

Guide d'installation de NSX-T Data Center

Modifié le 12 août 2021
VMware NSX-T Data Center 2.5

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

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

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 © 2020 VMware, Inc. Tous droits réservés. [Informations relatives aux copyrights et marques commerciales.](#)

Table des matières

Guide d'installation de NSX-T Data Center	8
1 Présentation de NSX-T Data Center	9
Concepts clés	10
Présentation de NSX Manager	14
2 Workflows d'installation de NSX-T Data Center	17
Workflow NSX-T Data Center pour vSphere	17
Workflow d'installation de NSX-T Data Center pour KVM	18
Workflow de configuration de NSX-T Data Center pour le serveur sans système d'exploitation	19
3 Préparation à l'installation	21
Configuration système requise	21
Configuration système requise pour le nœud de transport hôte et la machine virtuelle NSX Manager	21
Configuration système requise des machines virtuelles NSX Edge	25
Configuration requise pour NSX Edge sans système d'exploitation	27
Configuration requise système d'un serveur bare metal	29
Configuration requise du conteneur Linux de système bare metal	30
Ports et protocoles	30
Ports TCP et UDP utilisés par NSX Manager	31
Ports TCP et UDP utilisés par NSX Edge	32
Ports TCP et UDP utilisés par ESXi, les hôtes KVM et le serveur Bare Metal	34
4 Installation de NSX Manager	36
Modification de l'expiration du mot de passe administrateur par défaut	42
5 Installation de NSX-T Data Center sur vSphere	43
Installer NSX Manager et les dispositifs disponibles	43
Installer NSX Manager sur ESXi à l'aide de l'outil OVF de ligne de commande	48
Configurer NSX-T Data Center pour afficher le menu GRUB au démarrage	53
Se connecter à l'instance de NSX Manager qui vient d'être créée	54
Ajouter un gestionnaire de calcul	54
Déployer des nœuds NSX Manager pour constituer un cluster à partir de l'interface utilisateur	57
Configurer une adresse IP virtuelle (VIP) pour un cluster	63
Désactiver des snapshots sur des dispositifs NSX-T	65

6 Installation de NSX-T Data Center sur KVM 67

Configurer KVM 67

Gérer vos machines virtuelles invitées dans l'interface de ligne de commande de KVM 70

Installer NSX Manager sur KVM 71

Se connecter à l'instance de NSX Manager qui vient d'être créée 76

Installer des modules tiers sur un hôte KVM 77

Vérifier la version Open vSwitch sur les hôtes RHEL KVM 78

Vérifier la version d'Open vSwitch sur les hôtes SUSE KVM 79

Déploiement de nœuds NSX Manager pour former un cluster à l'aide de la ligne de commande 80

7 Configuration d'un serveur bare metal pour utiliser NSX-T Data Center 82

Installer les modules tiers sur un serveur bare metal 82

Créer une interface d'application pour les charges de travail de serveur Bare Metal 84

8 Configuration requise pour le cluster NSX Manager 86

Configuration requise du cluster NSX Manager pour un site unique, deux sites et plusieurs sites 86

9 Installation de NSX Edge 90

Conditions d'installation de NSX Edge 90

Configuration réseau de NSX Edge 93

Méthodes d'installation de NSX Edge 100

Créer un nœud de transport NSX Edge 102

Créer un cluster NSX Edge 107

Installer un dispositif NSX Edge sur ESXi à l'aide de l'interface utilisateur graphique de vSphere 108

Installer NSX Edge sur ESXi à l'aide de l'outil OVF de ligne de commande 112

Installer NSX Edge par le biais d'un fichier ISO en tant que dispositif virtuel 117

Installer un dispositif NSX Edge sur un système Bare Metal 121

Préparer le serveur PXE pour NSX Edge 122

Installer NSX Edge automatiquement via un fichier ISO 127

Installer NSX Edge de manière interactive via un fichier ISO 131

Relier NSX Edge au plan de gestion 133

Configurer un dispositif NSX Edge en tant que nœud de transport 134

10 Zones de transport et nœuds de transport 137

Créer des zones de transport 137

Créer un pool d'adresses IP pour les adresses IP des points de terminaison de tunnel 140

Chemin de données optimisé 141

Configuration de profils 145

Créer un profil de liaison montante 145

Configuration des profils Network I/O Control	149
Ajouter un profil de cluster NSX Edge	158
Ajouter un profil de pont NSX Edge	159
Ajouter un profil de nœud de transport	160
Migration de VMkernel vers un commutateur N-VDS	166
Erreurs de migration de VMkernel	172
Créer un nœud de transport d'hôte autonome ou de serveur bare metal	175
Configurer un nœud de transport d'hôte géré	185
Configurer un nœud de transport d'hôte ESXi avec agrégation de liens	190
Vérifier l'état des nœuds de transport	191
Migrer les adaptateurs physiques et VMkernel ESXi	193
Mode de maintenance NSX	194
Représentation visuelle de N-VDS	195
Contrôle de santé des plages d'ID VLAN et des paramètres MTU	197
Afficher l'état de détection de transfert bidirectionnel	200
Installation manuelle de modules de noyau NSX-T Data Center	201
Installer manuellement les modules de noyau NSX-T Data Center sur les hyperviseurs ESXi	202
Installer manuellement les modules des logiciels NSX-T Data Center sur des hyperviseurs KVM Ubuntu	205
Installer manuellement des modules de logiciels NSX-T Data Center sur des hyperviseurs KVM RHEL et CentOS	207
Installer manuellement les modules des logiciels NSX-T Data Center sur des hyperviseurs SUSE KVM	208
Déployer un cluster vSphere entièrement réduit pour NSX-T	209

11 Intégration de profils d'hôte avec NSX-T 222

Déployer automatiquement un cluster sans état	222
Tâches de haut niveau pour le déploiement automatique d'un cluster sans état	222
Conditions préalables et versions prises en charge	223
Créer un profil d'image personnalisé pour les hôtes sans état	224
Associer l'image personnalisée aux hôtes de référence et cibles	226
Définir la configuration réseau sur l'hôte de référence	227
Configurer l'hôte de référence en tant que nœud de transport dans NSX-T	228
Extraire et vérifier le profil d'hôte	230
Vérifier l'association de profil d'hôte à un cluster sans état	231
Mettre à jour la personnalisation de l'hôte	232
Déclencher le déploiement automatique sur les hôtes cibles	233
Dépanner le profil d'hôte et le profil de nœud de transport	243
Serveurs avec état	245
Versions NSX-T et ESXi prises en charge	246
Préparer un cluster cible avec état	246
Migration de VMkernel avec application du profil d'hôte	248

[Migration de VMkernel sans application du profil d'hôte](#) 250

12 Désinstallation de NSX-T Data Center d'un nœud de transport hôte 251

[Vérifier les mappages réseau de l'hôte pour la désinstallation](#) 251

[Désinstaller NSX-T Data Center d'un cluster vSphere](#) 253

[Désinstaller NSX-T Data Center d'un hôte dans un cluster vSphere](#) 255

[Désinstaller NSX-T Data Center d'un hôte autonome](#) 256

13 Installation de composants NSX Cloud 258

[Architecture et composants de NSX Cloud](#) 258

[Présentation du déploiement de NSX Cloud](#) 260

[Déployer des composants NSX-T Data Center sur site](#) 260

[Installation de CSM](#) 261

[Joindre CSM avec NSX Manager](#) 261

[Activer l'accès aux ports et aux protocoles](#) 262

[\(Facultatif\) Configurer les serveurs proxy](#) 263

[\(Facultatif\) Configurer vIDM pour Cloud Service Manager](#) 264

[Ajouter votre compte de cloud public](#) 264

[Connecter votre réseau Microsoft Azure à votre déploiement NSX-T Data Center sur site](#) 265

[Connecter votre réseau AWS \(Amazon Web Services\) à votre déploiement NSX-T Data Center sur site](#) 273

[Déployer la NSX Public Cloud Gateway](#) 279

[Déployer une PCG dans un VNet](#) 282

[Déployer PCG dans un VPC](#) 284

[Liaison vers un VPC ou VNet de transit](#) 287

[Entités logiques et groupes de sécurité cloud natifs créés automatiquement](#) 288

[\(Facultatif\) Installez NSX Tools sur vos machines virtuelles de charge de travail.](#) 295

[Annuler le déploiement ou annuler le lien des PCG](#) 295

[Supprimer la balise nsx.network dans le cloud public](#) 296

[Désactiver la stratégie de mise en quarantaine, fournir un groupe de sécurité de secours](#) 296

[Supprimer les entités logiques créés par l'utilisateur](#) 298

[Annuler le déploiement ou le lien de CSM](#) 298

[Dépannage lié à l'annulation du déploiement de PCG](#) 299

14 Installation et configuration de NSX Intelligence 300

[Workflow d'installation et de configuration de NSX Intelligence](#) 301

[Préparation à l'installation de NSX Intelligence](#) 302

[Configuration système requise pour NSX Intelligence](#) 303

[Ports TCP et UDP utilisés par NSX Intelligence](#) 303

[Télécharger et décompresser le bundle du programme d'installation NSX Intelligence](#) 304

Installez le dispositif NSX Intelligence	307
Dépannage lors de l'installation du dispositif NSX Intelligence	310
Les informations d'identification étaient incorrectes ou le compte fourni a été verrouillé	310
Le message d'état de déploiement du dispositif ayant échoué n'est pas effacé	311
Désinstaller le dispositif NSX Intelligence	311
15 Dépannage des problèmes d'installation	312
Échec de la l'installation en raison d'un espace insuffisant dans bootbank sur l'hôte ESXi	312

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 des publications techniques

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 <https://www.vmware.com/topics/glossary>.

Présentation de NSX-T Data Center

1

Tout comme la virtualisation des serveurs crée et gère des machines virtuelles de façon programmée, la virtualisation réseau NSX-T Data Center crée et gère 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. Ces trois plans sont implémentés sous la forme d'un ensemble de processus, de modules et d'agents résidant sur deux types de nœuds : NSX Manager et nœuds de transport.

- Chaque nœud héberge un agent du plan de gestion.
- Les nœuds NSX Manager hébergent les services API et les démons de cluster du plan de gestion.
- Les nœuds NSX Controller hébergent les démons de cluster du plan de contrôle central.
- Les nœuds de transport hébergent des démons du plan de contrôle local et des moteurs d'acheminement.

NSX Manager fournit une prise en charge de mise en cluster de trois nœuds qui fusionne le gestionnaire de stratégie, la gestion et les services de contrôle central sur un cluster de nœuds. La mise en cluster de NSX Manager fournit une haute disponibilité de l'interface utilisateur et de l'API. La convergence des nœuds de gestion et de plan de contrôle réduit le nombre de dispositifs virtuels devant être déployés et gérés par l'administrateur de NSX-T Data Center.

Le dispositif NSX Manager est proposé dans trois tailles pour différents scénarios de déploiement. Un petit dispositif pour les déploiements de laboratoire ou de validation technique. Un dispositif moyen pour les déploiements de jusqu'à 64 hôtes et un grand dispositif pour les clients procédant à des déploiements dans des environnements à grande échelle. Reportez-vous à [Configuration système requise pour le nœud de transport hôte et la machine virtuelle NSX Manager](#) et à l'outil [Valeurs maximales de configuration](#).

Ce chapitre contient les rubriques suivantes :

- [Concepts clés](#)
- [Présentation de NSX Manager](#)

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.

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

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.

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.

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 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

Le commutateur virtuel distribué géré par NSX (N-VDS, auparavant appelé commutateur hôte) ou OVS est utilisé pour NSX Edge partagé et le cluster de calcul. N-VDS est requis pour la configuration du trafic de superposition.

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).

NSX Manager

Nœud qui héberge les services d'API, le plan de gestion et les services d'agent. NSX Manager est un dispositif inclus dans le module d'installation de NSX-T Data Center. Vous pouvez déployer le dispositif avec le rôle de NSX Manager ou `nsx-cloud-service-manager`. Actuellement, le dispositif prend uniquement en charge un seul rôle à la fois.

Cluster NSX Manager

Un cluster de NSX Manager qui peut fournir une haute disponibilité.

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.

Segment

Entité qui fournit une commutation virtuelle de couche 2 pour les interfaces de machine virtuelle et les interfaces de passerelle. Un segment offre aux administrateurs de 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 segment 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. Un segment est également appelé commutateur logique.

Dans un cloud à locataires multiples, de nombreux segments peuvent exister côte à côte sur le même hyperviseur physique, les segments de couche 2 étant isolés les uns des autres. Les segments peuvent être connectés à l'aide de passerelles, qui peuvent fournir une connectivité au réseau physique externe.

Passerelle ou routeur logique de niveau 0

La passerelle de niveau 0 est appelée routeur logique de niveau 0 dans l'onglet **Mise en réseau et sécurité avancées**. Elle s'interface avec le réseau physique et peut être considérée comme un cluster actif-actif ou actif-en veille. La passerelle de niveau 0 exécute BGP et établit une relation homologue avec les routeurs physiques. Dans le mode actif-en veille, la passerelle peut également fournir des services avec état.

Passerelle ou routeur logique de niveau 1

La passerelle de niveau 1 est appelée routeur logique de niveau 1 dans l'onglet **Mise en réseau et sécurité avancées**. Elle se connecte à une passerelle de niveau 0 pour la connectivité ascendante et à un ou plusieurs réseaux de superposition pour la connectivité descendante. Une passerelle de niveau 1 peut être un cluster actif-en veille qui fournit 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 qui se trouvent sur ces hyperviseurs. Elle est également enregistrée avec le plan de gestion de NSX-T Data Center et dispose des modules NSX-T Data Center. Pour qu'un hôte d'hyperviseur ou un dispositif NSX Edge appartienne à la superposition NSX-T Data Center, il doit être ajouté à la zone de transport de NSX-T Data Center.

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. Le VLAN de transport défini dans les balises de profil de liaison montante est utilisé par le trafic de superposition uniquement et l'ID VLAN est utilisé par le point de terminaison TEP.

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

Chaque hyperviseur dispose d'un VTEP (Virtual Tunnel Endpoint) chargé d'encapsuler le trafic de machine virtuelle dans un en-tête VLAN et de router le paquet vers un VTEP de destination pour traitement supplémentaire. Le trafic peut être routé vers un autre VTEP sur un hôte différent ou vers la passerelle NSX Edge pour accéder au réseau physique.

Présentation de NSX Manager

NSX Manager fournit une interface utilisateur Web sur laquelle vous pouvez gérer l'environnement NSX-T. NSX Manager héberge également le serveur API qui traite les appels d'API.

L'interface utilisateur Web de NSX Manager fournit deux méthodes pour configurer les ressources.

- L'interface de stratégie : les onglets **Mise en réseau**, **Sécurité**, **Inventaire** et **Planifier et dépanner**.
- L'interface avancée : l'onglet **Mise en réseau et sécurité avancées**.

Quand utiliser la stratégie ou les interfaces avancées

Soyez cohérent à propos de l'interface utilisateur que vous voulez utiliser. Il existe plusieurs raisons d'utiliser une interface utilisateur plutôt qu'une autre.

- Si vous déployez un nouvel environnement avec NSX-T Data Center 2.4 ou version ultérieure, l'utilisation de la nouvelle interface utilisateur basée sur la stratégie pour créer et gérer votre environnement est le meilleur choix dans la plupart des cas.
 - Certaines fonctionnalités ne sont pas disponibles dans l'interface utilisateur basée sur la stratégie. Si vous avez besoin de ces fonctionnalités, utilisez l'interface utilisateur avancée pour toutes les configurations.
- Si vous effectuez une mise à niveau vers NSX-T Data Center 2.4 ou version ultérieure, continuez à modifier la configuration à l'aide de l'interface utilisateur **Mise en réseau et sécurité avancées**.

Tableau 1-1. Quand utiliser la stratégie ou les interfaces avancées


Interface de stratégie	Interface avancée
La plupart des nouveaux déploiements doivent utiliser l'interface basée sur la stratégie.	Les déploiements qui ont été créés à l'aide de l'interface avancée (par exemple, les mises à niveau de versions antérieures à l'interface basée sur la stratégie) sont présents.
Déploiements de NSX Cloud	Déploiements qui s'intègrent à d'autres plug-ins. Par exemple, NSX Container Plug-in, OpenStack et d'autres plates-formes de gestion de cloud.

Tableau 1-1. Quand utiliser la stratégie ou les interfaces avancées (suite)

Interface de stratégie	Interface avancée
<p>Fonctionnalités de mise en réseau disponibles dans l'interface de stratégie uniquement :</p> <ul style="list-style-type: none"> ■ Services DNS et zones DNS ■ VPN ■ Stratégies de transfert pour NSX Cloud 	<p>Fonctionnalités de mise en réseau disponibles dans l'interface avancée uniquement :</p> <ul style="list-style-type: none"> ■ Temporisateur d'activation du transfert ■ Routes statiques avec BFD et l'interface comme tronçon suivant ■ Proxy de métadonnées ■ Serveur DHCP associé à un segment isolé et une liaison statique
<p>Fonctionnalités de sécurité disponibles dans l'interface de stratégie uniquement :</p> <ul style="list-style-type: none"> ■ Protection du point de terminaison ■ Introspection réseau (Insertion de services Est-Ouest) ■ Profils de contexte <ul style="list-style-type: none"> ■ Applications L7 ■ Nom de domaine complet ■ Nouvelle disposition du pare-feu distribué et du pare-feu de passerelle <ul style="list-style-type: none"> ■ Catégories ■ Règles de services automatiques ■ Brouillons 	<p>Fonctionnalités de sécurité disponibles dans l'interface avancée uniquement :</p> <ul style="list-style-type: none"> ■ seuils du CPU et de mémoire ■ Pare-feu de pont ■ Règles de pare-feu distribué basées sur des adresses IP dans la source et la destination

Utilisation de l'interface de stratégie

Si vous décidez d'utiliser l'interface de stratégie, utilisez-la pour créer tous les objets. N'utilisez pas l'interface avancée pour créer des objets.

Vous pouvez utiliser l'interface avancée pour modifier les objets qui ont été créés dans l'interface de stratégie. Les paramètres d'un objet créé par une stratégie peuvent inclure un lien pour la **configuration avancée**. Ce lien vous dirige vers l'interface avancée dans laquelle vous pouvez ajuster la configuration. Vous pouvez également afficher les objets créés par la stratégie directement dans l'interface avancée. Cette icône  se trouve à côté des paramètres gérés par la stratégie, mais qui sont visibles dans l'interface avancée. Vous ne pouvez pas les modifier à partir de l'interface utilisateur avancée.

Où trouver les interfaces de stratégie et les interfaces avancées

Les interfaces basées sur les stratégies et les interfaces avancées s'affichent dans différentes parties de l'interface utilisateur de NSX Manager et utilisent des URI d'API différents.

Tableau 1-2. Interfaces de stratégie et interfaces avancées

Interface de stratégie	Interface avancée
<ul style="list-style-type: none"> ■ Onglet Mise en réseau ■ Onglet Sécurité ■ Onglet Inventaire ■ Onglet Planifier et dépanner 	Onglet Mise en réseau et sécurité avancées
URI d'API commençant par /policy/api	URI d'API commençant par /api

Note L'onglet **Système** est utilisé pour tous les environnements. Si vous modifiez des nœuds Edge, des clusters Edge ou des zones de transport, l'affichage de ces modifications peut prendre jusqu'à 5 minutes sur l'interface utilisateur basée sur la stratégie. Vous pouvez synchroniser immédiatement à l'aide de POST /policy/api/v1/infra/sites/default/enforcement-points/default?action=reload.

Pour plus d'informations sur l'utilisation de l'API de stratégie, reportez-vous au [Guide de démarrage de l'API de stratégie NSX-T](#).

Noms des objets créés dans la stratégie et les interfaces avancées

Les objets que vous créez ont des noms différents en fonction de l'interface utilisée pour les créer.

Tableau 1-3. Noms des objets

Objets créés à l'aide de l'interface de stratégie	Objets créés à l'aide de l'interface avancée
Segment	Commutateur logique
Passerelle de niveau 1	Routeur logique de niveau 1
Passerelle de niveau 0	Routeur logique de niveau 0
Groupe	NSGroup, ensembles d'adresses IP, ensembles d'adresses MAC
Stratégie de sécurité	Section de pare-feu
Règle	Règle de pare-feu
Pare-feu de passerelle	Edge Firewall

Workflows d'installation de NSX-T Data Center

2

Vous pouvez installer NSX-T Data Center sur vSphere ou des hôtes KVM. Vous pouvez également configurer un serveur Bare Metal afin d'utiliser NSX-T Data Center.

Pour installer ou configurer un hyperviseur ou un serveur Bare Metal, suivez les étapes recommandées dans les workflows.

Ce chapitre contient les rubriques suivantes :

- [Workflow NSX-T Data Center pour vSphere](#)
- [Workflow d'installation de NSX-T Data Center pour KVM](#)
- [Workflow de configuration de NSX-T Data Center pour le serveur sans système d'exploitation](#)

Workflow NSX-T Data Center pour vSphere

Utilisez la liste de contrôle pour suivre la progression de l'installation sur un hôte vSphere.

Suivez l'ordre des procédures recommandé.

- 1 Passez en revue la configuration requise pour l'installation de NSX Manager. Reportez-vous à la section [Chapitre 4 Installation de NSX Manager](#).
- 2 Configurez les ports et les protocoles nécessaires. Reportez-vous à la section [Ports et protocoles](#).
- 3 Installez NSX Manager. Reportez-vous à la section [Installer NSX Manager et les dispositifs disponibles](#).
- 4 Connectez-vous à l'instance de NSX Manager qui vient d'être créée. Reportez-vous à la section [Se connecter à l'instance de NSX Manager qui vient d'être créée](#).
- 5 Configurez un gestionnaire de calcul. Reportez-vous à la section [Ajouter un gestionnaire de calcul](#).
- 6 Déployez des nœuds NSX Manager supplémentaires pour former un cluster. Reportez-vous à la section [Déployer des nœuds NSX Manager pour constituer un cluster à partir de l'interface utilisateur](#).
- 7 Passez en revue la configuration requise pour l'installation de NSX Edge. Reportez-vous à la section [Conditions d'installation de NSX Edge](#).

- 8 Installez des instances de NSX Edge. Reportez-vous à [Installer un dispositif NSX Edge sur ESXi à l'aide de l'interface utilisateur graphique de vSphere](#).
- 9 Créez un cluster NSX Edge. Reportez-vous à la section [Créer un cluster NSX Edge](#).
- 10 Créez des zones de transport. Reportez-vous à la section [Créer des zones de transport](#).
- 11 Créez des nœuds de transport d'hôtes. Reportez-vous à la section [Créer un nœud de transport d'hôte autonome ou de serveur bare metal](#) ou [Configurer un nœud de transport d'hôte géré](#).

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.

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 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 les dispositifs NSX Edge et les hôtes.

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

Workflow d'installation de NSX-T Data Center pour KVM

Utilisez la liste de contrôle pour suivre la progression de l'installation sur un hôte KVM.

Suivez l'ordre des procédures recommandé.

- 1 Préparez votre environnement KVM. Reportez-vous à la section [Configurer KVM](#).
- 2 Passez en revue la configuration requise pour l'installation de NSX Manager. Reportez-vous à la section [Chapitre 4 Installation de NSX Manager](#).
- 3 Configurez les ports et les protocoles nécessaires. Reportez-vous à la section [Ports et protocoles](#).
- 4 Installez NSX Manager. Reportez-vous à la section [Installer NSX Manager sur KVM](#).
- 5 Connectez-vous à l'instance de NSX Manager qui vient d'être créée. Reportez-vous à la section [Se connecter à l'instance de NSX Manager qui vient d'être créée](#).
- 6 Configurez les modules tiers sur l'hôte KVM. Reportez-vous à la section [Installer des modules tiers sur un hôte KVM](#).
- 7 Déployez des nœuds NSX Manager supplémentaires pour former un cluster. Reportez-vous à la section [Déploiement de nœuds NSX Manager pour former un cluster à l'aide de la ligne de commande](#).

- 8 Passez en revue la configuration requise pour l'installation de NSX Edge. Reportez-vous à la section [Conditions d'installation de NSX Edge](#).
- 9 Installez des instances de NSX Edge. Reportez-vous à [Installer un dispositif NSX Edge sur un système Bare Metal](#).
- 10 Créez un cluster NSX Edge. Reportez-vous à la section [Créer un cluster NSX Edge](#).
- 11 Créez des zones de transport. Reportez-vous à la section [Créer des zones de transport](#).
- 12 Créez des nœuds de transport d'hôtes. Reportez-vous à la section [Créer un nœud de transport d'hôte autonome ou de serveur bare metal](#).

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.

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 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 les dispositifs NSX Edge et les hôtes.

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

Workflow de configuration de NSX-T Data Center pour le serveur sans système d'exploitation

Utilisez la liste de contrôle pour suivre la progression lors de la configuration du serveur sans système d'exploitation pour utiliser NSX-T Data Center.

Suivez l'ordre des procédures recommandé.

- 1 Passez en revue la configuration requise sans système d'exploitation. Reportez-vous à la section [Configuration requise système d'un serveur bare metal](#).
- 2 Configurez les ports et les protocoles nécessaires. Reportez-vous à la section [Ports et protocoles](#).
- 3 Installez NSX Manager. Reportez-vous à la section [Installer NSX Manager sur KVM](#).
- 4 Configurez des modules tiers sur le serveur sans système d'exploitation. Reportez-vous à la section [Installer les modules tiers sur un serveur bare metal](#).
- 5 Créez des nœuds de transport d'hôtes. Reportez-vous à la section [Créer un nœud de transport d'hôte autonome ou de serveur bare metal](#).

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.

- 6 Créez une interface d'application pour les charges de travail de serveur sans système d'exploitation. Reportez-vous à la section [Créer une interface d'application pour les charges de travail de serveur Bare Metal](#).

Préparation à l'installation

3

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](#)

Configuration système requise

Avant d'installer NSX-T Data Center, votre environnement doit répondre à des exigences spécifiques en matière de matériel et de ressources.

Configuration système requise pour le nœud de transport hôte et la machine virtuelle NSX Manager

Avant d'installer une instance de NSX Manager ou d'autres dispositifs NSX-T Data Center, assurez-vous que votre environnement répond à la configuration requise prise en charge.

Hyperviseurs pris en charge pour les nœuds de transport hôtes

Hyperviseur	Version	Cœurs de CPU	Mémoire
vSphere	Version de vSphere prise en charge	4	16 Go
CentOS Linux KVM	7.4, 7.5, 7.6	4	16 Go
Red Hat Enterprise Linux (RHEL) KVM	7.6, 7.5 et 7.4	4	16 Go
SUSE Linux Enterprise Server KVM	12 sp3, 12 sp4	4	16 Go
ubuntu KVM	16.04, 18.04.2 LTS	4	16 Go

Tableau 3-1. Hôtes pris en charge pour les instances de NSX Manager

Description de la prise en charge	Hyperviseur
ESXi	Pour connaître les hôtes pris en charge, consultez les Matrices d'interopérabilité des produits VMware .
KVM	RHEL 7.4 et Ubuntu 18.04.2 LTS Note À partir de NSX-T Data Center 2.5, un hôte Ubuntu exécutant la version 18.04.2 LTS peut être mis à niveau à partir de la version 16.04 ou est une nouvelle installation.

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 ultérieure. Pour plus d'informations, consultez *Description de vSphere Auto Deploy* dans la documentation *Installation et configuration de VMware ESXi*.

Attention Sur RHEL et Ubuntu, la commande `yum update` peut mettre à jour la version du noyau, qui ne doit pas être supérieure à la version 4.14.x 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 réseau d'hôtes d'hyperviseur

La carte réseau utilisée doit être compatible avec la version d'ESXi qui exécute NSX-T Data Center. Pour connaître les cartes réseau prises en charge, consultez le [Guide de compatibilité VMware](#).

Info-bulle Pour identifier rapidement les cartes compatibles dans le Guide de compatibilité, appliquez les critères suivants :

- Sous **Type de périphérique d'E/S**, sélectionnez **Réseau**.
- Facultativement, pour utiliser l'encapsulation GENEVE prise en charge, sous **Fonctionnalités**, sélectionnez les options GENEVE.
- Facultativement, pour utiliser le chemin de données amélioré, sélectionnez **Chemin de données optimisé N-VDS**.

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 1.1.0.26-10EM.670.0.0.7535516
Contrôleur Ethernet Intel(R) X710 pour 10GbE SFP+ Contrôleur Ethernet Intel(R) XL710 pour 40GbE QSFP+	i40en 1.2.0.0-10EM.670.0.0.8169922

Configuration requise des ressources de machine virtuelle NSX Manager

La taille du disque virtuel dynamique est 3,8 Go et celle du disque virtuel statique est 200 Go.

Taille du dispositif	Mémoire	vCPU	Espace disque	Version matérielle de machine virtuelle
NSX Manager très petit	8 Go	2	200 Go	10 ou une version ultérieure
Petite machine virtuelle NSX Manager	16 Go	4	200 Go	10 ou une version ultérieure
Machine virtuelle moyenne NSX Manager	24 Go	6	200 Go	10 ou une version ultérieure
Grande machine virtuelle NSX Manager	48 Go	12	200 Go	10 ou une version ultérieure

Note NSX Manager fournit plusieurs rôles qui nécessitaient auparavant des dispositifs distincts. Cela inclut le rôle de stratégie, le rôle de plan de gestion et le rôle central de plan de contrôle. Le rôle central de plan de contrôle a déjà été fourni par le dispositif NSX Controller.

- Vous pouvez utiliser la taille de ressource de machine virtuelle extra petite uniquement pour le dispositif Cloud Service Manager (CSM). Déployez CSM dans la taille de machine virtuelle extra petite ou supérieure, si nécessaire. Pour plus d'informations, reportez-vous à la section [Présentation du déploiement de NSX Cloud](#).
- La taille de dispositif Petite VM de NSX Manager est adaptée aux déploiements de laboratoire et de validation technique et ne doit pas être utilisée en production.
- La taille de dispositif Moyenne VM de NSX Manager est adaptée aux environnements de production types. Un cluster de gestion NSX-T formé à l'aide de cette taille de dispositif peut prendre en charge jusqu'à 64 hyperviseurs.
- La taille de dispositif Grande VM de NSX Manager est adaptée aux déploiements à grande échelle. Un cluster de gestion NSX-T formé à l'aide de cette taille de dispositif peut prendre en charge plus de 64 hyperviseurs.

Pour une échelle maximale utilisant la taille de dispositif Grande VM de NSX Manager, accédez à l'outil VMware Configuration Maximums à l'adresse <https://configmax.vmware.com/guest> et sélectionnez NSX-T Data Center dans la liste des produits.

Langues prises en charge

NSX Manager a été localisé en plusieurs langues : anglais, allemand, français, japonais, chinois simplifié, chinois traditionnel coréen, et espagnol.

Prise en charge du navigateur NSX Manager

Il est recommandé d'utiliser les navigateurs suivants avec NSX Manager.

Navigateur	Windows 10	Mac OS X 10.13, 10.14	Ubuntu 18.04
Google Chrome 76	Oui	Oui	Oui
Mozilla Firefox 68	Oui	Oui	Oui
Microsoft Edge 44	Oui		
Apple Safari 12		Oui	

Note

- Internet Explorer n'est pas pris en charge.
- La résolution minimale du navigateur prise en charge est 1 280x800 pixels.
- Langues prises en charge : NSX Manager a été localisé en plusieurs langues : anglais, allemand, français, japonais, chinois simplifié, chinois traditionnel coréen, et espagnol. Toutefois, comme la localisation de NSX Manager utilise les paramètres de langue du navigateur, assurez-vous que vos paramètres correspondent à la langue souhaitée. Il n'existe aucun paramètre de préférence de langue dans l'interface de NSX Manager.

Exigences de latence réseau

La latence réseau maximale entre des instances de NSX Manager dans un cluster NSX Manager est de 10 ms.

La latence réseau maximale entre des instances de NSX Manager et des nœuds de transport est de 150 ms.

Exigences de stockage

- La latence d'accès de disque maximale est inférieure à 10 ms.
- Il est recommandé de placer des instances de NSX Manager sur un stockage partagé.
- Le stockage doit être hautement disponible pour éviter une panne de stockage provoquant la mise en mode lecture seule de tous les systèmes de fichiers NSX Manager lors d'une panne de stockage.

Consultez la documentation de votre technologie de stockage sur la meilleure conception d'une solution de stockage hautement disponible.

Configuration système requise des machines virtuelles NSX Edge

Avant d'installer NSX Edge, assurez-vous que votre environnement répond à la configuration requise prise en charge.

Note Les conditions suivantes s'appliquent aux hôtes pour les nœuds NSX Edge :

- 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 NSX Edge, affichant un message d'erreur dans la console.

- Si le mode vSphere EVC est activé pour l'hôte pour la machine virtuelle NSX Edge, le CPU doit être Haswell ou version ultérieure.
- Seule la vNIC VMXNET3 est prise en charge pour la machine virtuelle NSX Edge.

Remarque concernant NSX Cloud Si vous utilisez NSX Cloud, notez que le NSX Public Cloud Gateway (PCG) est déployé dans une taille par défaut unique pour chaque cloud public pris en charge. Pour plus d'informations, reportez-vous à la section [Déployer la NSX Public Cloud Gateway](#) .

Configuration requise des ressources de machine virtuelle NSX Edge

Taille du dispositif	Mémoire	vCPU	Espace disque	Versión matérielle de machine virtuelle	Remarques
Petit NSX Edge	4 Go	2	200 Go	11 ou version ultérieure (vSphere 6.0 ou version ultérieure)	La taille de dispositif Petite VM de NSX Edge est adaptée aux déploiements de laboratoire et de validation technique. Note Les règles L7 ne sont pas réalisées sur une passerelle de niveau 1 si vous déployez une petite machine virtuelle NSX Edge.
NSX Edge moyen	8 Go	4	200 Go	11 ou version ultérieure (vSphere 6.0 ou version ultérieure)	La taille de dispositif Moyenne de NSX Edge est adaptée aux environnements de production typiques.
NSX Edge grand	32 Go	8	200 Go	11 ou version ultérieure (vSphere 6.0 ou version ultérieure)	La taille de dispositif Grande de NSX Edge convient aux environnements avec équilibrage de charge. Consultez Évolutivité des ressources d'équilibreur de charge dans le <i>Guide d'administration de NSX-T Data Center</i> .

Configuration requise de CPU pour les machines virtuelles NSX Edge

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.

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

Configuration requise pour NSX Edge sans système d'exploitation

Avant de configurer NSX Edge sans système d'exploitation, assurez-vous que votre environnement répond à la configuration requise prise en charge.

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

Configuration minimale requise

Mémoire	Cœurs de CPU	Espace disque
32 Go	8	200 Go

Configuration recommandée

Mémoire	Cœurs de CPU	Espace disque
256 Go	24	200 Go

Configuration requise de CPU DPDK pour NSX Edge sans système d'exploitation

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.

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

Configuration matérielle requise de NSX Edge sans système d'exploitation

Vérifiez que le matériel de NSX Edge sans système d'exploitation est répertorié dans cette URL <https://certification.ubuntu.com/server/models/?release=18.04%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 pour NSX Edge sans système d'exploitation

Type de carte réseau	Description	ID du périphérique PCI	Version de microprogramme
Mellanox ConnectX-4 EN	PCI_DEVICE_ID_MELLANOX_CONNECTX4	0x1013	12.21.1000 et supérieur
Mellanox ConnectX-4 Lx EN	PCI_DEVICE_ID_MELLANOX_CONNECTX4LX	0x1015	14.21.1000 et supérieur
Mellanox ConnectX-5	PCI_DEVICE_ID_MELLANOX_CONNECTX5	0x1017	16.21.1000 et supérieur
Mellanox ConnectX-5 EX	PCI_DEVICE_ID_MELLANOX_CONNECTX5EX	0x1019	16.21.1000 et supérieur
Intel XXV710	I40E_DEV_ID_25G_B	0x158A	6.0.1
	I40E_DEV_ID_25G_SFP28	0x158B	6.0.1
Intel X520/Intel 82599	IXGBE_DEV_ID_82599_KX4	0x10F7	s/o
	IXGBE_DEV_ID_82599_KX4_MEZZ	0x1514	s/o
		0x1517	s/o
	IXGBE_DEV_ID_82599_KR	0x10F8	s/o
	IXGBE_DEV_ID_82599_COMBO_BACKPLANE	0x000C	s/o
		0x10F9	s/o
	IXGBE_SUBDEV_ID_82599_KX4_KR_MEZZ	0x10FB	s/o
		0x11A9	s/o
	IXGBE_DEV_ID_82599_CX4	0x1F72	s/o
	IXGBE_DEV_ID_82599_SFP	0x17D0	s/o
	IXGBE_SUBDEV_ID_82599_SFP	0x0470	s/o
		0x1507	s/o
	IXGBE_SUBDEV_ID_82599_RNDC	0x154D	s/o
		0x154A	s/o
	IXGBE_SUBDEV_ID_82599_560FLR	0x1558	s/o
		0x1557	s/o
	IXGBE_SUBDEV_ID_82599_ECNA_DP	0x10FC	s/o
	IXGBE_DEV_ID_82599_SFP_EM	0x151C	s/o
	IXGBE_DEV_ID_82599_SFP_SF2		
	IXGBE_DEV_ID_82599_SFP_SF_QP		
	IXGBE_DEV_ID_82599_QSFP_SF_QP		
	IXGBE_DEV_ID_82599EN_SFP		
	IXGBE_DEV_ID_82599_XAUI_LOM		
	IXGBE_DEV_ID_82599_T3_LOM		

Type de carte réseau	Description	ID du périphérique PCI	Version de microprogramme
Intel X540	IXGBE_DEV_ID_X540T	0x1528	s/o
	IXGBE_DEV_ID_X540T1	0x1560	s/o
Intel X550	IXGBE_DEV_ID_X550T	0x1563	s/o
	IXGBE_DEV_ID_X550T1	0x15D1	s/o
Intel X710	I40E_DEV_ID_SFP_X710	0x1572	6.0.1
	I40E_DEV_ID_KX_C	0x1581	6.0.1
	I40E_DEV_ID_10G_BASE_T	0x1586	6.0.1
Intel XL710	I40E_DEV_ID_KX_B	0x1580	6.0.1
	I40E_DEV_ID_QSFP_A	0x1583	6.0.1
	I40E_DEV_ID_QSFP_B	0x1584	6.0.1
	I40E_DEV_ID_QSFP_C	0x1585	6.0.1
Cisco série VIC 1300	Carte d'interface virtuelle Cisco UCS 1300	0x0043	s/o

Note Pour toutes les cartes réseau prises en charge répertoriées ci-dessus, vérifiez que les adaptateurs multimédia et les câbles que vous utilisez suivent les types de support pris en charge par le fournisseur. Tout adaptateur multimédia ou câble non pris en charge par le fournisseur peut entraîner un comportement imprévisible, y compris l'incapacité de démarrer en raison d'un adaptateur multimédia non reconnu. Consultez la documentation du fournisseur de carte réseau pour plus d'informations sur les adaptateurs multimédia et les câbles pris en charge.

Configuration requise système d'un serveur bare metal

Avant de configurer le serveur bare metal, assurez-vous que votre serveur respecte la configuration requise de prise en charge.

Important L'utilisateur effectuant l'installation peut avoir besoin d'autorisations de commande `sudo` pour certaines des procédures. Reportez-vous à la section [Installer les modules tiers sur un serveur bare metal](#).

Configuration requise du serveur bare metal

Système d'exploitation	Version	Cœurs de CPU	Mémoire
CentOS Linux	7.4 (1708)	4	16 Go
	7.5		
Red Hat Enterprise Linux (RHEL)	7.6 (noyau : 3.10.0-957)	4	16 Go
	7.5		
	7.4 (noyau : 3.10.0-6**)		

Système d'exploitation	Version	Cœurs de CPU	Mémoire
SUSE Linux Enterprise Server	12 sp3, 12 sp4	4	16 Go
Ubuntu	16.04.2 LTS (noyau : 4.4.0-*) 18.04	4	16 Go

Note À partir de NSX-T Data Center 2.5, un hôte Ubuntu exécutant la version 18.04.2 LTS peut être mis à niveau à partir de la version 16.04 ou est une nouvelle installation.

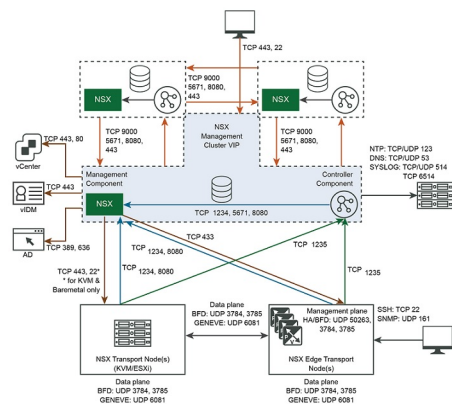
Configuration requise du conteneur Linux de système bare metal

Pour connaître la configuration requise du conteneur Linux de système bare metal, consultez le *Guide d'installation et d'administration de NSX Container Plug-in for OpenShift*.

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.

Note Les ports et protocoles requis doivent être ouverts sur les pare-feu d'hyperviseur physique et hôte.



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

- ESXi : netcpa, ESX-DP (dans le noyau)

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 aux protocoles](#) 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 3-2. Ports TCP et UDP utilisés par NSX Manager

Source	Cible	Port	Protocole	Description
NSX Manager, nœuds NSX Edge, nœuds de transport	NSX Manager	5671, 1234, 1235, 443	TCP	Messagerie NSX
NSX Manager, nœuds NSX Edge, nœuds de transport, vCenter Server	NSX Manager	8080	TCP	Référentiel HTTP d'installation-mise à niveau
NSX Manager	NSX Manager	9000, 5671, 1234, 443, 8080	TCP	Banque de données distribuée
NSX Manager	Serveurs DNS	53	TCP	DNS
NSX Manager	Serveurs DNS	53	UDP	DNS
NSX Manager	Serveurs SCP de gestion	22	TCP	SSH (télécharger le bundle de support, sauvegardes, etc.)
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

Tableau 3-2. Ports TCP et UDP utilisés par NSX Manager (suite)

Source	Cible	Port	Protocole	Description
NSX Manager	Serveurs Syslog	6514	TCP	Syslog
NSX Manager	Serveurs Syslog	6514	UDP	Syslog
NSX Manager	Serveurs d'autorité de certification intermédiaire et racine	80	TCP	Syslog (exporter sur TLS) Note Pour vérifier quel port TCP doit être utilisé pour récupérer les listes de révocation des certificats (CRL), vérifiez par rapport à l'URI CDP (CRL Distribution Point) de l'autorité de certification.
NSX Manager	Destination Traceroute	3343 - 3352	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.
Serveurs NTP	NSX Manager	123	UDP	NTP
Clients de gestion	NSX Manager	22	TCP	SSH (désactivé par défaut)
Clients de gestion	NSX Manager	443	TCP	Serveur NSX API
Serveurs SNMP	NSX Manager	161	UDP	SNMP

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 3-3. 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)
NSX Agent	Nœuds NSX Edge	5555	TCP	NSX Cloud - Agent sur l'instance communique avec la passerelle de NSX Cloud.

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

Source	Cible	Port	Protocole	Description
Nœuds NSX Edge	Serveurs DNS	53	UDP	DNS
Nœuds NSX Edge	Serveurs SCP ou SSH de gestion	22	TCP	SSH
Nœuds NSX Edge	NSX Manager	1235	TCP	Communication LCP (Lower Control Plane) vers CCP (Central Control Plane)
Nœuds NSX Edge	Nœuds NSX Edge	1167	TCP	DHCP principal
Nœuds NSX Edge	Nœuds NSX Edge	2480	TCP	Nestdb
Nœuds NSX Edge	Nœuds NSX Edge	6666	TCP	NSX Cloud - communications locales NSX Edge.
Nœuds NSX Edge	Nœuds NSX Edge	50263	UDP	Haute disponibilité
Nœuds NSX Edge	NSX Manager	443	TCP	HTTPS
Nœuds NSX Edge	NSX Manager	1234	TCP	Canal de messagerie NSX vers NSX Manager
Nœuds NSX Edge	NSX Manager	8080	TCP	NAPI, mise à niveau de NSX-T Data Center
Nœuds NSX Edge	Serveurs NTP	123	UDP	NTP
Nœuds NSX Edge	Serveur d'API OpenStack Nova	3000 - 9000	TCP	Proxy de métadonnées
Nœuds NSX Edge	Serveurs SNMP	161, 162	TCP	SNMP
Nœuds NSX Edge	Serveurs SNMP	161, 162	UDP	SNMP
Nœuds NSX Edge	Serveurs Syslog	514	TCP	Syslog
Nœuds NSX Edge	Serveurs Syslog	514	UDP	Syslog
Nœuds NSX Edge	Serveurs Syslog	6514	TCP	Syslog
Nœuds NSX Edge	Serveurs Syslog	6514	UDP	Syslog
Nœuds NSX Edge	Serveurs d'autorité de certification intermédiaire et racine	80	TCP	Syslog (exporter sur TLS)

Note Pour vérifier quel port TCP doit être utilisé pour récupérer les listes de révocation des certificats (CRL), vérifiez par rapport à l'URI CDP (CRL Distribution Point) de l'autorité de certification.

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

Source	Cible	Port	Protocole	Description
Nœuds NSX Edge	Destination Traceroute	33434 - 33523	UDP	Traceroute
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.
Serveurs NTP	Nœuds NSX Edge	123	UDP	NTP
Serveurs SNMP	Nœuds NSX Edge	161	UDP	SNMP

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

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

Tableau 3-4. Ports TCP et UDP utilisés par les hôtes ESXi et KVM

Source	Cible	Port	Protocole	Description
Hôte ESXi	NSX Manager	1235	TCP	Communication LCP (Local Control Plane) vers CCP (Central Control Plane)
Hôte ESXi	NSX Manager	1234	TCP	Canal de messagerie NSX vers NSX Manager Canal de communication AMQP vers NSX Manager
Hôte ESXi	NSX Manager	8080	TCP	Installer et mettre à niveau le référentiel HTTP
ESXi et hôte KVM	NSX Manager	443	TCP	Connexion de gestion et de provisionnement
ESXi et hôte KVM	NSX Manager	443	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	6081	UDP	Réseau de transport
Hôte KVM	NSX Manager	1234	TCP	Canal de messagerie NSX vers NSX Manager Canal de communication AMQP vers NSX Manager
Hôte du serveur Bare Metal	NSX Manager	5671, 1235, 1234, 8080	TCP	Canal de communication AMQP vers NSX Manager

Tableau 3-4. Ports TCP et UDP utilisés par les hôtes ESXi et KVM (suite)

Source	Cible	Port	Protocole	Description
Hôte KVM	NSX Manager	1235	TCP	Communication LCP (Local Control Plane) vers CCP (Central Control Plane)
Hôte KVM	NSX Manager	8080	TCP	Installer et mettre à niveau le référentiel HTTP
NSX Manager	Hôte ESXi	443	TCP	Connexion de gestion et de provisionnement
NSX Manager	Hôte KVM	443	TCP	Connexion de gestion et de provisionnement
Hôte	Serveurs Syslog	514	TCP	Syslog (reportez-vous à la documentation Syslog de l'hôte)
Hôte	Serveurs Syslog	514	UDP	Syslog (reportez-vous à la documentation Syslog de l'hôte)
Hôte	Serveurs Syslog	6514	TCP	Syslog (reportez-vous à la documentation Syslog de l'hôte)
Hôte	Serveurs Syslog	6514	UDP	Syslog (reportez-vous à la documentation Syslog de l'hôte)
Hôte	Serveurs d'autorité de certification intermédiaire et racine	80	TCP	Syslog (exporter sur TLS) Note Pour vérifier quel port TCP doit être utilisé pour récupérer les listes de révocation des certificats (CRL), vérifiez par rapport à l'URI CDP (CRL Distribution Point) de l'autorité de certification.
Noeud de transport NSX-T Data Center	Noeud de transport NSX-T Data Center	3784, 3785	UDP	Session BFD entre les TEP, dans le chemin de données, à l'aide de l'interface TEP

Installation de NSX Manager

4

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.

Pour la haute disponibilité, NSX-T Data Center prend en charge un cluster de gestion de trois instances de NSX Manager. Pour un environnement de production, le déploiement d'un cluster de gestion est recommandé. Pour un environnement de validation technique, vous pouvez déployer une seule instance de NSX Manager.

Dans un environnement vSphere, les fonctions suivantes sont prises en charge par NSX Manager :

- vCenter Server peut utiliser la fonction vMotion pour effectuer une migration en direct de NSX Manager sur des hôtes et des clusters.
- vCenter Server peut utiliser la fonction Storage vMotion pour effectuer une migration en direct de NSX Manager sur des hôtes et des clusters.
- vCenter Server peut utiliser la fonction Distributed Resource Scheduler pour rééquilibrer NSX Manager sur des hôtes et des clusters.
- vCenter Server peut utiliser la fonction d'anti-affinité pour gérer NSX Manager sur des hôtes et des clusters.

Exigences du déploiement, de la plate-forme et de l'installation de NSX Manager

Le tableau suivant décrit les 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 pour le nœud de transport hôte et la machine virtuelle NSX Manager.</p> <p>Sous ESXi, il est recommandé d'installer le dispositif NSX Manager sur un stockage partagé.</p>
Adresse IP	<p>Un système NSX Manager doit posséder une adresse IP statique. Vous ne pouvez pas modifier l'adresse IP après l'installation.</p>

Exigences	Description
Mot de passe du dispositif NSX-T Data Center	<ul style="list-style-type: none"> ■ Au moins 12 caractères ■ Au moins une lettre minuscule ■ Au moins une lettre majuscule ■ Au moins un chiffre ■ Au moins un caractère spécial ■ Au moins cinq caractères différents ■ Les règles de complexité de mot de passe par défaut sont appliquées par les arguments du module PAM Linux suivants : <ul style="list-style-type: none"> ■ <code>retry=3</code> : nombre maximal de fois qu'un nouveau mot de passe peut être entré, 3 fois au maximum pour cet argument, avant de renvoyer une erreur. ■ <code>minlen=12</code> : taille minimale acceptable pour le nouveau mot de passe. En plus du nombre de caractères dans le nouveau mot de passe, un crédit (de +1 dans la longueur) est donné pour chaque type de caractère différent (autre, supérieur, inférieur et chiffre). ■ <code>difok=0</code> : nombre minimal d'octets qui doivent être différents dans le nouveau mot de passe. Indique la similarité entre l'ancien et le nouveau mot de passe. Avec une valeur 0 attribuée à <code>difok</code>, il n'est pas nécessaire que l'ancien et le nouveau mot de passe soient différents. Une correspondance exacte est autorisée. ■ <code>lcredit=1</code> : crédit maximal pour avoir des lettres minuscules dans le nouveau mot de passe. Si vous avez au maximum 1 lettre minuscule, chaque lettre compte +1 pour répondre à la valeur <code>minlen</code> actuelle. ■ <code>ucredit=1</code> : crédit maximal pour avoir des lettres majuscules dans le nouveau mot de passe. Si vous avez au maximum 1 lettre majuscule, chaque lettre compte +1 pour répondre à la valeur <code>minlen</code> actuelle. ■ <code>dcredit=1</code> : crédit maximal pour avoir des chiffres dans le nouveau mot de passe. Si vous avez au maximum 1 chiffre, chaque chiffre compte +1 pour répondre à la valeur <code>minlen</code> actuelle. ■ <code>ocredit=1</code> : crédit maximal pour avoir d'autres caractères dans le nouveau mot de passe. Si vous avez au maximum 1 autre caractère, chaque caractère compte +1 pour répondre à la valeur <code>minlen</code> actuelle. ■ <code>enforce_for_root</code> : le mot de passe est défini pour l'utilisateur racine. <p>Note Pour plus d'informations sur le module PAM Linux pour vérifier le mot de passe par rapport aux mots du dictionnaire, reportez-vous à la page man.</p> <p>Par exemple, évitez les mots de passe simples et systématiques tels que VMware123!123 ou VMware12345. Les mots de passe qui répondent aux normes de complexité ne sont pas simples et systématiques, mais il s'agit d'une combinaison de lettres, de caractères spéciaux et de chiffres, comme VMware123!45, VMware1!2345 ou VMware@1az23x.</p>
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 (« - ») ou de caractères spéciaux comme un point (« . »). Si le nom d'hôte contient un caractère non valide ou des caractères spéciaux, après le déploiement, le nom d'hôte sera défini sur nsx-manager.</p> <p>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>

Exigences	Description
VMware Tools	VMTools est installé sur la machine virtuelle NSX Manager exécutée sur ESXi. Ne supprimez pas ou ne mettez pas VMTools à niveau.
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. ■ Assurez-vous qu'une banque de données est configurée et accessible sur l'hôte ESXi. ■ Vérifiez que vous disposez de l'adresse IP et de la passerelle, des adresses IP du serveur DNS, de la liste de recherche de domaines et de l'adresse IP du serveur NTP que NSX Manager utilisera. ■ Créez le réseau du groupe de ports de machines virtuelles cible, si celui-ci n'existe pas déjà. Placez les dispositifs NSX-T Data Center sur un réseau de machines virtuelles de gestion. <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'adressage IP IPv4 NSX Manager.
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 Client ou depuis la ligne de commande, les valeurs de propriété OVA/OVF, telles que les noms d'utilisateur et les mots de passe, ne sont pas validées avant la mise sous tension de la machine virtuelle. Toutefois, le champ Adresse IP statique est un champ obligatoire pour installer NSX Manager.

- 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 la configuration requise de complexité, vous devez vous connecter à NSX Manager via SSH ou sur la console en tant qu'utilisateur **admin** avec le mot de passe **default**. 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.

Configuration de NSX Manager pour l'accès par le serveur DNS

Par défaut, les nœuds de transport accèdent à des instances de NSX Manager en fonction de leurs adresses IP. Toutefois, cela peut être basé également sur les noms DNS des instances de NSX Manager.

En activant l'utilisation du nom de domaine complet (DNS) sur des instances de NSX Manager, l'adresse IP des gestionnaires peut changer sans affecter les nœuds de transport.

Vous activez l'utilisation du nom de domaine complet en publiant les noms de domaine complets des instances de NSX Manager.

Note L'activation de l'utilisation du nom de domaine complet (DNS) sur des instances de NSX Manager est requise pour les déploiements multisite de Lite, et NSX Cloud. (Il est facultatif pour tous les autres types de déploiement.) Reportez-vous à la section *Déploiement multisite de NSX-T Data Center* du *Guide d'administration de NSX-T Data Center* et à la section [Chapitre 13 Installation de composants NSX Cloud](#) de ce guide.

Publication des noms de domaine complets des instances de NSX Manager

Après l'installation des composants principaux de NSX-T Data Center et de CSM, pour activer NAT à l'aide du nom de domaine complet, vous devez configurer les entrées de recherche directe et inversée pour les nœuds de gestionnaire sur le serveur DNS.

Important Il est vivement recommandé de configurer les entrées de recherche directe et inversée pour le nom de domaine complet des instances de NSX Manager avec une durée de vie courte (par exemple, 600 secondes).

Vous devez également activer la publication du nom de domaine complet de 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.

Note Après la publication des noms de domaine complets, validez l'accès par les nœuds de transport comme décrit dans la section suivante.

Validation de l'accès via un nom de domaine complet par les nœuds de transport

Après la publication des noms de domaine complets des instances de NSX Manager, vérifiez que les nœuds de transport accèdent correctement aux instances de NSX Manager.

À l'aide de SSH, connectez-vous à un nœud de transport tel qu'un hyperviseur ou un nœud Edge, puis exécutez la commande d'interface de ligne de commande `get controllers`.

Exemple de réponse :

Controller IP	Port	SSL	Status	Is Physical Master	Session State	Controller FQDN
192.168.60.5	1235	enabled	connected	true	up	nsxmgr.corp.com

Ce chapitre contient les rubriques suivantes :

- [Modification de l'expiration du mot de passe administrateur par défaut](#)

Modification de l'expiration du mot de passe administrateur par défaut

Par défaut, le mot de passe administrateur des dispositifs NSX Manager et NSX Edge expire après 90 jours. Toutefois, vous pouvez réinitialiser la période d'expiration après l'installation et la configuration initiales.

Si le mot de passe expire, vous ne pourrez plus vous connecter et gérer les composants. De plus, toute tâche ou appel d'API nécessitant l'exécution du mot de passe administrateur échouera. Si votre mot de passe expire, consultez l'article 70691 de la base de connaissances [NSX-T admin password expired \(Le mot de passe administrateur de NSX-T est expiré\)](#).

Procédure

- 1 Utilisez un programme sécurisé pour vous connecter à la console de CLI de NSX.
- 2 Réinitialisez la période d'expiration.

Vous pouvez définir une période d'expiration comprise entre 1 et 9 999 jours.

```
nsxcli> set user admin password-expiration <1 - 9999>
```

Note Vous pouvez également utiliser des commandes API pour définir la période d'expiration du mot de passe administrateur.

- 3 (Facultatif) Vous pouvez désactiver l'expiration du mot de passe pour que le mot de passe n'expire jamais.

```
nsxcli> clear user audit password-expiration
```

Installation de NSX-T Data Center sur vSphere

5

Vous pouvez installer des composants de NSX-T Data Center, NSX Manager et NSX Edge à l'aide de l'interface utilisateur ou de la ligne de commande.

Assurez-vous que vous disposez de la version de vSphere prise en charge. Voir [Prise en charge de vSphere](#).

Ce chapitre contient les rubriques suivantes :

- [Installer NSX Manager et les dispositifs disponibles](#)
- [Configurer une adresse IP virtuelle \(VIP\) pour un cluster](#)
- [Désactiver des snapshots sur des dispositifs NSX-T](#)

Installer NSX Manager et les dispositifs disponibles

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

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

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](#).
- Assurez-vous qu'une banque de données est configurée et accessible sur l'hôte ESXi.
- Vérifiez que vous disposez de l'adresse IP et de la passerelle, des adresses IP du serveur DNS, de la liste de recherche de domaines et de l'adresse IP du serveur NTP que NSX Manager utilisera.
- Créez le réseau du groupe de ports de machines virtuelles cible, si celui-ci n'existe pas déjà. Placez les dispositifs NSX-T Data Center sur un réseau de machines virtuelles de gestion.

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

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

Procédure

- 1 Localisez le fichier OVA de NSX-T Data Center sur le portail de téléchargement de VMware.
Copiez l'URL de téléchargement ou téléchargez le fichier OVA.
- 2 Cliquez avec le bouton droit et sélectionnez **Déployer un modèle OVF** pour démarrer l'Assistant d'installation.
- 3 Entrez l'URL de téléchargement du fichier OVA ou accédez au fichier OVA, puis cliquez sur **Suivant**.
- 4 Entrez un nom et un emplacement pour la machine virtuelle NSX Manager, puis cliquez sur **Suivant**.

Le nom entré s'affiche dans l'inventaire de vSphere et de vCenter Server.

- 5 Sélectionnez une ressource de calcul pour le dispositif NSX Manager et cliquez sur **Suivant**.
 - ◆ Pour installer sur un hôte ESXi géré par vCenter, sélectionnez un hôte sur lequel déployer le dispositif NSX Manager.
 - ◆ Pour installer sur un hôte ESXi autonome, sélectionnez l'hôte sur lequel déployer le dispositif NSX Manager.
- 6 Examinez et vérifiez les détails du modèle OVF et cliquez sur **Suivant**.
- 7 Spécifiez la taille de configuration du déploiement et cliquez sur **Suivant**.
Le panneau Description sur le côté droit de l'assistant affiche les détails de la configuration sélectionnée.
- 8 Spécifiez le stockage pour les fichiers de configuration et de disque.
 - a Sélectionnez le format de disque virtuel.
 - b Sélectionnez la stratégie de stockage VM.
 - c Spécifiez la banque de données pour stocker les fichiers du dispositif NSX Manager.
 - d Cliquez sur **Suivant**.
- 9 Sélectionnez un réseau de destination pour chaque réseau source.
- 10 Sélectionnez le groupe de ports ou le réseau de destination du dispositif NSX Manager.
- 11 Configurez les paramètres de l'allocation d'adresses IP.
 - a Pour l'allocation d'adresses IP, spécifiez **Statique – Manuelle**.
 - b Pour le protocole IP, sélectionnez **IPv4**.
- 12 Cliquez sur **Suivant**.

Les étapes suivantes sont toutes situées dans la section Personnaliser le modèle de l'assistant Déployer un modèle OVF.

- 13** Dans la section Application, entrez les mots de passe de la racine du système, de l'administrateur de l'interface de ligne de commande et d'audit pour NSX Manager. Les informations d'identification de la **racine** et de l'**administrateur** sont obligatoires.

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

- Au moins 12 caractères
- Au moins une lettre minuscule
- Au moins une lettre majuscule
- Au moins un chiffre
- Au moins un caractère spécial
- Au moins cinq caractères différents
- Les règles de complexité de mot de passe par défaut sont appliquées par les arguments du module PAM Linux suivants :
 - `retry=3` : nombre maximal de fois qu'un nouveau mot de passe peut être entré, 3 fois au maximum pour cet argument, avant de renvoyer une erreur.
 - `minlen=12` : taille minimale acceptable pour le nouveau mot de passe. En plus du nombre de caractères dans le nouveau mot de passe, un crédit (de +1 dans la longueur) est donné pour chaque type de caractère différent (autre, supérieur, inférieur et chiffre).
 - `difok=0` : nombre minimal d'octets qui doivent être différents dans le nouveau mot de passe. Indique la similarité entre l'ancien et le nouveau mot de passe. Avec une valeur 0 attribuée à `difok`, il n'est pas nécessaire que l'ancien et le nouveau mot de passe soient différents. Une correspondance exacte est autorisée.
 - `lcredit=1` : crédit maximal pour avoir des lettres minuscules dans le nouveau mot de passe. Si vous avez au maximum 1 lettre minuscule, chaque lettre compte +1 pour répondre à la valeur `minlen` actuelle.
 - `ucredit=1` : crédit maximal pour avoir des lettres majuscules dans le nouveau mot de passe. Si vous avez au maximum 1 lettre majuscule, chaque lettre compte +1 pour répondre à la valeur `minlen` actuelle.
 - `dcredit=1` : crédit maximal pour avoir des chiffres dans le nouveau mot de passe. Si vous avez au maximum 1 chiffre, chaque chiffre compte +1 pour répondre à la valeur `minlen` actuelle.
 - `ocredit=1` : crédit maximal pour avoir d'autres caractères dans le nouveau mot de passe. Si vous avez au maximum 1 autre caractère, chaque caractère compte +1 pour répondre à la valeur `minlen` actuelle.

- `enforce_for_root` : le mot de passe est défini pour l'utilisateur racine.

Note Pour plus d'informations sur le module PAM Linux pour vérifier le mot de passe par rapport aux mots du dictionnaire, reportez-vous à la page man.

Par exemple, évitez les mots de passe simples et systématiques tels que **VMware123!123** ou **VMware12345**. Les mots de passe qui répondent aux normes de complexité ne sont pas simples et systématiques, mais il s'agit d'une combinaison de lettres, de caractères spéciaux et de chiffres, comme **VMware123!45**, **VMware1!2345** ou **VMware@1az23x**.

- 14** Dans la section Paramètres facultatifs, laissez les champs de mot de passe vides. Cela permet d'éviter le risque de compromission des mots de passe définis pour les rôles VMC par un utilisateur qui a accès à vCenter Server. Lors du déploiement de VMC pour NSX-T Data Center, ce champ est utilisé en interne pour définir des mots de passe pour les rôles Administrateur Cloud et Audit Cloud.

- 15** Dans la section Propriétés du réseau, entrez le nom d'hôte de NSX Manager.

Note Le nom d'hôte doit être un nom de domaine valide. Assurez-vous que chaque partie du nom d'hôte (domaine/sous-domaine) séparée par un point commence par un caractère alphabétique.

- 16** Sélectionnez un **Nom de rôle** pour le dispositif. Le rôle par défaut est **NSX Manager**.

- Pour installer un dispositif NSX Manager, sélectionnez le rôle **NSX Manager**.
- Pour installer un dispositif Cloud Service Manager (CSM) pour un déploiement de NSX Cloud, sélectionnez le rôle **nsx-cloud-service-manager**.

Pour plus d'informations, reportez-vous à la section [Présentation du déploiement de NSX Cloud](#).

- 17** (Champs obligatoires) Entrez la passerelle par défaut, l'adresse IPv4 du réseau de gestion et le masque du réseau de gestion.

Important Si vous laissez le champ Adresse IPv4 du réseau de gestion vide sans entrer d'adresse IP statique, aucune adresse IP n'est attribuée à NSX Manager lors du déploiement du dispositif. Vous ne pouvez pas accéder à NSX Manager lorsqu'il se met sous tension. La solution consiste à redéployer le dispositif NSX Manager.

- 18** Dans la section DNS, entrez la liste Serveur DNS et la liste Recherche de domaine.

- 19** Dans la section Configuration des services, entrez la liste Serveurs NTP.

Vous pouvez également activer le service SSH et autoriser la connexion SSH racine. (Non recommandé.)

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

L'installation peut prendre 7 à 8 minutes.

- 21** Pour des performances optimales, réservez de la mémoire pour le dispositif.

Définissez la réservation de manière à garantir que NSX Manager dispose de suffisamment de mémoire pour s'exécuter efficacement. Reportez-vous à la section [Configuration système requise pour le nœud de transport hôte et la machine virtuelle NSX Manager](#).

- 22** À partir de vSphere Client, ouvrez la console de machine virtuelle pour suivre le processus de démarrage du nœud.

- 23** Dès que le nœud 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.

- 24** Entrez la commande `get services` pour vérifier que tous les services par défaut sont en cours d'exécution.

Les services suivants ne sont pas requis par défaut et ne démarrent pas automatiquement.

- `liagent`
- `migration-coordinator` : ce service est utilisé uniquement lors de l'exécution du coordinateur de migration. Reportez-vous au *Guide du coordinateur de migration de NSX-T Data Center* avant de démarrer ce service.
- `snmp` : pour plus d'informations sur le démarrage de SNMP, reportez-vous à *Protocole simple de gestion de réseau* dans le *Guide d'administration de NSX-T Data Center*.
- `nsx-message-bus` : ce service n'est pas utilisé dans NSX-T Data Center 3.0.

- 25** Vérifiez que votre nœud NSX Manager ou Gestionnaire global dispose de la connectivité requise.

Assurez-vous que vous pouvez effectuer les tâches suivantes.

- Effectuer un test ping de votre nœud à partir d'une autre machine.
- Le nœud peut effectuer un test ping de sa passerelle par défaut.
- Le nœud peut effectuer un test ping des hôtes d'hyperviseur qui se trouvent dans le même réseau à l'aide de l'interface de gestion.
- Le nœud 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 nœud.

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

Étape suivante

Connectez-vous à NSX Manager à partir d'un navigateur Web pris en charge. Reportez-vous à la section [Se connecter à l'instance de NSX Manager qui vient d'être créée](#).

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](#).
- Assurez-vous qu'une banque de données est configurée et accessible sur l'hôte ESXi.
- Vérifiez que vous disposez de l'adresse IP et de la passerelle, des adresses IP du serveur DNS, de la liste de recherche de domaines et de l'adresse IP du serveur NTP que NSX Manager utilisera.
- Créez le réseau du groupe de ports de machines virtuelles cible, si celui-ci n'existe pas déjà. Placez les dispositifs NSX-T Data Center sur un réseau de machines virtuelles de gestion.

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

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

Procédure

- 1 Exécutez la commande `ovftool` avec les paramètres appropriés.

Le processus varie selon que l'hôte est autonome ou géré par vCenter Server.

- Pour un hôte autonome :
 - Exemple de Windows :

```
C:\Program Files\VMware\VMware OVF Tool>ovftool \
--sourceType=OVA \
--name=nsx-manager \
--deploymentOption=medium \
--X:injectOvfEnv \
--X:logFile=<filepath>\nsxovftool.log \
--allowExtraConfig \
--datastore=<datastore name> \
--network=<network name> \
```



```

--acceptAllEulas \
--noSSLVerify \
--diskMode=thin \
--powerOn \
--prop:"nsx_role=NSX Manager" \
--prop:"nsx_ip_0=10.168.110.75" \
--prop:"nsx_netmask_0=255.255.255.0" \
--prop:"nsx_gateway_0=10.168.110.1" \
--prop:"nsx_dns1_0=10.168.110.10" \
--prop:"nsx_domain_0=corp.local" \
--prop:"nsx_ntp_0=10.168.110.10" \
--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-manager" \
<nsx-unified-appliance-release>.ova \
vi://root:<password>@10.168.110.51

```

Note Le bloc de code Windows ci-dessus utilise la barre oblique inverse (\) pour indiquer la suite de la ligne de commande. Dans l'utilisation réelle, omettez la barre oblique inverse et placez l'intégralité de la commande sur une seule ligne.

Note Dans l'exemple ci-dessus, 10.168.110.51 est l'adresse IP de la machine hôte sur laquelle NSX Manager doit être déployé.

Note Dans l'exemple ci-dessus, --deploymentOption est défini sur la taille Moyenne par défaut. Pour connaître les autres tailles prises en charge, reportez-vous à la section [Configuration système requise pour le nœud de transport hôte et la machine virtuelle NSX Manager](#).

■ Exemple de Linux :

```

mgrformfactor="small"
ipAllocationPolicy="fixedPolicy"
mgrdatastore="QNAP-Share-VMs"
mgrnetwork="Management-VLAN-210"

mgrname01="nsx-manager-01"
mgrhostname01="nsx-manager-01"
mgrip01="192.168.210.121"

mgrnetmask="255.255.255.0"
mgrgw="192.168.210.254"
mgrdns="192.168.110.10"
mgrntp="192.168.210.254"
mgrpasswd="<password>"
mgrssh="<True|False>"
mgrroot="<True|False>"
logLevel="trivia"

```

```

mgresxhost01="192.168.110.113"

ovftool --noSSLVerify --skipManifestCheck --powerOn \
--deploymentOption=$mgrformfactor \
--diskMode=thin \
--acceptAllEulas \
--allowExtraConfig \
--ipProtocol=IPv4 \
--ipAllocationPolicy=$ipAllocationPolicy \
--datastore=$mgrdatastore \
--network=$mgrnetwork \
--name=$mgrname01 \
--prop:nsx_hostname=$mgrhostname01 \
--prop:nsx_role="NSX Manager" \
--prop:nsx_ip_0=$mgrip01 \
--prop:nsx_netmask_0=$mgrnetmask \
--prop:nsx_gateway_0=$mgrgw \
--prop:nsx_dns1_0=$mgrdns \
--prop:nsx_ntp_0=$mgrntp \
--prop:nsx_passwd_0=$mgrpasswd \
--prop:nsx_cli_passwd_0=$mgrpasswd \
--prop:nsx_cli_audit_passwd_0=$mgrpasswd \
--prop:nsx_isSSEnabled=$mgrssh \
--prop:nsx_allowSSHRootLogin=$mgrroot \
--X:logFile=nsxt-manager-ovf.log \
--X:logLevel=$logLevel \
/home/<user/nsxt-autodeploy/<nsx-unified-appliance-release>.ova \
vi://root:<password>@<mgresxhost01>

```

Le résultat doit ressembler à ce qui suit :

```

Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://root:<password>@10.168.110.51
Deploying to VI: vi://root:<password>@10.168.110.51
Transfer Completed
Powering on VM: NSX Manager
Task Completed
Completed successfully

```

- Pour un hôte géré par vCenter Server :
- Exemple de Windows :

```

C:\Users\Administrator\Downloads>ovftool
--name=nsx-manager \
--deploymentOption=medium \
--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=10.168.110.75" \
--prop:"nsx_netmask_0=255.255.255.0" \
--prop:"nsx_gateway_0=10.168.110.1" \
--prop:"nsx_dns1_0=10.168.110.10" \
--prop:"nsx_domain_0=corp.local" \
--prop:"nsx_ntp_0=10.168.110.10" \
--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=$mgrpasswd \
--prop:"nsx_hostname=nsx-manager" \
<nsx-unified-appliance-release>.ova \
vi://administrator@vsphere.local:<password>@10.168.110.24/?ip=10.168.110.51

```

Note Le bloc de code Windows ci-dessus utilise la barre oblique inverse (\) pour indiquer la suite de la ligne de commande. Dans l'utilisation réelle, omettez la barre oblique inverse et placez l'intégralité de la commande sur une seule ligne.

Note Dans l'exemple ci-dessus, --deploymentOption est défini sur la taille Moyenne par défaut. Pour connaître les autres tailles prises en charge, reportez-vous à la section [Configuration système requise pour le nœud de transport hôte et la machine virtuelle NSX Manager](#).

■ Exemple de Linux :

```

mgrformfactor="small"
ipAllocationPolicy="fixedPolicy"
mgrdatastore="QNAP-Share-VMs"
mgrnetwork="Management-VLAN-210"

mgrname01="nsx-manager-01"
mgrhostname01="nsx-manager-01"
mgrip01="192.168.210.121"

mgrnetmask="255.255.255.0"
mgrgw="192.168.210.254"
mgrdns="192.168.110.10"
mgrntp="192.168.210.254"
mgrpasswd="<password>"
mgrssh="<True|False>"
mgrroot="<True|False>"
logLevel="trivia"

vadmin="administrator@vsphere.local"
vcpass="<password>"
vcip="192.168.110.151"
mgresxhost01="192.168.110.113"

```

```

ovftool --noSSLVerify --skipManifestCheck --powerOn \
--deploymentOption=$mgrformfactor \
--diskMode=thin \
--acceptAllEulas \
--allowExtraConfig \
--ipProtocol=IPv4 \
--ipAllocationPolicy=$ipAllocationPolicy \
--datastore=$mgrdatastore \
--network=$mgrnetwork \
--name=$mgrname01 \
--prop:nsx_hostname=$mgrhostname01 \
--prop:nsx_role="NSX Manager" \
--prop:nsx_ip_0=$mgrip01 \
--prop:nsx_netmask_0=$mgrnetmask \
--prop:nsx_gateway_0=$mgrgw \
--prop:nsx_dns1_0=$mgrdns \
--prop:nsx_ntp_0=$mgrntp \
--prop:nsx_passwd_0=$mgrpasswd \
--prop:nsx_cli_passwd_0=$mgrpasswd \
--prop:nsx_cli_audit_passwd_0=$mgrpasswd \
--prop:nsx_isSSHEnabled=$mgrssh \
--prop:nsx_allowSSHRootLogin=$mgrroot \
--X:logFile=nsxt-manager-ovf.log \
--X:logLevel=$logLevel \
/home/<user/nsxt-autodeploy/<nsx-unified-appliance-release>.ova \
vi://$vcadmin:$vcpass@$vcip/?ip=$mgresxhost01

```

Le résultat doit ressembler à ce qui suit :

```

Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://administrator@vsphere.local@10.168.110.24:443/
Deploying to VI: vi://administrator@vsphere.local@10.168.110.24:443/
Transfer Completed
Powering on VM: NSX Manager
Task Completed
Completed successfully

```

- 2 Vous pouvez également exécuter l'outil OVF en mode de détection pour afficher le contenu d'une source. Les modules OVA et OVF peuvent être détectés parmi une liste d'autres types de sources pris en charge. Vous pouvez utiliser les informations renvoyées par le mode de sondage pour configurer les déploiements.

```
$> \ovftool --allowExtraConfig <OVA path or URL>
```

Où,--allowExtraConfig est le type de dispositif pris en charge pour Cloud Service Manager (CSM).

- 3 Pour des performances optimales, réservez de la mémoire pour le dispositif.

Définissez la réservation de manière à garantir que NSX Manager dispose de suffisamment de mémoire pour s'exécuter efficacement. Reportez-vous à la section [Configuration système requise pour le nœud de transport hôte et la machine virtuelle NSX Manager](#).

- 4 À partir de vSphere Client, ouvrez la console de machine virtuelle pour suivre le processus de démarrage du nœud.
- 5 Dès que le nœud 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.
- 6 Vérifiez que votre nœud NSX Manager ou Gestionnaire global dispose de la connectivité requise.

Assurez-vous que vous pouvez effectuer les tâches suivantes.

- Effectuer un test ping de votre nœud à partir d'une autre machine.
- Le nœud peut effectuer un test ping de sa passerelle par défaut.
- Le nœud peut effectuer un test ping des hôtes d'hyperviseur qui se trouvent dans le même réseau à l'aide de l'interface de gestion.
- Le nœud 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 nœud.

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

Étape suivante

Connectez-vous à NSX Manager à partir d'un navigateur Web pris en charge. Reportez-vous à la section [Se connecter à l'instance de NSX Manager qui vient d'être créée](#).

Configurer NSX-T Data Center pour afficher le menu GRUB au démarrage

La configuration du dispositif NSX-T Data Center pour afficher le menu GRUB au démarrage est requise pour réinitialiser le mot de passe racine du dispositif NSX-T Data Center.

Important Si vous n'effectuez pas la configuration après le déploiement du dispositif et que vous oubliez le nom d'utilisateur racine, le nom d'utilisateur d'administrateur ou le mot de passe d'audit, il devient impossible de réinitialiser ce dernier.

Procédure

- 1 Connectez-vous à la machine virtuelle en tant qu'utilisateur racine.
- 2 Modifiez la valeur du paramètre GRUB_HIDDEN_TIMEOUT dans le fichier `/etc/default/grub`.

```
GRUB_HIDDEN_TIMEOUT=2
```

- 3 (Facultatif) Modifiez le mot de passe GRUB dans le fichier `/etc/grub.d/40_custom`.

Le mot de passe par défaut est `VMware1`.

- 4 Mettez à jour la configuration GRUB.

`update-grub`

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. Vous y apprendrez également comment participer au programme et le quitter.

Conditions préalables

Vérifiez que NSX Manager est installé. Reportez-vous à la section [Installer NSX Manager et les dispositifs disponibles](#).

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 Lisez, puis acceptez les conditions du CLUF.
- 3 Indiquez si vous voulez rejoindre le Programme d'amélioration du produit de VMware.
- 4 Cliquez sur **Enregistrer**

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 collecter des informations sur le cluster à partir de vCenter Server.

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

`Extension.Register extension`

`Extension.Unregister extension`

`Extension.Update extension`

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

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

Conditions préalables

- Vérifiez que vous utilisez la version de vSphere prise en charge. Voir [Version de vSphere prise en charge](#)
- Communication IPv6 et IPv4 avec vCenter Server.
- Vérifiez que vous utilisez le nombre recommandé de gestionnaires de calcul. Reportez-vous à la section <https://configmax.vmware.com/home>.

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

3 Indiquez les détails des gestionnaires de calcul.

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

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

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

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

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

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

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

Résultats

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

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

Une fois l'enregistrement de l'instance de vCenter Server terminé, ne mettez pas hors tension et ne supprimez pas la machine virtuelle NSX Manager sans supprimer d'abord le gestionnaire de calcul. Dans le cas contraire, lorsque vous déploierez une nouvelle instance de NSX Manager, vous ne pourrez plus enregistrer la même instance de vCenter Server. Vous obtiendrez l'erreur indiquant que l'instance de vCenter Server est déjà enregistrée avec une autre instance de NSX Manager.

Note Une fois qu'un gestionnaire de calcul vCenter Server (VC) a été ajouté avec succès, il ne peut pas être supprimé si vous avez effectué l'une des actions suivantes :

- Machines virtuelles de service déployées sur un hôte ou un cluster dans le VC à l'aide de l'insertion de services NSX.
- Vous utilisez l'interface utilisateur de NSX Manager pour déployer des machines virtuelles NSX Edge, des machines virtuelles NSX Intelligence ou des nœuds NSX Manager sur un hôte ou un cluster dans le VC.

Si vous tentez d'effectuer l'une de ces actions et que vous rencontrez une erreur (par exemple, l'installation a échoué), vous pouvez supprimer le VC si vous n'avez effectué aucune des actions répertoriées ci-dessus.

Vous pouvez également supprimer le VC ensuite :

- Tous les nœuds de transport ne sont pas préparés.
- Les déploiements de toutes les machines virtuelles de service, de la machine virtuelle NSX Intelligence, de toutes les machines virtuelles NSX Edge et des nœuds NSX Manager sont annulés.

Cette restriction s'applique à une nouvelle installation de NSX-T Data Center 2.5.x ainsi qu'à une mise à niveau.

Déployer des nœuds NSX Manager pour constituer un cluster à partir de l'interface utilisateur

Vous pouvez déployer plusieurs nœuds NSX Manager pour assurer la fiabilité et la haute disponibilité.

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

Note Le déploiement de plusieurs nœuds NSX Manager à l'aide de l'interface utilisateur est pris en charge uniquement sur les hôtes ESXi gérés par vCenter Server.

Tous les détails de référentiel et le mot de passe du premier nœud NSX Manager déployé sont synchronisés avec les nœuds nouvellement déployés dans le cluster.

Conditions préalables

- Vérifiez qu'un nœud NSX Manager est installé. Reportez-vous à la section [Installer NSX Manager et les dispositifs disponibles](#).

- Vérifiez qu'un gestionnaire de calcul est configuré. Reportez-vous à la section [Ajouter un gestionnaire de calcul](#).
- 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](#).
- Assurez-vous qu'une banque de données est configurée et accessible sur l'hôte ESXi.
- Vérifiez que vous disposez de l'adresse IP et de la passerelle, des adresses IP du serveur DNS, de la liste de recherche de domaines et de l'adresse IP du serveur NTP que NSX Manager utilisera.
- Créez le réseau du groupe de ports de machines virtuelles cible, si celui-ci n'existe pas déjà. Placez les dispositifs NSX-T Data Center sur un réseau de machines virtuelles de gestion.

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

Procédure

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

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

Option	Description
Nom d'utilisateur de la ligne de commande et confirmation du mot de passe	<p>Définissez le mot de passe CLI et la confirmation de celui-ci pour le nouveau nœud.</p> <p>Votre mot de passe doit respecter les indications relatives au niveau de sécurité du mot de passe.</p> <ul style="list-style-type: none"> ■ Au moins 12 caractères ■ Au moins une lettre minuscule ■ Au moins une lettre majuscule ■ Au moins un chiffre ■ Au moins un caractère spécial ■ Au moins cinq caractères différents ■ Les règles de complexité de mot de passe par défaut sont appliquées par les arguments du module PAM Linux suivants : <ul style="list-style-type: none"> ■ <code>retry=3</code> : nombre maximal de fois qu'un nouveau mot de passe peut être entré, 3 fois au maximum pour cet argument, avant de renvoyer une erreur. ■ <code>minlen=12</code> : taille minimale acceptable pour le nouveau mot de passe. En plus du nombre de caractères dans le nouveau mot de passe, un crédit (de +1 dans la longueur) est donné pour chaque type de caractère différent (autre, supérieur, inférieur et chiffre). ■ <code>difok=0</code> : nombre minimal d'octets qui doivent être différents dans le nouveau mot de passe. Indique la similarité entre l'ancien et le nouveau mot de passe. Avec une valeur 0 attribuée à <code>difok</code>, il n'est pas nécessaire que l'ancien et le nouveau mot de passe soient différents. Une correspondance exacte est autorisée. ■ <code>lcredit=1</code> : crédit maximal pour avoir des lettres minuscules dans le nouveau mot de passe. Si vous avez au maximum 1 lettre minuscule, chaque lettre compte +1 pour répondre à la valeur <code>minlen</code> actuelle. ■ <code>ucredit=1</code> : crédit maximal pour avoir des lettres majuscules dans le nouveau mot de passe. Si vous avez au maximum 1 lettre majuscule, chaque lettre compte +1 pour répondre à la valeur <code>minlen</code> actuelle. ■ <code>dcredit=1</code> : crédit maximal pour avoir des chiffres dans le nouveau mot de passe. Si vous avez au maximum 1 chiffre, chaque chiffre compte +1 pour répondre à la valeur <code>minlen</code> actuelle. ■ <code>ocredit=1</code> : crédit maximal pour avoir d'autres caractères dans le nouveau mot de passe. Si vous avez au maximum 1 autre caractère, chaque caractère compte +1 pour répondre à la valeur <code>minlen</code> actuelle. ■ <code>enforce_for_root</code> : le mot de passe est défini pour l'utilisateur racine. <p>Note Pour plus d'informations sur le module PAM Linux pour vérifier le mot de passe par rapport aux mots du dictionnaire, reportez-vous à la page <code>man</code>.</p> <p>Par exemple, évitez les mots de passe simples et systématiques tels que VMware123!123 ou VMware12345. Les mots de passe qui répondent aux normes de complexité ne sont pas simples et systématiques, mais il s'agit d'une combinaison de lettres, de caractères spéciaux et de chiffres, comme VMware123!45, VMware1!2345 ou VMware@1az23x.</p> <p>Le nom d'utilisateur de la ligne de commande est déjà défini sur <code>admin</code>.</p>

Option	Description
Mot de passe racine et confirmation du mot de passe	<p>Définissez le mot de passe racine et la confirmation de ce dernier pour le nouveau nœud.</p> <p>Votre mot de passe doit respecter les indications relatives au niveau de sécurité du mot de passe.</p> <ul style="list-style-type: none"> ■ Au moins 12 caractères ■ Au moins une lettre minuscule ■ Au moins une lettre majuscule ■ Au moins un chiffre ■ Au moins un caractère spécial ■ Au moins cinq caractères différents ■ Les règles de complexité de mot de passe par défaut sont appliquées par les arguments du module PAM Linux suivants : <ul style="list-style-type: none"> ■ <code>retry=3</code> : nombre maximal de fois qu'un nouveau mot de passe peut être entré, 3 fois au maximum pour cet argument, avant de renvoyer une erreur. ■ <code>minlen=12</code> : taille minimale acceptable pour le nouveau mot de passe. En plus du nombre de caractères dans le nouveau mot de passe, un crédit (de +1 dans la longueur) est donné pour chaque type de caractère différent (autre, supérieur, inférieur et chiffre). ■ <code>difok=0</code> : nombre minimal d'octets qui doivent être différents dans le nouveau mot de passe. Indique la similarité entre l'ancien et le nouveau mot de passe. Avec une valeur 0 attribuée à <code>difok</code>, il n'est pas nécessaire que l'ancien et le nouveau mot de passe soient différents. Une correspondance exacte est autorisée. ■ <code>lcredit=1</code> : crédit maximal pour avoir des lettres minuscules dans le nouveau mot de passe. Si vous avez au maximum 1 lettre minuscule, chaque lettre compte +1 pour répondre à la valeur <code>minlen</code> actuelle. ■ <code>ucredit=1</code> : crédit maximal pour avoir des lettres majuscules dans le nouveau mot de passe. Si vous avez au maximum 1 lettre majuscule, chaque lettre compte +1 pour répondre à la valeur <code>minlen</code> actuelle. ■ <code>dcredit=1</code> : crédit maximal pour avoir des chiffres dans le nouveau mot de passe. Si vous avez au maximum 1 chiffre, chaque chiffre compte +1 pour répondre à la valeur <code>minlen</code> actuelle. ■ <code>ocredit=1</code> : crédit maximal pour avoir d'autres caractères dans le nouveau mot de passe. Si vous avez au maximum 1 autre caractère, chaque caractère compte +1 pour répondre à la valeur <code>minlen</code> actuelle. ■ <code>enforce_for_root</code> : le mot de passe est défini pour l'utilisateur racine. <p>Note Pour plus d'informations sur le module PAM Linux pour vérifier le mot de passe par rapport aux mots du dictionnaire, reportez-vous à la page man.</p> <p>Par exemple, évitez les mots de passe simples et systématiques tels que VMware123!123 ou VMware12345. Les mots de passe qui répondent aux normes de complexité ne sont pas simples et systématiques, mais il s'agit d'une combinaison de lettres, de caractères spéciaux et de chiffres, comme VMware123!45, VMware1!2345 ou VMware@1az23x.</p>
Serveurs DNS	Entrez l'adresse IP du serveur DNS disponible dans vCenter Server.
Serveurs NTP	Entrez l'adresse IP du serveur NTP.

4 Entrez les détails du nœud NSX Manager.

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

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

Répétez les étapes 3 à 4.

6 Cliquez sur **Terminer**.

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

7 Attendez 10 à 15 minutes que le déploiement, la formation du cluster et la synchronisation du référentiel soient terminées.

Tous les détails de référentiel et le mot de passe du premier nœud NSX Manager déployé sont synchronisés avec les nœuds nouvellement déployés dans le cluster.

Note Si le premier nœud redémarre lorsque le déploiement d'un nouveau nœud est en cours, le nouveau nœud peut ne pas parvenir à s'enregistrer dans le cluster et le message **Échec de l'enregistrement** de s'affiche sur la miniature du nouveau nœud. Pour redéployer manuellement le nœud sur le cluster, accédez à la miniature du nouveau nœud, sélectionnez les ellipses verticales, puis cliquez sur **Réessayer**.

8 Dès que le nœud 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.

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

Les services suivants ne sont pas requis par défaut et ne démarrent pas automatiquement.

- `liagent`
- `migration-coordinator` : ce service est utilisé uniquement lors de l'exécution du coordinateur de migration. Reportez-vous au *Guide du coordinateur de migration de NSX-T Data Center* avant de démarrer ce service.

- `snmp` : pour plus d'informations sur le démarrage de SNMP, reportez-vous à *Protocole simple de gestion de réseau* dans le *Guide d'administration de NSX-T Data Center*.
 - `nsx-message-bus` : ce service n'est pas utilisé dans NSX-T Data Center 3.0.
- 10** Connectez-vous au premier nœud NSX Manager déployé et entrez la commande `get cluster status` pour vérifier que les nœuds sont correctement ajoutés au cluster.
- 11** Vérifiez que votre nœud NSX Manager ou Gestionnaire global dispose de la connectivité requise.

Assurez-vous que vous pouvez effectuer les tâches suivantes.

- Effectuer un test ping de votre nœud à partir d'une autre machine.
- Le nœud peut effectuer un test ping de sa passerelle par défaut.
- Le nœud peut effectuer un test ping des hôtes d'hyperviseur qui se trouvent dans le même réseau à l'aide de l'interface de gestion.
- Le nœud 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 nœud.

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

Étape suivante

Configurez NSX Edge. Reportez-vous à la section [Installer un dispositif NSX Edge sur ESXi à l'aide de l'interface utilisateur graphique de vSphere](#).

Déploiement de nœuds NSX Manager pour former un cluster à l'aide de la ligne de commande

Le fait de joindre NSX Manager pour former un cluster à l'aide de la ligne de commande permet de garantir que tous les nœuds NSX Manager du cluster peuvent communiquer entre eux.

Conditions préalables

L'installation des composants de NSX-T Data Center doit être terminée.

Procédure

- 1** Ouvrez une session SSH sur le premier nœud NSX Manager déployé.
- 2** Connectez-vous avec les informations d'identification d'administrateur.
- 3** Sur le nœud NSX Manager, exécutez la commande `get certificate api thumbprint`.
La sortie de la commande est une chaîne numérique propre à ce dispositif NSX Manager.
- 4** Exécutez la commande `get cluster config` pour obtenir l'ID du premier cluster NSX Manager déployé.

5 Ajoutez un nœud NSX Manager au cluster.

Note Vous devez exécuter la commande de jonction sur le nœud NSX Manager que vous venez de déployer.

Fournissez les informations de NSX Manager suivantes :

- Nom d'hôte ou adresse IP du nœud que vous voulez joindre
- ID de cluster
- Nom d'utilisateur
- Mot de passe
- Empreinte numérique du certificat

Vous pouvez utiliser la commande de l'interface de ligne de commande ou l'appel d'API.

- Commande de l'interface de ligne de commande

```
host> join <NSX-Manager-IP> cluster-id <cluster-id> username <NSX-Manager-username> password
<NSX-Manager-password> thumbprint <NSX-Manager-thumbprint>
```

- Appel d'API POST `https://<nsx-mgr>/api/v1/cluster?action=join_cluster`

Le processus de jonction et de stabilisation du cluster peut durer 10 à 15 minutes.

6 Ajoutez le troisième nœud NSX Manager au cluster.

Répétez l'étape 5.

7 Vérifiez l'état du cluster en exécutant la commande `get cluster status` sur vos hôtes.

8 (Interface utilisateur de NSX Manager) Sélectionnez **Système > Dispositifs > Présentation** et vérifiez la connectivité du cluster.

Étape suivante

Créez une zone de transport. Reportez-vous à la section [Créer un nœud de transport d'hôte autonome ou de serveur bare metal](#).

Configurer une adresse IP virtuelle (VIP) pour un cluster

Pour fournir la tolérance de panne et la haute disponibilité à des nœuds NSX Manager, attribuez une adresse IP virtuelle (VIP) à un membre du cluster NSX-T.

Les instances de NSX Manager d'un cluster font partie d'un groupe HTTPS pour traiter les demandes d'API et d'interface utilisateur. Le nœud leader du cluster assume la propriété de la VIP définie du cluster pour traiter toute demande d'API et d'interface utilisateur. Toutes les demandes d'API et d'interface utilisateur entrantes dans les clients sont dirigées vers le nœud leader.

Note Lors de l'attribution d'une adresse IP virtuelle, toutes les machines virtuelles NSX Manager du cluster doivent être configurées dans le même sous-réseau.

Si le nœud leader qui détient la VIP devient indisponible, NSX-T choisit un nouveau leader. Le nouveau leader détient l'adresse IP virtuelle. Il envoie un paquet ARP gratuit pour annoncer le nouveau mappage d'adresses VIP vers des adresses MAC. Lorsqu'un nouveau nœud de leader est choisi, de nouvelles demandes API et d'interface utilisateur sont envoyées au nouveau nœud leader.

Le basculement de la VIP vers un nouveau nœud de leader du cluster peut prendre quelques minutes pour devenir fonctionnel. Si la VIP bascule vers un nouveau nœud leader en raison de l'indisponibilité du nœud leader précédent, réauthentifiez les informations d'identification pour que les demandes d'API soient dirigées vers le nouveau nœud leader.

Note L'adresse IP virtuelle n'est pas conçue pour servir d'équilibreur de charge et vous ne pouvez pas l'utiliser si vous activez l'**intégration d'équilibreur de charge externe** de vIDM à partir de **Système > Utilisateurs > Configuration**. Ne configurez pas d'adresse IP virtuelle si vous souhaitez utiliser l'équilibreur de charge externe de vIDM. Pour plus d'informations, reportez-vous à la section [Configurer l'intégration de VMware Identity Manager](#) du *Guide d'administration de NSX-T Data Center*.

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 **Système > Présentation**.
- 3 Dans le champ Adresse IP virtuelle, cliquez sur **Modifier**.
- 4 Entrez la VIP du cluster. Assurez-vous que la VIP fait partie du même sous-réseau que les autres nœuds de gestion.
- 5 Cliquez sur **Enregistrer**.
- 6 Pour vérifier l'état du cluster et le leader d'API du groupe HTTPS, entrez la NSX Manager commande CLI `get cluster status verbose` dans la console NSX Manager ou via SSH.

Vous trouverez ci-dessous un exemple de sortie avec le leader marqué en gras.

```
Group Type: HTTPS
Group Status: STABLE
```

```
Members:
```

```
  UUID
```

```
  FQDN
```

```
  IP
```


STATUS			
	cdb93642-ccba-fdf4-8819-90bf018cd727	nsx-manager	192.196.197.84
UP			
	51a13642-929b-8dfc-3455-109e6cc2a7ae	nsx-manager	192.196.198.156
UP			
	d0de3642-d03f-c909-9cca-312fd22e486b	nsx-manager	192.196.198.54
UP			
Leaders:			
SERVICE		LEADER	LEASE
VERSION			
api	cdb93642-ccba-fdf4-8819-90bf018cd727		8

- 7 Pour résoudre les VIP, vérifiez les journaux du proxy inverse à l'adresse `/var/log/proxy/reverse-proxy.log` et les journaux du gestionnaire de clusters à l'adresse `/var/log/cbm/cbm.log` dans la CLI de NSX Manager.

Résultats

Toutes les demandes d'API à NSX-T sont redirigées vers l'adresse IP virtuelle du cluster, qui est détenue par le nœud leader. Le nœud leader achemine ensuite la demande vers les autres composants du dispositif.

Désactiver des snapshots sur des dispositifs NSX-T

Comme les machines virtuelles, NSX Manager et des dispositifs NSX Edge peuvent être configurés pour que leurs snapshots soient pris et stockés. Toutefois, les clones et les snapshots de dispositifs NSX-T ne sont pas pris en charge et peuvent entraîner des problèmes de fonctionnalité et d'autres problèmes inconnus. C'est pourquoi il est vivement recommandé de désactiver les snapshots des machines virtuelles de dispositif NSX-T.

Effectuez la procédure suivante sur chaque machine virtuelle de dispositif NSX-T.

Procédure

- 1 Localisez les machines virtuelles de dispositif dans vSphere Client.
- 2 Mettez la machine virtuelle hors tension.
- 3 Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
- 4 Cliquez sur l'onglet **Options VM**, puis développez **Avancé**.
- 5 Dans le champ **Paramètres de configuration**, cliquez sur **Modifier la configuration...**
- 6 Dans la fenêtre **Paramètres de configuration**, cliquez sur **Ajouter des paramètres de configuration**.
- 7 Entrez les informations suivantes :
 - Pour Nom, entrez **snapshot.MaxSnapshots**.
 - Pour Valeur, entrez **-0**.

- 8 Cliquez sur **OK** pour enregistrer les modifications.
- 9 Remettez la machine virtuelle sous tension.

Installation de NSX-T Data Center sur KVM

6

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

Assurez-vous que vous disposez des versions de KVM prises en charge. Reportez-vous à la section [Configuration système requise pour le nœud de transport hôte et la machine virtuelle NSX Manager](#).

Ce chapitre contient les rubriques suivantes :

- [Configurer KVM](#)
- [Gérer vos machines virtuelles invitées dans l'interface de ligne de commande de KVM](#)
- [Installer NSX Manager sur KVM](#)
- [Se connecter à l'instance de NSX Manager qui vient d'être créée](#)
- [Installer des modules tiers sur un hôte KVM](#)
- [Vérifier la version Open vSwitch sur les hôtes RHEL KVM](#)
- [Vérifier la version d'Open vSwitch sur les hôtes SUSE KVM](#)
- [Déploiement de nœuds NSX Manager pour former un cluster à l'aide de la ligne de commande](#)

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, 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 (RHEL 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 Data Center Container Plug-in, qui a la configuration requise de compatibilité spécifique, excluez les modules associés aux conteneurs.

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

Les versions prises en charge sont RHEL 7.4 et 7.5.

- 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 ou CentOS Linux	<pre>yum groupinstall "Virtualization Hypervisor" yum groupinstall "Virtualization Client" yum groupinstall "Virtualization Platform" yum groupinstall "Virtualization Tools"</pre>
SUSE Linux Enterprise Server	Démarrez YaSt et sélectionnez Virtualisation > Installer l'hyperviseur et les outils . YaSt vous permet d'activer et de configurer automatiquement le pont réseau.

- 5 Pour que NSX Manager installe automatiquement les modules logiciels NSX sur l'hôte KVM, préparez la configuration réseau de l'interface de liaison montante/de données.

L'hôte KVM peut avoir plusieurs interfaces réseau. Concernant l'interface réseau que vous prévoyez de fournir comme interface de liaison montante (interface de données) pour NSX-T, il est important de renseigner correctement les fichiers de configuration réseau. NSX-T examine ces fichiers de configuration réseau pour créer des périphériques réseau spécifiques à NSX-T. Sur Ubuntu, renseignez le fichier `/etc/network/interfaces`. Sur RHEL, CentOS ou SUSE, renseignez le fichier `/etc/sysconfig/network-scripts/ifcfg-$uplinkdevice`.

Dans les exemples suivants, l'interface « ens32 » est le périphérique de liaison montante (interface de données). 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.

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 peut entraîner l'échec de la création du nœud de transport.

Distribution Linux	Configuration réseau
Ubuntu	<p>Modifiez /etc/network/interfaces :</p> <pre> auto eth0 iface eth0 inet manual auto ens32 iface ens32 inet manual </pre>
RHEL ou CentOS Linux	<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" </pre>
SUSE Linux Enterprise Server	<p>S'il existe déjà un hôte SLES, vérifiez que les interfaces de données sont déjà configurées sur l'hôte.</p> <p>Si vous ne disposez pas d'un hôte SLES préconfiguré, reportez-vous à la configuration de référence de l'interface de gestion et de données.</p> <p>Modifiez /etc/sysconfig/network/ifcfg-ens32 :</p> <pre> DEVICE="ens32" NAME="ens32" UUID="<UUID>" BOOTPROTO="none" LLADDR="<HWADDR>" STARTMODE="yes" </pre>

- Redémarrez le service de mise en réseau `systemctl restart network` ou redémarrez le serveur Linux pour que les modifications de mise en réseau prennent effet.
- Une fois que l'hôte KVM est configuré comme nœud de transport, l'interface de pont `nsx-vtep0.0` est automatiquement créée par NSX-T.

Dans Ubuntu, le fichier /etc/network/interfaces possède des entrées semblables 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, NSX Agent hôte (nsxa) crée un fichier de configuration appelé `ifcfg-nsx-vtep0.0`, qui contient des entrées semblables à celles-ci :

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

Dans SUSE,

```
DEVICE=nsx-vtep0.0
BOOTPROTO=static
NETMASK=255.255.255.0
IPADDR=192.168.13.119
MACADDR=ae:9d:b7:ca:20:4a
MTU=1600
USERCTL=no
STARTMODE=auto
```

- 8 Configurez la stratégie de rotation Syslog comme une stratégie basée sur l'heure au lieu de la stratégie basée sur la taille. Avec une stratégie de rotation Syslog basée sur la taille, les fichiers journaux générés peuvent être de très grande taille.

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

NSX Manager peut être installé en tant que machine virtuelle 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, utilisez 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)
```

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](#).
- Familiarisez-vous avec les besoins en ressources de NSX Manager. Reportez-vous à la section [Configuration système requise pour le nœud de transport hôte et la machine virtuelle NSX Manager](#).
- Si vous prévoyez d'installer Ubuntu OS, il est recommandé d'installer Ubuntu version 18.04 avant d'installer NSX Manager sur l'hôte KVM.

Procédure

- 1 Téléchargez l'image QCOW2 de NSX Manager à partir du dossier **nsx-unified-appliance > exports > kvm**.

- 2** Copiez-la vers la machine KVM qui va exécuter NSX Manager à l'aide de SCP ou de la synchronisation.
- 3** (Ubuntu uniquement) Ajoutez l'utilisateur connecté en tant qu'utilisateur libvirtd :

```
adduser $USER libvirtd
```


- 4 Dans le répertoire où vous avez enregistré l'image QCOW2, créez un fichier appelé `guestinfo.xml` et remplissez-le avec les propriétés de la machine virtuelle NSX Manager.

Propriété	Description
<ul style="list-style-type: none"> ■ <code>nsx_cli_passwd_0</code> ■ <code>nsx_cli_audit_passwd_0</code> ■ <code>nsx_passwd_0</code> 	<p>Vos mots de passe doivent respecter les indications relatives au niveau de sécurité du mot de passe.</p> <ul style="list-style-type: none"> ■ Au moins 12 caractères ■ Au moins une lettre minuscule ■ Au moins une lettre majuscule ■ Au moins un chiffre ■ Au moins un caractère spécial ■ Au moins cinq caractères différents <p>Les règles de complexité de mot de passe par défaut sont appliquées par les arguments du module PAM Linux suivants :</p> <ul style="list-style-type: none"> ■ <code>retry=3</code> : nombre maximal de fois qu'un nouveau mot de passe peut être entré, 3 fois au maximum pour cet argument, avant de renvoyer une erreur. ■ <code>minlen=12</code> : taille minimale acceptable pour le nouveau mot de passe. En plus du nombre de caractères dans le nouveau mot de passe, un crédit (de +1 dans la longueur) est donné pour chaque type de caractère différent (autre, supérieur, inférieur et chiffre). ■ <code>difok=0</code> : nombre minimal d'octets qui doivent être différents dans le nouveau mot de passe. Indique la similarité entre l'ancien et le nouveau mot de passe. Avec une valeur 0 attribuée à <code>difok</code>, il n'est pas nécessaire que l'ancien et le nouveau mot de passe soient différents. Une correspondance exacte est autorisée. ■ <code>lcredit=1</code> : crédit maximal pour avoir des lettres minuscules dans le nouveau mot de passe. Si vous avez au maximum 1 lettre minuscule, chaque lettre compte +1 pour répondre à la valeur <code>minlen</code> actuelle. ■ <code>ucredit=1</code> : crédit maximal pour avoir des lettres majuscules dans le nouveau mot de passe. Si vous avez au maximum 1 lettre majuscule, chaque lettre compte +1 pour répondre à la valeur <code>minlen</code> actuelle. ■ <code>dcredit=1</code> : crédit maximal pour avoir des chiffres dans le nouveau mot de passe. Si vous avez au maximum 1 chiffre, chaque chiffre compte +1 pour répondre à la valeur <code>minlen</code> actuelle. ■ <code>ocredit=1</code> : crédit maximal pour avoir d'autres caractères dans le nouveau mot de passe. Si vous avez au maximum 1 autre caractère, chaque caractère compte +1 pour répondre à la valeur <code>minlen</code> actuelle. ■ <code>enforce_for_root</code> : le mot de passe est défini pour l'utilisateur racine. <p>Note Pour plus d'informations sur le module PAM Linux pour vérifier le mot de passe par rapport aux mots du dictionnaire, reportez-vous à la page man.</p> <p>Par exemple, évitez les mots de passe simples et systématiques tels que VMware123!123 ou VMware12345. Les mots de passe qui répondent aux normes de complexité ne sont pas simples et systématiques, mais il s'agit d'une combinaison de lettres, de caractères spéciaux et de chiffres, comme VMware123!45, VMware1!2345 ou VMware@1az23x.</p>
<code>nsx_hostname</code>	Entrez le nom d'hôte de NSX Manager. Le nom d'hôte doit être un nom de domaine valide. Assurez-vous que chaque partie du nom d'hôte

Propriété	Description
	(domaine/sous-domaine) séparée par un point commence par un caractère alphabétique.
nsx_role	<ul style="list-style-type: none"> ■ <i>nsx-manager</i> : requis. Ce nom de rôle installe le dispositif NSX Manager. ■ <i>nsx-cloud-service-manager</i> : facultatif. Après l'installation de NSX Manager, utilisez ce nom de rôle pour installer le dispositif Cloud Service Manager pour NSX Cloud.
nsx_isSSHEnabled	Vous pouvez activer ou désactiver cette propriété. Si cette option est activée, vous pouvez vous connecter à NSX Manager à l'aide de SSH.
nsx_allowSSHRootLogin	Vous pouvez activer ou désactiver cette propriété. Si cette option est activée, vous pouvez vous connecter à NSX Manager à l'aide de SSH en tant qu'utilisateur racine. Pour pouvoir utiliser cette propriété, <i>nsx_isSSHEnabled</i> doit être activé.
<ul style="list-style-type: none"> ■ nsx_dns1_0 ■ nsx_ntp_0 ■ nsx_domain_0 ■ nsx_gateway_0 ■ nsx_netmask_0 ■ nsx_ip_0 	Entrez les adresses IP de la passerelle par défaut, l'adresse IPv4 du réseau de gestion, le masque du réseau de gestion, le DNS et l'adresse IP NTP.

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_cli_passwd_0" oe:value="<password>" />
    <Property oe:key="nsx_cli_audit_passwd_0" oe:value="<password>" />
    <Property oe:key="nsx_passwd_0" oe:value="<password>" />
    <Property oe:key="nsx_hostname" oe:value="nsx-manager1" />
    <Property oe:key="nsx_role" oe:value="nsx-manager" />
    <Property oe:key="nsx_isSSHEnabled" oe:value="True" />
    <Property oe:key="nsx_allowSSHRootLogin" oe:value="True" />
    <Property oe:key="nsx_dns1_0" oe:value="10.168.110.10" />
    <Property oe:key="nsx_ntp_0" oe:value="10.168.110.10" />
    <Property oe:key="nsx_domain_0" oe:value="corp.local" />
    <Property oe:key="nsx_gateway_0" oe:value="10.168.110.83" />
    <Property oe:key="nsx_netmask_0" oe:value="255.255.252.0" />
  </PropertySection>
</Environment>
```

```
<Property oe:key="nsx_ip_0" oe:value="10.168.110.19"/>
</PropertySection>
</Environment>
```

Note 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.

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

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

```
sudo guestfish --rw -i -a nsx-unified-appliance-<BuildNumber>.qcow2 upload guestinfo /config/
guestinfo
```

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

Les valeurs des vCPU et de la RAM conviennent à une machine virtuelle de grande taille. Le nom du réseau et le nom du groupe de ports sont spécifiques à votre environnement. Le modèle doit être `virtio`.

```
sudo virt-install \
--import \
--ram 48000 \
--vcpus 12 \
--name <manager-name> \
--disk path=<manager-qcow2-file-path>,bus=virtio,cache=none \
--network network=<network-name>,portgroup=<portgroup-name>,model=virtio \
--noautoconsole \
--cpu mode=host-passthrough,cache.mode=passthrough

Starting install...
Domain installation still in progress. Waiting for installation to complete.
```

- 7 Vérifiez que NSX Manager est déployé.

```
virsh list --all
```

Id	Name	State
18	nsx-manager1	running

8 Ouvrez la console de NSX Manager et connectez-vous.

```

virsh console 18
Connected to domain nsx-manager1
Escape character is ^]

nsx-manager1 login: admin
Password:

```

9 Dès que le nœud 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.**10** Exécutez `get services` pour vérifier que les services sont en cours d'exécution.**11** Vérifiez que votre nœud NSX Manager ou Gestionnaire global dispose de la connectivité requise.

Assurez-vous que vous pouvez effectuer les tâches suivantes.

- Effectuer un test ping de votre nœud à partir d'une autre machine.
- Le nœud peut effectuer un test ping de sa passerelle par défaut.
- Le nœud peut effectuer un test ping des hôtes d'hyperviseur qui se trouvent dans le même réseau à l'aide de l'interface de gestion.
- Le nœud 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 nœud.

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

12 Quittez la console KVM.

```
control-]
```

13 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.

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. Vous y apprendrez également comment participer au programme et le quitter.

Conditions préalables

Vérifiez que NSX Manager est installé. Reportez-vous à la section [Installer NSX Manager et les dispositifs disponibles](#).

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 Lisez, puis acceptez les conditions du CLUF.
- 3 Indiquez si vous voulez rejoindre le Programme d'amélioration du produit de VMware.
- 4 Cliquez sur **Enregistrer**

Installer des modules tiers sur un hôte KVM

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

Conditions préalables

- (RHEL et CentOS Linux) Avant d'installer les modules tiers, exécutez les commandes suivantes pour installer les modules de virtualisation.

```
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, exécutez les commandes suivantes pour installer les modules de virtualisation.

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

- (SUSE Linux Enterprise Server) Avant d'installer les modules tiers, exécutez les commandes suivantes pour installer les modules de virtualisation.

```
libcap-progs
```

Procédure

- ◆ Sur Ubuntu 18.04.2 LTS, exécutez `apt-get install <package_name>` pour installer les modules tiers suivants manuellement.

```
traceroute
python-mako
python-simplejson
python-unittest2
python-yaml
python-netaddr
dkms
libc6-dev
libelf-dev
```

- ◆ Sur RHEL et CentOS Linux, exécutez `yum install <package_name>` pour installer les modules tiers manuellement.

Si vous préparez manuellement l'hôte qui est déjà enregistré sur RHEL ou CentOS, vous n'avez pas besoin d'installer les modules tiers sur celui-ci.

RHEL 7.6, 7.5 et 7.4 CentOS Linux 7.5 et 7.4

```
wget
PyYAML
libunwind
python-gevent
python-mako
python-netaddr
redhat-lsb-core
tcpdump
net-tools
```

```
wget
PyYAML
libunwind
python-gevent
python-mako
python-netaddr
redhat-lsb-core
tcpdump
```

- ◆ Sur SUSE, exécutez `zypper install <package_name>` pour installer les modules tiers manuellement.

SUSE Linux Enterprise Server 12.0

```
python-simplejson
python-PyYAML
python-netaddr
lsb-release
```

Vérifier la version Open vSwitch sur les hôtes RHEL KVM

Ignorez cette rubrique si l'hôte RHEL ne dispose pas de modules OVS. Si des modules OVS existent déjà sur un hôte RHEL, vous devez supprimer les modules OVS existants et installer les modules OVS pris en charge par NSX-T ou mettre à niveau les modules OVS existants vers les applications NSX-T prises 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
```

Important Si les modules Open vSwitch existants exécutent la version la plus récente ou une version antérieure, vous devez les remplacer par la version prise en charge.

- 2 Supprimez les modules Open vSwitch suivants.

- kmod-openvswitch ou openvswitch-kmod
- openvswitch
- openvswitch-selinux-policy

- 3 Vous pouvez également effectuer la mise à niveau vers 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>-rhel75_x86_64.tar.gz
```

- d Naviguez jusqu'au répertoire du module.

```
cd nsx-lcp-rhel75_x86_64/
```

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

- Pour obtenir la version la plus récente d'Open vSwitch, utilisez la commande `--nodeps`.

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

- Pour obtenir la version la plus ancienne d'Open vSwitch, utilisez la commande `--force`.

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

Vérifier la version d'Open vSwitch sur les hôtes SUSE KVM

Ignorez cette rubrique s'il n'existe pas de modules OVS sur l'hôte SUSE. Si des modules OVS existent sur un hôte SUSE, vous devez supprimer les modules OVS existants et installer les modules OVS NSX-T pris en charge ou mettre à niveau les modules OVS existants vers ceux pris en charge par NSX-T.

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
```

Important Si les modules Open vSwitch existants exécutent la version la plus récente ou une version antérieure, vous devez les remplacer par la version prise en charge.

- 2 Supprimez les modules Open vSwitch suivants.

- kmod-openvswitch ou openvswitch-kmod
- openvswitch
- openvswitch-selinux-policy

- 3 Vous pouvez également effectuer la mise à niveau vers 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.

```
nsx-lcp-3.0.0.0.14335404-linux64-sles12sp3.tar.gz
```

- d Naviguez jusqu'au répertoire du module.

```
nsx-lcp-linux64-sles12sp3/
```

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

- Pour obtenir la version la plus récente d'Open vSwitch, utilisez la commande `--nodeps`.

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

- Pour obtenir la version la plus ancienne d'Open vSwitch, utilisez la commande `--force`.

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

Déploiement de nœuds NSX Manager pour former un cluster à l'aide de la ligne de commande

Le fait de joindre NSX Manager pour former un cluster à l'aide de la ligne de commande permet de garantir que tous les nœuds NSX Manager du cluster peuvent communiquer entre eux.

Conditions préalables

L'installation des composants de NSX-T Data Center doit être terminée.

Procédure

- 1 Ouvrez une session SSH sur le premier nœud NSX Managerdéployé.
- 2 Connectez-vous avec les informations d'identification d'administrateur.
- 3 Sur le nœud NSX Manager, exécutez la commande `get certificate api thumbprint`.
La sortie de la commande est une chaîne numérique propre à ce dispositif NSX Manager.
- 4 Exécutez la commande `get cluster config` pour obtenir l'ID du premier cluster NSX Manager déployé.
- 5 Ajoutez un nœud NSX Manager au cluster.

Note Vous devez exécuter la commande de jonction sur le nœud NSX Managerque vous venez de déployer.

Fournissez les informations de NSX Manager suivantes :

- Nom d'hôte ou adresse IP du nœud que vous voulez joindre
- ID de cluster
- Nom d'utilisateur
- Mot de passe
- Empreinte numérique du certificat

Vous pouvez utiliser la commande de l'interface de ligne de commande ou l'appel d'API.

- Commande de l'interface de ligne de commande

```
host> join <NSX-Manager-IP> cluster-id <cluster-id> username <NSX-Manager-username> password
<NSX-Manager-password> thumbprint <NSX-Manager-thumbprint>
```

- Appel d'API POST `https://<nsx-mgr>/api/v1/cluster?action=join_cluster`

Le processus de jonction et de stabilisation du cluster peut durer 10 à 15 minutes.

- 6 Ajoutez le troisième nœud NSX Manager au cluster.
Répétez l'étape 5.
- 7 Vérifiez l'état du cluster en exécutant la commande `get cluster status` sur vos hôtes.
- 8 (Interface utilisateur de NSX Manager) Sélectionnez **Système > Dispositifs > Présentation** et vérifiez la connectivité du cluster.

Étape suivante

Créez une zone de transport. Reportez-vous à la section [Créer un nœud de transport d'hôte autonome ou de serveur bare metal](#).

Configuration d'un serveur bare metal pour utiliser NSX-T Data Center

7

Pour utiliser NSX-T Data Center sur un serveur bare metal, vous devez installer les modules tiers pris en charge.

NSX-T Data Center prend en charge le serveur bare metal de deux façons : en tant que nœud de transport hôte et en tant qu'hôte pour NSX Manager.

Assurez-vous que vous disposez des versions de serveur bare metal prises en charge. Reportez-vous à la section [Configuration requise système d'un serveur bare metal](#).

Note Si vos dispositifs NSX Edge sont dans un format de machine virtuelle et que vous prévoyez d'utiliser le service DHCP NSX (déployé sur un commutateur logique supporté par VLAN), vous devez définir l'option Transmissions forgées sur Accepter sur les hôtes bare metal sur lesquels les dispositifs NSX Edge sont déployés. Reportez-vous à la section Transmissions forgées dans la documentation du produit vSphere.

Ce chapitre contient les rubriques suivantes :

- [Installer les modules tiers sur un serveur bare metal](#)
- [Créer une interface d'application pour les charges de travail de serveur Bare Metal](#)

Installer les modules tiers sur un serveur bare metal

Pour préparer un serveur Bare Metal à devenir un nœud d'infrastructure, vous devez installer des modules tiers.

Conditions préalables

- Vérifiez que l'utilisateur effectuant l'installation dispose d'une autorisation administrative pour effectuer les actions suivantes, dont certaines peuvent nécessiter des autorisations sudo :
 - Téléchargez et décompressez le bundle.
 - Exécutez les commandes `dpkg` ou `rpm` pour installer/désinstaller des composants NSX.
 - Exécutez la commande `nsxcli` pour exécuter les commandes du plan de gestion de jonction.

- Vérifiez que les modules de virtualisation sont installés.
 - RedHat ou CentOS - `yum install libvirt-libs`
 - Ubuntu - `apt-get install libvirt0`
 - SUSE - `zypper install libvirt-libs`

Procédure

- ◆ Sous Ubuntu, exécutez la commande `apt-get install <package_name>` pour installer les modules tiers.

Ubuntu 18.04.2	Ubuntu 16.04
traceroute python-mako python-netaddr python-simplejson python-unittest2 python-yaml python-openssl dkms libvirt0 libelf-dev	libunwind8 libgflags2v5 libgoogle-perftools4 traceroute python-mako python-simplejson python-unittest2 python-yaml python-netaddr python-openssl libboost-filesystem1.58.0 libboost-chrono1.58.0 libgoogle-glog0v5 dkms libboost-date-time1.58.0 python-protobuf python-gevent libsnappy1v5 libleveldb1v5 libboost-program-options1.58.0 libboost-thread1.58.0 libboost-iostreams1.58.0 libvirt0 libelf-dev

- ◆ Sous RHEL ou CentOS, exécutez la commande `yum install` pour installer les modules tiers.

RHEL 7.4, 7.5 et 7.6	CentOS 7.4, 7.5 et 7.6
tcpdump	tcpdump
boost-filesystem	boost-filesystem
PyYAML	PyYAML
boost-iostreams	boost-iostreams
boost-chrono	boost-chrono
python-mako	python-mako
python-netaddr	python-netaddr
python-six	python-six
gperftools-libs	gperftools-libs
libunwind	libunwind
libelf-dev	libelf-dev
snappy	snappy
boost-date-time	boost-date-time
c-ares	c-ares
redhat-lsb-core	redhat-lsb-core
wget	wget
net-tools	net-tools
yum-utils	yum-utils
lsof	lsof
python-gevent	python-gevent
libev	libev
python-greenlet	python-greenlet
libvirt-libs	libvirt-libs

- ◆ Sur SUSE, exécutez `zypper install <package_name>` pour installer les modules tiers manuellement.

```
net-tools
tcpdump
python-simplejson
python-netaddr
python-PyYAML
python-six
libunwind
wget
lsof
libcap-progs
libvirt-libs
```

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 NSX-T Data Center et installer des modules tiers Linux.

NSX-T Data Center ne prend pas en charge la liaison d'interface du système d'exploitation Linux. Vous devez utiliser la liaison Open vSwitch (OVS) pour les nœuds de transport de serveur bare metal. Consultez l'article 67835 de la base de connaissances [Bare Metal Server supports OVS bonding for Transport Node configuration in NSX-T \(Le serveur bare metal prend en charge la liaison OVS pour la configuration du nœud de transport dans NSX-T\)](#).

Procédure

- 1 Installez les modules tiers requis.

Reportez-vous à la section [Installer les modules tiers sur un serveur bare metal](#).

- 2 Configurez les ports TCP et UDP.

Reportez-vous à la section [Ports TCP et UDP utilisés par ESXi, les hôtes KVM et le serveur Bare Metal](#).

- 3 Ajoutez un serveur bare metal à l'infrastructure de NSX-T Data Center et créez un nœud de transport.

Reportez-vous à la section [Créer un nœud de transport d'hôte autonome ou de serveur bare metal](#).

- 4 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>.

Configuration requise pour le cluster NSX Manager

8

Les sous-sections suivantes décrivent la configuration requise du cluster NSX Manager et fournissent des recommandations pour des déploiements de sites spécifiques. Elles décrivent également comment vous pouvez utiliser vSphere HA avec NSX-T Data Center pour activer la récupération rapide si l'hôte exécutant le nœud NSX Manager échoue.

Ce chapitre contient les rubriques suivantes :

- [Configuration requise du cluster NSX Manager pour un site unique, deux sites et plusieurs sites](#)

Configuration requise du cluster NSX Manager pour un site unique, deux sites et plusieurs sites

La configuration de votre cluster NSX Manager varie selon que votre déploiement est destiné à un site unique, à deux sites ou à plusieurs sites.

Vous pouvez utiliser vSphere HA avec NSX-T Data Center pour activer la récupération rapide si l'hôte exécutant le nœud NSX Manager échoue.

Note Reportez-vous à la section *Créer et utiliser des clusters vSphere HA* dans la documentation du produit vSphere.

Configuration requise pour le cluster

- Dans un environnement de production, le cluster NSX Manager doit disposer de trois membres pour éviter une interruption des plans de gestion et de contrôle.

Chaque membre du cluster doit être placé sur un hôte d'hyperviseur unique avec trois hôtes d'hyperviseur physiques au total. Cela est nécessaire pour éviter une panne de l'hôte d'hyperviseur physique unique affectant le plan de contrôle NSX. Il est recommandé d'appliquer des règles d'anti-affinité pour vous assurer que les trois membres du cluster s'exécutent sur des hôtes différents.

L'état de fonctionnement normal de la production est un cluster NSX Manager à trois nœuds. Toutefois, vous pouvez ajouter des nœuds NSX Manager supplémentaires temporaires pour autoriser les modifications d'adresse IP.

Important À partir de NSX-T Data Center 2.4, NSX Manager contient le processus du plan de contrôle central NSX. Ce service est essentiel pour le fonctionnement de NSX. Si des instances de NSX Manager sont complètement perdues ou si le cluster est ramené de trois instances de NSX Manager à une seule instance de NSX Manager, vous ne pourrez pas apporter de modifications de topologie à votre environnement, et la migration vMotion des machines dépendant de NSX échouera.

- Pour les déploiements de laboratoire et de validation technique pour lesquels il n'y a aucune charge de travail de production, vous pouvez exécuter une seule instance de NSX Manager afin d'économiser des ressources. Les nœuds NSX Manager peuvent être déployés sur ESXi ou KVM. Toutefois, les déploiements mixtes de gestionnaires sur ESXi et KVM ne sont pas pris en charge.

Configuration requise et recommandations pour un site unique

Les recommandations suivantes s'appliquent aux déploiements de NSX-T Data Center sur un site unique.

- Il est recommandé de placer vos instances de NSX Manager sur différents hôtes pour éviter une panne d'hôte unique affectant plusieurs gestionnaires.
- La latence maximale entre des instances de NSX Manager est de 10 ms.
- Vous pouvez placer des instances de NSX Manager dans différents clusters vSphere ou dans un cluster vSphere commun.
- Il est recommandé de placer les instances de NSX Manager dans différents sous-réseaux de gestion ou dans un sous-réseau de gestion partagé. Lors de l'utilisation de vSphere HA, il est recommandé d'utiliser un sous-réseau de gestion partagé afin que les instances de NSX Manager qui sont récupérées par vSphere puissent conserver leur adresse IP.
- Il est également recommandé de placer les instances de NSX Manager sur le stockage partagé. Pour vSphere HA, vérifiez la configuration requise pour cette solution.

Vous pouvez également utiliser vSphere HA avec NSX-T pour fournir la récupération d'une instance de NSX Manager perdue lors de l'échec de l'hôte sur lequel NSX Manager est exécuté.

Exemple de scénario :

- Un cluster vSphere dans lequel les trois instances de NSX Manager sont déployées.
- Le cluster vSphere se compose d'au moins quatre hôtes :
 - Hôte-01 avec nsxmgr-01 déployé
 - Hôte-02 avec nsxmgr-02 déployé
 - Hôte-03 avec nsxmgr-03 déployé

- Hôte-04 sans NSX Manager déployé
- vSphere HA est configuré pour récupérer n'importe quelle instance de NSX Manager perdue (par exemple, nsxmgr-01) à partir de n'importe quel hôte (par exemple, Hôte-01) vers Hôte-04.

Ainsi, lors de la perte d'hôtes sur lesquels une instance de NSX Manager est en cours d'exécution, vSphere récupère l'instance de NSX Manager perdue sur Hôte-04.

Configuration requise et recommandations pour deux sites

Les recommandations suivantes s'appliquent aux déploiements de NSX-T Data Center sur deux sites (Site A/Site B).

- Il n'est pas recommandé de déployer des instances de NSX Manager dans un scénario à deux sites sans vSphere HA. Dans ce scénario, un site nécessite le déploiement de deux instances de NSX Manager et la perte de ce site aura un impact sur le fonctionnement de NSX-T Data Center.
- Le déploiement d'instances de NSX Manager dans un scénario à deux sites avec vSphere HA peut être effectué avec les considérations suivantes :
 - Un cluster vSphere étendu unique contient tous les hôtes pour des instances de NSX Manager.
 - Les trois instances de NSX Manager sont déployées sur un sous-réseau de gestion/VLAN commun pour pouvoir conserver l'adresse IP lors de la récupération d'une instance de NSX Manager perdue.
 - Pour la latence entre les sites, reportez-vous à la configuration requise du produit de stockage.

Exemple de scénario :

- Un cluster vSphere dans lequel les trois instances de NSX Manager sont déployées.
- Le cluster vSphere se compose de six hôtes ou plus, avec trois hôtes sur le Site A et trois hôtes sur le Site B.
- Les trois instances de NSX Manager sont déployées sur des hôtes distincts avec des hôtes supplémentaires pour le placement des instances de NSX Manager récupérées :

Site A :

- Hôte-01 avec nsxmgr-01 déployé
- Hôte-02 avec nsxmgr-02 déployé
- Hôte-03 avec nsxmgr-03 déployé

Site B :

- Hôte-04 sans NSX Manager déployé
- Hôte-05 sans NSX Manager déployé

- Hôte-06 sans NSX Manager déployé
- vSphere HA est configuré pour récupérer n'importe quelle instance de NSX Manager perdue (par exemple, nsxmgr-01) à partir de n'importe quel hôte (par exemple, Hôte-01) sur le Site A vers l'un des hôtes sur le Site B.

Par conséquent, en cas de panne du Site A, vSphere HA récupère toutes les instances de NSX Manager sur les hôtes du Site B.

Important Vous devez configurer correctement des règles d'anti-affinité pour empêcher la récupération des instances de NSX Manager sur le même hôte commun.

Configuration requise et recommandations pour plusieurs sites (trois ou plus)

Les recommandations suivantes s'appliquent aux déploiements de NSX-T Data Center sur plusieurs sites (Site A/Site B/Site C).

Dans un scénario comportant au moins trois sites, vous pouvez déployer des instances de NSX Manager avec ou sans vSphere HA.

Si vous déployez sans vSphere HA :

- Il est recommandé d'utiliser des sous-réseaux de gestion ou des VLAN distincts par site.
- La latence maximale entre des instances de NSX Manager est de 10 ms.

Exemple de scénario (trois sites) :

- Trois clusters vSphere distincts, un par site.
- Au moins un hôte par site exécutant NSX Manager :
 - Hôte-01 avec nsxmgr-01 déployé
 - Hôte-02 avec nsxmgr-02 déployé
 - Hôte-03 avec nsxmgr-03 déployé

Scénarios de panne :

- Panne de site unique : deux instances de NSX Manager restantes sur d'autres sites fonctionnent toujours. NSX-T Data Center est dans un état dégradé, mais reste opérationnel. Il est recommandé de déployer manuellement une troisième instance de NSX Manager pour remplacer le membre de cluster perdu.
- Panne de deux sites : perte de quorum et donc impact sur les opérations de NSX-T Data Center.

La récupération d'instances de NSX Manager peut prendre jusqu'à 20 minutes selon les conditions environnementales telles que la vitesse du CPU, les performances du disque et d'autres facteurs de déploiement.

Installation de NSX Edge

9

Installez NSX Edge sur ESXi à l'aide de l'interface utilisateur de NSX-T, du client Web vSphere ou de l'outil OVF de ligne de commande.

Ce chapitre contient les rubriques suivantes :

- [Conditions d'installation de NSX Edge](#)
- [Configuration réseau de NSX Edge](#)
- [Méthodes d'installation de NSX Edge](#)
- [Créer un nœud de transport NSX Edge](#)
- [Créer un cluster NSX Edge](#)
- [Installer un dispositif NSX Edge sur ESXi à l'aide de l'interface utilisateur graphique de vSphere](#)
- [Installer un dispositif NSX Edge sur un système Bare Metal](#)
- [Relier NSX Edge au plan de gestion](#)
- [Configurer un dispositif NSX Edge en tant que nœud de transport](#)

Conditions d'installation de NSX Edge

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

Note Il ne peut y avoir qu'un seul routeur de niveau 0 par nœud NSX Edge. Toutefois, plusieurs routeurs logiques de niveau 1 peuvent être hébergés sur un nœud NSX Edge. Des VM NSX Edge de différentes tailles peuvent être combinées dans le même cluster ; toutefois, cette opération n'est pas recommandée.

Tableau 9-1. 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 12 caractères ■ Au moins une lettre minuscule ■ Au moins une lettre majuscule ■ Au moins un chiffre ■ Au moins un caractère spécial ■ Au moins cinq caractères différents ■ Aucun mot issu du dictionnaire ■ Aucun palindrome ■ Une séquence de plus de quatre caractères monotones n'est pas autorisée
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	<p>Vérifiez que la configuration requise est respectée.</p> <p>Reportez-vous à la section Configuration système requise des machines virtuelles NSX Edge.</p>
Ports	Vérifiez que les ports requis sont ouverts. Reportez-vous à la section Ports et protocoles .
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'adressage IP IPv4 ou IPv6 NSX Edge.</p>

Tableau 9-1. Exigences du déploiement, des plates-formes et de l'installation de NSX Edge (suite)

Exigences	Description
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>localhost</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 une 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 toutes les machines virtuelles NSX Edge ou bare metal dans un cluster Edge.

Chipsets basés sur Intel

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.

Prise en charge NSX Edge des fonctionnalités de poursuite d'activité de vSphere

À partir de NSX-T Data Center 2.5.1, vMotion, DRS et vSphere HA sont pris en charge pour les nœuds NSX 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 la configuration requise de complexité, vous devez vous connecter à NSX Edge via SSH ou sur la console en tant qu'utilisateur **admin** avec le mot de passe **default**. 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.

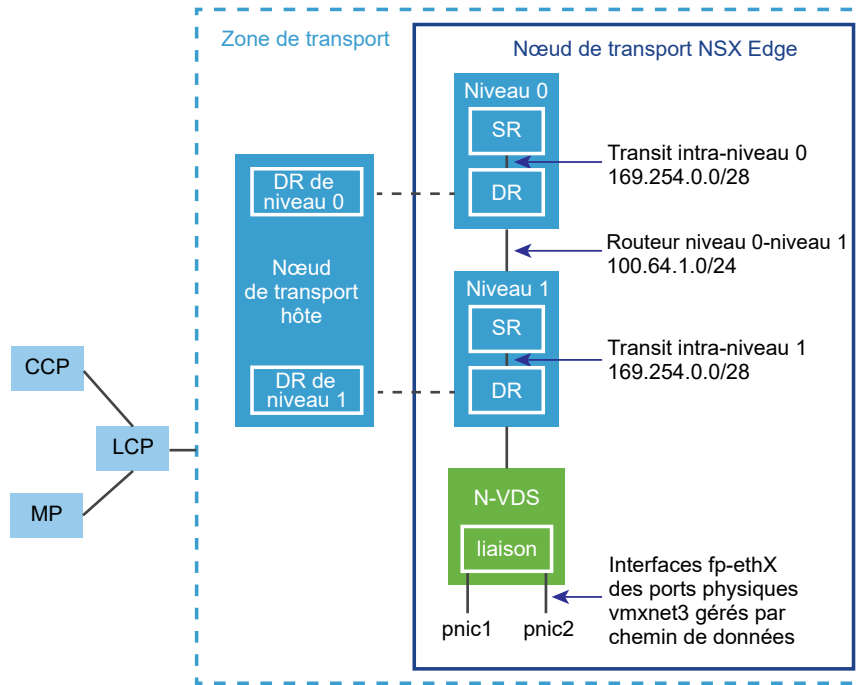
Configuration réseau de NSX Edge

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

La vue générale de NSX-T Data Center affiche deux nœuds de transport dans une zone de transport. L'un des nœuds de transport est un hôte. L'autre est un dispositif NSX Edge.

Figure 9-1. Présentation générale de NSX Edge



Lorsque vous déployez un dispositif NSX Edge pour la première fois, vous pouvez le considérer comme un conteneur vide. Le dispositif NSX Edge ne fait rien tant que vous n'avez pas créé de routeurs logiques. Le dispositif NSX Edge fournit la structure de calcul pour les routeurs logiques de niveau 0 et de niveau 1. Un routeur logique contient un routeur de services (SR) et un routeur distribué (DR). Un routeur distribué est un routeur qui est répliqué sur tous les nœuds de transport appartenant à une même zone de transport. Sur le schéma, le nœud de transport hôte contient les mêmes DR que les routeurs de niveau 0 et de niveau 1. Un routeur de services est requis si le routeur logique doit être configuré pour fournir des services, tels que NAT. Tous les routeurs logiques de niveau 0 contiennent un routeur de services. Un routeur de niveau 1 peut posséder un routeur de services si vos choix de conception l'exigent.

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 cluster 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.

Enfin, le schéma 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 NSX Edge qui est déployé en tant que machine virtuelle. 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 machine virtuelle NSX Edge, le premier lien trouvé pourrait être vnic1. Pour une installation sur système nu, 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 machines virtuelles 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, en vous connectant à l'interface de ligne de commande en tant qu'administrateur et en exécutant 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`. Les liens physiques sont décrits en détail à la section suivante.

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

Pour comprendre la mise en réseau de NSX Edge, vous devez avoir des connaissances sur les zones de transport et les 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. Un N-VDS a pour vocation de lier les liaisons montantes et les liaisons descendantes des routeurs logiques aux cartes réseau physiques. Pour chaque zone de transport à laquelle appartient le dispositif NSX Edge, un N-VDS distinct est installé sur le dispositif NSX Edge.

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.

Un dispositif NSX Edge peut appartenir à zéro ou à plusieurs zones de transport VLAN. Pour les zones de transport VLAN, NSX Edge peut toujours posséder des liaisons montantes, car les liaisons montantes de NSX Edge peuvent utiliser le N-VDS installé pour la zone de transport de superposition. 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 utiliser le même ID de VLAN pour un réseau de transport de trafic de superposition et pour d'autres trafics VLAN, comme une liaison montante VLAN, configurez l'ID sur deux N-VDS différents, un pour VLAN et l'autre pour la superposition.

Mise en réseau NSX Edge de dispositifs virtuels/machines virtuelles

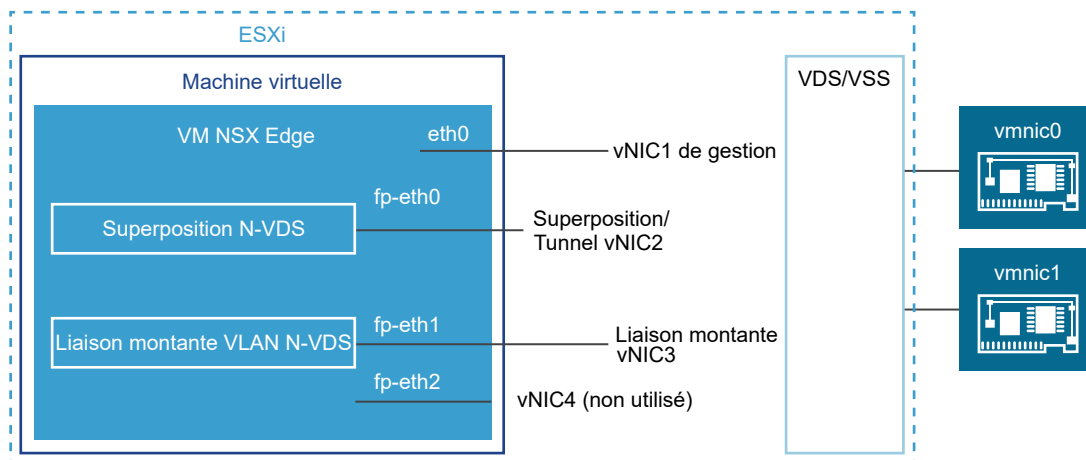
Lorsque vous installez NSX Edge en tant que dispositif virtuel ou machine virtuelle, des interfaces internes, appelées fp-ethX, sont créées (X correspond à 0, 1, 2 ou 3). Ces interfaces sont allouées pour des liaisons montantes vers des commutateurs ToR (Top-of-Rack) et pour la tunnellation de superposition NSX-T Data Center.

Lorsque vous créez le nœud de transport NSX Edge, vous pouvez sélectionner des interfaces fp-ethX à associer aux liaisons montantes et au tunnel de superposition. Vous pouvez décider du mode d'utilisation des interfaces fp-ethX.

Sur le commutateur distribué vSphere ou le commutateur vSphere Standard, vous devez allouer au moins deux vmnics au dispositif NSX Edge : l'un pour la gestion de NSX Edge, l'autre pour les liaisons montantes et les tunnels.

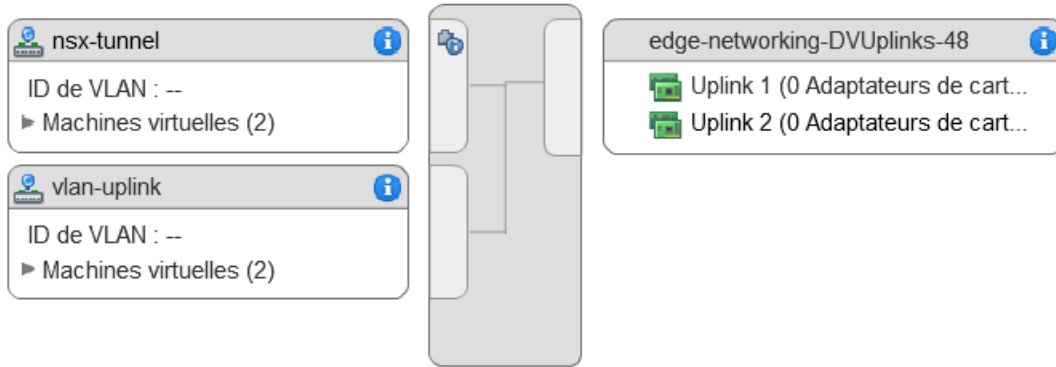
Dans l'exemple de topologie physique suivant, fp-eth0 est utilisé pour le tunnel de superposition NSX-T Data Center. fp-eth1 est utilisé pour la liaison montante du VLAN. fp-eth2 et fp-eth3 ne sont pas utilisés. vNIC1 est attribué au réseau de gestion.

Figure 9-2. 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.

Les groupes de ports de tunnel et de machines virtuelles de liaison montante configurés pour le dispositif NSX Edge n'ont pas besoin d'être associés aux ports VMkernel ou aux adresses IP données. En effet, ils sont utilisés dans la couche 2 uniquement. Si votre déploiement utilise DHCP pour fournir une adresse à l'interface de gestion, assurez-vous qu'une seule carte réseau est affectée au réseau de gestion.

Notez que les groupes de ports de réseau virtuel et de tunnel sont configurés en tant que ports de jonction. Cela est obligatoire. 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).**

Si vous utilisez un système NSX Edge basé sur un dispositif ou sur une machine virtuelle, vous pouvez utiliser des vSwitch standard ou des commutateurs distribués 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.

Vous pouvez éventuellement installer plusieurs dispositifs/machines virtuelles NSX Edge sur un même hôte, et les mêmes groupes de ports de gestion, de réseau local virtuel et de point de terminaison de tunnel peuvent être utilisés par tous les systèmes NSX Edge installés.

Une fois que les liens physiques sous-jacents sont activés et que les groupes de ports de machine virtuelle sont configurés, vous pouvez installer NSX Edge.

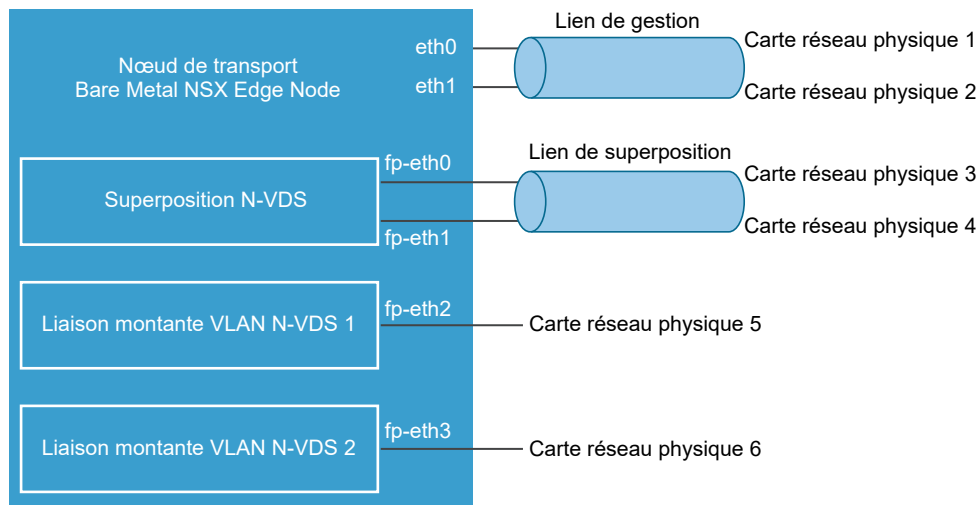
Mise en réseau de NSX Edge sur un système nu

NSX Edge installé sur un système nu contient des interfaces internes appelées fp-ethX, où X correspond à 0, 1, 2, 3 ou 4. Le nombre d'interfaces fp-ethX créées dépend du nombre de cartes réseau physiques que votre système nu NSX Edge possède. Jusqu'à quatre de ces interfaces peuvent être allouées pour des liaisons montantes à des commutateurs ToR (Top-of-Rack) et pour la tunellisation de superposition NSX-T Data Center.

Lorsque vous créez le nœud de transport NSX Edge, vous pouvez sélectionner des interfaces fp-ethX à associer aux liaisons montantes et au tunnel de superposition.

Vous pouvez décider du mode d'utilisation des interfaces fp-ethX. 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.

Figure 9-3. Configuration de lien suggérée pour la mise en réseau de NSX Edge sur système nu



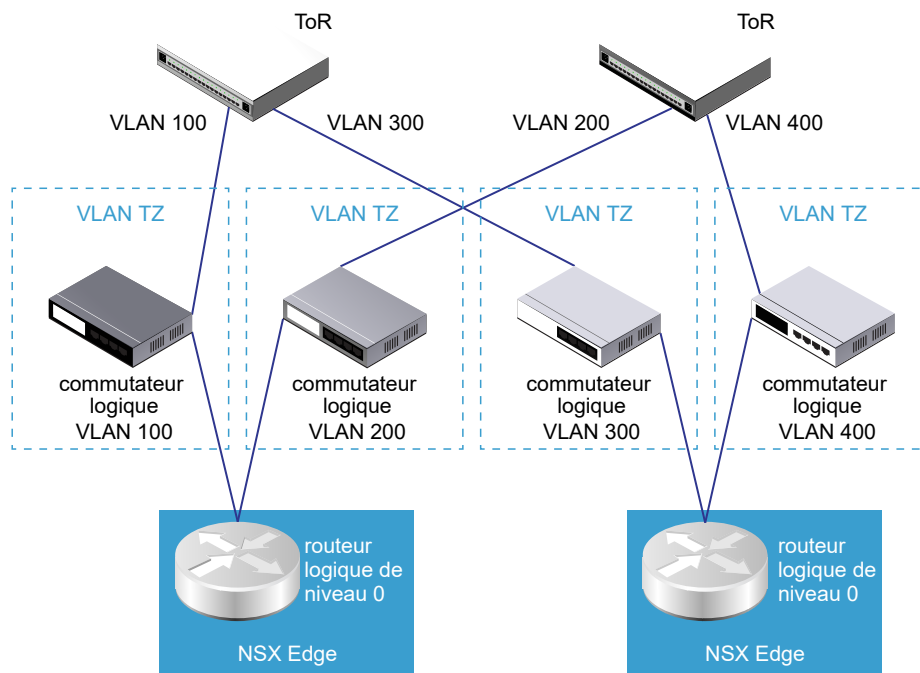
Redondance de liaison montante NSX Edge

La redondance de liaison montante NSX Edge permet à deux liaisons montantes ECMP de réseau local virtuel d'être utilisées sur la connexion réseau TOR NSX Edge dirigée vers l'extérieur.

Si vous disposez de deux liaisons montantes ECMP VLAN, vous devez également disposer de deux commutateurs ToR pour assurer une haute disponibilité et une connectivité entièrement maillée. Chaque commutateur logique de réseau virtuel possède un ID de réseau virtuel associé.

Lorsque vous ajoutez un système NSX Edge à une zone de transport de réseau virtuel, un nouveau N-VDS est installé. Par exemple, si vous ajoutez un nœud NSX Edge à quatre zones de transport de réseau virtuel, comme indiqué dans la figure, quatre N-VDS sont installés sur le dispositif NSX Edge.

Figure 9-4. Configuration VLAN ECMP suggérée pour la communication entre dispositifs NSX Edge et ToR



Note Pour une machine virtuelle Edge déployée sur un hôte ESXi disposant du vSphere Distributed Switch (vDS) et non du N-VDS, vous devez procéder comme suit :

- Activez la fausse transmission pour que DHCP fonctionne.
- Activez le mode Proximité pour que la machine virtuelle 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.

Méthodes d'installation de NSX Edge

Installez NSX Edge sur un hôte ESXi à l'aide de l'interface utilisateur de NSX Manager (méthode recommandée), de vSphere Web Client ou de l'outil OVF de ligne de commande vSphere.

Méthodes d'installation de NSX Edge

Méthode d'installation	Instructions
NSX Manager (méthode recommandée pour installer un dispositif de machine virtuelle NSX Edge uniquement)	<ul style="list-style-type: none"> ■ Assurez-vous que la configuration réseau requise de NSX Edge est respectée. Reportez-vous à la section Conditions d'installation de NSX Edge. ■ Créez un nœud de transport NSX Edge. Reportez-vous à la section Créer un nœud de transport NSX Edge. ■ Créez un cluster NSX Edge. Reportez-vous à la section Créer un cluster NSX Edge.
vSphere Web Client ou outil OVF de ligne de commande vSphere	<ul style="list-style-type: none"> ■ Assurez-vous que la configuration réseau requise de NSX Edge est respectée. Reportez-vous à la section Conditions d'installation de NSX Edge. ■ Choisissez vSphere Web Client ou l'outil OVF de ligne de commande vSphere pour installer NSX Edge. <ul style="list-style-type: none"> ■ (Web Client) Installez NSX Edge sur ESXi. Reportez-vous à la section Installer un dispositif NSX Edge sur ESXi à l'aide de l'interface utilisateur graphique de vSphere. ■ (Outil OVF de ligne de commande) Installez NSX Edge sur ESXi. Reportez-vous à la section Installer NSX Manager sur ESXi à l'aide de l'outil OVF de ligne de commande. ■ Joignez NSX Edge au plan de gestion. Reportez-vous à la section Relier NSX Edge au plan de gestion. ■ Configurez un dispositif NSX Edge en tant que nœud de transport. Reportez-vous à la section Configurer un dispositif NSX Edge en tant que nœud de transport. ■ Créez un cluster NSX Edge. Reportez-vous à la section Créer un cluster NSX Edge.
(Serveur Bare Metal) ISO (mode automatisé ou interactif par le biais d'un fichier ISO) ou en tant que dispositif de machine virtuelle NSX Edge	<p>Vous pouvez configurer l'installation automatisée de NSX Edge sur un serveur Bare Metal ou installer NSX Edge en tant que dispositif de machine virtuelle avec PXE. Notez que la procédure d'installation via l'environnement de démarrage PXE n'est pas prise en charge sur NSX Manager.</p> <ul style="list-style-type: none"> ■ Assurez-vous que la configuration réseau requise de NSX Edge est respectée. Reportez-vous à la section Conditions d'installation de NSX Edge. ■ Préparez le serveur PXE. Reportez-vous à la section Préparer le serveur PXE pour NSX Edge. Choisissez l'une des méthodes d'installation prises en charge : <ul style="list-style-type: none"> ■ (Installation automatisée) Installez NSX Edge par le biais d'un fichier ISO sur un serveur Bare Metal. Reportez-vous à la section Installer NSX Edge automatiquement via un fichier ISO. ■ (Installation automatisée) Installez NSX Edge par le biais d'un fichier ISO en tant que dispositif virtuel. Reportez-vous à la section Installer NSX Edge par le biais d'un fichier ISO en tant que dispositif virtuel. ■ (Installation manuelle) Installez manuellement NSX Edge par le biais d'un fichier ISO. Reportez-vous à la section Installer NSX Edge de manière interactive via un fichier ISO. ■ Joignez NSX Edge au plan de gestion. Reportez-vous à la section Relier NSX Edge au plan de gestion.

Méthode d'installation	Instructions
	<ul style="list-style-type: none"> ■ Configurez un dispositif NSX Edge en tant que nœud de transport. Reportez-vous à la section Configurer un dispositif NSX Edge en tant que nœud de transport. ■ Créez un cluster NSX Edge. Reportez-vous à la section Créer un cluster NSX Edge.

Créer un nœud de transport NSX Edge

Vous pouvez ajouter une machine virtuelle NSX Edge à l'infrastructure NSX-T Data Center et ensuite la configurer comme machine virtuelle de nœud de transport NSX Edge.

Un nœud NSX Edge est un nœud de transport qui exécute les démons du plan de contrôle local et les moteurs de transfert implémentant le plan de données NSX-T. Il exécute une instance du commutateur virtuel NSX-T appelé commutateur virtuel distribué NSX ou N-VDS. Les nœuds Edge sont des dispositifs de service dédiés à l'exécution de services réseau centralisés qui ne peuvent pas être distribués aux hyperviseurs. Ils peuvent être instanciés en tant que dispositif complet ou dans un facteur de forme de machine virtuelle. Ils sont regroupés en un ou plusieurs clusters, représentant un pool de capacité.

Un dispositif NSX Edge peut appartenir à une zone de transport de superposition et à plusieurs zones de transport VLAN. Un 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 certificat s'il en existe déjà un.

Conditions préalables

- Des zones de transport doivent être configurées. Reportez-vous à la section [Créer des zones de transport](#).
- Vérifiez qu'un gestionnaire de calcul est configuré. Reportez-vous à la section [Ajouter un gestionnaire de calcul](#).
- Un profil de liaison montante doit être configuré ou vous pouvez utiliser le profil de liaison montante par défaut pour les nœuds NSX Edge. Reportez-vous à la section [Créer un profil de liaison montante](#).
- Un pool d'adresses IP doit être configuré et doit être disponible dans le déploiement réseau. Reportez-vous à la section [Créer un pool d'adresses IP pour les adresses IP des points de terminaison de tunnel](#).

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.

2 Sélectionnez **Système > Infrastructure > Nœuds > Nœuds de transport 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 Pour des performances optimales, réservez de la mémoire pour le dispositif NSX Edge.

Définissez la réservation de manière à garantir que NSX Edge dispose de suffisamment de mémoire pour s'exécuter efficacement. Reportez-vous à la section [Configuration système requise des machines virtuelles NSX Edge](#).

6 Spécifiez les mots de passe d'interface de ligne de commande et racine pour NSX Edge.

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

- Au moins 12 caractères
- Au moins une lettre minuscule
- Au moins une lettre majuscule
- Au moins un chiffre
- Au moins un caractère spécial
- Au moins cinq caractères différents
- Les règles de complexité de mot de passe par défaut sont appliquées par les arguments du module PAM Linux suivants :
 - `retry=3` : nombre maximal de fois qu'un nouveau mot de passe peut être entré, 3 fois au maximum pour cet argument, avant de renvoyer une erreur.
 - `minlen=12` : taille minimale acceptable pour le nouveau mot de passe. En plus du nombre de caractères dans le nouveau mot de passe, un crédit (de +1 dans la longueur) est donné pour chaque type de caractère différent (autre, supérieur, inférieur et chiffre).
 - `difok=0` : nombre minimal d'octets qui doivent être différents dans le nouveau mot de passe. Indique la similarité entre l'ancien et le nouveau mot de passe. Avec une valeur 0 attribuée à `difok`, il n'est pas nécessaire que l'ancien et le nouveau mot de passe soient différents. Une correspondance exacte est autorisée.
 - `lcredit=1` : crédit maximal pour avoir des lettres minuscules dans le nouveau mot de passe. Si vous avez au maximum 1 lettre minuscule, chaque lettre compte +1 pour répondre à la valeur `minlen` actuelle.
 - `ucredit=1` : crédit maximal pour avoir des lettres majuscules dans le nouveau mot de passe. Si vous avez au maximum 1 lettre majuscule, chaque lettre compte +1 pour répondre à la valeur `minlen` actuelle.

- `dcredit=1` : crédit maximal pour avoir des chiffres dans le nouveau mot de passe. Si vous avez au maximum 1 chiffre, chaque chiffre compte +1 pour répondre à la valeur `minlen` actuelle.
- `ocredit=1` : crédit maximal pour avoir d'autres caractères dans le nouveau mot de passe. Si vous avez au maximum 1 autre caractère, chaque caractère compte +1 pour répondre à la valeur `minlen` actuelle.
- `enforce_for_root` : le mot de passe est défini pour l'utilisateur racine.

Note Pour plus d'informations sur le module PAM Linux pour vérifier le mot de passe par rapport aux mots du dictionnaire, reportez-vous à la page `man`.

Par exemple, évitez les mots de passe simples et systématiques tels que **VMware123!123** ou **VMware12345**. Les mots de passe qui répondent aux normes de complexité ne sont pas simples et systématiques, mais il s'agit d'une combinaison de lettres, de caractères spéciaux et de chiffres, comme **VMware123!45**, **VMware1!2345** ou **VMware@1az23x**.

7 Entrez les détails de NSX Edge.

Option	Description
Gestionnaire de calcul	Sélectionnez le gestionnaire de calcul dans le menu déroulant. Le gestionnaire de calcul est le dispositif vCenter Server enregistré dans le plan de gestion.
Cluster	Désignez le cluster que NSX Edge va rejoindre dans le menu déroulant.
Pool de ressources ou hôte	Attribuez un pool de ressources ou un hôte spécifique pour NSX Edge dans le menu déroulant.
Banque de données	Dans le menu déroulant, sélectionnez une banque de données pour les fichiers de NSX Edge.

8 Entrez les détails de l'interface NSX Edge.

Option	Description
Attribution IP	Il s'agit de l'adresse IP attribuée au nœud NSX Edge, qui est requise pour communiquer avec NSX Manager et NSX Controller. Sélectionnez l'adressage IP DHCP ou Statique . Si vous sélectionnez Statique , spécifiez des valeurs pour les champs suivants : <ul style="list-style-type: none"> ■ Adresse IP de gestion : entrez l'adresse IP de NSX Edge dans la notation CIDR. ■ Passerelle par défaut : entrez l'adresse IP de passerelle de NSX Edge.
Interface de gestion	Sélectionnez l'interface réseau de gestion dans le menu déroulant. Ces interfaces doivent être accessibles depuis NSX Manager ou doivent se trouver dans la même interface de gestion que NSX Manager et NSX Controller. L'interface de gestion de NSX Edge établit la communication avec l'interface de gestion de NSX Manager.

9 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.

Note Les nœuds NSX Edge prennent en charge plusieurs tunnels de superposition (multi-TEP) lorsque les conditions prérequis suivantes sont satisfaites :

- La configuration TEP doit être effectuée uniquement sur un N-VDS.
 - Tous les TEP doivent utiliser le même VLAN de transport pour le trafic de superposition.
 - Toutes les adresses IP de TEP doivent se trouver dans le même sous-réseau et utiliser la même passerelle par défaut.
-

10 Entrez les informations N-VDS.

Option	Description
Nom du commutateur Edge	Sélectionnez un commutateur de superposition ou VLAN dans le menu déroulant.
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	<p>L'adresse IP est attribuée au commutateur NSX Edge qui est configuré. Elle est utilisée pour router les paquets sur un réseau de superposition ou VLAN. Sélectionnez Utiliser le pool IP ou Utiliser la liste d'adresses IP statiques pour le N-VDS de superposition.</p> <ul style="list-style-type: none"> ■ Si vous sélectionnez Utiliser la liste d'adresses IP statiques, spécifiez des valeurs pour les champs suivants : <ul style="list-style-type: none"> ■ Liste d'adresses IP statiques : entrez une liste d'adresses IP séparées par des virgules à utiliser par le commutateur NSX Edge. ■ Passerelle : entrez l'adresse IP de passerelle par défaut, qui sert à acheminer les paquets entre les nœuds de transport NSX Edge dans un réseau de superposition. ■ Masque de sous-réseau : entrez le masque de sous-réseau de la passerelle configurée. ■ Si vous avez sélectionné l'option Utiliser le pool IP pour l'attribution d'adresse IP, spécifiez le nom du pool d'adresses IP.
Interfaces du chemin d'accès rapide DPDK/cartes réseau virtuelles	<p>Sélectionnez le nom d'interface du chemin de données pour l'interface de liaison montante.</p> <p>Note Si le profil de liaison montante appliqué au nœud Edge utilise une stratégie d'association nommée, assurez-vous que la condition suivante est remplie :</p> <ul style="list-style-type: none"> ■ Toutes les liaisons montantes dans la stratégie d'association par défaut doivent être mappées aux interfaces réseau physiques sur la machine virtuelle Edge pour que le trafic circule via un commutateur logique qui utilise les stratégies d'association nommées.

Note

- Le profil LLDP n'est pas pris en charge sur un dispositif de machine virtuelle NSX Edge.
- Les interfaces de liaison montante sont affichées sous la forme **Interfaces du chemin d'accès rapide DPDK** si le dispositif NSX Edge est installé à l'aide de NSX Manager ou sur un serveur bare metal.
- Les interfaces de liaison montante sont affichées sous la forme **Cartes réseau virtuelles** si NSX Edge est installé manuellement à l'aide de vCenter Server.

11 Observez l'état de connexion sur la page **Nœuds de Transport**.

Une fois que vous avez ajouté NSX Edge comme nœud de transport, l'état de la connexion devient actif en 10 à 12 minutes.

12 (Facultatif) Affichez le nœud de transport à l'aide de l'appel d'API GET `https://<nsx-manager>/api/v1/transport-nodes/<transport-node-id>`.

13 (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`.

- 14** Après la migration d'un nœud NSX Edge vers un nouvel hôte à l'aide de vCenter Server, l'interface utilisateur de NSX Manager peut signaler des détails de configuration périmés (calcul, banque de données, réseau, SSH, NTP, DNS, recherche de domaines) de NSX Edge. Pour obtenir les informations de configuration les plus récentes de NSX Edge sur le nouvel hôte, exécutez la commande API.

```
POST api/v1/transport-nodes/<transport-node-id>?
action=refresh_node_configuration&resource_type=EdgeNode
```

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'équilibreur 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.
- Avant de joindre le nœud au cluster, vérifiez que le nœud NSX Edge est stable, avec tous les services actifs et en cours d'exécution et que tous les groupes sont stables.
- Reliez les dispositifs NSX Edge au plan de gestion.
- Ajoutez les dispositifs NSX Edge en tant que nœuds de transport.
- (Facultatif) Créez un profil de cluster NSX Edge pour la haute disponibilité (HA). 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** Sélectionnez **Système > Infrastructure > Nœuds > Clusters Edge > Ajouter**.
- 3** Entrez un nom pour le cluster NSX Edge.

- 4 Sélectionnez un profil de cluster NSX Edge dans le menu déroulant.
- 5 Dans le menu déroulant Type de membre, sélectionnez **Nœud Edge** si la machine virtuelle est déployée sur site ou **Passerelle de cloud public** si la machine virtuelle est déployée dans un cloud public.
- 6 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*.

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

Vous pouvez utiliser vSphere Web Client ou vSphere Client pour installer de manière interactive un dispositif NSX Edge sur ESXi.

Note À partir de NSX-T Data Center 2.5.1, la machine virtuelle NSX Edge prend en charge vMotion.

Conditions préalables

Consultez les conditions de réseau de NSX Edge dans [Conditions d'installation de NSX Edge](#).

Procédure

- 1 Localisez le fichier OVA du dispositif NSX Edge sur le portail de téléchargement de VMware. Copiez l'URL de téléchargement ou téléchargez le fichier OVA sur votre ordinateur.
- 2 Dans vSphere Client, sélectionnez l'hôte sur lequel installer le dispositif NSX Edge.
- 3 Cliquez avec le bouton droit et sélectionnez **Déployer un modèle OVF** pour démarrer l'Assistant d'installation.
- 4 Entrez l'URL de téléchargement de l'OVA ou accédez au fichier OVA enregistré.
- 5 Entrez un nom pour la machine virtuelle NSX Edge.
Le nom saisi s'affiche dans l'inventaire.
- 6 Sélectionnez une ressource de calcul pour le dispositif NSX Edge.
- 7 Pour des performances optimales, réservez de la mémoire pour le dispositif NSX Edge.
Définissez la réservation de manière à garantir que NSX Edge dispose de suffisamment de mémoire pour s'exécuter efficacement. Reportez-vous à la section [Configuration système requise des machines virtuelles NSX Edge](#).
- 8 Vérifiez les informations du modèle OVF.

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

10 Acceptez l'interface réseau source et de destination par défaut.

Vous pouvez accepter la destination réseau par défaut pour le reste des réseaux et modifier la configuration du réseau une fois NSX Edge déployé.

11 Sélectionnez l'allocation d'adresse IP dans le menu déroulant.

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

Note Dans la fenêtre Personnaliser le modèle, ignorez le message Toutes les propriétés ont des valeurs valides qui s'affiche même avant l'entrée de valeurs dans l'un des champs. Ce message s'affiche, car tous les paramètres sont facultatifs. La validation réussit puisque vous n'avez entré aucune valeur dans l'un des champs.

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

- Au moins 12 caractères
- Au moins une lettre minuscule
- Au moins une lettre majuscule
- Au moins un chiffre
- Au moins un caractère spécial
- Au moins cinq caractères différents
- Les règles de complexité de mot de passe par défaut sont appliquées par les arguments du module PAM Linux suivants :
 - `retry=3` : nombre maximal de fois qu'un nouveau mot de passe peut être entré, 3 fois au maximum pour cet argument, avant de renvoyer une erreur.
 - `minlen=12` : taille minimale acceptable pour le nouveau mot de passe. En plus du nombre de caractères dans le nouveau mot de passe, un crédit (de +1 dans la longueur) est donné pour chaque type de caractère différent (autre, supérieur, inférieur et chiffre).
 - `difok=0` : nombre minimal d'octets qui doivent être différents dans le nouveau mot de passe. Indique la similarité entre l'ancien et le nouveau mot de passe. Avec une valeur 0 attribuée à `difok`, il n'est pas nécessaire que l'ancien et le nouveau mot de passe soient différents. Une correspondance exacte est autorisée.
 - `lcredit=1` : crédit maximal pour avoir des lettres minuscules dans le nouveau mot de passe. Si vous avez au maximum 1 lettre minuscule, chaque lettre compte +1 pour répondre à la valeur `minlen` actuelle.

- `ucredit=1` : crédit maximal pour avoir des lettres majuscules dans le nouveau mot de passe. Si vous avez au maximum 1 lettre majuscule, chaque lettre compte +1 pour répondre à la valeur `minlen` actuelle.
- `dcredit=1` : crédit maximal pour avoir des chiffres dans le nouveau mot de passe. Si vous avez au maximum 1 chiffre, chaque chiffre compte +1 pour répondre à la valeur `minlen` actuelle.
- `ocredit=1` : crédit maximal pour avoir d'autres caractères dans le nouveau mot de passe. Si vous avez au maximum 1 autre caractère, chaque caractère compte +1 pour répondre à la valeur `minlen` actuelle.
- `enforce_for_root` : le mot de passe est défini pour l'utilisateur racine.

Note Pour plus d'informations sur le module PAM Linux pour vérifier le mot de passe par rapport aux mots du dictionnaire, reportez-vous à la page `man`.

Par exemple, évitez les mots de passe simples et systématiques tels que **VMware123!123** ou **VMware12345**. Les mots de passe qui répondent aux normes de complexité ne sont pas simples et systématiques, mais il s'agit d'une combinaison de lettres, de caractères spéciaux et de chiffres, comme **VMware123!45**, **VMware1!2345** ou **VMware@1az23x**.

- 13 (Facultatif) Si un dispositif NSX Manager est disponible et que vous souhaitez enregistrer le dispositif NSX Edge avec le plan de gestion pendant le déploiement d'OVA, renseignez les champs Adresse IP, Empreinte numérique et Jeton du gestionnaire.
 - a Entrez l'adresse IP et l'empreinte numérique du nœud NSX Managerparent.
 - b Exécutez l'appel d'API POST `https://<nsx-manager>/api/v1/aaa/registration-token` pour récupérer le jeton NSX Manager.

```
{
  "token": "4065a7c0-9658-4058-bb01-c149f20f238a",
  "roles": [
    "enterprise_admin"
  ],
  "user": "admin"
}
```

- c Entrez le jeton de NSX Manager.

Note Le champ UUID du nœud est uniquement destiné à une utilisation interne. Laissez le champ vide.

- 14 Entrez le nom d'hôte de la machine virtuelle NSX Edge.
- 15 Entrez la passerelle par défaut, l'adresse IPv4 du réseau de gestion, le masque du réseau de gestion, le DNS et l'adresse IP NTP.

Note Ignorez les paramètres VMC. Entrez uniquement des valeurs pour les déploiements de VMC.

- 16** (Facultatif) N'activez pas SSH si vous préférez accéder à NSX Edge à l'aide de la console. Cependant, si vous souhaitez la connexion SSH racine et la connexion CLI à la ligne de commande de NSX Edge, activez l'option SSH.

Par défaut, l'accès SSH est désactivé pour des raisons de sécurité.

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

L'installation peut prendre 7 à 8 minutes.

- 18** 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.

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

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

- 20** Exécutez la commande `get interface eth0` (sans VLAN) ou `get interface eth0.<vlan_ID>` (avec un VLAN) pour vérifier que l'adresse IP a été appliquée comme prévu.

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

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

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

- 21** Exécutez la commande `get managers` pour vérifier que NSX Edge est enregistré.

```
- 10.29.14.136 Standby
- 10.29.14.135 Standby
- 10.29.14.134 Connected
```

- 22** Si NSX Edge n'est pas enregistré dans le plan de gestion, reportez-vous à la section [Relier NSX Edge au plan de gestion](#).

23 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.

24 Résolvez les problèmes de connectivité.

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

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

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

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

Étape suivante

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

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.

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](#).
- Assurez-vous qu'une banque de données est configurée et accessible sur l'hôte ESXi.
- Vérifiez que vous disposez de l'adresse IP et de la passerelle, des adresses IP du serveur DNS, de la liste de recherche de domaines et de l'adresse IP du serveur NTP que NSX Manager utilisera.
- Créez le réseau du groupe de ports de machines virtuelles cible, si celui-ci n'existe pas déjà. Placez les dispositifs NSX-T Data Center sur un réseau de machines virtuelles de gestion.

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

- Planifiez votre schéma d'adressage IP IPv4 NSX Manager.
- Consultez les conditions de réseau de NSX Edge dans [Conditions d'installation 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 4.3 ou ultérieure.
- Prenez connaissance des paramètres que vous pouvez utiliser pour déployer une machine virtuelle NSX Edge et la joindre au plan de gestion.

Nom du champ	Paramètre OVF	Type de champ
Mot de passe racine du système	nsx_passwd_0	Obligatoire pour effectuer l'installation de NSX Edge.
Mot de passe d'administrateur CLI	nsx_cli_passwd_0	Obligatoire pour effectuer l'installation de NSX Edge.
Mot de passe d'audit CLI	nsx_cli_audit_passwd_0	Facultatif
Nom d'utilisateur d'administrateur CLI	nsx_cli_username	Facultatif
Nom d'utilisateur d'audit CLI	nsx_cli_audit_username	Facultatif
Adresse IP de NSX Manager	mpIp	Obligatoire pour joindre la machine virtuelle NSX Edge à NSX Manager.
Jeton de NSX Manager	mpToken	Obligatoire pour joindre la machine virtuelle NSX Edge à NSX Manager. Pour récupérer le jeton, sur NSX Manager, exécutez POST <code>https://<nsx-manager>/api/v1/aaa/registration-token</code> .
Empreinte numérique de NSX Manager	mpThumbprint	Obligatoire pour joindre la machine virtuelle NSX Edge à NSX Manager. Pour récupérer l'empreinte numérique, sur le nœud NSX Manager, exécutez <code>get certificate api thumbprint</code> .

Nom du champ	Paramètre OVF	Type de champ
ID de nœud	mpNodeId	Destiné à une utilisation interne.
Nom d'hôte	nsx_hostname	Facultatif
Passerelle IPv4 par défaut	nsx_gateway_0	Facultatif
Adresse IP du réseau de gestion	nsx_ip_0	Facultatif
Masque du réseau de gestion	nsx_netmask_0	Facultatif
Serveurs DNS	nsx_dns1_0	Facultatif
Suffixe de recherche de domaines	nsx_domain_0	Facultatif
Serveurs NTP	nsx_ntp_0	Facultatif
Le service SSH est-il activé ?	nsx_isSSHEnabled	Facultatif
SSH est-il activé pour la connexion racine ?	nsx_allowSSHRootLogin	Facultatif

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
--prop:mpIp=<NSXManager-IP>
```

```
--prop:mpToken=<NSXManager-Token>
--prop:mpThumbprint=<NSXManager-Thumbprint>
<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
--prop:mpIp=<NSXManager-IP>
--prop:mpToken=<NSXManager-Token>
```

```
--prop:mpThumbprint=<NSXManager-Thumbprint>
<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
```

- ◆ Pour des performances optimales, réservez de la mémoire pour le dispositif.
Définissez la réservation de manière à garantir que NSX Manager dispose de suffisamment de mémoire pour s'exécuter efficacement. Reportez-vous à la section [Configuration système requise pour le nœud de transport hôte et la machine virtuelle NSX Manager](#).
- ◆ Ouvrez la console de NSX Edge pour suivre le processus de démarrage.
- ◆ Une fois que NSX Edge a démarré, connectez-vous à l'interface de ligne de commande avec des informations d'identification d'administrateur.
- ◆ Exécutez la commande `get interface eth0` (sans VLAN) ou `get interface eth0.<vlan_ID>` (avec un VLAN) pour vérifier que l'adresse IP a été appliquée comme prévu.

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

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

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

- ◆ 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.
- ◆ Réolvez les problèmes de connectivité.

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

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

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

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

Étape suivante

Si vous n'avez pas joint 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 [Conditions d'installation de NSX Edge](#).

Procédure

- 1 Accédez à votre compte MyVMware (myvmware.com) et accédez à **VMware NSX-T Data Center > Téléchargements**.

- 2 Localisez et téléchargez le fichier ISO pour NSX Edge.
- 3 Dans vSphere Client, sélectionnez la banque de données hôte.
- 4 Sélectionnez **Fichiers > Télécharger des fichiers > Télécharger un fichier vers une banque de données**, accédez au fichier ISO, puis téléchargez-le.

Si vous utilisez un certificat auto-signé, ouvrez l'adresse IP dans un navigateur, acceptez le certificat et téléchargez à nouveau le fichier ISO.

- 5 Dans l'inventaire de vSphere Client, sélectionnez l'hôte sur lequel vous avez téléchargé le fichier ISO. ou dans le vSphere Client,
- 6 Cliquez avec le bouton droit et sélectionnez **Nouvelle machine virtuelle**.
- 7 Sélectionnez une ressource de calcul pour le dispositif NSX Edge.
- 8 Sélectionnez une banque de données pour stocker les fichiers du dispositif NSX Edge.
- 9 Acceptez la compatibilité par défaut pour votre machine virtuelle NSX Edge.
- 10 Sélectionnez les systèmes d'exploitation ESXi pris en charge pour votre machine virtuelle NSX Edge.
- 11 Configurez le matériel virtuel.

- Nouveau disque dur - **200 Go**
- Nouveau réseau - **Réseau de la VM**
- Nouveau lecteur de CD/DVD - **Fichier ISO de la banque de données**

Vous devez cliquer sur **Connecter** pour lier le fichier ISO NSX Edge à la machine virtuelle.

- 12 Mettez sous-tension la nouvelle machine virtuelle NSX Edge.
- 13 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.

Lors de l'installation, le programme d'installation vous invite à entrer un ID de VLAN pour l'interface de gestion. Sélectionnez **Oui** et entrez un ID de VLAN pour créer une sous-interface VLAN pour l'interface réseau. Sélectionnez **Non** si vous ne voulez pas configurer le balisage VLAN sur le paquet.

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

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

- 14** Pour des performances optimales, réservez de la mémoire pour le dispositif NSX Edge.

Définissez la réservation de manière à garantir que NSX Edge dispose de suffisamment de mémoire pour s'exécuter efficacement. Reportez-vous à la section [Configuration système requise des machines virtuelles NSX Edge](#).

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

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

- 16** Il existe trois façons de configurer une interface de gestion.

Note Si le serveur utilise des cartes réseau Mellanox, ne configurez pas le dispositif Edge dans l'interface de gestion en bande.

- Interface sans balise. Ce type d'interface crée une interface de gestion hors bande.

(DHCP) `set interface eth0 dhcp plane mgmt`

(Statique) `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt`

- Interface avec balise.

`set interface eth0 vlan <vlan_ID> plane mgmt`

(DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

```
(Statique) set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane
mgmt
```

- Interface en bande.

```
set interface mac <mac_address> vlan <vlan_ID> in-band plane mgmt
```

```
(DHCP) set interface eth0.<vlan_ID> dhcp plane mgmt
```

```
(Statique) set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane
mgmt
```

17 (Facultatif) Démarrez le service SSH. Exécutez `start service ssh`.

18 Exécutez la commande `get interface eth0` (sans VLAN) ou `get interface eth0.<vlan_ID>` (avec un VLAN) pour vérifier que l'adresse IP a été appliquée comme prévu.

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

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

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

19 (Interface avec balise et interface en bande) Toute interface de gestion VLAN existante doit être effacée avant d'en créer une nouvelle.

```
Clear interface eth0.<vlan_ID>
```

Pour définir une nouvelle interface, reportez-vous à l'étape 15.

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

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

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

21 Résolvez les problèmes de connectivité.

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

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

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

Si vous n'avez pas joint NSX Edge au plan de gestion, reportez-vous à la section [Relier NSX Edge au plan de gestion](#).

Installer un dispositif NSX Edge sur un système Bare Metal

Utilisez le serveur PXE pour automatiser l'installation de NSX Edge sur un serveur sans système d'exploitation ou utilisez un fichier ISO pour installer NSX Edge en tant que dispositif de machine virtuelle ou sur un serveur bare metal.

L'installation via l'environnement de démarrage PXE n'est pas prise en charge pour NSX Manager. 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.

Conditions préalables

- Si le serveur NSX Edge bare metal exécute la version 6.7u3 ou une version antérieure, ne mettez pas à niveau NSX Edge `virtualHW.version` vers **14** ou une version ultérieure dans vCenter Server. Par défaut, `virtualHW.version` est défini sur **13**.
- Par défaut, les périphériques de liaison bare metal NSX Edge qui regroupent des périphériques Ethernet pour former un LAG sont optimisés pour l'équilibrage de charge. Par conséquent, un périphérique de liaison utilise uniquement des périphériques réseau qui se trouvent sur un nœud NUMA local dont le CPU transmet des paquets. Si les périphériques formant la liaison s'étendent sur plusieurs nœuds NUMA, mais que les CPU alloués au

traitement des paquets appartiennent à un sous-ensemble de nœuds NUMA, seuls certains périphériques envoient du trafic. En bref, tous les terminaux ne sont pas utilisés pour équilibrer le trafic qui est envoyé en dehors du périphérique de liaison. Vous ne pouvez pas désactiver l'optimisation par défaut.

Cependant, si vous souhaitez utiliser tous les périphériques Ethernet de la liaison pour équilibrer la charge du trafic, vous devez transférer tous les périphériques Ethernet vers les nœuds NUMA auxquels les CPU de traitement de paquets sont attachés.

Note Le basculement est exclusif de l'équilibrage de charge. Si le périphérique Ethernet connecté au nœud NUMA local est inactif, la liaison envoie le trafic vers l'autre périphérique, même s'il n'est pas local NUMA. L'optimisation de l'équilibrage de charge n'a pas d'incidence sur la fonctionnalité de basculement.

Préparer le serveur PXE pour 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 [Conditions d'installation 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 <manager-ip> thumbprint <manager-thumbprint> username <manager-username>
password <manager 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[...]FcoHLij0uFD
```

- 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 6tgml...`

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 sur un système sans système d'exploitation à l'aide d'un fichier ISO. Reportez-vous à la section [Installer NSX Edge automatiquement via un fichier ISO](#).

Installer NSX Edge automatiquement via un fichier ISO

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 [Conditions d'installation de NSX Edge](#).

Procédure

- 1** Accédez à votre compte MyVMware (myvmware.com) et accédez à **VMware NSX-T Data Center > Téléchargements**.
- 2** Localisez et téléchargez le fichier ISO pour NSX Edge sur un système Bare Metal.
- 3** Connectez-vous à l'interface de gestion hors bande (par exemple, Integrated Lights-Out (ILO) sur des serveurs HP) du système bare metal.
- 4** Cliquez sur **Lancer** dans l'aperçu de la console virtuelle.
- 5** Sélectionnez **Supports virtuels > Connecter des supports virtuels**.
Attendez quelques secondes que les supports virtuels se connectent.
- 6** Sélectionnez **Supports virtuels > Mapper CD/DVD** et accédez au fichier ISO.

7 Sélectionnez **Démarrage suivant > CD/DVD/ISO virtuel**.

8 Sélectionnez **Alimentation > Réinitialiser le système (démarrage à chaud)**.

La durée de l'installation dépend de l'environnement bare metal.

9 Choisissez **Installation automatique**.

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

10 Sélectionnez l'interface réseau principale applicable.

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.

11 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.

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

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

13 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**.

14 Il existe trois façons de configurer une interface de gestion.

Note Si le serveur utilise des cartes réseau Mellanox, ne configurez pas le dispositif Edge dans l'interface de gestion en bande.

- Interface sans balise. Ce type d'interface crée une interface de gestion hors bande.
 (DHCP) `set interface eth0 dhcp plane mgmt`
 (Statique) `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt`
- Interface avec balise.
`set interface eth0 vlan <vlan_ID> plane mgmt`
 (DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`
 (Statique) `set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`
- Interface en bande.


```
set interface mac <mac_address> vlan <vlan_ID> in-band plane mgmt
(DHCP) set interface eth0.<vlan_ID> dhcp plane mgmt
(Statique) set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt
```

- (Facultatif) Créez une interface **bond0** pour l'interface HA de gestion avec plusieurs interfaces.

Vous pouvez configurer une interface de gestion de liaison sur une instance de NSX Edge à l'aide de la commande CLI suivante. Utilisez la console pour effacer l'adresse IP de gestion existante avant de créer une liaison et d'y ajouter une interface.

Note Seul le mode de sauvegarde active est autorisé sur une interface de liaison. Il ne vous permet pas de configurer VLAN. Par conséquent, vous devez configurer VLAN sur un VLAN d'accès qui se situe plus près du commutateur physique.

```
set interface bond0 ip x.x.x.x/mask gateway x.x.x.x plane mgmt mode active-backup members eth0, eth1 primary eth0
```

- 15** Exécutez la commande `get interface eth0` (sans VLAN) ou `get interface eth0.<vlan_ID>` (avec un VLAN) pour vérifier que l'adresse IP a été appliquée comme prévu.

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

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

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

- 16** (Interface avec balise et interface en bande) Toute interface de gestion VLAN existante doit être effacée avant d'en créer une nouvelle.

```
clear interface eth0.<vlan_ID>
```

Pour définir une nouvelle interface, reportez-vous à l'étape 13.

- 17** Définissez des cartes réseau physiques à utiliser par le plan de données NSX-T Data Center dans la liste des périphériques PCI disponibles.

- a `get dataplane device list`
- b `set dataplane device list <NIC1>, <NIC2>, <NIC3>`
- c `restart service dataplane`

d `get physical-port`

Après la sélection des cartes réseau physiques, redémarrez les services du plan de données NSX-T Data Center pour que les modifications prennent effet.

Note Réclamez jusqu'à 16 cartes réseau physiques.

- 18** Pour éviter les erreurs de configuration réseau, vérifiez que les cartes réseau physiques sélectionnées correspondent aux cartes réseau configurées dans les profils de nœud de transport.

- 19** Avant de créer NSX Edge en tant que nœud de transport, réinitialisez la liste des cartes réseau sur le plan de données.

`reset dataplane nic list`

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

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

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

- 21** Résolvez les problèmes de connectivité.

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

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

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

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

Étape suivante

Si vous n'avez pas joint NSX Edge au plan de gestion, reportez-vous à la section [Relier NSX Edge au plan de gestion](#).

Installer NSX Edge de manière interactive via un fichier ISO

Installez des périphériques NSX Edge sur un système Bare Metal à l'aide d'un fichier ISO en mode interactif.

Conditions préalables

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

Procédure

1 Accédez à votre compte MyVMware (myvmware.com) et accédez à **VMware NSX-T Data Center > Téléchargements**.

2 Localisez et téléchargez le fichier ISO pour NSX Edge sur un système Bare Metal.

3 Connectez-vous à l'ILO du système bare metal.

4 Cliquez sur **Lancer** dans l'aperçu de la console virtuelle.

5 Sélectionnez **Supports virtuels > Connecter des supports virtuels**.

Attendez quelques secondes que les supports virtuels se connectent.

6 Sélectionnez **Supports virtuels > Mapper CD/DVD** et accédez au fichier ISO.

7 Sélectionnez **Démarrage suivant > CD/DVD/ISO virtuel**.

8 Sélectionnez **Alimentation > Réinitialiser le système (démarrage à chaud)**.

La durée de l'installation dépend de l'environnement bare metal.

9 Sélectionnez **Installation interactive**.

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

10 Dans la fenêtre Configurer le clavier, sélectionnez **Oui** si le programme d'installation doit détecter automatiquement le clavier ou **Non** si le clavier ne doit pas être détecté par la console.

11 Sélectionnez Anglais américain comme langue.

12 Dans la fenêtre Configurer le réseau, sélectionnez l'interface réseau principale applicable.

13 Entrez le nom d'hôte qui se connecte à l'interface principale sélectionnée et cliquez sur **OK**.

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.

14 Dans la fenêtre Configurer le dispositif NSX à l'aide de la fenêtre de démarrage rapide :

- Entrez l'URL du fichier de configuration de démarrage rapide de NSX si vous souhaitez automatiser la configuration de NSX sur le serveur Bare Metal.
- Laissez le champ vide si vous souhaitez configurer manuellement NSX sur le serveur Bare Metal.

15 Dans la fenêtre Partitionner les disques, sélectionnez l'une des options suivantes :

- Sélectionnez **Oui** si vous souhaitez démonter des partitions existantes afin que de nouvelles partitions puissent être créées sur des disques.
- Sélectionnez **Non** si vous souhaitez utiliser des partitions existantes.

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

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

17 Exécutez la commande `get interface eth0` (sans VLAN) ou `get interface eth0.<vlan_ID>` (avec un VLAN) pour vérifier que l'adresse IP a été appliquée comme prévu.

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

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

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

18 Résolvez les problèmes de connectivité.

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

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

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

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

Étape suivante

Si vous n'avez pas joint 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 ou une session de console sur l'un des dispositifs NSX Manager.
- 2 Ouvrez une session SSH ou une session de console sur la machine virtuelle du nœud 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
659442c1435350edbbc0e87ed5a6980d892b9118f851c17a13ec76a8b985f57
```

- 4 Sur la machine virtuelle du nœud 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 d'utilisateur du dispositif NSX Manager
- Empreinte numérique de certificat du dispositif NSX Manager
- Mot de passe du dispositif NSX Manager

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

Répétez cette commande sur chaque machine virtuelle de nœud NSX Edge.

- 5 Vérifiez le résultat en exécutant la commande `get managers` sur vos machines virtuelles de nœud NSX Edge.

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

- 6 Dans l'interface utilisateur de NSX Manager, accédez à **Système > Infrastructure > Nœuds > Nœuds de transport Edge**.

Sur la page Nœud de transport NSX Edge :

- La colonne **État de configuration** affiche Configurer NSX. Cliquez sur Configurer NSX pour commencer la configuration sur le nœud. Si la colonne **Version de NSX** n'affiche pas le numéro de version installé sur le nœud, essayez d'actualiser la fenêtre du navigateur.
- Avant de configurer NSX sur le nœud NSX Edge, les colonnes **État du nœud** et **État du tunnel** affichent l'état Non disponible. Les colonnes **Zones de transport** et **Commutateurs N-VDS** affichent 0, ce qui indique qu'aucune zone de transport n'est attachée ou qu'aucun commutateur N-VDS n'est configuré sur le nœud NSX Edge.

Étape suivante

Lors de l'installation de NSX Edge à l'aide de NSX Manager, reportez-vous à [Créer un nœud de transport NSX Edge](#).

Lors de l'installation de NSX Edge manuellement, reportez-vous à [Configurer un dispositif NSX Edge en tant que nœud de transport](#).

Configurer un dispositif NSX Edge en tant que nœud de transport

Après avoir installé manuellement NSX Edge sur ESXi ou sur un système Bare Metal, configurez un dispositif NSX Edge sur l'infrastructure NSX-T Data Center en tant que nœud de transport.

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 ne sont pas limités à NSX Edge.

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.

Conditions préalables

- Des zones de transport doivent être configurées.
- Vérifiez qu'un gestionnaire de calcul est configuré. Reportez-vous à la section [Ajouter un gestionnaire de calcul](#).
- 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 **Système > Infrastructure > Nœuds > Nœuds de transport Edge > Modifier le dispositif Edge**.
- 3 Sélectionnez le nœud de transport et cliquez sur **Modifier**.
- 4 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.

Note Plusieurs VTEP dans une zone de transport doivent être configurés sur le même segment de réseau. Si des VTEP dans une zone de transport sont configurés sur des segments de réseau différents, les sessions BFD ne peuvent pas être établies entre les VTEP.

- 5 Entrez les informations N-VDS.

Option	Description
Nom du commutateur Edge	Sélectionnez un commutateur VLAN dans le menu déroulant.
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	<p>Sélectionnez Utiliser le pool IP ou Utiliser la liste d'adresses IP statiques pour le N-VDS de superposition. Ces adresses IP sont attribuées en tant que VTEP au nœud de transport NSX Edge. Plusieurs VTEP sur un dispositif NSX Edge doivent se trouver dans le même sous-réseau.</p> <ul style="list-style-type: none"> ■ 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. ■ Si vous avez sélectionné l'option Utiliser le pool IP pour l'attribution d'adresse IP, spécifiez le nom du pool d'adresses IP.
Interfaces du chemin d'accès rapide DPDK/cartes réseau virtuelles	<p>Sélectionnez le nom d'interface du chemin de données pour l'interface de liaison montante.</p> <p>Note Pour vous assurer que le trafic circule via des commutateurs logiques configurés avec des stratégies d'association nommées, mappez toutes les liaisons montantes dans la stratégie d'association par défaut aux interfaces réseau physiques sur la machine virtuelle NSX Edge.</p>

6 Observez l'état de connexion sur la page **Nœuds de Transport**.

Une fois que vous avez ajouté NSX Edge comme nœud de transport, l'état de la connexion devient actif en 10 à 12 minutes.

7 (Facultatif) Affichez le nœud de transport à l'aide de l'appel d'API GET `https://<nsx-manager>/api/v1/transport-nodes/<transport-node-id>`.

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`.

9 Après la migration d'un nœud NSX Edge vers un nouvel hôte à l'aide de vCenter Server, l'interface utilisateur de NSX Manager peut signaler des détails de configuration périmés (calcul, banque de données, réseau, SSH, NTP, DNS, recherche de domaines) de NSX Edge. Pour obtenir les informations de configuration les plus récentes de NSX Edge sur le nouvel hôte, exécutez la commande API.

```
POST api/v1/transport-nodes/<transport-node-id>?
action=refresh_node_configuration&resource_type=EdgeNode
```

Étape suivante

Ajoutez le nœud NSX Edge à un cluster NSX Edge. Reportez-vous à la section [Créer un cluster NSX Edge](#).

Zones de transport et nœuds de transport

10

Les zones de transport et nœuds de transport sont des concepts importants dans NSX-T Data Center.

Ce chapitre contient les rubriques suivantes :

- [Créer des zones de transport](#)
- [Créer un pool d'adresses IP pour les adresses IP des points de terminaison de tunnel](#)
- [Chemin de données optimisé](#)
- [Configuration de profils](#)
- [Créer un nœud de transport d'hôte autonome ou de serveur bare metal](#)
- [Installation manuelle de modules de noyau NSX-T Data Center](#)
- [Déployer un cluster vSphere entièrement réduit pour NSX-T](#)

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 et les nœuds de transport hôtes pour leurs 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 **Système > 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.
 - Mode **Standard** qui s'applique à tous les hôtes pris en charge.
 - **Chemin de données optimisé** est un mode de pile réseau qui s'applique uniquement aux nœuds de transport de l'hôte ESXi de type version 6.7 et ultérieure qui peuvent appartenir à une zone de transport.
- 6 Si le mode N-VDS est défini sur Standard, sélectionnez un type de trafic.
Les options sont **Superposition** et **VLAN**.
- 7 Si le mode N-VDS est défini sur 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. Veillez à 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-ccbcfe50b416tz-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-ccbcfe50b416",
      "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 d'hôte autonome ou de serveur bare metal](#).

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 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 être, par exemple, 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 **Mise en réseau et sécurité avancées > Inventaire > Groupes > IP Pools > Ajouter**.
- 3 Entrez les détails du pool IP.

Option	Exemple de paramètre
Nom et description	Entrez le pool d'adresses IP et une description facultative.
Plages d'adresses IP	Plages d'allocation IP 192.168.200.100 - 192.168.200.115
Passerelle	192.168.200.1
CIDR	Adresse réseau au format CIDR 192.168.200.0/24
Serveurs DNS	Liste des serveurs DNS séparés par une virgule 192.168.66.10
Suffixe DNS	corp.local

Résultats

Le pool d'adresses IPv4 ou IPv6 est répertorié sur la page du pool d'adresses IP.

Vous pouvez également utiliser l'appel d'API GET `https://<nsx-mgr>/api/v1/pools/ip-pools` pour afficher la liste du pool d'adresses IP.

Étape suivante

Créez un profil de liaison montante. Reportez-vous à la section [Créer un profil de liaison montante](#).

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 destiné aux charges de travail NFV, qui offrent des avantages en matière de performances en exploitant la fonctionnalité DPDK.

Le commutateur N-VDS ne peut être configuré dans le mode de chemin de données optimisé que sur un hôte ESXi. ENS prend également en charge le trafic circulant à travers les machines virtuelles Edge.

En mode de chemin de données optimisé, les deux modes de trafic sont pris en charge :

- Trafic de superposition
- Trafic VLAN

Cartes réseau VMkernel prises en charge

Avec NSX-T Data Center prenant en charge plusieurs commutateurs hôtes ENS, le nombre maximal de cartes réseau VMkernel prises en charge par hôte est 32.

Processus de haut niveau 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'équilibreur 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 derniers pilotes de carte réseau depuis la [page My VMware](#).

- a Accédez à **Pilotes et outils > CD de pilote**.

- b Téléchargez des pilotes de cartes réseau :

Pilote de carte réseau VMware ESXi 6.7 ixgben-ens 1.1.3 pour les contrôleurs Intel Ethernet de la gamme 82599, x520, x540, x550 et x552

Pilote de carte réseau VMware ESXi 6.7 i40en-ens 1.1.3 pour les contrôleurs Intel Ethernet de la gamme X710, XL710, XXV710 et X722

- c Pour utiliser l'hôte comme hôte ENS, au moins une carte réseau compatible ENS doit être disponible sur le système. En l'absence de cartes réseau compatibles ENS, le plan de gestion n'autorise pas l'ajout d'hôtes aux zones de transport ENS.

- d Répertoriez le pilote ENS.

```
esxcli software vib list | grep -E "i40|ixgben"
```

- e Vérifiez si la carte réseau est capable de traiter le trafic du chemin de données d'ENS.

```
esxcfg-nics -e
```

Name	Driver	ENS Capable	ENS Driven	MAC Address	Description
vmnic0	ixgben	True	False	e4:43:4b:7b:d2:e0	Intel(R) Ethernet Controller X550
vmnic1	ixgben	True	False	e4:43:4b:7b:d2:e1	Intel(R) Ethernet Controller X550
vmnic2	ixgben	True	False	e4:43:4b:7b:d2:e2	Intel(R) Ethernet Controller X550
vmnic3	ixgben	True	False	e4:43:4b:7b:d2:e3	Intel(R) Ethernet Controller X550
vmnic4	i40en	True	False	3c:fd:fe:7c:47:40	Intel(R) Ethernet Controller X710/X557-AT 10GBASE-T
vmnic5	i40en	True	False	3c:fd:fe:7c:47:41	Intel(R) Ethernet Controller X710/X557-AT 10GBASE-T
vmnic6	i40en	True	False	3c:fd:fe:7c:47:42	Intel(R) Ethernet Controller X710/X557-AT 10GBASE-T
vmnic7	i40en	True	False	3c:fd:fe:7c:47:43	Intel(R) Ethernet Controller X710/X557-AT 10GBASE-T

- f Installez le pilote ENS.

```
esxcli software vib install -v file:///<DriverInstallerURL> --no-sig-check
```

- g Vous pouvez également télécharger le pilote sur le système et l'installer.

```
wget <DriverInstallerURL>
```

```
esxcli software vib install -v file:///<DriverInstallerURL> --no-sig-check
```

- h Redémarrez l'hôte pour charger le pilote. Passez à l'étape suivante.

- i Pour décharger le pilote, procédez comme suit :

```
vmkload_mod -u i40en
```

```
ps | grep vmkdevmgr
```

```
kill -HUP "$(ps | grep vmkdevmgr | awk {'print $1'})"
```

```
ps | grep vmkdevmgr
```

```
kill -HUP <vmkdevmgrProcessID>
```

```
kill -HUP "$(ps | grep vmkdevmgr | awk {'print $1'})"
```

- j Pour désinstaller le pilote ENS, `esxcli software vib remove --vibname=i40en-ens --force --no-live-install`.

- 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](#).

Note Zones de transport ENS configurées pour le trafic de superposition : pour une machine virtuelle Microsoft Windows exécutant une version de VMware Tools antérieure à la version 11.0.0 et lorsque le type vNIC est VMXNET3, assurez-vous que le MTU est défini sur 1500. Pour une machine virtuelle Microsoft Windows exécutant vSphere 6.7 U1 et VMware Tools 11.0.0 et versions ultérieures, assurez-vous que le MTU est défini sur une valeur inférieure à 8900. Pour les machines virtuelles exécutant d'autres systèmes d'exploitation pris en charge, assurez-vous que le MTU de la machine virtuelle est défini sur une valeur inférieure à 8900.

- 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 d'hôte autonome ou de serveur bare metal](#).

Mode de stratégie d'association de source d'équilibreur de charge prenant en charge NUMA

Le mode de stratégie d'association d'équilibreur 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'équilibreur 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 :

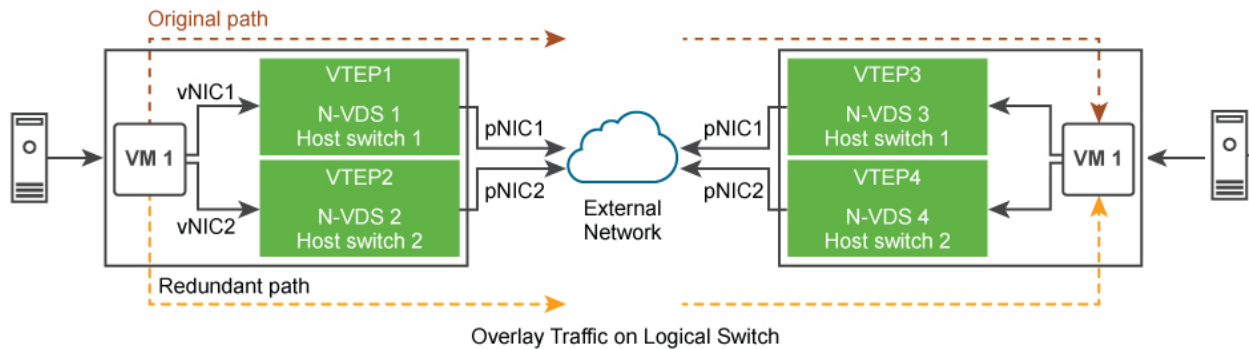
- La liaison montante LAG est configurée avec des liens physiques de plusieurs nœuds NUMA.
- La machine virtuelle bénéficie d'une affinité à plusieurs nœuds NUMA.
- L'hôte ESXi n'a pas pu définir les informations NUMA pour une machine virtuelle ou des liens physiques.

Prise en charge d'ENS pour les applications nécessitant la fiabilité du trafic

Les charges de travail NFV peuvent utiliser les fonctionnalités d'hébergement multiple et de redondance fournies par le protocole SCTP (Stream Control Transmission Protocol) pour augmenter la résilience et la fiabilité du trafic exécuté sur les applications. L'hébergement multiple est la capacité de prendre en charge des chemins redondants entre une machine virtuelle source et une machine virtuelle de destination.

Selon le nombre de cartes réseau physiques disponibles pour être utilisées comme liaison montante pour un réseau de superposition ou un VLAN, ces différents chemins réseau redondants sont disponibles pour permettre à une machine virtuelle d'envoyer le trafic à la machine virtuelle cible. Les chemins redondants sont utilisés lorsque la carte réseau physique liée à un commutateur logique est défaillante. Le commutateur de chemin de données optimisé fournit des chemins réseau redondants entre les hôtes.

Figure 10-1. Hébergement multiple et redondance du trafic sur ENS



Les tâches de haut niveau sont les suivantes :

- 1 Préparer l'hôte comme nœud de transport NSX-T Data Center.
- 2 Préparer le VLAN ou la zone de transport de superposition avec deux commutateurs N-VDS en mode de chemin de données optimisé.
- 3 Sur le N-VDS 1, lier la première carte réseau physique au commutateur.
- 4 Sur le N-VDS 2, lier la deuxième carte réseau physique au commutateur.

Le N-VDS en mode de chemin de données optimisé garantit que si la carte réseau physique 1 (pNIC1) devient indisponible, le trafic provenant de la machine virtuelle 1 est acheminé via le chemin redondant - vNIC 1 → point de terminaison de tunnel 2 → pNIC 2 → VM 2.

Configuration de profils

Les profils vous permettent de configurer de manière cohérente des fonctionnalités identiques pour tous les adaptateurs réseau sur plusieurs hôtes ou nœuds.

Les profils 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, puis les appliquer à plusieurs hôtes ou nœuds.

Créer un profil de liaison montante

Une liaison montante est un lien reliant les nœuds NSX Edge aux commutateurs ToR (Top-of-Rack) ou aux commutateurs logiques NSX-T Data Center. Une liaison est établie entre une interface réseau physique sur un nœud de NSX Edge et un commutateur.

Un profil de liaison montante définit des stratégies pour les liaisons montantes. Les paramètres définis par les profils de liaison montante peuvent inclure les stratégies d'association, les liaisons actives et en veille, l'ID de VLAN de transport et le paramètre MTU.

Configuration de liaisons montantes pour les nœuds de NSX Edge basés sur un dispositif de machine virtuelle et les nœuds de transport hôtes :

- Si la règle d'association de basculement est configurée pour un profil de liaison montante, vous ne pouvez configurer qu'une seule liaison montante active dans la stratégie d'association. Les liaisons montantes en veille ne sont pas prises en charge et ne doivent pas être configurées dans la stratégie d'association de basculement. Lorsque vous installez NSX Edge en tant que dispositif virtuel ou nœud de transport hôte, utilisez le profil de liaison montante par défaut.
- Si la stratégie d'association de source à équilibreur de charge est configurée pour un profil de liaison montante, vous pouvez configurer plusieurs liaisons montantes actives sur le même N-VDS. Chaque liaison montante est associée à une carte réseau physique avec un nom et une adresse IP distincts. L'adresse IP attribuée à un point de terminaison de liaison montante peut être configurée à l'aide de l'attribution d'adresses IP pour le N-VDS.

Vous devez utiliser la stratégie d'association **Source avec équilibreur de charge** pour l'équilibrage de charge du trafic.

Conditions préalables

- Consultez les conditions de réseau de NSX Edge dans [Conditions d'installation 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 **Système > Infrastructure > Profils > Profils de liaison montante > Ajouter**.

3 Renseignez les détails du profil de liaison montante.

Option	Description
Nom et description	<p>Entrez un nom de profil de liaison montante.</p> <p>Ajoutez une description de profil de liaison montante facultative.</p>
LAG	<p>(Facultatif) Dans la section LAG, cliquez sur Ajouter pour les 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>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, vous pouvez entrer une stratégie d'association par défaut ou vous pouvez choisir d'entrer une stratégie d'association nommée. Cliquez sur Ajouter pour ajouter une stratégie d'association de dénomination. Une stratégie d'association définit la manière dont le N-VDS utilise sa liaison montante pour la redondance et l'équilibrage de charge du trafic. Vous pouvez configurer une stratégie d'association dans les modes suivants :</p> <ul style="list-style-type: none"> ■ Ordre de basculement : sélectionnez une liaison montante active 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 d'équilibreur de charge : sélectionnez une liste de liaisons montantes actives. Lorsque vous configurez un nœud de transport, vous pouvez épingler chaque interface du nœud de transport sur une liaison montante active. Cette configuration permet l'utilisation de plusieurs liaisons montantes actives en même temps.

Option	Description
	<ul style="list-style-type: none"> ■ Adresse MAC de la source d'équilibrage de charge : sélectionnez une liaison montante sur la base d'un hash d'Ethernet source. <hr/> <p>Note</p> <ul style="list-style-type: none"> ■ Sur les hôtes KVM : seule la stratégie d'association Ordre de basculement est prise en charge, tandis que les stratégies d'association Source d'équilibreur de charge et Adresse MAC de la source d'équilibreur de charge ne sont pas prises en charge. ■ Sur NSX Edge : pour la stratégie d'association par défaut, les stratégies d'association Source d'équilibreur de charge et Ordre de basculement sont prises en charge. Pour la stratégie d'association nommée, seule la stratégie Ordre de basculement est prise en charge. ■ Sur les hôtes ESXi : les stratégies d'association Adresse MAC de la source d'équilibreur de charge, Source d'équilibreur de charge et Ordre de basculement sont prises en charge. <hr/> <p>(Hôtes ESXi et NSX Edge) 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 ou segment logique basé sur le VLAN. ■ Une stratégie d'association par défaut pour l'ensemble du N-VDS. <p>Stratégie d'association nommée : avec une stratégie d'association nommée, pour chaque commutateur logique ou segment basé sur le VLAN, vous pouvez définir un mode de stratégie d'association et des noms de liaisons montantes spécifiques. Ce type de stratégie vous donne la possibilité de sélectionner des liaisons montantes spécifiques selon la stratégie de direction du trafic, par exemple en fonction de la bande passante requise.</p> <ul style="list-style-type: none"> ■ Si vous définissez une stratégie d'association nommée, le N-VDS l'utilise si elle est attachée à la zone de transport basée sur le VLAN et finalement sélectionnée pour le commutateur logique ou le segment basé sur le VLAN lié dans l'hôte. ■ Si vous ne définissez pas de stratégies d'association nommées, le N-VDS utilise la stratégie d'association par défaut. <hr/>

- 4 Entrez une valeur du VLAN de transport. Le VLAN de transport défini dans les balises de profil de liaison montante est utilisé par le trafic de superposition uniquement et l'ID VLAN est utilisé par le point de terminaison TEP.

- 5 Entrez la valeur de MTU.

La valeur par défaut de MTU du profil de liaison montante est 1600.

Le MTU global de liaison montante physique configure la valeur de MTU de toutes les instances N-VDS dans le domaine NSX-T Data Center. Si le MTU global de liaison montante physique n'est pas spécifié, la valeur de MTU est déduite du MTU de profil de liaison montante s'il est configuré ou la valeur par défaut 1600 est utilisée. La valeur de MTU du profil de liaison montante peut remplacer la valeur de MTU de liaison montante physique globale sur un hôte spécifique.

Le MTU global d'interface logique configure la valeur de MTU de toutes les interfaces de routeur logique. Si la valeur de MTU globale d'interface logique n'est pas spécifiée, la valeur de MTU est déduite du routeur logique de niveau 0. La valeur de MTU de liaison montante du routeur logique peut remplacer sur un port spécifique la valeur de MTU globale d'interface logique.

Résultats

Outre l'interface utilisateur, vous pouvez également afficher les profils de liaison montante avec l'appel d'API GET `/api/v1/host-switch-profiles`.

Étape suivante

Créez une zone de transport. Reportez-vous à la section [Créer des zones de transport](#).

Configuration 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 du trafic système associée aux machines virtuelles et aux services d'infrastructure, comme vSphere Fault Tolerance. Le trafic système est exclusivement associé à un hôte ESXi.

Note Les profils NIOC ne peuvent pas être appliqués à des nœuds de transport NSX Edge.

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 d'un 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.

vCenter Server propage l'allocation à partir de 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.
- Réserve : 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 N-VDS

Pour garantir la bande passante minimale pour le trafic système en cours d'exécution sur les hôtes NSX-T Data Center, activez et configurez la gestion de ressources réseau sur un 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 **Système > Infrastructure > Profils > Profils NIOC > Ajouter**.
- 3 Entrez les détails du profil NIOC.

Option	Description
Nom et description	Entrez un nom de profil NIOC. Vous pouvez éventuellement entrer les détails du profil, comme les types de trafic activés.
État	Faites basculer ce bouton pour activer les allocations de bande passante répertoriées dans les ressources du trafic.
L'hôte Infra ressources du trafic	Vous pouvez accepter les ressources de trafic répertoriées par défaut. Cliquez sur Ajouter et entrez votre ressource de trafic pour personnaliser le profil NIOC. (Facultatif) Sélectionnez un type de trafic existant et cliquez sur Supprimer pour supprimer la ressource du profil NIOC.

Le 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 N-VDS en utilisant des API

Vous pouvez utiliser les 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`.

L'exemple de réponse montre le profil NIOC appliqué à l'hôte.

```
{
  "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 S'il n'existe pas de profil NIOC, 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\n\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 le fichier `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 Vérifiez les informations du profil NIOC.

```
# [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
}
```

Résultats

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.

Ajouter un profil de cluster NSX Edge

Le profil de cluster NSX Edge définit les stratégies pour le nœud de transport NSX Edge.

Conditions préalables

Vérifiez que le cluster NSX Edge est disponible.

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Système > Infrastructure > Profils > Profils de cluster Edge > Ajouter**.
- 3 Entrez les détails du profil du cluster NSX Edge.

Option	Description
Nom et description	Entrez un nom de profil de cluster NSX Edge. Vous pouvez éventuellement entrer les détails du profil, par exemple, le paramètre BFD (Bidirectional Forwarding Detection).
Intervalle de détection BFD	Acceptez le paramètre par défaut. BFD est le protocole de détection utilisé pour identifier les défaillances du chemin de transfert. Vous pouvez définir la durée de l'intervalle selon lequel BFD détecte une défaillance du chemin de transfert.
Tronçons BFD autorisés	Acceptez le paramètre par défaut. Vous pouvez définir le nombre de sessions BFD à tronçons multiples autorisées pour le profil.
Multiplis déclarations d'inactivité de BFD	Acceptez le paramètre par défaut. Vous pouvez définir le nombre de fois que le paquet BFD n'est pas reçu avant que la session ne soit marquée comme arrêtée.
Seuil de déplacement en veille	Acceptez le paramètre par défaut.

Ajouter un profil de pont NSX Edge

Le profil de pont NSX Edge définit les stratégies pour le cluster de ponts ESXi.

Un cluster de ponts est un ensemble de nœuds de transport hôtes ESXi.

Conditions préalables

- Vérifiez que le cluster NSX Edge est disponible.
- Vérifiez que le cluster de ponts ESXi est disponible.

Procédure

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

3 Entrez les détails du profil du cluster NSX Edge.

Option	Description
Nom et description	Entrez un nom de profil de cluster de ponts NSX Edge. Vous pouvez éventuellement entrer les détails du profil, tels que les informations du nœud principal et de sauvegarde.
Cluster Edge	Sélectionnez le cluster NSX Edge que vous pouvez utiliser.
Nœud principal	Désignez le nœud NSX Edge préféré dans le cluster.
Nœud de sauvegarde	Désignez le nœud NSX Edge de sauvegarde si le nœud principal est défaillant.
Mode de basculement	Sélectionnez le mode Préemptif ou Non préemptif . Le mode HA par défaut est préemptif, ce qui peut ralentir le trafic lorsque le nœud NSX Edge préféré revient en ligne. Le mode non préemptif n'entraîne pas de ralentissement du trafic.

Ajouter un profil de nœud de transport

Un profil de nœud de transport capture la configuration requise pour créer un nœud de transport. Le profil de nœud de transport peut être appliqué à un cluster vCenter Server existant pour créer des nœuds de transport pour les hôtes membres. Les profils de nœud de transport définissent les zones de transport, les hôtes membres, la configuration du commutateur N-VDS y compris le profil de liaison montante, l'attribution d'adresse IP, le mappage des cartes réseau physiques aux interfaces virtuelles de liaison montante, etc.

Note Les profils de nœud de transport ne doivent pas être appliqués à des nœuds de transport NSX Edge.

La création d'un nœud de transport commence lorsqu'un profil de nœud de transport est appliqué à un cluster vCenter Server. NSX Manager prépare les hôtes du cluster et installe les composants NSX-T Data Center sur tous les hôtes. Les nœuds de transport pour les hôtes sont créés en fonction de la configuration spécifiée dans le profil de nœud de transport.

Pour supprimer un profil de nœud de transport, vous devez d'abord détacher le profil du cluster associé. Les nœuds de transport existants ne sont pas affectés. Les nouveaux hôtes ajoutés au cluster ne sont plus automatiquement convertis en nœuds de transport.

Considérations relatives à la création d'un profil de nœud de transport :

- Vous pouvez ajouter un maximum de quatre commutateurs N-VDS pour chaque configuration : N-VDS amélioré créé pour la zone de transport VLAN, N-VDS standard créé pour la zone de transport de superposition, N-VDS amélioré créé pour la zone de transport de superposition.
- Il n'y a pas de limite pour le nombre de commutateurs N-VDS standard créés pour la zone de transport VLAN.

- Dans une topologie de cluster à hôte unique exécutant plusieurs commutateurs N-VDS standard de superposition et machines virtuelles Edge sur le même hôte, NSX-T Data Center offre une isolation du trafic de telle sorte que le trafic transitant par le premier N-VDS est isolé du trafic transitant par le deuxième N-VDS, etc. Les cartes réseau physiques sur chaque N-VDS doivent être mappées sur la machine virtuelle Edge sur l'hôte pour permettre la connectivité du trafic nord-sud avec le monde externe. Les paquets sortant d'une machine virtuelle sur la première zone de transport doivent être routés via un routeur externe ou une machine virtuelle externe vers la machine virtuelle sur la deuxième zone de transport.
- Chaque nom de commutateur N-VDS doit être unique. NSX-T Data Center n'autorise pas les doublons dans les noms de commutateurs.
- Chaque ID de zone de transport doit être unique. NSX-T Data Center n'autorise pas les doublons dans les ID.
- Vous pouvez ajouter un maximum de 1 000 zones de transport dans le profil de nœud de transport.
- Pour ajouter une zone de transport, celle-ci doit être réalisée par n'importe quel N-VDS présent dans le profil de nœud de transport.

Conditions préalables

- Vérifiez que les hôtes font partie d'un cluster vCenter Server.
- vCenter Server doit disposer d'au moins un cluster.
- Vérifiez qu'une zone de transport est configurée. Reportez-vous à la section [Créer des zones de transport](#).
- Vérifiez qu'un cluster est disponible. Reportez-vous à la section [Déployer des nœuds NSX Manager pour constituer un cluster à partir de l'interface utilisateur](#).
- Vérifiez qu'un pool d'adresses IP est configuré ou que DHCP est disponible dans le déploiement du réseau. Reportez-vous à la section [Créer un pool d'adresses IP pour les adresses IP des points de terminaison de tunnel](#).
- Vérifiez qu'un gestionnaire de calcul est configuré. Reportez-vous à la section [Ajouter un gestionnaire de calcul](#).

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Système > Infrastructure > Profils > Profils de nœud de transport > Ajouter**.
- 3 Entrez un nom pour identifier le profil de nœud de transport.

Vous pouvez éventuellement ajouter la description du profil de nœud de transport.

- 4 Sélectionnez les zones de transport disponibles et cliquez sur le bouton > pour inclure les zones de transport dans le profil de nœud de transport.

Note Vous pouvez ajouter plusieurs zones de transport.

- 5 Cliquez sur l'onglet **N-VDS** et fournissez les informations sur le commutateur.

Option	Description
Nom du N-VDS	Si le nœud de transport est connecté à une zone de transport, vérifiez que le nom entré pour le N-VDS est le même que le nom de N-VDS spécifié dans la zone de transport. Il est possible de créer un nœud de transport sans l'attacher à une zone de transport.
Zones de transport associées	Affiche les zones de transport qui sont réalisées par les commutateurs hôtes associés. Vous ne pouvez pas ajouter une zone de transport si elle n'est pas réalisée par un N-VDS dans le profil de nœud de transport.
Profil NIOC	Sélectionnez le profil NIOC dans le menu déroulant. Les allocations de bande passante spécifiées dans le profil pour les ressources de trafic sont appliquées.
Profil de liaison montante	Sélectionnez un profil de liaison montante existant dans le menu déroulant ou créez un profil de liaison montante personnalisé. Vous pouvez également utiliser le profil de liaison montante par défaut.
Profil LLDP	Par défaut, NSX-T reçoit uniquement les paquets LLDP d'un voisin LLDP. Toutefois, NSX-T peut être réglé pour envoyer des paquets LLDP à un voisin LLDP et pour en recevoir de sa part.
Attribution IP	Sélectionnez Utiliser DHCP , Utiliser le pool IP ou Utiliser la liste d'adresses IP statiques pour attribuer une adresse IP aux points de terminaison de tunnel virtuels (VTEP) du nœud de transport. 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. Tous les VTEP du nœud de transport doivent être dans le même sous-réseau, sinon la session de flux bidirectionnelle (BFD) n'est pas établie.
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.

Option	Description
Cartes réseau physiques	<p>Ajoutez des cartes réseau physiques au nœud de transport. 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 configurer des cartes réseau physiques supplémentaires sur le nœud de transport.</p> <hr/> <p>Note La migration des cartes réseau physiques que vous ajoutez dans ce champ dépend de la façon dont vous configurez Migration de carte réseau physique uniquement, Mappages de réseau pour l'installation, et Mappages de réseau pour la désinstallation.</p> <hr/> <ul style="list-style-type: none"> ■ Pour migrer une carte réseau physique utilisée (par exemple, par un vSwitch standard ou par un commutateur distribué vSphere) sans un mappage VMkernel associé, assurez-vous que Migration de carte réseau physique uniquement est activé. Sinon, le nœud de transport reste à l'état réussite partielle et l'établissement de la connectivité LCP du nœud d'infrastructure échoue. ■ Pour migrer une carte réseau physique avec un mappage de réseau VMkernel associé, désactivez Migration de carte réseau physique uniquement et configurez le mappage de réseau VMkernel. ■ Pour migrer une carte réseau physique libre, activez Migration de carte réseau physique uniquement. <hr/>

Option	Description
Migration de carte réseau physique uniquement	<p>Avant de configurer ce champ, tenez compte des points suivants :</p> <ul style="list-style-type: none"> ■ Déterminez si la carte réseau physique définie est une carte réseau utilisée ou une carte réseau libre. ■ Déterminez si les interfaces VMkernel d'un hôte doivent être migrées en même temps que les cartes réseau physiques. <p>Définissez les champs comme suit :</p> <ul style="list-style-type: none"> ■ Activez Migration de carte réseau physique uniquement si vous souhaitez uniquement migrer des cartes réseau physiques d'un commutateur VSS ou DVS vers un commutateur N-VDS. ■ Désactivez Migration de carte réseau physique uniquement si vous souhaitez migrer une carte réseau physique utilisée et son mappage d'interface VMkernel associé. Une carte réseau physique libre ou disponible est connectée au commutateur N-VDS lorsqu'un mappage de migration d'interface VMkernel est spécifié. <p>Sur un hôte avec plusieurs commutateurs hôtes :</p> <ul style="list-style-type: none"> ■ Si tous les commutateurs hôtes doivent migrer uniquement des cartes réseau physiques, vous pouvez migrer ces cartes en une seule opération. ■ Si certains commutateurs hôtes doivent migrer des interfaces VMkernel et les autres commutateurs hôtes doivent migrer uniquement des cartes réseau physiques : <ol style="list-style-type: none"> 1 Lors de la première opération, migrez uniquement les cartes réseau physiques. 2 Lors de la deuxième opération, migrez les interfaces VMkernel. Assurez-vous que Migration de carte réseau physique uniquement est désactivé. <p>La migration de carte réseau physique uniquement et la migration d'interface VMkernel ne sont pas prises en charge simultanément sur plusieurs hôtes.</p> <hr/> <p>Note Pour migrer une carte du réseau de gestion, configurez son mappage de réseau VMkernel associé et conservez Migration de carte réseau physique uniquement désactivé. Si vous migrez uniquement la carte réseau de gestion, l'hôte perd la connectivité.</p> <hr/> <p>Pour plus d'informations, consultez Migration de VMkernel vers un commutateur N-VDS.</p>

Option	Description
Mappages de réseau pour l'installation	<p>Pour migrer des VMkernel vers le commutateur N-VDS lors de l'installation, mappez les VMkernel à un commutateur logique existant. NSX Manager migre le VMkernel vers le commutateur logique mappé sur N-VDS.</p> <hr/> <p>Attention Assurez-vous que la carte réseau de gestion et l'interface VMkernel de gestion sont migrées vers un commutateur logique qui est connecté au même VLAN que celui auquel la carte réseau de gestion était connectée avant la migration. Si vmnic <n> et VMkernel<n> sont migrés vers un VLAN différent, la connectivité à l'hôte est perdue.</p> <hr/> <p>Attention Pour les cartes réseau physiques liées, assurez-vous que le mappage du commutateur hôte de la carte réseau physique à une interface VMkernel correspond à la configuration spécifiée dans le profil de nœud de transport. Dans le cadre de la procédure de validation, NSX-T Data Center vérifie le mappage et si la validation réussit, la migration d'interfaces VMkernel vers un commutateur N-VDS réussit également. Il est également obligatoire de configurer le mappage réseau pour la désinstallation, car NSX-T Data Center ne stocke pas la configuration de mappage du commutateur hôte après la migration des interfaces VMkernel vers le commutateur N-VDS. Si le mappage n'est pas configuré, la connectivité aux services, tels que vSAN, peut être perdue après la migration de restauration vers le commutateur VSS ou VDS.</p> <hr/> <p>Pour plus d'informations, consultez Migration de VMkernel vers un commutateur N-VDS.</p>
Mappages de réseau pour la désinstallation	<p>Pour restaurer la migration de VMkernel lors de la désinstallation, mappez les VMkernel aux groupes de ports sur VSS ou DVS, afin que NSX Manager sache vers quel groupe de ports VMkernel doit être remigré sur le VSS ou le DVS. Pour un commutateur DVS, assurez-vous que le groupe de ports est de type Éphémère.</p> <hr/> <p>Attention Pour les cartes réseau physiques liées, assurez-vous que le mappage du profil du nœud de transport de la carte réseau physique à l'interface VMkernel correspond à la configuration spécifiée dans le commutateur hôte. Il est obligatoire de configurer le mappage réseau pour la désinstallation, car NSX-T Data Center ne stocke pas la configuration de mappage du commutateur hôte après la migration des interfaces VMkernel vers le commutateur N-VDS. Si le mappage n'est pas configuré, la connectivité aux services, tels que vSAN, peut être perdue après la migration de restauration vers le commutateur VSS ou VDS.</p> <hr/> <p>Pour plus d'informations, consultez Migration de VMkernel vers un commutateur N-VDS.</p>

- 6 Si vous avez sélectionné plusieurs zones de transport, cliquez de nouveau sur **+ AJOUTER UN N-VDS** pour configurer le commutateur pour les autres zones de transport.
- 7 Cliquez sur **Terminer** pour terminer la configuration.

Étape suivante

Appliquez le profil de nœud de transport à un cluster vSphere existant. Reportez-vous à la section [Configurer un nœud de transport d'hôte géré](#).

Migration de VMkernel vers un commutateur N-VDS

Pour migrer les interfaces VMkernel depuis un commutateur VSS ou DVS vers un commutateur N-VDS au niveau du cluster, configurez le profil de nœud de transport avec les détails du mappage réseau requis pour la migration (mappage des interfaces VMkernel vers les commutateurs logiques). De même, pour migrer les interfaces VMkernel sur un nœud hôte, configurez la configuration du nœud de transport. Pour restaurer les interfaces VMkernel migrées vers un commutateur VSS ou DVS, configurez la désinstallation du mappage réseau (mappage des ports logiques vers l'interface VMkernel) dans le profil de nœud de transport afin qu'elle soit réalisée lors de la désinstallation.

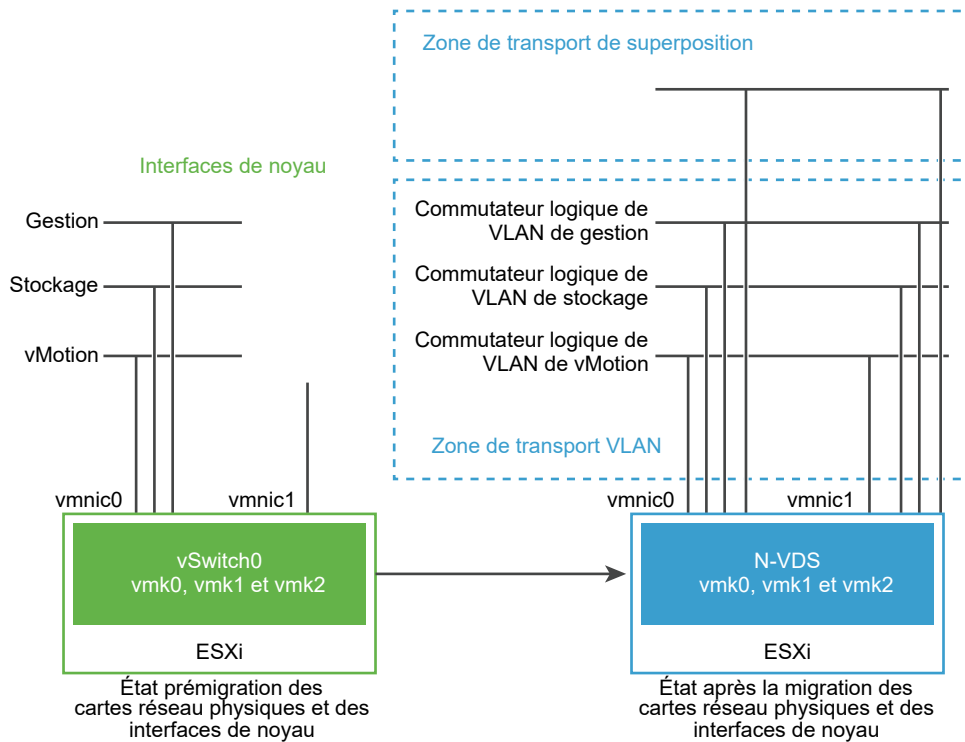
Au cours de la migration, les cartes réseau physique en cours d'utilisation sont migrées vers un commutateur N-VDS, alors que les cartes réseau physiques disponibles ou libres sont attachées au commutateur N-VDS après la migration.

Note Les profils de nœud de transport sont appliqués à tous les hôtes membres d'un cluster. Si vous souhaitez plutôt limiter la migration d'interfaces VMkernel sur des hôtes spécifiques, vous pouvez configurer l'hôte directement. Après la migration, le N-VDS gère le trafic sur le réseau VLAN et de superposition pour ces interfaces attachées au commutateur N-VDS.

Important Les configurations effectuées sur des hôtes individuels sont marquées avec l'indicateur **Remplacé**. Toute mise à jour ultérieure au profil de nœud de transport n'est pas appliquée à ces hôtes remplacés. Ces hôtes restent en état de remplacement jusqu'à la désinstallation de NSX-T Data Center.

Dans la figure suivante, si un hôte possède seulement deux cartes réseau physiques, vous voudrez peut-être attribuer ces deux cartes réseau au N-VDS pour la redondance et leurs interfaces VMkernel associées afin que les interfaces ne perdent pas la connectivité avec l'hôte.

Figure 10-2. Prémigration et post-migration des interfaces réseau vers un N-VDS



Avant la migration, l'hôte 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, tandis que vmnic1 n'est pas utilisée. En outre, il existe trois interfaces VMkernel : vmk0, vmk1 et vmk2.

Vous pouvez migrer les interfaces VMkernel en utilisant l'interface utilisateur de NSX-T Data Center Manager ou les 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.

Considérations relatives à la migration de VMkernel

- **Migration PNIC et VMkernel :** avant de migrer des cartes réseau physiques liées et les interfaces VMkernel associées à un commutateur N-VDS, notez le mappage réseau (mappage de cartes réseau physiques au groupe de ports) sur le commutateur hôte.
- **Migration PNIC uniquement :** si vous prévoyez de migrer uniquement les cartes PNIC, assurez-vous que la carte réseau physique de gestion connectée à l'interface VMkernel de gestion n'est pas migrée. Cela entraîne une perte de connectivité avec l'hôte. Pour plus de détails, voir le champ **Migration PNIC uniquement** dans la section [Ajouter un profil de nœud de transport](#).

- Restaurer la migration : avant de prévoir la restauration d'interfaces VMkernel migrées vers le commutateur hôte VSS ou DVS pour les cartes réseau physiques liées, assurez-vous d'avoir noté le mappage réseau (mappage de carte réseau physique au groupe de ports) sur le commutateur hôte. Il est obligatoire de configurer le profil de nœud de transport avec le mappage du commutateur d'hôte dans le champ **Mappage réseau pour la désinstallation**. Sans ce mappage, NSX-T Data Center ne sait pas vers quels groupes de ports les interfaces VMkernel doivent être remigrées. Cette situation peut entraîner une perte de connectivité au réseau vSAN.
- Enregistrement de vCenter Server avant la migration : si vous prévoyez de migrer un VMkernel ou une carte PNIC connectée vers un commutateur DVS, assurez-vous que vCenter Server est enregistré avec NSX Manager.
- Faire correspondre l'ID de VLAN : après la migration, l'interface de la carte réseau de gestion et de la VMkernel de gestion doit être sur le même VLAN auquel la carte réseau était connectée avant la migration. Si vmnic0 et vmk0 sont connectées au réseau de gestion et migrées vers un autre VLAN, la connectivité à l'hôte est perdue.
- Migration vers le commutateur VSS : il est impossible de remigrer deux interfaces VMkernel vers le même groupe de ports qu'un commutateur VSS.
- vMotion : effectuez une migration vMotion pour déplacer des charges de travail de VM vers un autre hôte avant la migration VMkernel et/ou PNIC. En cas d'échec de la migration, les VM de charge de travail ne sont pas affectées.
- vSAN : si le trafic vSAN est en cours d'exécution sur l'hôte, placez l'hôte en mode de maintenance via vCenter Server et déplacez les VM hors de l'hôte en utilisant la fonctionnalité vMotion avant la migration VMkernel et/ou PNIC.
- Migration : si un VMkernel est déjà connecté à un commutateur cible, il peut toujours être sélectionné pour être migré vers le même commutateur. Cette propriété rend l'opération de migration VMK et/ou PNIC idempotent. Elle vous permet de migrer uniquement des PNIC vers un commutateur cible. Comme la migration requiert toujours au moins un VMkernel et un PNIC, vous sélectionnez un VMkernel déjà migré vers un commutateur cible lorsque vous migrez uniquement des PNIC vers un commutateur cible. Si aucun VMkernel ne doit être migré, créez un VMkernel temporaire via un serveur vCenter Server dans le commutateur source ou le commutateur cible. Ensuite, migrez-le avec les PNIC et supprimez le VMkernel temporaire via vCenter Server une fois la migration terminée.
- Partage d'adresses MAC : si une interface VMkernel et un PNIC partagent la même adresse MAC et qu'ils se trouvent dans le même commutateur, ils doivent être migrés ensemble vers le même commutateur cible s'ils sont tous les deux utilisés après la migration. Conservez toujours vmk0 et vmnic0 dans le même commutateur.

Vérifiez les adresses MAC utilisées par tous les VMK et les PNIC de l'hôte en exécutant les commandes suivantes :

```
esxcfg-vmknics -l
```

```
esxcfg-nics -l
```


- Ports logiques VIF créés après la migration : après la migration de VMkernel d'un commutateur VSS ou DVS vers un commutateur N-VDS, un port de commutateur logique de type VIF est créé sur l'instance de NSX Manager. Vous ne devez pas créer de règles de pare-feu distribué sur ces ports de commutateur logique VIF.

Migrer les interfaces VMkernel vers un commutateur N-VDS

Workflow de haut niveau utilisé pour migrer les interfaces VMkernel vers un commutateur N-VDS :

- 1 Créez un commutateur logique si nécessaire.
- 2 Mettez hors tension les machines virtuelles sur l'hôte depuis lequel les interfaces VMkernel et PNIC sont migrées vers un commutateur N-VDS.
- 3 Configurez un profil de nœud de transport avec un mappage réseau utilisé pour migrer les interfaces VMkernel lors de la création de nœuds de transport. Le mappage réseau correspond au mappage d'une interface VMkernel à un commutateur logique.
Pour plus de détails, reportez-vous à la section [Ajouter un profil de nœud de transport](#).
- 4 Vérifiez que les mappages d'adaptateur réseau dans vCenter Server reflètent une nouvelle association du commutateur VMkernel avec un commutateur N-VDS. En cas de cartes réseau physiques liées, vérifiez que le mappage dans NSX-T Data Center reflète tout VMkernel lié à une carte réseau physique dans vCenter Server.
- 5 Dans NSX Manager, accédez à **Mise en réseau avancée et sécurité > Mise en réseau > Commutation**. Sur la page **Commutateurs**, vérifiez que l'interface VMkernel est associée au commutateur logique via un port logique nouvellement créé.
- 6 Accédez à **Système > Nœuds > Nœud de transport hôte**. Pour chaque nœud de transport, vérifiez que l'état dans la colonne **État du nœud** est Réussite pour confirmer que la configuration de nœud de transport est correctement validée.
- 7 Sur la page **Nœud de transport hôte**, vérifiez que l'état dans **État de configuration** est Réussite pour confirmer que l'hôte est correctement réalisé avec la configuration spécifiée.

Une fois que vous avez migré des interfaces VMkernel et des PNIC depuis un VDS vers un commutateur N-VDS à l'aide de l'interface utilisateur de NSX-T ou de l'API de nœud de transport, vCenter Server affiche des avertissements pour le VDS. Si l'hôte doit être connecté au VDS, supprimez l'hôte du VDS. Le serveur vCenter Server n'affiche plus d'avertissement pour le VDS.

Pour plus de détails sur les erreurs que vous pouvez rencontrer lors de la migration, reportez-vous à la section [Erreurs de migration de VMkernel](#)

Restaurer la migration d'interfaces VMkernel vers un commutateur VSS ou DVS

Workflow de haut niveau utilisé pour restaurer la migration d'interfaces VMkernel depuis un commutateur N-VDS vers un commutateur VSS ou DVS lors de la désinstallation de NSX-T Data Center :

- 1 Sur l'hôte ESXi, mettez hors tension les machines virtuelles connectées aux ports logiques qui hébergent l'interface VMkernel après la migration.
- 2 Configurez le profil de nœud de transport avec un mappage réseau utilisé pour migrer les interfaces VMkernel lors du processus de désinstallation. Le mappage réseau pendant la désinstallation mappe les interfaces VMkernel vers un groupe de ports sur un commutateur VSS ou DVS de l'hôte ESXi.

Note Lors de la restauration de la migration d'un VMkernel vers un groupe de ports sur un commutateur DVS, assurez-vous que le type de groupe de ports est défini sur **Éphémère**.

Pour plus de détails, reportez-vous à la section [Ajouter un profil de nœud de transport](#).

- 3 Vérifiez que les mappages d'adaptateur réseau dans vCenter Server reflètent une nouvelle association du commutateur VMkernel avec un groupe de ports du commutateur VSS ou DVS.
- 4 Dans NSX Manager, accédez à **Mise en réseau avancée et sécurité > Mise en réseau > Commutation**. Sur la page **Commutateurs**, vérifiez que les commutateurs logiques contenant les interfaces VMkernel sont supprimés.

Pour plus de détails sur les erreurs que vous pouvez rencontrer lors de la migration, reportez-vous à la section [Erreurs de migration de VMkernel](#)

Mettre à jour le mappage du commutateur d'hôte

Important

- **Hôtes avec état** : les opérations d'ajout et de mise à jour sont prises en charge. Pour mettre à jour un mappage existant, vous pouvez ajouter une nouvelle entrée d'interface VMkernel à la configuration du mappage réseau. Si vous mettez à jour la configuration du mappage réseau d'une interface VMkernel qui est déjà migrée vers le commutateur N-VDS, le mappage réseau mis à jour n'est pas réalisé sur l'hôte.
- **Hôtes sans état** : les opérations d'ajout, de mise à jour et de suppression sont prises en charge. Les modifications apportées à la configuration du mappage réseau sont réalisées après le redémarrage de l'hôte.

Pour mettre à jour les interfaces VMkernel vers un nouveau commutateur logique, vous pouvez modifier le profil de nœud de transport afin d'appliquer les mappages réseau au niveau du cluster. Si vous souhaitez que les mises à jour s'appliquent uniquement à un hôte spécifique, configurez le nœud de transport à l'aide des API au niveau de l'hôte.

Note Après avoir mis à jour la configuration du nœud de transport pour un hôte unique, toutes les mises à jour appliquées via le profil de nœud de transport ne sont pas appliquées à cet hôte. L'état de cet hôte est passé à **Remplacé**.

- 1 Pour mettre à jour tous les hôtes d'un cluster, modifiez le champ **Mappage réseau pendant l'installation** pour mettre à jour le mappage VMkernel vers des commutateurs logiques.

Pour plus de détails, reportez-vous à la section [Ajouter un profil de nœud de transport](#).

- 2 Enregistrez les modifications. Les modifications apportées à un profil de nœud de transport sont automatiquement appliquées à tous les hôtes membres du cluster, sauf sur les hôtes marqués avec l'état Remplacé.
- 3 De même, pour mettre à jour un hôte unique, vous devez modifier le mappage VMkernel dans la configuration de nœud de transport.

Note Si vous mettez à jour le champ **Mappage réseau pendant l'installation** avec un nouveau mappage VMkernel, alors la même interface VMkernel doit être ajoutée au champ **Mappage réseau pendant la désinstallation**.

Pour plus de détails sur les erreurs que vous pouvez rencontrer lors de la migration, reportez-vous à la section [Erreurs de migration de VMkernel](#)

Migrer les interfaces VMkernel sur un cluster sans état

- 1 Préparez et configurez un hôte comme hôte de référence à l'aide des API du nœud de transport.
- 2 Extrayez le profil d'hôte à partir de l'hôte de référence.
- 3 Dans vCenter Server, appliquez le profil d'hôte au cluster sans état.
- 4 Dans NSX-T Data Center, appliquez le profil de nœud de transport au cluster sans état.
- 5 Redémarrez chaque hôte du cluster.

Les hôtes du cluster peuvent prendre plusieurs minutes pour réaliser les états mis à jour.

Scénarios d'échec de la migration

- Si la migration échoue pour une raison quelconque, l'hôte tente de migrer les cartes réseau physiques et les interfaces VMkernel à trois reprises.
- Si l'échec de la migration persiste, l'hôte effectue une restauration à la configuration précédente en conservant la connectivité de VMkernel avec la carte réseau physique de gestion, vmnic0.
- Si la restauration échoue à tel point que le VMkernel configuré pour la carte réseau physique de gestion a été perdu, vous devez réinitialiser l'hôte.

Scénarios de migration non pris en charge

Les scénarios suivants ne sont pris en charge :

- Les interfaces VMkernel migrées en même temps à partir de deux commutateurs VSS ou DVS différents.
- Sur les hôtes avec état, le mappage réseau est mis à jour pour mapper l'interface VMkernel vers un autre commutateur logique. Par exemple, avant la migration, le VMkernel est mappé au commutateur logique 1 et l'interface VMkernel est mappée au commutateur logique 2.

Erreurs de migration de VMkernel

Vous pouvez rencontrer des erreurs lors de la migration d'interfaces VMkernel et de cartes réseau physiques à partir d'un commutateur VSS ou DVS vers un commutateur N-VDS ou du rétablissement d'interfaces migrantes sur un commutateur hôte VSS ou DVS.

Tableau 10-1. Erreurs de migration de VMkernel

Code d'erreur	Problème	Cause	Résolution
8224	Impossible de trouver le commutateur hôte spécifié par la configuration du nœud de transport.	ID du commutateur hôte introuvable.	<ul style="list-style-type: none"> ■ Assurez-vous que la zone de transport est créée avec le nom du commutateur hôte, puis créez le nœud de transport. ■ Assurez-vous qu'un commutateur hôte valide est utilisé dans la configuration de nœud de transport.
8225	La migration de VMkernel est en cours.	La migration est en cours.	Attendez la fin de la migration avant d'effectuer une autre action.
8226	La migration de VMkernel n'est prise en charge que sur un hôte ESXi.	La migration est uniquement valide pour les hôtes ESXi.	Assurez-vous que l'hôte est un hôte ESXi avant de lancer la migration.
8227	L'interface VMkernel n'est pas ajoutée avec le nom du commutateur hôte.	Sur un hôte disposant de plusieurs commutateurs hôtes, NSX-T Data Center ne peut pas identifier l'association de chaque interface VMkernel à son commutateur hôte.	<p>Si l'hôte dispose de plusieurs commutateurs hôtes N-VDS, assurez-vous que l'interface VMkernel est ajoutée avec le nom de commutateur hôte du N-VDS auquel l'hôte est connecté.</p> <p>Par exemple, le mappage réseau pour la désinstallation d'un hôte avec un nom de commutateur hôte N-VDS nsxvswitch1 et VMkernel1 et un autre nom de commutateur hôte N-VDS nsxvswitch2 et VMkernel2 doit être défini comme suit : <code>device_name : VMkernel1@nsxvswitch1</code>, <code>destination_network : DPortGroup</code>.</p>
8228	Commutateur hôte utilisé dans le champ <code>device_name</code> introuvable sur l'hôte.	Nom de commutateur hôte incorrect.	Entrez le nom de commutateur hôte correct.
8229	Le nœud de transport n'a pas spécifié la zone de transport du commutateur logique.	Zone de transport non ajoutée.	Ajoutez la zone de transport à la configuration du nœud de transport.

Tableau 10-1. Erreurs de migration de VMkernel (suite)

Code d'erreur	Problème	Cause	Résolution
8230	Aucune carte réseau physique sur le commutateur hôte.	Il faut au moins une carte réseau physique sur le commutateur hôte.	Spécifiez au moins une carte réseau physique dans un profil de liaison montante et la configuration de mappage du réseau VMkernel sur un commutateur logique.
8231	Le nom du commutateur hôte ne correspond pas.	Si le nom du commutateur hôte utilisé dans <code>vmk1@host_switch</code> ne correspond pas au nom de commutateur hôte utilisé par le commutateur logique de destination de l'interface.	Assurez-vous que le nom du commutateur hôte spécifié dans la configuration du mappage réseau correspond au nom utilisé par le commutateur logique de l'interface.
8232	Commutateur logique non réalisé sur l'hôte.	La réalisation du commutateur logique sur l'hôte a échoué.	Synchronisez l'hôte avec NSX Manager.
8233	Commutateur logique inattendu dans le mappage de l'interface réseau.	Le mappage d'interface réseau pour l'installation et la désinstallation répertorie des commutateurs logiques et des groupes de ports.	Le mappage réseau pour l'installation ne doit contenir que des commutateurs logiques comme cibles de destination. De même, un mappage réseau pour la désinstallation ne doit contenir que des groupes de ports comme cibles de destination.
8294	Le commutateur logique n'existe pas dans le mappage d'interface réseau.	Commutateurs logiques non spécifiés.	Assurez-vous que des commutateurs logiques sont spécifiés dans la configuration de mappage d'interface réseau.
8296	Incompatibilité de commutateur hôte.	Le mappage d'interface réseau pour la désinstallation est configuré avec un nom de commutateur hôte incorrect.	Assurez-vous que le nom du commutateur hôte utilisé dans la configuration du mappage correspond au nom entré sur le commutateur hôte hébergeant les interfaces VMkernel.
8297	VMkernel en double.	Des interfaces VMkernel en double sont spécifiées pour la migration.	Assurez-vous qu'aucune interface VMkernel en double n'est spécifiée dans la configuration du mappage d'installation ou de désinstallation.
8298	Incompatibilité du nombre d'interfaces VMkernel et de destinations.	Configuration incorrecte	Assurez-vous que chaque interface VMkernel dispose d'une destination correspondante spécifiée dans la configuration.

Tableau 10-1. Erreurs de migration de VMkernel (suite)

Code d'erreur	Problème	Cause	Résolution
8299	Impossible de supprimer le nœud de transport, car l'interface VMkernel utilise des ports sur N-VDS.	Les interfaces VMkernel utilisent des ports du commutateur N-VDS.	Restaurez la migration de toutes les interfaces VMkernel du commutateur N-VDS vers un commutateur VSS/DVS. Essayez ensuite de supprimer le nœud de transport.
9412	VMkernel ne peut pas être migré d'un N-VDS vers un autre N-VDS.	Action non prise en charge.	Restaurez la migration de l'interface VMkernel vers un commutateur VSS ou DVS. Ensuite, vous pouvez migrer l'interface VMkernel vers un autre commutateur N-VDS.
9413	Les interfaces VMkernel ne peuvent pas être migrées vers un autre commutateur logique.	Sur les hôtes avec état, un VMkernel connecté à un commutateur logique ne peut pas être migré vers un autre commutateur logique.	Restaurez la migration du VMkernel du commutateur logique vers un commutateur VSS/DVS. Ensuite, migrez le VMkernel vers un autre commutateur logique sur le N-VDS.
9414	Dupliquez les interfaces VMkernel.	Dupliquez les interfaces VMkernel mappées dans la configuration de mappage de l'installation et de la désinstallation.	Assurez-vous que chaque interface VMkernel est unique dans les mappages d'installation et de désinstallation.
9415	Machine virtuelle sous tension sur l'hôte.	Avec des machines virtuelles sous tension, la migration ne s'exécute pas.	Mettez hors tension les machines virtuelles sur l'hôte avant de lancer la migration d'interfaces VMkernel.
9416	VMkernel introuvable sur l'hôte.	Vous n'avez pas spécifié un VMkernel qui existe sur l'hôte dans la configuration du mappage réseau.	Spécifiez un VMkernel qui existe dans la configuration du mappage réseau.
9417	Groupe de ports introuvable.	Vous n'avez pas spécifié un groupe de ports qui existe sur l'hôte dans la configuration du mappage réseau.	Spécifiez un groupe de ports qui existe dans la configuration du mappage réseau.
9419	Commutateur logique introuvable pendant la migration.	Impossible de trouver le commutateur logique défini dans la configuration du mappage de l'interface réseau.	Spécifiez un commutateur logique qui existe dans la configuration du mappage de l'interface réseau.
9420	Port logique introuvable pendant la migration.	Pendant la migration, NSX-T Data Center ne trouve pas les ports créés sur le commutateur logique.	Assurez-vous qu'aucun port logique n'est supprimé du commutateur logique afin de garantir la réussite de la migration.

Tableau 10-1. Erreurs de migration de VMkernel (suite)

Code d'erreur	Problème	Cause	Résolution
9421	Informations sur l'hôte manquantes pour valider le processus de migration.	Impossible de récupérer les informations sur l'hôte à partir de l'inventaire.	Réessayez le processus de migration.
9423	Les cartes réseau physiques liées à une interface VMkernel ne sont pas migrées vers le commutateur d'hôte approprié.	Une carte réseau physique liée a été trouvée dans l'environnement, mais le VMkernel et la carte réseau physique ne sont pas migrés vers le même commutateur hôte.	Une carte réseau physique liée à l'interface VMkernel doit avoir une configuration de nœud de transport qui mappe la carte réseau physique avec le noyau VMkernel sur le même commutateur hôte.
600	Objet introuvable.	La zone de transport spécifiée utilisée par le commutateur logique n'existe pas. Le commutateur logique dans la destination de mappage VMK est introuvable.	<ul style="list-style-type: none"> ■ Spécifiez une zone de transport qui existe dans l'environnement. ■ Créez le commutateur logique souhaité ou utilisez un commutateur logique VLAN existant.
8310	Le type de commutateur logique est incorrect.	Le type de commutateur logique est superposition.	Créez un commutateur logique VLAN.
9424	Migration impossible si les options Migration exclusivement PNIC et Mappage réseau des paramètres d'installation ou de désinstallation sont configurées à la même heure.	La migration progresse uniquement lorsqu'un de ces paramètres est configuré.	Assurez-vous que le paramètre Migration exclusivement PNIC ou Mappage réseau pour installation ou désinstallation est configuré.

Créer un nœud de transport d'hôte autonome ou de serveur bare metal

Vous devez d'abord ajouter votre hôte ESXi, l'hôte KVM ou le serveur bare metal à l'infrastructure NSX-T Data Center puis configurer le nœud de transport.

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 ou un serveur bare metal doit d'abord être ajouté à l'infrastructure NSX-T Data Center.

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 ou un serveur bare metal, 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.

Vous pouvez ajouter un maximum de quatre commutateurs N-VDS pour chaque configuration : N-VDS standard créé pour la zone de transport VLAN, N-VDS amélioré créé pour la zone de transport VLAN, N-VDS standard créé pour la zone de transport de superposition, N-VDS amélioré créé pour la zone de transport de superposition.

Dans une topologie de cluster à hôte unique exécutant plusieurs commutateurs N-VDS standard de superposition et machines virtuelles Edge sur le même hôte, NSX-T Data Center offre une isolation du trafic de telle sorte que le trafic transitant par le premier N-VDS est isolé du trafic transitant par le deuxième N-VDS, etc. Les cartes réseau physiques sur chaque N-VDS doivent être mappées sur la machine virtuelle Edge sur l'hôte pour permettre la connectivité du trafic nord-sud avec le monde externe. Les paquets sortant d'une machine virtuelle sur la première zone de transport doivent être routés via un routeur externe ou une machine virtuelle externe vers la machine virtuelle sur la deuxième zone de transport.

Conditions préalables

- L'hôte doit être associé au plan de gestion et la connectivité doit être active.
- 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.

- 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
- Vérifiez que les modules tiers requis sont installés. Reportez-vous à la section [Installer des modules tiers sur un hôte KVM](#).

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 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:A
2:4E: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 Sélectionnez **Système > Infrastructure > Nœuds > Nœuds de transport hôtes**.
- 3 Dans le champ Géré par, sélectionnez **Hôtes autonomes** et cliquez sur **+ Ajouter**.
- 4 Entrez les détails de l'hôte autonome ou du serveur bare metal à ajouter à l'infrastructure.

Option	Description
Nom et description	Entrez le nom pour identifier l'hôte autonome ou le serveur bare metal. Vous pouvez éventuellement ajouter la description du système d'exploitation utilisé pour l'hôte ou le serveur bare metal.
Adresses IP	Entrez l'adresse IP de l'hôte ou du serveur bare metal.

Option	Description
Système d'exploitation	<p>Sélectionnez le système d'exploitation dans le menu déroulant.</p> <p>Selon votre hôte ou serveur bare metal, vous pouvez sélectionner n'importe lequel des systèmes d'exploitation pris en charge. Reportez-vous à la section Configuration système requise.</p> <hr/> <p>Important Parmi les différentes versions de Linux prises en charge, vous devez connaître la différence entre un serveur bare metal exécutant une distribution Linux et l'utilisation d'une distribution Linux comme hôte d'hyperviseur. Par exemple, la sélection d'Ubuntu Server comme système d'exploitation entraîne la configuration d'un serveur bare metal exécutant un serveur Linux, tandis que la sélection d'Ubuntu KVM signifie que l'hyperviseur Linux déployé est Ubuntu.</p>
Nom d'utilisateur et mot de passe	Entrez le nom d'utilisateur et le mot de passe de l'hôte.
Empreinte numérique SHA-256	<p>Entrez la valeur d'empreinte de l'hôte pour l'authentification.</p> <p>Si vous laissez la valeur d'empreinte vide, vous êtes invité à accepter la valeur fournie par le serveur. Il faut quelques secondes à NSX-T Data Center pour détecter et authentifier l'hôte.</p>

- 5 (Requis) Pour un hôte KVM ou un serveur bare metal, sélectionnez le type de N-VDS.

Option	Description
NSX créé	<p>NSX Manager crée le N-VDS.</p> <p>Cette option est sélectionnée par défaut.</p>
Préconfiguré	Le N-VDS est déjà configuré.

Pour un hôte ESXi, le type de N-VDS est toujours défini sur **Créé par NSX**.

- 6 Entrez les détails N-VDS standards. Plusieurs commutateurs N-VDS peuvent être configurés sur un seul hôte.

Option	Description
Zone de transport	Dans le menu déroulant, sélectionnez la zone de transport à laquelle appartient ce nœud de transport.
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	Pour un hôte ESXi, sélectionnez le profil NIOC 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>Vous pouvez également utiliser le profil de liaison montante par défaut.</p>
Profil LLDP	<p>Par défaut, NSX-T reçoit uniquement les paquets LLDP d'un voisin LLDP.</p> <p>Toutefois, NSX-T peut être réglé pour envoyer des paquets LLDP à un voisin LLDP et pour en recevoir de sa part.</p>

Option	Description
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	<p>Si vous avez sélectionné l'option Utiliser le pool IP pour l'attribution d'adresse IP, spécifiez le nom du pool d'adresses IP.</p>
Cartes réseau physiques	<p>Ajoutez des cartes réseau physiques au nœud de transport. 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 configurer des cartes réseau physiques supplémentaires sur le nœud de transport.</p> <p>Note La migration des cartes réseau physiques que vous ajoutez dans ce champ dépend de la façon dont vous configurez Migration de carte réseau physique uniquement, Mappages de réseau pour l'installation, et Mappages de réseau pour la désinstallation.</p> <ul style="list-style-type: none"> ■ Pour migrer une carte réseau physique utilisée (par exemple, par un vSwitch standard ou par un commutateur distribué vSphere) sans un mappage VMkernel associé, assurez-vous que Migration de carte réseau physique uniquement est activé. Sinon, le nœud de transport reste à l'état réussite partielle et l'établissement de la connectivité LCP du nœud d'infrastructure échoue. ■ Pour migrer une carte réseau physique avec un mappage de réseau VMkernel associé, désactivez Migration de carte réseau physique uniquement et configurez le mappage de réseau VMkernel. ■ Pour migrer une carte réseau physique libre, activez Migration de carte réseau physique uniquement.

Option	Description
Migration de carte réseau physique uniquement	<p>Avant de configurer ce champ, tenez compte des points suivants :</p> <ul style="list-style-type: none"> ■ Déterminez si la carte réseau physique définie est une carte réseau utilisée ou une carte réseau libre. ■ Déterminez si les interfaces VMkernel d'un hôte doivent être migrées en même temps que les cartes réseau physiques. <p>Définissez les champs comme suit :</p> <ul style="list-style-type: none"> ■ Activez Migration de carte réseau physique uniquement si vous souhaitez uniquement migrer des cartes réseau physiques d'un commutateur VSS ou DVS vers un commutateur N-VDS. ■ Désactivez Migration de carte réseau physique uniquement si vous souhaitez migrer une carte réseau physique utilisée et son mappage d'interface VMkernel associé. Une carte réseau physique libre ou disponible est connectée au commutateur N-VDS lorsqu'un mappage de migration d'interface VMkernel est spécifié. <p>Sur un hôte avec plusieurs commutateurs hôtes :</p> <ul style="list-style-type: none"> ■ Si tous les commutateurs hôtes doivent migrer uniquement des cartes réseau physiques, vous pouvez migrer ces cartes en une seule opération. ■ Si certains commutateurs hôtes doivent migrer des interfaces VMkernel et les autres commutateurs hôtes doivent migrer uniquement des cartes réseau physiques : <ol style="list-style-type: none"> 1 Lors de la première opération, migrez uniquement les cartes réseau physiques. 2 Lors de la deuxième opération, migrez les interfaces VMkernel. Assurez-vous que Migration de carte réseau physique uniquement est désactivé. <p>La migration de carte réseau physique uniquement et la migration d'interface VMkernel ne sont pas prises en charge simultanément sur plusieurs hôtes.</p> <hr/> <p>Note Pour migrer une carte du réseau de gestion, configurez son mappage de réseau VMkernel associé et conservez Migration de carte réseau physique uniquement désactivé. Si vous migrez uniquement la carte réseau de gestion, l'hôte perd la connectivité.</p> <hr/> <p>Pour plus d'informations, consultez Migration de VMkernel vers un commutateur N-VDS.</p>

Option	Description
Mappages de réseau pour l'installation	<p>Pour migrer des VMkernel vers le commutateur N-VDS lors de l'installation, mappez les VMkernel à un commutateur logique existant. NSX Manager migre le VMkernel vers le commutateur logique mappé sur N-VDS.</p> <hr/> <p>Attention Assurez-vous que la carte réseau de gestion et l'interface VMkernel de gestion sont migrées vers un commutateur logique qui est connecté au même VLAN que celui auquel la carte réseau de gestion était connectée avant la migration. Si vmnic <n> et VMkernel<n> sont migrés vers un VLAN différent, la connectivité à l'hôte est perdue.</p> <hr/> <p>Attention Pour les cartes réseau physiques liées, assurez-vous que le mappage du commutateur hôte de la carte réseau physique à une interface VMkernel correspond à la configuration spécifiée dans le profil de nœud de transport. Dans le cadre de la procédure de validation, NSX-T Data Center vérifie le mappage et si la validation réussit, la migration d'interfaces VMkernel vers un commutateur N-VDS réussit également. Parallèlement, il est obligatoire de configurer le mappage réseau pour la désinstallation, car NSX-T Data Center ne stocke pas la configuration de mappage du commutateur hôte après la migration des interfaces VMkernel vers le commutateur N-VDS. Si le mappage n'est pas configuré, la connectivité aux services, tels que vSAN, peut être perdue après la migration de restauration vers le commutateur VSS ou VDS.</p> <hr/> <p>Pour plus d'informations, consultez Migration de VMkernel vers un commutateur N-VDS.</p>
Mappages de réseau pour la désinstallation	<p>Pour restaurer la migration de VMkernel lors de la désinstallation, mappez les VMkernel aux groupes de ports sur VSS ou DVS, afin que NSX Manager sache vers quel groupe de ports VMkernel doit être remigré sur le VSS ou le DVS. Pour un commutateur DVS, assurez-vous que le groupe de ports est de type Éphémère.</p> <hr/> <p>Attention Pour les cartes réseau physiques liées, assurez-vous que le mappage du profil du nœud de transport de la carte réseau physique à l'interface VMkernel correspond à la configuration spécifiée dans le commutateur hôte. Il est obligatoire de configurer le mappage réseau pour la désinstallation, car NSX-T Data Center ne stocke pas la configuration de mappage du commutateur hôte après la migration des interfaces VMkernel vers le commutateur N-VDS. Si le mappage n'est pas configuré, la connectivité aux services, tels que vSAN, peut être perdue après la migration de restauration vers le commutateur VSS ou VDS.</p> <hr/> <p>Pour plus d'informations, consultez Migration de VMkernel vers un commutateur N-VDS.</p>

- 7 Entrez les détails N-VDS du chemin de données amélioré. Plusieurs commutateurs N-VDS peuvent être configurés sur un seul hôte.

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	<p>Ajoutez des cartes réseau physiques au nœud de transport. 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 configurer des cartes réseau physiques supplémentaires sur le nœud de transport.</p> <p>Note La migration des cartes réseau physiques que vous ajoutez dans ce champ dépend de la façon dont vous configurez Migration de carte réseau physique uniquement, Mappages de réseau pour l'installation, et Mappages de réseau pour la désinstallation.</p> <ul style="list-style-type: none"> ■ Pour migrer une carte réseau physique utilisée (par exemple, par un vSwitch standard ou par un commutateur distribué vSphere) sans un mappage VMkernel associé, assurez-vous que Migration de carte réseau physique uniquement est activé. Sinon, le nœud de transport reste à l'état réussite partielle et l'établissement de la connectivité LCP du nœud d'infrastructure échoue. ■ Pour migrer une carte réseau physique avec un mappage de réseau VMkernel associé, désactivez Migration de carte réseau physique uniquement et configurez le mappage de réseau VMkernel. ■ Pour migrer une carte réseau physique libre, activez Migration de carte réseau physique uniquement.
Liaison montante	Sélectionnez le profil de liaison montante dans le menu déroulant.

Option	Description
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>

8 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.

9 Observez l'état de connexion sur la page **Nœuds de transport hôtes**.

Après l'ajout de l'hôte ou du serveur bare metal comme nœud de transport, la connexion à NSX Manager passe à l'état actif en 3 à 4 minutes.

Note Si la préparation de l'hôte échoue en raison d'une incompatibilité de hachage de configuration qui entraîne une boucle de détection, essayez l'une des options suivantes :

- Rendez le nom de domaine complet « false » et redémarrez nsx-proxy dans l'hôte. Cela forcera l'hôte et NSX Manager à ne pas utiliser le nom de domaine complet.
- OU

Si vous souhaitez utiliser le mode de nom de domaine complet, assurez-vous de déployer le dispositif NSX Manager à l'aide du nom de domaine complet du nom d'hôte et assurez-vous que l'orthographe sensible à la casse correspond à la recherche DNS directe et inversée pour l'adresse IP de NSX Manager. Ce paramètre doit être cohérent dans tous les nœuds NSX Manager.

10 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 -
```

11 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.

Les modules sur des différents hôtes sont regroupés comme suit :

- KVM sur RHEL ou CentOS - RPM.
- KVM sur Ubuntu - DEB
- Sur ESXi, entrez la commande `esxcli software vib list | grep nsx`.

La date est le jour où vous avez effectué l'installation.

- Sur RHEL ou CentOS, entrez la commande `yum list installed` ou `rpm -qa`.
- Sur Ubuntu, entrez la commande `dpkg --get-selections`.

12 (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.

- 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.
- Exécutez le script, qui se trouve dans le magasin de fichiers NSX-T Data Center.

```
python aggsvc_change_intervals.py -m '<NSX ManagerIPAddress>' -u 'admin' -p '<password>' -i 900
```

- (Facultatif) Rétablissez les valeurs par défaut des intervalles d'interrogation.

```
python aggsvc_change_intervals.py -m '<NSX ManagerIPAddress>' -u 'admin' -p '<password>' -r
```


Résultats

Note Pour un N-VDS créé par NSX-T Data Center, une fois le nœud de transport créé, si vous souhaitez modifier la configuration, telle que l'attribution IP au 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 N-VDS. Reportez-vous à la section [Migration de VMkernel vers un commutateur N-VDS](#).

Configurer un nœud de transport d'hôte géré

Si vous disposez d'un serveur vCenter Server, vous pouvez automatiser l'installation et la création des nœuds de transport sur tous les hôtes NSX-T Data Center au lieu de les configurer manuellement.

Si le nœud de transport est déjà configuré, la création de nœuds de transport automatisée n'est pas applicable pour ce nœud.

Conditions préalables

- Vérifiez que tous les hôtes du serveur vCenter Server sont sous tension.
- Vérifiez que la configuration requise est respectée. Reportez-vous à la section [Configuration système requise](#).
- Vérifiez qu'une zone de transport est disponible. Reportez-vous à la section [Créer des zones de transport](#).
- Vérifiez qu'un profil de nœud de transport est configuré. Reportez-vous à la section [Ajouter un profil de nœud de transport](#).
- L'installation de NSX-T Data Center sur vSphere échoue si votre liste d'exceptions pour le mode de verrouillage vSphere inclut des comptes d'utilisateurs ayant expiré. Assurez-vous de supprimer tous les comptes d'utilisateurs ayant expiré avant de commencer l'installation. Pour plus d'informations sur les comptes disposant de privilèges d'accès en mode de verrouillage, reportez-vous à la section *Spécification de comptes disposant de privilèges d'accès en mode de verrouillage* du *Guide de sécurité de vSphere*.

Procédure

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

- 3 Dans le menu déroulant **Géré par**, sélectionnez un serveur vCenter Server existant.

La page répertorie les clusters vSphere et/ou les hôtes ESXi disponibles à partir du serveur vCenter Server sélectionné. Vous devrez peut-être développer un cluster pour afficher les hôtes ESXi.

- 4 Sélectionnez un hôte unique dans la liste et cliquez sur **Configurer NSX**.

La boîte de dialogue Configurer NSX s'ouvre.

- Vérifiez le nom d'hôte dans le volet Détails de l'hôte. Vous pouvez éventuellement ajouter une description.
- Cliquez sur **Suivant** pour passer au volet **Configurer NSX**.
- Sélectionnez les zones de transport disponibles et cliquez sur le bouton > pour inclure les zones de transport dans le profil de nœud de transport.

- 5 Vérifiez le nom d'hôte dans le volet Détails de l'hôte et cliquez sur **Suivant**.

Vous pouvez éventuellement ajouter une description.

- 6 Dans le volet **Configurer NSX**, sélectionnez les zones de transport souhaitées.

Vous pouvez sélectionner plusieurs zones de transport.

- 7 Cliquez sur l'onglet **N-VDS** et fournissez les informations sur le commutateur.

Option	Description
Nom du N-VDS	Si le nœud de transport est connecté à une zone de transport, vérifiez que le nom entré pour le N-VDS est le même que le nom de N-VDS spécifié dans la zone de transport. Il est possible de créer un nœud de transport sans l'attacher à une zone de transport.
Zones de transport associées	Affiche les zones de transport qui sont réalisées par les commutateurs hôtes associés. Vous ne pouvez pas ajouter une zone de transport si elle n'est pas réalisée par un N-VDS dans le profil de nœud de transport.
Profil NIOC	Sélectionnez le profil NIOC dans le menu déroulant. Les allocations de bande passante spécifiées dans le profil pour les ressources de trafic sont appliquées.
Profil de liaison montante	Sélectionnez un profil de liaison montante existant dans le menu déroulant ou créez un profil de liaison montante personnalisé. Vous pouvez également utiliser le profil de liaison montante par défaut.
Profil LLDP	Par défaut, NSX-T reçoit uniquement les paquets LLDP d'un voisin LLDP. Toutefois, NSX-T peut être réglé pour envoyer des paquets LLDP à un voisin LLDP et pour en recevoir de sa part.
Attribution IP	Sélectionnez Utiliser DHCP , Utiliser le pool IP ou Utiliser la liste d'adresses IP statiques pour attribuer une adresse IP aux points de terminaison de tunnel virtuels (VTEP) du nœud de transport. 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. Tous les VTEP du nœud de transport doivent être dans le même sous-réseau, sinon la session de flux bidirectionnelle (BFD) n'est pas établie.

Option	Description
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	<p>Ajoutez des cartes réseau physiques au nœud de transport. 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 configurer des cartes réseau physiques supplémentaires sur le nœud de transport.</p> <p>Note La migration des cartes réseau physiques que vous ajoutez dans ce champ dépend de la façon dont vous configurez Migration de carte réseau physique uniquement, Mappages de réseau pour l'installation, et Mappages de réseau pour la désinstallation.</p> <ul style="list-style-type: none"> ■ Pour migrer une carte réseau physique utilisée (par exemple, par un vSwitch standard ou par un commutateur distribué vSphere) sans un mappage VMkernel associé, assurez-vous que Migration de carte réseau physique uniquement est activé. Sinon, le nœud de transport reste à l'état réussite partielle et l'établissement de la connectivité LCP du nœud d'infrastructure échoue. ■ Pour migrer une carte réseau physique avec un mappage de réseau VMkernel associé, désactivez Migration de carte réseau physique uniquement et configurez le mappage de réseau VMkernel. ■ Pour migrer une carte réseau physique libre, activez Migration de carte réseau physique uniquement.

Option	Description
Migration de carte réseau physique uniquement	<p>Avant de configurer ce champ, tenez compte des points suivants :</p> <ul style="list-style-type: none"> ■ Déterminez si la carte réseau physique définie est une carte réseau utilisée ou une carte réseau libre. ■ Déterminez si les interfaces VMkernel d'un hôte doivent être migrées en même temps que les cartes réseau physiques. <p>Définissez les champs comme suit :</p> <ul style="list-style-type: none"> ■ Activez Migration de carte réseau physique uniquement si vous souhaitez uniquement migrer des cartes réseau physiques d'un commutateur VSS ou DVS vers un commutateur N-VDS. ■ Désactivez Migration de carte réseau physique uniquement si vous souhaitez migrer une carte réseau physique utilisée et son mappage d'interface VMkernel associé. Une carte réseau physique libre ou disponible est connectée au commutateur N-VDS lorsqu'un mappage de migration d'interface VMkernel est spécifié. <p>Sur un hôte avec plusieurs commutateurs hôtes :</p> <ul style="list-style-type: none"> ■ Si tous les commutateurs hôtes doivent migrer uniquement des cartes réseau physiques, vous pouvez migrer ces cartes en une seule opération. ■ Si certains commutateurs hôtes doivent migrer des interfaces VMkernel et les autres commutateurs hôtes doivent migrer uniquement des cartes réseau physiques : <ol style="list-style-type: none"> 1 Lors de la première opération, migrez uniquement les cartes réseau physiques. 2 Lors de la deuxième opération, migrez les interfaces VMkernel. Assurez-vous que Migration de carte réseau physique uniquement est désactivé. <p>La migration de carte réseau physique uniquement et la migration d'interface VMkernel ne sont pas prises en charge simultanément sur plusieurs hôtes.</p> <hr/> <p>Note Pour migrer une carte du réseau de gestion, configurez son mappage de réseau VMkernel associé et conservez Migration de carte réseau physique uniquement désactivé. Si vous migrez uniquement la carte réseau de gestion, l'hôte perd la connectivité.</p> <hr/> <p>Pour plus d'informations, consultez Migration de VMkernel vers un commutateur N-VDS.</p>

Option	Description
Mappages de réseau pour l'installation	<p>Pour migrer des VMkernel vers le commutateur N-VDS lors de l'installation, mappez les VMkernel à un commutateur logique existant. NSX Manager migre le VMkernel vers le commutateur logique mappé sur N-VDS.</p> <p>Attention Assurez-vous que la carte réseau de gestion et l'interface VMkernel de gestion sont migrées vers un commutateur logique qui est connecté au même VLAN que celui auquel la carte réseau de gestion était connectée avant la migration. Si vmnic <n> et VMkernel<n> sont migrés vers un VLAN différent, la connectivité à l'hôte est perdue.</p> <p>Attention Pour les cartes réseau physiques liées, assurez-vous que le mappage du commutateur hôte de la carte réseau physique à une interface VMkernel correspond à la configuration spécifiée dans le profil de nœud de transport. Dans le cadre de la procédure de validation, NSX-T Data Center vérifie le mappage et si la validation réussit, la migration d'interfaces VMkernel vers un commutateur N-VDS réussit également. Il est également obligatoire de configurer le mappage réseau pour la désinstallation, car NSX-T Data Center ne stocke pas la configuration de mappage du commutateur hôte après la migration des interfaces VMkernel vers le commutateur N-VDS. Si le mappage n'est pas configuré, la connectivité aux services, tels que vSAN, peut être perdue après la migration de restauration vers le commutateur VSS ou VDS.</p> <p>Pour plus d'informations, consultez Migration de VMkernel vers un commutateur N-VDS.</p>
Mappages de réseau pour la désinstallation	<p>Pour restaurer la migration de VMkernel lors de la désinstallation, mappez les VMkernel aux groupes de ports sur VSS ou DVS, afin que NSX Manager sache vers quel groupe de ports VMkernel doit être remigré sur le VSS ou le DVS. Pour un commutateur DVS, assurez-vous que le groupe de ports est de type Éphémère.</p> <p>Attention Pour les cartes réseau physiques liées, assurez-vous que le mappage du profil du nœud de transport de la carte réseau physique à l'interface VMkernel correspond à la configuration spécifiée dans le commutateur hôte. Il est obligatoire de configurer le mappage réseau pour la désinstallation, car NSX-T Data Center ne stocke pas la configuration de mappage du commutateur hôte après la migration des interfaces VMkernel vers le commutateur N-VDS. Si le mappage n'est pas configuré, la connectivité aux services, tels que vSAN, peut être perdue après la migration de restauration vers le commutateur VSS ou VDS.</p> <p>Pour plus d'informations, consultez Migration de VMkernel vers un commutateur N-VDS.</p>

- 8 Si vous avez sélectionné plusieurs zones de transport, cliquez de nouveau sur **+ AJOUTER UN N-VDS** pour configurer le commutateur pour les autres zones de transport.
- 9 Cliquez sur **Terminer** pour terminer la configuration.
- 10 (Facultatif) Affichez l'état de connexion ESXi.

```
# esxcli network ip connection list | grep 1235
tcp 0 0 192.168.210.53:20514 192.168.110.34:1234 ESTABLISHED 1000144459 newreno netcpa
```

- 11 À partir de la page Nœud de transport hôte, vérifiez que l'état de connectivité NSX Manager des hôtes du cluster est Actif et que l'état de configuration de NSX-T Data Center est Réussite.

Vous pouvez également voir que la zone de transport est appliquée aux hôtes du cluster.

- 12 (Facultatif) Supprimez un nœud d'installation et de transport de NSX-T Data Center d'un hôte de la zone de transport.

- a Sélectionnez un ou plusieurs hôtes et cliquez sur **Actions > Supprimer NSX**.

La désinstallation prend jusqu'à 3 minutes. La désinstallation de NSX-T Data Center supprime la configuration du nœud de transport sur les hôtes et ceux-ci sont détachés de la ou des zones de transport et du commutateur N-VDS. Tout nouvel hôte ajouté au cluster vCenter Server ne sera pas automatiquement configuré tant que le profil de nœud de transport n'est pas réappliqué au cluster.

- 13 (Facultatif) Supprimez un nœud de transport de la zone de transport.

- a Sélectionnez un seul nœud de transport et cliquez sur **Actions > Supprimer de la zone de transport**.

Étape suivante

Créez un commutateur logique et attribuez des ports logiques. Reportez-vous à la section Commutation avancée dans le *Guide d'administration de NSX-T Data Center*.

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 d'hôte autonome ou de serveur bare metal](#).

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Système > Infrastructure > Profils > Profils de liaison montante > 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 **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 Entrez une valeur pour **Transport VLAN** et **MTU**.
- 8 Cliquez sur **Ajouter** en bas de la boîte de dialogue.
- 9 Sous **Associations**, cliquez sur **Ajouter** pour ajouter une entrée pour l'agrégation de liens.
- 10 Sélectionnez **Infrastructure > Nœuds > Nœuds de transport hôtes > Ajouter**.
- 11 Dans l'onglet **Détails de l'hôte**, entrez l'adresse IP, le nom du système d'exploitation, les informations d'identification de l'administrateur et l'empreinte numérique SHA-256 de l'hôte.
- 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**, la liste déroulante des cartes réseau physiques et des liaisons montantes reflète les nouvelles cartes réseau et le nouveau profil de liaison montante. 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 sont indiquées. Sélectionnez une carte réseau physique pour **lag1-0** et une carte réseau physique pour **lag1-1**.
- 14 Renseignez les autres champs.

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 N-VDS.
- 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 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 l'API pour des informations d'état du nœud de transport.

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"
}
```

Migrer les adaptateurs physiques et VMkernel ESXi

Après la préparation d'un hôte en tant que nœud de transport, vous pouvez apporter des modifications à la configuration de migration actuelle des adaptateurs VMkernel et des adaptateurs physiques.

Conditions préalables

- Assurez-vous que l'hôte dispose d'au moins un adaptateur physique libre.
- Assurez-vous que des adaptateurs VMkernel et des groupes de ports existent sur l'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 Accédez à **Système > Infrastructure > Nœuds de transport hôtes**.
- 3 Sélectionnez un nœud de transport et cliquez sur **Actions > Migrer les adaptateurs physiques et VMkernel ESX**.
- 4 Dans la section Migrer les adaptateurs physiques et VMkernel ESX, entrez les détails suivants.

Champ	Description
Direction	Faites une sélection : <ul style="list-style-type: none"> ■ Migrer vers des commutateurs logiques : pour migrer des adaptateurs VMkernel depuis un commutateur VSS ou VDS vers un commutateur N-VDS dans NSX-T Data Center. ■ Migrer vers des groupes de ports : pour migrer les adaptateurs VMkernel depuis un commutateur N-VDS vers un commutateur VSS ou VDS.
Sélectionner un commutateur	Sélectionnez le commutateur à partir duquel vous souhaitez migrer les adaptateurs VMkernel et les adaptateurs physiques. Vous pouvez choisir parmi les commutateurs disponibles.
Sélectionner les adaptateurs VMkernel à migrer	Cliquez sur Ajouter pour entrer le nom de l'adaptateur VMkernel et sélectionnez destination comme commutateur logique ou groupe de ports en fonction de l'emplacement vers lequel vous voulez effectuer la migration.
Modifier les adaptateurs physiques dans N-VDS	Cliquez sur Ajouter pour entrer le nom de l'adaptateur physique et le mapper à une liaison montante sur le commutateur d'hôte.

- 5 Cliquez sur **Enregistrer** pour commencer la migration des adaptateurs VMkernel et des adaptateurs physiques.

Résultats

Les adaptateurs VMkernel et les adaptateurs physiques mis à jour sont migrés vers le commutateur N-VDS ou sont migrés vers le commutateur VSS ou VDS dans l'hôte ESXi.

Mode de maintenance NSX

Si vous souhaitez éviter la migration par vMotion de machines virtuelles vers un nœud de transport qui n'est pas fonctionnel, placez ce nœud de transport en mode de maintenance NSX.

Pour mettre un nœud de transport en mode de maintenance NSX, sélectionnez le nœud et cliquez sur Actions → Mode de maintenance NSX.

Lorsque vous mettez un hôte en mode de maintenance NSX, le nœud de transport ne peut pas participer à la mise en réseau. En outre, les machines virtuelles exécutées sur d'autres nœuds de transport disposant de N-VDS ou de vSphere Distributed Switch en tant que commutateur d'hôte ne peuvent pas être migrées par vMotion vers ce nœud de transport. De plus, le réseau logique ne peut pas être configuré sur des hôtes ESXi ou KVM.

Scénarios de placement du nœud de transport en mode de maintenance NSX :

- Un nœud de transport n'est pas fonctionnel.
- Si un hôte présente des problèmes matériels ou logiciels qui ne sont pas liés à NSX-T, mais que vous souhaitez conserver le nœud et ses configurations dans NSX-T, placez l'hôte en mode de maintenance NSX.
- Un nœud de transport est automatiquement mis en mode de maintenance NSX lorsqu'une mise à niveau sur ce nœud de transport échoue.

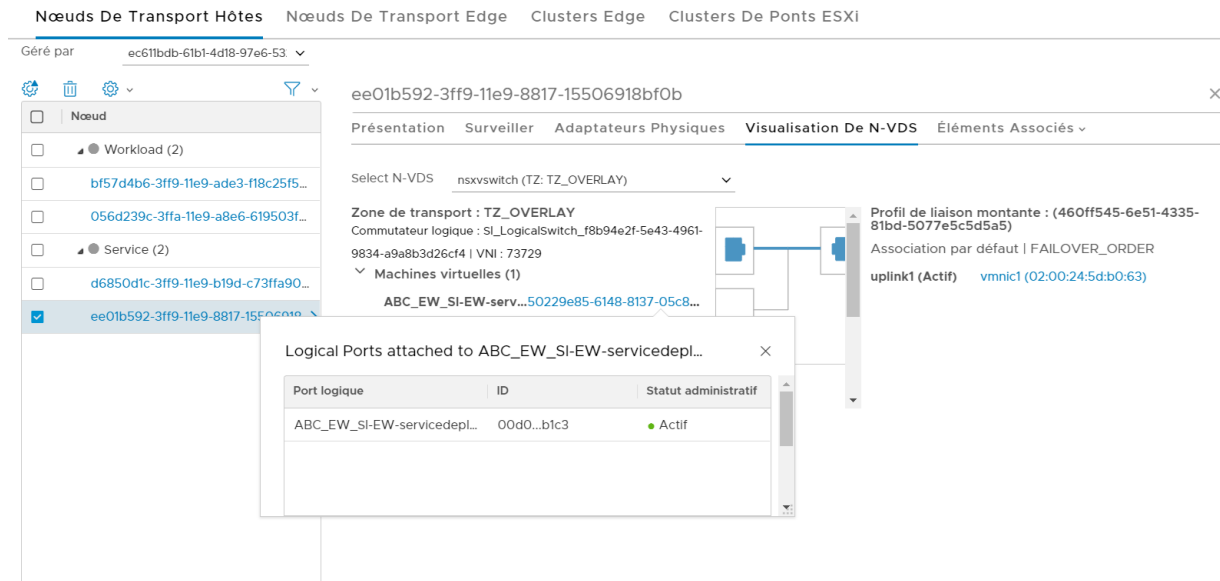
Tous les nœuds de transport placés en mode de maintenance NSX ne sont pas mis à niveau.

Représentation visuelle de N-VDS

Vous obtenez une vue détaillée de N-VDS à un niveau d'hôtes individuels. NSX-T Data Center fournit une représentation visuelle de l'état de connectivité entre la liaison montante de N-VDS et les machines virtuelles associées à une zone de transport. Les objets représentés visuellement incluent la stratégie d'association - liaison montante et carte réseau physique qui fournissent la connectivité aux machines virtuelles. L'autre ensemble d'objets visuellement représenté inclut des machines virtuelles, des ports logiques et des commutateurs associés, ainsi que l'état de machines virtuelles. La représentation visuelle simplifie la gestion de N-VDS.

Note Seuls les hôtes ESXi prennent en charge la visualisation d'un objet N-VDS.

Figure 10-3. Visualisation de 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 **Système > Infrastructure > Nœuds > Nœuds de transport hôtes**.
- 3 Dans le champ Géré par, sélectionnez **Hôte autonome** ou un *gestionnaire de calcul*.
- 4 Sélectionnez l'hôte.
- 5 Cliquez sur l'onglet **Visualisation N-VDS**.
- 6 Sélectionnez un N-VDS.
NSX-T représente visuellement les profils de liaison montante connectés aux machines virtuelles, les ports logiques associés aux machines virtuelles, les commutateurs logiques connectés à une zone de transport.
- 7 Pour afficher les profils de liaison montante connectés à une machine virtuelle et le port logique auquel une machine virtuelle est connectée, sélectionnez une machine virtuelle.
NSX-T représente visuellement la connectivité entre une machine virtuelle et un profil de liaison montante.
- 8 Pour afficher les machines virtuelles connectées à un profil de liaison montante, sélectionnez le profil de liaison montante.

- 9 Pour afficher les ports logiques associés à une machine virtuelle, développez le commutateur logique, cliquez sur la machine virtuelle.

Les détails du port logique sont affichés dans une boîte de dialogue distincte.

Note Le statut administratif d'un port logique s'affiche dans la boîte de dialogue. Si l'état de fonctionnement est inactif, il ne s'affiche pas dans la boîte de dialogue.

Contrôle de santé des plages d'ID VLAN et des paramètres MTU

Exécutez les API de contrôle de santé pour vérifier la compatibilité entre les plages d'ID VLAN que vous avez spécifiées et les paramètres MTU sur un nœud de transport avec les paramètres correspondants sur un commutateur physique.

La différence de configuration de VLAN ou MTU est une erreur de configuration courante qui peut entraîner une interruption de la connectivité.

Note

- Les résultats du contrôle de santé ne sont que des indicateurs d'erreurs possibles de la configuration réseau. Par exemple, le contrôle de santé exécuté sur des hôtes à partir de domaines L2 différents entraîne des ID VLAN non joints. Ce résultat ne peut pas être considéré comme une erreur de configuration, car les hôtes doivent se trouver dans le même domaine L2 pour que l'outil de contrôle de santé puisse obtenir des résultats corrects.
 - Seules 50 opérations de contrôle de santé peuvent être en cours à un moment précis.
 - Après la fin d'un contrôle de santé, NSX-T Data Center conserve ce résultat sur le système uniquement pendant 24 heures.
-

Dans une opération de contrôle de santé, l'agent NSX-T Data Center Ops envoie des paquets de sondage d'un nœud de transport vers un autre nœud pour vérifier la compatibilité entre la plage d'ID VLAN que vous avez spécifiée et la valeur MTU sur le nœud de transport avec les paramètres correspondants sur le commutateur physique.

Comme le nombre de plages d'ID VLAN à vérifier augmente, le temps d'attente augmente également.

Nombre de VLAN	Temps d'attente (en secondes)
[3073, 4095]	150
[1025, 3072]	120
[513, 1024]	80
[128, 512]	60
[64, 127]	30
[1, 63]	20

Conditions préalables

- Au moins deux liaisons montantes configurées sur N-VDS pour que le contrôle de VLAN et de MTU fonctionne.
- Nœuds de transport sur le même domaine L2.
- Contrôle de santé pris en charge sur les hôtes ESX exécutant la version 6.7 U2 ou des versions ultérieures.

Procédure

- 1 Créez un contrôle de santé manuel.

POST https://<NSXManager_IP>/api/v1/manual-health-checks

Example Request:

POST <https://<nsx-mgr>/api/v1/manual-health-checks>

```
{
  "resource_type": "ManualHealthCheck",
  "display_name": "Manual HealthCheck 002",
  "transport_zone_id": "7754341c-8f3c-443f-9c1a-2d635d5b0d1c",
  "vlangs": {
    "vlan_ranges": [{
      "start": 0,
      "end": 6
    },]
  },
}
```

Example Response:

```
{
  "operation_status": "FINISHED",
  "transport_zone_id": "7754341c-8f3c-443f-9c1a-2d635d5b0d1c",
  "vlangs": {
    "vlan_ranges": [
      {
        "start": 0,
        "end": 6
      }
    ]
  },
  "result": {
    "vlan_mtu_status": "UNTRUNKED",
    "results_per_transport_node": [
      {
        "transport_node_id": "dfcabffa-8839-11e9-b30e-6f45344d8a04",
        "result_on_host_switch": {
          "host_switch_name": "nsxvswitch",
          "results_per_uplink": [
            {
              "uplink_name": "uplink1",
              "vlan_and_mtu_allowed": [
                {
                  "start": 0,
                  "end": 0
                }
              ]
            }
          ]
        }
      }
    ]
  }
}
```

```

        }
      ],
      "mtu_disallowed": [],
      "vlan_disallowed": [
        {
          "start": 1,
          "end": 6
        }
      ]
    }
  ]
},
{
  "transport_node_id": "a300ea62-8839-11e9-a94e-31732bb71949",
  "result_on_host_switch": {
    "host_switch_name": "nsxvswitch",
    "results_per_uplink": [
      {
        "uplink_name": "uplink1",
        "vlan_and_mtu_allowed": [
          {
            "start": 0,
            "end": 0
          }
        ],
        "mtu_disallowed": [],
        "vlan_disallowed": [
          {
            "start": 1,
            "end": 6
          }
        ]
      }
    ]
  }
}
],
{
  "resource_type": "ManualHealthCheck",
  "id": "8a56ed9e-a31b-479e-987b-2dbfbde07c38",
  "display_name": "mc1",
  "_create_user": "admin",
  "_create_time": 1560149933059,
  "_last_modified_user": "system",
  "_last_modified_time": 1560149971220,
  "_system_owned": false,
  "_protection": "NOT_PROTECTED",
  "_revision": 0
}
]

```

Un nouvel objet de contrôle de santé est créé avec l'ID 8a56ed9e-a31b-479e-987b-2dbfbde07c38.

- 2 Pour obtenir une liste de toutes les opérations de contrôle de santé manuelles lancées, effectuez l'appel d'API.

```
GET https://<NSXManager_IP>/api/v1/manual-health-checks
```

- 3 Pour supprimer un contrôle de santé manuel, effectuez l'appel d'API.

```
DELETE https://<NSXManager_IP>/api/v1/manual-health-checks/<Health-check-ID>
```

- 4 Pour obtenir un seul contrôle de santé lancé manuellement, effectuez l'appel d'API.

```
GET https://<NSXManager_IP>/api/v1/manual-health-checks/< Health-check-ID>
```

Résultats

La section réponse de l'API contient les résultats du contrôle de santé. L'agent NSX Ops attend un paquet d'accusé de réception du nœud de transport de destination pour récupérer les plages d'ID VLAN prises en charge sur le commutateur physique.

- Non joints : répertorie les plages d'ID VLAN qui ne sont pas compatibles avec un commutateur physique. Les plages d'ID VLAN compatibles avec le commutateur physique sont également répertoriées.
- Joints : répertorie les plages d'ID VLAN qui sont compatibles avec un commutateur physique.
- Inconnu : il n'existe aucun résultat valide pour certaines ou toutes les liaisons montantes en raison de problèmes d'infrastructure ou de types de plate-forme non pris en charge, tels que KVM et Edge.

Paramètres dans la section réponse de l'API :

- `vlan_and_mtu_allowed` : répertorie les plages d'ID VLAN qui sont compatibles.
- `mtu_disallowed` : répertorie les plages d'ID VLAN pour lesquelles la valeur MTU n'est pas compatible avec un commutateur physique.
- `vlan_disallowed` : répertorie les plages d'ID VLAN qui ne sont pas compatibles avec un commutateur physique.

Étape suivante

- Dans une zone de transport basée sur la superposition, mettez à jour à la fois l'ID VLAN et la configuration MTU dans le profil de liaison montante sur N-VDS. De même, mettez à jour VLAN ou MTU sur le commutateur physique.
- Dans une zone de transport basée sur VLAN, mettez à jour la configuration MTU dans le profil de liaison montante. Ensuite, mettez à jour la configuration VLAN sur les commutateurs logiques de cette zone de transport. De même, mettez à jour VLAN ou MTU sur le commutateur physique.

Afficher l'état de détection de transfert bidirectionnel

Affichez l'état BFD (Bidirectional Forwarding Detection, détection de transfert bidirectionnel) entre les nœuds de transport. Chaque nœud de transport détecte l'état de la connectivité avec

un autre nœud de transport distant par le biais d'un état du tunnel qui affiche l'état BFD parmi d'autres informations liées au nœud.

Les nœuds de transport hôtes (autonomes et les hôtes enregistrés sur un vCenter) et les nœuds Edge affichent l'état du tunnel. Les paquets BFD prennent en charge l'encapsulation GENEVE et STT. GENEVE est l'encapsulation par défaut.

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 **Système > Infrastructure > Nœuds > Nœuds de transport hôtes**.
- 3 Dans la colonne Tunnel, cliquez sur le numéro du tunnel qui s'affiche.

La page Surveiller affiche l'état du tunnel, le code de diagnostic BFD, l'UUID du nœud distant, l'encapsulation sur les paquets BFD et le nom du tunnel.

Le code de diagnostic BFD du tunnel indique la raison de la modification de l'état de la session.

Code	Description
0	Aucun diagnostic
1	Temps de détection du contrôle expiré
2	Échec de la fonction d'écho
3	Session signalée par le voisin hors service
4	Réinitialisation du plan de transfert
5	Chemin d'accès hors service
6	Chemin d'accès concaténé hors service
7	Hors service d'un point de vue administratif
8	Chemin d'accès concaténé inversé

Résultats

Si l'état BFD est hors service, utilisez le code de diagnostic pour établir la connectivité entre les nœuds 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`.

Résultats

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-adf

(Infrastructure de diagnostic automatisé) Collecte et analyse les données de performance pour produire des diagnostics locaux (sur l'hôte) et centraux (dans le centre de données) des problèmes de performances.

nsx-aggservice

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-cli-libs

Fournit l'interface de ligne de commande de NSX-T Data Center sur les hôtes d'hyperviseur.

nsx-common-libs

Fournit certaines classes d'utilitaires comme AES, SHA-1, UUID, bitmap, etc.

nsx-context-mux

Fournit la fonctionnalité de relais NSX Guest Introspection. Permet aux agents invités VMware Tools de relayer le contexte d'invité aux dispositifs de partenaires tiers en interne et enregistrés.

nsx-esx-datapath

Fournit la fonctionnalité de traitement des paquets de plan de données de 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-metrics-libs

Fournit des classes d'utilitaires de mesure pour collecter des mesures de démon.

nsx-mpa

Fournit des communications entre NSX Manager et les hôtes d'hyperviseur.

nsx-nestdb-libs

NestDB est une base de données qui stocke les configurations NSX associées à l'hôte (état souhaité/d'exécution, etc.).

nsx-netcpa

Fournit des communications 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-opsagent

Communique les exécutions d'agent des opérations (réalisation du nœud de transport, LLDP - Link Layer Discovery Protocol, traceflow, capture de paquets, etc.) avec le plan de gestion.

nsx-platform-client

Fournit un agent d'exécution d'interface de ligne de commande commun, pour une interface de ligne de commande centralisée et une collecte de journaux d'audit.

nsx-profiling-lib

Fournit la fonctionnalité de profilage basée sur gpeftool qui est utilisé pour le profilage de processus démon.

nsx-proxy

Fournit le seul agent de point de contact ascendant qui communique avec le plan de contrôle central et le plan de gestion.

nsx-python-gevent

Contient Python Gevent.

nsx-python-greenlet

Contient la bibliothèque Python Greenlet (bibliothèques tierces).

nsx-python-logging

Contient les journaux Python.

nsx-python-protobuf

Fournit des liaisons Python pour les zones tampons de protocole.

nsx-rpc-lib

Cette bibliothèque fournit la fonctionnalité nsx-rpc.

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.

nsx-shared-libs

Contient les bibliothèques NSX partagées.

nsx-upm-libs

Fournit une fonctionnalité de gestion de profil unifiée pour aplatir la configuration côté client et éviter la transmission des données en double.

nsx-vdpi

Fournit des capacités Deep Packet Inspection pour le pare-feu distribué NSX-T Data Center.

nsxcli

Fournit l'interface de ligne de commande de NSX-T Data Center sur les hôtes d'hyperviseur.

vsipfwlib

Fournit la fonctionnalité de pare-feu distribué.

À des fins de vérifications, vous pouvez exécuter les commandes `esxcli software vib list | grep nsx` et `esxcli software vib list | grep vsipfwlib` sur l'hôte ESXi. Vous pouvez également exécuter la commande `esxcli software vib list | grep <yyyy-mm-dd>`, où la date correspond au jour de l'installation.

Étape suivante

Ajoutez l'hôte au plan de gestion NSX-T Data Center. Reportez-vous à la section [Déploiement de nœuds NSX Manager pour former un cluster à l'aide de la ligne de commande](#).

Installer manuellement les modules des logiciels NSX-T Data Center sur des hyperviseurs KVM Ubuntu

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 des modules tiers sur un hôte KVM](#).

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 | egrep 'nsx|openvswitch'`.

Les modules installés dans la sortie doivent correspondre aux modules présents dans le répertoire `nsx-lcp-trusty_amd64`.

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 [Déploiement de nœuds NSX Manager pour former un cluster à l'aide de la ligne de commande](#).

Installer manuellement des modules de logiciels 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.

```
/usr/share/openvswitch/scripts/ovs-systemd-reload 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'`.

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 [Déploiement de nœuds NSX Manager pour former un cluster à l'aide de la ligne de commande](#).

Installer manuellement les modules des logiciels NSX-T Data Center sur des hyperviseurs SUSE 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 SUSE 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 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 SUSE.

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-3.0.0.0.14335404-linux64-sles12sp3.tar.gz
```

- 4 Naviguez jusqu'au répertoire du module.

```
cd nsx-lcp-linux64-sles12sp3
```

- 5 Installez les modules.

```
sudo zypper --no-gpg-checks install -y *.rpm
```

Lorsque vous exécutez la commande d'installation `zypper`, toutes les dépendances NSX-T Data Center sont résolues, en partant du principe que les hôtes SUSE peuvent accéder à leurs référentiels respectifs.

6 Rechargez le module de noyau OVS.

```
/usr/share/openvswitch/scripts/ovs-systemd-reload 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 `zypper packages --installed-only | grep System | egrep 'openvswitch|nsx'`.

Les modules installés dans la sortie doivent correspondre aux modules présents dans le répertoire `nsx-lcp-linux64-sles12sp3`.

Étape suivante

Ajoutez l'hôte au plan de gestion NSX-T Data Center. Reportez-vous à la section [Déploiement de nœuds NSX Manager pour former un cluster à l'aide de la ligne de commande](#).

Déployer un cluster vSphere entièrement réduit pour NSX-T

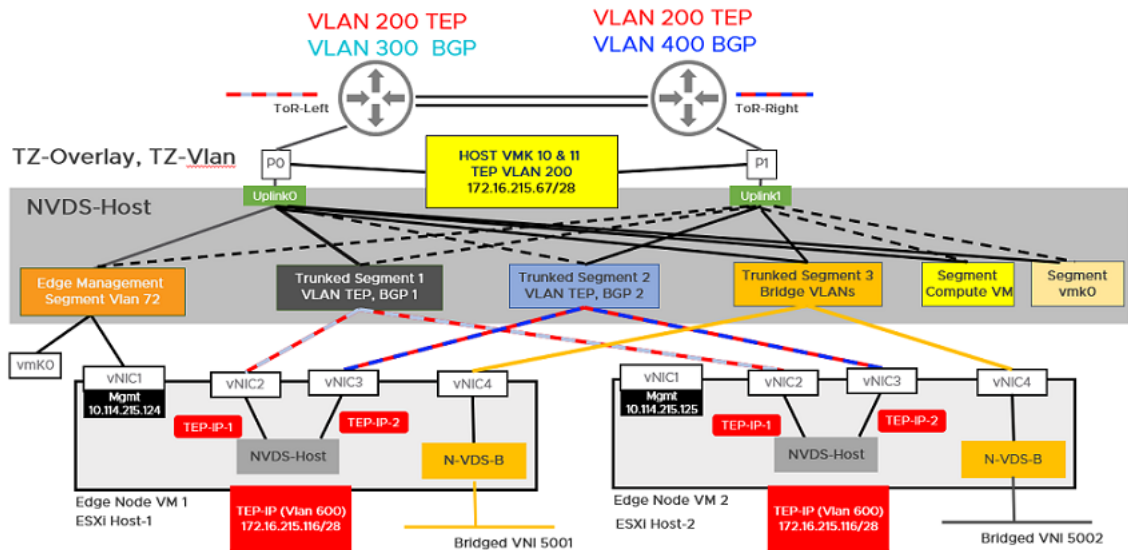
Vous pouvez configurer NSX Manager, des nœuds de transport hôtes et des machines virtuelles NSX Edge sur un cluster unique. Chaque hôte du cluster fournit deux cartes réseau physiques configurées pour NSX-T.

Important Déployez la topologie de cluster vSphere unique entièrement réduite à partir de la version NSX-T 2.4.2 ou 2.5.

La topologie référencée dans cette procédure utilise :

- Le vSAN configuré avec les hôtes du cluster.
- Un minimum de deux cartes réseau physiques par hôte.
- Les interfaces vMotion et VMkernel de gestion.

Figure 10-4. Topologie : commutateur N-VDS unique gérant la communication des hôtes avec NSX Edge et les machines virtuelles



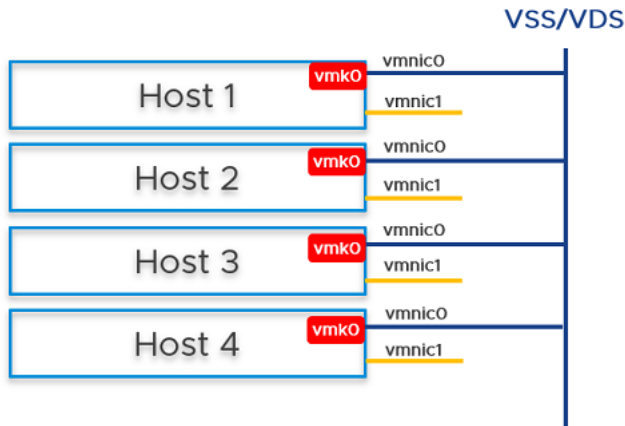
invitées

Conditions préalables

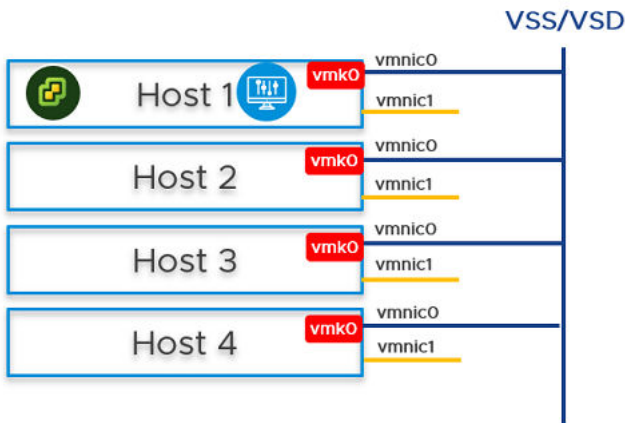
- Tous les hôtes doivent appartenir à un cluster vSphere.
- Deux cartes réseau physiques sont activées sur chaque hôte.
- Enregistrez tous les hôtes dans un vCenter Server.
- Vérifiez sur vCenter Server que le stockage partagé est disponible pour une utilisation par les hôtes.
- L'adresse IP TEP de l'hôte et l'adresse IP TEP de NSX Edge doivent se trouver dans un VLAN différent. Le trafic nord-sud des charges de travail de l'hôte est encapsulé dans GENEVE et envoyé à un nœud NSX Edge avec l'adresse IP source comme TEP d'hôte et l'adresse IP de destination comme TEP NSX Edge. Comme ces TEP doivent se trouver sur des VLAN ou des sous-réseaux différents, ce trafic doit être acheminé via des commutateurs ToR (Top-of-Rack). Le VLAN de transport utilisé pour l'hôte est VLAN 200 et le VLAN de transport utilisé pour NSX Edge est VLAN 600.

Procédure

- 1 La préparation de quatre hôtes ESXi avec vmnic0 sur vSS ou vDS, vmnic1 est gratuite.



- 2 Sur l'hôte 1, installez vCenter Server, configurez un groupe de ports vSS/vDS et installez NSX Manager sur le groupe de ports créé sur l'hôte.

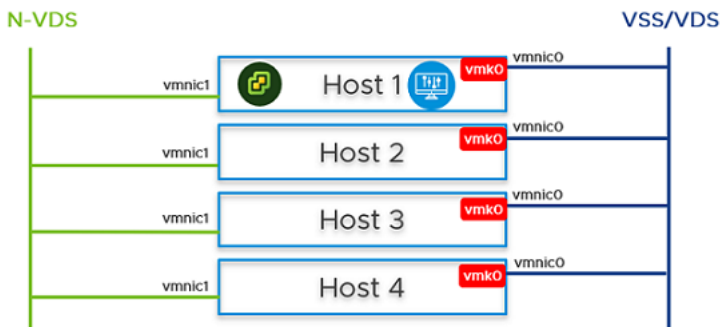


- 3 Préparez les hôtes ESXi 1, 2, 3 et 4 comme nœuds de transport.
 - a Créer une zone de transport VLAN et une zone de transport de superposition avec une stratégie d'association nommée. Reportez-vous à la section [Créer des zones de transport](#).
 - b Créez un pool d'adresses IP ou DHCP pour les adresses IP du point de terminaison de tunnel pour les hôtes. Reportez-vous à la section [Créer un pool d'adresses IP pour les adresses IP des points de terminaison de tunnel](#).
 - c Créez un pool d'adresses IP ou DHCP pour les adresses IP du point de terminaison de tunnel pour le nœud Edge. Reportez-vous à la section [Créer un pool d'adresses IP pour les adresses IP des points de terminaison de tunnel](#).
 - d Créez un profil de liaison montante avec une stratégie d'association nommée. Reportez-vous à la section [Créer un profil de liaison montante](#).

- e Configurez des hôtes de cluster en tant que nœuds de transport en appliquant un profil de nœud de transport. Dans cette étape, le profil de nœud de transport migre uniquement vmnic1 (la carte réseau physique inutilisée) vers le commutateur N-VDS. Une fois le profil de nœud de transport appliqué aux hôtes du cluster, le commutateur N-VDS est créé et la carte réseau vmnic1 est connectée au commutateur N-VDS. Reportez-vous à la section [Ajouter un profil de nœud de transport](#).

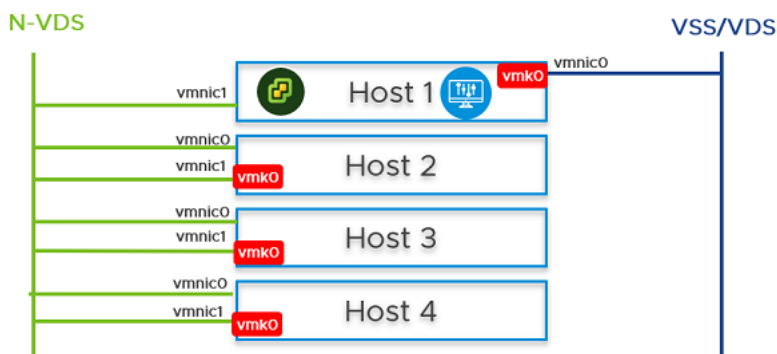
Modifier le profil du nœud de transport - TNP-... ?

Nom du N-VDS *	vds-1	▼
Zones de transport associées	tz	
Profil NIOC *	nsx-default-nioc-hostswitch-profile	▼
	OU créer un profil NIOC	
Profil de liaison montante *	hostnodeprofile	▼
	OU créer un profil de liaison montante	
Profil LLDP *	LLDP [Send Packet Enabled]	▼
Attribution IP *	Utiliser le pool IP	▼
Pool IP *	ippoolhostnode	▼
	OU créer et utiliser un pool IP	
Cartes réseau physiques	vmnic1	activeuplinkhost ▼
	Ajouter une PNIC	
Migration de carte réseau physique uniquement	<input checked="" type="checkbox"/> Oui	
Activer cette option si aucun VMK n'existe sur la carte réseau physique sélectionnée pour la migration		
Mappages de réseau pour l'installation	Ajouter un mappage	
Mappages de réseau pour la désinstallation	Ajouter un mappage	

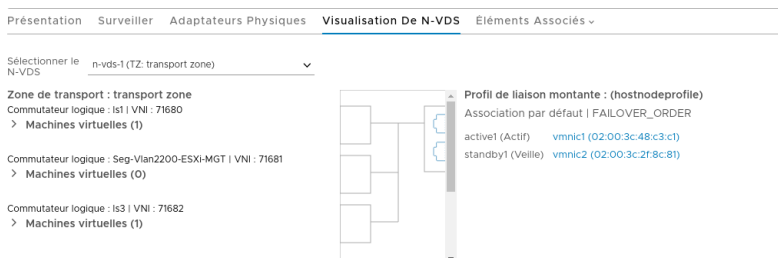


La carte réseau vmnic1 sur tous les hôtes est ajoutée au commutateur N-VDS. Ainsi, sur les deux cartes réseau physiques, l'une est migrée vers le commutateur N-VDS. L'interface vmnic0 est toujours connectée au commutateur vSS ou vDS, ce qui garantit la disponibilité de la connectivité avec l'hôte.

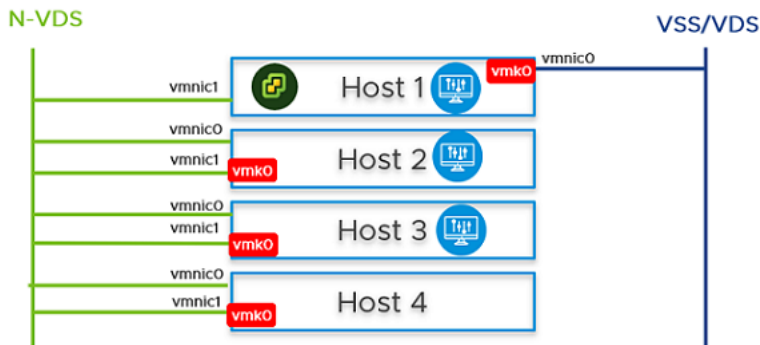
- 4 Dans l'interface utilisateur de NSX Manager, créez des segments basés sur le VLAN pour NSX Manager, vCenter Server et NSX Edge. Veillez à sélectionner la stratégie d'association appropriée pour chacun des segments basés sur le VLAN. N'utilisez pas le commutateur logique de jonction VLAN en tant que cible. Lors de la création des segments cibles dans l'interface utilisateur de NSX Manager, dans le champ **Entrez une liste de VLAN**, entrez une seule valeur de VLAN.
- 5 Sur l'hôte 2, l'hôte 3 et l'hôte 4, vous devez migrer l'adaptateur vmk0 et vmnic0 ensemble de VSS/VDS vers le commutateur N-VDS. Mettez à jour la configuration de NSX-T sur chaque hôte. Lors de la migration, assurez-vous que :
 - vmk0 est mappé au **segment de gestion Edge**.
 - vmnic0 est mappée à une liaison montante active, **liaison montante 1**.



- 6 Dans le vCenter Server, accédez à l'hôte 2, à l'hôte 3 et à l'hôte 4, puis vérifiez que l'adaptateur vmk0 est connecté à la carte réseau physique vmnic0 sur le N-VDS et accessible.
- 7 Dans l'interface utilisateur de NSX Manager, accédez à l'hôte 2, à l'hôte 3 et à l'hôte 4, puis vérifiez que les deux cartes PNIC se trouvent sur le commutateur N-VDS.

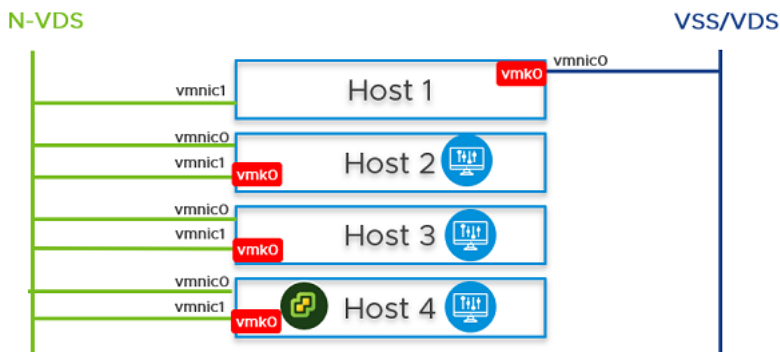


- 8 Sur l'hôte 2 et l'hôte 3, à partir de l'interface utilisateur de NSX Manager, installez NSX Manager et attachez NSX Manager au segment. Attendez environ 10 minutes que le cluster se forme et vérifiez que le cluster s'est formé.



- 9 Désactivez le premier nœud NSX Manager. Attendez environ 10 minutes.
- 10 Rattachez le dispositif NSX Manager et vCenter Server au commutateur logique créé précédemment. Sur l'hôte 4, mettez le dispositif NSX Manager sous tension. Attendez environ 10 minutes pour vérifier que le cluster est dans un état stable. Avec la première instance de NSX Manager hors tension, procédez à une opération vMotion à froid pour migrer le dispositif NSX Manager et vCenter Server de l'hôte 1 vers l'hôte 4.

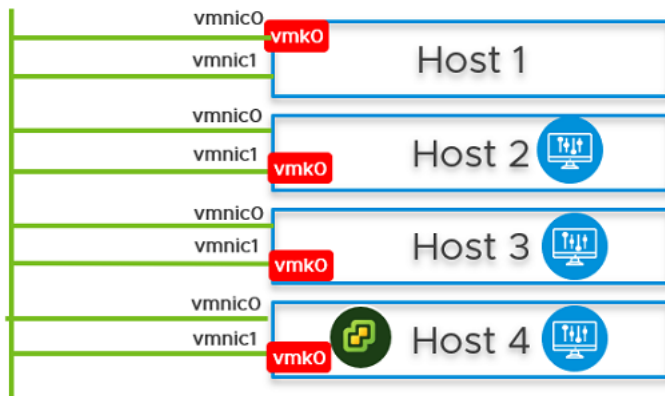
Pour connaître les limitations de vMotion, reportez-vous à la section <https://kb.vmware.com/s/article/56991>.



- 11 Dans l'interface utilisateur de NSX Manager, accédez à l'hôte 1, migrez vmk0 et vmnic0 ensemble de VSS vers le commutateur N-VDS.

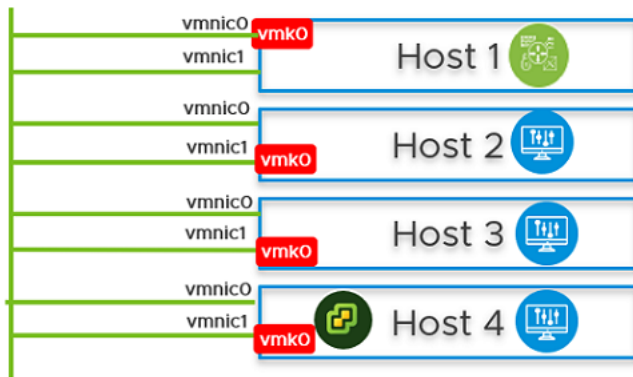
- 12** Dans le champ **Mappage réseau pour l'installation**, assurez-vous que l'adaptateur vmk0 est mappé au **segment de gestion Edge** sur le commutateur N-VDS.

N-VDS



- 13** Sur l'hôte 1, installez la machine virtuelle NSX Edge à partir de l'interface utilisateur de NSX Manager.

Reportez-vous à la section [Créer un nœud de transport NSX Edge](#).

N-VDS

- 14 Reliez la machine virtuelle NSX Edge au plan de gestion.
Reportez-vous à la section [Relier NSX Edge au plan de gestion](#).
- 15 Pour établir la connectivité du trafic vertical, configurez la VM NSX Edge avec un routeur externe.
- 16 Vérifiez que la connectivité du trafic nord-sud entre la machine virtuelle NSX Edge et le routeur externe.
- 17 En cas de scénario de panne de courant lors du redémarrage du cluster entier, le composant de gestion NSX-T peut ne pas s'afficher et communiquer avec N-VDS. Pour éviter ce scénario, suivez les étapes décrites ci-dessous :

Attention Toute commande d'API exécutée de manière incorrecte entraîne une perte de connectivité avec NSX Manager.

Note Dans une configuration à cluster unique, les composants de gestion sont hébergés sur un commutateur N-VDS en tant que machines virtuelles. Le port N-VDS auquel le composant de gestion se connecte par défaut est initialisé en tant que port bloqué pour des raisons de sécurité. Si une coupure électrique se produit et nécessite que les quatre hôtes redémarrent, le port de la machine virtuelle de gestion sera initialisé sur un état bloqué. Pour éviter les dépendances circulaires, il est recommandé de créer un port sur N-VDS à l'état non bloqué. Un port non bloqué garantit que lors du redémarrage du cluster, le composant de gestion NSX-T peut communiquer avec N-VDS pour reprendre un fonctionnement normal.

À la fin de la sous-tâche, la commande de migration prend les éléments suivants :

- UUID du nœud hôte sur lequel réside NSX Manager.
- UUID de la VM NSX Manager et le migre vers le port logique statique qui est dans un état non bloqué.

Si tous les hôtes sont mis hors tension ou mis sous tension ou si une machine virtuelle NSX Manager est transférée vers un autre hôte, lorsqu'une instance de NSX Manager est rétablie, elle est alors attachée au port non bloqué, ce qui empêche toute perte de connectivité avec le composant de gestion de NSX-T.

- a Dans l'interface utilisateur de NSX Manager, accédez à l'onglet **Mise en réseau et sécurité avancées** (2.5.1 et versions antérieures). Recherchez le segment de la **Machine virtuelle de calcul de segment**. Sélectionnez l'onglet **Présentation**, recherchez et copiez l'UUID. L'UUID utilisé dans cet exemple est `c3fd8e1b-5b89-478e-abb5-d55603f04452`.
- b Créez une charge utile JSON pour chaque NSX Manager.
 - Dans la charge utile JSON, créez des ports logiques avec l'état d'initialisation dans l'état **UNBLOCKED_VLAN** en remplaçant la valeur de `logical_switch_id` par l'UUID du **segment de gestion du dispositif Edge** précédemment créé.
 - Dans la charge utile pour chaque NSX Manager, les valeurs `attachment_type_id` et `display_name` sont différentes.

Important Répétez cette étape pour créer un total de quatre fichiers JSON : trois pour les instances de NSX Manager et un pour vCenter Server Appliance (VCSA).

```
port1.json
{
  "admin_state": "UP",
  "attachment": {
    "attachment_type": "VIF",
    "id": "nsxmgr-port-147"
  },
  "display_name": "NSX Manager Node 147 Port",
  "init_state": "UNBLOCKED_VLAN",
  "logical_switch_id": "c3fd8e1b-5b89-478e-abb5-d55603f04452"
}
```

Où :

- `admin_state` : il s'agit de l'état du port. Il doit être activé.
- `attachment_type` : doit être défini sur VIF. Toutes les machines virtuelles sont connectées à des ports de commutateur NSX-T à l'aide d'un ID de VIF.
- `id` : il s'agit de l'ID de VIF. Il doit être unique pour chaque NSX Manager. Si vous disposez de trois NSX Manager, il y aura trois charges utiles, et chacune d'entre elles doit avoir un ID de VIF différent. Pour générer un UUID unique, connectez-vous à l'interpréteur de commandes racine de NSX Manager et exécutez `/usr/bin/uuidgen` pour générer un UUID unique.
- `display_name` : il doit être unique pour aider l'administrateur NSX à l'identifier à partir d'autres noms d'affichage NSX Manager.
- `init_state` : avec la valeur définie sur UNBLOCKED_VLAN, NSX débloquent le port pour NSX Manager, même si NSX Manager n'est pas disponible.

- `logical_switch_id` : il s'agit de l'ID du commutateur logique du **segment de gestion Edge**.

- c Si trois NSX Manager sont déployés, vous devez créer trois sections de configuration, une pour chaque port logique d'un NSX Manager. Par exemple, port1.json, port2.json, port3.json.

Exécutez les commandes suivantes pour créer des charges utiles.

```
curl -X POST -k -u '<username>:<password>' -H 'Content-Type:application/json' -d @port1.json https://nsxmgr/api/v1/logical-ports
```

```
curl -X POST -k -u '<username>:<password>' -H 'Content-Type:application/json' -d @port2.json https://nsxmgr/api/v1/logical-ports
```

```
curl -X POST -k -u '<username>:<password>' -H 'Content-Type:application/json' -d @port3.json https://nsxmgr/api/v1/logical-ports
```

Exemple d'exécution d'API pour créer un port logique.

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -X POST -k -u
'<username>:<password>' -H 'Content-Type:application/json' -d @port1.json https://
localhost/api/v1/logical-ports
{
  "logical_switch_id" : "c3fd8e1b-5b89-478e-abb5-d55603f04452",
  "attachment" : {
    "attachment_type" : "VIF",
    "id" : "nsxmgr-port-147"
  },
  "admin_state" : "UP",
  "address_bindings" : [ ],
  "switching_profile_ids" : [ {
    "key" : "SwitchSecuritySwitchingProfile",
    "value" : "fbc4fb17-83d9-4b53-a286-ccdf04301888"
  }, {
    "key" : "SpoofGuardSwitchingProfile",
    "value" : "fad98876-d7ff-11e4-b9d6-1681e6b88ec1"
  }, {
    "key" : "IpDiscoverySwitchingProfile",
    "value" : "0c403bc9-7773-4680-a5cc-847ed0f9f52e"
  }, {
    "key" : "MacManagementSwitchingProfile",
    "value" : "1e7101c8-cfef-415a-9c8c-ce3d8dd078fb"
  }, {
    "key" : "PortMirroringSwitchingProfile",
    "value" : "93b4b7e8-f116-415d-a50c-3364611b5d09"
  }, {
    "key" : "QosSwitchingProfile",
    "value" : "f313290b-eba8-4262-bd93-fab5026e9495"
  } ],
  "init_state" : "UNBLOCKED_VLAN",
  "ignore_address_bindings" : [ ],
  "resource_type" : "LogicalPort",
  "id" : "02e0d76f-83fa-4839-a525-855b47ecb647",
  "display_name" : "NSX Manager Node 147 Port",
  "_create_user" : "admin",
  "_create_time" : 1574716624192,
  "_last_modified_user" : "admin",
```

```
"_last_modified_time" : 1574716624192,
"_system_owned" : false,
"_protection" : "NOT_PROTECTED",
"_revision" : 0
```

- d Vérifiez que le port de commutateur logique est créé.

Commutateurs **Ports** Profils De Commutation

+ AJOUTER MODIFIER SUPPRIMER ACTIONS

Rechercher

<input type="checkbox"/>	Port logique	ID	Statut administré	État opérationnel	Profils de commutation	Attachement	Commutateur logique
<input type="checkbox"/>	1356a49d-dc33-42be-9e83-4c6...	1356...d0ee	Actif	Actif	nsx-default-switch-security-non...	LR :80fb...2662	Is3
<input type="checkbox"/>	61d5708b-a4ff-4954-b217-8338...	61d5...b43a	Actif	Actif	nsx-default-switch-security-non...	LR :42ac...a24	Is1
<input type="checkbox"/>	NSX Manager Node 147 Port	58ad...a1cb	Actif	Inactif	nsx-default-switch-security-vif...	VM:nsx-mgr-147	Is1
<input type="checkbox"/>	ubuntu12.04.1-2G-LAMP/ubuntu1...	3fb2...f698	Actif	Actif	nsx-default-switch-security-vif...	VM :vm1	Is1
<input type="checkbox"/>	vmnic@n-vds-1@94b323e6-1ee...	2021...4d76	Actif	Actif	nsx-default-switch-security-vif...	VIF :abf2...0495	Seg-Vlan2200-ESXi-MGT
<input type="checkbox"/>	worker/worker.vmx@94b323e6...	50b7...9b4c	Actif	Actif	nsx-default-switch-security-vif...	VM :vm3	Is3

- e Recherchez l'ID d'instance de machine virtuelle pour chaque NSX Manager. Vous pouvez récupérer l'ID d'instance dans **Inventaire** → **Machines virtuelles**, sélectionnez la machine virtuelle NSX Manager, sélectionnez l'onglet **Présentation** et copiez l'ID de l'instance. Vous pouvez également rechercher l'ID de l'instance dans le MOB (Managed Object Browser) de vCenter Server. Ajoutez **:4000** à l'ID pour obtenir l'index matériel VNIC d'une machine virtuelle NSX Manager.

Par exemple, si l'UUID d'instance de la machine virtuelle est 503c9e2b-0abf-a91c-319c-1d2487245c08, son index vNIC est 503c9e2b-0abf-a91c-319c-1d2487245c08:4000. Les trois indices vnic de NSX Manager sont les suivants :

mgr1 vnic: 503c9e2b-0abf-a91c-319c-1d2487245c08:4000

mgr2 vnic: 503c76d4-3f7f-ed5e-2878-cffc24df5a88:4000

mgr3 vnic: 503cafd5-692e-d054-6463-230662590758:4000

- f Recherchez l'ID du nœud de transport qui héberge NSX Manager. Si vous disposez de trois NSX Manager, chacun hébergé sur un nœud de transport différent, notez les ID de nœud de transport. Par exemple, les trois ID de nœud de transport sont les suivants :

tn1: 12d19875-90ed-4c78-a6bb-a3b1dfe0d5ea

tn2: 4b6e182e-0ee3-403f-926a-fb7c8408a9b7

tn3: d7cec2c9-b776-4829-beea-1258d8b8d59b

- g Récupérez la configuration du nœud de transport qui doit être utilisée comme charge utile lors de la migration de NSX Manager vers le port récemment créé.

Par exemple,

```
curl -k -u '<user>:<password>' https://nsxmgr/api/v1/transport-nodes/12d19875-90ed-4c78-a6bb-a3b1dfe0d5ea > tn1.json
```

```
curl -k -u '<user>:<password>' https://nsxmgr/api/v1/transport-nodes/4b6e182e-0ee3-403f-926a-fb7c8408a9b7 > tn2.json
```

```
curl -k -u '<user>:<password>' https://nsxmgr/api/v1/transport-nodes/d7cec2c9-b776-4829-beea-1258d8b8d59b > tn3.json
```

- h Migrez le NSX Manager du port précédent vers le port logique non bloqué récemment créé sur le **segment de gestion du dispositif Edge**. La valeur VIF-ID est l'ID d'attachement des ports créés précédemment pour NSX Manager.

Les paramètres suivants sont nécessaires pour migrer NSX Manager :

- ID du nœud de transport
- Configuration du nœud de transport
- Index matériel de la VNIC de NSX Manager
- ID de la VIF de NSX Manager

La commande API pour migrer NSX Manager vers le port non bloqué récemment créé est la suivante :

```
/api/v1/transport-nodes/<TN-ID>?vnic=<VNIC-ID>&vif=<VIF-ID>
```

Par exemple,

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -k -X PUT -u 'admin:VMware1!VMware1!' -H 'Content-Type:application/json' -d @mgr.json 'https://localhost/api/v1/transport-nodes/11161331-11f8-45c7-8747-34e7218b687f?vnic=5028d756-d36f-719e-3db5-7ae24aa1d6f3:4000&vif=nsxmgr-port-147'
```

- i Assurez-vous que le port logique créé statiquement est Actif.

Commutateurs **Ports** Profils De Commutation

+ AJOUTER

MODIFIER

SUPPRIMER

ACTIONS

Rechercher

<input type="checkbox"/>	Port logique ↑	ID	Statut administr	État opérationnel	Profils de commutation	Attachement	Commutateur logique
<input type="checkbox"/>	1356a49d-dc33-42be-9e83-4c6...	1356...d0ee	● Actif	● Actif	nsx-default-switch-security-non...	LR :80fb...2662	Is3
<input type="checkbox"/>	61d5708b-a4ff-4954-b217-8338...	61d5...b43a	● Actif	● Actif	nsx-default-switch-security-non...	LR :42ac...ad24	Is1
<input type="checkbox"/>	NSX Manager Node 147 Port	58ad...a1cb	● Actif	● Actif	nsx-default-switch-security-vif...	VM:nsx-mgr-147	Is1
<input type="checkbox"/>	ubuntu12.04.1-2G-LAMP/ubuntu1...	3fb2...f698	● Actif	● Actif	nsx-default-switch-security-vif...	VM :vm1	Is1
<input type="checkbox"/>	vmknic@n-vds-1@94b323e6-lee...	2021...4d76	● Actif	● Actif	nsx-default-switch-security-vif...	VIF :abf2...0495	Seq-Vlan2200-ESXi-MGT
<input type="checkbox"/>	worker/worker.vmx@94b323e6...	50b7...9b4c	● Actif	● Actif	nsx-default-switch-security-vif...	VM :vm3	Is3

- j Répétez les étapes précédentes sur chaque instance de NSX Manager du cluster.

Intégration de profils d'hôte avec NSX-T

11

Intégrez les profils d'hôte extraits d'un hôte ESXi avec NSX-T pour déployer les VIB NSX-T et ESXi sur des serveurs avec et sans état.

Ce chapitre contient les rubriques suivantes :

- [Déployer automatiquement un cluster sans état](#)
- [Serveurs avec état](#)

Déployer automatiquement un cluster sans état

Étant donné que les hôtes sans état ne conservent pas la configuration, ils ont besoin d'un serveur de déploiement automatique pour fournir les fichiers de démarrage requis lors de la mise sous tension des hôtes.

Cette section vous aide à configurer un cluster sans état à l'aide de vSphere Auto Deploy et du profil de nœud de transport NSX-T pour reprovisionner un hôte avec un nouveau profil d'image contenant une autre version d' ESXi et de NSX-T. Les hôtes qui sont configurés pour vSphere Auto Deploy utilisent un serveur de déploiement automatique et les profils d'hôte vSphere pour la personnalisation. Ces hôtes peuvent également être configurés pour le profil de nœud de transport NSX-T afin de configurer NSX-T sur les hôtes.

Par conséquent, un hôte sans état peut être configuré pour vSphere Auto Deploy et le profil de nœud de transport NSX-T afin de reprovisionner un hôte avec une version d'ESXi et de NSX-T personnalisée.

Tâches de haut niveau pour le déploiement automatique d'un cluster sans état

Tâches de haut niveau pour déployer automatiquement un cluster sans état.

Les tâches de haut niveau permettant de configurer un cluster sans état Auto Deploy sont les suivantes :

- 1 Conditions préalables et versions prises en charge. Reportez-vous à la section [Conditions préalables et versions prises en charge](#).

- 2 (Hôte de référence) Créer un profil d'image personnalisé. Reportez-vous à la section [Créer un profil d'image personnalisé pour les hôtes sans état](#).
- 3 (Hôtes de référence et cibles) Associer le profil d'image personnalisé. Reportez-vous à la section [Associer l'image personnalisée aux hôtes de référence et cibles](#).
- 4 (Hôte de référence) Configurer la configuration réseau dans ESXi. Reportez-vous à la section [Définir la configuration réseau sur l'hôte de référence](#).
- 5 (Hôte de référence) Configurer en tant que nœud de transport dans NSX. Reportez-vous à la section [Configurer l'hôte de référence en tant que nœud de transport dans NSX-T](#).
- 6 (Hôte de référence) Extraire et vérifier le profil d'hôte. Reportez-vous à la section [Extraire et vérifier le profil d'hôte](#).
- 7 (Hôtes de référence et cibles) Vérifier l'association de profils d'hôte avec un cluster sans état. Reportez-vous à la section [Vérifier l'association de profil d'hôte à un cluster sans état](#).
- 8 (Hôte de référence) Mettre à jour la personnalisation de l'hôte. Reportez-vous à la section [Mettre à jour la personnalisation de l'hôte](#).
- 9 (Hôtes cibles) Déclencher le déploiement automatique. Reportez-vous à la section [Déclencher le déploiement automatique sur les hôtes cibles](#).
 - a Avant d'appliquer le profil de nœud de transport. Reportez-vous à la section [Redémarrer les hôtes avant l'application de TNP](#).
 - b Appliquer le profil de nœud de transport. Reportez-vous à la section [Appliquer TNP sur un cluster sans état](#).
 - c Après l'application du profil de nœud de transport. Reportez-vous à la section [Redémarrer les hôtes après l'application de TNP](#).
- 10 Dépanner le profil d'hôte et le profil de nœud de transport. Reportez-vous à la section [Dépanner le profil d'hôte et le profil de nœud de transport](#).

Conditions préalables et versions prises en charge

Conditions préalables et versions d' ESXi et de NSX-T prises en charge.

Workflows pris en charge

- Avec le profil d'image et HostProfile

Conditions préalables

- Seuls les clusters homogènes (tous les hôtes d'un cluster doivent être sans état ou avec état) sont pris en charge.
- Le service de générateur d'images doit être activé.
- Le service de déploiement automatique doit être activé.

Versions d'ESXi et de NSX prises en charge

Version d'ESXi prise en charge	ESXi 67ep6	ESXi 67u2	ESXi 67u3	ESXi 67ep7	ESXi 67ep15	ESXi 67ep17
NSX-T Data Center 2.4	Oui	Oui	Non	Non	Non	Non
NSX-T Data Center 2.4.1	Oui	Oui	Non	Non	Non	Non
NSX-T Data Center 2.4.2	Oui	Oui	Non	Non	Non	Non
NSX-T Data Center 2.4.3	Oui	Oui	Non	Non	Non	Non
NSX-T Data Center 2.5	Oui	Oui	Oui	Oui	Non	Non
NSX-T Data Center 2.5.1	Oui	Oui	Oui	Oui	Oui	Oui

Créer un profil d'image personnalisé pour les hôtes sans état

Dans votre centre de données, identifiez un hôte à préparer comme hôte de référence.

La première fois que l'hôte de référence démarre, ESXi associe la règle par défaut à l'hôte de référence. Dans cette procédure, nous ajoutons un profil d'image personnalisé (les VIB ESXi et NSX) et nous associons l'hôte de référence à la nouvelle image personnalisée. Un profil d'image avec l'image NSX-T réduit considérablement le temps d'installation. La même image personnalisée est associée aux hôtes cibles dans le cluster sans état.

Note Vous pouvez également ajouter uniquement un profil d'image ESXi au cluster sans état de référence et cible. Les VIB NSX-T sont téléchargés lorsque vous appliquez le profil de nœud de transport sur le cluster sans état. Reportez-vous à la section [Ajouter un dépôt de logiciels](#).

Conditions préalables

Assurez-vous que le service Auto Deploy et le service Image Builder sont activés. Reportez-vous à la section [Utiliser vSphere Auto Deploy pour réapprovisionner des hôtes](#).

Procédure

- 1 Pour importer des modules NSX-T, créez un dépôt de logiciels.
- 2 Téléchargez les modules nsx-lcp.
 - a Connectez-vous à <https://my.vmware.com>.
 - b Sur la page Télécharger VMware NSX-T Data Center, sélectionnez la version de NSX-T.
 - c Sur la page des téléchargements de produits, recherchez NSX-T Modules de noyau pour une version de VMware ESXi spécifique.
 - d Cliquez sur **Télécharger maintenant** pour commencer à télécharger le module nsx-lcp.
 - e Importez les modules nsx-lcp dans le dépôt de logiciels.

NSX Kernel Module for VMware ESXi 6.7
 Taille du fichier: 37.64 MB
 Type de fichier: zip

Télécharger maintenant

Name: nsx-lcp-2.5.0.0.14663975-esx67.zip
Date de version: 2019-09-19
Numéro de build: 14663974

NSX Kernel Module for VMware ESXi 6.7
 This package includes the required kernel modules to enable NSX on ESXi 6.7 if needed for a manual installation. Use esxcli to install manually or include as part of an automated deployment system of the ESXi hosts.
MD5SUM: f224a0e12fc1722ae5b5259d279bfba1
SHA1SUM: a97d3125a26a47b94ec8408acd369d42681d3027
SHA256SUM:
 1ed76de6a7f22d227eb4be30a2e0aa91492a876b7b164814198de3
 1eec77bc44

- 3 Créez un autre dépôt de logiciels pour importer des modules ESXi.
vSphere Web Client affiche deux dépôts créés sur l'hôte de référence.
- 4 Créez un dépôt de logiciels personnalisé pour cloner l'image ESXi précédemment importée et les modules nsx-lcp.
 - a Sélectionnez le profil d'image ESXi dans le dépôt de logiciels ESXi créé à l'étape précédente.
 - b Cliquez sur **Cloner**.
 - c Dans l'assistant Cloner un profil d'image, entrez un nom pour l'image personnalisée à créer.
 - d Sélectionnez le dépôt de logiciels personnalisé dans lequel l'image clonée (ESXi) doit être disponible.
 - e Dans la fenêtre Sélectionner des modules logiciels, sélectionnez le niveau d'acceptation **Certifié par VMware**. Les VIB ESXi sont présélectionnés.
 - f Identifiez et sélectionnez manuellement des modules NSX-T dans la liste des modules et cliquez sur **Suivant**.
 - g Dans l'écran Prêt à terminer, vérifiez les détails et cliquez sur **Terminer** pour créer l'image clonée contenant les modules ESXi et NSX-T dans le dépôt de logiciels personnalisé.

Modifier un profil d'image

1 Nom et détails

2 Sélectionner les modules logiciels

3 Prêt à terminer

Sélectionner les modules logiciels

Niveau d'acceptation

Certifié par VMware

	Nom	Version	Niveau d'acceptation	Fournisseur	Dépôt
<input checked="" type="checkbox"/>	bnxtnet	216.0.50.0-4vmw.700.1...	Certifié par VMw...	VMW	esx70
<input checked="" type="checkbox"/>	bnxtroce	216.0.58.0-1vmw.700.1...	Certifié par VMw...	VMW	esx70
<input checked="" type="checkbox"/>	brcmfcoe	12.0.1500.0-1vmw.700.1...	Certifié par VMw...	VMW	esx70
<input checked="" type="checkbox"/>	brcmvmefc	12.4.293.2-3vmw.700.1...	Certifié par VMw...	VMW	esx70
<input checked="" type="checkbox"/>	cpu-microcode	7.0.0-1.0.15735143	Certifié par VMw...	VMware	esx70
<input checked="" type="checkbox"/>	crx	7.0.0-1.0.15735143	Certifié par VMw...	VMware	esx70
<input checked="" type="checkbox"/>	elx-esx-ibbelxima...	12.0.1200.0-2vmw.700...	Certifié par VMw...	VMware	esx70
<input checked="" type="checkbox"/>	elxiscsi	12.0.1200.0-1vmw.700.1...	Certifié par VMw...	VMW	esx70
<input checked="" type="checkbox"/>	elxnet	12.0.1250.0-5vmw.700...	Certifié par VMw...	VMW	esx70
<input checked="" type="checkbox"/>	esx-base	7.0.0-1.0.15735143	Certifié par VMw...	VMware	esx70
<input checked="" type="checkbox"/>	esx-dvfilter-gene...	7.0.0-1.0.15735143	Certifié par VMw...	VMware	esx70
<input checked="" type="checkbox"/>	esx-ui	1.34.0-15603211	Certifié par VMw...	VMware	esx70
<input checked="" type="checkbox"/>	esx-update	7.0.0-1.0.15735143	Certifié par VMw...	VMware	esx70
<input checked="" type="checkbox"/>	esx-xserver	7.0.0-1.0.15735143	Certifié par VMw...	VMware	esx70
<input checked="" type="checkbox"/>	i40en	1.8.116-1vmw.700.1.0.15...	Certifié par VMw...	VMW	esx70
<input checked="" type="checkbox"/>	i40iwn	1.12.5-1vmw.700.1.0.157...	Certifié par VMw...	VMW	esx70

98 éléments sélectionnés sur 98

ANNULER

PRÉCÉDENT

SUIVANT

Étape suivante

Associez l'image personnalisée aux hôtes de référence et cibles. Reportez-vous à la section [Associer l'image personnalisée aux hôtes de référence et cibles](#).

Associer l'image personnalisée aux hôtes de référence et cibles

Pour démarrer l'hôte de référence et les hôtes cibles avec la nouvelle image personnalisée contenant des modules ESXi et NSX, associez le profil d'image personnalisée.

À ce stade de la procédure, l'image personnalisée est uniquement associée aux hôtes de référence et cibles, mais l'installation de NSX ne se produit pas.

Important Effectuez cette procédure d'association de l'image personnalisée sur les hôtes de référence et cibles.

Conditions préalables

Procédure

- 1 Sur l'hôte ESXi, accédez à **Menu > Déploiement automatique > Hôtes déployés**.
- 2 Pour associer le profil d'image personnalisée à un hôte, sélectionnez l'image personnalisée.
- 3 Cliquez sur **Modifier l'association de profil d'image**.
- 4 Dans l'assistant Modifier l'association de profil d'image, cliquez sur **Parcourir**, puis sélectionnez le dépôt personnalisé et le profil d'image personnalisée.
- 5 Activez **Ignorer la vérification de la signature des profils d'image**.

6 Cliquez sur **OK**.

Dépôts de logiciels	Règles de déploiement	Hôtes déployés	Hôtes découverts	Bundles de scripts	Configurer
<p>① Le profil d'image, le profil d'hôte et l'emplacement associé aux hôtes par Auto Deploy sont répertoriés ci-dessous. Les associations peuvent être différentes de l'état réel de l'hôte.</p> <p>VÉRIFIER LA CONFORMITÉ DES ASSOCIATIONS D'HÔTES CORRIGER LES ASSOCIATIONS D'HÔTES MODIFIER L'ASSOCIATION DE PROFILS D'IMAGE</p>					
<input type="checkbox"/>	Hôte	Profil d'image associé	Profil d'hôte associé	Emplacement associé	Bundle de scripts associé
<input type="checkbox"/>	10.144.139.147	CustomDepot(ESXi and NSX)		1-datacenter-1964	
<input type="checkbox"/>	10.144.137.225	CustomDepot(ESXi and NSX)		Statless-Cluster	

Résultats

Étape suivante

Définissez la configuration réseau sur l'hôte de référence. Reportez-vous à la section [Définir la configuration réseau sur l'hôte de référence](#).





Définir la configuration réseau sur l'hôte de référence

Sur l'hôte de référence, un commutateur standard avec un adaptateur VMkernel est créé pour définir la configuration réseau sur ESXi.

Cette configuration réseau est capturée dans le profil d'hôte extrait de l'hôte de référence. Lors d'un déploiement sans état, le profil d'hôte réplique ce paramètre de configuration réseau sur chaque hôte cible.

Procédure

- 1 Sur l'hôte ESXi, configurez un commutateur vSphere standard (VSS) ou un commutateur virtuel distribué (DVS) en ajoutant un adaptateur VMkernel.
- 2 Vérifiez que le commutateur VSS/DVS récemment ajouté s'affiche sur la page des adaptateurs VMkernel.

Résumé	Surveiller	Configurer	Autorisations	VM	Banques de données	Réseaux
<h3>Adaptateurs VMkernel</h3> <p>  Ajouter une mise en réseau...  Actualiser  Modifier...  Supprimer </p>						
Périphérique	Étiquette réseau	Commutateur	Adresse IP	Pile TCP/IP	vH	
vmk0	Management N...	vSwitch0	10.192.193.193	Par défaut	D	
vmk1	VMkernel	vSwitch2	192.163.242.185	Par défaut	D	

Étape suivante

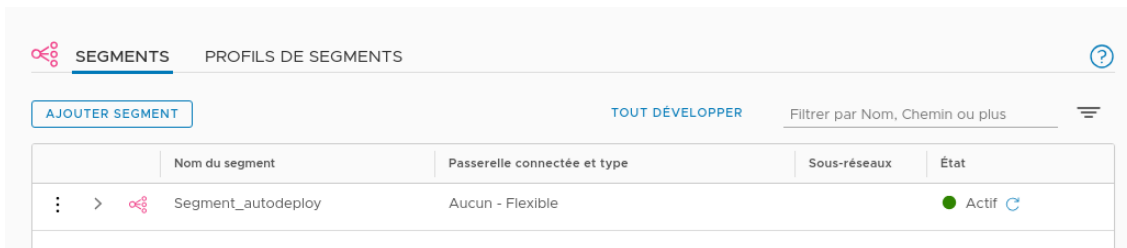
Configurez l'hôte de référence en tant que nœud de transport dans NSX-T. Reportez-vous à la section [Configurer l'hôte de référence en tant que nœud de transport dans NSX-T](#).

Configurer l'hôte de référence en tant que nœud de transport dans NSX-T

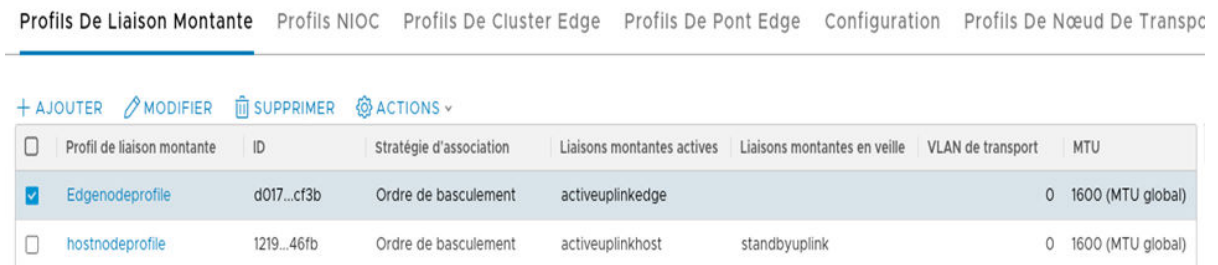
Une fois que l'hôte de référence est associé au profil d'image personnalisée et configuré avec un commutateur VSS, configurez l'hôte de référence en tant que nœud de transport dans NSX-T.

Procédure

- 1 À partir d'un navigateur, connectez-vous à NSX-T sur `https://<NSXManager_IPaddress>`.
- 2 Pour localiser l'hôte de référence, accédez à **Système -> Nœuds -> Nœuds de transport hôte**.
- 3 Créez une zone de transport VLAN pour définir l'étendue du réseau virtuel. L'étendue est définie en attachant des commutateurs N-VDS à la zone de transport. En fonction de cette pièce jointe, N-VDS peut accéder aux segments définis dans la zone de transport. Reportez-vous à la section [Créer une zone de transport](#).
- 4 Créez un segment VLAN sur la zone de transport. Le segment créé s'affiche sous la forme d'un commutateur logique.
 - a Accédez à **Mise en réseau -> Segments**.
 - b Sélectionnez la zone de transport à attacher au segment.
 - c Entrez l'ID VLAN.
 - d Cliquez sur **Enregistrer**.



- 5 Créez un profil de liaison montante pour l'hôte de référence, qui définit la manière dont le N-VDS se connecte au réseau physique. Reportez-vous à la section [Créer un profil de liaison montante](#).



- 6 Configurez l'hôte de référence en tant que nœud de transport. Reportez-vous à la section [Configurer un nœud de transport hôte géré](#).
 - a Sur la page Nœud de transport hôte, sélectionnez l'hôte de référence.
 - b Cliquez sur Configurer NSX et sélectionnez la zone de transport, le N-VDS et le profil de liaison montante précédemment créés.

- 7 Dans la section Mappages réseau à installer, cliquez sur **Ajouter un mappage** pour ajouter le VMkernel au mappage Segment/commutateur logique.

Mappages de réseau pour l'installation



La connectivité de l'hôte peut être perdue lorsque vmnic0 et vmk0 sont migrés.

La modification du commutateur logique pour l'hôte avec état (autonome ou en cluster) ne sera pas affectée et l'opération échouera.

[+ AJOUTER](#) [SUPPRIMER](#)

<input checked="" type="checkbox"/> Adaptateur VMkernel *	Segment VLAN/Commutateur logique *
<input checked="" type="checkbox"/> vmk0	segment-autodeploy

- 8 Cliquez sur **Terminer** pour commencer l'installation de NSX-T sur l'hôte de référence.

Lors de l'installation, les adaptateurs VMkernel et les cartes réseau physiques sont migrés d'un commutateur VSS ou DVS vers un commutateur N-VDS. Après l'installation, l'état de configuration de l'hôte de référence affiche Réussite.

Note L'hôte de référence est répertorié sous Autres hôtes.

Nœuds De Transport Hôtes										
Géré par vc										
CONFIGURER NSX SUPPRIMER NSX ACTIONS										
Nœud	ID	Adresses IP	Type de systèm	Configuration d	État de configur	État du nœud	Tunnels	Zones de transp	Version de NSX	N-VDS
Other Hosts (2)	ID moR...					1 hôte dégrad...				
10.192.193.193	42ea...8...	10.192.193.1...	ESXi 6.7.0	Configuré	Réussite	Dégradé @	Non dis...	tz	2.5.0.0.0.14...	1
hostnode	6d4c...f...	10.160.169.8...	ESXi 6.7.0	Configuré	Réussite	Actif @	↑ 1	tz	2.5.0.0.0.14...	1

- 9 Dans vCenter Server, vérifiez que les cartes réseau physiques et les adaptateurs VMkernel sur le commutateur VSS sont migrés et connectés au commutateur N-VDS.

Adaptateurs VMkernel				
Ajouter une mise en réseau... Actualiser Modifier... Supprimer				
Périphérique	Étiquette réseau	Commutateur	Adresse IP	Pile TCP/IP
vmk0	Management Network	vSwitch0	10.160.169.87	Par défaut
vmk1	Segment_autodeploy	vds-1	169.254.171.95	Par défaut

Étape suivante

Extrayez et vérifiez le profil d'hôte. Reportez-vous à la section [Extraire et vérifier le profil d'hôte](#).

Extraire et vérifier le profil d'hôte

Après avoir extrait le profil d'hôte à partir de l'hôte de référence, vérifiez la configuration de NSX-T extraite dans le profil d'hôte. Il se compose de la configuration d' ESXi et de NSX-T qui est appliquée aux hôtes cibles.

Procédure

- 1 Pour extraire le profil d'hôte, [extrairez et configurez le profil d'hôte de l'hôte de référence](#).

2 Vérifiez la configuration de NSX dans le profil d'hôte extrait.

FAVORIS

TOUT

Q Filtrer

> Autre

> Configuration de stockage

> Configuration réseau

> Commutateur standard

> Groupe de ports de la machine virtuelle

> Groupe de ports de l'hôte

> Configuration de carte réseau physique

vSphere Distributed Switch

Carte réseau virtuelle hôte

> vNIC de l'hôte NSX :

> vNIC de l'hôte NSX : Segment_autodeploy

> Instance de pile réseau

Paramètres coredump réseau

> Paramètres de configuration avancés

> Paramètres système généraux

> Sécurité et services

vNIC de l'hôte NSX : Segment_autodeploy

Déterminer le LogicSwitch auquel cette NIC virtuelle doit être connectée

Choisir un LogicSwitch auquel se connecter

*Nom du LogicSwitch

Segment_autodeploy

Déterminer le moment de création de la NIC virtuelle dans LogicSwitch

Toujours créer l'objet

Propriétés de démarrage sans état pour la NIC virtuelle dans LogicSwitch

Paramètres de configuration de démarrage sans état (consultez la documentation avant d'apporter des modifications)

*VLAN (consultez la documentation avant d'apporter des modifications)	0
*Stratégie d'association (consultez la documentation avant d'apporter des modifications)	first uplink
Liaisons montantes actives utilisées (consultez la documentation avant d'apporter des modifications)	vmnic1
Liaisons montantes en veille utilisées (consultez la documentation avant d'apporter des modifications)	--
*Nom du OpaqueSwitch utilisé (consultez la documentation avant d'apporter des modifications)	vds-1

> Configuration réseau

> Commutateur standard

> Groupe de ports de la machine virtuelle

> Groupe de ports de l'hôte

> Configuration de carte réseau physique

vSphere Distributed Switch

Carte réseau virtuelle hôte

> vNIC de l'hôte NSX :

> vNIC de l'hôte NSX : Segment_autodeploy

> Instance de pile réseau

Paramètres coredump réseau

> Paramètres de configuration avancés

> Paramètres système généraux

> Sécurité et services

Déterminer comment l'adresse MAC pour vmknic doit être décidée

Inviter l'utilisateur à spécifier l'adresse MAC si aucune adresse par défaut n'est disponible.

Stratégie de nom de l'adaptateur réseau VMkernel

Nom d'interface attribué

Adaptateur réseau VMkernel

vmk1

Règle MTU

Assigner le MTU spécifié

*MTU

1500

Pile TCP/IP :

Instance de pile réseau à laquelle la carte vmknic est connectée.

*Nom

defaultTcpipStack

Résultats

Le profil d'hôte contient une configuration liée à ESXi et NSX, car l'hôte a été préparé pour les deux environnements.

Étape suivante

Vérifiez l'association du profil d'hôte avec un cluster sans état. Reportez-vous à la section [Vérifier l'association de profil d'hôte à un cluster sans état](#).

Vérifier l'association de profil d'hôte à un cluster sans état

Pour préparer le cluster sans état cible avec une configuration ESXi et NSX, associez le profil d'hôte extrait de l'hôte de référence au cluster sans état cible.

Sans le profil d'hôte associé au cluster sans état, les nouveaux nœuds qui rejoignent le cluster ne peuvent pas être déployés automatiquement avec les VIB ESXi et NSX.

Procédure

- 1 Attachez un profil d'hôte à un cluster sans état ou détachez-le de celui-ci. Reportez-vous à la section [Détacher des entités d'un profil d'hôte ou les y attacher](#).
- 2 Dans l'onglet Hôtes déployés, vérifiez que l'hôte sans état existant est associé à l'image appropriée et au profil d'hôte.
- 3 Si l'association de profil d'hôte est manquante, sélectionnez l'hôte cible et cliquez sur Corriger les associations d'hôtes pour forcer la mise à jour de l'image et du profil d'hôte vers l'hôte cible.

Dépôts de logiciels	Règles de déploiement	Hôtes déployés	Hôtes découverts	Bundles de scripts	Configurer
<p>① Le profil d'image, le profil d'hôte et l'emplacement associé aux hôtes par Auto Deploy sont répertoriés ci-dessous. Les associations peuvent être différentes de l'état réel de l'hôte.</p> <p>VÉRIFIER LA CONFORMITÉ DES ASSOCIATIONS D'HÔTES CORRIGER LES ASSOCIATIONS D'HÔTES MODIFIER L'ASSOCIATION DE PROFILS D'IMAGE</p>					
<input type="checkbox"/>	Hôte	Profil d'image associé	Profil d'hôte associé	Emplacement associé	Bundle de scripts associé
<input type="checkbox"/>	10.144.139.147	CustomDepot(ESXi and NSX)		1-datacenter-1964	
<input type="checkbox"/>	10.144.137.225	CustomDepot(ESXi and NSX)	Host Profile_ReferenceHost	Statless-Cluster	

Étape suivante

Mettez à jour la personnalisation de l'hôte. Reportez-vous à la section [Mettre à jour la personnalisation de l'hôte](#).

Mettre à jour la personnalisation de l'hôte

Une fois le profil d'hôte attaché au cluster cible, des entrées personnalisées supplémentaires peuvent être requises sur l'hôte pour déployer automatiquement les modules ESXi et NSX-T sur celui-ci.

Procédure

- 1 Après l'attachement du profil d'hôte au cluster cible, si les hôtes ne sont pas mis à jour avec des valeurs personnalisées, le système affiche le message suivant.

Host Profile


ACTIONS

Résumé

Surveiller

Configurer

Hôtes



Nom :

Description :

Créé le :

Dernière modification :

Version :

Host Profile

7 nov. 2019 14:36

7 nov. 2019 14:36

6.7.0

⚠ L'hôte 10.160.183.211 nécessite une personnalisation supplémentaire.

⚠ L'hôte 10.160.170.243 nécessite une personnalisation supplémentaire.

- 2 Pour mettre à jour les personnalisations de l'hôte, accédez au profil d'hôte, cliquez sur **Actions -> Modifier les personnalisations de l'hôte**.

- 3 Pour les versions d' ESXi 67ep6, 67ep7 et 67u2, entrez le mot de passe de l'utilisateur MUX.

Customize hosts

Enter host customizations.

IMPORT HOST CUSTOMIZATIONS ⓘ

Required	Property Name	Path	Value
No	MAC Address	Networking configu...	02:00:0c:23:e9:9a
Yes	Adapter MA...	Storage configurati...	02:00:0c:23:e9:9a
Yes	Activate	Storage configurati...	false
Yes	Password	Security and	Security and Services > Security Settings > Security > User Configuration > mux_user > Pass

- 4 Vérifiez que tous les champs requis sont mis à jour avec les valeurs appropriées.

Étape suivante

Déclenchez le déploiement automatique sur les hôtes cibles. Reportez-vous à la section [Déclencher le déploiement automatique sur les hôtes cibles](#).

Déclencher le déploiement automatique sur les hôtes cibles

Lorsqu'un nouveau nœud est ajouté au cluster, il doit être redémarré manuellement pour que les VIB ESXi et NSX-T soient configurés.

Note S'applique uniquement aux hôtes sans état.

Il existe deux façons de préparer les hôtes afin de déclencher le déploiement automatique des VIB ESXi et NSX-T à configurer.

- Redémarrez les hôtes avant d'appliquer TNP au cluster sans état.
- Redémarrez les hôtes après avoir appliqué TNP au cluster sans état.

Si vous souhaitez migrer des adaptateurs VMkernel lors de l'installation de NSX-T sur les hôtes, reportez-vous aux sections suivantes :

- [Scénarios lorsque l'hôte sans état se trouve dans le cluster cible](#)
- [Scénarios lorsque l'hôte sans état se trouve à l'extérieur du cluster cible](#)

Étape suivante

Redémarrez les hôtes avant d'appliquer TNP au cluster sans état. Reportez-vous à la section [Redémarrer les hôtes avant l'application de TNP](#).

Redémarrer les hôtes avant l'application de TNP

S'applique uniquement aux hôtes sans état. Dans ce scénario, le profil de nœud de transport n'est pas appliqué au cluster sans état, ce qui signifie que NSX-T n'est pas installé et configuré sur l'hôte cible.

Procédure

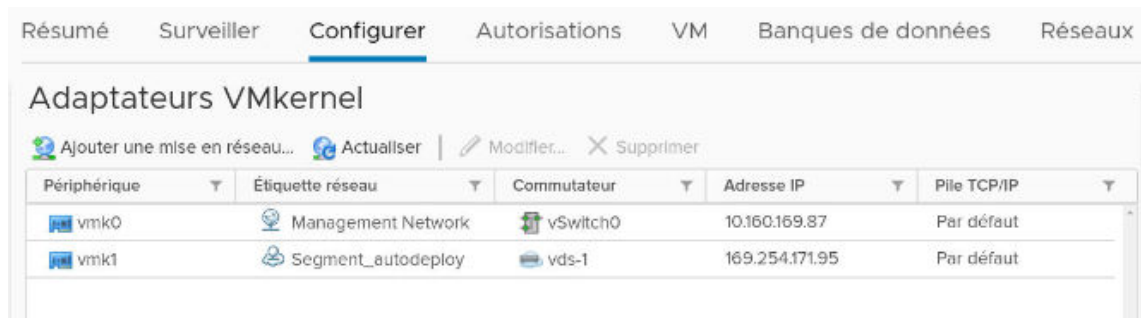
1 Redémarrez les hôtes.

L'hôte cible commence par l'image ESXi. Après le démarrage, l'hôte cible reste en mode de maintenance jusqu'à ce que le profil TNP soit appliqué à l'hôte cible et que l'installation de NSX-T soit terminée. Les profils sont appliqués sur les hôtes dans l'ordre suivant :

Les profils sont appliqués sur les hôtes dans l'ordre suivant.

- Le profil d'image est appliqué à l'hôte.
- La configuration du profil d'hôte est appliquée à l'hôte.
- La configuration de NSX-T est appliquée à l'hôte.

2 Sur l'hôte ESXi, l'adaptateur VMkernel est attaché à un segment temporaire nommé <N-LogicalSegment>, car l'hôte n'est pas encore un nœud de transport. Après l'installation de NSX-T, le commutateur temporaire est remplacé par le commutateur N-VDS réel et le segment logique.



Périphérique	Étiquette réseau	Commutateur	Adresse IP	Pile TCP/IP
vmk0	Management Network	vSwitch0	10.160.169.87	Par défaut
vmk1	Segment_autodeploy	vds-1	169.254.171.95	Par défaut

Les VIB ESXi sont appliqués à tous les hôtes redémarrés. Un commutateur NSX temporaire dans un hôte ESXi. Lorsque TNP est appliqué aux hôtes, le commutateur temporaire est remplacé par le commutateur NSX-T réel.

Étape suivante

Appliquez TNP au cluster sans état. Reportez-vous à la section [Appliquer TNP sur un cluster sans état](#).

Appliquer TNP sur un cluster sans état

La configuration et l'installation de NSX-T se produisent uniquement sur les hôtes cibles lorsque TNP est appliqué au cluster.

Procédure

- 1 Notez les paramètres extraits du profil d'hôte à partir de l'hôte de référence. Les entités correspondantes dans le profil TNP doivent avoir la même valeur. Par exemple, le nom du N-VDS utilisé dans le profil d'hôte et TNP doit être le même.

Pour plus d'informations sur les paramètres de profil d'hôte extraits, reportez-vous à la section [Extraire et vérifier le profil d'hôte](#).

- 2 Ajoutez un TNP. Reportez-vous à la section [Ajouter un profil de nœud de transport](#).
- 3 Assurez-vous que les valeurs des paramètres suivants sont les mêmes sur le nouveau profil TNP et le profil d'hôte existant.
 - Nom du N-VDS : assurez-vous que le nom du N-VDS référencé dans le profil d'hôte et TNP est le même.
 - Profil de liaison montante : assurez-vous que le profil de liaison montante référencé dans le profil d'hôte et TNP est le même.
 - PNIC : lors du mappage d'une carte réseau physique à un profil de liaison montante, vérifiez d'abord la carte réseau utilisée dans le profil d'hôte et mappez-la au profil de liaison montante.
 - Mappage réseau pour l'installation : lors du mappage du réseau pendant l'installation, vérifiez d'abord le mappage VMkernel vers le segment sur le profil d'hôte et ajoutez le même mappage dans TNP.
 - Mappage réseau pour la désinstallation : lors du mappage du réseau lors de la désinstallation, vérifiez d'abord le mappage VMkernel vers le commutateur VSS/DVS sur le profil d'hôte et ajoutez le même mappage dans TNP.

- 4 Ajoutez un TNP en entrant tous les champs requis. Reportez-vous à la section [Ajouter un profil de nœud de transport](#).

Assurez-vous que les valeurs des paramètres suivants sont les mêmes sur le nouveau profil TNP et le profil d'hôte existant.

- Zone de transport : assurez-vous que la zone de transport référencée dans le profil d'hôte et TNP est la même.
- Nom du N-VDS : assurez-vous que le nom du N-VDS référencé dans le profil d'hôte et TNP est le même.
- Profil de liaison montante : assurez-vous que le profil de liaison montante référencé dans le profil d'hôte et TNP est le même.
- PNIC : lors du mappage d'une carte réseau physique à un profil de liaison montante, vérifiez d'abord la carte réseau utilisée dans le profil d'hôte et mappez-la au profil de liaison montante.

- Mappage réseau pour l'installation : lors du mappage du réseau pendant l'installation, vérifiez d'abord le mappage VMkernel vers le commutateur logique sur le profil d'hôte et ajoutez le même mappage dans TNP.
- Mappage réseau pour la désinstallation : lors du mappage du réseau lors de la désinstallation, vérifiez d'abord le mappage VMkernel vers le commutateur VSS/DVS sur le profil d'hôte et ajoutez le même mappage dans TNP.

Nom du N-VDS *	vds-tzvian	
Zones de transport associées	tz-33	
Profil NIOC *	nsx-default-nioc-hostswitch-profile	
	OU créer un profil NIOC	
Profil de liaison montante *	nsx-default-uplink-hostswitch-profile	
	OU créer un profil de liaison montante	
Profil LLDP *	LLDP [Send Packet Enabled]	
Attribution IP *		
Cartes réseau physiques	vmnic1	uplink-1
	Ajouter une PNIC	
Migration de carte réseau physique uniquement	<input type="checkbox"/> Non	
Activer cette option si aucun VMK n'existe sur la carte réseau physique sélectionnée pour la migration		
Mappages de réseau pour l'installation	1 mappage	
Mappages de réseau pour la désinstallation	Ajouter un mappage	

Après l'application de TNP sur les nœuds cibles, si la configuration de TNP ne correspond pas à la configuration du profil d'hôte, le nœud peut ne pas apparaître en raison d'erreurs de conformité.

- 5 Vérifiez que le profil TNP a bien été créé.

- 6 Appliquez le profil TNP au cluster cible et cliquez sur **Enregistrer**.

Configurer NSX

NSX sera installé sur le cluster sélectionné avec la configuration de déploiement définie dans le profil du nœud de transport

Sélectionner le profil de déploiement TNP_StatelessCluster

[Créer un profil de nœud de transport](#)

ANNULER ENREGISTRER

- 7 Vérifiez que le profil TNP est correctement appliqué au cluster cible. Cela signifie que NSX est correctement configuré sur tous les nœuds du cluster.
- 8 Dans vSphere, vérifiez que les cartes réseau physiques ou les adaptateurs VMkernel sont attachés au commutateur N-VDS.

Adaptateurs VMkernel

[Ajouter une mise en réseau...](#) [Actualiser](#) | [Modifier...](#) [Supprimer](#)

Périphérique	Étiquette réseau	Commutateur	Adresse IP	Pile TCP/IP
vmk0	Management Network	vSwitch0	10.160.169.87	Par défaut
vmk1	Segment_autodeploy	vds-1	169.254.171.95	Par défaut

- 9 Dans NSX, vérifiez que l'hôte ESXi est correctement configuré en tant que nœud de transport.

Étape suivante

Vous pouvez également redémarrer un hôte cible après avoir appliqué TNP au cluster. Reportez-vous à la section [Redémarrer les hôtes après l'application de TNP](#).

Redémarrer les hôtes après l'application de TNP

S'applique uniquement aux hôtes sans état. Lorsqu'un nouveau nœud est ajouté au cluster, redémarrez manuellement le nœud pour que les modules ESXi et NSX-T soient configurés sur celui-ci.

Procédure

- 1 Appliquez TNP au cluster sans état qui est déjà préparé avec le profil d'hôte. Reportez-vous à la section [Créer et appliquer TNP sur un cluster sans état](#).
- 2 Redémarrez les hôtes.

Lorsque vous redémarrez un nouveau nœud rejoignant le cluster après l'application du profil TNP au cluster sans état, ce nœud est automatiquement configuré avec NSX-T sur l'hôte.

Étape suivante

Assurez-vous de redémarrer tous les nouveaux nœuds rejoignant le cluster afin de déployer et de configurer automatiquement ESXi et NSX-T sur le nœud redémarré.

Pour résoudre les problèmes liés au profil d'hôte et au profil de nœud de transport lors de la configuration du déploiement automatique, reportez-vous à la section [Dépanner le profil d'hôte et le profil de nœud de transport](#).

Scénarios lorsque l'hôte sans état se trouve dans le cluster cible

Cette section traite des cas d'utilisation lorsqu'un hôte sans état existe dans le cluster cible.

Important Sur un hôte cible sans état :

- La migration de l'adaptateur vmk0 de VSS/DVS vers N-VDS n'est pas prise en charge sur NSX-T 2.4 et NSX-T 2.4.1.
 - La migration de l'adaptateur vmk0 de VSS/DVS vers N-VDS est prise en charge sur NSX-T 2.5.
-

Hôte cible	Configuration de l'hôte de référence	Étapes du déploiement automatique des hôtes cibles
L'hôte cible dispose d'un adaptateur vmkO configuré.	Le profil d'hôte extrait de l'hôte de référence dispose de l'adaptateur vmkO configuré sur un commutateur N-VDS. Dans NSX-T, TNP ne dispose que du mappage de migration vmkO configuré.	<ol style="list-style-type: none"> 1 Attachez le profil d'hôte à l'hôte cible. L'adaptateur vmkO est attaché à un vSwitch. 2 Mettez à jour les personnalisations de l'hôte, si nécessaire. 3 Redémarrez l'hôte. Le profil d'hôte est appliqué à l'hôte. vmkO est attaché à un commutateur temporaire. 4 Appliquez TNP. L'adaptateur vmkO migre vers N-VDS. <p>L'hôte cible est correctement déployé avec les VIB ESXi et NSX-T.</p>
L'hôte cible dispose d'un adaptateur vmkO configuré.	Le profil d'hôte extrait de l'hôte de référence dispose de vmkO sur vSwitch et de vmk1 sur un commutateur N-VDS. Dans NSX-T, TNP n'a que le mappage de migration vmk1 configuré.	<ol style="list-style-type: none"> 1 Attachez le profil d'hôte à l'hôte cible. L'adaptateur vmkO est attaché à un vSwitch, mais vmk1 n'est pas réalisé sur un commutateur. 2 Mettez à jour les personnalisations de l'hôte, si nécessaire. 3 Redémarrez l'hôte. vmkO est attaché à un vSwitch et vmk1 est attaché à un commutateur NSX temporaire. 4 Appliquez TNP. L'adaptateur vmk1 migre vers N-VDS. 5 (Facultatif) Si l'hôte reste non conforme au profil d'hôte, redémarrez-le pour le mettre en conformité. <p>L'hôte cible est correctement déployé avec les VIB ESXi et NSX-T.</p>
L'hôte cible dispose d'un adaptateur vmkO configuré.	Le profil d'hôte extrait de l'hôte de référence dispose de vmkO configuré sur un vSwitch et de vmk1 configuré sur un commutateur N-VDS. Dans NSX-T, TNP dispose de mappages de migration vmkO et vmk1 configurés.	<ol style="list-style-type: none"> 1 Attachez le profil d'hôte à l'hôte cible. L'adaptateur vmkO est attaché à un vSwitch, mais vmk1 n'est pas réalisé sur un commutateur. 2 Mettez à jour les personnalisations de l'hôte, si nécessaire. 3 Redémarrez l'hôte. L'adaptateur vmkO est attaché à un vSwitch, alors que vmk1 est attaché à un commutateur NSX temporaire. 4 Appliquez TNP. 5 (Facultatif) Si l'hôte reste non conforme au profil d'hôte, redémarrez-le pour le mettre en conformité. <p>L'hôte cible est correctement déployé avec les VIB ESXi et NSX-T.</p>

Hôte cible	Configuration de l'hôte de référence	Étapes du déploiement automatique des hôtes cibles
Les adaptateurs vmk0 et vmk1 sont configurés sur l'hôte cible.	Le profil d'hôte extrait de l'hôte de référence dispose de vmk0 sur le vSwitch et de vmk1 configuré sur un commutateur N-VDS. Dans NSX-T, TNP a un mappage de migration vmk1 configuré.	<ol style="list-style-type: none"> 1 Attachez le profil d'hôte à l'hôte cible. Les adaptateurs vmk0 et vmk1 sont attachés à un vSwitch. 2 Mettez à jour les personnalisations de l'hôte, si nécessaire. 3 Redémarrez l'hôte. 4 Appliquez TNP. L'adaptateur vmk0 est attaché à un vSwitch, alors que vmk1 est attaché à un commutateur N-VDS. 5 (Facultatif) Si l'hôte reste non conforme au profil d'hôte, redémarrez-le pour le mettre en conformité. <p>L'hôte cible est correctement déployé avec les VIB ESXi et NSX-T.</p>
Les adaptateurs vmk0 et vmk1 sont configurés sur l'hôte cible.	Le profil d'hôte extrait de l'hôte de référence dispose de vmk0 et de vmk1 configurés sur un commutateur N-VDS. Dans NSX-T, TNP dispose de mappages de migration vmk0 et vmk1 configurés.	<ol style="list-style-type: none"> 1 Attachez le profil d'hôte à l'hôte cible. Les adaptateurs vmk0 et vmk1 sont attachés à un vSwitch. 2 Mettez à jour les personnalisations de l'hôte, si nécessaire. 3 Redémarrez l'hôte. 4 Appliquez TNP. Les adaptateurs vmk0 et vmk1 sont migrés vers un commutateur N-VDS. <p>L'hôte cible est correctement déployé avec les VIB ESXi et NSX-T.</p>

Scénarios lorsque l'hôte sans état se trouve à l'extérieur du cluster cible

Cette section traite des cas d'utilisation lorsqu'un hôte sans état existe en dehors du cluster cible.

Important Sur les hôtes sans état :

- La migration de l'adaptateur vmk0 de VSS/DVS vers N-VDS n'est pas prise en charge sur NSX-T 2.4 et NSX-T 2.4.1.
- La migration de l'adaptateur vmk0 de VSS/DVS vers N-VDS est prise en charge sur NSX-T 2.5.

État de l'hôte cible	Configuration de l'hôte de référence	Étapes du déploiement automatique des hôtes cibles
<p>L'hôte est dans l'état hors tension (premier démarrage). Il est ensuite ajouté au cluster.</p> <p>La règle de déploiement automatique par défaut est configurée pour le cluster cible et associée au profil d'hôte.</p> <p>Le TNP est appliqué au cluster.</p>	<p>Le profil d'hôte extrait de l'hôte de référence dispose de l'adaptateur VMkernel 0 (vmk0) sur un vSwitch et de l'adaptateur VMkernel 1 (vmk1) configuré sur un commutateur N-VDS.</p> <p>Dans NSX-T, TNP n'a que le mappage de migration vmk1 configuré.</p>	<p>1 Mettez l'hôte sous tension.</p> <p>Après la mise sous tension de l'hôte.</p> <ul style="list-style-type: none"> ■ L'hôte est ajouté au cluster. ■ Le profil d'hôte est appliqué à l'hôte cible. ■ L'adaptateur vmk0 se trouve sur un vSwitch, tandis que l'adaptateur vmk1 est sur un commutateur temporaire. ■ TNP est déclenché. ■ Une fois TNP appliqué au cluster, l'adaptateur vmk0 se trouve sur un vSwitch et vmk1 est migré vers le commutateur N-VDS. <p>2 (Facultatif) Si l'hôte reste non conforme au profil d'hôte, redémarrez-le pour le mettre en conformité.</p> <p>L'hôte est correctement déployé avec les VIB ESXi et NSX-T.</p>
<p>L'hôte est dans l'état hors tension (premier démarrage). Il est ensuite ajouté au cluster.</p> <p>La règle de déploiement automatique par défaut est configurée pour le cluster cible et associée au profil d'hôte.</p> <p>Le TNP est appliqué au cluster.</p>	<p>Le profil d'hôte extrait de l'hôte de référence dispose de l'adaptateur VMkernel 0 (vmk0) et de l'adaptateur VMkernel 1 (vmk1) configurés sur un commutateur N-VDS.</p> <p>Dans NSX-T, TNP dispose de la migration vmk0 et vmk1 configurée.</p>	<p>1 Mettez l'hôte sous tension.</p> <p>Après la mise sous tension de l'hôte.</p> <ul style="list-style-type: none"> ■ L'hôte est ajouté au cluster. ■ Le profil d'hôte est appliqué à l'hôte cible. ■ Les adaptateurs vmk0 et vmk1 se trouvent sur un commutateur temporaire. ■ TNP est déclenché. ■ Une fois TNP appliqué au cluster, les adaptateurs vmk0 et vmk1 sont migrés vers le commutateur N-VDS. <p>L'hôte est correctement déployé avec les VIB ESXi et NSX-T.</p>

État de l'hôte cible	Configuration de l'hôte de référence	Étapes du déploiement automatique des hôtes cibles
<p>L'hôte est dans l'état sous tension. Il est ensuite ajouté au cluster.</p> <p>La règle de déploiement automatique par défaut est configurée pour le cluster cible et associée au profil d'hôte.</p> <p>Un adaptateur vmk0 est configuré sur l'hôte cible uniquement.</p>	<p>Le profil d'hôte extrait de l'hôte de référence dispose de l'adaptateur VMkernel 0 (vmk0) sur un vSwitch et de l'adaptateur VMkernel 1 (vmk1) configuré sur un commutateur N-VDS.</p> <p>Dans NSX-T, TNP a un mappage de migration vmk1 configuré.</p>	<ol style="list-style-type: none"> Déplacez l'hôte pour qu'il fasse partie du cluster. Redémarrez l'hôte. <p>Après le redémarrage de l'hôte, le profil d'hôte est appliqué à l'hôte cible.</p> <ul style="list-style-type: none"> ■ L'adaptateur vmk0 est attaché à un vSwitch, alors que l'adaptateur vmk1 est attaché à un commutateur NSX temporaire. ■ TNP est déclenché. ■ vmk1 est migré vers le commutateur N-VDS. <ol style="list-style-type: none"> (Facultatif) Si l'hôte reste non conforme au profil d'hôte, redémarrez-le pour le mettre en conformité. <p>L'hôte est correctement déployé avec les VIB ESXi et NSX-T.</p>
<p>L'hôte est dans l'état sous tension. Il est ensuite ajouté au cluster.</p> <p>La règle de déploiement automatique par défaut est configurée pour le cluster cible et associée au profil d'hôte.</p> <p>Un adaptateur vmk0 est configuré sur l'hôte cible uniquement.</p>	<p>Le profil d'hôte extrait de l'hôte de référence dispose de l'adaptateur VMkernel 0 (vmk0) et de l'adaptateur VMkernel 1 (vmk1) configurés sur N-VDS.</p> <p>Dans NSX-T, TNP dispose de la migration vmk0 et vmk1 configurée.</p>	<ol style="list-style-type: none"> Déplacez l'hôte pour qu'il fasse partie du cluster. Redémarrez l'hôte. <p>Après le redémarrage de l'hôte, le profil d'hôte est appliqué à l'hôte cible.</p> <ul style="list-style-type: none"> ■ Les adaptateurs vmk0 et vmk1 sont attachés à un commutateur NSX temporaire. ■ TNP est déclenché. ■ vmk0 et vmk1 sont attachés à un commutateur N-VDS. <p>L'hôte est correctement déployé avec les VIB ESXi et NSX-T.</p>

État de l'hôte cible	Configuration de l'hôte de référence	Étapes du déploiement automatique des hôtes cibles
<p>L'hôte est dans l'état sous tension. Il est ensuite ajouté au cluster.</p> <p>La règle de déploiement automatique par défaut est configurée pour le cluster cible et associée au profil d'hôte.</p> <p>L'hôte cible a un mappage réseau vmk0 et vmk1 configuré.</p>	<p>Le profil d'hôte extrait de l'hôte de référence dispose de l'adaptateur VMkernel 0 (vmk0) sur un vSwitch et de l'adaptateur VMkernel 1 (vmk1) configuré sur un commutateur N-VDS.</p> <p>Dans NSX-T, TNP a une migration vmk1 configurée.</p>	<ol style="list-style-type: none"> Déplacez l'hôte pour qu'il fasse partie du cluster. Redémarrez l'hôte. <p>Après le redémarrage de l'hôte, le profil d'hôte est appliqué à l'hôte cible.</p> <ul style="list-style-type: none"> ■ L'adaptateur vmk0 est attaché à un vSwitch, alors que l'adaptateur vmk1 est attaché à un commutateur NSX temporaire. ■ TNP est déclenché. ■ vmk1 est migré vers le commutateur N-VDS. <ol style="list-style-type: none"> (Facultatif) Si l'hôte reste non conforme au profil d'hôte, redémarrez-le pour le mettre en conformité. <p>L'hôte est correctement déployé avec les VIB ESXi et NSX-T.</p>
<p>L'hôte est dans l'état sous tension. Il est ensuite ajouté au cluster.</p> <p>La règle de déploiement automatique par défaut est configurée pour le cluster cible et associée au profil d'hôte.</p> <p>L'hôte a un mappage réseau vmk0 et vmk1 configuré.</p>	<p>Dans l'hôte de référence, le profil d'hôte dispose de l'adaptateur VMkernel 0 (vmk0) et de l'adaptateur VMkernel 1 (vmk1) configurés sur un commutateur N-VDS.</p> <p>Dans NSX-T, TNP dispose de la migration vmk0 et vmk1 configurée.</p>	<ol style="list-style-type: none"> Déplacez l'hôte pour qu'il fasse partie du cluster. Redémarrez l'hôte. <p>Après le redémarrage de l'hôte, le profil d'hôte est appliqué à l'hôte cible.</p> <ul style="list-style-type: none"> ■ Les adaptateurs vmk0 et vmk1 sont attachés à un commutateur NSX temporaire. ■ TNP est déclenché. ■ Les adaptateurs vmk0 et vmk1 sont migrés vers le commutateur N-VDS. <p>L'hôte est correctement déployé avec les VIB ESXi et NSX-T.</p>

Dépanner le profil d'hôte et le profil de nœud de transport

Résolvez les problèmes liés aux profils d'hôte et aux TNP lorsqu'ils sont utilisés pour déployer automatiquement les clusters sans état.

Scénario	Description
Le profil d'hôte n'est pas portable.	<p>Problème : aucune des instances de vCenter Server ne peut utiliser le profil d'hôte contenant la configuration de NSX-T.</p> <p>Solution : aucune.</p>
Moteur de règles de déploiement automatique	<p>Problème : le profil d'hôte ne peut pas être utilisé dans les règles de déploiement automatique pour déployer de nouveaux clusters. Si de nouveaux clusters sont déployés, les hôtes sont déployés avec une mise en réseau de base et restent en mode de maintenance.</p> <p>Solution : préparez chaque cluster à partir de l'interface utilisateur graphique de NSX-T. Reportez-vous à la section Appliquer TNP sur un cluster sans état.</p>
Recherche des erreurs de conformité.	<p>Problème : la correction du profil d'hôte ne parvient pas à corriger les erreurs de conformité liées à la configuration de NSX-T.</p> <ul style="list-style-type: none"> ■ Cartes réseau physiques différentes configurées sur le profil d'hôte et TNP. ■ Mappage entre les vNIC par rapport au mappage LS. Le profil d'hôte détecte une incompatibilité dans le commutateur logique au niveau du mappage vNIC avec le profil TNP. ■ Incompatibilité du VMkernel connecté à N-VDS sur le profil d'hôte et TNP. ■ Incompatibilité du commutateur opaque sur le profil d'hôte et TNP. <p>Solution : assurez-vous que la configuration de NSX-T correspond sur le profil d'hôte et TNP. Redémarrez l'hôte pour que les modifications de configuration prennent effet. L'hôte s'affiche.</p>
Correction	<p>Problème : s'il existe des erreurs de conformité spécifiques à NSX-T, la correction du profil d'hôte sur ce cluster est bloquée.</p> <p>Configuration incorrecte :</p> <ul style="list-style-type: none"> ■ Mappage entre les vNIC par rapport au mappage LS ■ Mappage des cartes réseau physiques <p>Solution : assurez-vous que la configuration de NSX-T correspond sur le profil d'hôte et TNP. Redémarrez l'hôte pour que les modifications de configuration prennent effet. L'hôte s'affiche.</p>
Attachement	<p>Problème : dans un cluster configuré avec NSX-T, le profil d'hôte ne peut pas être attaché au niveau de l'hôte.</p> <p>Solution : aucune.</p>
Détachement	<p>Problème : le détachement et l'attachement d'un nouveau profil d'hôte dans un cluster configuré avec NSX-T ne supprime pas la configuration de NSX-T. Même si le cluster est conforme à la nouvelle association du profil d'hôte, il dispose toujours de la configuration de NSX-T d'un profil précédent.</p> <p>Solution : aucune.</p>
Mise à jour	<p>Problème : si l'utilisateur a modifié la configuration de NSX-T dans le cluster, extrayez un nouveau profil d'hôte. Mettez à jour le profil d'hôte manuellement pour tous les paramètres qui ont été perdus.</p> <p>Solution : aucune.</p>

Scénario	Description
Configuration du nœud de transport au niveau de l'hôte	<p>Problème : une fois que le nœud de transport a été déployé automatiquement, il agit comme une entité individuelle. Toute mise à jour de ce nœud de transport peut ne pas correspondre au TNP.</p> <p>Solution : mettez à jour le cluster. Toute mise à jour d'un nœud de transport autonome ne peut pas conserver sa spécification de migration. La migration peut échouer à publier le redémarrage.</p>
Impossible d'appliquer le profil d'hôte, car la stratégie de mot de passe mux_user et le mot de passe n'ont pas été réinitialisés.	<p>Problème : survient uniquement sur les hôtes exécutant des versions antérieures à vSphere 6.7 U3. La correction de l'hôte et l'application du profil d'hôte sur les hôtes peuvent échouer sauf si le mot de passe mux_user est réinitialisé.</p> <p>Solution : sous Stratégies et profils, modifiez le profil d'hôte afin de modifier la stratégie de mot de passe mux_user, puis réinitialisez le mot de passe mux_user.</p>
La configuration PeerDNS n'est pas prise en charge sur l'adaptateur VMkernel sélectionné pour la migration vers le commutateur NVDS.	<p>Problème : si un adaptateur VMkernel sélectionné pour la migration vers NVDS est activé pour le DNS homologue, l'application du profil d'hôte échoue.</p> <p>Solution : modifiez le profil d'hôte extrait en désactivant le paramètre de DNS homologue sur l'adaptateur VMkernel qui doit être migré vers un commutateur NVDS. Vous pouvez également vous assurer ne pas migrer les adaptateurs VMkernel activés pour le DNS homologue vers un commutateur NVDS.</p>
Adresse DHCP de l'adresse de la carte réseau VMkernel non conservée	<p>Problème : si l'hôte de référence est avec état, tous les hôtes sans état utilisant le profil extrait de l'hôte de référence avec état ne peuvent pas conserver leur adresse MAC de gestion VMkernel dérivée du MAC démarré par PXE. Cela entraîne des problèmes d'adressage DHCP.</p> <p>Solution : modifiez le profil d'hôte extrait de l'hôte avec état et redéfinissez « Déterminer comment l'adresse MAC pour vmknic doit être décidée » en « Utiliser l'adresse MAC à partir de laquelle le système a été démarré par PXE ».</p>
L'échec de l'application du profil d'hôte dans vCenter peut entraîner des erreurs de configuration de NSX sur l'hôte.	<p>Problème : si l'application du profil d'hôte échoue dans vCenter, la configuration de NSX peut également échouer.</p> <p>Solution : dans vCenter, vérifiez que le profil d'hôte a bien été appliqué. Corriguez les erreurs et réessayez.</p>
Les LAG ne sont pas pris en charge sur les hôtes ESXi sans état.	<p>Problème : le profil de liaison montante configuré en tant que LAG dans NSX n'est pas pris en charge sur un hôte ESXi sans état géré par une instance de vCenter Server ou dans NSX.</p> <p>Solution : aucune.</p>

Serveurs avec état

Intégrez les profils d'hôte d'un hôte ESXi avec NSX-T sur des serveurs avec état.

Un hôte avec état est un hôte qui conserve toutes les configurations et les VIB installés, même après son redémarrage. Bien qu'un serveur de déploiement automatique soit nécessaire pour les hôtes sans état, car les fichiers de démarrage requis pour faire apparaître un hôte sans état sont stockés sur le serveur de déploiement automatique, un hôte avec état ne nécessite pas une infrastructure similaire. En effet, les fichiers de démarrage nécessaires pour faire apparaître un hôte avec état sont stockés sur son disque dur.

Dans cette procédure, l'hôte de référence se trouve en dehors du cluster avec état et des hôtes cibles dans le cluster. Un hôte cible peut se trouver dans un cluster ou un hôte autonome hors du cluster. Préparez un cluster en appliquant un profil d'hôte et un profil de nœud de transport (profil TN), afin que tous les nouveaux hôtes cibles rejoignant le cluster soient automatiquement préparés avec les VIB NSX-T. Configurez l'hôte cible en tant que nœud de transport. De même, pour un hôte autonome, appliquez le profil d'hôte et configurez NSX-T pour installer les VIB NSX-T. Une fois la configuration de NSX-T terminée, il devient un nœud de transport.

Note Les VIB NSX-T sont installés à partir du profil TN et les configurations de l'hôte ESXi sont appliquées par les profils d'hôte.

Lors de la configuration d'un hôte cible dans un nœud de transport, les adaptateurs VMkernel et les cartes réseau de VM ou les interfaces réseau physiques qui sont attachées au commutateur VSS ou VDS peuvent être migrés et connectés au commutateur distribué virtuel NSX-T, le commutateur N-VDS.

Versions NSX-T et ESXi prises en charge

Versions NSX-T et ESXi prises en charge sur les serveurs avec état.

Nom de la version	67ep6	67U2	67U3	67ep7	67U2C	6.5U3	6.5p03
NSX-T 2.4	Oui	Non	Non	Non	Non	Non	Oui
NSX-T 2.4.1	Oui	Oui	Non	Non	Non	Non	Oui
NSX-T 2.4.2	Oui	Oui	Non	Non	Non	Non	Oui
NSX-T 2.4.3	Oui	Oui	Non	Non	Non	Non	Oui
NSX-T 2.5	Oui	Oui	Oui	Oui	Oui	Oui	Oui
NSX-T 2.5.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Préparer un cluster cible avec état

Préparez un cluster cible avec état afin que tout nouvel hôte rejoignant le cluster soit automatiquement déployé avec les VIB ESXi et NSX-T.

Vous pouvez sélectionner un hôte dans le cluster ou hors de ce dernier comme hôte de référence. Vous devez créer un hôte de référence, car le profil d'hôte de l'hôte de référence est extrait et appliqué à un hôte cible. Dans cette procédure, à titre d'exemple, les instructions stipulent de migrer vmk0 (trafic de gestion) et vmk1 (trafic vMotion) vers un commutateur N-VDS.

Conditions préalables

Procédure

- 1 Sur l'hôte de référence, déployez une version de ESXi prise en charge.
 - a Dans vSphere, ajoutez l'adaptateur vmk1. vmk0 est déjà présent pour servir le trafic de gestion.
- 2 Configurez le nœud de référence en tant que nœud de transport.
 - a À l'aide de vSphere Web Client, avant de migrer vmk0 et vmk1, assurez-vous qu'un commutateur logique est créé dans NSX-T.
 - b (Facultatif) Dans l'interface utilisateur de NSX-T Manager, configurez NSX afin qu'au terme de l'installation de NSX-T, l'adaptateur vmk1 mappé à un commutateur logique soit migré vers le commutateur N-VDS.
 - c (Facultatif) Dans l'interface utilisateur de NSX-T Manager, configurez NSX-T afin qu'au terme de l'installation de NSX-T, l'adaptateur vmk0 mappé à un commutateur logique soit migré vers le commutateur N-VDS.

Note vmk0 et vmk1 peuvent se trouver sur différents commutateurs VSS ou DVS.

- d À l'aide de vSphere Web Client, assurez-vous que vmk0 et vmk1 sont connectés à un commutateur logique sur le commutateur N-VDS.
- 3 Extrayez le profil d'hôte de l'hôte de référence.
- 4 Dans votre environnement, il peut être nécessaire de migrer un certain nombre d'adaptateurs VMkernel vers le commutateur N-VDS. Cependant, avant de migrer les adaptateurs VMK de VSS/DVS vers un commutateur N-VDS, assurez-vous que les paramètres de configuration sur l'hôte cible correspondent à ceux de l'hôte de référence.
- 5 Sur un hôte cible qui est un hôte autonome :
 - a Attachez le profil d'hôte à l'hôte cible.
 - b Configurez manuellement NSX-T sur l'hôte. Lors de la configuration de l'hôte en tant que nœud de transport en raison du profil d'hôte sur l' ESXi, assurez-vous que les conditions ci-après sont réunies.
 - c L'hôte doit appartenir à la même zone de transport.
 - d L'adaptateur vmk1 doit être connecté au même commutateur logique que celui qui est utilisé par l'hôte de référence.
 - e L'hôte cible doit utiliser le même pool d'adresses IP que celui qui est utilisé par l'hôte de référence.
 - f Le profil de liaison montante, LLDP, NIOC, le mappage réseau pour l'installation, le N-VDS configuré sur l'hôte cible doivent être identiques à ceux qui sont configurés sur l'hôte de référence.

- g Ajoutez manuellement l'adaptateur VMkernel, vmk1 et vmnic1 afin qu'il soit migré du commutateur VSS/DVS vers le commutateur N-VDS. Reportez-vous aux scénarios de migration de vmk1.
 - h Ajoutez manuellement l'adaptateur de gestion, vmk0 et/ou vmnic0.
- 6** Sur un hôte cible appartenant à un cluster :
- a Attachez le profil d'hôte à l'hôte cible avec état.
 - b Créez et appliquez le profil TN sur le cluster.
 - c Pour configurer l'adaptateur vmk1 et la carte réseau vmnic1 à migrer, reportez-vous aux scénarios de migration de vmk1.
 - d Pour configurer l'adaptateur vmk0 et la carte réseau vmnic0 à migrer, reportez-vous aux scénarios de migration de vmk0.
 - e Appliquez le profil TN sur le cluster.

Étape suivante

Scénarios de migration des adaptateurs VMkernel avec et sans application des profils d'hôte à NSX-T.

Migration de VMkernel avec application du profil d'hôte

Dans le scénario illustré dans cette section, l'adaptateur VMkernel 1 (vmk1) est migré vers le commutateur N-VDS avec application du profil d'hôte dans NSX-T. L'adaptateur vmk1 prend en charge le trafic d'infrastructure pour vMotion, Fault Tolerance et d'autres services d'infrastructure.

Scénario	Erreur	Solution
Migration de vmk1 sur un hôte cible autonome en appliquant un profil d'hôte de référence.	<p>L'hôte cible n'est pas configuré en tant que nœud de transport. Étant donné que l'hôte cible ignore l'existence d'objets NSX-T, l'application de profil d'hôte échoue. La correction du profil d'hôte sur l'hôte cible échoue.</p> <pre>Error: Received SOAP response fault : generate HostConfigTask Spec..</pre>	<p>1 Avant d'appliquer le profil d'hôte de référence pour migrer vmk1 vers le commutateur logique sur l'hôte cible, configurez l'hôte cible en tant que nœud de transport, qui installe les VIB NSX-T, crée un commutateur N-VDS et migre l'adaptateur vmk1 du commutateur VSS vers le commutateur N-VDS.</p> <p>Lors de la configuration de l'hôte en tant que nœud de transport en raison du profil d'hôte sur le ESXi, assurez-vous que les conditions suivantes sont réunies :</p> <ul style="list-style-type: none"> ■ L'hôte doit appartenir à la même zone de transport. ■ L'adaptateur vmk1 doit être connecté au même commutateur logique que celui qui est utilisé par l'hôte de référence. ■ L'hôte cible doit utiliser le même pool d'adresses IP que celui qui est utilisé par l'hôte de référence. ■ Le profil de liaison montante, LLDP, NIOC, le mappage réseau pour l'installation, le N-VDS configuré sur l'hôte cible doivent être identiques à ceux qui sont configurés sur l'hôte de référence. <p>La correction du profil d'hôte réussit lorsque l'hôte cible est configuré avec le même nom de commutateur logique que celui qui est présent dans le profil d'hôte.</p>
Migration de vmk1 sur les hôtes cibles dans un cluster avec état.	<p>Avant d'appliquer le profil d'hôte à l'hôte cible, si vous préparez le cluster en appliquant le profil TN configuré avec vmk1 mappé au commutateur logique, la migration de vmk1 échoue.</p> <pre>Error: vmk1 missing on the host.</pre>	<p>1 Appliquez le profil d'hôte de référence à l'hôte cible qui a rejoint le cluster.</p> <p>2 Corrigez le profil d'hôte sur l'hôte cible pour créer l'adaptateur vmk1 sur l'hôte cible.</p>

Scénario	Erreur	Solution
		3 Appliquez à nouveau le profil TN au cluster pour migrer vmk1 vers le cluster cible.
Migration de vmk0 et de vmk1 sur un hôte autonome.	Lors de la configuration de NSX-T sur l'hôte autonome, si le champ Mappages de réseau pour l'installation ne spécifie pas les mappages de vmk0 ou vmk1, la migration échoue.	Lors de la configuration de NSX-T sur l'hôte cible, assurez-vous que le champ Mappages de réseau pour l'installation est spécifié avec vmk0 et vmk1 mappés sur le même commutateur logique du N-VDS.
Migration de vmk0 et de vmk1 sur un hôte de cluster.	Lors de l'application du profil TN à un cluster, si le champ Mappages de réseau pour l'installation ne spécifie pas les mappages de vmk0 ou vmk1, la migration échoue.	Appliquez le profil TN au cluster. Lors de la configuration du profil TN sur le cluster, assurez-vous que le champ Mappages de réseau pour l'installation est spécifié avec vmk0 et vmk1 mappés sur un commutateur logique du N-VDS.

Migration de VMkernel sans application du profil d'hôte

Dans le scénario illustré dans cette section, l'adaptateur VMkernel 0 (vmk0) est migré vers le commutateur N-VDS sans application du profil d'hôte dans NSX-T. L'adaptateur vmk0 prend en charge le trafic de gestion pour NSX-T.

Il n'est pas nécessaire d'appliquer un profil d'hôte à l'hôte cible, car vmk0 existe déjà sur celui-ci. L'adaptateur vmk0 prend en charge le trafic de gestion sur un hôte ESXi.

Scénario	Procédure	Résultat
Migration de vmk0 sur un hôte autonome.	Lors de la configuration de NSX-T sur l'hôte cible, assurez-vous que le champ Mappages de réseau pour l'installation est spécifié avec vmk0 mappé à un commutateur logique sur le N-VDS.	vmk0 est migré vers le commutateur logique sur l'hôte cible.
Migration de vmk0 sur un hôte de cluster.	Appliquez le profil TN au cluster. Lors de la configuration du profil TN sur le cluster, assurez-vous que le champ Mappages de réseau pour l'installation est spécifié avec vmk0 mappé à un commutateur logique sur le N-VDS.	vmk0 est migré vers le commutateur logique sur l'hôte cible.

Désinstallation de NSX-T Data Center d'un nœud de transport hôte

12

Les étapes de désinstallation de NSX-T Data Center d'un nœud de transport hôte varient selon le type d'hôte et de son mode de configuration.

- [Vérifier les mappages réseau de l'hôte pour la désinstallation](#)

Avant de désinstaller NSX-T Data Center d'un hôte ESXi, vérifiez que les mappages réseau appropriés sont configurés pour la désinstallation. Les mappages sont requis si l'hôte ESXi dispose d'interfaces VMkernel connectées à N-VDS.

- [Désinstaller NSX-T Data Center d'un cluster vSphere](#)

Si vous avez installé NSX-T Data Center sur un cluster vSphere à l'aide de profils de nœuds de transport, vous pouvez suivre ces instructions pour désinstaller NSX-T Data Center de tous les hôtes du cluster.

- [Désinstaller NSX-T Data Center d'un hôte dans un cluster vSphere](#)

Vous pouvez désinstaller NSX-T Data Center d'un seul hôte géré par vCenter Server. Les autres hôtes du cluster ne sont pas affectés.

- [Désinstaller NSX-T Data Center d'un hôte autonome](#)

Vous pouvez désinstaller NSX-T Data Center d'un hôte autonome. Les hôtes autonomes peuvent être ESXi ou KVM.

Vérifier les mappages réseau de l'hôte pour la désinstallation

Avant de désinstaller NSX-T Data Center d'un hôte ESXi, vérifiez que les mappages réseau appropriés sont configurés pour la désinstallation. Les mappages sont requis si l'hôte ESXi dispose d'interfaces VMkernel connectées à N-VDS.

Le mappage de désinstallation détermine l'emplacement de connexion des interfaces après la désinstallation. Il existe des mappages de désinstallation pour les interfaces physiques (vmnicX) et les interfaces VMkernel (vmkX). En cas de désinstallation, les interfaces VMkernel sont transférées depuis leurs connexions actuelles vers les groupes de ports spécifiés dans

le mappage de désinstallation. Si une interface physique est comprise dans le mappage de désinstallation, l'interface physique est connectée à l'instance de vSphere Distributed Switch ou de commutateur vSphere Standard appropriée en fonction du groupe de ports de destination des interfaces VMkernel.

Attention La désinstallation de NSX-T Data Center d'un hôte ESXi peut entraîner des perturbations si les interfaces physiques ou les interfaces VMkernel sont connectées à N-VDS. Si l'hôte ou le cluster fait partie d'autres applications, telles que vSAN, celles-ci peuvent être affectées par la désinstallation.




Vous pouvez configurer des mappages réseau à deux emplacements pour la désinstallation.




- Dans la configuration du nœud de transport, qui s'applique à cet hôte.
- Dans une configuration de profil de nœud de transport, qui peut ensuite être appliquée à un cluster.

Note Vous devez disposer d'un gestionnaire de calcul configuré pour appliquer un profil de nœud de transport à un cluster.

Si un gestionnaire de calcul est configuré, un hôte peut disposer d'une configuration de nœud de transport et d'une configuration de profil de nœud de transport. La dernière configuration appliquée est active. Vérifiez que les mappages réseau pour la désinstallation sont correctement configurés dans la configuration active.

Dans cet exemple, le profil de nœud de transport TNP-1 est appliqué au cluster cluster-1. L'hôte tn-1 affiche « Incompatibilité de configuration ». Ce message d'incompatibilité indique qu'une configuration différente a été appliquée à tn-1 après l'application du profil de nœud de transport. Le nœud de transport tn-2 utilise les mappages réseau du profil de nœud de transport, et le nœud de transport tn-1 utilise sa propre configuration.

 CONFIGURER NSX
  SUPPRIMER NSX
  ACTIONS ▼

<input type="checkbox"/>	Nœud	ID	Adresses	Type de s	Configuration de NSX
<input type="checkbox"/>	 New Cluster (2)	MoR...			 TNP-1
<input type="checkbox"/>	tn-1	926...	10....	ESXi ...	 Incompatibilité de configuration
<input type="checkbox"/>	tn-2	901f....	10....	ESXi ...	Configuré

Conditions préalables

- Vérifiez que les groupes de ports appropriés sont configurés pour être utilisés dans le mappage de désinstallation. Vous devez utiliser des groupes de ports éphémères vSphere Distributed Switch ou des groupes de ports de commutateur vSphere Standard.

- Configurez un gestionnaire de calcul si vous souhaitez utiliser un groupe de ports vSphere Distributed Switch dans les mappages de désinstallation d'un hôte ESXi autonome. Reportez-vous à la section [Ajouter un gestionnaire de calcul](#). Si aucun gestionnaire de calcul n'est configuré, vous devez utiliser un groupe de ports de commutateur vSphere Standard.

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Système > Infrastructure > Nœuds > Nœuds de transport hôtes**.
- 3 Pour chaque hôte à désinstaller, vérifiez que le mappage réseau pour la désinstallation inclut un groupe de ports pour chaque interface VMkernel qui se trouve sur N-VDS. Ajoutez les mappages manquants.

Important Le groupe de ports dans le mappage réseau pour la désinstallation doit être un groupe de ports éphémères vSphere Distributed Switch ou un groupe de ports de commutateur vSphere Standard.

- a Pour afficher les interfaces VMkernel, connectez-vous à vCenter Server, sélectionnez l'hôte, puis cliquez sur **Configurer > Adaptateurs VMkernel**.
- b Si la configuration du nœud de transport est la configuration active, sélectionnez l'hôte et cliquez sur **Modifier** (pour les hôtes autonomes) ou **Configurer NSX** (pour les hôtes gérés). Cliquez sur **Suivant**, puis cliquez sur **Mappages de réseau pour la désinstallation**. Affichez les mappages dans les onglets **Mappages de VMKNic** et **Mappages de carte réseau physique**.
- c Si le profil de nœud de transport est la configuration active, cliquez sur le nom du profil de nœud de transport pour le cluster dans la colonne **Configuration de NSX** et cliquez sur **Modifier**. Dans l'onglet **N-VDS**, cliquez sur **Mappages de réseau pour la désinstallation**. Affichez les mappages dans les onglets **Mappages de VMKNic** et **Mappages de carte réseau physique**.

Désinstaller NSX-T Data Center d'un cluster vSphere

Si vous avez installé NSX-T Data Center sur un cluster vSphere à l'aide de profils de nœuds de transport, vous pouvez suivre ces instructions pour désinstaller NSX-T Data Center de tous les hôtes du cluster.

Pour plus d'informations sur les profils de nœuds de transport, reportez-vous à la section [Ajouter un profil de nœud de transport](#).

Attention La désinstallation de NSX-T Data Center d'un hôte ESXi peut entraîner des perturbations si les interfaces physiques ou les interfaces VMkernel sont connectées à N-VDS. Si l'hôte ou le cluster fait partie d'autres applications, telles que vSAN, celles-ci peuvent être affectées par la désinstallation.

Si vous n'avez utilisé aucun profil de nœud de transport pour installer NSX-T Data Center, ou si vous souhaitez supprimer NSX-T Data Center d'un sous-ensemble d'hôtes dans le cluster, reportez-vous à la section [Désinstaller NSX-T Data Center d'un hôte dans un cluster vSphere](#).

Note La suppression d'un hôte d'un cluster ne désinstalle pas NSX-T Data Center. Suivez ces instructions pour désinstaller NSX-T Data Center d'un hôte dans un cluster : [Désinstaller NSX-T Data Center d'un hôte dans un cluster vSphere](#).

Conditions préalables

- Vérifiez que les mappages de désinstallation réseau sont configurés sur les hôtes que vous souhaitez désinstaller. Reportez-vous à la section [Vérifier les mappages réseau de l'hôte pour la désinstallation](#).
- Vérifiez que les hôtes que vous souhaitez désinstaller sont en mode de maintenance dans vSphere.

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Système > Infrastructure > Nœuds > Nœuds de transport hôtes**.
- 3 Dans le menu déroulant **Géré par**, sélectionnez vCenter Server.
- 4 Sélectionnez le cluster à désinstaller, puis cliquez sur **Supprimer NSX**.
- 5 Vérifiez que le logiciel NSX-T Data Center est supprimé de l'hôte.
 - a Connectez-vous à l'interface de ligne de commande de l'hôte en tant que racine.
 - b Exécutez cette commande pour vérifier la présence de VIB NSX-T Data Center

```
esxcli software vib list | grep -E 'nsx|vsipfwlib'
```

Si le logiciel NSX-T Data Center est correctement supprimé, aucun VIB n'est répertorié. Si des VIB NSX restent sur l'hôte, contactez le support VMware.

- 6 Si NSX Intelligence est également déployé sur l'hôte, la désinstallation de NSX-T Data Center échouera, car tous les nœuds de transport feront partie d'un groupe de sécurité réseau par défaut. Pour désinstaller :
 - a Sélectionnez le cluster et cliquez sur **Supprimer NSX**.
 - b Dans la fenêtre contextuelle de confirmation, sélectionnez l'option **Forcer la suppression**.
NSX-T est désinstallé de tous les hôtes du cluster.

Désinstaller NSX-T Data Center d'un hôte dans un cluster vSphere

Vous pouvez désinstaller NSX-T Data Center d'un seul hôte géré par vCenter Server. Les autres hôtes du cluster ne sont pas affectés.

Attention La désinstallation de NSX-T Data Center d'un hôte ESXi peut entraîner des perturbations si les interfaces physiques ou les interfaces VMkernel sont connectées à N-VDS. Si l'hôte ou le cluster fait partie d'autres applications, telles que vSAN, celles-ci peuvent être affectées par la désinstallation.

Conditions préalables

- Vérifiez que les mappages de désinstallation réseau sont configurés sur les hôtes que vous souhaitez désinstaller. Reportez-vous à la section [Vérifier les mappages réseau de l'hôte pour la désinstallation](#).
- Vérifiez que les hôtes que vous souhaitez désinstaller sont en mode de maintenance dans vSphere.

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Système > Infrastructure > Nœuds > Nœuds de transport hôtes**.
- 3 Dans le menu déroulant **Géré par**, sélectionnez vCenter Server.
- 4 Si un profil de nœud de transport a été appliqué au cluster, sélectionnez celui-ci, puis cliquez sur **Actions > Détacher un profil TN**.

Si un profil de nœud de transport a été appliqué au cluster, la colonne **Configuration de NSX** du cluster affiche le nom du profil.

- 5 Sélectionnez l'hôte et cliquez sur **Supprimer NSX**.
- 6 Vérifiez que le logiciel NSX-T Data Center est supprimé de l'hôte.
 - a Connectez-vous à l'interface de ligne de commande de l'hôte en tant que racine.
 - b Exécutez cette commande pour vérifier la présence de VIB NSX-T Data Center

```
esxcli software vib list | grep -E 'nsx|vsipfwlib'
```

Si le logiciel NSX-T Data Center est correctement supprimé, aucun VIB n'est répertorié. Si des VIB NSX restent sur l'hôte, contactez le support VMware.

- 7 Si un profil de nœud de transport avait été appliqué au cluster, et que vous voulez le réappliquer, sélectionnez le cluster, cliquez sur **Configurer NSX**, puis sélectionnez le profil dans le menu déroulant **Sélectionner le profil de déploiement**.

Désinstaller NSX-T Data Center d'un hôte autonome

Vous pouvez désinstaller NSX-T Data Center d'un hôte autonome. Les hôtes autonomes peuvent être ESXi ou KVM.

Attention La désinstallation de NSX-T Data Center d'un hôte ESXi peut entraîner des perturbations si les interfaces physiques ou les interfaces VMkernel sont connectées à N-VDS. Si l'hôte ou le cluster fait partie d'autres applications, telles que vSAN, celles-ci peuvent être affectées par la désinstallation.

Conditions préalables

Si vous désinstallez NSX-T Data Center à partir d'un hôte ESXi autonome, vérifiez les paramètres suivants :

- Vérifiez que les mappages de désinstallation réseau sont configurés sur les hôtes que vous souhaitez désinstaller. Reportez-vous à la section [Vérifier les mappages réseau de l'hôte pour la désinstallation](#).
- Vérifiez que les hôtes que vous souhaitez désinstaller sont en mode de maintenance dans vSphere.

Procédure

- 1 Dans un navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Système > Infrastructure > Nœuds > Nœuds de transport hôtes**.
- 3 Dans le menu déroulant **Géré par**, sélectionnez **Aucun : hôtes autonomes**.
- 4 Sélectionnez l'hôte et cliquez sur **Supprimer**. Dans la boîte de dialogue de confirmation qui s'affiche, assurez-vous que l'option **Désinstaller les composants NSX** est sélectionnée et que l'option **Forcer la suppression** est désélectionnée. Cliquez sur **Supprimer**.

Le logiciel NSX-T Data Center est supprimé de l'hôte. La suppression de tous les logiciels NSX-T Data Center peut prendre jusqu'à 5 minutes.

- 5 Si la désinstallation échoue, sélectionnez l'hôte et cliquez de nouveau sur **Supprimer**. Dans la boîte de dialogue de confirmation, désélectionnez **Désinstaller les composants NSX** et sélectionnez **Forcer la suppression**.

Le nœud de transport hôte est supprimé du plan de gestion, mais il est possible que le logiciel NSX-T Data Center soit encore installé sur l'hôte.

- 6 Vérifiez que le logiciel NSX-T Data Center est supprimé de l'hôte.
 - a Connectez-vous à l'interface de ligne de commande de l'hôte en tant que racine.
 - b Exécutez la commande appropriée pour vérifier les modules logiciels NSX-T Data Center.

Tableau 12-1. Commandes de liste de modules

Système d'exploitation hôte	Commande
ESXi	<code>esxcli software vib list grep -E 'nsx vsipfwlib'</code>
Red Hat Enterprise Linux et CentOS Linux	<code>rpm -qa grep -E 'nsx vsipfwlib'</code>
Ubuntu	<code>dpkg -l grep -E 'nsx vsipfwlib'</code>
SUSE Linux Enterprise Server	<code>zypper packages --installed-only grep -E 'nsx vsipfwlib'</code>

Si le logiciel NSX-T Data Center est correctement supprimé, aucun package n'est répertorié. Si des modules logiciels NSX restent sur l'hôte, contactez le support VMware.

Installation de composants NSX Cloud

13

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.

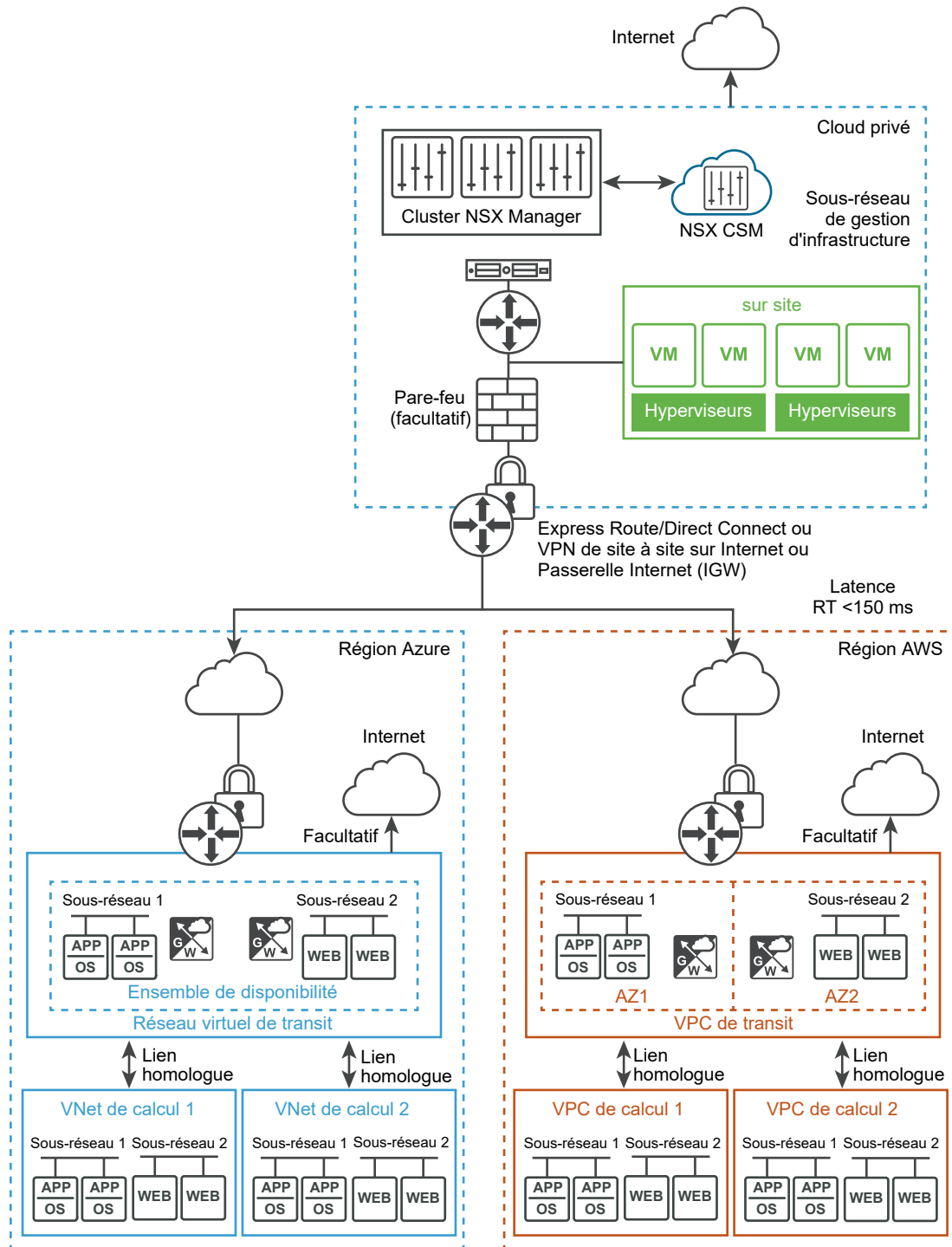
Ce chapitre contient les rubriques suivantes :

- [Architecture et composants de NSX Cloud](#)
- [Présentation du déploiement de NSX Cloud](#)
- [Déployer des composants NSX-T Data Center sur site](#)
- [Ajouter votre compte de cloud public](#)
- [Déployer la NSX Public Cloud Gateway](#)
- [\(Facultatif\) Installez NSX Tools sur vos machines virtuelles de charge de travail.](#)
- [Annuler le déploiement ou annuler le lien des PCG](#)

Architecture et composants de NSX Cloud

NSX Cloud intègre les principaux composants de NSX-T Data Center dans votre cloud public pour offrir le réseau et la sécurité dans vos implémentations.

Figure 13-1. Architecture de NSX Cloud



Composants principaux

Composants principaux de NSX Cloud :

- **NSX Manager** pour le plan de gestion avec routage basé sur des stratégies, contrôle d'accès basé sur les rôles (RBAC), plan de contrôle et états d'exécution définis.

- **Cloud Service Manager (CSM)** pour l'intégration à NSX Manager afin de fournir au plan de gestion des informations spécifiques au cloud public.
- **Passerelle de cloud public (PCG)** pour la connectivité à la gestion de NSX et aux plans de contrôle, pour les services de passerelle NSX Edge et pour les communications d'API avec les entités du cloud public.
- Fonctionnalité **NSX Tools** qui fournit le chemin de données géré par NSX pour les machines virtuelles de la charge de travail.

Présentation du déploiement de NSX Cloud

Reportez-vous à cette présentation pour comprendre le processus général d'installation et de configuration des composants de NSX Cloud afin de permettre à NSX-T Data Center de gérer vos machines virtuelles de charge de travail de cloud public.



Note Lors de la planification de votre déploiement, assurez-vous que les dispositifs NSX-T Data Center sur site disposent d'une bonne connectivité avec la PCG déployée dans le cloud public et que les VPC/VNet de transit se trouvent dans la même région que les VPC/VNet de calcul.

Tableau 13-1. Workflow pour le déploiement de NSX Cloud

Tâche	Instructions
<input type="checkbox"/> Installez CSM et connectez-vous à NSX Manager.	Reportez-vous à la section Déployer des composants NSX-T Data Center sur site .
<input type="checkbox"/> Ajoutez un ou plusieurs de vos comptes de cloud public à CSM.	Reportez-vous à la section Ajouter votre compte de cloud public .
<input type="checkbox"/> Déployez la PCG dans les VPC ou VNet de transit, et créez la liaison avec les VPC ou VNet de calcul.	Reportez-vous à la section Déployer la NSX Public Cloud Gateway .
Étape suivante	Suivez les instructions fournies à la section Utilisation de NSX Cloud du <i>Guide d'administration de NSX-T Data Center</i> .

Déployer des composants NSX-T Data Center sur site

Vous devez avoir déjà installé NSX Manager pour poursuivre l'installation des CSM.

Installation de CSM

Cloud Service Manager (CSM) est un composant essentiel de NSX Cloud.

Après l'installation de NSX Manager, installez CSM en suivant les mêmes étapes que pour l'installation de NSX Manager et en sélectionnant **nsx-cloud-service-manager** comme rôle de machine virtuelle. Reportez-vous à la section [Installer NSX Manager et les dispositifs disponibles](#) pour obtenir des instructions.

Vous pouvez déployer CSM dans la taille de machine virtuelle extra petite ou supérieure, si nécessaire. Pour plus d'informations, reportez-vous à la section [Configuration système requise pour le nœud de transport hôte et la machine virtuelle NSX Manager](#).

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 du nom d'utilisateur et du mot de passe pour le compte d'administrateur afin de vous connecter à NSX Manager
- CSM doit être installé et vous devez disposer du rôle d'administrateur d'entreprise dans CSM.

Procédure

- 1 Connectez-vous à CSM par le biais d'un navigateur.
- 2 Lorsque vous y êtes invité dans l'Assistant de configuration, cliquez sur **Commencer l'installation**.
- 3 Dans l'écran d'informations d'identification de NSX Manager, entrez les informations suivantes :

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 et un mot de passe d'administrateur d'entreprise pour NSX Manager.
Empreinte numérique du responsable	Éventuellement, entrez la valeur de l'empreinte numérique de NSX Manager. Si vous laissez ce champ vide, le système identifie l'empreinte numérique et l'affiche dans l'écran suivant.

- 4 (Facultatif) Si vous n'avez pas fourni de valeur d'empreinte numérique pour NSX Manager, ou si la valeur était incorrecte, l'écran **Vérifier l'empreinte** s'affiche. Cochez la case pour accepter l'empreinte numérique détectée par le système.

5 Cliquez sur **Connecter**.

Note Si ce paramètre vous manquait dans l'Assistant de configuration ou si vous souhaitez modifier NSX Manager associé, connectez-vous à CSM, cliquez sur **Système > Paramètres** et cliquez sur **Configurer** sur le panneau intitulé **Nœud NSX associé**.

CSM vérifie l'empreinte numérique du dispositif NSX Manager et établit la connexion.

6 (Facultatif) Configurez le serveur proxy. Voir les instructions dans [\(Facultatif\) Configurer les serveurs proxy](#).

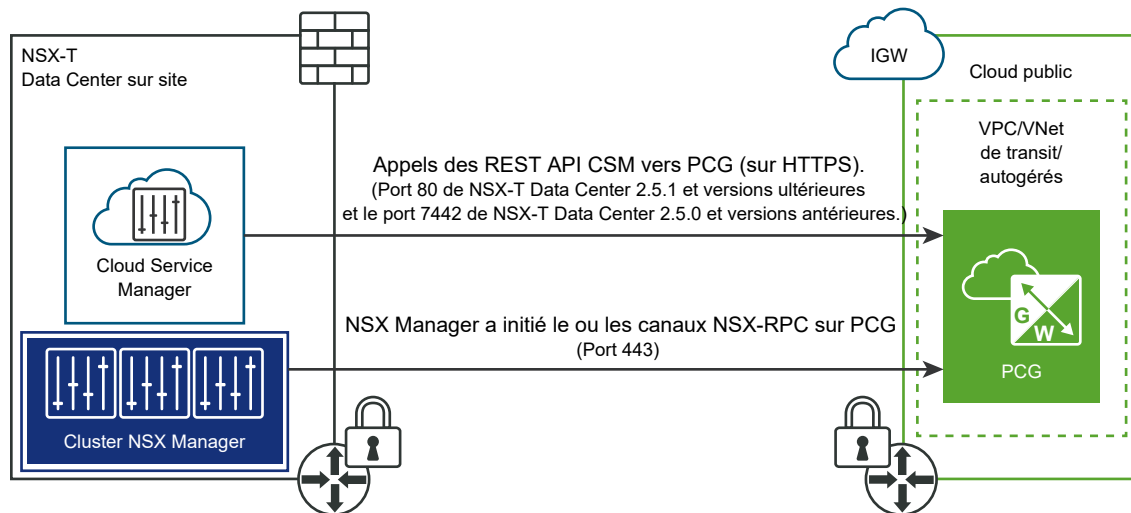
Activer l'accès aux ports et aux protocoles

Aucun port entrant ne doit être ouvert dans votre déploiement sur site de NSX-T Data Center pour activer la connectivité de cloud public.

Les ports sortants suivants sont requis :

Tableau 13-2. Ports et protocoles requis pour la connectivité de cloud public avec NSX-T Data Center

De	Vers	Port	Protocole	Requis pour :
CSM	PCG	80	TCP	Configuration CSM, telle que le workflow de mise à niveau, sur HTTPS.
Note Si vous utilisez NSX-T Data Center version 2.5.0, vous devez ouvrir le port non standard 7442 à la place, et vous assurer que votre pare-feu autorise le trafic SSL sur celui-ci.				
NSX Manager	PCG	443	TCP	Canaux NSX RPC.
CSM	NSX Manager	443	TCP	CSM pour accéder à NSX Manager. Reportez-vous à la section Ports et protocoles pour des détails sur le déploiement sur site.



(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.
Serveur proxy	Entrez l'adresse IP du serveur proxy. Cette information est obligatoire.

Option	Description
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.

(Facultatif) Configurer vIDM pour Cloud Service Manager

Si vous utilisez VMware Identity Manager, vous pouvez le configurer pour accéder à CSM depuis NSX Manager.

Procédure

- 1 Configurez vIDM pour NSX Manager et CSM. Consultez les instructions dans la section [Configurer l'intégration de VMware Identity Manager](#) dans le *Guide d'administration de NSX-T Data Center*.
- 2 Attribuez le même rôle à l'utilisateur de vIDM pour NSX Manager et CSM, par exemple **Administrateur d'entreprise** attribué à l'utilisateur nommé **vIDM_admin**. Vous devez vous connecter à NSX Manager et à CSM et attribuer le même rôle au même nom d'utilisateur. Reportez-vous à la section [Ajouter une attribution de rôle ou une identité de principal](#) dans le *Guide d'administration de NSX-T Data Center* pour obtenir des instructions détaillées.
- 3 Connectez-vous à NSX Manager. Vous êtes redirigé vers la connexion vIDM.
- 4 Entrez les informations d'identification de l'utilisateur de vIDM. Une fois que vous êtes connecté, vous pouvez basculer entre NSX Manager et CSM en cliquant sur l'icône Applications.



Ajouter votre compte de cloud public

Pour ajouter votre inventaire de cloud public, vous devez connecter votre compte de cloud public au déploiement sur site de NSX-T Data Center, créer des sous-réseaux requis dans votre VPC/VNet et créer des rôles dans votre cloud public pour autoriser l'accès à NSX Cloud.

Ces étapes ne sont pas dans un ordre spécifique et peuvent être effectuées indépendamment les unes des autres.

Note

- Connectez les VPC/VNet au déploiement sur site en utilisant des méthodes appropriées, telles que Direct Connect pour AWS, Express Route pour Microsoft Azure ou un VPN site à site avec n'importe quel point de terminaison VPN sur site et PCG agissant en tant que point de terminaison VPN dans votre cloud public.
 - Si vous choisissez d'avoir une topologie de transit/calcul, assurez-vous qu'il existe des connexions d'homologation établies entre les VPC/VNet de transit et de calcul. Une seule PCG vous permet de gérer plusieurs VPC/VNet de calcul. Vous pouvez également choisir d'avoir une architecture de VPC/VNet de calcul plate avec une paire de PCG installée sur chaque VPC/VNet.
-

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 Microsoft 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.

Reportez-vous à [Déployer la NSX Public Cloud Gateway](#) pour plus d'informations sur la manière dont ces sous-réseaux sont utilisés.

Configurer un accès sécurisé à l'inventaire Microsoft Azure

Pour que NSX Cloud fonctionne dans votre abonnement, créez un principal de service afin d'accorder les autorisations requises, ainsi que les rôles CSM et PCG, d'après la fonctionnalité Microsoft Azure de gestion des identités pour les ressources Azure.

Présentation :

- Votre abonnement Microsoft Azure contient un ou plusieurs réseaux virtuels que vous souhaitez inclure dans la gestion de NSX-T Data Center. Le réseau virtuel peut être en mode de calcul ou de transit. Un réseau virtuel de transit est un réseau virtuel dans lequel vous déployez la PCG. Vous pouvez lier d'autres réseaux virtuels au réseau virtuel de transit et intégrer les machines virtuelles de charge de travail hébergées sur ces VNet. Les réseaux virtuels liés au réseau virtuel de transit sont appelés réseaux virtuels de calcul.

- NSX Cloud fournit un script PowerShell qui permet de générer le principal de service et les rôles qui exploitent la fonctionnalité d'identité gérée de Microsoft Azure pour gérer l'authentification, tout en assurant la sécurité de vos informations d'identification Microsoft Azure. Vous pouvez également inclure plusieurs abonnements sous un principal de service à l'aide de ce script.
- Vous pouvez réutiliser le principal de service pour tous vos abonnements, ou bien créer de nouveaux principaux de service, si nécessaire. Un script supplémentaire permet de créer des principaux de service distincts pour des abonnements supplémentaires.
- Dans le cas de plusieurs abonnements, que vous utilisiez un seul principal de service pour tous les abonnements ou différents principaux de service, mettez à jour les fichiers JSON pour les rôles CSM et PCG en ajoutant tout nom d'abonnement supplémentaire dans la section *AssignableScopes*.
- Si vous avez déjà un principal de service NSX Cloud dans votre réseau virtuel et que vous souhaitez le mettre à jour, exécutez à nouveau les scripts en ignorant le nom de principal de service dans les paramètres.
- Le nom de principal de service doit être unique dans Microsoft Azure Active Directory. Vous pouvez utiliser le même principal de service dans différents abonnements sous le même domaine Active Directory, ou différents principaux de service par abonnement. Cependant, vous ne pouvez pas créer deux principaux de service portant le même nom.
- Vous devez être le titulaire des abonnements Microsoft Azure ou être autorisé à créer et à attribuer des rôles dans ces abonnements.
- Les scénarios suivants sont pris en charge :
 - **Scénario 1 :** vous disposez d'un seul abonnement Microsoft Azure et vous souhaitez l'activer avec NSX Cloud.
 - **Scénario 2 :** vous disposez de plusieurs abonnements Microsoft Azure dans le même annuaire Microsoft Azure. Vous souhaitez les activer avec NSX Cloud, en utilisant un seul principal de service NSX Cloud pour tous vos abonnements.
 - **Scénario 3 :** vous disposez de plusieurs abonnements Microsoft Azure dans le même annuaire Microsoft Azure. Vous souhaitez les activer avec NSX Cloud, en utilisant différents noms de principaux de service NSX Cloud pour les différents abonnements.

Le processus s'effectue de la façon suivante :

- 1 Utilisez le script NSX Cloud PowerShell pour :
 - Créez un compte de principal du service pour NSX Cloud.
 - Créer un rôle pour CSM.
 - Créer un rôle pour PCG.
- 2 (Facultatif) Créer des principaux de service pour les autres abonnements que vous souhaitez lier.

3 Ajoutez l'abonnement Microsoft Azure dans CSM.

Note Si vous utilisez plusieurs abonnements, que vous utilisiez le même principal de service ou des principaux différents, vous devez ajouter séparément chaque abonnement dans CSM.

Générer le principal de service et les rôles

NSX Cloud fournit les scripts PowerShell qui vous permettent de générer le principal de service et les rôles requis pour un ou plusieurs abonnements.

Conditions préalables

- Vous devez disposer de PowerShell 5.0 ou version ultérieure, et le module AzureRM doit être installé.
- Vous devez être le titulaire des abonnements Microsoft Azure ou être autorisé à créer et à attribuer des rôles dans ces abonnements.

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.

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 :

Script/Fichier	Description
CreateNSXRoles.ps1	<p>Script PowerShell permettant de générer le principal de service NSX Cloud et les rôles d'identité gérés pour CSM et PCG. Le script prend les paramètres suivants :</p> <ul style="list-style-type: none"> ■ <code>-subscriptionId <the Transit_VNet's_Azure_subscription_ID></code> ■ (Facultatif) <code>-servicePrincipalName <Service_Principal_Name></code> ■ (Facultatif) <code>-useOneServicePrincipal</code>
AddServicePrincipal.ps1	<p>Script facultatif. Il est nécessaire pour ajouter plusieurs abonnements et attribuer différents principaux de service à chaque abonnement. Reportez-vous au Scénario 3 dans les étapes ci-dessous. Le script prend les paramètres suivants :</p> <ul style="list-style-type: none"> ■ <code>-computeSubscriptionId <the_Compute_VNet's_Azure_subscription_ID></code> ■ <code>-transitSubscriptionId <the Transit_VNet's_Azure_Subscription_ID></code> ■ <code>-csmRoleName <CSM_Role_Name></code> ■ <code>-servicePrincipalName <Service_Principal_Name></code>

Script/Fichier	Description
nsx_csm_role.json	Modèle JSON pour le nom et les autorisations du rôle CSM. Ce fichier est requis comme entrée dans le script PowerShell doit se trouver dans le même dossier que le script.
nsx_pcg_role.json	Modèle JSON pour le nom et les autorisations du rôle PCG. Ce fichier est requis comme entrée dans le script PowerShell doit se trouver dans le même dossier que le script. Note Le nom du rôle PCG (passerelle) par défaut est <code>nsx-pcg-role</code> . Vous devez fournir cette valeur lors de l'ajout de votre abonnement dans CSM.

3 Scénario 1 : vous disposez d'un seul abonnement Microsoft Azure et vous souhaitez l'activer avec NSX Cloud.

- a À partir d'une instance de PowerShell, accédez au répertoire dans lequel vous avez téléchargé les scripts Microsoft Azure et les fichiers JSON.
- b Exécutez le script `CreateNSXRoles.ps1` avec le paramètre `-SubscriptionId`, comme suit :

```
.\CreateNSXRoles.ps1 -subscriptionId <the_single_Azure_subscription_ID>
```

Note Si vous souhaitez remplacer le nom de principal de service par défaut de `nsx-service-admin`, vous pouvez également utiliser le paramètre `-servicePrincipalName`. Le nom de principal de service doit être unique dans Microsoft Azure Active Directory.

4 Scénario 2 : vous disposez de plusieurs abonnements Microsoft Azure dans le même annuaire Microsoft Azure. Vous souhaitez les activer avec NSX Cloud, en utilisant un seul principal de service NSX Cloud pour tous vos abonnements.

- a À partir d'une instance de PowerShell, accédez au répertoire dans lequel vous avez téléchargé les scripts Microsoft Azure et les fichiers JSON.
- b Modifiez chacun des fichiers JSON pour y ajouter la liste des autres ID d'abonnement dans la section *AssignableScopes*, par exemple :

```
"AssignableScopes": [
  "/subscriptions/aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",
  "/subscriptions/aaaaaaaa-bbbb-cccc-dddd-ffffffffffff",
  "/subscriptions/aaaaaaaa-bbbb-cccc-dddd-000000000000"
```

Note Vous devez utiliser le format indiqué dans l'exemple pour ajouter des ID d'abonnement : `"/subscriptions/<Subscription_ID>"`

- c Exécutez le script `CreateNSXRoles.ps1` avec les paramètres `-subscriptionID` et `-useOneServicePrincipal` :

```
.\CreateNSXRoles.ps1 -subscriptionId <the_Transit_VNet's_Azure_subscription_ID>
-useOneServicePrincipal
```

Note Vous pouvez omettre le nom du principal de service si vous souhaitez utiliser le nom par défaut : `nsx-service-admin`. Si vous exécutez le script sans nom de principal de service, alors que ce nom de principal de service existe déjà dans Microsoft Azure Active Directory, alors ce principal de service est mis à jour.

5 Scénario 3 : vous disposez de plusieurs abonnements Microsoft Azure dans le même annuaire Microsoft Azure. Vous souhaitez les activer avec NSX Cloud, en utilisant différents noms de principaux de service NSX Cloud pour les différents abonnements.

- a À partir d'une instance de PowerShell, accédez au répertoire dans lequel vous avez téléchargé les scripts Microsoft Azure et les fichiers JSON.
- b Suivez les étapes **b** et **c** du deuxième scénario pour ajouter plusieurs abonnements dans la section *AssignableScopes* de chaque fichier JSON.

- c Exécutez le script `CreateNSXRoles.ps1` avec le paramètre `-subscriptionID` :

```
.\CreateNSXRoles.ps1 -subscriptionId <One of the subscription_IDs>
```

Note Vous pouvez omettre le nom du principal de service si vous souhaitez utiliser le nom par défaut : `nsx-service-admin`. Si vous exécutez le script sans nom de principal de service, alors que ce nom de principal de service existe dans Microsoft Azure Active Directory, alors ce principal de service est mis à jour.

- d Exécutez le script `AddServicePrincipal.ps1` avec les paramètres suivants :

Paramètre	Valeur
<code>-computeSubscriptionId</code>	ID d'abonnement Azure du VNet de calcul
<code>-transitSubscriptionId</code>	ID d'abonnement Azure du VNet de transit
<code>-csmRoleName</code>	Obtenez cette valeur à partir du fichier <code>nsx_csm_role.JSON</code>
<code>-servicePrincipalName</code>	Nouveau nom du principal de service

```
./AddServicePrincipal.ps1 -computeSubscriptionId <the_Compute_VNet's_Azure_subscription_ID>
-transitSubscriptionId <the_Transit_VNet's_Azure_Subscription_ID>
-csmRoleName <CSM_Role_Name>
-servicePrincipalName <new_Service_Principal_Name>
```

- 6 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 requises pour ajouter votre abonnement Microsoft Azure dans CSM.

- ID de client
- Clé de client
- ID de locataire
- ID d'abonnement

Résultats

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.

- un fichier au nom semblable à `NSXCloud_ServicePrincipal_<your_subscription_ID>_<NSX_Cloud_Service_Principal_name>`. Il est créé dans le répertoire où vous avez exécuté le script PowerShell. Ce fichier contient les informations requises pour ajouter votre abonnement Microsoft Azure dans CSM.

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

Note Lorsque vous activez NSX Cloud pour plusieurs abonnements, vous devez les ajouter individuellement à CSM. Par exemple, si vous disposez de cinq abonnements, ajoutez cinq comptes Microsoft Azure à CSM, avec différents ID d'abonnement, mais toutes les autres valeurs identiques.

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. La valeur par défaut est `nsx-pcg-role`.

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** sous trois minutes.

5 Mettez sur liste blanche toutes les machines virtuelles du VNet sur lesquelles vous souhaitez que les machines virtuelles soient gérées. Cette opération n'est pas obligatoire, mais elle est fortement recommandée pour les déploiements existants en raison de l'incidence de la stratégie de mise en quarantaine lorsqu'elle passe de l'état désactivé à l'état activé.

Étape suivante

[Déployer une PCG dans un VNet](#)

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 ; pour plus d'informations, 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.

Reportez-vous à [Déployer la NSX Public Cloud Gateway](#) pour plus de détails.

- 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.

Configurer un accès sécurisé à l'inventaire AWS

Vous disposez peut-être d'un ou de plusieurs comptes AWS comprenant des VPC et des machines virtuelles de charge de travail que vous souhaitez inclure dans la gestion NSX-T Data Center.

Présentation :

- Vous pouvez utiliser une topologie de VPC de transit/calcul : déployez la PCG dans un VPC (qui devient le VPC de transit), puis liez d'autres VPC (appelés les VPC de calcul) à ce premier VPC.
- NSX Cloud fournit un script shell que vous pouvez exécuter à partir de la CLI AWS de votre compte AWS afin de créer le profil et le rôle IAM, et d'établir une relation de confiance pour les VPC de calcul et de transit.
- Les scénarios suivants sont pris en charge :
 - **Scénario 1 :** vous souhaitez utiliser un seul compte AWS avec NSX Cloud.
 - **Scénario 2 :** vous souhaitez utiliser plusieurs sous-comptes qui sont définis dans AWS et gérés par un compte AWS maître.
 - **Scénario 3 :** vous souhaitez utiliser plusieurs comptes AWS avec NSX Cloud.

Le processus s'effectue de la façon suivante :

- 1 Utiliser le script shell NSX Cloud (CLI AWS requise) pour effectuer les opérations suivantes :
 - Créer un profil de liaison montante.
 - Créer un rôle pour PCG.
 - (Facultatif) Créer une relation de confiance entre le compte AWS qui héberge le VPC de transit et le compte AWS qui héberge le VPC de calcul.
- 2 Ajouter le compte AWS dans CSM.

Générer le profil IAM et le rôle PCG

NSX Cloud propose un script shell qui permet de configurer un ou plusieurs comptes AWS en générant un profil IAM, ainsi qu'un rôle pour la PCG attachée au profil qui fournit les autorisations nécessaires à votre compte AWS.

Si vous prévoyez d'héberger un VPC de transit lié à plusieurs VPC de calcul résidant dans deux comptes AWS distincts, vous pouvez utiliser le script pour créer une relation de confiance entre ces comptes.

Note Par défaut, le nom du rôle PCG (passerelle) est `nsx_pcg_service`. Si vous souhaitez modifier le nom de rôle de passerelle, vous pouvez lui attribuer une autre valeur dans le script, mais prenez bien note de cette valeur, car elle est requise pour ajouter le compte AWS à CSM.

Conditions préalables

Avant d'exécuter le script, assurez-vous d'installer et de configurer les éléments suivants sur votre système Linux ou compatible :

- CLI AWS
- jq (analyseur JSON)

■ openssl

Note Si vous utilisez plusieurs comptes AWS, ils doivent être appairés à l'aide d'une méthode appropriée.

Procédure

- 1 Sur un poste de travail ou serveur Linux ou compatible, téléchargez le script shell `nsx_csm_iam_script.sh` à partir de la page de téléchargement de NSX-T Data Center > **Pilotes et outils > Scripts NSX Cloud > AWS.**

- 2 **Scénario 1 :** vous souhaitez utiliser un seul compte AWS avec NSX Cloud.

- a Exécutez le script, par exemple :

```
bash nsx_csm_iam_script.sh
```

- b Entrez `yes` lorsque la question `Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no]` s'affiche.
- c Entrez le nom que vous souhaitez attribuer à l'utilisateur IAM lorsque le système affiche la question `What do you want to name the IAM User?`

Note Le nom d'utilisateur IAM doit être unique dans votre compte AWS.

- d Entrez `no` lorsque le système affiche la question `Do you want to add trust relationship for any Transit VPC account? [yes/no]`

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 `aws_details.txt`, dans le répertoire où vous avez exécuté le script. Suivez ensuite les instructions de la section [Ajouter votre compte AWS dans CSM](#), puis celles de la section [Déployer PCG dans un VPC](#), pour terminer le processus de configuration d'un VPC autogéré ou de transit.

- 3 **Scénario 2 :** vous souhaitez utiliser plusieurs sous-comptes qui sont définis dans AWS et gérés par un seul compte AWS maître.

- a Exécutez le script à partir de votre compte AWS maître.

```
bash nsx_csm_iam_script.sh
```

- b Entrez `yes` lorsque la question `Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no]` s'affiche.

- c Entrez le nom que vous souhaitez attribuer à l'utilisateur IAM lorsque le système affiche la question `What do you want to name the IAM User?`

Note Le nom d'utilisateur IAM doit être unique dans votre compte AWS.

- d Entrez `no` lorsque le système affiche la question `Do you want to add trust relationship for any Transit VPC account?` `[yes/no]`

Note Lorsque vous utilisez un compte AWS maître, si le VPC de transit est autorisé à visualiser les VPC de calcul résidant dans les sous-comptes, il est inutile d'établir une relation de confiance avec les sous-comptes. S'il n'y est pas autorisé, suivez les étapes du **scénario 3** pour configurer plusieurs comptes.

Si le script s'exécute sans erreur, le profil IAM et un rôle pour la PCG sont créés dans votre compte AWS maître. Les valeurs sont enregistrées dans le fichier de sortie dans le répertoire où vous avez exécuté le script. Le nom du fichier est `aws_details.txt`. Suivez ensuite les instructions de la section [Ajouter votre compte AWS dans CSM](#), puis celles de la section [Déployer PCG dans un VPC](#), pour terminer le processus de configuration d'un VPC autogéré ou de transit.

4 Scénario 3 : vous souhaitez utiliser plusieurs comptes AWS avec NSX Cloud.

Note Avant de continuer, vérifiez que les comptes AWS sont appairés.

- a Prenez note du numéro de compte AWS à 12 chiffres correspondant au compte dans lequel vous souhaitez héberger le VPC de transit.
- b Configurez le VPC de transit dans le compte AWS en suivant les étapes a à d du *scénario 1* et terminez le processus d'ajout du compte dans CSM.
- c Téléchargez et exécutez le script NSX Cloud à partir d'un système Linux ou compatible dans l'autre compte AWS où vous souhaitez héberger le VPC de calcul.

Note Si vous préférez, vous pouvez aussi utiliser des profils AWS avec différentes informations d'identification de compte afin de réexécuter le script pour l'autre compte AWS à l'aide du même système.

- d Entrez `yes` lorsque le système affiche la question `Do you want to create an IAM user for CSM and an IAM role for PCG?` `[yes/no]`

Note Si vous avez déjà ajouté ce compte AWS dans CSM et que vous souhaitez réutiliser le script pour la connexion à un autre compte AWS, vous pouvez entrer `no` et ignorer la création de l'utilisateur IAM.

- e Entrez le nom que vous souhaitez attribuer à l'utilisateur IAM lorsque le système affiche la question `What do you want to name the IAM User?`

Note Le nom d'utilisateur IAM doit être unique dans votre compte AWS.

- f Entrez **yes** lorsque le système affiche la question `Do you want to add trust relationship for any Transit VPC account? [yes/no]`
- g Entrez ou copiez-collez le numéro de compte AWS à 12 chiffres que vous avez noté à l'étape 1 lorsque le système a affiché la question `What is the Transit VPC account number?`

Une relation de confiance IAM est établie entre les deux comptes AWS, et le script génère un ID externe.

Si le script s'exécute sans erreur, le profil IAM et un rôle pour la PCG sont créés dans votre compte AWS maître. Les valeurs sont enregistrées dans le fichier de sortie dans le répertoire où vous avez exécuté le script. Le nom du fichier est `aws_details.txt`. Suivez ensuite les instructions de la section [Ajouter votre compte AWS dans CSM](#), puis celles de la section [Liaison vers un VPC ou VNet de transit](#), pour terminer le processus de liaison vers un VPC de transit.

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
Découvrir les 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.

- 4 Mettez sur liste blanche toutes les machines virtuelles du VPC sur lesquelles vous souhaitez que les machines virtuelles soient gérées. Cette opération n'est pas obligatoire, mais elle est fortement recommandée pour les déploiements existants en raison de l'incidence de la stratégie de mise en quarantaine lorsqu'elle passe de l'état désactivé à l'état activé.

Étape suivante

[Déployer PCG dans un VPC](#)

Déployer la NSX Public Cloud Gateway

La NSX Public Cloud Gateway (PCG) fournit une connectivité nord-sud entre le cloud public et les composants de gestion sur site de NSX-T Data Center.

Familiarisez-vous avec la terminologie suivante qui explique les modes d'architecture et de déploiement de la PCG pour la gestion des machines virtuelles de charge de travail.

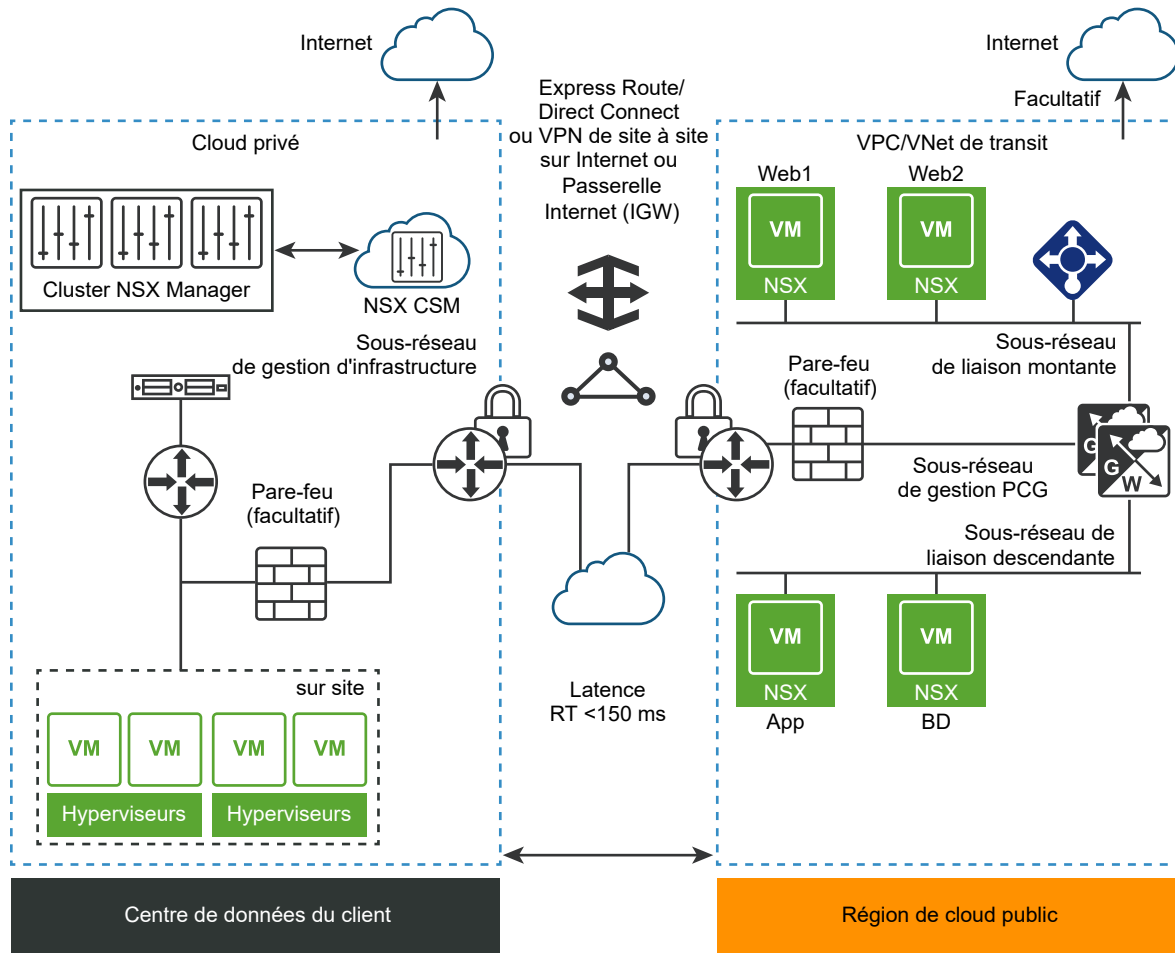
Note Le PCG est déployé dans une taille par défaut unique pour chaque cloud public pris en charge :

Cloud public	Type d'instance PCG
AWS	C4.xlarge
	Note Certaines régions peuvent ne pas prendre en charge le type d'instance C4.xlarge. Pour plus d'informations, reportez-vous à la documentation d'AWS.
Microsoft Azure	Norme DS3 v.2

Architecture

La PCG peut être un dispositif de passerelle autonome, ou bien être partagée entre vos réseaux virtuels ou VPC de cloud public, pour réaliser une topologie structurée en étoile.

Figure 13-2. Architecture de NSX Public Cloud Gateway



Modes de déploiement

VPC/VNet autogéré : lorsque vous déployez la PCG dans un VPC ou VNet, ce dernier remplit les conditions pour devenir un VPC/VNet *autogéré*. Autrement dit, vous pouvez importer des machines virtuelles hébergées sur ce VPC ou VNet géré à l'aide de NSX.

VPC/VNet de transit : un VPC/VNet autogéré devient un VPC/VNet de *transit* lorsque vous le liez à des VPC/VNet de calcul.

VPC/VNet de calcul : les VPC/VNet dans lesquels la PCG n'est pas déployée, mais qui sont liés à un VPC/VNet de transit, sont appelés VPC/VNet de *calcul*.

Sous-réseaux requis dans votre VPC/VNet pour déployer PCG

La PCG utilise les sous-réseaux suivants que vous avez configuré dans votre VPC/VNet. Reportez-vous à la section [Connecter votre réseau Microsoft Azure à votre déploiement NSX-T Data Center sur site](#) ou [Connecter votre réseau AWS \(Amazon Web Services\) à votre déploiement NSX-T Data Center sur site](#).

- **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 pour le débogage.

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.

Modes de gestion des machines virtuelles

Mode d'application NSX : dans ce mode, les machines virtuelles de charge de travail sont gérées par NSX par le biais de NSX Tools qui doit être installé sur chaque machine virtuelle de charge de travail après l'application de la balise « nsx.network=default » dans AWS ou Microsoft Azure.

Mode d'application du Cloud natif : dans ce mode, les machines virtuelles de charge de travail peuvent être gérées par NSX sans le recours à NSX Tools.

Stratégie de mise en quarantaine

Stratégie de mise en quarantaine : il s'agit de la fonctionnalité de détection des menaces de NSX Cloud qui fonctionne avec vos groupes de sécurité de cloud public.

- Dans le Mode d'application NSX, vous pouvez activer ou désactiver la stratégie de mise en quarantaine. Il est recommandé d'avoir désactivé la stratégie de mise en quarantaine et placé toutes vos machines virtuelles sur liste blanche lors de l'intégration des machines virtuelles de charge de travail.
- Dans le Mode d'application du Cloud natif, la stratégie de mise en quarantaine est toujours activée et ne peut pas être désactivée.

Options de conception possibles

Quel que soit le mode dans lequel vous déployez la PCG, vous pouvez la lier à un VPC/VNet de calcul dans n'importe quel mode.

Tableau 13-3. Options de conception possibles avec les modes de déploiement de PCG

Mode de déploiement de PCG dans le VPC/VNet de transit	Modes possibles lors de la liaison de VPC/VNet de calcul à ce VPC/VNet de transit
Mode d'application NSX	<ul style="list-style-type: none"> ■ Mode d'application NSX ■ Mode d'application du Cloud natif
Mode d'application du Cloud natif	<ul style="list-style-type: none"> ■ Mode d'application NSX ■ Mode d'application du Cloud natif

Note Une fois qu'un mode est sélectionné pour un VPC/VNet de transit ou de calcul, vous ne pouvez pas le changer. Si vous souhaitez changer de mode, vous devez annuler le déploiement de la PCG et redéployer cette dernière dans le mode souhaité.

Déployer une PCG dans un VNet

Suivez ces instructions pour déployer une PCG dans un réseau virtuel Microsoft Azure.

Le réseau virtuel dans lequel vous déployez une PCG peut tenir lieu de réseau virtuel de transit auquel les autres réseaux virtuels (appelés réseaux virtuels de calcul) peuvent se connecter. Ce réseau virtuel peut également gérer les machines virtuelles et se comporter comme un réseau virtuel autogéré.

Suivez ces instructions pour déployer une PCG. Si vous souhaitez créer une liaison vers un réseau virtuel de transit existant, reportez-vous à la section [Liaison vers un VPC ou VNet de transit](#).

Conditions préalables

- Vos comptes de cloud public doivent être déjà ajoutés dans CSM.
- Le réseau virtuel sur lequel vous déployez la PCG doit être doté des sous-réseaux requis, configurés de manière à prendre en charge la haute disponibilité (*liaison montante, liaison descendante et gestion*).

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 VNet sur lequel vous souhaitez déployer la PCG.
- 4 Cliquez sur **Déployer des passerelles**. L'assistant **Déployer la passerelle** 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	<p>Vous pouvez uniquement modifier le paramètre de stratégie de mise en quarantaine si vous choisissez de gérer les machines virtuelles de charge de travail à l'aide de NSX Tools (Mode d'application NSX). La stratégie de mise en quarantaine est toujours activée dans le Mode d'application du Cloud natif.</p> <p>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.</p>
Gérer avec NSX Tools	Conservez l'état désactivé par défaut pour les machines virtuelles de charge de travail intégrées dans le Mode d'application du Cloud natif. Si vous souhaitez installer NSX Tools sur vos machines virtuelles de charge de travail pour utiliser le Mode d'application NSX, activez cette option.
Installer automatiquement NSX Tools	Cette fonction est disponible uniquement lorsque vous activez Gérer avec NSX Tools. Si cette option est sélectionnée, NSX Tools est installé automatiquement sur toutes les machines virtuelles de charge de travail dans le VNet de calcul de transit/autogéré/lié si la balise <code>nsx.network=default</code> lui est appliquée.
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> <p>Note Le format d'URL du VHD doit être correct. Nous vous recommandons d'utiliser l'option Cliquer pour copier dans Microsoft Azure.</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	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

Option	Description
Obtenir les paramètres à partir du DHCP du fournisseur de cloud public	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.
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 dans ce réseau virtuel.
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 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.

6 Cliquez sur **Suivant**.

7 Pour l'option **Sous-réseaux**, utilisez les directives suivantes :

Option	Description
Activer la fonctionnalité HA pour NSX Cloud Gateway	Sélectionnez cette option pour activer la haute disponibilité.
Sous-réseaux	Sélectionnez cette option pour activer la haute disponibilité.
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.

Étape suivante

Suivez les instructions fournies à la section [Utilisation de NSX Cloud](#) du *Guide d'administration de NSX-T Data Center*.

Déployer PCG dans un VPC

Suivez ces instructions pour déployer une PCG dans un VPC AWS.

Le VPC dans lequel vous déployez une PCG peut tenir lieu de VPC de transit auquel les autres VPC (appelés VPC de calcul) peuvent se connecter. Ce VPC peut également gérer les machines virtuelles et se comporter comme un VPC autogéré.

Suivez ces instructions pour déployer une PCG. Si vous souhaitez créer une liaison vers un VPC de transit existant, reportez-vous à la section [Liaison vers un VPC ou VNet de transit](#).

Conditions préalables

- Vos comptes de cloud public doivent être déjà ajoutés dans CSM.
- Le VPC dans lequel vous déployez la PCG doit être doté des sous-réseaux requis, configurés de manière à prendre en charge la haute disponibilité (*liaison montante, liaison descendante et gestion*).
- La configuration de la liste de contrôle d'accès réseau de votre VPC doit inclure une règle entrante ALLOW.

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	<p>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.</p> <p>Cela identifie de façon unique votre compte AWS.</p>
Stratégie de mise en quarantaine sur le VPC associé	<p>Vous pouvez uniquement modifier le paramètre de stratégie de mise en quarantaine si vous choisissez de gérer les machines virtuelles de charge de travail à l'aide de NSX Tools (Mode d'application NSX). La stratégie de mise en quarantaine est toujours activée dans le Mode d'application du Cloud natif.</p> <p>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.</p>
Gérer avec NSX Tools	<p>Conservez l'état désactivé par défaut pour les machines virtuelles de charge de travail intégrées dans le Mode d'application du Cloud natif. Si vous souhaitez installer NSX Tools sur vos machines virtuelles de charge de travail pour utiliser le Mode d'application NSX, activez cette option.</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>

Option	Description
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.
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 la passerelle de cloud public	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

Suivez les instructions fournies à la section [Utilisation de NSX Cloud](#) du *Guide d'administration de NSX-T Data Center*.

Liaison vers un VPC ou VNet de transit

Vous pouvez lier un ou plusieurs VPC ou VNet de calcul à un VPC ou VNet de transit.

Conditions préalables

- Vérifiez que vous disposez d'un VPC ou d'un VNet de transit doté d'une PCG.
- Vérifiez que le VPC/VNet à lier est connecté au VPC ou VNet de transit par VPN ou appairage.
- Vérifiez que le VPC/VNet de calcul se trouve dans la même région que le VPC/VNet de transit.

Note Dans la configuration VPN IPSec basée sur le routage, vous devez spécifier l'adresse IP du port VTI (Virtual Tunnel Interface). Cette adresse IP doit se trouver dans un sous-réseau différent de celui des machines virtuelles de charge de travail. Cela empêche le trafic entrant de la machine virtuelle de charge de travail d'être dirigé vers le port VTI à partir duquel il sera abandonné.

Note Dans le cloud public, il existe une limite par défaut pour le nombre de règles entrantes/sortantes par groupe de sécurité et NSX Cloud crée des groupes de sécurité par défaut. Cela affecte le nombre de VPC/VNet de calcul pouvant être liés à un VPC/VNet de transit. En supposant un seul bloc CIDR par VPC/VNet, NSX Cloud prend en charge 10 VPC/VNet de calcul par VPC/VNet de transit. Si vous avez plusieurs CIDR dans un VPC/VNet de calcul, le nombre de VPC/VNet de calcul pris en charge par VPC/VNet de transit diminue. Vous pouvez ajuster les limites par défaut en contactant votre fournisseur de cloud public.

Procédure

- 1 Connectez-vous à CSM à l'aide d'un compte disposant du rôle d'administrateur d'entreprise.
- 2 Cliquez sur **Clouds > AWS/Azure > <public cloud_account_name>** et accédez à l'onglet **VPC/VNet**.
- 3 Sous l'onglet **VPC** ou **VNet**, sélectionnez le nom d'une région où vous hébergez un ou plusieurs VPC ou VNet de calcul.
- 4 Sélectionnez un VPC/VNet de calcul configuré pour NSX Cloud.
- 5 Cliquez sur **Lier au VPC de transit** ou sur **Lier au réseau virtuel de transit**.

6 Renseignez les options dans la fenêtre **Lier au VPC ou réseau virtuel de transit** :

Option	Description
VPC ou VNet de transit	<p>Dans le menu déroulant, sélectionnez un VPC ou VNet de transit. Le VPC ou VNet de transit que vous sélectionnez doit être déjà lié à ce VPC, par VPN ou appairage.</p> <p>Note Si vous vous connectez à un VNet de transit, vous devez disposer d'un redirecteur DNS configuré dans ce VNet et la balise <code>nsx.dnsserver=<IP address of the DNS forwarder></code> appliquée au VNet de transit. Pour plus d'informations sur la configuration du redirecteur DNS, consultez la documentation de Microsoft Azure.</p>
Stratégie de mise en quarantaine par défaut	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.
Gérer avec NSX Tools	Conservez l'état désactivé par défaut pour les machines virtuelles de charge de travail intégrées dans le Mode d'application du Cloud natif. Si vous souhaitez installer NSX Tools sur vos machines virtuelles de charge de travail pour utiliser le Mode d'application NSX, activez cette option.
Installer automatiquement NSX Tools	Cette fonction est disponible uniquement lorsque vous choisissez l'option Gérer avec NSX Tools et uniquement pour les VNet Microsoft Azure. Si cette option est sélectionnée, NSX Tools est installé automatiquement sur toutes les machines virtuelles de charge de travail dans le VNet de calcul de transit/autogéré/lié si la balise <code>nsx.network=default</code> lui est appliquée.

Étape suivante

Suivez les instructions fournies à la section [Utilisation de NSX Cloud](#) du *Guide d'administration de NSX-T Data Center*.

Entités logiques et groupes de sécurité cloud natifs créés automatiquement

Le déploiement d'une PCG sur un VPC/VNet de transit et la liaison d'un VPC/VNet de calcul vers ce premier VPC/VNet déclenchent les configurations requises dans NSX-T Data Center et le cloud public.

Entités logiques NSX-T créées automatiquement

Un ensemble d'entités logiques est créé automatiquement dans NSX Manager.

Connectez-vous à NSX Manager pour afficher les entités logiques créées automatiquement.

Important Ne supprimez aucune de ces entités créées automatiquement, sauf si vous annulez manuellement le déploiement de PCG. Pour plus d'informations, reportez-vous à la section [Dépannage lié à l'annulation du déploiement de PCG](#).

Entités système

Les entités suivantes s'affichent dans l'onglet **Système** :

Tableau 13-4. Entités système créées automatiquement

Entité système logique	Nombre d'éléments créés	Nomenclature	Portée
Zones de transport	Deux zones de transport sont créées pour chaque VPC/VNet de transit.	<ul style="list-style-type: none"> ■ TZ-<VPC/VNet-ID>-OVERLAY ■ TZ-<VPC/VNet-ID>-VLAN 	Étendue : global
Nœuds de transport Edge	Pour chaque PCG déployée, un nœud de transport Edge est créé, voire deux si le déploiement s'effectue en mode de haute disponibilité.	<ul style="list-style-type: none"> ■ PublicCloudGateway TN-<VPC/VNET-ID> ■ PublicCloudGateway TN-<VPC/VNET-ID>-preferred 	Étendue : global
Cluster Edge	Un cluster Edge est créé pour chaque PCG déployée (seule ou dans une paire de haute disponibilité).	PCG-cluster-<VPC/VNet-ID>	Étendue : global

Entités d'inventaire

Les entités suivantes sont disponibles dans l'onglet **Inventaire** :

Tableau 13-5. Groupes

Groupes	Portée
Deux groupes nommés : <ul style="list-style-type: none"> ■ cloud-default-route ■ cloud-metadata services 	Étendue : partagée entre toutes les PCG
Un groupe créé au niveau du VPC/VNet de transit en tant que groupe parent pour les segments individuels créés au niveau du VPC/VNet de calcul. cloud-<Transit VPC/VNet ID>-all-segments	Étendue : partagée entre tous les VPC/VNet de calcul

Tableau 13-5. Groupes (suite)

Groupes	Portée
<p>Deux groupes pour chaque VPC/VNet de calcul :</p> <ul style="list-style-type: none"> ■ Groupe de CIDR réseau pour tous les CIDR du VPC/VNet de calcul : <code>cloud-<Compute VPC/VNet ID>-cidr</code> ■ Groupe de segments locaux pour tous les segments gérés dans le VPC/VNet de calcul : <code>cloud-<Compute VPC/VNet ID>-local-segments</code> 	Étendue : partagée entre tous les VPC/VNet de calcul
<p>Les groupes suivants sont créés pour les services de cloud public actuellement pris en charge :</p> <ul style="list-style-type: none"> ■ <code>aws-dynamo-db-service-endpoint</code> ■ <code>aws-elb-service-endpoint</code> ■ <code>aws-rds-service-endpoint</code> ■ <code>aws-s3-service-endpoint</code> ■ <code>azure-cosmos-db-service-endpoint</code> ■ <code>azure-load-balancer-service-endpoint</code> ■ <code>azure-sql-service-endpoint</code> ■ <code>azure-storage-service-endpoint</code> 	Étendue : partagée entre toutes les PCG

Note Pour les PCG déployées ou liées dans le Mode d'application du Cloud natif, toutes les machines virtuelles de charge de travail dans le VPC/VNet sont disponibles sous Machines virtuelles dans NSX Manager.

Entités de sécurité

Les entités suivantes sont disponibles dans l'onglet **Sécurité** :

Tableau 13-6. Entités de sécurité créées automatiquement

Entité de sécurité logique	Nombre d'éléments créés	Nomenclature	Portée
Pare-feu distribué (est-ouest)	<p>Deux par VPC/VNet de transit :</p> <ul style="list-style-type: none"> ■ Sans état ■ Avec état 	<ul style="list-style-type: none"> ■ <code>cloud-stateless-<VPC/VNet ID></code> ■ <code>cloud-stateful-<VPC/VNet ID></code> 	<ul style="list-style-type: none"> ■ Règle avec état pour autoriser le trafic dans les segments gérés locaux ■ Règle avec état pour refuser le trafic provenant des machines virtuelles non gérées
Pare-feu de passerelle (nord-sud)	Un par VPC/VNet de transit	<code>cloud-<Transit VPC/VNet ID></code>	

Entités de mise en réseau

Les entités suivantes sont créées à différentes étapes de l'intégration et se trouvent sous l'onglet **Mise en réseau** :

Figure 13-3. Entités de mise en réseau NSX-T Data Center créées automatiquement après le déploiement de PCG

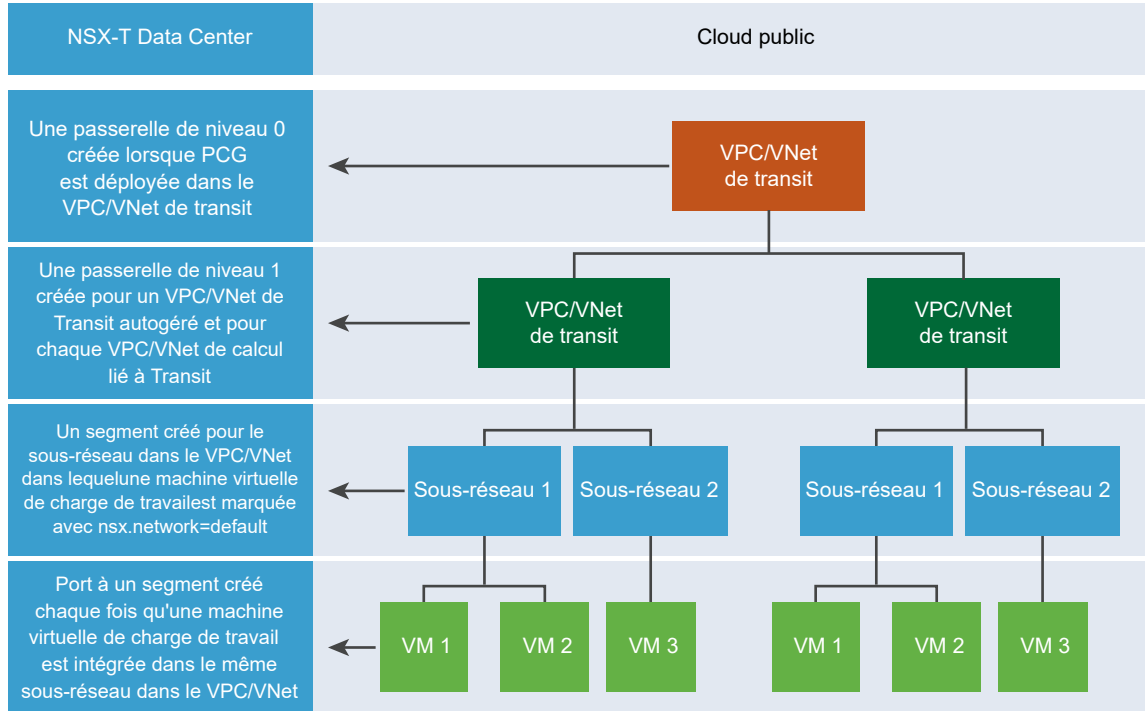


Tableau 13-7. Entités de mise en réseau créées automatiquement

Tâche d'intégration	Entités logiques créées dans NSX-T Data Center
Déploiement de la PCG sur le VPC/VNet de transit	<ul style="list-style-type: none"> ■ Passerelle de niveau 0 ■ Infra segment (commutateur VLAN par défaut) ■ Routeur de niveau 1
Liaison du VPC/VNet de calcul au VPC/VNet de transit	<ul style="list-style-type: none"> ■ Routeur de niveau 1

Tableau 13-7. Entités de mise en réseau créées automatiquement (suite)

Tâche d'intégration	Entités logiques créées dans NSX-T Data Center
La machine virtuelle de charge de travail sur laquelle NSX Agent est installé est balisée à l'aide de la clé:valeur « nsx.network:default » dans le sous-réseau d'un VPC/VNet autogéré ou de calcul.	<ul style="list-style-type: none"> ■ Un segment est créé pour ce sous-réseau spécifique du VPC/VNet autogéré ou de calcul. ■ Des ports hybrides sont créés pour chaque machine virtuelle de charge de travail balisée sur laquelle NSX Agent est installé.
D'autres machines virtuelles de charge de travail sont balisées dans le même sous-réseau du VPC/VNet autogéré ou de calcul.	<ul style="list-style-type: none"> ■ Des ports hybrides sont créés pour chaque machine virtuelle de charge de travail balisée sur laquelle NSX Agent est installé.

Stratégies de transfert

Les trois règles de transfert suivantes sont configurées pour un VPC/VNet de calcul, y compris le VPC/VNet de transit autogéré :

- Accéder à un CIDR du VPC de calcul sur le réseau du cloud public (sous-couche)
- Acheminer le trafic relevant des services de métadonnées de cloud public sur le réseau du cloud public (sous-couche)
- Acheminer tout ce qui ne se trouve pas dans le bloc CIDR du VPC/VNet de calcul, ou un service connu, via le réseau NSX-T Data Center (superposition)

Configurations de cloud public créées automatiquement

Dans vos clouds publics, certaines configurations sont définies automatiquement après le déploiement de PCG.

Configurations de cloud public dans les deux modes : Mode d'application NSX et Mode d'application du Cloud natif

Dans AWS :

- Dans le VPC AWS, un nouvel ensemble d'enregistrements de type A est ajouté sous le nom `nsx-gw.vmware.local` dans une zone hébergée privée sur Amazon Route 53. L'adresse IP mappée sur cet enregistrement correspond à l'adresse IP de gestion de la PCG qui est attribuée par AWS à l'aide de DHCP et qui est différente pour chaque VPC. NSX Cloud utilise cette entrée DNS définie dans la zone hébergée privée dans Amazon Route 53 pour résoudre l'adresse IP de la PCG.

Note Lorsque vous utilisez des noms de domaine DNS personnalisés définis dans une zone hébergée privée dans Amazon Route 53, les attributs **Résolution DNS** et **Noms d'hôte DNS** doivent être définis sur **Oui** pour les paramètres de VPC dans AWS.

- 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 le Mode d'application du Cloud natif :

Les groupes de sécurité suivants sont créés lorsque la PCG est déployée.

Une fois que les machines virtuelles de charge de travail sont mises en corrélation avec des groupes et des stratégies de sécurité correspondantes dans NSX Manager, des groupes de sécurité nommés `nsx-<GUID>` sont créés dans le cloud public pour chaque stratégie de sécurité correspondante.

Note Dans AWS, des groupes de sécurité sont créés. Dans Microsoft Azure, des groupes de sécurité d'application sont créés correspondant à des groupes dans NSX Manager, tandis que des groupes de sécurité réseau sont créés correspondant à des stratégies de sécurité dans NSX Manager.

Nom du groupe de sécurité	Disponible dans Microsoft Azure ?	Disponible dans AWS ?	Description
vm-quarantine-sg	Oui	Non	Groupe de sécurité créé par NSX Cloud dans Microsoft Azure pour attribution à des machines virtuelles qui ne correspondent pas à une stratégie de sécurité dans NSX-T.
default	Non	Oui	Groupe de sécurité préexistant dans AWS utilisé par NSX Cloud pour attribution à des machines virtuelles qui ne correspondent pas à une stratégie de sécurité dans NSX-T.
vm-overlay-sg	Oui	Oui	Groupe de sécurité réseau de superposition de VM (non utilisé dans la version actuelle)

Groupes de sécurité de cloud public créés par NSX Cloud pour les interfaces PCG lors de l'utilisation du Mode d'application NSX

Les groupes de sécurité **gw** sont appliqués aux interfaces PCG respectives.

Tableau 13-8. 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 ?	Description
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

Les groupes de sécurité suivants sont créés pour les machines virtuelles de charge de travail.

Tableau 13-9. Groupes de sécurité de cloud public créés par NSX Cloud pour les machines virtuelles de charge de travail dans le Mode d'application NSX

Nom du groupe de sécurité	Disponible dans Microsoft Azure ?	Disponible dans AWS ?	Description
vm-quarantine-sg	Oui	Non	Groupe de sécurité créé par NSX Cloud dans Microsoft Azure pour les workflows de détection des menaces dans le Mode d'application NSX
default	Non	Oui	Groupe de sécurité préexistant dans AWS utilisé par NSX Cloud pour les workflows de détection des menaces dans le Mode d'application NSX
vm-underlay-sg	Oui	Oui	Groupe de sécurité de non-superposition de machine virtuelle
vm-overlay-sg	Oui	Oui	Groupe de sécurité réseau de superposition de VM (non utilisé dans la version actuelle)

(Facultatif) Installez NSX Tools sur vos machines virtuelles de charge de travail.

Si vous utilisez le Mode d'application NSX, procédez à installation de NSX Tools dans vos machines virtuelles de charge de travail.

Reportez-vous aux instructions et à des informations complémentaires dans la section [Intégration des machines virtuelles en mode forcé NSX](#) du *Guide d'administration de NSX-T Data Center*.

Annuler le déploiement ou annuler le lien des PCG

Reportez-vous à cette présentation des étapes impliquées dans l'annulation du déploiement ou l'annulation du lien de PCG.

Dans le Mode d'application NSX

- Supprimez la balise `nsx.network=default` des machines virtuelles de charge de travail gérées par NSX.
- Désactivez la stratégie de mise en quarantaine si elle est activée dans le Mode d'application NSX.
- Fournissez un groupe de sécurité dans votre cloud public que NSX Cloud peut utiliser comme groupe de sécurité de secours.

- Supprimez toutes les entités logiques créées par l'utilisateur et associées à la PCG.

Dans le Mode d'application du Cloud natif

- Fournissez un groupe de sécurité dans votre cloud public que NSX Cloud peut utiliser comme groupe de sécurité de secours.
- Supprimez toutes les entités logiques créées par l'utilisateur et associées à la PCG.

Procédure

1 Supprimer la balise `nsx.network` 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, fournir un groupe de sécurité de secours

Dans les deux modes, Mode d'application NSX et Mode d'application du Cloud natif, vous devez préparer un nouveau groupe de sécurité ou un groupe de sécurité existant dans votre cloud public et le fournir comme groupe de sécurité de secours dans CSM pour poursuivre l'annulation du déploiement de PCG ou l'annulation du lien de VPC/VNet.

3 Supprimer les entités logiques créés par l'utilisateur

Toutes les entités logiques créées par l'utilisateur associées à la passerelle PCG doivent être supprimées.

4 Annuler le déploiement ou le lien de CSM

Suivez ces instructions pour annuler le déploiement ou le lien d'un PCG après avoir rempli les conditions préalables.

5 Dépannage lié à l'annulation du déploiement de PCG

Si l'annulation du déploiement de PCG échoue, vous devez supprimer manuellement toutes les entités créées par NSX Cloud dans NSX Manager et dans le cloud public.

Supprimer la balise `nsx.network` dans le cloud public

Avant que vous puissiez annuler le déploiement de PCG, toutes les machines virtuelles doivent être non gérées.

Note Cet onglet est uniquement applicable dans le Mode d'application NSX.

Accédez au VPC ou au VNet dans votre cloud public et supprimez la balise `nsx.network=default` des machines virtuelles gérées.

Désactiver la stratégie de mise en quarantaine, fournir un groupe de sécurité de secours

Dans les deux modes, Mode d'application NSX et Mode d'application du Cloud natif, vous devez préparer un nouveau groupe de sécurité ou un groupe de sécurité existant dans votre cloud

public et le fournir comme groupe de sécurité de secours dans CSM pour poursuivre l'annulation du déploiement de PCG ou l'annulation du lien de VPC/VNet.

Si vous utilisez le Mode d'application NSX, vous devez désactiver la stratégie de mise en quarantaine si celle-ci était précédemment activée.

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 [Entités logiques et groupes de sécurité cloud natifs créés automatiquement](#) pour obtenir la liste des groupes de sécurité NSX Cloud.

Dans AWS, vous pouvez configurer le groupe de sécurité `default` en tant que groupe de sécurité de secours, car il n'est pas créé par NSX Cloud.

Si vous avez déjà fourni un groupe de sécurité de secours, mais que vous avez annulé le lien d'un VPC/VNet de calcul et avez par la suite recréé un lien avec un VPC/VNet de transit, vous devez configurer un autre groupe de sécurité de secours.

Si la stratégie de mise en quarantaine est activée dans le Mode d'application NSX

Lorsque la stratégie de mise en quarantaine est activée, des groupes de sécurité définis par NSX Cloud sont attribués à vos machines virtuelles dans votre cloud public. 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.

Désactivez la stratégie de mise en quarantaine pour le VPC/VNet à partir duquel vous annulez le déploiement de PCG et fournissez l'ID du groupe de sécurité de secours :

- 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=default` de ces machines virtuelles pour les retirer de la gestion NSX, le groupe de sécurité de secours leur est également attribué.

En cas d'utilisation du Mode d'application du Cloud natif

Fournissez l'ID du groupe de sécurité de secours :

- Accédez au VPC ou VNet dans CSM.
- Cliquez sur **Actions > Modifier les configurations**
- Entrez l'ID du groupe de sécurité à partir d'AWS ou l'ID de ressource du groupe de sécurité réseau à partir de Microsoft Azure en tant que groupe de sécurité de secours auquel les machines virtuelles peuvent être attribuées après l'annulation du déploiement de PCG.

Note Pour les machines virtuelles sur liste blanche, NSX Cloud n'effectue aucune action et ne déplace donc pas les machines virtuelles vers le groupe de sécurité de secours. Si vous disposez d'une machine virtuelle sur liste blanche dans tous les groupes de sécurité attribués par NSX Cloud, vous devez la déplacer manuellement vers le groupe de sécurité de secours désigné. Reportez-vous à la section [Détection des menaces à l'aide de la stratégie de mise en quarantaine de NSX Cloud](#) du 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

Toutes les entités logiques créées par l'utilisateur associées à la passerelle PCG doivent être supprimées.

Identifiez des entités qui sont associées à PCG et supprimez-les.

Note Ne supprimez pas les entités logiques créées automatiquement. Elles sont supprimées automatiquement après que vous avez cliqué sur **Annuler le déploiement** ou **Supprimer le lien à partir du VPC/VNet de transit** de CSM. Reportez-vous à [Entités logiques et groupes de sécurité cloud natifs créés automatiquement](#) pour plus de détails.

Annuler le déploiement ou le lien de CSM

Suivez ces instructions pour annuler le déploiement ou le lien d'un PCG après avoir rempli les conditions préalables.

- 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 deux PCG sont déployés et en cours d'exécution.
 - Si vous utilisez Microsoft Azure, accédez à **Clouds > Azure > VNet**. Cliquez sur le VNet sur lequel un ou deux PCG sont déployés et en cours d'exécution.
- 2 Cliquez sur **Annuler le déploiement** ou **Supprimer le lien à partir du VPC/VNet de transit**.

Les entités par défaut créées par NSX Cloud sont supprimées automatiquement lorsque le déploiement ou le lien d'un PCG est annulé.

Dépannage lié à l'annulation du déploiement de PCG

Si l'annulation du déploiement de PCG échoue, vous devez supprimer manuellement toutes les entités créées par NSX Cloud dans NSX Manager et dans le cloud public.

- Dans votre cloud public :
 - Mettez fin à toutes les PCG dans le VPC/VNet de transit.
 - Déplacez toutes vos machines virtuelles de charge de travail vers un groupe de sécurité non créé par NSX Cloud.
 - Supprimez les groupes de sécurité créés par NSX Cloud dans le cloud public, comme indiqué ici : [Configurations de cloud public créées automatiquement](#) .
 - Pour Microsoft Azure, supprimez également le groupe de ressources créé par NSX Cloud nommé **nsx-gw-<vnet ID>-rg**.
- Resynchronisez votre inventaire de cloud public dans CSM.
- Supprimez les entités créées automatiquement avec l'ID VPC/VNet dans NSX Manager comme indiqué ici : [Entités logiques NSX-T créées automatiquement](#).

Note Ne supprimez pas les entités globales qui sont créées automatiquement. Supprimez uniquement celles dont le nom contient l'ID VPC/VNet.

Installation et configuration de NSX Intelligence

14

VMware NSX® Intelligence™ fournit une interface utilisateur graphique qui permet de visualiser la position de sécurité et les flux de trafic réseau qui sont survenus dans votre environnement NSX-T Data Center sur site.

NSX Intelligence est disponible pour les hôtes basés sur ESXi à partir de la version 2.5 de NSX-T Data Center. Il fournit les fonctionnalités suivantes.

- Visualisation graphique des composants de NSX-T, tels que les groupes, les machines virtuelles et les flux réseau, dans votre NSX-T Data Center. Les données utilisées sont basées sur les flux de réseau agrégés au cours de la période spécifiée.
- Recommandations concernant les stratégies de sécurité, les groupes de sécurité de stratégie et les services pour les applications. Les recommandations vous aident à mettre en œuvre la micro-segmentation au niveau de l'application. Elles vous permettent d'appliquer une stratégie de sécurité plus dynamique en mettant en corrélation les modèles de trafic de communication qui se produit entre les machines virtuelles dans votre environnement de centre de données NSX-T.

Vous pouvez utiliser NSX Intelligence si vous disposez d'une licence NSX-T Data Center Enterprise Plus ou pendant la période d'évaluation si vous disposez d'une licence d'évaluation de NSX-T Data Center.

Important Vous devez disposer d'un rôle d'administrateur d'entreprise pour avoir l'autorisation d'installer, de configurer et d'utiliser NSX Intelligence.

Le dispositif NSX Intelligence est disponible dans deux scénarios de déploiement différents. Un dispositif de petite taille est disponible pour un déploiement de laboratoire ou de validation technique, ou un environnement de production à petite échelle. Vous pouvez utiliser un dispositif de grande taille pour un environnement de production à grande échelle. Reportez-vous à la section [Configuration système requise pour NSX Intelligence](#).

Pour activer la fonctionnalité NSX Intelligence, vous devez installer le dispositif NSX Intelligence, qui est livré séparément du dispositif NSX-T Data Center. Vous utilisez l'interface utilisateur de NSX Manager pour installer le dispositif NSX Intelligence. Reportez-vous à la section [Installez le dispositif NSX Intelligence](#).

Après avoir installé et configuré le dispositif NSX Intelligence, vous accédez aux fonctionnalités de NSX Intelligence à l'aide de l'onglet **Planifier et dépanner > Découvrir et planifier** dans l'interface utilisateur de NSX Manager. Reportez-vous à la section « Démarrage de NSX Intelligence » dans le *Guide d'administration de NSX-T Data Center*.

Ce chapitre contient les rubriques suivantes :

- [Workflow d'installation et de configuration de NSX Intelligence](#)
- [Préparation à l'installation de NSX Intelligence](#)
- [Télécharger et décompresser le bundle du programme d'installation NSX Intelligence](#)
- [Installez le dispositif NSX Intelligence](#)
- [Dépannage lors de l'installation du dispositif NSX Intelligence](#)
- [Désinstaller le dispositif NSX Intelligence](#)

Workflow d'installation et de configuration de NSX Intelligence

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

Effectuez les procédures dans l'ordre dans lequel elles sont répertoriées.

- 1 Installez NSX-T Data Center 2.5 ou version ultérieure sur des hôtes basés sur ESXi. VMware NSX® Intelligence™ est pris en charge sur les hôtes basés sur ESXi uniquement. Reportez-vous à la section [Chapitre 2 Workflows d'installation de NSX-T Data Center](#).
- 2 Assurez-vous que la configuration système requise de NSX Intelligence est respectée. Reportez-vous à la section [Configuration système requise pour NSX Intelligence](#).
- 3 Synchronisez l'heure sur la machine virtuelle NSX Manager et sur le cluster de calcul sur lequel le dispositif NSX Intelligence doit être déployé.
- 4 Téléchargez le fichier TAR du programme d'installation de NSX Intelligence sur un serveur Web local. Ce fichier TAR contient le fichier OVF de NSX Intelligence que vous utilisez pour installer le dispositif NSX Intelligence. Reportez-vous à la section [Télécharger et décompresser le bundle du programme d'installation NSX Intelligence](#).
- 5 Installez le dispositif NSX Intelligence. Reportez-vous à la section [Installez le dispositif NSX Intelligence](#).
- 6 Pour activer l'interface utilisateur de NSX Intelligence dans l'interface utilisateur de NSX Manager, actualisez le navigateur Web que vous utilisez pour la session NSX Manager.
- 7 Commencez à utiliser les fonctionnalités de NSX Intelligence. Reportez-vous à la section « Démarrage de NSX Intelligence » dans le *Guide d'administration de NSX-T Data Center*.

Préparation à l'installation de NSX Intelligence

Vous devez préparer l'environnement de déploiement pour qu'il réponde à la configuration système requise minimale pour l'installation de NSX Intelligence.

Le tableau suivant décrit les exigences du déploiement, de la plate-forme et de l'installation de NSX Intelligence.

Exigences	Description
Méthode de déploiement prise en charge	<p>OVF déployé à l'aide de NSX Manager sur le VMware vCenter Server™ qui a été ajouté en tant que gestionnaire de calcul.</p> <hr/> <p>Important Le dispositif NSX Intelligence ne peut être installé qu'à l'aide de NSX Manager et n'est pas pris en charge lorsqu'OVF est installé de manière indépendante.</p>
Plateforme prise en charge	Hôtes ESXi Géré par vCenter Server
Adresse IP	Un dispositif NSX Intelligence doit posséder une adresse IP statique. Vous ne pouvez pas modifier l'adresse IP après l'installation.
Mot de passe du dispositif NSX Intelligence	<ul style="list-style-type: none"> ■ Au moins 12 caractères ■ Au moins une lettre minuscule ■ Au moins une lettre majuscule ■ Au moins un chiffre ■ Au moins un caractère spécial ■ Au moins cinq caractères différents ■ Aucun mot issu du dictionnaire ■ Aucun palindrome ■ Plus de quatre séquences de caractères monotones ne sont pas autorisées.
VMware Tools	VMTools est installé sur la machine virtuelle NSX Intelligence exécutée sur un hôte ESXi. Ne supprimez pas VMTools.
Système	<ul style="list-style-type: none"> ■ Vérifiez que la configuration requise est respectée. Reportez-vous à la section Configuration système requise pour NSX Intelligence. ■ Vérifiez que les ports requis sont ouverts. Reportez-vous à la section Ports TCP et UDP utilisés par NSX Intelligence. ■ Obtenez les informations de l'adresse IP du sous-réseau et de la passerelle de gestion, de l'adresse IP du serveur DNS et de l'adresse IP du serveur NTP que le dispositif NSX Intelligence doit utiliser. ■ Vérifiez qu'une banque de données basée sur SSD est configurée et accessible au dispositif NSX Intelligence.

Configuration système requise pour NSX Intelligence

Avant d'installer le dispositif NSX Intelligence, assurez-vous que votre environnement répond à la configuration système minimale prise en charge pour l'hôte serveur sur lequel vous prévoyez d'installer le dispositif et le client sur lequel les visualisations de VM s'affichent.

Configuration requise des ressources du dispositif NSX Intelligence

Le tableau suivant répertorie les tailles de dispositif NSX Intelligence disponibles et la ressource de VM requise pour chacune d'elles. La taille de dispositif Petite VM de NSX Intelligence est adaptée aux déploiements de laboratoire et de validation technique ou à un environnement de production à petite échelle. La taille de dispositif Grande VM de NSX Intelligence est adaptée aux environnements de production.

Taille du dispositif	Mémoire	vCPU	Espace disque
Petit NSX Intelligence	64 Go	16	2 To
NSX Intelligence grand	128 Go	32	2 To

Note Un seul dispositif NSX Intelligence est pris en charge par cluster NSX Manager.

Mémoire de client Web, CPU et navigateur requis pour NSX Intelligence

Pour des performances optimales, votre système client doit disposer d'au moins deux cœurs de CPU de 1,4 GHz et d'au moins 16 Go de RAM.

Le tableau suivant répertorie les versions de navigateur Web prises en charge pour NSX Intelligence. La résolution de navigateur minimale prise en charge est de 1 280 x 800 pixels.

Navigateur	Windows 10	Mac OS X 10.14, 10.13	Ubuntu 18.4
Chrome 76	Oui	Oui	Oui
Firefox 68	Oui	Oui	Oui
Microsoft Edge 44	Oui	S/O	S/O

Note Il existe des problèmes de performance connus lors de l'utilisation de Microsoft Edge. Pour plus d'informations, reportez-vous à la section *Notes de mise à jour de NSX-T Data Center*.

Ports TCP et UDP utilisés par NSX Intelligence

NSX Intelligence utilise certains ports TCP et UDP pour communiquer avec d'autres composants et produits. Ces ports doivent être ouverts sur les pare-feu d'hyperviseur physique et hôte.

Important Pour obtenir l'accès au nœud NSX Intelligence, vous devez activer SSH sur ce nœud.

Tableau 14-1. Ports TCP et UDP utilisés par NSX Intelligence

Source	Cible	Port	Protocole	Description
NSX Intelligence	Serveurs DNS	53	TCP	DNS
NSX Intelligence	Serveurs DNS	53	UDP	DNS
NSX Intelligence	Serveurs SCP de gestion	22	TCP	SSH (télécharger le bundle de support, sauvegardes, etc.)
NSX Intelligence	Serveurs NTP	123	UDP	NTP
NSX Intelligence	vCenter Server/NSX Unified Appliance	443	TCP	NSX Intelligence avec les communications du gestionnaire de calcul (vCenter Server) et de NSX Unified Appliance, lorsque configuré.
NSX Intelligence	NSX Unified Appliance/Nœuds de transport NSX	9092	TCP	Communication sortante de NSX Intelligence vers NSX Unified Appliance ou des nœuds de transport
Serveurs NTP	NSX Intelligence	123	UDP	NTP
Clients de gestion	NSX Intelligence	22	TCP	SSH (désactivé par défaut)
Clients de gestion/NSX Unified Appliance	NSX Intelligence	443	TCP	Serveur NSX API
NSX Unified Appliance/Nœuds de transport	NSX Intelligence	9092	TCP	Messages entrants de NSX Unified Appliance ou des nœuds de transport vers le dispositif NSX Intelligence

Télécharger et décompresser le bundle du programme d'installation NSX Intelligence

Pour installer le dispositif NSX Intelligence, téléchargez le fichier du bundle de programme d'installation de NSX Intelligence sur un serveur Web local et décompressez-le. Le fichier du bundle contient le fichier OVF et d'autres fichiers de support utilisés pour l'installation du dispositif NSX Intelligence.

Conditions préalables

- Vérifiez que vous êtes autorisé à utiliser NSX Intelligence. Vous pouvez utiliser NSX Intelligence si vous disposez d'une licence NSX-T Data Center Enterprise Plus ou pendant la période d'évaluation si vous disposez d'une licence d'évaluation de NSX-T Data Center.
- Vous devez disposer d'un rôle d'administrateur d'entreprise pour installer, configurer et utiliser NSX Intelligence.
- Vérifiez que l'utilisateur effectuant le téléchargement dispose des autorisations appropriées pour télécharger et extraire le contenu du fichier .tar sur un serveur Web local.
- Assurez-vous que le serveur Web local, que vous prévoyez d'utiliser pour télécharger le fichier du bundle du programme d'installation NSX Intelligence, utilise le port par défaut 80 pour HTTP.

Procédure

- 1 Localisez le fichier TAR du programme d'installation NSX Intelligence sur le portail de téléchargement de VMware.
- 2 Téléchargez et enregistrez le fichier du bundle de programme d'installation NSX Intelligence dans un emplacement de serveur Web local accessible à partir de l'interface utilisateur de NSX Manager.

Note Le serveur Web actuellement pris en charge est IIS pour Windows et Apache pour Linux ou Mac OS. Vous pouvez utiliser un autre serveur Web de votre choix, mais IIS et Apache sont les serveurs Web testés et pris en charge pour ces systèmes d'exploitation.

Le nom de fichier du bundle de programme d'installation présente le format suivant : `VMware-NSX-Intelligence-appliance-<release-number>.<build-number>.tar`. Par exemple, `VMware-NSX-Intelligence-appliance-1.0.0.0.14303803.tar`.

3 Extrayez le contenu du fichier TAR dans le même emplacement que le serveur Web local.

- a Pour décompresser le contenu du fichier TAR sur l'un des serveurs Web pris en charge, utilisez les informations suivantes.

Système d'exploitation	Serveur Web	Déballage de l'outil à utiliser
Windows	IIS	<p>Application 7-Zip</p> <p>Utilisez l'interface utilisateur de 7-Zip File Manager ou une fenêtre d'invite de commande. Par exemple, pour utiliser une fenêtre d'invite de commande pour décompresser le fichier TAR modèle, accédez à l'emplacement où se trouve le fichier TAR NSX Intelligence téléchargé et entrez la commande suivante.</p> <pre>7z x VMware-NSX-Intelligence-appliance-1.0.0.0.14303803.tar</pre>
Linux	Apache	<p>Utilitaire de ligne de commande tar</p> <p>Par exemple, pour décompresser le fichier TAR modèle, entrez ce qui suit à partir d'une invite de commande.</p> <pre>tar -xvf VMware-NSX-Intelligence-appliance-1.0.0.0.14303803.tar</pre>
Mac OS	Apache	<p>Utilitaire de ligne de commande tar</p> <p>Par exemple, pour décompresser le fichier TAR, entrez ce qui suit à partir d'une ligne de commande Terminal.</p> <pre>tar -xvf VMware-NSX-Intelligence-appliance-1.0.0.0.14303803.tar</pre>

À l'aide du nom de fichier du bundle modèle de l'étape précédente, le contenu extrait doit inclure les lignes suivantes :

- nsx-intelligence-appliance-1.0.0.0.14303803.cert
 - nsx-intelligence-appliance-1.0.0.0.14303803.mf
 - nsx-intelligence-appliance-1.0.0.0.14303803.ovf
 - nsx-intelligence-appliance.vmdk
- b Avant de poursuivre l'installation, assurez-vous que les sommes de contrôle des fichiers décompressés sont identiques à celles indiquées dans le fichier manifeste.
- ### 4 Utilisez les informations suivantes pour vérifier que le serveur Web que vous utilisez est configuré pour le type MIME à utiliser pour chaque type de fichier du programme d'installation de NSX Intelligence. Si nécessaire, mettez à jour manuellement votre serveur Web.

Type de fichier du programme d'installation NSX Intelligence	Type MIME
.ovf	application/vmware
.vmdk	application/octet-stream

Type de fichier du programme d'installation NSX Intelligence	Type MIME
.mf	text/cache-manifest
.cert	application/x-x509-user-cert

- 5 Copiez le chemin d'accès au fichier OVF de NSX Intelligence. Par exemple, `http://local-web-server/nsx-intelligence-appliance-1.0.0.0.14303803.ovf`. Vous fournissez ce chemin pendant le processus d'installation du dispositif NSX Intelligence.

Étape suivante

Poursuivez l'installation du dispositif NSX Intelligence. Reportez-vous à la section [Installez le dispositif NSX Intelligence](#).

Installez le dispositif NSX Intelligence

Vous utilisez l'interface utilisateur de NSX Manager pour installer et configurer le dispositif NSX Intelligence.

Avant de pouvoir commencer à utiliser les fonctionnalités de NSX Intelligence, vous devez installer et configurer le dispositif NSX Intelligence pour intégrer les services et les plug-ins NSX Intelligence à NSX Manager.

Conditions préalables

- Vérifiez que NSX-T Data Center 2.5 ou version ultérieure est installé. Reportez-vous à la section [Chapitre 2 Workflows d'installation de NSX-T Data Center](#).
- Vous devez disposer d'un rôle d'administrateur d'entreprise pour installer, configurer et utiliser NSX Intelligence.
- Localisez le fichier du bundle de programme d'installation de NSX Intelligence sur le portail de téléchargement de VMware et téléchargez-le sur un serveur Web local. Reportez-vous à la section [Télécharger et décompresser le bundle du programme d'installation NSX Intelligence](#).
- Assurez-vous que le serveur Web local qui contient le fichier du bundle du programme d'installation NSX Intelligence utilise le port par défaut 80 pour HTTP.
- Déterminez la taille du dispositif NSX Intelligence à configurer. Un dispositif de petite taille est adapté à un déploiement de laboratoire ou de preuve de concept, ou à un environnement de production à petite échelle. La taille Grand est adaptée à un environnement de production à grande échelle.
- Vérifiez que la configuration système requise de NSX Intelligence est respectée pour la taille du dispositif que vous voulez installer. Reportez-vous à la section [Configuration système requise pour NSX Intelligence](#).
- Synchronisez l'heure sur le cluster de calcul, sur lequel le dispositif NSX Intelligence doit être déployé, avec le serveur NSX Manager.

- Obtenez les adresses IP du sous-réseau de gestion, la passerelle, le serveur DNS et le serveur NTP qui sont nécessaires à la configuration du dispositif NSX Intelligence.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur d'entreprise à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Dans NSX Manager, sélectionnez **Système > Dispositifs**.
- 3 Faites défiler le volet Présentation des dispositifs vers le bas pour localiser la carte du dispositif NSX Intelligence et cliquez sur **Ajouter un dispositif NSX Intelligence**.
- 4 Dans l'assistant Ajouter un dispositif, entrez les détails du dispositif NSX Intelligence.

Élément de détail	Action à prendre
Fichier OVF	Entrez l'URL du fichier OVF NSX Intelligence que vous avez téléchargé sur votre serveur Web local. Par exemple, http://localhost/nsx-intelligence-appliance-1.1.0.0.13912394.ovf .
Nom	Entrez un nom pour le dispositif NSX Intelligence. Cette valeur peut être un nom de domaine complet ou un nom simple, tel que mytest-lab .
Sous-réseau de gestion	Entrez l'adresse IP, y compris la plage, à utiliser pour le dispositif NSX Intelligence. Par exemple, 10.11.22.33/24
Adresse IP de la passerelle	Entrez une adresse IP de passerelle que le dispositif NSX Intelligence utilisera.
Serveur DNS	Entrez une ou plusieurs adresses IP du serveur DNS.
Serveur NTP	Entrez une ou plusieurs adresses IP du serveur NTP.
Taille du nœud	Sélectionnez la taille du dispositif NSX Intelligence à configurer. Un dispositif de petite taille peut être utilisé pour un environnement de laboratoire ou de validation technique, ou un environnement de production à petite échelle. La taille de dispositif Grand est adaptée à un environnement de production à grande échelle.

- 5 Cliquez sur **Suivant**.
- 6 Entrez les détails de l'emplacement de déploiement du dispositif NSX Intelligence.

Élément de détail	Action à prendre
Gestionnaire de calcul	Dans le menu déroulant, sélectionnez le gestionnaire de calcul sur lequel installer le dispositif NSX Intelligence.
Cluster	Utilisez le menu déroulant pour sélectionner le cluster à utiliser.
Pool de ressources	(Facultatif) Sélectionnez le pool de ressources dans le menu déroulant.

Élément de détail	Action à prendre
Hôte	<p>(Facultatif) Sélectionnez l'hôte dans le menu déroulant. Si vous utilisez un cluster avec plusieurs nœuds de transport, choisissez le nœud de transport à utiliser.</p> <hr/> <p>Note La sélection explicite d'un hôte remplace la vérification du nombre de vCPU. Assurez-vous que l'hôte sélectionné dispose d'un nombre suffisant de vCPU pour prendre en charge la taille du dispositif NSX Intelligence que vous installez. Sinon, le dispositif NSX Intelligence résultant peut présenter une configuration incorrecte. En cas de doute, laissez la zone de texte vide ; l'hôte approprié est alors sélectionné automatiquement.</p>
Banque de données	Dans le menu déroulant, sélectionnez la banque de données sur laquelle stocker la configuration et les données de NSX Intelligence.
Réseau	Sélectionnez le réseau à utiliser dans le menu déroulant.
Activer SSH et Activer l'accès à la racine	<p>Spécifiez si vous voulez activer un accès SSH ou un accès racine à l'interface de ligne de commande du dispositif NSX Intelligence.</p> <p>Par défaut, ces options sont désactivées pour des raisons de sécurité. Vous utilisez l'interface de ligne de commande pour configurer un serveur de fichiers de sauvegarde, sauvegarder la configuration du dispositif NSX Intelligence et restaurer la sauvegarde.</p>

7 Cliquez sur **Suivant**.

8 Configurez les informations d'identification administratives et l'accès au dispositif NSX Intelligence.

- Si vous avez activé un accès racine, définissez le mot de passe racine. Utilisez les exigences de mot de passe affichées sur l'interface utilisateur.
- Configurez les informations d'identification CLI et les informations d'identification CLI d'audit. Sélectionnez **Identique au mot de passe racine** si vous souhaitez utiliser le mot de passe racine pour le mot de passe CLI ou le mot de passe de CLI d'audit. Sinon, entrez les mots de passe dans **Mot de passe CLI** et **Mot de passe CLI d'audit**.

9 Cliquez sur **Installer le dispositif**.

La progression de l'installation est affichée dans l'onglet **Planifier et dépanner**. L'installation peut prendre entre 5 et 30 minutes, car le programme d'installation découvre tous les services et les plug-ins requis par le dispositif NSX Intelligence.

Note Si une erreur est signalée, utilisez les informations fournies dans les messages d'erreur pour résoudre le problème signalé. Une fois le problème résolu, vous devez d'abord désinstaller le dispositif NSX Intelligence et essayer de le réinstaller à partir de l'onglet **Système > Dispositifs**. Reportez-vous à la section [Désinstaller le dispositif NSX Intelligence](#) ou [Dépannage lors de l'installation du dispositif NSX Intelligence](#) pour obtenir des conseils sur la résolution des problèmes que vous avez pu rencontrer.

- 10 Une fois le dispositif NSX Intelligence correctement installé, cliquez sur **Actualiser pour afficher**.

L'interface utilisateur de NSX Manager est actualisée avec les fonctionnalités de NSX Intelligence activées dans l'onglet **Planifier et dépanner > Découvrir et planifier**.

Étape suivante

Commencez à utiliser les fonctionnalités de NSX Intelligence. Reportez-vous à la section « Utilisation de NSX Intelligence » dans le *Guide d'administration de NSX-T Data Center*.

Dépannage lors de l'installation du dispositif NSX Intelligence

Cette section fournit des informations pour résoudre les problèmes que vous pouvez rencontrer lors de l'installation du dispositif NSX Intelligence.

Les informations d'identification étaient incorrectes ou le compte fourni a été verrouillé

Une tentative de déploiement du dispositif NSX Intelligence a généré le message d'erreur Les informations d'identification étaient incorrectes ou le compte spécifié a été verrouillé.

Problème

Une fois le programme d'installation du dispositif NSX Intelligence exécuté, le message d'erreur Les informations d'identification étaient incorrectes ou le compte spécifié a été verrouillé s'affiche lorsque le programme d'installation tentait d'enregistrer le serveur NSX Intelligence avec NSX Manager

Cause

L'étape d'enregistrement a peut-être échoué pour l'une des raisons suivantes.

- Le jeton du plan de gestion a peut-être expiré. Le jeton n'est valide que pendant 30 minutes.
- L'heure système n'est pas synchronisée entre l'hôte serveur NSX Intelligence et l'hôte NSX Manager.

Solution

- 1 Assurez-vous que l'heure système est synchronisée entre l'hôte serveur NSX Intelligence et l'hôte NSX Manager.
- 2 Si les heures système sont synchronisées, vérifiez l'existence d'une latence réseau.
- 3 Supprimez le dispositif NSX Intelligence et réessayez de l'installer après la synchronisation des heures système ou lorsque la latence du réseau est résolue.

Le message d'état de déploiement du dispositif ayant échoué n'est pas effacé

Le déploiement du dispositif NSX Intelligence a réussi, mais l'état Échec de déploiement du dispositif demeure affiché.

Problème

Lorsque la tentative initiale de déploiement du dispositif NSX Intelligence échoue, par exemple en raison d'un problème d'insuffisance des ressources, le message d'état de déploiement ayant échoué n'est pas effacé même après la résolution du problème signalé.

Cause

Lorsque la cause principale sous-jacente du problème de déploiement signalé a été résolue, le dispositif NSX Intelligence n'en a pas connaissance, car la résolution est effectuée à l'extérieur du dispositif NSX Intelligence.

Solution

- 1 Après avoir résolu le problème signalé lors de la tentative précédente de déploiement du dispositif, désinstallez le dispositif NSX Intelligence.
- 2 Tentative de réinstallation du dispositif NSX Intelligence à partir de l'onglet **Système > Dispositifs**
- 3 (Facultatif) Pour connaître l'état de déploiement mis à jour du dispositif NSX Intelligence, actualisez votre navigateur Web.

Désinstaller le dispositif NSX Intelligence

Si vous voulez désinstaller complètement NSX Intelligence, procédez comme suit.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur d'entreprise à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Dans l'interface utilisateur de NSX Manager, sélectionnez **Système > Dispositifs**.
- 3 Localisez la carte du dispositif NSX Intelligence.
- 4 Cliquez sur **Supprimer**.
- 5 Dans la boîte de dialogue Confirmer la suppression du dispositif, cliquez sur **Confirmer**.

Dépannage des problèmes d'installation

15

Liste des problèmes liés à l'installation et à la configuration de NSX-T Data Center

Problème	Solution
Les hôtes vCenter Server et/ou ESXi affichent des réseaux opaques après la suppression de NSX-T d'un hôte ou d'un cluster	https://kb.vmware.com/s/article/75234
Échec de l'installation en raison d'un espace insuffisant dans bootbank sur l'hôte ESXi	https://kb.vmware.com/s/article/74864

Ce chapitre contient les rubriques suivantes :

- [Échec de la l'installation en raison d'un espace insuffisant dans bootbank sur l'hôte ESXi](#)

Échec de la l'installation en raison d'un espace insuffisant dans bootbank sur l'hôte ESXi

L'installation de NSX-T Data Center peut échouer si l'espace est insuffisant dans bootbank ou dans alt-bootbank sur un hôte ESXi.

Problème

Sur l'hôte ESXi, vous pouvez voir un message de journal (esxupdate.log) similaire :

```
20**_**_**T13:37:50Z esxupdate: 5557508: BootBankInstaller.pyc:
ERROR: The pending transaction requires 245 MB free space,
however the maximum supported size is 239 MB.^@
```

Cause

Les VIB inutilisés sur l'hôte ESXi peuvent être d'une taille relativement grande. Ces VIB inutilisés peuvent entraîner un espace insuffisant dans bootbank ou dans alt-bootbank lors de l'installation des VIB requis.

Solution

- Désinstallez les VIB inutiles et libérez de l'espace disque supplémentaire.

Pour plus d'informations sur la suppression des VIB inutilisés, consultez l'article de la base de connaissances VMware à l'adresse <https://kb.vmware.com/s/article/74864>.