d'une fonctionnalité système.

Configurer Network I/O Control et l'allocation de bande passante pour le trafic système sur un commutateur N-VDS

Pour garantir la bande passante minimale pour le trafic système en cours d'exécution sur les hôtes NSX-T, activez et configurez la gestion des ressources réseau sur un Distributed Switch NSX-T.

Procédure

- 1 Connectez-vous à NSX Manager Manager (<https://<nsx-manager-IP-address>>).
- 2 Accédez à **Infrastructure > Profils**.
- 3 Sélectionnez **Profils NIOC**.
- 4 Cliquez sur **+ AJOUTER**.
- 5 Dans l'écran Nouveau profil NIOC, entrez les détails requis.
 - a Entrez un nom pour le profil NIOC.
 - b Définissez l'état sur **Activé**.
 - c Dans la section consacrée aux ressources allouées au trafic de l'infrastructure hôte, sélectionnez un type de trafic et entrez des valeurs pour la limite, les parts et la réservation.
- 6 Cliquez sur **Ajouter**.

Un nouveau profil NIOC est ajouté à la liste des profils NIOC.

Configurer Network I/O Control et l'allocation de bande passante pour le trafic système sur un commutateur N-VDS en utilisant des API

Utilisez des API NSX-T Data Center pour configurer le réseau et la bande passante pour les applications en cours d'exécution sur l'hôte.

Procédure

- 1 Interrogez l'hôte pour afficher les deux profils de commutateur d'hôte définis par le système et définis par l'utilisateur.
- 2 GET https://<nsx-mgr>/api/v1/host-switch-profiles?include_system_owned=true.

Dans l'exemple de réponse ci-dessous, le profil NIOC appliqué à l'hôte est affiché.

```
{
  "description": "This profile is created for Network I/O Control (NIOC).",
  "extends": {
    "$ref": "BaseHostSwitchProfile"+
  },
  "id": "NiocProfile",
  "module_id": "NiocProfile",
  "polymorphic-type-descriptor": {
    "type-identifier": "NiocProfile"
```

```

},
"properties": {
  "_create_time": {
    "$ref": "EpochMsTimestamp"+,
    "can_sort": true,
    "description": "Timestamp of resource creation",
    "readonly": true
  },
  "_create_user": {
    "description": "ID of the user who created this resource",
    "readonly": true,
    "type": "string"
  },
  "_last_modified_time": {
    "$ref": "EpochMsTimestamp"+,
    "can_sort": true,
    "description": "Timestamp of last modification",
    "readonly": true
  },
  "_last_modified_user": {
    "description": "ID of the user who last modified this resource",
    "readonly": true,
    "type": "string"
  },
  "_links": {
    "description": "The server will populate this field when returning the resource. Ignored on PUT
and POST.",
    "items": {
      "$ref": "ResourceLink"+
    },
    "readonly": true,
    "title": "References related to this resource",
    "type": "array"
  },
  "_protection": {
    "description": "Protection status is one of the following:
      PROTECTED – the client who retrieved the entity is not allowed to modify it.
      NOT_PROTECTED – the client who retrieved the entity is allowed to modify it
      REQUIRE_OVERRIDE – the client who retrieved the entity is a super user and can modify it,
      but only when providing the request header X-Allow-Overwrite=true.
      UNKNOWN – the _protection field could not be determined for this entity.",
    "readonly": true,
    "title": "Indicates protection status of this resource",
    "type": "string"
  },
  "_revision": {
    "description": "The _revision property describes the current revision of the resource.
      To prevent clients from overwriting each other's changes, PUT operations must include the
      current _revision of the resource,
      which clients should obtain by issuing a GET operation.
      If the _revision provided in a PUT request is missing or stale, the operation will

```

```

be rejected.",
  "readonly": true,
  "title": "Generation of this resource config",
  "type": "int"
},

"_schema": {
  "readonly": true,
  "title": "Schema for this resource",
  "type": "string"
},

"_self": {
  "$ref": "SelfResourceLink+",
  "readonly": true,
  "title": "Link to this resource"
},

"_system_owned": {
  "description": "Indicates system owned resource",
  "readonly": true,
  "type": "boolean"
},

"description": {
  "can_sort": true,
  "maxLength": 1024,
  "title": "Description of this resource",
  "type": "string"
},

"display_name": {
  "can_sort": true,
  "description": "Defaults to ID if not set",
  "maxLength": 255,
  "title": "Identifier to use when displaying entity in logs or GUI",
  "type": "string"
},

"enabled": {
  "default": true,
  "description": "The enabled property specifies the status of NIOC feature.

When enabled is set to true, NIOC feature is turned on and the bandwidth allocations
  specified for the traffic resources are enforced.
When enabled is set to false, NIOC feature is turned off and no bandwidth allocation is
  guaranteed.

By default, enabled will be set to true.",
  "nsx_feature": "Nioc",
  "required": false,
  "title": "Enabled status of NIOC feature",
  "type": "boolean"
},

```

```

    "host_infra_traffic_res": {
      "description": "host_infra_traffic_res specifies bandwidth allocation for various traffic
resources.",
      "items": {
        "$ref": "ResourceAllocation"+
      },
      "nsx_feature": "Nioc",
      "required": false,
      "title": "Resource allocation associated with NiocProfile",
      "type": "array"
    },

    "id": {
      "can_sort": true,
      "readonly": true,
      "title": "Unique identifier of this resource",
      "type": "string"
    },

    "required_capabilities": {
      "help_summary":
        "List of capabilities required on the fabric node if this profile is
used.
        The required capabilities is determined by whether specific features are enabled in the
profile.",
      "items": {
        "type": "string"
      },
      "readonly": true,
      "required": false,
      "type": "array"
    },

    "resource_type": {
      "$ref": "HostSwitchProfileType"+,
      "required": true
    },

    "tags": {
      "items": {
        "$ref": "Tag"+
      },
    },

    "maxItems": 30,
    "title": "Opaque identifiers meaningful to the API user",
    "type": "array"
  }
},
"title": "Profile for Nioc",
"type": "object"
}

```

3 Si un profil NIOC n'existe pas, créez-en un.

POST <https://<nsx-mgr>/api/v1/host-switch-profiles>

```
{
  "description": "Specify limit, shares and reservation for all kinds of traffic.
  Values for limit and reservation are expressed in percentage. And for shares,
  the value is expressed as a number between 1-100.\n\nThe overall reservation among all traffic
  types should not exceed 75%.
  Otherwise, the API request will be rejected.",

  "id": "ResourceAllocation",
  "module_id": "NiocProfile",
  "nsx_feature": "Nioc",
  "properties": {
    "limit": {
      "default": -1.0,
      "description": "The limit property specifies the maximum bandwidth allocation for a given
      traffic type and is expressed in percentage. The default value for this
      field is set to -1 which means the traffic is unbounded for the traffic
      type. All other negative values for this property is not supported\nand will be rejected by
      the API.",
      "maximum": 100,
      "minimum": -1,
      "required": true,
      "title": "Maximum bandwidth percentage",
      "type": "number"
    },

    "reservation": {
      "default": 0.0,
      "maximum": 75,
      "minimum": 0,
      "required": true,
      "title": "Minimum guaranteed bandwidth percentage",
      "type": "number"
    },

    "shares": {
      "default": 50,
      "maximum": 100,
      "minimum": 1,
      "required": true,
      "title": "Shares",
      "type": "int"
    },

    "traffic_type": {
      "$ref": "HostInfraTrafficType+",
      "required": true,
      "title": "Resource allocation traffic type"
    }
  }
}
```

```

},

"title": "Resource allocation information for a host infrastructure traffic type",
"type": "object"

```

- 4 Mettez à jour la configuration du nœud de transport avec l'ID de profil NIOC du profil NIOC récemment créé.

PUT <https://<nsx-mgr>/api/v1/transport-nodes/<TN-id>>

```

{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  "display_name": "NSX Configured TN",
  "host_switch_spec": {
    "resource_type": "StandardHostSwitchSpec",
    "host_switches": [
      {
        "host_switch_profile_ids": [
          {
            "value": "e331116d-f59e-4004-8cfd-c577aefe563a",
            "key": "UplinkHostSwitchProfile"
          },
          {
            "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
            "key": "LldpHostSwitchProfile"
          },
          {
            "value": "b0185099-8003-4678-b86f-edd47ca2c9ad",
            "key": "NiocProfile"
          }
        ],
        "host_switch_name": "nsxvswitch",
        "pnics": [
          {
            "device_name": "vmnic1",
            "uplink_name": "uplink1"
          }
        ],
        "ip_assignment_spec": {
          "resource_type": "StaticIpPoolSpec",
          "ip_pool_id": "ecddcdde-4dc5-4026-ad4f-8857995d4c92"
        }
      }
    ],
  },
  "transport_zone_endpoints": [
    {
      "transport_zone_id": "e14c6b8a-9edd-489f-b624-f9ef12afbd8f",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ]
    }
  ]
}

```

```

    }
  ]
}
],

"host_switches": [
{
  "host_switch_profile_ids": [
    {
      "value": "e331116d-f59e-4004-8cfd-c577aefe563a",
      "key": "UplinkHostSwitchProfile"
    },
    {
      "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
      "key": "LldpHostSwitchProfile"
    }
  ],
  "host_switch_name": "nsxvswitch",
  "pnics": [
    {
      "device_name": "vmnic1",
      "uplink_name": "uplink1"
    }
  ],
  "static_ip_pool_id": "ecddcdde-4dc5-4026-ad4f-8857995d4c92"
}
],
"node_id": "41a4eebd-d6b9-11e6-b722-875041b9955d",
"_revision": 0
}

```

- 5 Vérifiez que les paramètres du profil NIOC sont mis à jour dans la section `com.vmware.common.respools.cfg`.

```
# [root@ host:] net-dvs -l
```

```

switch 1d 73 f5 58 99 7a 46 6a-9c cc d0 93 17 bb 2a 48 (vswitch)
max ports: 2560
global properties:

com.vmware.common.opaqueDvs = true ,      propType = CONFIG
com.vmware.nsx.kcp.enable = true ,        propType = CONFIG
com.vmware.common.alias = nsxvswitch ,    propType = CONFIG
com.vmware.common.uplinkPorts: uplink1    propType = CONFIG
com.vmware.common.portset.mtu = 1600, propType = CONFIG
com.vmware.etherswitch.cdp = LLDP, listen propType = CONFIG
com.vmware.common.respools.version = version3, propType = CONFIG
com.vmware.common.respools.cfg:
netsched.pools.persist.ft:0:50:-1:255
netsched.pools.persist.hbr:0:50:-1:255
netsched.pools.persist.vmotion:0:50:-1:255
netsched.pools.persist.vm:0:100:-1:255
netsched.pools.persist.iscsi:0:50:-1:255

```

```

netsched.pools.persist.nfs:0:50:-1:255
netsched.pools.persist.mgmt:0:50:-1:255
netsched.pools.persist.vdp:0:50:-1:255
netsched.pools.persist.vsan:0:50:-1:255
propType = CONFIG

```

6 Vérifiez les profils NIOC dans le noyau de l'hôte.

```
# [root@ host:] /get /net/portsets/DvsPortset-1/ports/50335755/niocVnicInfo
```

```

Vnic NIOC Info
{
  Uplink reserved on:vmnic4
  Reservation in Mbps:200
  Shares:50
  Limit in Mbps:4294967295
  World ID:1001400726
  vNIC Index:0
  Respool Tag:0
  NIOC Version:3
  Active Uplink Bit Map:15
  Parent Respool ID:netsched.pools.persist.vm
}

```

7 # [root@ host:] /get /net/portsets/DvsPortset-1/uplinks/vmnic4/niocInfo

```

Uplink NIOC Info
{
  Uplink device:vmnic4
  Link Capacity in Mbps:750
  vm respool reservation:275
  link status:1
  NetSched Ready:1
  Infrastructure reservation:0
  Total VM reservation:200
  Total vnics on this uplink:1
  NIOC Version:3
  Uplink index in BitMap:0
}

```

Le profil NIOC est configuré avec une allocation de bande passante prédéfinie pour les applications qui s'exécutent sur des hôtes NSX-T Data Center.

Créer un nœud de transport NSX Edge

Un nœud de transport est un nœud capable de participer à une superposition NSX-T Data Center ou à une mise en réseau VLAN NSX-T Data Center. Tout nœud peut servir de nœud de transport s'il contient un N-VDS. Ces nœuds comprennent, mais sans s'y limiter, les dispositifs NSX Edge. Cette procédure indique comment ajouter un dispositif NSX Edge en tant que nœud de transport.

Un dispositif NSX Edge peut appartenir à une zone de transport de superposition et à plusieurs zones de transport VLAN. Si une machine virtuelle a besoin d'accéder au monde extérieur, le dispositif NSX Edge doit appartenir à la même zone de transport que le commutateur logique de la machine virtuelle. Généralement, le dispositif NSX Edge appartient à au moins une zone de transport VLAN pour fournir l'accès en liaison montante.

Note Si vous prévoyez de créer des nœuds de transport à partir d'une machine virtuelle modèle, assurez-vous qu'il n'existe aucun certificat sur l'hôte dans `/etc/vmware/nsx/`. L'agent netcpa ne crée pas de nouveau certificat s'il en existe déjà un.

Conditions préalables

- Le dispositif NSX Edge doit être relié au plan de gestion et la connectivité MPA doit être activée sur la page **Infrastructure > Dispositifs Edge**. Reportez-vous à la section [Relier NSX Edge au plan de gestion](#).
- Des zones de transport doivent être configurées.
- Un profil de liaison montante doit être configuré ou vous pouvez utiliser le profil de liaison par défaut pour les nœuds de dispositifs NSX Edge bare-metal.
- Un pool d'adresses IP doit être configuré et doit être disponible dans le déploiement réseau.
- Au moins une carte réseau physique non utilisée doit être disponible sur le nœud hôte ou sur le nœud NSX Edge.

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Infrastructure > Nœuds > Nœuds de transport > Ajouter**.
- 3 Tapez un nom pour le nœud de transport NSX Edge.
- 4 Sélectionnez un nœud d'infrastructure NSX Edge dans la liste déroulante.
- 5 Sélectionnez les zones de transport appartenant à ce nœud de transport.

Un nœud de transport NSX Edge appartient à au moins deux zones de transport : une zone de superposition pour la connectivité NSX-T Data Center et une zone VLAN pour la connectivité en liaison montante.

- 6 Cliquez sur l'onglet **N-VDS** et fournissez les informations VDS-N.

Option	Description
Nom du N-VDS	Il doit correspondre aux noms que vous avez configurés lorsque vous avez créé les zones de transport.
Profil de liaison montante	Sélectionnez le profil de liaison montante dans le menu déroulant. Les liaisons montantes disponibles dépendent de la configuration du profil de liaison montante sélectionné.

Option	Description
Attribution IP	Sélectionnez Utiliser le pool IP ou Utiliser la liste d'adresses IP statiques pour le N-VDS de superposition. Si vous sélectionnez Utiliser la liste d'adresses IP statiques , vous devez spécifier une liste d'adresses IP séparées par des virgules, une passerelle et un masque de sous-réseau.
Pool IP	Si vous avez sélectionné l'option Utiliser le pool IP pour l'attribution d'adresse IP, spécifiez le nom du pool d'adresses IP.
Cartes réseau physiques	Contrairement à un nœud de transport hôte qui utilise vmnicX comme carte réseau physique, un nœud de transport NSX Edge utilise fp-ethX.

- 7 (Facultatif) Affichez le nœud de transport à l'aide de l'appel d'API GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>`.

```
GET https://<nsx-mgr>/api/v1/transport-nodes/78a03020-a3db-44c4-a8fa-f68ad4be6a0c
```

```
{
  "resource_type": "TransportNode",
  "id": "78a03020-a3db-44c4-a8fa-f68ad4be6a0c",
  "display_name": "node-comp-01b",
  "transport_zone_endpoints": [
    {
      "transport_zone_id": "efd7f38f-c5da-437d-af03-ac598f82a9ec",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ]
    }
  ],
  "host_switches": [
    {
      "host_switch_profile_ids": [
        {
          "value": "8abdb6c0-db83-4e69-8b99-6cd85bfcc61d",
          "key": "UplinkHostSwitchProfile"
        },
        {
          "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
          "key": "LldpHostSwitchProfile"
        }
      ]
    },
    {
      "host_switch_name": "overlay-hostswitch",
      "pnics": [
        {
          "device_name": "vmnic1",
          "uplink_name": "uplink-1"
        }
      ]
    },
    {
      "static_ip_pool_id": "c78ac522-2a50-43fe-816a-c459a210127e"
    }
  ],
}
```

```

    "node_id": "c551290a-f682-11e5-ae84-9f8726e1de65",
    "_create_time": 1459547122893,
    "_last_modified_user": "admin",
    "_last_modified_time": 1459547126740,
    "_create_user": "admin",
    "_revision": 1
  }

```

- 8 (Facultatif) Pour obtenir des informations sur l'état, utilisez l'appel d'API GET <https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/status>.

```

{
  "control_connection_status": {
    "degraded_count": 0,
    "down_count": 0,
    "up_count": 1,
    "status": "UP"
  },
  "tunnel_status": {
    "down_count": 0,
    "up_count": 0,
    "status": "UNKNOWN",
    "bfd_status": {
      "bfd_admin_down_count": 0,
      "bfd_up_count": 0,
      "bfd_init_count": 0,
      "bfd_down_count": 0
    },
  },
  "bfd_diagnostic": {
    "echo_function_failed_count": 0,
    "no_diagnostic_count": 0,
    "path_down_count": 0,
    "administratively_down_count": 0,
    "control_detection_time_expired_count": 0,
    "forwarding_plane_reset_count": 0,
    "reverse_concatenated_path_down_count": 0,
    "neighbor_signaled_session_down_count": 0,
    "concatenated_path_down_count": 0
  },
  },
  "pnic_status": {
    "degraded_count": 0,
    "down_count": 0,
    "up_count": 4,
    "status": "UP"
  },
  },
  "mgmt_connection_status": "UP",
  "node_uuid": "cd4a8501-0ffc-44cf-99cd-55980d3d8aa6",
  "status": "UNKNOWN"
}

```

Étape suivante

Ajoutez le nœud NSX Edge à un cluster NSX Edge. Reportez-vous à la section [Créer un cluster NSX Edge](#).

Créer un cluster NSX Edge

Un cluster multinœud de dispositifs NSX Edge contribue à garantir qu'au moins un dispositif NSX Edge est toujours disponible. Pour créer un routeur logique de niveau 0 ou un routeur de niveau 1 avec les services avec état tels que NAT, l'équilibrage de charge, etc. vous devez l'associer à un cluster NSX Edge. Ainsi, même si vous avez uniquement un dispositif NSX Edge, celui-ci doit tout de même appartenir à un cluster NSX Edge pour avoir une utilité.

Un nœud de transport NSX Edge peut uniquement être ajouté à un cluster NSX Edge.

Un cluster NSX Edge peut être utilisé pour soutenir plusieurs routeurs logiques.

Après sa création, le cluster NSX Edge peut être modifié en ajoutant d'autres dispositifs NSX Edge.

Conditions préalables

- Installez au moins un nœud NSX Edge.
- Reliez les dispositifs NSX Edge au plan de gestion.
- Ajoutez les dispositifs NSX Edge en tant que nœuds de transport.
- Éventuellement, créez un profil de cluster NSX Edge pour la haute disponibilité (HA) dans **Infrastructure > Profils > Profils de cluster Edge**. Vous pouvez également utiliser le profil de cluster par défaut NSX Edge.

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Accédez à **Infrastructure > Nœuds > Clusters Edge > Ajouter**.
- 3 Entrez un nom pour le cluster NSX Edge.
- 4 Sélectionnez un profil de cluster NSX Edge.

- 5 Cliquez sur **Modifier** et sélectionnez **Machine physique** ou **Machine virtuelle**.

Machine physique fait référence aux dispositifs NSX Edge qui sont installés sur un système nu.

Machine virtuelle fait référence aux dispositifs NSX Edge qui sont installés en tant que machines virtuelles/dispositifs.

- 6 Pour Machine virtuelle, sélectionnez Nœud NSX Edge ou **Nœud de passerelle de cloud public** dans le menu déroulant Type de membre.

Si la machine virtuelle est déployée dans un environnement de cloud public, sélectionnez Passerelle de cloud public, sinon sélectionnez Nœud NSX Edge.

- 7 Dans la colonne **Disponible**, sélectionnez les dispositifs NSX Edge et cliquez sur la flèche vers la droite pour les déplacer dans la colonne **Sélectionné**.

Étape suivante

Vous pouvez maintenant créer des topologies de réseau logique et configurer des services. Reportez-vous à *Guide d'administration de NSX-T Data Center*.

Installation des composants NSX Cloud

9

NSX Cloud fournit un panneau de contrôle unique pour gérer vos réseaux de cloud public.

NSX Cloud est indépendant de la mise en réseau spécifique à un fournisseur qui ne nécessite pas d'accès hyperviseur dans un cloud public.

Il offre plusieurs avantages :

- Vous pouvez développer et tester des applications en utilisant les profils de réseau et de sécurité utilisés dans l'environnement de production.
- Les développeurs peuvent gérer leurs applications jusqu'à ce qu'elles soient prêtes pour le déploiement.
- Avec la récupération d'urgence, vous pouvez vous remettre d'une panne non planifiée ou d'une menace de sécurité à votre cloud public.
- Si vous migrez vos charges de travail entre des clouds publics, NSX Cloud garantit que des stratégies de sécurité semblables sont appliquées aux machines virtuelles de charge de travail indépendamment de leur nouvel emplacement.

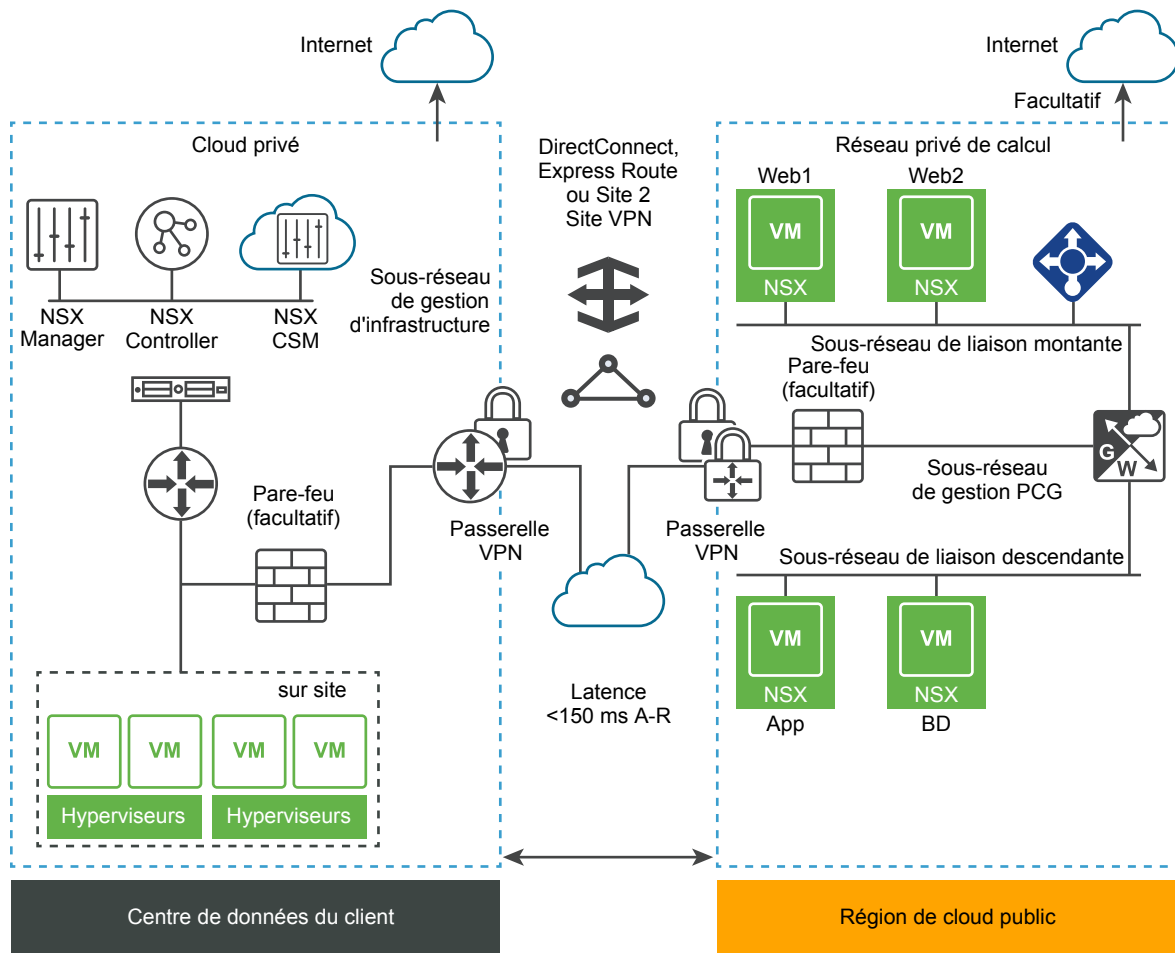
Ce chapitre contient les rubriques suivantes :

- [Architecture et composants de NSX Cloud](#)
- [Présentation de l'installation de composants NSX Cloud](#)
- [Installer CSM et se connecter à NSX Manager](#)
- [Connecter le cloud public avec déploiement sur site](#)
- [Ajouter votre compte de cloud public](#)
- [Déployer PCG](#)
- [Annuler le déploiement de PCG](#)

Architecture et composants de NSX Cloud

NSX Cloud intègre les composants principaux NSX-T Data Center, NSX Manager et NSX Controller dans votre cloud public pour fournir réseau et sécurité dans vos implémentations.

Chiffre 9-1. Architecture de NSX Cloud



Composants principaux de NSX Cloud :

- *NSX Manager* pour le plan de gestion avec un contrôle d'accès basé sur les rôles (RBAC) défini.
- *NSX Controller* pour le plan de contrôle et l'état d'exécution.
- *Cloud Service Manager* pour l'intégration à NSX Manager pour fournir des informations spécifiques au cloud public au plan de gestion.
- *NSX Public Cloud Gateway* pour la connectivité aux plans de gestion et de contrôle NSX, pour les services de passerelle NSX Edge et pour les communications basées sur API avec les entités du cloud public.
- Fonctionnalité *NSX Agent* qui fournit le chemin de données géré par NSX pour les machines virtuelles de la charge de travail.

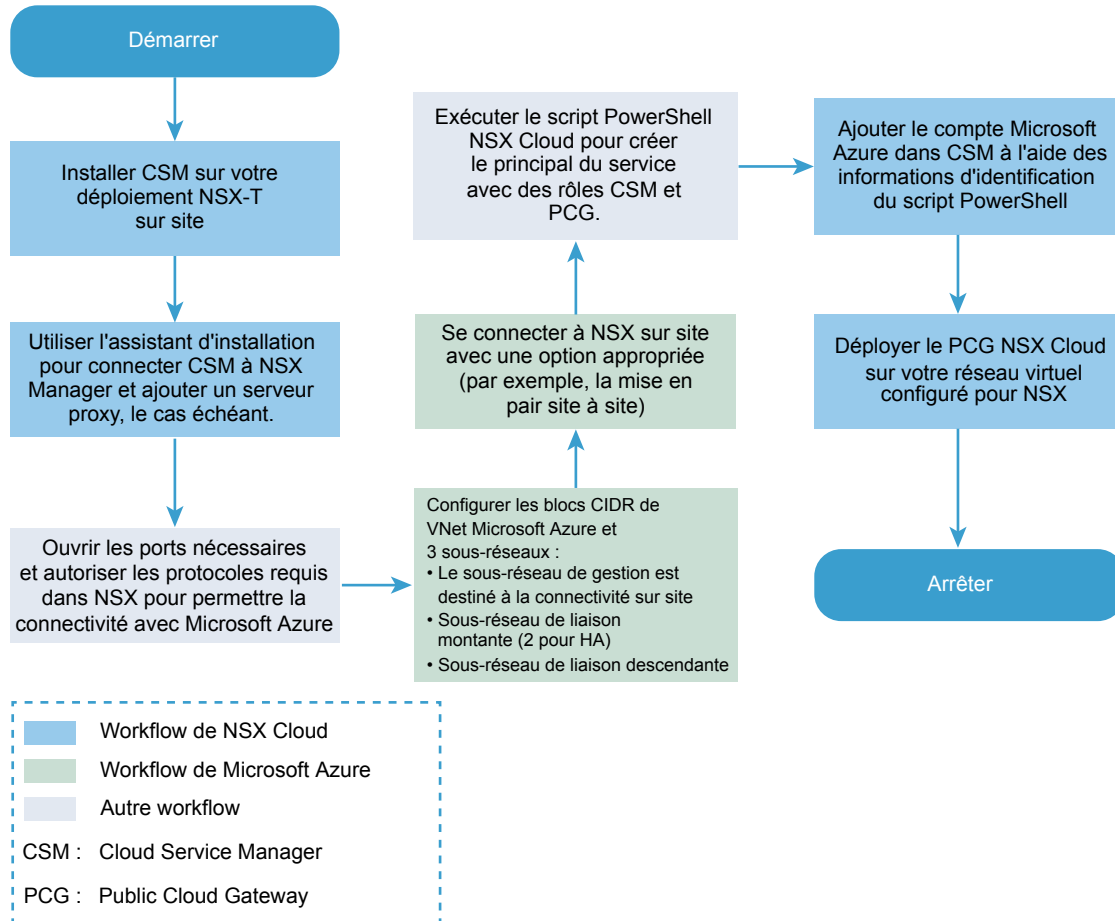
Présentation de l'installation de composants NSX Cloud

Reportez-vous à ces organigrammes afin d'obtenir un aperçu des opérations de jour 0 pour l'activation de NSX-T Data Center en vue de gérer vos machines virtuelles de charge de travail sur le cloud public.

Workflow de jour 0 pour Microsoft Azure

Cet organigramme présente un aperçu des étapes impliquées dans l'ajout d'un VNet Microsoft Azure à NSX Cloud.

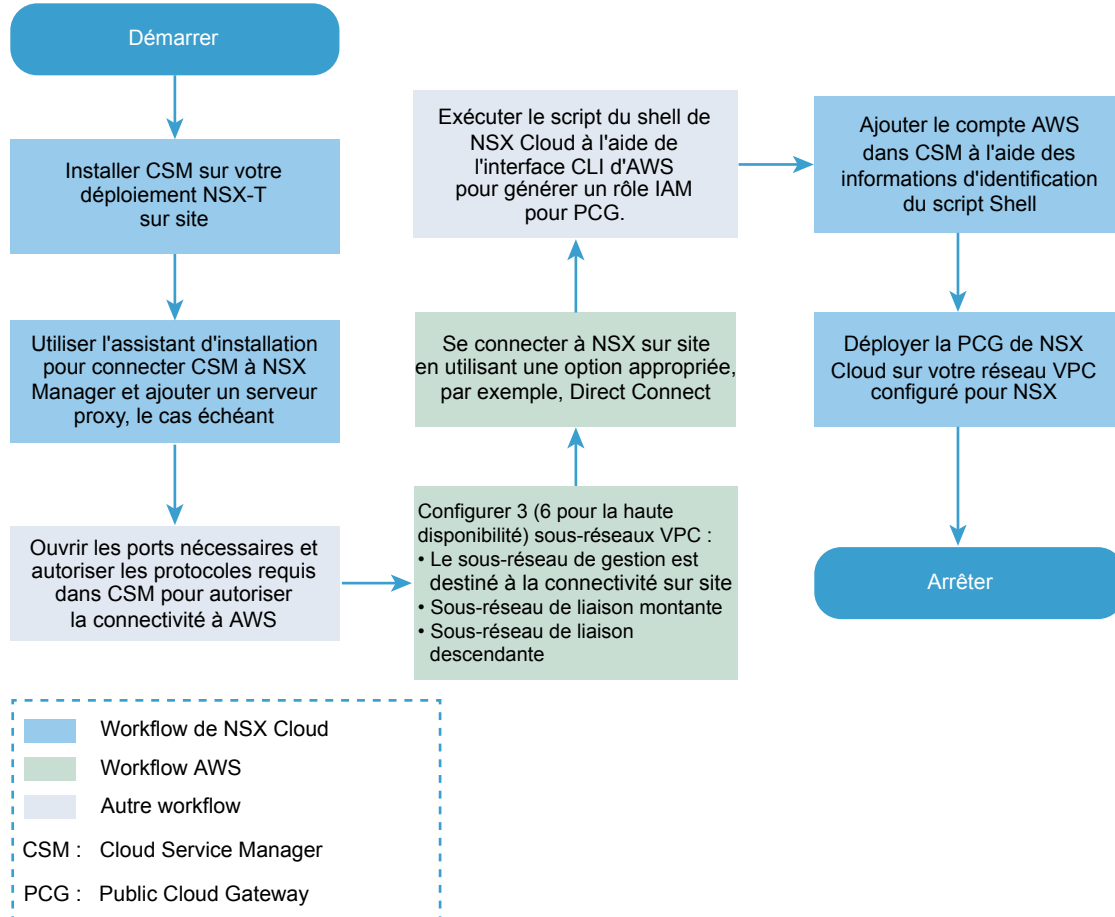
Chiffre 9-2. Workflow de jour 0 NSX Cloud pour Microsoft Azure



Workflow de jour 0 pour AWS

Cet organigramme présente un aperçu des étapes impliquées dans l'ajout d'un VPC AWS à NSX Cloud.

Chiffre 9-3. Workflow de jour 0 NSX Cloud pour AWS



Installer CSM et se connecter à NSX Manager

Utilisez l'assistant de configuration pour connecter CSM à NSX Manager et configurer des serveurs proxy, le cas échéant.

Installation de CSM

Cloud Service Manager (CSM) est un composant essentiel de NSX Cloud.

Installez CSM après avoir installé les composants principaux de NSX-T Data Center.

Reportez-vous à [Installer NSX Manager et les dispositifs disponibles](#) pour obtenir des instructions détaillées.

Publication du nom de domaine complet de NSX Manager

Après l'installation des composants principaux de NSX-T Data Center et de CSM, pour activer la fonctionnalité NAT à l'aide du nom de domaine complet, configurez les entrées de recherche et de recherche inversée sur le serveur DNS NSX-T dans votre déploiement.

Vous devez également activer la publication du nom de domaine complet du dispositif NSX Manager à l'aide de l'API NSX-T :

Exemple de demande : **PUT https://<nsx-mgr>/api/v1/configs/management**

```
{
  "publish_fqdns": true,
  "_revision": 0
}
```

Exemple de réponse :

```
{
  "publish_fqdns": true,
  "_revision": 1
}
```

Reportez-vous à *Guide de l'API de NSX-T Data Center* pour plus de détails.

Joindre CSM avec NSX Manager

Vous devez connecter le dispositif CSM à NSX Manager pour autoriser ces composants à communiquer entre eux.

Conditions préalables

- NSX Manager doit être installé et vous devez disposer des privilèges d'administrateur pour vous connecter à NSX Manager
- CSM doit être installé et vous devez disposer du rôle d'administrateur d'entreprise dans CSM.

Procédure

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

```
NSX-Manager> get certificate api thumbprint
```

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

- 3 Connectez-vous à CSM avec le rôle d'administrateur d'entreprise.

- 4 Cliquez sur **Système > Paramètres**. Puis, cliquez sur **Configurer** dans le panneau **Nœud NSX associé**.

Note Vous pouvez également fournir ces détails lors de l'utilisation de l'assistant de configuration de CSM qui est disponible lors de l'installation initiale de CSM.

- 5 Entrez les détails du dispositif NSX Manager.

Option	Description
Nom d'hôte de NSX Manager	Entrez le nom de domaine complet (FQDN) du dispositif NSX Manager, s'il est disponible. Vous pouvez également entrer l'adresse IP de NSX Manager.
Identifiants de l'administrateur	Entrez un nom d'utilisateur disposant du rôle d'administrateur d'entreprise et le mot de passe correspondant.
Empreinte numérique du responsable	Entrez la valeur de l'empreinte numérique du dispositif NSX Manager que vous avez obtenue à l'étape 2.

- 6 Cliquez sur **Connecter**.

CSM vérifie l'empreinte numérique du dispositif NSX Manager et établit la connexion.

(Facultatif) Configurer les serveurs Proxy

Si vous souhaitez router et surveiller l'ensemble du trafic HTTP/HTTPS dédié à Internet via un proxy HTTP fiable, vous pouvez configurer jusqu'à cinq serveurs proxy dans CSM.

Toutes les communications du cloud public depuis PCG et CSM sont acheminées via le serveur proxy sélectionné.

Les paramètres de proxy de PCG sont indépendants des paramètres de proxy de CSM. Vous pouvez choisir de n'avoir aucun serveur proxy ou un serveur proxy différent pour PCG.

Vous pouvez choisir les niveaux d'authentification suivants :

- Authentification par informations d'identification.
- Authentification par certificat pour l'interception HTTPS.
- Aucune authentification.

Procédure

- 1 Cliquez sur **Système > Paramètres**. Puis, cliquez sur **Configurer** sur le panneau **Serveurs proxy**.

Note Vous pouvez également fournir ces détails lors de l'utilisation de l'assistant de configuration de CSM qui est disponible lors de l'installation initiale de CSM.

- 2 Dans l'écran Configurer les serveurs proxy, entrez les informations suivantes :

Option	Description
Par défaut	Utilisez cette case d'option pour indiquer le serveur proxy par défaut.
Nom du profil	Fournissez un nom de profil de serveur proxy. Cette information est obligatoire.

Option	Description
Serveur proxy	Entrez l'adresse IP du serveur proxy. Cette information est obligatoire.
Port	Entrez le port du serveur proxy. Cette information est obligatoire.
Authentification	Facultative. Si vous souhaitez configurer une authentification supplémentaire, cochez cette case et fournissez un nom d'utilisateur et un mot de passe valides.
Nom d'utilisateur	Ceci est nécessaire si vous cochez la case Authentification.
Mot de passe	Ceci est nécessaire si vous cochez la case Authentification.
Certificat	Facultative. Si vous souhaitez fournir un certificat d'authentification pour l'interception HTTPS, cochez cette case et copiez-collez le certificat dans la zone de texte qui s'affiche.
Aucun proxy	Sélectionnez cette option si vous ne souhaitez utiliser aucun des serveurs proxy configurés.

Connecter le cloud public avec déploiement sur site

Vous devez utiliser des options de connectivité adaptées pour connecter votre déploiement sur site à vos comptes ou abonnements de cloud public .

Activer l'accès aux ports et protocoles sur CSM pour la connectivité hybride

Ouvrez les ports réseau nécessaires et autorisez les protocoles requis dans NSX Manager pour activer la connectivité de cloud public.

Autoriser l'accès à NSX Manager depuis le cloud public

Ouvrez les ports réseau et les protocoles suivants pour activer la connectivité avec votre déploiement de NSX Manager sur site :

Tableau 9-1.

De	Vers	Protocole/Port	Description
PCG	NSX Manager	TCP/5671	Trafic entrant du cloud public vers le NSX-T Data Center sur site pour la communication du plan de gestion.
PCG	NSX Manager	TCP/8080	Trafic entrant du cloud public vers le NSX-T Data Center sur site pour la mise à niveau.
PCG	NSX Controller	TCP/1234, TCP/1235	Trafic entrant du cloud public vers le NSX-T Data Center sur site pour la Communication du plan de contrôle.

Tableau 9-1. (Suite)

De	Vers	Protocole/Port	Description
PCG	DNS	UDP/53	Trafic entrant du cloud public vers le DNS du NSX-T Data Center sur site (si vous utilisez le serveur DNS sur site).
CSM	PCG	TCP/7442	Transfert de configuration CSM
Quelconque	NSX Manager	TCP/443	Interface utilisateur NSX Manager
Quelconque	CSM	TCP/443	Interface utilisateur CSM

Important Toutes les communications de l'infrastructure NSX-T Data Center tirent parti du chiffrement basé sur SSL. Assurez-vous que le pare-feu autorise le trafic SSL sur les ports non standard.

Connecter votre réseau Microsoft Azure à votre déploiement NSX-T Data Center sur site

Une connexion doit être établie entre votre réseau Microsoft Azure et vos dispositifs NSX-T Data Center sur site.

Note Vous devez avoir déjà installé et connecté NSX Manager avec CSM dans votre déploiement sur site.

Présentation

- Connectez votre abonnement Microsoft Azure à l'instance de NSX-T Data Center sur site.
- Configurez vos VNet avec les blocs CIDR nécessaires et les sous-réseaux requis par NSX Cloud.
- Synchronisez l'heure du dispositif CSM avec le serveur de stockage Microsoft Azure ou NTP.

Connecter votre abonnement Microsoft Azure à l'instance de NSX-T Data Center sur site

Chaque cloud public fournit des options pour établir une connexion avec un déploiement sur site. Vous pouvez sélectionner l'une des options de connectivité disponibles qui répond le mieux à vos besoins. Pour plus d'informations, reportez-vous à la [documentation de référence de Microsoft Azure](#).

Note Vous devez examiner et implémenter les considérations de sécurité applicables et les meilleures pratiques de Microsoft Azure. Par exemple, l'authentification à plusieurs facteurs (MFA) doit être activée sur tous les comptes d'utilisateurs privilégiés qui accèdent au portail ou à l'API Microsoft Azure. MFA garantit que seul un utilisateur légitime peut accéder au portail et réduit le risque d'accès, même si les informations d'identification sont volées ou divulguées. Pour plus d'informations et de recommandations, reportez-vous à la [Documentation du centre de sécurité Azure](#).

Configurer votre VNet

Dans Microsoft Azure, créez des blocs CIDR routables et configurez les sous-réseaux requis.

- Un sous-réseau de gestion avec une plage recommandée d'au moins /28 pour gérer :
 - Le trafic de contrôle vers les dispositifs sur site
 - Le trafic d'API vers les points de terminaison d'API de fournisseur de cloud
- Un sous-réseau de liaison descendante avec une plage recommandée de /24 pour les VM de charge de travail.
- Un ou deux sous-réseaux de liaison montante pour la HA avec une plage recommandée de /24 pour le routage du trafic nord-sud en provenance de, ou à destination du, réseau virtuel.

Connecter votre réseau AWS (Amazon Web Services) à votre déploiement NSX-T Data Center sur site

Une connexion doit être établie entre votre réseau AWS (Amazon Web Services) et vos dispositifs NSX-T Data Center sur site.

Note Vous devez avoir déjà installé et connecté NSX Manager avec CSM dans votre déploiement sur site.

Présentation

- Connectez votre compte AWS à des dispositifs NSX Manager sur site en utilisant l'une des options disponibles répondant le mieux à vos besoins.
- Configurez votre VPC avec des sous-réseaux et en respectant d'autres conditions pour NSX Cloud.

Connectez votre compte AWS à votre déploiement de NSX-T Data Center sur site.

Chaque cloud public fournit des options pour établir une connexion avec un déploiement sur site. Vous pouvez sélectionner l'une des options de connectivité disponibles qui répond le mieux à vos besoins. Pour plus d'informations, reportez-vous à la [documentation de référence AWS](#).

Note Vous devez examiner et mettre en œuvre les éléments à prendre en compte pour la sécurité applicables et les meilleures pratiques AWS ; reportez-vous à [Meilleures pratiques de sécurité AWS](#).

Configurer votre VPC

Vous avez besoin des configurations suivantes :

- six sous-réseaux pour la prise en charge de PCG avec High Availability (HA) ;
- une passerelle Internet (IGW) ;
- une table de routage privée et une table de routage publique ;
- association de sous-réseau avec tables de routage ;
- résolution DNS et noms d'hôtes DNS activés.

Suivez ces directives pour configurer votre VPC :

- 1 En partant du principe que votre VPC utilise un réseau /16, pour chaque passerelle à déployer, configurez trois sous-réseaux.

Important Si vous utilisez High Availability, configurez trois sous-réseaux supplémentaires dans une autre zone de disponibilité.

- **Sous-réseau de gestion** : ce sous-réseau est utilisé pour le trafic de gestion entre NSX-T Data Center et PCG sur site. La plage recommandée est /28.
- **Sous-réseau de liaison montante** : ce sous-réseau est utilisé pour le trafic internet nord-sud. La plage recommandée est /24.
- **Sous-réseau de liaison descendante** : ce sous-réseau englobe la plage d'adresses IP des machines virtuelles de charge de travail et doit être dimensionné en conséquence. Gardez à l'esprit que vous devrez peut-être incorporer des interfaces supplémentaires sur les machines virtuelles de charge de travail à des fins de débogage.

Note Étiquetez les sous-réseaux correctement, par exemple, **sous-réseau de gestion**, **sous-réseau de liaison montante**, **sous-réseau de liaison descendante**, car vous devrez sélectionner les sous-réseaux lors du déploiement de PCG sur ce VPC.

- 2 Assurez-vous que vous disposez d'une passerelle Internet (IGW) rattachée à ce VPC.
- 3 Pour la table de routage du VPC, assurez-vous que **Destination** est définie sur **0.0.0.0/0** et que la **Cible** est la passerelle Internet (IGW) associée au VPC.
- 4 Assurez-vous que vous disposez d'une résolution DNS et de noms d'hôte DNS activés pour ce VPC.

Ajouter votre compte de cloud public

Pour ajouter votre inventaire de cloud public, vous devez créer des rôles dans votre cloud public pour autoriser l'accès à NSX Cloud et ajouter les informations requises dans CSM.

Activer CSM pour accéder à votre inventaire de Microsoft Azure

Votre abonnement Microsoft Azure contient un ou plusieurs VNet que vous souhaitez inclure dans la gestion de NSX-T Data Center.

Note Si vous avez déjà ajouté un compte AWS à CSM, mettez à jour la valeur MTU dans **NSX Manager > Infrastructure > Profils > Profils de liaison montante > PCG-Uplink-HostSwitch-Profile** à 1 500 avant d'ajouter le compte Microsoft Azure. Cela peut également être effectué à l'aide d'API REST NSX Manager.

Pour que NSX Cloud puisse fonctionner dans votre abonnement, vous devez créer un nouveau principal du service afin d'accorder l'accès nécessaire à NSX-T Data Center. Vous devez également créer des rôles MSI pour CSM et PCG.

NSX Cloud fournit un script PowerShell qui permet de générer le principal du service.

Il s'agit d'un processus en deux étapes :

- 1 Utilisez le script PowerShell NSX Cloud :
 - Créez un compte de principal du service pour NSX Cloud.
 - Créez un rôle pour CSM et associez-le au principal du service.
 - Créez un rôle pour PCG et associez-le au principal du service.
- 2 Ajoutez l'abonnement Microsoft Azure dans CSM.

Générer les rôles requis

NSX Cloud utilise la fonctionnalité MSI (Managed Service Identity) de Microsoft Azure pour gérer l'authentification tout en maintenant sécurisées vos informations d'identification Microsoft.

Pour que NSX Cloud fonctionne dans votre abonnement Microsoft Azure, vous devez générer des rôles MSI pour CSM et PCG, et un principal du service pour NSX Cloud.

Cela est possible en exécutant le script PowerShell NSX Cloud. En outre, vous avez besoin de deux fichiers au format JSON comme paramètres. Lorsque vous exécutez le script PowerShell avec les paramètres requis, les constructions suivantes sont créées :

- une application Azure AD pour NSX Cloud.
- un principal du service Azure Resource Manager pour l'application NSX Cloud.
- un rôle pour CSM associé au compte du principal du service.

- un rôle pour PCG afin de lui permettre de travailler sur votre inventaire de cloud public.

Note Le temps de réponse de Microsoft Azure peut provoquer l'échec du script lorsque vous l'exécutez la première fois. Si le script échoue, essayez de l'exécuter à nouveau.

Conditions préalables

- Vous devez disposer de PowerShell 5.0 et versions ultérieures avec le module AzureRM installé.
- Vous devez être le propriétaire de l'abonnement Microsoft Azure pour lequel vous souhaitez exécuter le script afin de générer le principal du service NSX Cloud.

Procédure

- 1 Sur un poste de travail ou serveur Windows, téléchargez le fichier ZIP nommé `CreateNSXCloudCredentials.zip` depuis NSX-T Data Center **Page de téléchargement > Pilotes et outils > Scripts NSX Cloud > Microsoft Azure**.
- 2 Extrayez le contenu suivant du fichier ZIP dans votre système Windows :

Nom du fichier	Description
<code>CreateNSXRoles.ps1</code>	Il s'agit du script PowerShell permettant de générer les rôles principal du service et MSI NSX Cloud pour CSM et PCG
<code>nsx_csm_role.json</code>	Ce fichier contient le nom du rôle CSM et les autorisations de ce rôle dans Microsoft Azure. Cette entrée dans le script PowerShell doit se trouver dans le même dossier que le script.
<code>nsx_pcg_role.json</code>	Ce fichier contient le nom du rôle PCG et les autorisations de ce rôle dans Microsoft Azure. Cette entrée dans le script PowerShell doit se trouver dans le même dossier que le script. Le nom du rôle PCG (passerelle) par défaut est <code>nsx-pcg-role</code> .

Note Si vous créez des rôles pour plusieurs abonnements dans votre annuaire Active Directory de Microsoft Azure, vous devez modifier les noms de rôle CSM et PCG pour chaque abonnement dans les fichiers JSON respectifs et exécuter à nouveau le script.

- 3 Exécutez le script avec votre ID d'abonnement Microsoft Azure en tant que paramètre. Le nom du paramètre est `subscriptionId`.

Par exemple,

```
.\CreateNSXRoles.ps1 -subscriptionId <your_subscription_ID>
```

Cela crée un principal du service pour NSX Cloud, un rôle disposant des privilèges appropriés pour CSM et PCG, et associe les rôles CSM et PCG au principal du service de NSX Cloud.

- 4 Recherchez un fichier dans le répertoire où vous avez exécuté le script PowerShell. Il porte un nom semblable à :
`NSXCloud_ServicePrincipal_<votre_ID_abonnement>_<nom_principal_du_service_NSX_Cloud>`. Ce fichier contient les informations dont vous avez besoin pour ajouter votre abonnement Microsoft Azure dans CSM.

- ID de client
- Clé de client
- ID de locataire
- ID d'abonnement

Note Consultez les fichiers JSON qui sont utilisés pour créer les rôles CSM et PCG afin d'obtenir la liste des autorisations qui leur sont accessibles après leur création.

Étape suivante

[Ajouter votre abonnement Microsoft Azure dans CSM](#)

Ajouter votre abonnement Microsoft Azure dans CSM

Dès que vous disposez des détails du principal du service NSX Cloud, et des rôles CSM et PCG, vous êtes prêt à ajouter votre abonnement Microsoft Azure dans CSM.

Conditions préalables

- Vous devez disposer du rôle d'administrateur d'entreprise dans NSX-T Data Center.
- Vous devez disposer de la sortie du script PowerShell avec les détails du principal du service NSX Cloud.
- Vous devez disposer de la valeur du rôle PCG que vous avez fournie lors de l'exécution du script PowerShell de création des rôles et du principal du service.

Procédure

- 1 Connectez-vous à CSM à l'aide d'un compte disposant du rôle d'administrateur d'entreprise.
- 2 Accédez à **CSM > Clouds > Azure**.
- 3 Cliquez sur **+ Ajouter**, puis entrez les détails suivants :

Option	Description
Nom	Indiquez un nom approprié pour identifier ce compte dans CSM. Plusieurs abonnements Microsoft Azure peuvent être associés au même ID de locataire Microsoft Azure. Vous pouvez nommer vos comptes dans CSM de manière à pouvoir les identifier facilement, par exemple, Compte-DevOps-Azure, Compte-Finance-Azure, etc.
ID de client	Copiez et collez cette valeur à partir de la sortie du script PowerShell.
Clé	Copiez et collez cette valeur à partir de la sortie du script PowerShell.
ID d'abonnement	Copiez et collez cette valeur à partir de la sortie du script PowerShell.

Option	Description
ID de locataire	Copiez et collez cette valeur à partir de la sortie du script PowerShell.
Nom de rôle de passerelle	La valeur par défaut est <code>nsx-pcg-role</code> . Cette valeur est disponible dans le fichier <code>nsx_pcg_role.json</code> si vous avez modifié la valeur par défaut.
Balises cloud	Par défaut, cette option est activée et permet la visibilité de vos balises Microsoft Azure dans NSX Manager

4 Cliquez sur **Enregistrer**.

CSM ajoute le compte, lequel apparaît dans la section **Comptes** en quelques minutes.

Étape suivante

[Déployer PCG dans un réseau virtuel Microsoft Azure](#)

Activer CSM pour accéder à votre inventaire AWS

Votre compte AWS contient un ou plusieurs VPC que vous souhaitez inclure dans la gestion de NSX-T Data Center.

Il s'agit d'un processus en trois étapes :

- 1 Utilisez le script NSX Cloud (interface utilisateur de ligne de commande AWS requis) pour effectuer les opérations suivantes :
 - Créer un profil de liaison montante.
 - Créer un rôle pour PCG.
- 2 Ajouter le compte AWS dans CSM.

Générer les rôles requis

NSX Cloud a recours à l'IAM AWS pour générer un rôle associé au profil NSX Cloud qui fournit les autorisations nécessaires à la passerelle PCG pour accéder à votre compte AWS.

Pour que NSX Cloud fonctionne dans votre compte AWS, vous devez générer un profil et un rôle IAM pour PCG.

Cela est possible en exécutant le script shell NSX Cloud à l'aide de l'interface de ligne de commande AWS qui crée les constructions suivantes :

- un profil IAM pour NSX Cloud ;
- un rôle pour PCG afin de lui permettre de travailler sur votre inventaire de cloud public.

Conditions préalables

- L'interface de ligne de commande AWS doit être installée et configurée à l'aide de la clé d'accès et de la clé secrète de votre compte AWS.
- Vous devez disposer d'un nom de profil IAM unique à fournir au script. Le nom de rôle de passerelle est associé à ce profil IAM



Procédure

- 1 Sur un poste de travail ou serveur Linux ou compatible, téléchargez le script SHELL nommé `AWS_create_credentials.sh` depuis NSX-T Data Center **Page de téléchargement > Pilotes et outils > Scripts NSX Cloud > AWS**.

- 2 Exécutez le script et entrez un nom pour le profil IAM lorsque vous y êtes invité. Par exemple,

```
bash AWS_create_NSXCloud_credentials.sh
```

- 3 Lorsque le script s'exécute avec succès, le profil IAM et un rôle pour PCG sont créés dans votre compte AWS. Les valeurs sont enregistrées dans le fichier de sortie dans le répertoire où vous avez exécuté le script. Le nom de fichier est `aws_details.txt`.

Note Par défaut, le nom du rôle PCG (passerelle) est `nsx_pcg_service`. Vous pouvez le modifier dans le script si vous souhaitez une valeur différente pour le nom du rôle de passerelle. Cette valeur est requise pour l'ajout du compte AWS dans CSM, vous devez donc en prendre note si vous modifiez la valeur par défaut.

Étape suivante

[Ajouter votre compte AWS dans CSM](#)

Ajouter votre compte AWS dans CSM

Ajoutez votre compte AWS en utilisant les valeurs générées par le script.

Procédure

- 1 Connectez-vous à CSM en utilisant le rôle d'administrateur d'entreprise.
- 2 Accédez à **CSM > Clouds > AWS**.
- 3 Cliquez sur **+Ajouter** et entrez les informations suivantes en utilisant le fichier de sortie `aws_details.txt` généré à partir du script NSX Cloud :

Option	Description
Nom	Entrez un nom descriptif pour ce compte AWS
clé d'accès	Entrez la clé d'accès de votre compte
Clé secrète	Entrez la clé secrète de votre compte
Balises cloud	Par défaut, cette option est activée et permet à vos balises AWS d'être visibles dans NSX Manager
Nom de rôle de passerelle	La valeur par défaut est <code>nsx_pcg_service</code> . Vous pouvez trouver cette valeur dans la sortie du script dans le fichier <code>aws_details.txt</code> .

Le compte AWS est ajouté dans CSM.

Dans l'onglet VPC de CSM, vous pouvez voir tous les VPC dans votre compte AWS.

Dans l'onglet Instances de CSM, vous pouvez afficher les instances d'EC2 dans ce VPC.

Étape suivante

[Déployer PCG dans VPC AWS](#)

Déployer PCG

La NSX Public Cloud Gateway (PCG) fournit une connectivité nord-sud entre le cloud public et les composants de gestion NSX-T Data Center sur site.

Conditions préalables

- Vos comptes de cloud public doivent être déjà ajoutés dans CSM.
- Le VPC ou le VNet sur lequel vous déployez PCG doit disposer des sous-réseaux requis réglés de façon appropriée pour High Availability : *liaison montante*, *liaison descendante* et *gestion*.

Le déploiement de PCG s'aligne sur votre plan d'adressage réseau avec des noms de domaine complets pour les composants NSX-T Data Center et un serveur DNS pouvant résoudre ces noms de domaine complets.

Note Il est déconseillé d'utiliser des adresses IP pour établir une connexion entre le cloud public et NSX-T Data Center à l'aide de PCG, mais si vous décidez de choisir cette option, ne modifiez pas vos adresses IP.

Déployer PCG dans un réseau virtuel Microsoft Azure

Suivez ces instructions pour déployer PCG dans votre abonnement Microsoft Azure.

Procédure

- 1 Connectez-vous à CSM à l'aide d'un compte disposant du rôle d'administrateur d'entreprise.
- 2 Cliquez sur **Clouds > Azure** et accédez à l'onglet **VNet**.
- 3 Cliquez sur un réseau virtuel sur lequel vous souhaitez déployer PCG.
- 4 Cliquez sur **Déployer des passerelles**. L'assistant **Déployer une passerelle principale** s'ouvre.
- 5 Pour les propriétés générales, utilisez les directives suivantes :

Option	Description
Clé publique SSH	Fournissez une clé publique SSH qui peut être validée lors du déploiement de PCG. Cette clé est nécessaire pour chaque déploiement de PCG.
Stratégie de mise en quarantaine sur le VNet associé	Laissez cette option dans le mode désactivé par défaut lorsque vous déployez PCG pour la première fois. Vous pourrez modifier cette valeur après l'intégration des VM. Reportez-vous à la section Gérer la stratégie de mise en quarantaine dans le <i>Guide d'administration de NSX-T Data Center</i> pour plus de détails.

Option	Description
Compte de stockage local	<p>Lorsque vous ajoutez un abonnement Microsoft Azure à CSM, une liste de vos comptes de stockage Microsoft Azure est mise à la disposition de CSM. Sélectionnez le compte de stockage dans le menu déroulant. Lors du processus de déploiement de PCG, CSM copie le fichier VHD publiquement disponible de PCG dans ce compte de stockage de la région sélectionnée.</p> <p>Note Si l'image VHD a déjà été copiée vers ce compte de stockage de la région dans le cadre d'un précédent déploiement de PCG, elle est utilisée à partir de cet emplacement pour les déploiements suivants afin de réduire le temps de déploiement global.</p>
URL de l'image VHD	<p>Si vous souhaitez utiliser une image de PCG différente qui n'est pas disponible dans le référentiel VMware public, entrez ici l'URL de l'image VHD de PCG. L'image VHD doit être présente dans le même compte et dans la même région où ce réseau virtuel est créé.</p>
Serveur proxy	<p>Sélectionnez un serveur proxy à utiliser pour le trafic Internet à partir de cette PCG. Les serveurs proxy sont configurés dans CSM. Vous pouvez sélectionner le même serveur proxy que CSM le cas échéant, sélectionner un serveur proxy autre que CSM ou sélectionner Aucun serveur proxy.</p> <p>Reportez-vous à la section (Facultatif) Configurer les serveurs Proxy pour plus d'informations sur la configuration des serveurs proxy dans CSM.</p>
Avancé	<p>Les paramètres DNS avancés apportent de la souplesse pour sélectionner des serveurs DNS afin de résoudre les composants de gestion de NSX-T Data Center</p>
Obtenir les paramètres à partir du DHCP du fournisseur de cloud public	<p>Sélectionnez cette option si vous souhaitez utiliser les paramètres DNS de Microsoft Azure. Il s'agit du paramètre DNS par défaut si vous ne sélectionnez aucune autre option pour le remplacer.</p>
Remplacer le serveur DNS du fournisseur de cloud public	<p>Sélectionnez cette option si vous souhaitez fournir manuellement l'adresse IP d'un ou plusieurs serveurs DNS pour résoudre les dispositifs NSX-T Data Center ainsi que les machines virtuelles de charge de travail dans ce réseau virtuel.</p>
Utiliser le serveur DNS du fournisseur de cloud public uniquement pour les dispositifs NSX-T Data Center	<p>Sélectionnez cette option si vous souhaitez utiliser le serveur DNS Microsoft Azure pour résoudre les composants de gestion NSX-T Data Center. Ce paramètre vous permet d'utiliser deux serveurs DNS : un pour PCG qui résout les dispositifs NSX-T Data Center, l'autre pour le réseau virtuel qui résout vos machines virtuelles de charge de travail dans ce réseau virtuel.</p>

6 Cliquez sur **Suivant**.

7 Pour l'option **Sous-réseaux**, utilisez les directives suivantes :

Option	Description
Activer la fonctionnalité HA pour NSX Cloud Gateway	<p>Sélectionnez cette option pour activer la haute disponibilité.</p>
Sous-réseaux	<p>Sélectionnez cette option pour activer la haute disponibilité.</p>
Adresse IP publique sur la carte réseau de gestion	<p>Sélectionnez Allouer une nouvelle adresse IP pour fournir une adresse IP publique à la carte réseau de gestion. Vous pouvez fournir manuellement l'adresse IP publique si vous souhaitez réutiliser une adresse IP publique libre.</p>
Adresse IP publique sur la carte réseau de liaison montante	<p>Sélectionnez Allouer une nouvelle adresse IP pour fournir une adresse IP publique à la carte réseau de liaison montante. Vous pouvez fournir manuellement l'adresse IP publique si vous souhaitez réutiliser une adresse IP publique libre.</p>

Étape suivante

Intégrez vos machines virtuelles de charge de travail. Reportez-vous à la section **Intégration et gestion des VM de charge de travail** dans le *Guide d'administration de NSX-T Data Center* pour le workflow day-N.

Déployer PCG dans VPC AWS

Suivez ces instructions pour déployer PCG dans votre compte AWS.

Procédure

- 1 Connectez-vous à CSM à l'aide d'un compte disposant du rôle d'administrateur d'entreprise.
- 2 Cliquez sur **Clouds > AWS > <AWS_account_name>** et accédez à l'onglet **VPC**.
- 3 Dans l'onglet **VPC**, sélectionnez un nom de région AWS, par exemple, us-west. La région AWS doit être celle où vous avez créé le VPC de calcul.
- 4 Sélectionnez un VPC de calcul configuré pour NSX Cloud.
- 5 Cliquez sur **Déployer des passerelles**.
- 6 Renseignez les informations générales de la passerelle :

Option	Description
Fichier PEM	Sélectionnez l'un de vos fichiers PEM dans le menu déroulant. Ce fichier doit se trouver dans la région où NSX Cloud a été déployé et où vous avez créé votre VPC de calcul. Cela identifie de façon unique votre compte AWS.
Stratégie de mise en quarantaine sur le VPC associé	La sélection par défaut est activée. Cela est recommandé pour les déploiements dans des environnements vierges. Si des machines virtuelles sont déjà lancées dans votre VPC, désactivez la stratégie de mise en quarantaine. Reportez-vous à la section Gérer la stratégie de mise en quarantaine dans le <i>Guide d'administration de NSX-T Data Center</i> pour plus de détails.
Serveur proxy	Sélectionnez un serveur proxy à utiliser pour le trafic Internet à partir de cette PCG. Les serveurs proxy sont configurés dans CSM. Vous pouvez sélectionner le même serveur proxy que CSM le cas échéant, sélectionner un serveur proxy autre que CSM ou sélectionner Aucun serveur proxy . Reportez-vous à la section (Facultatif) Configurer les serveurs Proxy pour plus d'informations sur la configuration des serveurs proxy dans CSM.
Avancé	Les paramètres avancés fournissent des options supplémentaires si nécessaire.
Remplacer l'ID d'AMI	Utilisez cette fonctionnalité avancée afin de fournir pour la PCG un ID d'AMI différent de celui disponible dans votre compte AWS.
Obtenir les paramètres à partir du DHCP du fournisseur de cloud public	Sélectionnez cette option si vous souhaitez utiliser les paramètres AWS. Il s'agit du paramètre DNS par défaut si vous ne sélectionnez aucune autre option pour le remplacer.

Option	Description
Remplacer le serveur DNS du fournisseur de cloud public	Sélectionnez cette option si vous souhaitez fournir manuellement l'adresse IP d'un ou plusieurs serveurs DNS pour résoudre les dispositifs NSX-T Data Center ainsi que les machines virtuelles de charge de travail de ce VPC.
Utiliser le serveur DNS du fournisseur de cloud public uniquement pour les dispositifs NSX-T Data Center	Sélectionnez cette option si vous souhaitez utiliser le serveur DNS AWS pour résoudre les composants de gestion de NSX-T Data Center. Ce paramètre vous permet d'utiliser deux serveurs DNS : un pour PCG qui résout les dispositifs NSX-T Data Center, l'autre pour le VPC qui résout vos machines virtuelles de charge de travail dans ce VPC.

7 Cliquez sur **Suivant**.

8 Renseignez les détails du sous-réseau.

Option	Description
Activer la fonctionnalité HA pour Public Cloud Gateway	Le paramètre recommandé est Activer, qui définit une paire HA Active/En veille pour éviter une interruption de service non planifiée.
Paramètres de la passerelle principale	Sélectionnez une Zone de disponibilité telle que us-west-1a dans le menu déroulant en tant que passerelle principale pour HA. Attribuez les sous-réseaux de liaison montante, de liaison descendante et de gestion dans le menu déroulant.
Paramètres de la passerelle secondaire	Sélectionnez une autre Zone de disponibilité telle que us-west-1b dans le menu déroulant en tant que passerelle secondaire pour HA. La passerelle secondaire est utilisée lorsque la passerelle principale tombe en panne. Attribuez les sous-réseaux de liaison montante, de liaison descendante et de gestion dans le menu déroulant.
Adresse IP publique sur la carte réseau de gestion	Sélectionnez Allouer une nouvelle adresse IP pour fournir une adresse IP publique à la carte réseau de gestion. Vous pouvez fournir manuellement l'adresse IP publique si vous souhaitez réutiliser une adresse IP publique libre.
Adresse IP publique sur la carte réseau de liaison montante	Sélectionnez Allouer une nouvelle adresse IP pour fournir une adresse IP publique à la carte réseau de liaison montante. Vous pouvez fournir manuellement l'adresse IP publique si vous souhaitez réutiliser une adresse IP publique libre.

Cliquez sur **Déployer**.

9 Surveillez l'état du déploiement PCG principal (et du déploiement secondaire, si vous l'avez sélectionné) . L'opération peut durer 10 à 12 minutes.

10 Cliquez sur **Terminer** lorsque PCG est correctement déployé.

Étape suivante

Intégrez vos machines virtuelles de charge de travail. Reportez-vous à la section **Intégration et gestion des VM de charge de travail** dans le *Guide d'administration de NSX-T Data Center* pour le workflow day-N.

Constructions créées après le déploiement de PCG

Des entités NSX-T Data Center essentielles sont créées et configurées dans NSX Manager, et des groupes de sécurité sont créés dans votre cloud public après que PCG est déployé avec succès.

Configurations de NSX Manager

Les entités suivantes sont automatiquement créées dans NSX Manager :

- Un nœud Edge nommé **Passerelle de cloud public** (PCG) est créé.
- PCG est ajouté au cluster Edge. Dans un déploiement HA, il y a deux PCG.
- Le PCG (ou les PCG) est enregistré comme nœud de transport avec deux zones de transport créées.
- Deux commutateurs logiques par défaut sont créés.
- Un routeur logique de niveau 0 est créé.
- Un profil de découverte IP est créé. Il est utilisé pour les commutateurs logiques de superposition.
- Un profil DHCP est créé. Il est utilisé pour les serveurs DHCP.
- Un groupe NS par défaut appelé **PublicCloudSecurityGroup** est créé avec les membres suivants :
 - Le commutateur logique VLAN par défaut.
 - Les ports logiques, un pour chacun des ports de liaison montante PCG, si la fonctionnalité HA est activée.
 - Adresse IP
- Trois règles DFW (Default Distributed Firewall) sont créées :
 - LogicalSwitchToLogicalSwitch
 - LogicalSwitchToAnywhere
 - AnywhereToLogicalSwitch

Note Ces règles DFW bloquent tout le trafic et doivent être ajustées en fonction de vos besoins spécifiques.

Vérifiez ces configurations dans NSX Manager :

- 1 Dans le tableau de bord NSX Cloud, cliquez sur **NSX Manager**.
- 2 Accédez à **Infrastructure > Nœuds > Edge**. La passerelle de cloud public doit être répertoriée comme un nœud Edge.
- 3 Vérifiez que État de déploiement, Gestionnaire de connexion et Connexion du contrôleur sont connectés (l'état indique **Actif** avec un point vert).
- 4 Accédez à **Infrastructure > Nœuds > Clusters Edge** pour vérifier que le cluster Edge et PCG ont été ajoutés comme partie intégrante de ce cluster.

- 5 Accédez à **Infrastructure > Nœuds > Nœuds de transport** pour vérifier que PCG est enregistré comme nœud de transport et est connecté à deux zones de transport qui ont été créés automatiquement lors du déploiement de PCG :
 - Type de trafic VLAN -- il se connecte à la liaison montante PCG
 - Type de superposition de trafic -- il s'agit de la mise en réseau logique de superposition
- 6 Vérifiez que les commutateurs logiques et le routeur logique de niveau 0 ont été créés et que le routeur logique est ajouté au cluster Edge.

Important Ne supprimez pas les entités créées par NSX.

Configurations de cloud public

Dans AWS :

- Dans le VPC AWS, un nouvel ensemble d'enregistrements de type A est ajouté sous le nom `nsx-gw.vmware.local`. L'adresse IP mappée à cet enregistrement correspond à l'adresse IP de gestion de PCG. Elle est attribuée par AWS à l'aide de DHCP et est différente pour chaque VPC.
- Une adresse IP secondaire pour l'interface de liaison montante pour PCG est créée. Une adresse IP élastique AWS est associée à cette adresse IP secondaire. Cette configuration est destinée à SNAT.

Dans AWS et Microsoft Azure :

Les groupes de sécurité **gw** sont appliqués aux interfaces PCG respectives.

Tableau 9-2. Groupes de sécurité de cloud public créés par NSX Cloud pour les interfaces PCG

Nom du groupe de sécurité	Disponible dans Microsoft Azure ?	Disponible dans AWS ?	Nom complet
gw-mgmt-sg	Oui	Oui	Groupe de sécurité de gestion de passerelle
gw-uplink-sg	Oui	Oui	Groupe de sécurité de liaison montante de passerelle
gw-vtep-sg	Oui	Oui	Groupe de sécurité de liaison descendante de passerelle

Tableau 9-3. Groupes de sécurité de cloud public créés par NSX Cloud pour les machines virtuelles de charge de travail

Nom du groupe de sécurité	Disponible dans Microsoft Azure ?	Disponible dans AWS ?	Description
quarantine	Oui	Non	Groupe de sécurité de quarantaine pour Microsoft Azure
default	Non	Oui	Groupe de sécurité de quarantaine pour AWS
vm-underlay-sg	Oui	Oui	Groupe de sécurité de non-superposition de VM

Tableau 9-3. Groupes de sécurité de cloud public créés par NSX Cloud pour les machines virtuelles de charge de travail (Suite)

Nom du groupe de sécurité	Disponible dans Microsoft Azure ?	Disponible dans AWS ?	Description
vm-override-sg	Oui	Oui	Groupe de sécurité de remplacement de VM
vm-overlay-sg	Oui	Oui	Groupe de sécurité réseau de superposition de VM (non utilisé dans la version actuelle)
vm-outbound-bypass-sg	Oui	Oui	Groupe de sécurité de contournement sortant de VM (non utilisé dans la version actuelle)
vm-inbound-bypass-sg	Oui	Oui	Groupe de sécurité de contournement entrant de VM (non utilisé dans la version actuelle)

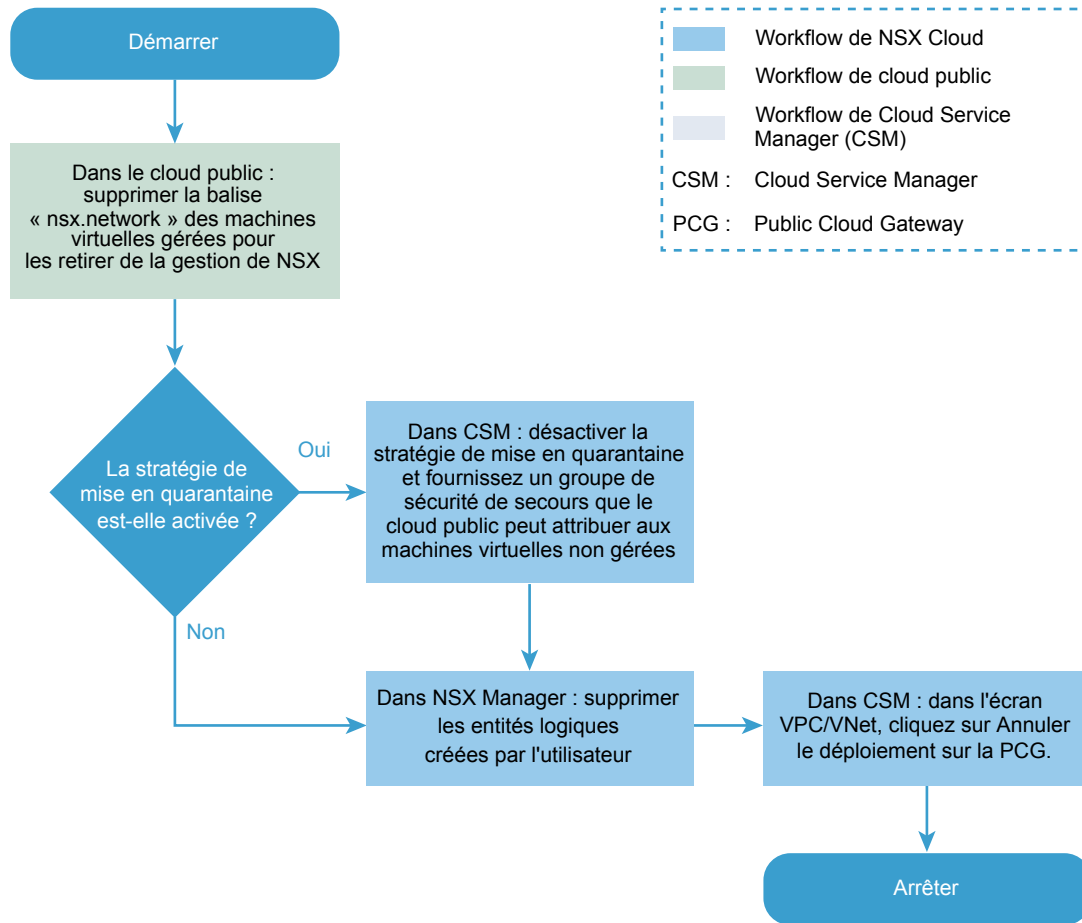
Annuler le déploiement de PCG

Reportez-vous à cet organigramme pour connaître les étapes impliquées dans l'annulation du déploiement de PCG.

- Pour annuler le déploiement de PCG, les conditions suivantes doivent être remplies : aucune machine virtuelle dans le VPC ou VNet ne doit être gérée par NSX.
- La stratégie de mise en quarantaine doit être désactivée.

- Toutes les entités logiques créées par l'utilisateur associées à la passerelle PCG doivent être supprimées.

Chiffre 9-4. Annulation du déploiement de PCG



1 Annuler la balise de machines virtuelles dans le cloud public

Avant que vous puissiez annuler le déploiement de PCG, toutes les machines virtuelles doivent être non gérées.

2 Désactiver la stratégie de mise en quarantaine, si elle est activée

Si elle avait été précédemment activée, la stratégie de mise en quarantaine doit être désactivée pour annuler le déploiement de PCG.

3 Supprimer les entités logiques créés par l'utilisateur

Supprimez toutes les entités logiques que vous avez créées dans NSX Manager.

4 Annuler le déploiement depuis CSM

Pour annuler le déploiement de PCG une fois les conditions préalables remplies, cliquez sur **Annuler le déploiement de passerelle** depuis **Clouds > <Cloud public> > <VNet/VPC>** dans CSM.

Annuler la balise de machines virtuelles dans le cloud public

Avant que vous puissiez annuler le déploiement de PCG, toutes les machines virtuelles doivent être non gérées.

Accédez au VPC ou au VNet dans votre cloud public et supprimez la balise `nsx.network` des machines virtuelles gérées.

Désactiver la stratégie de mise en quarantaine, si elle est activée

Si elle avait été précédemment activée, la stratégie de mise en quarantaine doit être désactivée pour annuler le déploiement de PCG.

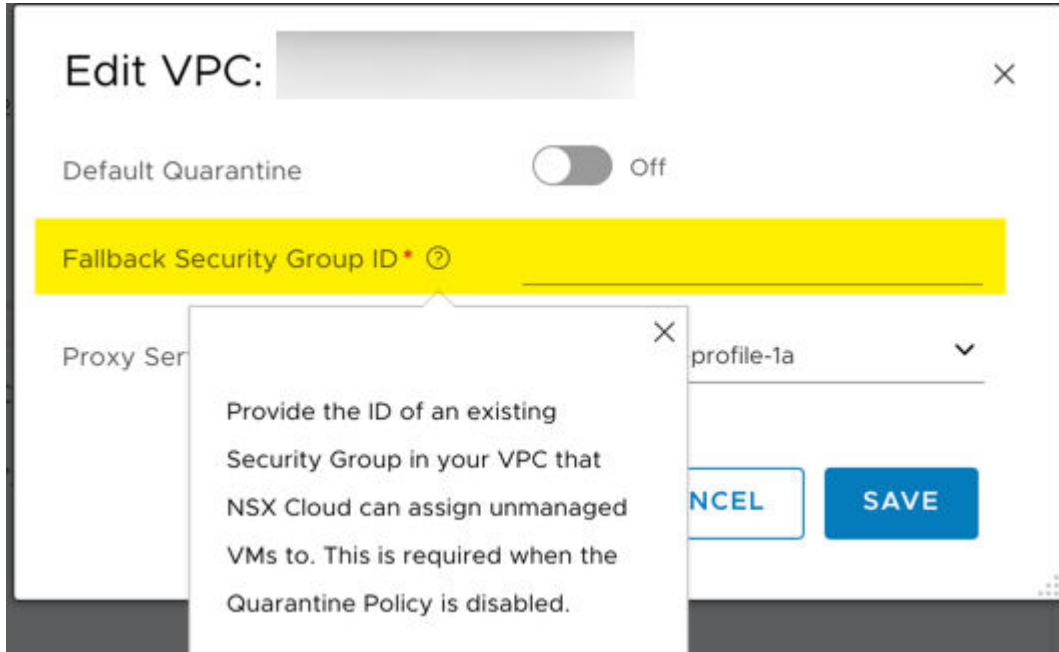
Lorsque la stratégie de mise en quarantaine est activée, des groupes de sécurité définis par NSX Cloud sont attribués à vos machines virtuelles. Lorsque vous annulez le déploiement de PCG, vous devez désactiver la stratégie de mise en quarantaine et spécifier un groupe de sécurité à attribuer aux machines virtuelles lorsqu'elles sont supprimées des groupes de sécurité de NSX Cloud.

Note Le groupe de sécurité de secours doit être un groupe de sécurité défini par l'utilisateur existant dans votre cloud public. Vous ne pouvez pas utiliser les groupes de sécurité NSX Cloud comme un groupe de sécurité de secours. Reportez-vous à la section [Constructions créées après le déploiement de PCG](#) pour obtenir la liste des groupes de sécurité NSX Cloud.

Désactivez la stratégie de mise en quarantaine du VPC ou du VNet à partir duquel vous annulez le déploiement de PCG :

- Accédez au VPC ou VNet dans CSM.
- Depuis **Actions > Modifier les configurations >**, désactivez le paramètre **Mise en quarantaine par défaut**.

- Entrez une valeur pour un groupe de sécurité de secours qui sera attribué aux machines virtuelles.



- Le groupe de sécurité de secours sera attribué à toutes les machines virtuelles non gérées ou mises en quarantaine dans ce VPC ou VNet.
- Si toutes les machines virtuelles ne sont pas gérées, le groupe de sécurité de secours leur est attribué.
- En présence de machines virtuelles gérées lors de la désactivation de la stratégie de mise en quarantaine, ces machines conservent les groupes de sécurité leur étant attribués par NSX Cloud. La première fois que vous supprimez la balise `nsx.network` de ces machines virtuelles pour les retirer de la gestion NSX, le groupe de sécurité de secours leur est également attribué.

Note Reportez-vous à **Gestion de la stratégie de mise en quarantaine** dans le document *Guide d'administration de NSX-T Data Center* pour obtenir des instructions et des précisions sur l'effet de l'activation et de la désactivation de la stratégie de mise en quarantaine.

Supprimer les entités logiques créés par l'utilisateur

Supprimez toutes les entités logiques que vous avez créées dans NSX Manager.

Reportez-vous à la liste ci-dessous pour trouver vos entités à supprimer :

Note Ne supprimez pas les entités logiques créées automatiquement lors du déploiement de PCG. Reportez-vous à la rubrique [Constructions créées après le déploiement de PCG](#)

- Entrée DNS de cloud public
- DDI : profil DHCP
- Routage : règle SNAT

- Routage : routeur statique
- Routage : port de routeur logique
- Routage : routeur logique
- Nœuds d'infrastructure : cluster de bordure
- Nœuds d'infrastructure : nœuds de transport
- Nœuds d'infrastructure : bordures
- Profils d'infrastructure : PCG-Uplink-HostSwitch-Profile
- Commutation : ports de commutateur logique
- Commutation : commutateurs logiques
- Zones de transport d'infrastructure : zones de Transport
- Commutation : PublicCloud-Global-SpoofGuardProfile

Annuler le déploiement depuis CSM

Pour annuler le déploiement de PCG une fois les conditions préalables remplies, cliquez sur **Annuler le déploiement de passerelle** depuis **Clouds > <Cloud public> > <VNet/VPC>** dans CSM.

- 1 Connectez-vous à CSM et accédez à votre cloud public :
 - Si vous utilisez AWS, accédez à **Clouds > AWS > VPC**. Cliquez sur le VPC sur lequel un ou une paire de PCG est déployée et en cours d'exécution.
 - Si vous utilisez Microsoft Azure, accédez à **Clouds > Azure > VNets**. Cliquez sur le réseau virtuel sur lequel un ou une paire de PCG est déployé(e) et en cours d'exécution.
- 2 Cliquez sur **Annuler le déploiement de passerelle**.

Les entités par défaut créées par NSX Cloud sont supprimées automatiquement lorsque le déploiement d'une PCG est annulé.

Désinstallation de NSX-T Data Center

10

Vous pouvez supprimer des éléments d'une superposition NSX-T Data Center, supprimer un hôte d'hyperviseur de NSX-T Data Center ou désinstaller NSX-T Data Center complètement.

Ce chapitre contient les rubriques suivantes :

- [Annuler la configuration d'une superposition NSX-T Data Center](#)
- [Supprimer un hôte de NSX-T Data Center ou désinstaller complètement NSX-T Data Center](#)

Annuler la configuration d'une superposition NSX-T Data Center

Si vous souhaitez supprimer une superposition tout en conservant vos nœuds de transport, procédez comme suit.

Procédure

- 1 Connectez-vous à vSphere Client.
- 2 Dans votre outil de gestion de machines virtuelles, dissociez toutes les machines virtuelles des commutateurs logiques et connectez les machines virtuelles à des réseaux autres que ceux de NSX-T Data Center.
- 3 Pour les hôtes KVM, ouvrez une session SSH sur les hôtes et mettez hors tension les machines virtuelles.

`shutdown -h now`
- 4 Dans l'interface utilisateur ou l'API NSX Manager, supprimez tous les routeurs logiques.
- 5 Dans l'interface utilisateur ou l'API NSX Manager, supprimez tous les ports de commutateurs logiques, puis tous les commutateurs logiques.
- 6 Dans l'interface utilisateur ou l'API NSX Manager, supprimez tous les dispositifs NSX Edge, puis tous les clusters NSX Edge.
- 7 Configurez une nouvelle superposition NSX-T Data Center, si nécessaire.

Supprimer un hôte de NSX-T Data Center ou désinstaller complètement NSX-T Data Center

Si vous souhaitez désinstaller complètement NSX-T Data Center ou simplement supprimer un hôte d'hyperviseur de NSX-T Data Center, de sorte que l'hôte n'appartienne plus à la superposition NSX-T Data Center, procédez comme suit.

La procédure suivante explique comment désinstaller NSX-T Data Center proprement.

Conditions préalables

Si l'outil de gestion des machines virtuelles est vCenter Server, placez l'hôte vSphere en mode de maintenance.

Procédure

- 1 Dans NSX Manager, sélectionnez **Infrastructure > Nœuds > Nœuds de transport** et supprimez les nœuds de transport d'hôtes.

Si on supprime le nœud de transport, le N-VDS est retiré de l'hôte. Pour le confirmer, exécutez la commande suivante.

```
[root@host:~] esxcli network vswitch dvs vmware list
```

Sur KVM, la commande est la suivante :

```
ovs-vsctl show
```

- 2 Dans l'interface de ligne de commande de NSX Manager, vérifiez que le service d'installation-mise à niveau de NSX-T Data Center est en cours d'exécution.

```
nsx-manager-1> get service install-upgrade
Service name: install-upgrade
Service state: running
Enabled: True
```

- 3 Désinstallez l'hôte du plan de gestion et supprimez les modules NSX-T Data Center.

La suppression de tous les modules NSX-T Data Center peut prendre jusqu'à 5 minutes.

Pour supprimer les modules NSX-T Data Center, vous disposez de plusieurs méthodes distinctes :

- Dans NSX Manager, sélectionnez **Infrastructure > Nœuds > Hôtes > Supprimer**.

Vérifiez que **Désinstaller les composants NSX** est coché. Cela désinstalle les modules NSX-T Data Center sur l'hôte.

Supprimez les modules de dépendance RHEL 7.4 : json_spirit, python-greenlet, libev, protobuf, leveldb, python-gevent, python-simplejson, glog.

Supprimez les modules de dépendance Ubuntu 16.04.x : `nicira-ovs-hypervisor-node`, `openvswitch-switch`, `openvswitch-datapath-dkms`, `openvswitch-pki`, `python-openvswitch`, `openvswitch-common`, `libjson-spirit`.

Notez que l'utilisation de **Infrastructure > Nœuds > Hôtes > Supprimer** avec l'option **Désinstaller les composants NSX** non cochée n'est pas conseillée pour annuler l'inscription d'un hôte. Il s'agit uniquement d'une solution de contournement pour les hôtes dont l'état est incorrect.

- (Hôtes gérés par un gestionnaire de calcul) Dans NSX Manager, sélectionnez **Infrastructure > Nœuds > Hôtes > Nœuds de transport > Supprimer l'hôte**.

Dans NSX Manager, sélectionnez **Infrastructure > Nœuds > Hôtes > Gestionnaire de calcul > Configurer le gestionnaire de cluster** et désélectionnez la case **Installer automatiquement NSX**. Sélectionnez un nœud et cliquez sur **Désinstaller NSX**.

Vérifiez que **Désinstaller les composants NSX** est coché. Cela désinstalle les modules NSX-T Data Center sur l'hôte.

- Utilisez l'API DELETE `/api/v1/fabric/nodes/<node-id>`.

Note Cette API ne supprime pas les modules de dépendance dans le bundle `nsx-lcp`.

Supprimez les modules de dépendance RHEL 7.4 : `json_spirit`, `python-greenlet`, `libev`, `protobuf`, `leveldb`, `python-gevent`, `python-simplejson`, `glog`.

Supprimez les modules de dépendance Ubuntu 16.04.x : `nicira-ovs-hypervisor-node`, `openvswitch-switch`, `openvswitch-datapath-dkms`, `openvswitch-pki`, `python-openvswitch`, `openvswitch-common`, `libjson-spirit`.

- Utilisez l'interface de ligne de commande de vSphere.

- a Obtenez l'empreinte numérique du responsable.

```
manager> get certificate api thumbprint
```

- b Sur l'interface de ligne de commande NSX-T Data Center de l'hôte, exécutez la commande suivante afin de détacher l'hôte du plan de gestion.

```
host> detach management-plane <MANAGER> username <ADMIN-USER> password <ADMIN-PASSWORD>
thumbprint <MANAGER-THUMBPRINT>
```

- c Sur l'hôte, exécutez la commande suivante pour supprimer les filtres.

```
[root@host:~] vsiioctl clearallfilters
```

- d Sur l'hôte, exécutez la commande suivante pour arrêter netcpa.

```
[root@host:~] /etc/init.d/netcpad stop
```

- e Mettez hors tension les machines virtuelles sur l'hôte ou migrez-les vers un autre hôte.

- f Sur l'hôte, exécutez la commande suivante pour désinstaller manuellement la configuration et les modules de NSX-T Data Center. Cette commande est prise en charge sur tous les types d'hôtes.

```
[root@host:~] clear management-plane
```

Étape suivante

Après cette modification, l'hôte est retiré du plan de gestion et n'appartient plus à la superposition NSX-T Data Center.

Si vous retirez complètement NSX-T Data Center, dans votre outil de gestion de machines virtuelles, arrêtez NSX Manager, les dispositifs NSX Controller et NSX Edge, puis supprimez-les du disque.