

Guide d'administration de NSX-T Data Center

Modifié le 24 mai 2019
VMware NSX-T Data Center 2.3



vmware®

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

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

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

docfeedback@vmware.com

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

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

Copyright © 2018, 2019 VMware, Inc. Tous droits réservés. [Informations relatives aux copyrights et marques commerciales.](#)

Table des matières

À propos de l'administration de VMware NSX-T Data Center	9
1 Commutateurs logiques et configuration d'un attachement de VM	10
Comprendre les modes de réplication de trame BUM	11
Créer un commutateur logique	13
Pontage de couche 2	14
Créer un cluster de pont	16
Créer un profil de pont	17
Créer un commutateur logique sauvegardé par pont de couche 2	17
Créer un commutateur logique VLAN pour la liaison montante NSX Edge	19
Connexion d'une machine virtuelle à un commutateur logique	21
Attacher une VM hébergée sur vCenter Server à un commutateur logique NSX-T Data Center	21
Attacher une machine virtuelle autonome hébergée sur un hôte ESXi autonome à un commutateur logique NSX-T Data Center	23
Attacher une VM hébergée sur KVM à un commutateur logique NSX-T Data Center	28
Tester la connectivité de couche 2	29
2 Port de commutateur logique	33
Créer un port de commutateur logique	33
Surveiller l'activité d'un port de commutateur logique	34
3 Basculement des profils pour commutateurs logiques et ports logiques	36
Comprendre le profil de commutation QoS	37
Configurer un profil de commutation QoS personnalisé	38
Comprendre le profil de commutation de découverte d'adresses IP	40
Configurer un profil de commutation de découverte d'adresses IP	41
Comprendre SpoofGuard	42
Configurer des liaisons d'adresse de port	43
Configurer un profil de commutation SpoofGuard	43
Comprendre le profil de commutation de sécurité de commutateur	44
Configurer un profil de commutation de sécurité de commutateur personnalisé	44
Comprendre le profil de commutation de gestion MAC	46
Configurer le profil de commutation de gestion MAC	46
Associer un profil personnalisé à un commutateur logique	47
Associer un profil personnalisé à un port logique	48
4 Routeur logique de niveau 1	50
Créer un routeur logique de niveau 1	51

- Ajouter un port de liaison descendante sur un routeur logique de niveau 1 52
- Ajouter un port VLAN sur un routeur logique de niveau 0 ou de niveau 1 53
- Configurer l'annonce d'itinéraires sur un routeur logique de niveau 1 54
- Configurer l'itinéraire statique d'un routeur logique de niveau 1 56
- Créer un routeur logique de niveau 1 autonome 58

5 Routeur logique de niveau 0 60

- Créer un routeur logique de niveau 0 62
- Attacher le niveau 0 et le niveau 1 63
 - Vérifier qu'un routeur de niveau 0 a appris des itinéraires d'un routeur de niveau 1 65
- Connecter un routeur logique de niveau 0 à un commutateur logique VLAN pour la liaison montante NSX Edge 66
 - Vérifier le routeur logique de niveau 0 et la connexion ToR 68
- Ajouter un port de routeur de bouclage 70
- Ajouter un port VLAN sur un routeur logique de niveau 0 ou de niveau 1 70
- Configurer un itinéraire statique 71
 - Vérifier l'itinéraire statique 73
- Options de configuration de BGP 75
 - Configurer BGP sur un routeur logique de niveau 0 77
 - Vérifier les connexions BGP à partir d'un routeur de service de niveau 0 79
- Configurer BFD sur un routeur logique de niveau 0 80
- Activer la redistribution d'itinéraire sur le routeur logique de niveau 0 81
 - Vérifier la connectivité nord-sud et la redistribution d'itinéraires 82
- Comprendre le routage ECMP 84
 - Ajouter un port de liaison montante pour le second nœud Edge 85
 - Ajouter un second voisin BGP et activer le routage ECMP 86
 - Vérifier la connectivité du routage ECMP 87
- Créer une liste de préfixes IP 89
- Créer une liste de communauté 90
- Créer une carte de route 90
- Configurer le temporisateur d'activation du transfert 91

6 Traduction d'adresse réseau 93

- NAT de niveau 1 94
 - Configurer la NAT source sur un routeur de niveau 1 94
 - Configurer la NAT de destination sur un routeur de niveau 1 96
 - Annoncer des itinéraires NAT de niveau 1 au routeur de niveau 0 en amont 98
 - Annoncer des itinéraires NAT de niveau 1 à l'architecture physique 99
 - Vérifier la NAT de niveau 1 100
- NAT de niveau 0 101
 - Configurer la NAT source et de destination sur un routeur de niveau 0 101
- NAT réflexive 102

[Configurer une NAT réflexive sur un routeur logique de niveau 0 ou 1](#) 104

7 Sections de pare-feu et règles de pare-feu 106

- [Ajouter une section de règles de pare-feu](#) 107
- [Supprimer une section de règles de pare-feu](#) 108
- [Activer et désactiver des règles de section](#) 108
- [Activer et désactiver des journaux de sections](#) 109
- [À propos des règles de pare-feu](#) 109
- [Ajouter une règle de pare-feu](#) 111
- [Suppression d'une règle de pare-feu](#) 113
- [Modifier la règle du pare-feu distribué par défaut](#) 113
- [Modifier l'ordre d'une règle de pare-feu](#) 114
- [Filtrer les règles de pare-feu](#) 115
- [Configurer le pare-feu pour un port de pont de commutateur logique](#) 115
- [Configurer une liste d'exclusion de pare-feu](#) 116
- [Activer et désactiver le pare-feu](#) 116
- [Ajouter ou supprimer une règle de pare-feu à un routeur logique](#) 117

8 Réseaux privés virtuels 118

- [Configuration du VPN IPSec](#) 119
- [Configuration de VPN L2](#) 122

9 Gestion d'objets, de groupes, de services et de machines virtuelles 124

- [Créer un ensemble d'adresses IP](#) 124
- [Créer un pool d'adresses IP](#) 125
- [Créer un ensemble d'adresses MAC](#) 125
- [Créer un NSGroup](#) 126
- [Configuration de services et de groupes de services](#) 128
 - [Créer un NSService](#) 128
- [Gérer les balises d'une machine virtuelle](#) 129

10 Équilibrage de charge logique 130

- [Concepts clés de l'équilibrage de charge](#) 131
 - [Évolutivité des ressources d'équilibrage de charge](#) 131
 - [Fonctionnalités d'équilibrage de charge prises en charge](#) 132
 - [Topologies d'équilibrage de charge](#) 133
- [Configuration des composants d'équilibrage de charge](#) 134
 - [Créer un équilibrage de charge](#) 135
 - [Configurer un moniteur de santé actif](#) 136
 - [Configurer les moniteurs de santé passifs](#) 140
 - [Ajouter un pool de serveurs pour l'équilibrage de charge](#) 141

[Configuration des composants de serveur virtuel](#) 145

11 DHCP 167

[Créer un profil de serveur DHCP](#) 167

[Créer un serveur DHCP](#) 168

[Attacher un serveur DHCP à un commutateur logique](#) 169

[Détacher un serveur DHCP d'un commutateur logique](#) 169

[Créer un profil de relais DHCP](#) 169

[Créer un service de relais DHCP](#) 170

[Ajouter un service DHCP à un port de routeur logique](#) 170

12 Proxys de métadonnées 172

[Ajouter un serveur proxy de métadonnées](#) 172

[Attacher un serveur proxy de métadonnées à un commutateur logique](#) 174

[Détacher un serveur proxy de métadonnées d'un commutateur logique](#) 174

13 Gestion des adresses IP 176

[Gérer des blocs d'adresses IP](#) 176

[Gérer des sous-réseaux pour des blocs d'adresses IP](#) 177

14 Stratégie NSX 178

[Présentation](#) 178

[Ajouter un point d'application](#) 179

[Ajouter un service](#) 180

[Ajouter un domaine](#) 181

[Configurer la sauvegarde de NSX Policy Manager](#) 182

[Sauvegarder l'instance de NSX Policy Manager](#) 182

[Restaurer NSX Policy Manager](#) 183

[Associer un hôte vIDM avec NSX Policy Manager](#) 184

[Gérer les attributions de rôles](#) 185

15 Insertion de services 187

[Présentation](#) 187

[Enregistrer un service](#) 188

[Déployer une instance de service](#) 190

[Configurer la redirection du trafic](#) 191

[Surveiller la redirection du trafic](#) 191

16 NSX Cloud 193

[Cloud Service Manager](#) 193

[Clouds](#) 194

- Système 201
- Gérer la stratégie de mise en quarantaine 203
 - Comment activer ou désactiver la stratégie de mise en quarantaine 204
 - Impact de la stratégie de mise en quarantaine lorsqu'elle est désactivée 205
 - Impact de la stratégie de mise en quarantaine lorsqu'elle est activée 206
 - Groupes de sécurité NSX Cloud pour le cloud public 208
- Présentation de l'intégration et la gestion des machines virtuelles de charge de travail 209
 - Systèmes d'exploitation pris en charge 209
 - Comment intégrer les machines virtuelles de charge de travail à partir de Microsoft Azure 210
 - Comment intégrer des machines virtuelles de charge de travail à partir d'AWS 211
- Intégrer les machines virtuelles de charge de travail 212
 - Baliser des machines virtuelles dans le cloud public 213
 - Installer NSX Agent 213
 - Installer Agent NSX automatiquement 218
- Gérer les machines virtuelles de charge de travail 220
 - Accéder aux machines virtuelles de charge de travail gérées 220
 - Regrouper les machines virtuelles à l'aide de NSX-T Data Center et de balises de cloud public 221
 - Configurer la microsegmentation pour les machines virtuelles de charge de travail 224
 - Comment utiliser des fonctionnalités NSX-T Data Center avec le cloud public 225
- Utilisation des fonctionnalités avancées de NSX Cloud 229
 - Activer le transfert Syslog 229
- Dépannage 229
 - Vérifier les composants de NSX Cloud 229
 - FAQ de dépannage 230
- 17 Opérations et gestion 232**
 - Ajouter une clé de licence 233
 - Gestion des comptes d'utilisateur et du contrôle d'accès basé sur les rôles 233
 - Modifier le mot de passe de l'utilisateur de l'interface de ligne de commande 234
 - Paramètres de stratégie d'authentification 234
 - Obtenir l'empreinte numérique de certificat à partir d'un hôte vIDM 235
 - Associer un hôte vIDM à NSX-T 236
 - Synchronisation de l'heure entre NSX Manager, vIDM et les composants associés 237
 - Contrôle d'accès basé sur les rôles 238
 - Gérer les attributions de rôles 244
 - Afficher des identités de principal 244
 - Configuration de certificats 245
 - Créer un fichier de demande de signature de certificat 245
 - Importer un certificat d'autorité de certification 247
 - Importer un certificat 247
 - Créer un certificat auto-signé 248

Remplacer un certificat	249
Importer une liste de révocation des certificats	249
Importer un certificat pour une demande de signature de certificat	250
Configuration de dispositifs	251
Ajouter un gestionnaire de calcul	252
Gérer les balises	253
Rechercher des objets	254
Rechercher l'empreinte digitale SSH d'un serveur distant	255
Sauvegarde et restauration de NSX Manager	256
Sauvegarder la configuration de NSX Manager	257
Restauration de la configuration de NSX Manager	259
Restaurer un cluster NSX Controller	263
Gestion de dispositifs et de clusters de dispositifs	265
Gestion de NSX Manager	265
Gérer le cluster NSX Controller	266
Gérer le cluster NSX Edge	272
Messages de journal	278
Configurer la journalisation à distance	279
ID de messages de journal	281
Configurer IPFIX	282
Configurer des profils IPFIX de commutateur	283
Configurer des collecteurs IPFIX de pare-feu	284
Modèles IPFIX ESXi	285
Modèles IPFIX KVM	290
Suivre le chemin d'un paquet avec Traceflow	450
Afficher les informations de connexion du port	452
Surveiller l'activité d'un port de commutateur logique	452
Surveiller des sessions de mise en miroir de ports	453
Surveiller les nœuds d'infrastructure	456
Afficher des données sur les applications exécutées sur des machines virtuelles	456
Collecte des bundles de support	457
Programme d'amélioration du produit	458
Modifier la configuration du Programme d'amélioration du produit	458

À propos de l'administration de VMware NSX-T Data Center

Le *Guide d'administration de NSX-T Data Center* traite de la configuration et de la gestion réseau de VMware NSX-T™ Data Center. Il indique notamment comment créer des commutateurs et des ports logiques, et comment configurer la mise en réseau de routeurs logiques en niveaux. Il décrit également la façon de configurer NAT, les pare-feu, SpoofGuard, le groupement et DHCP.

Public visé

Ces informations sont destinées à toutes les personnes qui souhaitent configurer NSX-T Data Center. Elles sont destinées aux administrateurs Windows ou Linux expérimentés qui maîtrisent les technologies de machine virtuelle, la mise en réseau et les opérations de sécurité.

Glossaire VMware Technical Publications

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

Commutateurs logiques et configuration d'un attachement de VM

1

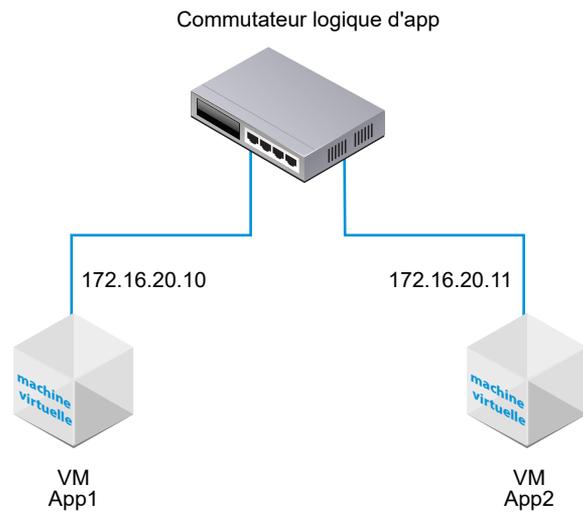
Un commutateur logique NSX-T Data Center reproduit la fonctionnalité de commutation, le trafic de diffusion, monodiffusion inconnue et multidiffusion (BUM), dans un environnement virtuel complètement dissocié du matériel sous-jacent.

Remarques concernant NSX Cloud Si vous utilisez NSX Cloud, reportez-vous à la section [Comment utiliser des fonctionnalités NSX-T Data Center avec le cloud public](#) pour obtenir la liste des entités logiques générées automatiquement, les fonctionnalités prises en charge et les configurations requises pour NSX Cloud.

Les commutateurs logiques sont semblables aux VLAN en ce qu'ils fournissent des connexions réseau auxquelles vous pouvez associer des machines virtuelles. Les VM peuvent ainsi communiquer entre elles sur des tunnels entre des hyperviseurs si elles sont connectées au même commutateur logique. Chaque commutateur logique dispose d'un identifiant de réseau virtuel (VNI), tel qu'un ID de VLAN. Contrairement à VLAN, les VNI s'étendent bien au-delà de la limite des ID de VLAN.

Pour voir et modifier le pool VNI de valeurs, connectez-vous à NSX Manager, accédez à **Infrastructure > Profils**, puis cliquez sur l'onglet **Configuration**. Notez que si vous définissez un pool trop petit, la création d'un commutateur logique peut échouer si toutes les valeurs VNI sont utilisées. Si vous supprimez un commutateur logique, la valeur VNI sera réutilisée, mais seulement après 6 heures.

Lorsque vous ajoutez des commutateurs logiques, il est important que vous planifiez la topologie que vous créez.

Figure 1-1. Topologie du commutateur logique

Par exemple, la topologie indique un commutateur logique connecté à deux VM. Les deux machines virtuelles peuvent être situées sur des hôtes distincts ou un seul et même hôte, dans différents clusters d'hôtes ou le même cluster d'hôtes. Comme les VM dans l'exemple se trouvent sur le même réseau virtuel, les adresses IP sous-jacentes configurées sur les VM doivent se trouver dans le même sous-réseau.

Ce chapitre contient les rubriques suivantes :

- [Comprendre les modes de réplication de trame BUM](#)
- [Créer un commutateur logique](#)
- [Pontage de couche 2](#)
- [Créer un commutateur logique VLAN pour la liaison montante NSX Edge](#)
- [Connexion d'une machine virtuelle à un commutateur logique](#)
- [Tester la connectivité de couche 2](#)

Comprendre les modes de réplication de trame BUM

Chaque nœud de transport hôte est un point de terminaison de tunnel. Chaque point de terminaison de tunnel dispose d'une adresse IP. Ces adresses IP peuvent se trouver dans le même sous-réseau ou dans des sous-réseaux différents, en fonction de votre configuration de pools IP ou DHCP pour vos nœuds de transport.

Lorsque deux VM sur des hôtes différents communiquent directement, le trafic de monodiffusion encapsulé est échangé entre les adresses IP des deux points de terminaison de tunnel associées aux deux hyperviseurs sans propagation nécessaire.

Toutefois, comme avec tout réseau de couche 2, il peut arriver que le trafic provenant d'une VM doive être propagé, ce qui signifie qu'il doit être envoyé à toutes les autres VM appartenant au même commutateur logique. C'est le cas avec le trafic BUM (diffusion, monodiffusion inconnue et multidiffusion) de couche 2. Rappelez-vous qu'un seul commutateur logique NSX-T Data Center peut s'étendre sur plusieurs hyperviseurs. Le trafic BUM provenant d'une VM sur un hyperviseur donné doit être répliqué vers des hyperviseurs distants qui hébergent d'autres VM connectées au même commutateur logique. Pour activer cette propagation, NSX-T Data Center prend en charge deux modes de réplication différents :

- Deux niveaux hiérarchiques (parfois appelé MTEP)
- Tête (parfois appelé source)

Le mode de réplication Deux niveaux hiérarchiques est expliqué dans l'exemple suivant . Supposons que vous disposez d'un Hôte A, ayant des VM connectées aux identifiants de réseau virtuel (VNI) 5000, 5001 et 5002. Voyez les VNI comme étant semblables à des VLAN, mais chaque commutateur logique n'a qu'un seul VNI associé. Pour cette raison, les termes VNI et commutateur logique sont parfois utilisés de façon interchangeable. Lorsque nous disons qu'un hôte se trouve sur un VNI, nous voulons dire qu'il dispose de VM connectées à un commutateur logique avec ce VNI.

Un tableau de point de terminaison de tunnel indique les connexions hôte-VNI. L'Hôte A examine le tableau de point de terminaison de tunnel pour le VNI 5000 et détermine les adresses IP du point de terminaison de tunnel pour les autres hôtes sur le VNI 5000.

Certaines de ces connexions de VNI se trouveront sur le même sous-réseau IP, également appelé segment IP, que le point de terminaison de tunnel sur l'Hôte A. Pour chacune d'elles, l'Hôte A crée une copie séparée de chaque trame BUM et envoie la copie directement à chaque hôte.

Les points de terminaison de tunnel des autres hôtes se trouvent sur des sous-réseaux ou segments IP différents. Pour chaque segment avec plusieurs points de terminaison de tunnel, l'Hôte A nomme l'un de ces points de terminaison comme réplicateur.

Le réplicateur reçoit de la part de l'Hôte A une copie de chaque trame BUM pour le VNI 5000. Cette copie est marquée comme Réplica localement dans l'en-tête d'encapsulation. L'Hôte A n'envoie pas de copies aux autres hôtes dans le même segment IP que le réplicateur. Il est de la responsabilité du réplicateur de créer une copie de la trame BUM pour chaque hôte qu'il connaît se trouvant sur le VNI 5000 et dans le même segment IP que cet hôte réplicateur.

Le processus est répliqué pour les VNI 5001 et 5002. La liste de points de terminaison de tunnel et les réplicateurs résultants peuvent être différents pour des VNI différents.

Avec la réplication de tête, également appelée réplication de tête de réseau, il n'y a pas de réplicateur. L'Hôte A crée simplement une copie de chaque trame BUM pour chaque point de terminaison de tunnel qu'il connaît sur le VNI 5000 et l'envoie.

Si tous les points de terminaison de tunnel hôtes se trouvent sur le même sous-réseau, le choix du mode de réplication ne fait aucune différence, car le comportement ne changera pas. Si les points de terminaison de tunnel hôtes se trouvent sur des sous-réseaux différents, la réplication de deux niveaux hiérarchiques permet de distribuer la charge sur plusieurs hôtes. Deux niveaux hiérarchiques est le mode par défaut.

Créer un commutateur logique

Les commutateurs logiques sont attachés à une ou plusieurs VM dans le réseau. Les VM connectées à un commutateur logique peuvent communiquer entre elles à l'aide des tunnels entre les hyperviseurs.

Conditions préalables

- Vérifiez qu'une zone de transport est configurée. Reportez-vous à *Guide d'installation de NSX-T Data Center*.
- Vérifiez que des nœuds d'infrastructure sont correctement connectés à un agent de plan de gestion (MPA) NSX-T Data Center et à un plan de contrôle local (LCP) NSX-T Data Center.

Dans l'appel API GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state`, l'état doit être réussi. Reportez-vous à *Guide d'installation de NSX-T Data Center*.
- Vérifiez que des nœuds de transport sont ajoutés à la zone de transport. Reportez-vous à *Guide d'installation de NSX-T Data Center*.
- Vérifiez que les hyperviseurs sont ajoutés à l'infrastructure NSX-T Data Center et que des VM sont hébergées sur ces hyperviseurs.
- Familiarisez-vous avec la topologie du commutateur logique et les concepts de réplication de trames BUM. Reportez-vous aux sections [Chapitre 1 Commutateurs logiques et configuration d'un attachement de VM](#) et [Comprendre les modes de réplication de trame BUM](#).
- Vérifiez que votre cluster NSX Controller est stable.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Commutation > Commutateurs**.
- 3 Cliquez sur **Ajouter**.
- 4 Entrez un nom pour le commutateur logique et éventuellement une description.
- 5 Sélectionnez une zone de transport pour le commutateur logique.

Les VM attachées à des commutateurs logiques se trouvant dans la même zone de transport peuvent communiquer entre elles.
- 6 Entrez le nom d'une stratégie d'association de liaisons montantes.
- 7 Définissez **État administratif** sur **Actif** ou **Inactif**.

8 Sélectionnez un mode de réplication pour le commutateur logique.

Le mode de réplication (deux niveaux hiérarchiques ou tête) est requis pour les commutateurs logiques de superposition, mais pas pour les commutateurs logiques basés sur VLAN.

Mode de réplication	Description
Deux niveaux hiérarchiques	Le réplicateur est un hôte qui exécute la réplication de trafic BUM sur d'autres hôtes dans le même VNI. Chaque hôte désigne un point de terminaison de tunnel hôte dans chaque VNI comme réplicateur. Et ce pour chaque VNI.
HEAD	Les hôtes créent une copie de chaque trame BUM et envoient cette copie à chaque point de terminaison de tunnel qu'ils connaissent pour chaque VNI.

9 (Facultatif) Spécifiez un ID de VLAN ou des plages d'ID de VLAN pour le balisage VLAN.

Pour prendre en charge le balisage VLAN client pour les machines virtuelles connectées à ce commutateur, vous devez spécifier des plages d'ID de VLAN, également appelées jonctions de plages d'ID de VLAN. Le port logique filtre les paquets en fonction des jonctions de plages d'ID de VLAN et une VM cliente peut marquer ses paquets avec son propre ID de VLAN en fonction des jonctions de plages d'ID de VLAN.

10 (Facultatif) Cliquez sur l'onglet **Profils de commutation** et sélectionnez des profils de commutation.

11 Cliquez sur **Enregistrer**.

Dans l'interface utilisateur de NSX Manager, le nouveau commutateur logique est un lien hypertexte.

Étape suivante

Attachez des VM à votre commutateur logique. Reportez-vous à la section [Connexion d'une machine virtuelle à un commutateur logique](#).

Pontage de couche 2

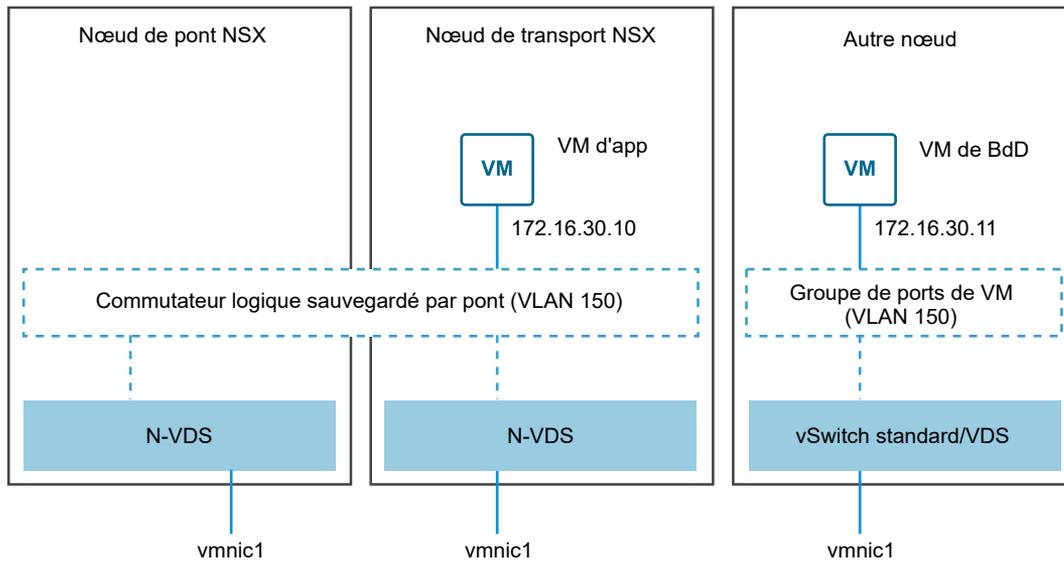
Lorsqu'un commutateur logique NSX-T Data Center requiert une connexion de couche 2 vers un groupe de ports sauvegardé par VLAN ou s'il a besoin d'atteindre un autre périphérique, tel qu'une passerelle, qui réside en dehors d'un déploiement de NSX-T Data Center, vous pouvez utiliser un pont de couche 2 NSX-T Data Center. Cela est particulièrement utile dans un scénario de migration dans lequel vous devez diviser un sous-réseau entre des charges de travail physiques et virtuelles.

Les concepts de NSX-T Data Center impliqués dans le pontage de couche 2 sont des clusters de pont, des points de terminaison de pont et des nœuds de pont. Un cluster de pont est un ensemble de nœuds de pont de haute disponibilité (HA). Un nœud de pont est un nœud de transport qui sert au pontage. Chaque commutateur logique utilisé pour le pontage d'un déploiement virtuel et physique dispose d'un ID de VLAN associé. Un point de terminaison de pont identifie les attributs physiques du pont, tels que l'ID de cluster du pont et l'ID de VLAN associé.

Vous pouvez configurer le pontage de couche 2 à l'aide de nœuds de transport hôtes ESXi ou de nœuds de transport NSX Edge. Pour utiliser des nœuds de transport hôtes ESXi pour le pontage, vous créez un cluster de pont. Pour utiliser des nœuds de transport NSX Edge pour le pontage, vous créez un profil de pont.

Dans l'exemple suivant, deux nœuds de transport NSX-T Data Center font partie de la même zone de transport de superposition. Cela permet d'attacher les commutateurs virtuels distribués (N-VDS, auparavant appelé commutateur hôte) gérés par NSX au même commutateur logique sauvegardé par pont.

Figure 1-2. Topologie du pont



Le nœud de transport de gauche appartient à un cluster de pont ; il s'agit donc d'un nœud de pont.

Comme le commutateur logique est attaché à un cluster de pont, il est appelé commutateur logique sauvegardé par pont. Pour pouvoir être sauvegardé par pont, un commutateur logique doit se trouver dans une zone de transport de superposition, pas dans une zone de transport VLAN.

Le nœud de transport du milieu ne fait pas partie du cluster de pont. Il s'agit d'un nœud de transport normal. Il peut s'agir d'un hôte KVM ou ESXi. Dans le schéma, une VM sur ce nœud appelée « VM d'app » est attachée au commutateur logique sauvegardé par pont.

Le nœud de droite ne fait pas partie de la superposition NSX-T Data Center. Il peut s'agir de n'importe quel hyperviseur avec une VM (comme indiqué sur le schéma) ou d'un nœud de réseau physique. Si le nœud non-NSX-T Data Center est un hôte ESXi, vous pouvez utiliser un vSwitch standard ou un commutateur distribué vSphere pour l'attachement de port. Il est requis que l'ID de VLAN associé à l'attachement de port corresponde à celui sur le commutateur logique sauvegardé par pont. De plus, la communication a lieu sur la couche 2, donc les deux périphériques finaux doivent avoir des adresses IP sur le même sous-réseau.

Comme indiqué, l'objectif du pont est d'activer la communication de couche 2 entre les deux VM. Lorsque le trafic est transmis entre les deux VM, il traverse le nœud de pont.

Note Lorsque vous utilisez des machines virtuelles Edge s'exécutant sur un hôte ESXi pour fournir le pontage de couche 2, le groupe de ports sur le commutateur standard ou distribué qui envoie et reçoit le trafic du côté du VLAN doit être en mode Promiscuité. Pour des performances optimales, notez les points suivants :

- Vous ne devez pas avoir d'autres groupes de ports en mode Promiscuité sur le même hôte partageant le même ensemble de VLAN.
- Les machines virtuelles Edge actives et en veille doivent se trouver sur des hôtes différents. Si elles se trouvent sur le même hôte, le débit peut chuter à 7 Gbits/s, car le trafic VLAN doit être transféré aux deux machines virtuelles en mode Promiscuité.

Créer un cluster de pont

Un cluster de pont est un ensemble de nœuds de transport hôtes ESXi qui peut fournir un pontage de couche 2 avec un commutateur logique.

Un cluster de pont peut comporter un maximum de deux nœuds de transport hôtes ESXi comme nœuds de pont. Avec deux nœuds de pont, un cluster de pont assure la haute disponibilité en mode actif-veille. Même si vous ne souhaitez avoir qu'un seul nœud de pont, vous devez toujours créer un cluster de pont. Après avoir créé le cluster de pont, vous pouvez ajouter un nœud de pont supplémentaire ultérieurement.

Conditions préalables

- Créez au moins un nœud de transport NSX-T Data Center à utiliser comme nœud de pont.
- Le nœud de transport utilisé comme nœud de pont doit être un hôte ESXi. KVM n'est pas pris en charge pour les nœuds de pont.
- Il est recommandé que les nœuds de pont ne contiennent aucune VM hébergée.
- Un nœud de transport peut être ajouté à un seul cluster de pont. Vous ne pouvez pas ajouter le même nœud de transport à plusieurs clusters de pont.

Procédure

- 1 Sélectionnez **Infrastructure > Nœuds** dans le panneau de navigation.
- 2 Cliquez sur l'onglet **Clusters de ponts ESXi**.
- 3 Cliquez sur **Ajouter**.
- 4 Entrez un nom et éventuellement une description.
- 5 Sélectionnez une zone de transport pour le cluster de pont.
- 6 Dans la colonne **Disponible**, sélectionnez des nœuds de transport et cliquez sur la flèche droite pour les déplacer dans la colonne **Sélectionné**.
- 7 Cliquez sur le bouton **Ajouter**.

Étape suivante

Vous pouvez maintenant associer un commutateur logique au cluster de pont.

Créer un profil de pont

Un profil de pont rend un cluster NSX Edge capable de fournir un pontage de couche 2 vers un commutateur logique.

Conditions préalables

- Vérifiez que vous disposez d'un cluster NSX Edge avec deux nœuds de transport NSX Edge.

Procédure

- 1 Sélectionnez **Infrastructure > Profils** dans le panneau de navigation.
- 2 Cliquez sur l'onglet **Profils de pont Edge**.
- 3 Cliquez sur **Ajouter**.
- 4 Entrez un nom et éventuellement une description.
- 5 Sélectionnez un cluster NSX Edge.
- 6 Sélectionnez un nœud principal.
- 7 Sélectionnez un nœud de secours.
- 8 Sélectionnez un mode de basculement.

Les options sont **Préemptif** et **Non-préemptif**.

- 9 Cliquez sur le bouton **Ajouter**.

Étape suivante

Vous pouvez maintenant associer un commutateur logique au profil de pont.

Créer un commutateur logique sauvegardé par pont de couche 2

Lorsque vous possédez des machines virtuelles qui sont connectées à la superposition NSX-T Data Center, vous pouvez configurer un commutateur logique sauvegardé par pont pour fournir une connectivité de couche 2 avec d'autres périphériques ou VM se trouvant à l'extérieur de votre déploiement de NSX-T Data Center.

Pour voir un exemple de topologie, reportez-vous à la section [Figure 1-2. Topologie du pont](#).

Conditions préalables

- Vérifiez que vous disposez d'un cluster de pont ou d'un profil de pont.
- Au moins un hôte ESXi ou KVM pour servir de nœud de transport normal. Ce nœud dispose de VM hébergées qui requièrent une connectivité avec des périphériques se trouvant à l'extérieur d'un déploiement de NSX-T Data Center.

- Une VM ou un autre périphérique final à l'extérieur du déploiement de NSX-T Data Center. Ce périphérique final doit être attaché à un port VLAN correspondant à l'ID de VLAN du commutateur logique sauvegardé par pont.
- Un commutateur logique dans une zone de transport de superposition pour servir de commutateur logique sauvegardé par pont.

Procédure

- 1 À partir d'un navigateur, connectez-vous à un dispositif NSX Manager sur `https://<nsx-mgr>`.
- 2 Sélectionnez **Mise en réseau > Commutation** dans le panneau de navigation.
- 3 Cliquez sur le nom d'un commutateur de superposition (type de trafic : superposition).
- 4 Cliquez sur **Éléments associés > Clusters de ponts ESXi** ou sur **Éléments associés > Profils de pont Edge**.
- 5 Cliquez sur **Attacher**.
- 6 Pour établir l'association avec un cluster de pont,
 - a Sélectionnez un cluster de pont.
 - b Saisissez un ID de VLAN.
 - c Activez ou désactivez **HA sur VLAN**.
 - d Cliquez sur **Attacher**.
- 7 Pour établir l'association avec un profil de pont,
 - a sélectionnez un profil de pont.
 - b Sélectionnez une zone de transport.
 - c Entrez un ID de VLAN.
 - d Cliquez sur **Enregistrer**.
- 8 Connectez des VM au commutateur logique, si ce n'est pas déjà fait.

Les machines virtuelles doivent se trouver sur des nœuds de transport dans la même zone de transport que le cluster de pont ou le profil de pont.

Résultats

Vous pouvez tester la fonctionnalité du pont en effectuant un test ping à partir de la VM interne à NSX-T Data Center sur un nœud externe à NSX-T Data Center. Par exemple, dans [Figure 1-2. Topologie du pont](#), la VM d'application sur le nœud de transport NSX-T Data Center doit pouvoir effectuer un test ping sur la VM de BD sur le nœud externe, et inversement.

Vous pouvez surveiller le trafic sur le commutateur de pont en cliquant sur l'onglet **Surveiller**.

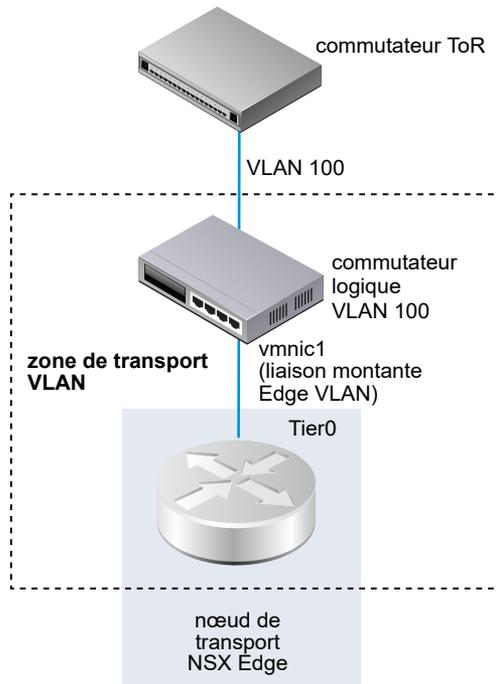
Vous pouvez également afficher le trafic du pont à l'aide de l'appel d'API GET <https://192.168.110.31/api/v1/bridge-endpoints/<endpoint-id>/statistics> :

```
{
  "tx_packets": {
    "total": 134416,
    "dropped": 0,
    "multicast_broadcast": 0
  },
  "rx_bytes": {
    "total": 22164,
    "multicast_broadcast": 0
  },
  "tx_bytes": {
    "total": 8610134,
    "multicast_broadcast": 0
  },
  "rx_packets": {
    "total": 230,
    "dropped": 0,
    "multicast_broadcast": 0
  },
  "last_update_timestamp": 1454979822860,
  "endpoint_id": "ba5ba59d-22f1-4a02-b6a0-18ef0e37ef31"
}
```

Créer un commutateur logique VLAN pour la liaison montante NSX Edge

Des liaisons montantes Edge sortent via des commutateurs logiques VLAN.

Lorsque vous créez un commutateur logique VLAN, il est important que vous réfléchissiez à la topologie particulière que vous créez. Par exemple, la topologie simple suivante montre un commutateur logique VLAN à l'intérieur d'une zone de transport VLAN. Le commutateur logique VLAN dispose de l'ID de VLAN 100. Cela correspond à l'ID de VLAN sur le port TOR connecté au port hôte d'hyperviseur utilisé pour la liaison montante VLAN du dispositif Edge.



Conditions préalables

- Pour créer un commutateur logique VLAN, vous devez d'abord créer une zone de transport VLAN.
- Un vSwitch NSX-T Data Center doit être ajouté au dispositif NSX Edge. Pour confirmer sur un dispositif Edge, exécutez la commande `get host-switches`. Par exemple :

```
nsx-edge1> get host-switches

Host Switch      : c0a78378-1c20-432a-9e23-ddb34f1c80c9
Switch Name     : hs1
Transport Zone  : c46dcd72-808a-423d-b4cc-8752c33f6b2c
Transport Zone  : 73def985-d122-4b7b-ab6a-a58176dfc32d
Physical Port   : fp-eth0
Uplink Name     : uplink-1
Transport VLAN  : 4096
Default Gateway : 192.168.150.1
Subnet Mask     : 255.255.255.0
Local VTEP Device : fp-eth0
Local VTEP IP   : 192.168.150.102
```

- Vérifiez que votre cluster NSX Controller est stable.
- Vérifiez que des nœuds d'infrastructure sont correctement connectés à l'agent de plan de gestion (MPA) NSX-T Data Center et au plan de contrôle local (LCP) NSX-T Data Center.

Dans l'appel API GET `https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state`, l'état doit être réussi. Reportez-vous à *Guide d'installation de NSX-T Data Center*.

Procédure

- 1 À partir d'un navigateur, connectez-vous à un dispositif NSX Manager sur `https://<nsx-mgr>`.

- 2 Sélectionnez **Mise en réseau > Commutation** dans le panneau de navigation.
- 3 Cliquez sur **Ajouter**.
- 4 Tapez un nom pour le commutateur logique.
- 5 Sélectionnez une zone de transport pour le commutateur logique.
- 6 Sélectionnez une stratégie d'association de liaison montante.
- 7 Pour l'état d'administration, sélectionnez **Actif** ou **Inactif**.
- 8 Tapez un ID de VLAN.
Entrez 0 dans le champ VLAN s'il n'existe aucun ID de VLAN pour la liaison montante vers le TOR physique.
- 9 (Facultatif) Cliquez sur l'onglet **Profils de commutation** et sélectionnez des profils de commutation.

Résultats

Note Si vous avez deux commutateurs logiques VLAN avec le même ID de VLAN, ils ne peuvent pas être connectés au même commutateur N-VDS Edge (auparavant nommé commutateur hôte). Si vous disposez d'un commutateur logique VLAN et d'un commutateur logique de superposition, et l'ID de VLAN du commutateur logique VLAN est identique à l'ID de VLAN de transport du commutateur logique de superposition, ils ne peuvent également pas être connectés au même commutateur N-VDS Edge.

Étape suivante

Ajoutez un routeur logique.

Connexion d'une machine virtuelle à un commutateur logique

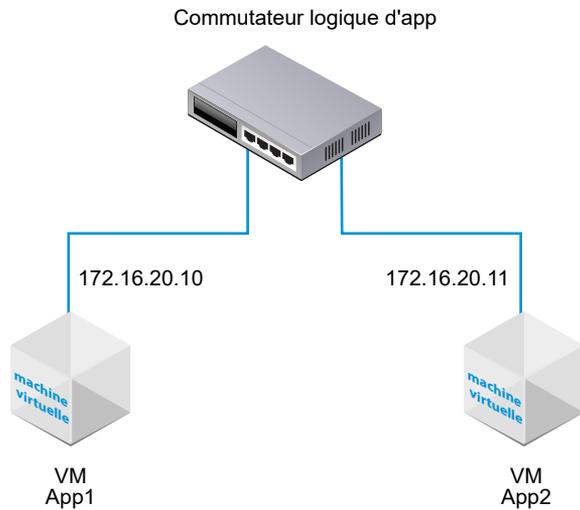
La configuration pour la connexion d'une machine virtuelle à un port logique peut varier en fonction de l'hôte.

Les hôtes pris en charge pour la connexion à un commutateur logique sont : un hôte ESXi géré dans vCenter Server, un hôte ESXi autonome et un hôte KVM.

Attacher une VM hébergée sur vCenter Server à un commutateur logique NSX-T Data Center

Si vous disposez d'un hôte ESXi géré dans vCenter Server, vous pouvez accéder aux VM hôtes via vSphere Web Client basé sur le Web. Dans ce cas, vous pouvez utiliser cette procédure pour attacher des machines virtuelles à des commutateurs logiques NSX-T Data Center.

L'exemple indiqué dans cette procédure montre comment attacher une machine virtuelle nommée app-vm à un commutateur logique nommé app-switch.



L'application vSphere Client basée sur l'installation ne prend pas en charge l'association d'une VM à un commutateur logique NSX-T Data Center. Si vous ne disposez pas de vSphere Web Client (basé sur le Web), consultez [Attacher une machine virtuelle autonome hébergée sur un hôte ESXi autonome à un commutateur logique NSX-T Data Center](#).

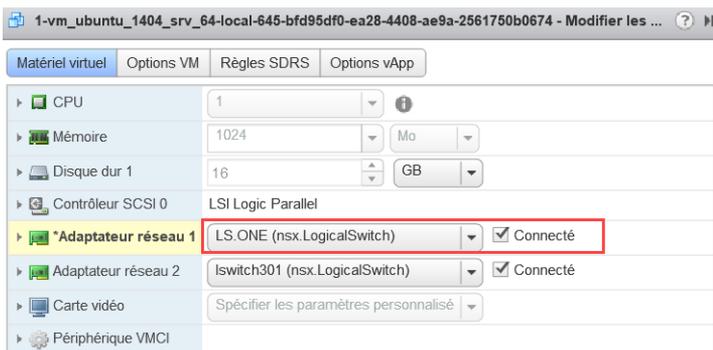
Conditions préalables

- Les VM doivent être hébergées sur des hyperviseurs qui ont été ajoutés à l'infrastructure NSX-T Data Center.
- Les nœuds d'infrastructure doivent disposer d'une connectivité de plan de gestion (MPA) NSX-T Data Center et de plan de contrôle (LCP) NSX-T Data Center.
- Les nœuds d'infrastructure doivent être ajoutés à une zone de transport.
- Un commutateur logique doit être créé.

Procédure

- 1 Dans vSphere Web Client, modifiez les paramètres de la VM, puis attachez la VM au commutateur logique NSX-T Data Center.

Par exemple :



- 2 Cliquez sur **OK**.

Résultats

Après avoir attaché une VM à un commutateur logique, des ports de commutateur logique sont ajoutés au commutateur logique. Vous pouvez voir les ports de commutateur logique sur le dispositif NSX Manager dans **Commutation > Ports**.

Dans l'API NSX-T Data Center, vous pouvez voir les VM attachées NSX-T Data Center avec l'appel API GET `https://<nsx-mgr>/api/v1/fabric/virtual-machines`.

Dans l'interface utilisateur de NSX-T Data Center, sous **Commutation > Ports**, l'ID d'attachement VIF correspond à l'ExternalID trouvé dans l'appel API. Recherchez l'ID d'attachement VIF correspondant à l'externalId de la VM et vérifiez que les états administratif et opérationnel sont Actif/Actif.

Si deux machines virtuelles sont attachées au même commutateur logique et qu'elles disposent d'adresses IP configurées dans le même sous-réseau, elles doivent pouvoir effectuer un test ping l'une sur l'autre.

Étape suivante

Ajoutez un routeur logique.

Vous pouvez surveiller l'activité sur le port du commutateur logique pour résoudre les problèmes. Reportez-vous à la section « Surveiller l'activité d'un port de commutateur logique » dans le *Guide d'administration de NSX-T Data Center*.

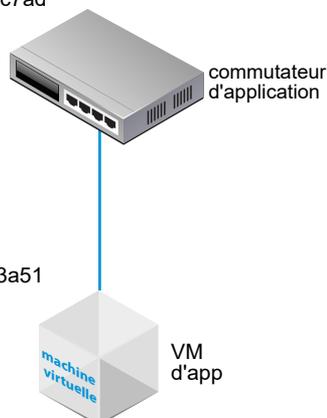
Attacher une machine virtuelle autonome hébergée sur un hôte ESXi autonome à un commutateur logique NSX-T Data Center

Si vous disposez d'un hôte ESXi autonome, vous ne pouvez pas accéder aux machines virtuelles hôtes via le client vSphere Web Client basé sur le Web. Dans ce cas, vous pouvez utiliser cette procédure pour attacher des machines virtuelles à des commutateurs logiques NSX-T Data Center.

L'exemple indiqué dans cette procédure montre comment attacher une machine virtuelle nommée app-vm à un commutateur logique nommé app-switch.

ID de réseau opaque du commutateur :
22b22448-38bc-419b-bea8-b51126bec7ad

ID externe de la VM :
50066bae-0f8a-386b-e62e-b0b9c6013a51



Conditions préalables

- La machine virtuelle doit être hébergée sur des hyperviseurs qui ont été ajoutés à l'infrastructure NSX-T Data Center.
- Les nœuds d'infrastructure doivent disposer d'une connectivité de plan de gestion (MPA) NSX-T Data Center et de plan de contrôle (LCP) NSX-T Data Center.
- Les nœuds d'infrastructure doivent être ajoutés à une zone de transport.
- Un commutateur logique doit être créé.
- Vous devez avoir accès à l'API NSX Manager.
- Vous devez avoir un accès en écriture au fichier VMX de la machine virtuelle.

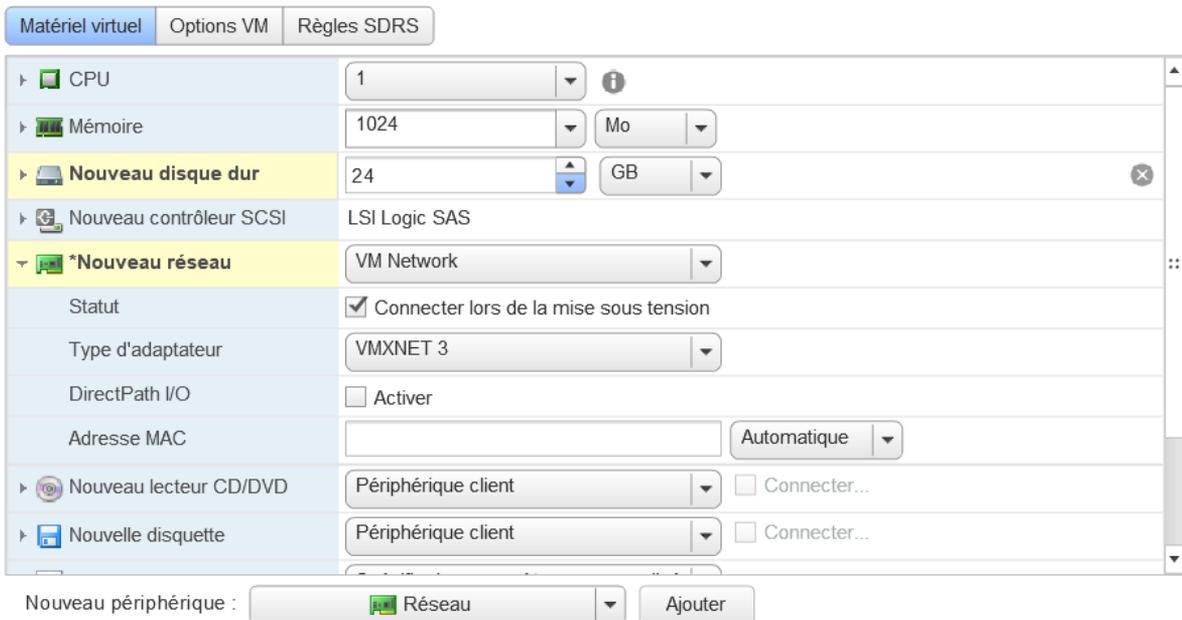
Procédure

- 1 À l'aide de l'application vSphere Client (installée) ou d'un autre outil de gestion des machines virtuelles, modifiez la machine virtuelle et ajoutez un adaptateur Ethernet VMXNET 3.

Sélectionnez n'importe quel réseau nommé. Vous modifierez la connexion réseau lors d'une étape ultérieure.

Personnaliser le matériel

Configurez le matériel de la machine virtuelle



- 2 Utilisez l'API NSX-T Data Center pour émettre l'appel d'API GET <https://<nsx-mgr>/api/v1/fabric/virtual-machines/<VM-ID>>.

Dans les résultats, recherchez l'externalId de la machine virtuelle.

Par exemple :

```
GET https://<nsx-mgr>/api/v1/fabric/virtual-machines/60a5a5d5-ea2b-407e-a806-4fdc8468f735

{
  "resource_type": "VirtualMachine",
  "id": "60a5a5d5-ea2b-407e-a806-4fdc8468f735",
  "display_name": "app-vm",
  "compute_ids": [
    "instanceUuid:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "moIdOnHost:5",
    "externalId:50066bae-0f8a-386b-e62e-b0b9c6013a51",
    "hostLocalId:5",
    "locationId:564dc020-1565-e3f4-f591-ee3953eef3ff",
    "biosUuid:4206f47d-fe7f-08c5-5bf7-ea26a4c6b18d"
  ],
  "external_id": "50066bae-0f8a-386b-e62e-b0b9c6013a51",
  "type": "REGULAR",
  "host_id": "cb82b0fa-a8f1-11e5-92a9-6b7d1f8661fa",
  "local_id_on_host": "5"
}
```

3 Éteignez la machine virtuelle et désinscrivez-la de l'hôte.

Vous pouvez utiliser votre outil de gestion des machines virtuelles ou l'interface de ligne de commande ESXi, comme indiqué ici.

```
[user@host:~] vim-cmd /vmsvc/getallvms
Vmid   Name      File                Guest OS      Version  Annotation
5      app-vm   [ds2] app-vm/app-vm.vmx  ubuntuGuest  vmx-08
8      web-vm   [ds2] web-vm/web-vm.vmx  ubuntu64Guest vmx-08

[user@host:~] vim-cmd /vmsvc/power.off 5
Powering off VM:

[user@host:~] vim-cmd /vmsvc/unregister 5
```

4 À partir de l'interface utilisateur de NSX Manager, obtenez l'ID du commutateur logique.

Par exemple :

app-switch

Présentation Surveiller Gérer ▾ Éléments Associés ▾

▾ Résumé | MODIFIER

Nom	app-switch
ID	b68e7ac3-877a-420e-af47-53e974c17915
Emplacement	
Description	lswitch202 (created through automation)
Statut administratif	● Actif
Mode de répllication	Répllication de tête
VLAN	S/O
VNI	71681
Ports logiques	1
Type de trafic	Superposition
Zone de transport	transportzone1
Nom de la stratégie d'associa...	[Use Default]
Mode N-VDS	STANDARD
Crée le	9/10/2018, 12:20:46 PM par admin
Dernière mise à jour	9/26/2018, 2:01:14 PM par admin

5 Modifiez le fichier VMX de la machine virtuelle.

Supprimez le champ **ethernet1.networkName = "<nom>"** et ajoutez les champs suivants :

- ethernet1.opaqueNetwork.id = "<ID du commutateur logique>"
- ethernet1.opaqueNetwork.type = "nsx.LogicalSwitch"
- ethernet1.externalId = "<ExternalId de la machine virtuelle>"
- ethernet1.connected = "TRUE"
- ethernet1.startConnected = "TRUE"

Par exemple :

```

ANCIEN
ethernet1.pciSlotNumber = "224"
ethernet1.virtualDev = "vmxnet3"
ethernet1.networkName = "VM Network"
ethernet1.addressType = "vpx"
    
```

```

ethernet1.generatedAddress = "00:50:56:86:7b:d7"
ethernet1.uptCompatibility = "true"
ethernet1.present = "TRUE"

```

NOUVEAU

```

ethernet1.pciSlotNumber = "224"
ethernet1.virtualDev = "vmxnet3"
ethernet1.addressType = "vpx"
ethernet1.generatedAddress = "00:50:56:86:7b:d7"
ethernet1.uptCompatibility = "true"
ethernet1.present = "TRUE"
ethernet1.opaqueNetwork.id = "22b22448-38bc-419b-bea8-b51126bec7ad"
ethernet1.opaqueNetwork.type = "nsx.LogicalSwitch"
ethernet1.externalId = "50066bae-0f8a-386b-e62e-b0b9c6013a51"
ethernet1.connected = "TRUE"
ethernet1.startConnected = "TRUE"

```

- 6 Dans l'interface utilisateur de NSX Manager, ajoutez un port de commutateur logique et utilisez l'externalId de la VM pour le rattachement à l'interface virtuelle (VIF).
- 7 Enregistrez la machine virtuelle et mettez-la sous tension.

Vous pouvez utiliser votre outil de gestion des machines virtuelles ou l'interface de ligne de commande ESXi, comme indiqué ici.

```
[user@host:~] vim-cmd /solo/register /path/to/file.vmx
```

For example:

```
[user@host:~] vim-cmd solo/registervm /vmfs/volumes/355f2049-6c704347/app-vm/app-vm.vmx
9
```

```
[user@host:~] vim-cmd /vmsvc/power.on 9
Powering on VM:
```

Résultats

Dans l'interface utilisateur de NSX Manager sous **Commutation > Ports**, retrouvez l'ID du rattachement à l'interface virtuelle qui correspond à l'externalId de la machine virtuelle et assurez-vous que l'état administratif et opérationnel est Actif/Actif.

Si deux machines virtuelles sont attachées au même commutateur logique et qu'elles disposent d'adresses IP configurées dans le même sous-réseau, elles doivent pouvoir effectuer un test ping l'une sur l'autre.

Étape suivante

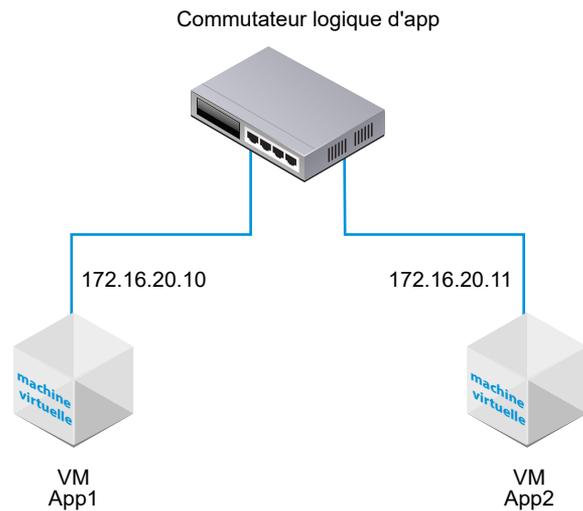
Ajoutez un routeur logique.

Vous pouvez surveiller l'activité sur le port du commutateur logique pour résoudre les problèmes. Reportez-vous à la section « Surveiller l'activité d'un port de commutateur logique » dans le *Guide d'administration de NSX-T Data Center*.

Attacher une VM hébergée sur KVM à un commutateur logique NSX-T Data Center

Si vous disposez d'un hôte KVM, vous pouvez utiliser cette procédure pour attacher des VM à des commutateurs logiques NSX-T Data Center.

L'exemple indiqué dans cette procédure montre comment attacher une machine virtuelle nommée app-vm à un commutateur logique nommé app-switch.



Conditions préalables

- La machine virtuelle doit être hébergée sur des hyperviseurs qui ont été ajoutés à l'infrastructure NSX-T Data Center.
- Les nœuds d'infrastructure doivent disposer d'une connectivité de plan de gestion (MPA) NSX-T Data Center et de plan de contrôle (LCP) NSX-T Data Center.
- Les nœuds d'infrastructure doivent être ajoutés à une zone de transport.
- Un commutateur logique doit être créé.

Procédure

- 1 Dans l'interface de ligne de commande KVM, exécutez la commande `virsh dumpxml <your vm> | grep interfaceid`.
- 2 Dans l'interface utilisateur de NSX Manager, ajoutez un port de commutateur logique et utilisez l'ID d'interface de la VM pour l'attachement VIF.

Résultats

Dans l'interface utilisateur de NSX Manager, sous **Commutation > Ports**, recherchez l'ID d'attachement VIF et vérifiez que les états administratif et opérationnel sont Actif/Actif.

Si deux machines virtuelles sont attachées au même commutateur logique et qu'elles disposent d'adresses IP configurées dans le même sous-réseau, elles doivent pouvoir effectuer un test ping l'une sur l'autre.

Étape suivante

Ajoutez un routeur logique.

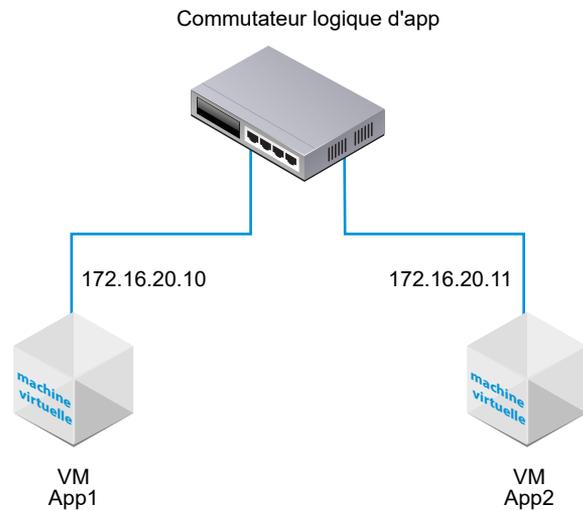
Vous pouvez surveiller l'activité sur le port du commutateur logique pour résoudre les problèmes. Reportez-vous à la section « Surveiller l'activité d'un port de commutateur logique » dans le *Guide d'administration de NSX-T Data Center*.

Tester la connectivité de couche 2

Une fois que vous avez réussi à configurer votre commutateur logique et à attacher des VM au commutateur logique, vous pouvez tester la connectivité réseau des VM attachées.

Si votre environnement réseau est configuré correctement, en fonction de la topologie, la VM App2 peut effectuer un test ping sur la VM App1.

Figure 1-3. Topologie du commutateur logique



Procédure

- 1 Connectez-vous à l'une des VM attachées au commutateur logique en utilisant SSH ou la console de VM.

Par exemple, VM App2 172.16.20.11.

- 2 Effectuez un test ping sur la seconde VM attachée au commutateur logique pour tester la connectivité.

```
$ ping -c 2 172.16.20.10
PING 172.16.20.10 (172.16.20.10) 56(84) bytes of data.
64 bytes from 172.16.20.10: icmp_seq=1 ttl=63 time=0.982 ms
64 bytes from 172.16.20.10: icmp_seq=2 ttl=63 time=0.654 ms
64 bytes from 172.16.20.10: icmp_seq=3 ttl=63 time=0.791 ms

--- 172.16.20.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1990ms
rtt min/avg/max/mdev = 0.654/0.809/0.902/0.104 ms
```

- 3 (Facultatif) Identifiez le problème qui cause l'échec du test ping.
 - a Vérifiez que les paramètres du réseau de VM sont corrects.
 - b Vérifiez que l'adaptateur réseau de VM est connecté au commutateur logique correct.
 - c Vérifiez que l'état administratif du commutateur logique est Actif.
 - d À partir de NSX Manager, sélectionnez **Commutation > Commutateurs**.

- e Cliquez sur le commutateur logique et notez l'UUID et les informations VNI.
- f À partir de NSX Controller, exécutez les commandes suivantes pour résoudre le problème.

vdmadmin	Description
get logical-switch <vni-or-uuid> arp-table	Affiche la table ARP du commutateur logique spécifié. Exemple de résultat.
	<pre>nsx-controller1> get logical-switch 41866 arp-table VNI IP MAC Connection-ID 41866 172.16.20.11 00:50:56:b1:70:5e 295422</pre>
get logical-switch <vni-or-uuid> connection-table	Affiche les connexions du commutateur logique spécifié. Exemple de résultat.
	<pre>nsx-controller1> get logical-switch 41866 connection-table Host-IP Port ID 192.168.110.37 36923 295420 192.168.210.53 37883 295421 192.168.210.54 57278 295422</pre>
get logical-switch <vni-or-uuid> mac-table	Affiche la table MAC du commutateur logique spécifié. Exemple de résultat.
	<pre>nsx-controller1> get logical-switch 41866 mac-table VNI MAC VTEP-IP Connection-ID 41866 00:50:56:86:f2:b2 192.168.250.102 295421 41866 00:50:56:b1:70:5e 192.168.250.101 295422</pre>
get logical-switch <vni-or-uuid> stats	Affiche des statistiques sur le commutateur logique spécifié. Exemple de résultat.
	<pre>nsx-controller1> get logical-switch 41866 stats update.member 11 update.vtep 11 update.mac 4 update.mac.invalidate 0 update.arp 7 update.arp.duplicate 0 query.mac 2 query.mac.miss 0 query.arp 9 query.arp.miss 6</pre>
get logical-switch <vni-or-uuid> stats-sample	Affiche un résumé de toutes les statistiques du commutateur logique au fil du temps. Exemple de résultat.
	<pre>nsx-controller1> get logical-switch 41866 stats-sample 21:00:00 21:10:00 21:20:00 21:30:00 21:40:00 update.member 0 0 0 0 0 update.vtep 0 0 0 0 0 update.mac 0 0 0 0 0 update.mac.invalidate 0 0 0 0 0 update.arp 0 0 0 0 0 update.arp.duplicate 0 0 0 0 0</pre>

vdmadmin	Description
	<pre>query.mac 0 0 0 0 0 query.mac.miss 0 0 0 0 0 query.arp 0 0 0 0 0 query.arp.miss 0 0 0 0 0</pre>
<pre>get logical-switch <vni-or- uuid> vtep</pre>	<p>Affiche tous les points de terminaison de tunnel virtuels liés au commutateur logique spécifié.</p> <p>Exemple de résultat.</p> <pre>nsx-controller1> get logical-switch 41866 vtep VNI IP LABEL Segment MAC Connection-ID 41866 192.168.250.102 0x8801 192.168.250.0 00:50:56:65:f5:fc 295421 41866 192.168.250.100 0x1F801 192.168.250.0 02:50:56:00:00:00 295420 41866 192.168.250.101 0x16001 192.168.250.0 00:50:56:64:7c:28 295422</pre>

Résultats

La première VM attachée au commutateur logique peut envoyer des paquets à la seconde.

Port de commutateur logique

2

Un commutateur logique possède plusieurs ports de commutateur. Les entités telles que les routeurs, les machines virtuelles ou les conteneurs peuvent se connecter à un commutateur logique via ses ports.

Ce chapitre contient les rubriques suivantes :

- [Créer un port de commutateur logique](#)
- [Surveiller l'activité d'un port de commutateur logique](#)

Créer un port de commutateur logique

Un port de commutateur logique vous permet de connecter un autre composant réseau, une machine virtuelle ou un conteneur à un commutateur logique.

Pour plus d'informations sur la connexion d'une machine virtuelle à un commutateur logique, reportez-vous à la section [Connexion d'une machine virtuelle à un commutateur logique](#). Pour plus d'informations sur la connexion d'un conteneur à un commutateur logique, consultez le *Guide d'installation et d'administration de NSX-T Container Plug-in for Kubernetes*.

Note L'adresse IP et l'adresse MAC liées à un port de commutateur logique pour un conteneur sont allouées par NSX Manager. Ne modifiez pas la liaison d'adresse manuellement.

Conditions préalables

Vérifiez qu'un port de commutateur logique est créé. Reportez-vous à la section [Chapitre 1 Commutateurs logiques et configuration d'un attachement de VM](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Commutation** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Ports**.
- 4 Cliquez sur **Ajouter**.

- 5 Dans l'onglet **Général**, indiquez les détails du port.

Option	Description
Nom et description	Entrez un nom et éventuellement une description.
Commutateur logique	Sélectionnez un commutateur logique dans la liste déroulante.
Statut Admin	Sélectionnez Haut ou Bas .
Type de pièce jointe	Sélectionnez Aucun ou VIF .
Identifiant de pièce jointe	Si le type de pièce jointe est VIF, entrez l'identifiant de pièce jointe.

- 6 (Facultatif) Dans l'onglet **Profils de commutation**, sélectionnez des profils de commutation.

- 7 Cliquez sur **Enregistrer**.

Surveiller l'activité d'un port de commutateur logique

Vous pouvez surveiller l'activité du port logique pour, par exemple, dépanner la surcharge du réseau et des paquets abandonnés.

Conditions préalables

Vérifiez qu'un port de commutateur logique est configuré. Reportez-vous à la section [Connexion d'une machine virtuelle à un commutateur logique](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Commutation** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Ports**.
- 4 Cliquez sur le nom d'un port.
- 5 Cliquez sur l'onglet **Surveiller**.
L'état du port et les statistiques sont affichés.
- 6 Pour télécharger un fichier CSV des adresses MAC apprises par l'hôte, cliquez sur **Télécharger la table MAC**.
- 7 Pour contrôler l'activité sur le port, cliquez sur **Commencer le suivi**.

Une page de suivi du port s'ouvre. Vous pouvez voir le trafic de port bidirectionnel et identifier les paquets abandonnés. La page de suivi du port répertorie également les profils de commutation attachés au port de commutateur logique.

Résultats

Par exemple, si vous remarquez des paquets abandonnés en raison d'une surcharge du réseau, vous pouvez configurer un profil de commutation QoS pour le port de commutateur logique afin d'éviter toute

perte de données sur les paquets préférés. Reportez-vous à la section [Comprendre le profil de commutation QoS](#).

Basculement des profils pour commutateurs logiques et ports logiques

3

Les profils de commutation comportent les informations de configuration réseau de couche 2 des commutateurs logiques et ports logiques. NSX Manager prend en charge plusieurs types de profils de commutation et conserve un ou plusieurs profils de commutation par défaut définis par le système pour chaque type de profil.

Les types de profils disponibles sont les suivants :

- QoS (qualité de service)
- Découverte d'adresses IP
- SpoofGuard
- Sécurité de commutateur
- Gestion MAC

Note Il est impossible de modifier ou de supprimer les profils de commutation par défaut du dispositif NSX Manager. Vous pouvez par contre créer des profils de commutation personnalisés.

Chaque profil de commutation par défaut ou personnalisé dispose d'un identifiant unique qui lui est réservé. Cet identifiant est utilisé pour associer le profil de commutation à un commutateur logique ou à un port logique. Par exemple, l'ID du profil de commutation QoS par défaut est f313290b-eba8-4262-bd93-fab5026e9495.

Un commutateur logique ou un port logique peut être associé à un profil de commutation de chaque type. Par exemple, vous ne pouvez pas avoir deux profils de commutation QoS différents associés à un commutateur logique ou port logique.

Si vous n'associez aucun type de profil de commutation lors de la création ou de la mise à jour d'un commutateur logique, le dispositif NSX Manager associe le profil de commutation par défaut défini par le système correspondant. Les ports logiques enfants héritent du commutateur logique parent le profil de commutation par défaut défini par le système.

Lorsque vous créez ou mettez à jour un commutateur logique ou un port logique, vous pouvez choisir de leur associer un profil de commutation par défaut ou un profil personnalisé. Lorsque le profil de commutation est associé ou dissocié d'un commutateur logique, le profil de commutation des ports logiques enfants est appliqué sur la base des critères ci-dessous.

- Si un profil est associé au commutateur logique parent, le port logique enfant hérite du profil de commutation du parent.
- Si aucun profil n'est associé au commutateur logique parent, un profil de commutation par défaut est attribué au commutateur logique et le port logique hérite de ce profil de commutation par défaut.
- Si vous associez explicitement un profil personnalisé au port logique, le profil personnalisé remplace le profil de commutation existant.

Note Si vous avez associé un profil de commutation personnalisé à un commutateur logique, mais que vous souhaitez conserver le profil de commutation par défaut pour l'un des ports logiques enfants, vous devez effectuer une copie du profil de commutation par défaut et l'associer au port logique concerné.

Il est impossible de supprimer un profil de commutation personnalisé, si celui-ci est associé à un commutateur logique ou à un port logique. Pour savoir si des commutateurs logiques et ports logiques sont associés à un profil de commutation personnalisé, accédez à la section Attribué à de la vue Résumé et cliquez sur les commutateurs logiques et ports logiques répertoriés.

Ce chapitre contient les rubriques suivantes :

- [Comprendre le profil de commutation QoS](#)
- [Comprendre le profil de commutation de découverte d'adresses IP](#)
- [Comprendre SpoofGuard](#)
- [Comprendre le profil de commutation de sécurité de commutateur](#)
- [Comprendre le profil de commutation de gestion MAC](#)
- [Associer un profil personnalisé à un commutateur logique](#)
- [Associer un profil personnalisé à un port logique](#)

Comprendre le profil de commutation QoS

QoS fournit des performances réseau dédiées et de haute qualité pour le trafic préféré qui requiert une bande passante élevée. Le mécanisme QoS parvient à cela en hiérarchisant la bande passante suffisante, en contrôlant la latence et la gigue et en réduisant la perte de données pour les paquets préférés, même en cas de surcharge du réseau. Ce niveau de service réseau est fourni en utilisant efficacement les ressources réseau existantes.

Pour cette version, la formation et le marquage du trafic, CoS et DSCP sont pris en charge. La classe de service (CoS) de couche 2 vous permet de spécifier la priorité des paquets de données lorsque le trafic est mis en mémoire tampon dans le commutateur logique en raison d'une surcharge. La valeur DSCP (Differentiated Services Code Point) de couche 3 détecte les paquets en fonction de leurs valeurs DSCP. CoS est toujours appliqué au paquet de données quel que soit le mode approuvé.

NSX-T Data Center approuve le paramètre DSCP appliqué par une machine virtuelle ou en modifiant et en définissant la valeur DSCP au niveau du commutateur logique. Dans chaque cas, la valeur DSCP est propagée vers l'en-tête Adresse IP externe de trames encapsulées. Cela permet au réseau physique externe de hiérarchiser le trafic en fonction du paramètre DSCP sur l'en-tête externe. Lorsque DSCP est en mode approuvé, la valeur DSCP est copiée à partir de l'en-tête interne. En mode non approuvé, la valeur DSCP n'est pas conservée pour l'en-tête interne.

Note Les paramètres DSCP ne fonctionnent que sur le trafic par tunnel. Ces paramètres ne s'appliquent pas au trafic à l'intérieur du même hyperviseur.

Vous pouvez utiliser le profil de commutation QoS pour configurer les valeurs de bande passante d'entrée et de sortie moyennes afin de définir la limite de transmission. Le taux de bande passante maximale est utilisé pour supporter le trafic de rafale auquel a droit un commutateur logique pour éviter toute surcharge sur les liens de réseau vers le nord. Ces paramètres ne garantissent pas la bande passante, mais permettent de limiter l'utilisation de la bande passante réseau. La bande passante que vous observez est déterminée par la valeur la plus petite entre la vitesse de liaison du port et les valeurs du profil de commutation.

Les paramètres du profil de commutation QoS s'appliquent au commutateur logique et sont hérités par le port de commutateur logique enfant.

Configurer un profil de commutation QoS personnalisé

Vous pouvez définir la valeur DSCP et configurer les paramètres d'entrée et de sortie pour créer un profil de commutation QoS personnalisé.

Conditions préalables

- Familiarisez-vous avec le concept de profil de commutation QoS. Reportez-vous à la section [Comprendre le profil de commutation QoS](#).
- Identifiez le trafic réseau auquel vous voulez donner la priorité.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Commutation** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Profils de commutation**.
- 4 Cliquez sur **Ajouter** et sélectionnez **QoS**.

5 Renseignez les détails du profil de commutation QoS.

Option	Description
Nom et description	<p>Attribuez un nom au profil de commutation QoS personnalisé.</p> <p>En option, vous pouvez décrire le paramètre que vous avez modifié dans le profil.</p>
Mode	<p>Sélectionnez l'option Approuvé ou Non approuvé dans le menu déroulant Mode. Lorsque vous sélectionnez le mode Approuvé, la valeur DSCP de l'en-tête interne s'applique à l'en-tête Adresse IP externe pour le trafic IP/IPv6. Pour le trafic non-IP/IPv6, l'en-tête Adresse IP externe prend la valeur par défaut. Le mode Approuvé est pris en charge sur un port logique basé sur la superposition. La valeur par défaut est 0.</p> <p>Le mode Non approuvé est pris en charge sur les ports logiques basés sur la superposition et sur VLAN. Pour le port logique basé sur la superposition, la valeur DSCP de l'en-tête Adresse IP sortante est définie sur la valeur configurée quel que soit le type de paquet interne pour le port logique. Pour le port logique basé sur VLAN, la valeur DSCP du paquet IP/IPv6 sera définie sur la valeur configurée. La plage de valeurs DSCP pour le mode Non approuvé est comprise entre 0 et 63.</p> <p>Note Les paramètres DSCP ne fonctionnent que sur le trafic par tunnel. Ces paramètres ne s'appliquent pas au trafic à l'intérieur du même hyperviseur.</p>
Priorité	<p>Définissez la valeur de priorité CoS.</p> <p>La plage des valeurs CoS est comprise entre 0 et 63, où 0 est la priorité la plus élevée.</p>
Classe de service	<p>Définissez la valeur CoS.</p> <p>CoS est pris en charge sur le port logique basé sur VLAN. CoS groupe des types semblables de trafic dans le réseau et chaque type de trafic est traité comme une classe avec son propre niveau de priorité de service. Le trafic avec la priorité la plus faible est ralenti ou, dans certains cas, abandonné pour fournir un meilleur débit pour un trafic avec une priorité supérieure. CoS peut également être configuré pour l'ID de VLAN avec zéro paquet.</p> <p>Les valeurs CoS sont comprises entre 0 et 7, où 0 est le service conseillé.</p>
Entrée	<p>Définissez des valeurs personnalisées pour le trafic réseau sortant de la VM vers le réseau logique.</p> <p>Vous pouvez utiliser la bande passante moyenne pour réduire la surcharge du réseau. Le taux de bande passante maximale est utilisé pour prendre en charge le trafic de rafale et la durée de rafale est définie dans le paramètre de taille de rafale. Vous ne pouvez pas garantir la bande passante. Toutefois, vous pouvez utiliser le paramètre pour limiter la bande passante réseau. La valeur par défaut de 0 désactive le trafic d'entrée.</p> <p>Par exemple, lorsque vous définissez la bande passante moyenne pour le commutateur logique sur 30 Mbit/s, la stratégie limite la bande passante. Vous pouvez plafonner le trafic de rafale à 100 Mbit/s pour une durée de 20 octets.</p>

Option	Description
Diffusion d'entrée	Définissez des valeurs personnalisées pour le trafic réseau sortant de la VM vers le réseau logique en fonction de la diffusion. La valeur par défaut de 0 désactive le trafic de diffusion d'entrée. Par exemple, lorsque vous définissez la bande passante moyenne pour un commutateur logique sur 50 Kbit/s, la stratégie limite la bande passante. Vous pouvez plafonner le trafic de rafale à 400 Kbit/s pour une durée de 60 octets.
Sortie	Définissez des valeurs personnalisées pour le trafic réseau entrant du réseau logique vers la VM. La valeur par défaut de 0 désactive le trafic de sortie.

Si les options Entrée, Diffusion d'entrée et Sortie ne sont pas configurées, les valeurs par défaut sont utilisées comme tampons de protocole.

6 Cliquez sur **Enregistrer**.

Résultats

Un profil de commutation QoS personnalisé s'affiche sous forme de lien.

Étape suivante

Attachez ce profil de commutation QoS personnalisé à un commutateur logique ou à un port logique pour que les paramètres modifiés dans le profil de commutation s'appliquent au trafic réseau. Reportez-vous à la section [Associer un profil personnalisé à un commutateur logique](#) ou [Associer un profil personnalisé à un port logique](#).

Comprendre le profil de commutation de découverte d'adresses IP

La découverte d'adresses IP utilise l'écoute DHCP, l'écoute ARP ou VM Tools pour apprendre les adresses MAC et IP de la machine virtuelle. Une fois les adresses MAC et IP apprises, les entrées sont partagées avec NSX Controller pour effectuer la suppression ARP. La suppression ARP réduit la propagation du trafic ARP dans les VM connectées au même commutateur logique.

L'écoute DHCP inspecte les paquets DHCP échangés entre le client DHCP de la VM et le serveur DHCP pour apprendre les adresses IP et MAC de la VM.

L'écoute ARP inspecte les trafics ARP et les GARP sortants de la VM pour apprendre les adresses IP et MAC.

VM Tools est un logiciel qui s'exécute sur une machine virtuelle hébergée par ESXi et peut fournir les informations de configuration de la machine virtuelle, y compris les adresses IP et MAC. Cette méthode de découverte d'adresses IP est disponible pour les machines virtuelles en cours d'exécution sur les hôtes ESXi uniquement.

Note Pour les machines virtuelles Linux, le problème de flux ARP peut empêcher l'écoute ARP d'obtenir des informations incorrectes. Le problème peut être évité à l'aide d'un filtre ARP. Pour plus d'informations, consultez <http://linux-ip.net/html/ether-arp.html#ether-arp-flux>.

Configurer un profil de commutation de découverte d'adresses IP

Vous pouvez activer l'écoute ARP, l'écoute DHCP ou VM Tools pour créer un profil de commutation de découverte d'adresses IP personnalisé qui apprend les adresses IP et MAC afin de garantir l'intégrité IP d'un commutateur logique. La méthode de découverte d'adresses IP de VM Tools est disponible uniquement pour les machines virtuelles hébergées par ESXi.

Conditions préalables

Familiarisez-vous avec le concept de profil de commutation de découverte d'adresses IP. Reportez-vous à la section [Comprendre le profil de commutation de découverte d'adresses IP](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Commutation** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Profils de commutation**.
- 4 Cliquez sur **Ajouter** et sélectionnez **Découverte d'adresses IP**.
- 5 Renseignez les détails du profil de commutation de découverte d'adresses IP.

Option	Description
Nom et description	Entrez un nom et éventuellement une description.
Écoute ARP	Basculez le bouton Écoute ARP pour activer la fonctionnalité. L'écoute ARP inspecte le trafic ARP et GARP sortant de la VM pour apprendre les adresses MAC et IP de la VM. L'écoute ARP s'applique si la VM utilise une adresse IP statique plutôt que DHCP.
Limite de liaison ARP	Spécifiez une limite de liaison ARP de 1 à 128.
Écoute DHCP	Basculez le bouton Écoute DHCP pour activer la fonctionnalité. L'écoute DHCP inspecte les paquets DHCP échangés entre le client DHCP de la VM et le serveur DHCP, pour apprendre les adresses MAC et IP de la VM.
VM Tools	Basculez le bouton VM Tools pour activer la fonctionnalité. Cette option n'est disponible que pour les machines virtuelles hébergées par ESXi. VM Tools est un logiciel qui s'exécute sur une machine virtuelle hébergée par ESXi et peut fournir les adresses IP et MAC de la machine virtuelle.

- 6 Cliquez sur **Enregistrer**.

Résultats

Un profil de commutation de découverte d'adresses IP personnalisé s'affiche sous forme de lien.

Étape suivante

Attachez ce profil de commutation de découverte d'adresses IP personnalisé à un commutateur logique ou à un port logique pour que les paramètres modifiés dans le profil de commutation s'appliquent au trafic réseau. Reportez-vous à la section [Associer un profil personnalisé à un commutateur logique](#) ou [Associer un profil personnalisé à un port logique](#).

Comprendre SpoofGuard

SpoofGuard permet d'éviter une forme d'attaque malveillante appelée « falsification Web » ou « hameçonnage ». Une stratégie SpoofGuard bloque le trafic considéré comme falsifié.

SpoofGuard est un outil conçu pour empêcher les machines virtuelles de votre environnement d'envoyer du trafic avec une adresse IP depuis laquelle elles ne sont pas autorisées à mettre fin au trafic. Dans le cas où l'adresse IP d'une machine virtuelle ne correspond pas à l'adresse IP sur le port logique et la liaison d'adresse de commutateur correspondants dans SpoofGuard, la vNIC de la machine virtuelle ne peut pas du tout accéder au réseau. SpoofGuard peut être configuré au niveau du port ou du commutateur. SpoofGuard peut être utilisé dans votre environnement pour plusieurs raisons :

- Il empêche une machine virtuelle non autorisée de supposer l'adresse IP d'une VM existante.
- Il garantit que les adresses IP de machines virtuelles ne peuvent pas être modifiées sans intervention : dans certains environnements, il est préférable que les machines virtuelles ne puissent pas modifier leurs adresses IP sans un examen correct du contrôle des modifications. SpoofGuard facilite cela en s'assurant que le propriétaire de la machine virtuelle ne peut pas simplement modifier l'adresse IP et continuer à travailler sans problème.
- Il garantit que les règles DFW (Distributed Firewall) ne seront pas contournées par inadvertance (ou délibérément) : pour les règles DFW créées à l'aide d'ensembles d'IP comme sources ou destinations, il existe toujours une possibilité que l'adresse IP d'une machine virtuelle puisse être falsifiée dans l'en-tête de paquet, ce qui contourne les règles en question.

La configuration SpoofGuard de NSX-T Data Center couvre les points suivants :

- SpoofGuard MAC : authentifie l'adresse MAC d'un paquet
- SpoofGuard IP : authentifie les adresses MAC et IP d'un paquet
- L'inspection ARP (Address Resolution Protocol) dynamique, la validation SpoofGuard GARP (Gratuitous Address Resolution Protocol) et ND (Neighbor Discovery) se font toutes par rapport au mappage source MAC, source IP et source IP-MAC dans la charge utile ARP/GARP/ND.

Au niveau du port, la liste blanche de MAC/VLAN/IP autorisés est fournie via la propriété Liaisons d'adresse du port. Lorsque la machine virtuelle envoie du trafic, elle est abandonnée si son IP/MAC/VLAN ne correspond pas aux propriétés IP/MAC/VLAN du port. SpoofGuard de niveau port traite l'authentification du trafic, c'est-à-dire qu'il regarde si le trafic est cohérent avec la configuration de VIF.

Au niveau du commutateur, la liste blanche de MAC/VLAN/IP autorisés est fournie via la propriété Liaisons d'adresse du commutateur. En général, il s'agit d'une plage d'adresses IP/sous-réseau autorisés pour le commutateur et SpoofGuard de niveau commutateur traite l'autorisation du trafic.

Le trafic doit être autorisé par SpoofGuard de niveau port ET de niveau commutateur avant qu'il soit autorisé dans le commutateur. L'activation ou la désactivation de SpoofGuard de niveau port et commutateur peut être contrôlée à l'aide du profil de commutateur SpoofGuard.

Configurer des liaisons d'adresse de port

Les liaisons d'adresse spécifient l'adresse IP et l'adresse MAC d'un port logique et sont utilisées pour spécifier la liste blanche de ports dans SpoofGuard.

Avec des liaisons d'adresse de port, vous spécifiez l'adresse IP et l'adresse MAC, et VLAN si applicable, du port logique. Lorsque SpoofGuard est activé, il garantit que les liaisons d'adresse spécifiées sont appliquées dans le chemin d'accès aux données. En plus de SpoofGuard, les liaisons d'adresse de port sont utilisées pour les traductions de règles DFW.

Procédure

- 1 Dans NSX Manager, accédez à **Mise en réseau > Commutation**.
- 2 Cliquez sur l'onglet **Ports**.
- 3 Cliquez sur le port logique auquel vous voulez appliquer la liaison d'adresse.
Le résumé du port logique s'affiche.
- 4 Dans l'onglet **Présentation**, développez **Liaisons d'adresses**.
- 5 Cliquez sur **Ajouter**.
La boîte de dialogue Ajouter une liaison d'adresse s'affiche.
- 6 Spécifiez l'adresse IP et l'adresse MAC du port logique auquel vous voulez appliquer la liaison d'adresse. Vous pouvez également spécifier un ID VLAN.
- 7 Cliquez sur **Ajouter**.

Étape suivante

Utilisez les liaisons d'adresse de port lorsque vous voulez [Configurer un profil de commutation SpoofGuard](#).

Configurer un profil de commutation SpoofGuard

Lorsque SpoofGuard est configuré, si l'adresse IP d'une machine virtuelle change, le trafic de la machine virtuelle peut être bloqué jusqu'à ce que les liaisons d'adresse de port/commutateur correspondantes soient mises à jour avec la nouvelle adresse IP.

Activez SpoofGuard pour le ou les groupes de ports contenant les invités. Lorsqu'il est activé pour chaque adaptateur réseau, SpoofGuard inspecte les paquets de l'adresse MAC prescrite et son adresse IP correspondante.

Procédure

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

- 2 Sélectionnez **Mise en réseau > Commutation** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Profils de commutation**.
- 4 Cliquez sur **Ajouter** et sélectionnez **SpoofGuard**.
- 5 Entrez un nom et éventuellement une description.
- 6 Pour activer SpoofGuard de niveau port, définissez **Liaisons de port** sur **Activé**.
- 7 Cliquez sur **Ajouter**.

Résultats

Un profil de commutation a été créé avec un profil SpoofGuard.

Étape suivante

Associez le profil Spoofguard à un commutateur logique ou à un port logique. Reportez-vous à la section [Associer un profil personnalisé à un commutateur logique](#) ou [Associer un profil personnalisé à un port logique](#).

Comprendre le profil de commutation de sécurité de commutateur

La sécurité de commutateur offre une sécurité de couche 2 et de couche 3 sans état en vérifiant le trafic d'entrée vers le commutateur logique et en abandonnant les paquets non autorisés envoyés à partir de VM en faisant correspondre l'adresse IP, l'adresse MAC et les protocoles avec un ensemble d'adresses et de protocoles autorisés. Vous pouvez utiliser la sécurité de commutateur pour protéger l'intégrité du commutateur logique en éliminant les attaques malveillantes sur les VM du réseau.

Vous pouvez configurer les options de filtre BPDU (Bridge Protocol Data Unit), d'écoute DHCP, de bloc de serveur DHCP et de limitation du taux pour personnaliser le profil de commutation de sécurité de commutateur sur un commutateur logique.

Configurer un profil de commutation de sécurité de commutateur personnalisé

Vous pouvez créer un profil de commutation de sécurité de commutateur personnalisé avec des adresses MAC de destination à partir de la liste de BPDU autorisés et configurer une limitation du taux.

Conditions préalables

Familiarisez-vous avec le concept de profil de commutation de sécurité de commutateur. Reportez-vous à la section [Comprendre le profil de commutation de sécurité de commutateur](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Commutation** dans le panneau de navigation.

- 3 Cliquez sur l'onglet **Profils de commutation**.
- 4 Cliquez sur **Ajouter** et sélectionnez **Sécurité des commutateurs**.
- 5 Renseignez les détails du profil de sécurité de commutateur.

Option	Description
Nom et description	Attribuez un nom au profil de sécurité de commutateur personnalisé. En option, vous pouvez décrire le paramètre que vous avez modifié dans le profil.
Filtre BPDU	Basculez le bouton Filtre BPDU pour activer le filtrage BPDU. Lorsque le filtre BPDU est activé, tout le trafic vers l'adresse MAC de destination du BPDU est bloqué. Le filtre BPDU activé désactive également STP sur les ports de commutateur logique, car il n'est pas prévu que ces ports agissent dans STP.
Liste d'autorisation de filtre BPDU	Cliquez sur l'adresse MAC de destination dans la liste d'adresses MAC de destination de BPDU pour autoriser le trafic vers la destination autorisée.
Filtre DHCP	Basculez les boutons Bloc de serveur et Bloc de client pour activer le filtrage DHCP. Bloc de serveur DHCP bloque le trafic entre un serveur DHCP et un client DHCP. Notez qu'il ne bloque pas le trafic entre un serveur DHCP et un agent du relais DHCP. Bloc de client DHCP empêche une VM d'acquiescer une adresse IP DHCP en bloquant les demandes DHCP.
Bloquer le trafic non-IP	Basculez le bouton Bloquer le trafic non-IP pour autoriser uniquement le trafic IPv4, IPv6, ARP, GARP et BPDU. Le reste du trafic non-IP est bloqué. Le trafic IPv4, IPv6, ARP, GARP et BPDU autorisé est basé sur d'autres stratégies définies dans la configuration de lien d'adresse et SpoofGuard. Par défaut, cette option est désactivée pour autoriser la gestion du trafic non-IP comme trafic normal.
Limites de débit	Définissez un débit maximal pour le trafic de diffusion et de multidiffusion d'entrée ou de sortie. Des débits maximaux sont configurés pour protéger le commutateur logique ou la VM contre, par exemple, les tempêtes de trafic de diffusion. Pour éviter tout problème de connectivité, la valeur minimale du débit maximal doit être ≥ 10 pps.

- 6 Cliquez sur **Ajouter**.

Résultats

Un profil de sécurité de commutateur personnalisé s'affiche sous forme de lien.

Étape suivante

Attachez ce profil de commutation personnalisé de sécurité des commutateurs à un commutateur logique ou à un port logique pour que les paramètres modifiés dans le profil de commutation s'appliquent au trafic réseau. Reportez-vous à la section [Associer un profil personnalisé à un commutateur logique](#) ou [Associer un profil personnalisé à un port logique](#).

Comprendre le profil de commutation de gestion MAC

Le profil de commutation de gestion MAC prend en charge deux fonctionnalités : apprentissage MAC et changement d'adresse MAC.

La fonctionnalité de changement d'adresse MAC permet à une machine virtuelle de modifier son adresse MAC. Une machine virtuelle connectée à un port peut exécuter une commande administrative pour modifier l'adresse MAC de sa vNIC et toujours envoyer et recevoir le trafic sur cette vNIC. Cette fonctionnalité est prise en charge sur ESXi uniquement et pas sur KVM. Cette propriété est désactivée par défaut.

L'apprentissage MAC fournit la connectivité réseau à des déploiements où plusieurs adresses MAC sont configurées derrière une vNIC, par exemple, dans un déploiement d'hyperviseur imbriqué où une VM ESXi est exécutée sur un hôte ESXi et où plusieurs VM sont exécutées dans la VM ESXi. Sans l'apprentissage MAC, lorsque la vNIC de la VM ESXi se connecte à un port de commutateur, son adresse MAC est statique. Les VM exécutées dans la VM ESXi ne bénéficient pas de la connectivité réseau, car leurs paquets ont des adresses MAC sources différentes. Avec l'apprentissage MAC, le vSwitch inspecte l'adresse MAC source de chaque paquet provenant de la vNIC, apprend l'adresse MAC et autorise le paquet à passer. Si une adresse MAC apprise n'est pas utilisée pendant un certain temps, elle est supprimée. Cette propriété de durée n'est pas configurable.

Si vous activez l'apprentissage MAC ou le changement d'adresse MAC, pour améliorer la sécurité, configurez également SpoofGuard.

Configurer le profil de commutation de gestion MAC

Vous pouvez créer un profil de commutation de gestion MAC pour gérer les adresses MAC.

Conditions préalables

Familiarisez-vous avec le concept de profil de commutation de gestion MAC. Reportez-vous à la section [Comprendre le profil de commutation de gestion MAC](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Commutation** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Profils de commutation**.
- 4 Cliquez sur **Ajouter** et sélectionnez **Gestion MAC**.

5 Renseignez les détails du profil de gestion MAC.

Option	Description
Nom et description	Attribuez un nom au profil de gestion MAC. En option, vous pouvez décrire le paramètre que vous avez modifié dans le profil.
Modification de MAC	Activez ou désactivez la fonctionnalité de changement d'adresse MAC.
État	Activez ou désactivez la fonctionnalité d'apprentissage MAC.

6 Cliquez sur **Ajouter**.

Résultats

Un profil de gestion MAC s'affiche sous forme de lien.

Étape suivante

Attachez le profil de commutation à un commutateur logique ou à un port logique. Reportez-vous à la section [Associer un profil personnalisé à un commutateur logique](#) ou [Associer un profil personnalisé à un port logique](#).

Associer un profil personnalisé à un commutateur logique

Vous pouvez associer un profil de commutation personnalisé à un commutateur logique afin que le profil s'applique à tous les ports sur le commutateur.

Lorsque des profils de commutation personnalisés sont attachés à un commutateur logique, ils remplacent les profils de commutation par défaut déjà en place. Les ports de commutateur logique enfants héritent du profil de commutation personnalisé.

Note Si vous avez associé un profil de commutation personnalisé à un commutateur logique, mais que vous souhaitez conserver le profil de commutation par défaut pour l'un des ports de commutateur logique enfants, vous devez effectuer une copie du profil de commutation par défaut et l'associer au port de commutation logique concerné.

Conditions préalables

- Vérifiez qu'un commutateur logique est configuré. Reportez-vous à la section [Créer un commutateur logique](#).
- Vérifiez qu'un profil de commutation personnalisé est configuré. Reportez-vous à la section [Chapitre 3 Basculement des profils pour commutateurs logiques et ports logiques](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Commutation** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Commutateurs**.

- 4 Cliquez sur le commutateur logique pour appliquer le profil de commutation personnalisé.
- 5 Cliquez sur l'onglet **Gérer**.
- 6 Sélectionnez le type de profil de commutation personnalisé dans le menu déroulant.
 - **QoS**
 - **Mise en miroir de ports**
 - **Découverte d'adresses IP**
 - **SpoofGuard**
 - **Sécurité de commutateur**
 - **Gestion MAC**
- 7 Cliquez sur **Modifier**.
- 8 Sélectionnez le profil de commutation personnalisé créé précédemment dans le menu déroulant.
- 9 Cliquez sur **Enregistrer**.

Le commutateur logique est maintenant associé au profil de commutation personnalisé.
- 10 Vérifiez que le nouveau profil de commutation personnalisé avec la configuration modifiée s'affiche dans l'onglet **Gérer**.
- 11 (Facultatif) Cliquez sur l'onglet **Éléments associés** et sélectionnez **Ports** dans le menu déroulant pour vérifier que le profil de commutation personnalisé est appliqué aux ports logiques enfants.

Étape suivante

Si vous ne souhaitez pas utiliser le profil de commutation hérité d'un commutateur logique, vous pouvez appliquer un profil de commutation personnalisé au port de commutateur logique enfant. Reportez-vous à la section [Associer un profil personnalisé à un port logique](#).

Associer un profil personnalisé à un port logique

Un port logique fournit un point de connexion logique pour un VIF, une connexion de correctif à un routeur ou une connexion de passerelle de couche 2 à un réseau externe. Les ports logiques exposent également des profils de commutation, des compteurs de statistiques de port et un état de lien logique.

Vous pouvez modifier le profil de commutation hérité du commutateur logique vers un profil de commutation personnalisé différent pour le port logique enfant.

Conditions préalables

- Vérifiez qu'un port logique est configuré. Reportez-vous à la section [Connexion d'une machine virtuelle à un commutateur logique](#).
- Vérifiez qu'un profil de commutation personnalisé est configuré. Reportez-vous à la section [Chapitre 3 Basculement des profils pour commutateurs logiques et ports logiques](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur *https://<adresse-ip-nsx-manager>*.
- 2 Sélectionnez **Mise en réseau > Commutation** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Ports**.
- 4 Cliquez sur le port logique pour appliquer le profil de commutation personnalisé.
- 5 Cliquez sur l'onglet **Gérer**.
- 6 Sélectionnez le type de profil de commutation personnalisé dans le menu déroulant.
 - **QoS**
 - **Mise en miroir de ports**
 - **Découverte d'adresses IP**
 - **SpoofGuard**
 - **Sécurité de commutateur**
 - **Gestion MAC**
- 7 Cliquez sur **Modifier**.
- 8 Sélectionnez le profil de commutation personnalisé créé précédemment dans le menu déroulant.
- 9 Cliquez sur **Enregistrer**.

Le port logique est maintenant associé au profil de commutation personnalisé.
- 10 Vérifiez que le nouveau profil de commutation personnalisé avec la configuration modifiée s'affiche dans l'onglet **Gérer**.

Étape suivante

Vous pouvez surveiller l'activité sur le port du commutateur logique pour résoudre les problèmes. Reportez-vous à la section « Surveiller l'activité d'un port de commutateur logique » dans le *Guide d'administration de NSX-T Data Center*.

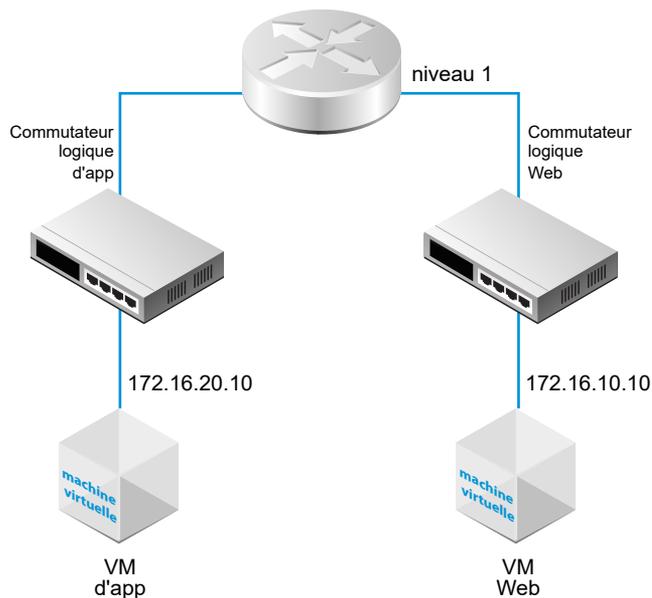
Routeur logique de niveau 1

4

Un routeur logique NSX-T Data Center reproduit la fonctionnalité de routage dans un environnement virtuel complètement découplé du matériel sous-jacent. Les routeurs logiques de niveau 1 disposent de ports de liaison descendante pour se connecter à des commutateurs logiques NSX-T Data Center et des ports de liaison montante pour se connecter à des routeurs logiques de niveau 0 NSX-T Data Center.

Lorsque vous ajoutez un routeur logique, il est important que vous planifiez la topologie de mise en réseau que vous créez.

Figure 4-1. Topologie de routeur logique de niveau 1



Par exemple, cette topologie simple montre deux commutateurs logiques connectés à un routeur logique de niveau 1. Une seule VM est connectée à chaque commutateur logique. Les deux machines virtuelles peuvent être situées sur des hôtes distincts ou un seul et même hôte, dans différents clusters d'hôtes ou le même cluster d'hôtes. Si aucun routeur logique ne sépare les VM, les adresses IP sous-jacentes configurées sur les VM doivent être sur le même sous-réseau. Si un routeur logique les sépare, les adresses IP sur les VM doivent être sur des sous-réseaux différents.

Ce chapitre contient les rubriques suivantes :

- [Créer un routeur logique de niveau 1](#)
- [Ajouter un port de liaison descendante sur un routeur logique de niveau 1](#)
- [Ajouter un port VLAN sur un routeur logique de niveau 0 ou de niveau 1](#)
- [Configurer l'annonce d'itinéraires sur un routeur logique de niveau 1](#)
- [Configurer l'itinéraire statique d'un routeur logique de niveau 1](#)
- [Créer un routeur logique de niveau 1 autonome](#)

Créer un routeur logique de niveau 1

Le routeur logique de niveau 1 doit être connecté au routeur logique de niveau 0 pour pouvoir accéder au routeur physique ascendant.

Conditions préalables

- Vérifiez que les commutateurs logiques sont configurés. Reportez-vous à la section [Créer un commutateur logique](#).
- Vérifiez qu'un cluster NSX Edge est déployé pour effectuer la configuration de la NAT (Network Address Translation). Reportez-vous à *Guide d'installation de NSX-T Data Center*.
- Familiarisez-vous avec la topologie du routeur logique de niveau 1. Reportez-vous à la section [Chapitre 4 Routeur logique de niveau 1](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Cliquez sur **Ajouter** et sélectionnez **Routeur de niveau 1**.
- 4 Entrez un nom pour le routeur logique et éventuellement une description.
- 5 (Facultatif) Sélectionnez un routeur logique de niveau 0 à connecter à ce routeur logique de niveau 1.
Si aucun routeur logique de niveau 0 n'est encore configuré, vous pouvez laisser ce champ vide pour le moment et modifier la configuration du routeur ultérieurement.
- 6 (Facultatif) Sélectionnez un cluster NSX Edge à connecter à ce routeur logique de niveau 1.
Si le routeur logique de niveau 1 est utilisé pour la configuration de la NAT, il doit être connecté à un cluster NSX Edge. Si vous n'avez encore configuré aucun cluster NSX Edge, vous pouvez laisser ce champ vide pour le moment et modifier la configuration du routeur ultérieurement.

7 (Facultatif) Si vous avez sélectionné un cluster NSX Edge, sélectionnez un mode de basculement.

Option	Description
Préemptif	Si le nœud préféré échoue et récupère, il prévaut sur son homologue et devient le nœud actif. L'homologue modifie son état sur veille. Il s'agit de l'option par défaut.
Non préemptif	Si le nœud préféré échoue et récupère, il vérifie si son homologue est le nœud actif. Si c'est le cas, le nœud préféré ne prévaut pas sur son homologue et est le nœud en veille.

8 (Facultatif) Cliquez sur l'onglet **Avancé** et entrez une valeur pour **Sous-réseau de transit intra Tier1**.

9 Cliquez sur **Ajouter**.

Dans l'interface utilisateur de NSX Manager, le nouveau routeur logique est un lien hypertexte.

Résultats

Si ce routeur logique prend en charge plus de 5 000 machines virtuelles, vous devez exécuter les commandes suivantes sur chaque nœud du cluster NSX Edge pour augmenter la taille de la table ARP.

```
set debug-mode
set dataplane neighbor max-arp-logical-router 10000
```

Vous devez exécuter de nouveau les commandes après un redémarrage du plan de données ou un redémarrage du nœud, car la modification n'est pas persistante.

Étape suivante

Créez des ports de liaison descendante pour votre routeur logique de niveau 1. Reportez-vous à la section [Ajouter un port de liaison descendante sur un routeur logique de niveau 1](#).

Ajouter un port de liaison descendante sur un routeur logique de niveau 1

Lorsque vous créez un port de liaison descendante sur un routeur logique de niveau 1, le port sert de passerelle par défaut pour les VM se trouvant dans le même sous-réseau.

Conditions préalables

Vérifiez qu'un routeur logique de niveau 1 est configuré. Reportez-vous à la section [Créer un routeur logique de niveau 1](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Cliquez sur le nom d'un routeur.
- 4 Cliquez sur l'onglet **Configuration** et sélectionnez **Ports de routeur**.

- 5 Cliquez sur **Ajouter**.
- 6 Entrez un nom pour le port de routeur et éventuellement une description.
- 7 Dans le champ **Type**, sélectionnez **Liaison descendante**.
- 8 Pour **Mode URPF**, sélectionnez **Strict** ou **Aucun**.
URPF (Unicast Reverse Path Forwarding) est une fonctionnalité de sécurité.
- 9 (Facultatif) Sélectionnez un commutateur logique.
- 10 Indiquez si cette association crée un port de commutateur ou met à jour un port de commutateur existant.

Si l'association est destinée à un port de commutateur existant, sélectionnez le port dans le menu déroulant.
- 11 Entrez l'adresse IP du port de routeur dans la notation CIDR.

Par exemple, l'adresse IP peut être 172.16.10.1/24.
- 12 (Facultatif) Sélectionnez un service de relais DHCP.
- 13 Cliquez sur **Ajouter**.

Étape suivante

Activez l'annonce d'itinéraires pour fournir une connectivité Nord-Sud entre les VM et les réseaux physiques externes ou entre différents routeurs logiques de niveau 1 qui sont connectés au même routeur logique de niveau 0. Reportez-vous à la section [Configurer l'annonce d'itinéraires sur un routeur logique de niveau 1](#).

Ajouter un port VLAN sur un routeur logique de niveau 0 ou de niveau 1

Si vous disposez uniquement de commutateurs logiques reposant sur un VLAN, vous pouvez connecter les commutateurs aux ports VLAN sur un routeur de niveau 0 ou de niveau 1 de sorte que NSX-T Data Center puisse fournir des services de niveau 3.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Cliquez sur le nom d'un routeur.
- 4 Cliquez sur l'onglet **Configuration** et sélectionnez **Ports de routeur**.
- 5 Cliquez sur **Ajouter**.
- 6 Entrez un nom pour le port de routeur et éventuellement une description.
- 7 Dans le champ **Type**, sélectionnez **Centralisé**.

8 Pour **Mode URPF**, sélectionnez **Strict** ou **Aucun**.

URPF (Unicast Reverse Path Forwarding) est une fonctionnalité de sécurité.

9 (Requis) Sélectionnez un commutateur logique.

10 Indiquez si cette association crée un port de commutateur ou met à jour un port de commutateur existant.

Si l'association est destinée à un port de commutateur existant, sélectionnez le port dans le menu déroulant.

11 Entrez l'adresse IP du port de routeur dans la notation CIDR.

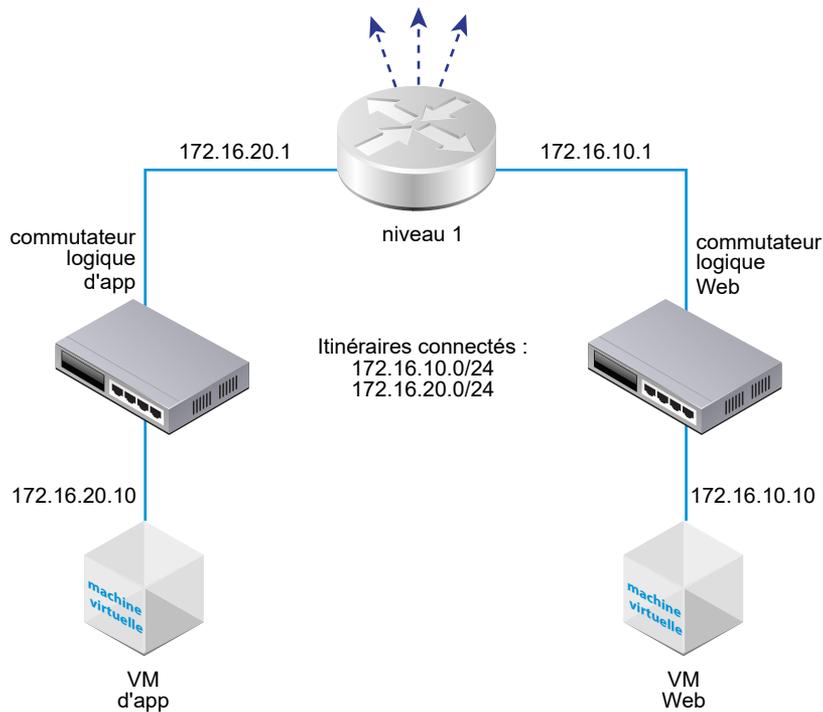
12 Cliquez sur **Ajouter**.

Configurer l'annonce d'itinéraires sur un routeur logique de niveau 1

Pour fournir une connectivité de couche 3 entre des VM connectées à des commutateurs logiques attachés à différents routeurs logiques de niveau 1, il est nécessaire d'activer l'annonce d'itinéraires de niveau 1 vers le niveau 0. Vous n'avez pas besoin de configurer un protocole de routage ou des itinéraires statiques entre des routeurs logiques de niveau 1 et des routeurs logiques de niveau 0. NSX-T Data Center crée des itinéraires statiques NSX-T Data Center automatiquement lorsque vous activez l'annonce d'itinéraires.

Par exemple, pour fournir une connectivité vers et depuis les VM via d'autres routeurs homologues, l'annonce d'itinéraires doit être configurée sur le routeur logique de niveau 1 pour les itinéraires connectés. Si vous ne voulez pas annoncer tous les itinéraires connectés, vous pouvez spécifier les itinéraires à annoncer.

Annoncer des itinéraires connectés



Conditions préalables

- Vérifiez que des VM sont attachées à des commutateurs logiques. Reportez-vous à la section [Chapitre 1 Commutateurs logiques et configuration d'un attachement de VM](#).
- Vérifiez que des ports de liaison descendante pour le routeur logique de niveau 1 sont configurés. Reportez-vous à la section [Ajouter un port de liaison descendante sur un routeur logique de niveau 1](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Cliquez sur le nom d'un routeur de niveau 1.
- 4 Sélectionnez **Annonce de route** dans le menu déroulant **Routage**.
- 5 Cliquez sur **Modifier** pour modifier la configuration de l'annonce de route.

Vous pouvez basculer les commutateurs suivants :

- **État**
- **Annoncer toutes les routes connectées à NSX**
- **Annoncer toutes les routes NAT**
- **Annoncer toutes les routes statiques**

- **Annoncer toutes les routes VIP de LB**
- **Annoncer toutes routes IP du SNAT LB**

a Cliquez sur **Enregistrer**.

6 Cliquez sur **Ajouter** pour annoncer des routes.

- a Entrez un nom et éventuellement une description.
- b Entrez un préfixe de route au format CIDR.
- c Cliquez sur **Appliquer le filtre** pour définir les options suivantes :

Action	Spécifiez Autoriser ou Refuser .
Faire correspondre les types de route	Sélectionnez une ou plusieurs des options suivantes : <ul style="list-style-type: none"> ■ Quelconque ■ NSX connecté ■ VIP d'équilibrage de charge de niveau 1 ■ Statique ■ NAT de niveau 1 ■ SNAT d'équilibrage de charge de niveau 1
Opérateur de préfixe	Sélectionnez GE ou EQ .

d Cliquez sur **Ajouter**.

Étape suivante

Familiarisez-vous avec la topologie de routeur logique de niveau 0 et créez le routeur logique de niveau 0. Reportez-vous à la section [Chapitre 5 Routeur logique de niveau 0](#).

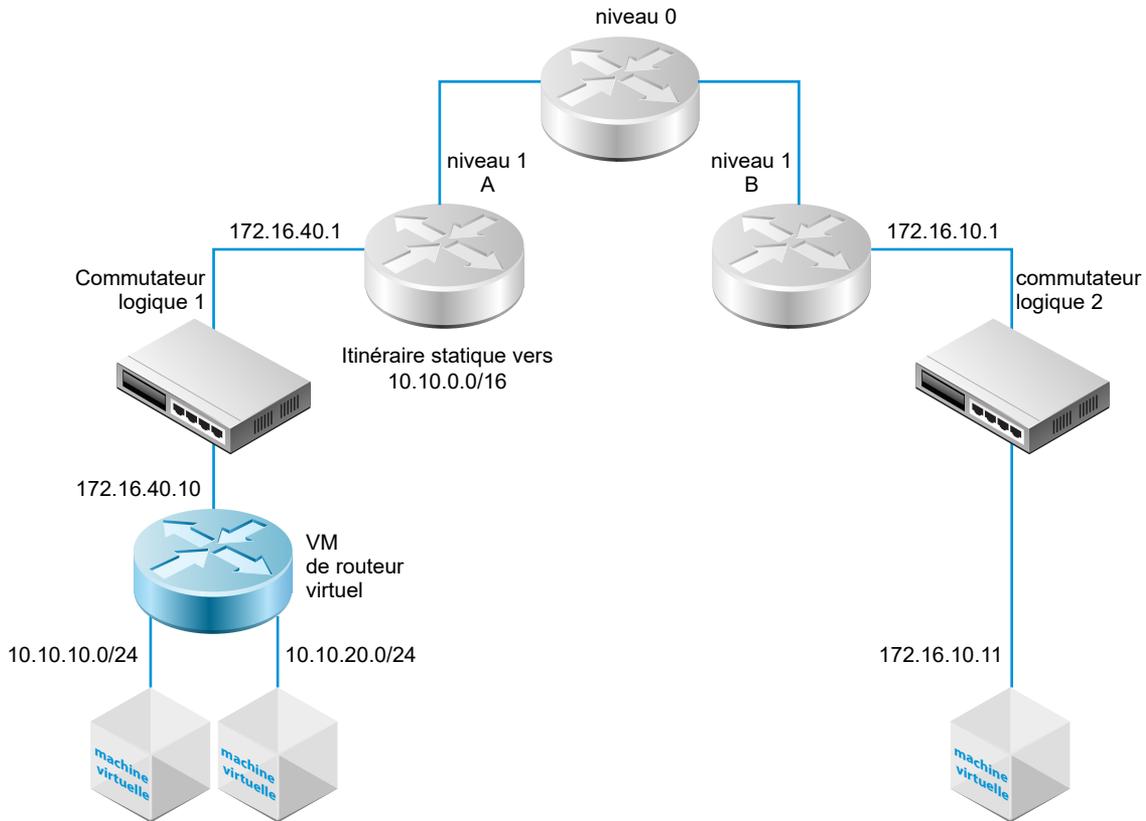
Si vous disposez déjà d'un routeur logique de niveau 0 connecté au routeur logique de niveau 1, vous pouvez vérifier que le routeur de niveau 0 apprend les itinéraires connectés du routeur de niveau 1. Reportez-vous à la section [Vérifier qu'un routeur de niveau 0 a appris des itinéraires d'un routeur de niveau 1](#).

Configurer l'itinéraire statique d'un routeur logique de niveau 1

Vous pouvez configurer un itinéraire statique sur un routeur logique de niveau 1 pour fournir à NSX-T Data Center une connectivité à un ensemble de réseaux accessibles via un routeur virtuel.

Par exemple, sur le diagramme suivant, le routeur logique de niveau 1 a un port de liaison descendante vers un commutateur logique NSX-T Data Center. Ce port de liaison descendante (172.16.40.1) sert de passerelle par défaut à la machine virtuelle du routeur virtuel. La machine virtuelle du routeur virtuel et le niveau 1 A sont connectés via le même commutateur logique NSX-T Data Center. Le routeur logique de niveau 1 a un itinéraire statique 10.10.0.0/16 qui synthétise les réseaux disponibles via le routeur virtuel. La fonction d'annonce d'itinéraires est configurée sur le niveau 1 A pour annoncer l'itinéraire statique au niveau 1 B.

Figure 4-2. Topologie de l'itinéraire statique du routeur logique de niveau 1



Conditions préalables

Vérifiez qu'un port de liaison descendante est configuré. Reportez-vous à la section [Ajouter un port de liaison descendante sur un routeur logique de niveau 1](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Cliquez sur le nom d'un routeur de niveau 1.
- 4 Cliquez sur l'onglet **Routage** et sélectionnez **Itinéraires statiques** dans le menu déroulant.
- 5 Cliquez sur **Ajouter**.
- 6 Entrez une adresse réseau au format CIDR.
Par exemple, 10.10.10.0/16.
- 7 Cliquez sur **Ajouter** pour ajouter une adresse IP de tronçon suivant.
Par exemple, 172.16.40.10. Vous pouvez également spécifier un itinéraire nul en cliquant sur l'icône de crayon et en sélectionnant **NULL** dans la liste déroulante. Pour ajouter d'autres adresses de tronçon suivant, cliquez de nouveau sur **Ajouter**.

8 Cliquez sur **Ajouter** en bas de la boîte de dialogue.

L'adresse réseau d'itinéraire statique qui vient d'être créée s'affiche dans la ligne.

9 À partir du routeur logique de niveau 1, sélectionnez **Routage > Annonce d'itinéraires**.

10 Cliquez sur **Modifier** et sélectionnez **Annoncer toutes les routes statiques**.

11 Cliquez sur **Enregistrer**.

L'itinéraire statique est propagé dans toute la superposition NSX-T Data Center.

Créer un routeur logique de niveau 1 autonome

Un routeur logique de niveau 1 autonome ne dispose d'aucune liaison descendante et d'aucune connexion à un routeur de niveau 0. Il dispose d'un routeur de services, mais d'aucun routeur distribué. Le routeur de services peut être déployé sur un seul nœud NSX Edge ou sur deux nœuds NSX Edge en mode actif-veille.

Un routeur logique de niveau 1 autonome :

- Ne doit pas disposer d'une connexion à un routeur logique de niveau 0.
- Ne doit pas disposer d'une liaison descendante.
- Peut n'avoir qu'un seul port de service centralisée (CSP) s'il est utilisé pour joindre un service d'équilibrage de charge.
- Peut se connecter à un commutateur logique de superposition ou à un commutateur logique VLAN.
- Prend en charge l'équilibrage de charge et les services NAT uniquement.

Généralement, un routeur logique de niveau 1 autonome est connecté à un commutateur logique également connecté à un routeur logique de niveau 1 ordinaire. Le routeur logique de niveau 1 autonome peut communiquer avec d'autres périphériques via le routeur logique de niveau 1 ordinaire après que des annonces d'itinéraires et d'itinéraires statiques ont été configurés.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Cliquez sur **Ajouter** et sélectionnez **Routeur de niveau 1**.
- 4 Entrez un nom pour le routeur logique et éventuellement une description.
- 5 (Requis) Sélectionnez un cluster NSX Edge à connecter à ce routeur logique de niveau 1.

6 (Requis) Sélectionnez un mode de basculement et les membres du cluster.

Option	Description
Préemptif	Si le nœud préféré échoue et récupère, il prévaut sur son homologue et devient le nœud actif. L'homologue modifie son état sur veille. Il s'agit de l'option par défaut.
Non préemptif	Si le nœud préféré échoue et récupère, il vérifie si son homologue est le nœud actif. Si c'est le cas, le nœud préféré ne prévaut pas sur son homologue et est le nœud en veille.

7 Cliquez sur **Ajouter**.

8 Cliquez sur le nom du routeur que vous venez de créer.

9 Cliquez sur l'onglet **Configuration** et sélectionnez **Ports de routeur**.

10 Cliquez sur **Ajouter**.

11 Entrez un nom pour le port de routeur et éventuellement une description.

12 Dans le champ **Type**, sélectionnez **Centralisé**.

13 Pour **Mode URPF**, sélectionnez **Strict** ou **Aucun**.

URPF (Unicast Reverse Path Forwarding) est une fonctionnalité de sécurité.

14 (Requis) Sélectionnez un commutateur logique.

15 Indiquez si cette association crée un port de commutateur ou met à jour un port de commutateur existant.

16 Entrez l'adresse IP du port de routeur dans la notation CIDR.

17 Cliquez sur **Ajouter**.

Résultats

Avant de pouvoir utiliser le routeur logique de niveau 1 autonome, notez les points suivants :

- Pour spécifier la passerelle par défaut pour le routeur logique de niveau 1 autonome, vous devez ajouter un itinéraire statique. Le sous-réseau doit être 0.0.0.0/0 et le saut suivant est l'adresse IP d'un routeur de niveau 1 ordinaire connecté au même commutateur.
- Le proxy ARP sur le routeur autonome n'est pas pris en charge. Par conséquent, vous ne devez pas configurer l'adresse IP d'un serveur virtuel LB ou l'adresse IP d'un LB SNAT dans le sous-réseau du fournisseur du CSP, sauf si vous utilisez l'adresse IP de CSP. Par exemple, si l'adresse IP de CSP est 1.1.1.1/24, l'adresse IP virtuelle doit être 1.1.1.1 ou d'autres adresses IP de sous-réseau. Il ne peut pas s'agir d'une autre adresse du sous-réseau 1.1.1.1/24.
- Pour une VM NSX Edge, vous ne pouvez pas disposer de plusieurs CSP qui sont connectés au même commutateur logique basé sur VLAN ou différents commutateurs logiques basés sur VLAN ayant le même ID de VLAN.

Routeur logique de niveau 0

5

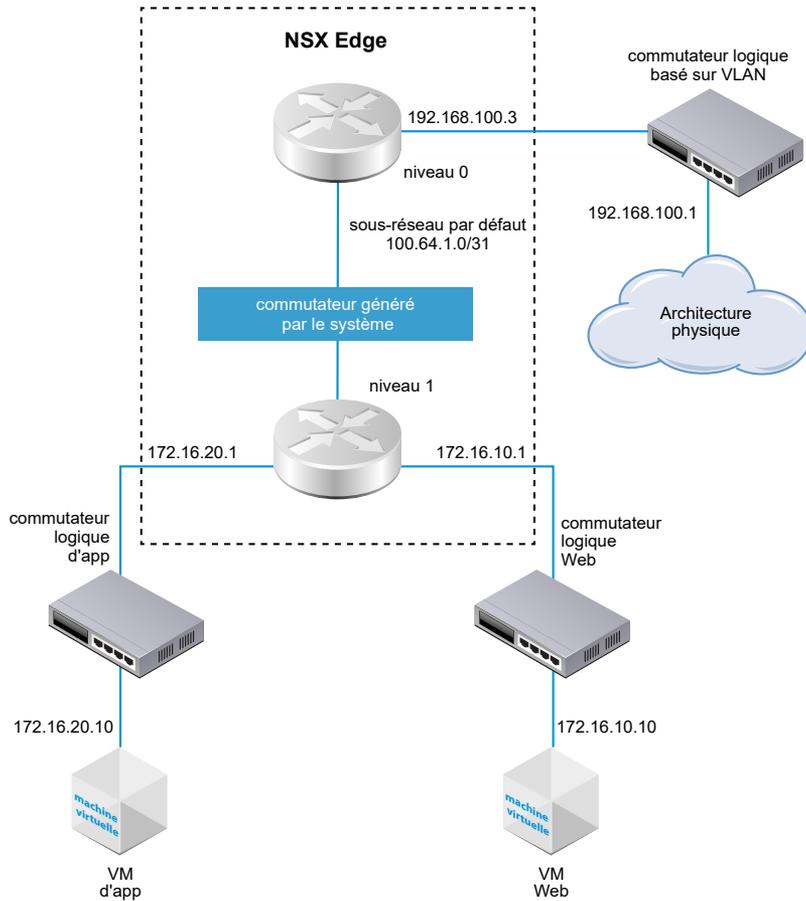
Un routeur logique NSX-T Data Center reproduit la fonctionnalité de routage dans un environnement virtuel complètement découplé du matériel sous-jacent. Le routeur logique de niveau 0 fournit un service de passerelle par intermittence entre le réseau logique et le réseau physique.

Remarques concernant NSX Cloud Si vous utilisez NSX Cloud, reportez-vous à la section [Comment utiliser des fonctionnalités NSX-T Data Center avec le cloud public](#) pour obtenir la liste des entités logiques générées automatiquement, les fonctionnalités prises en charge et les configurations requises pour NSX Cloud.

Un cluster NSX Edge peut sauvegarder plusieurs routeurs logiques de niveau 0. Les routeurs de niveau 0 prennent en charge le protocole de routage dynamique BGP et ECMP.

Lorsque vous ajoutez un routeur logique de niveau 0, il est important que vous planifiez la topologie de mise en réseau que vous créez.

Figure 5-1. Topologie du routeur logique de niveau 0



À des fins de simplicité, l'exemple de topologie montre un routeur logique de niveau 1 connecté à un routeur logique de niveau 0 hébergé sur un nœud NSX Edge. Rappelez-vous qu'il ne s'agit pas d'une topologie recommandée. Dans l'idéal, vous devez disposer d'un minimum de deux nœuds NSX Edge pour profiter complètement de la conception du routeur logique.

Le routeur logique de niveau 1 dispose d'un commutateur logique Web et d'un commutateur logique d'application avec des VM respectives attachées. Le commutateur routeur-lien entre le routeur de niveau 1 et le routeur de niveau 0 est créé automatiquement lorsque vous attachez le routeur de niveau 1 au routeur de niveau 0. Par conséquent, ce commutateur est étiqueté comme généré par le système.

Ce chapitre contient les rubriques suivantes :

- [Créer un routeur logique de niveau 0](#)
- [Attacher le niveau 0 et le niveau 1](#)
- [Connecter un routeur logique de niveau 0 à un commutateur logique VLAN pour la liaison montante NSX Edge](#)
- [Ajouter un port de routeur de bouclage](#)
- [Ajouter un port VLAN sur un routeur logique de niveau 0 ou de niveau 1](#)

- [Configurer un itinéraire statique](#)
- [Options de configuration de BGP](#)
- [Configurer BFD sur un routeur logique de niveau 0](#)
- [Activer la redistribution d'itinéraire sur le routeur logique de niveau 0](#)
- [Comprendre le routage ECMP](#)
- [Créer une liste de préfixes IP](#)
- [Créer une liste de communauté](#)
- [Créer une carte de route](#)
- [Configurer le temporisateur d'activation du transfert](#)

Créer un routeur logique de niveau 0

Les routeurs logiques de niveau 0 disposent de ports de liaison descendante pour se connecter à des routeurs logiques de niveau 1 NSX-T Data Center et des ports de liaison montante pour se connecter à des réseaux externes.

Conditions préalables

- Vérifiez qu'au moins un dispositif NSX Edge est installé. Consultez le *Guide d'installation de NSX-T Data Center*.
- Vérifiez que votre cluster NSX Controller est stable.
- Vérifiez qu'un cluster NSX Edge est configuré. Reportez-vous à *Guide d'installation de NSX-T Data Center*.
- Familiarisez-vous avec la topologie de mise en réseau du routeur logique de niveau 0. Reportez-vous à la section [Chapitre 5 Routeur logique de niveau 0](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Cliquez sur **Ajouter** pour créer un routeur logique de niveau 0.
- 4 Sélectionnez **Routeur de niveau 0** dans le menu déroulant.
- 5 Attribuez un nom au routeur logique de niveau 0.
- 6 Sélectionnez un cluster NSX Edge existant dans le menu déroulant pour sauvegarder ce routeur logique de niveau 0.

7 (Facultatif) Sélectionnez un mode haute disponibilité.

Par défaut, le mode actif-actif est utilisé. En mode actif-actif, le trafic est à équilibrage de charge sur tous les membres. En mode actif-veille, tout le trafic est traité par un membre actif choisi. Si le membre actif échoue, un nouveau membre est choisi pour être actif.

8 (Facultatif) Cliquez sur l'onglet **Avancé** pour entrer un sous-réseau pour le sous-réseau de transit intra-niveau 0.

Il s'agit du sous-réseau qui se connecte au routeur de services de niveau 0 vers son routeur distribué. Si vous laissez cette case vide, le sous-réseau 169.0.0.0/28 par défaut est utilisé.

9 (Facultatif) Cliquez sur l'onglet **Avancé** pour entrer un sous-réseau pour le sous-réseau de transit niveau 0-niveau 1.

Il s'agit du sous-réseau qui se connecte au routeur de niveau 0 à n'importe quels routeurs de niveau 1 qui se connectent à ce routeur de niveau 0. Si vous laissez cette case vide, l'espace d'adressage par défaut attribué pour ces connexions de niveau 0 à niveau 1 est 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.

10 Cliquez sur **Enregistrer**.

Le nouveau routeur logique de niveau 0 s'affiche sous forme de lien.

11 (Facultatif) Cliquez sur le lien du routeur logique de niveau 0 pour voir le résumé.

Étape suivante

Attachez des routeurs logiques de niveau 1 à ce routeur logique de niveau 0.

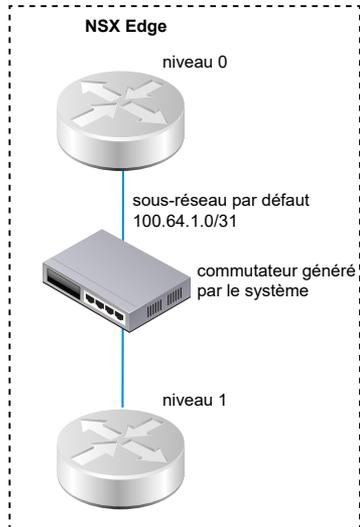
Configurez le routeur logique de niveau 0 pour le connecter à un commutateur logique VLAN afin de créer une liaison montante vers un réseau externe. Reportez-vous à la section [Connecter un routeur logique de niveau 0 à un commutateur logique VLAN pour la liaison montante NSX Edge](#).

Attacher le niveau 0 et le niveau 1

Vous pouvez attacher le routeur logique de niveau 0 au routeur logique de niveau 1 pour que le routeur logique de niveau 1 soit en direction du nord et obtienne la connectivité réseau est-ouest.

Lorsque vous attachez un routeur logique de niveau 1 à un routeur logique de niveau 0, un commutateur routeur-lien entre les deux routeurs est créé. Ce commutateur est étiqueté comme généré par le système dans la topologie. L'espace d'adressage par défaut attribué pour ces connexions de niveau 0 à niveau 1 est 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. En option, vous pouvez configurer l'espace d'adressage dans la configuration de niveau 0 **Résumé > Avancé**.

La figure suivante montre un exemple de topologie.



Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Sélectionnez le routeur logique de niveau 1.
- 4 Dans l'onglet **Résumé**, cliquez sur **Modifier**.
- 5 Sélectionnez le routeur logique de niveau 0 dans le menu déroulant.
- 6 (Facultatif) Sélectionnez un cluster NSX Edge dans le menu déroulant.

Le routeur de niveau 1 doit être sauvegardé par un périphérique Edge si le routeur est utilisé pour des services, tels que NAT. Si vous ne sélectionnez pas un cluster NSX Edge, le routeur de niveau 1 ne peut pas effectuer NAT.

- 7 Spécifiez des membres et un membre préféré.

Si vous sélectionnez un cluster NSX Edge et que vous laissez les champs des membres et du membre préféré vides, NSX-T Data Center définit automatiquement le périphérique Edge de sauvegarde à partir du cluster spécifié.

- 8 Cliquez sur **Enregistrer**.
- 9 Cliquez sur l'onglet **Configuration** du routeur de niveau 1 pour vérifier qu'une nouvelle adresse IP de port lié point-à-point est créée.

Par exemple, l'adresse IP du port lié peut être 100.64.1.1/31.

- 10 Sélectionnez le routeur logique de niveau 0 dans le panneau de navigation.
- 11 Cliquez sur l'onglet **Configuration** du routeur de niveau 0 pour vérifier qu'une nouvelle adresse IP de port lié point-à-point est créée.

Par exemple, l'adresse IP du port lié peut être 100.64.1.1/31.

Étape suivante

Vérifiez que le routeur de niveau 0 apprend les itinéraires qui sont annoncés par les routeurs de niveau 1.

Vérifier qu'un routeur de niveau 0 a appris des itinéraires d'un routeur de niveau 1

Lorsqu'un routeur logique de niveau 1 annonce des itinéraires à un routeur logique de niveau 0, les itinéraires sont répertoriés dans la table de routage du routeur de niveau 0 sous la forme d'itinéraires statiques NSX-T Data Center.

Procédure

- 1 Sur le dispositif NSX Edge, exécutez la commande `get logical-routers` pour rechercher le numéro VRF du routeur de service de niveau 0.

```
nsx-edge-1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 0
type       : TUNNEL

Logical Router
UUID       : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf        : 6
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf        : 7
type       : SERVICE_ROUTER_TIER1

Logical Router
UUID       : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf        : 8
type       : DISTRIBUTED_ROUTER
```

- 2 Exécutez la commande `vrf <number>` pour entrer le contexte du routeur de service de niveau 0.

```
nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>
```

- 3 Sur le routeur de service de niveau 0, exécutez la commande `get route` et assurez-vous que les itinéraires attendus s'affichent dans la table de routage.

Notez que les itinéraires statiques NSX-T Data Center (ns) sont appris par le routeur de niveau 0, car le routeur de niveau 1 annonce des itinéraires.

```
nsx-edge1(tier0_sr)> get route

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

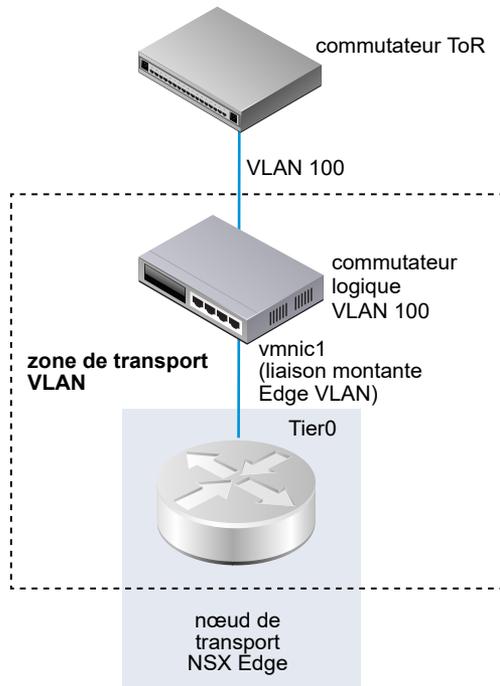
Total number of routes: 7

b  10.10.10.0/24      [20/0]      via 192.168.100.254
rl 100.91.176.0/31   [0/0]      via 169.254.0.1
c  169.254.0.0/28    [0/0]      via 169.254.0.2
ns 172.16.10.0/24 [3/3] via 169.254.0.1 ns 172.16.20.0/24 [3/3] via 169.254.0.1
c  192.168.100.0/24 [0/0]      via 192.168.100.2
```

Connecter un routeur logique de niveau 0 à un commutateur logique VLAN pour la liaison montante NSX Edge

Pour créer une liaison montante NSX Edge, vous devez connecter un routeur de niveau 0 à un commutateur VLAN.

La topologie simple suivante montre un commutateur logique VLAN à l'intérieur d'une zone de transport VLAN. Le commutateur logique VLAN dispose d'un ID de VLAN qui correspond à l'ID de VLAN sur le port TOR pour la liaison montante VLAN du dispositif Edge.



Conditions préalables

Créez un commutateur logique VLAN. Reportez-vous à la section [Créer un commutateur logique VLAN pour la liaison montante NSX Edge](#).

Créez un routeur de niveau 0.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Sélectionnez le routeur logique de niveau 0.
- 4 Dans l'onglet **Configuration**, ajoutez un nouveau port de routeur logique.
- 5 Tapez un nom pour le port, tel que liaison montante.
- 6 Sélectionnez le type **Liaison montante**.
- 7 Sélectionnez un nœud de transport Edge.
- 8 Sélectionnez un commutateur logique VLAN.
- 9 Tapez une adresse IP au format CIDR dans le même sous-réseau que le port connecté sur le commutateur TOR.

Résultats

Un nouveau port de liaison montante est ajouté pour le routeur de niveau 0.

Étape suivante

Configurez BGP ou un itinéraire statique.

Vérifier le routeur logique de niveau 0 et la connexion ToR

Pour que le routage fonctionne sur la liaison montante à partir du routeur de niveau 0, la connectivité avec l'appareil ToR doit être configurée.

Conditions préalables

- Vérifiez que le routeur logique de niveau 0 est connecté à un commutateur logique VLAN. Reportez-vous à la section [Connecter un routeur logique de niveau 0 à un commutateur logique VLAN pour la liaison montante NSX Edge](#).

Procédure

- 1 Connectez-vous à l'interface de ligne de commande de NSX Manager.
- 2 Sur le dispositif NSX Edge, exécutez la commande `get logical-routers` pour rechercher le numéro VRF du routeur de service de niveau 0.

```
nsx-edge-1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 0
type       : TUNNEL

Logical Router
UUID       : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf        : 6
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf        : 7
type       : SERVICE_ROUTER_TIER1

Logical Router
UUID       : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf        : 8
type       : DISTRIBUTED_ROUTER
```

- 3 Exécutez la commande `vrf <number>` pour entrer le contexte du routeur de service de niveau 0.

```
nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>
```

- 4 Sur le routeur de services de niveau 0, exécutez la commande `get route` et assurez-vous que l'itinéraire attendu apparaît bien dans la table de routage.

Notez que l'itinéraire vers l'appareil TOR apparaît comme connecté (c).

```
nsx-edge1(tier0_sr)> get route

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

Total number of routes: 7

b   10.10.10.0/24      [20/0]      via 192.168.100.254
rl  100.91.176.0/31   [0/0]       via 169.254.0.1
c   169.254.0.0/28    [0/0]       via 169.254.0.2
ns  172.16.10.0/24    [3/3]       via 169.254.0.1
ns  172.16.20.0/24   [3/3]       via 169.254.0.1
c  192.168.100.0/24 [0/0]      via 192.168.100.2
```

- 5 Envoyez une requête Ping vers l'appareil TOR.

```
nsx-edge1(tier0_sr)> ping 192.168.100.254
PING 192.168.100.254 (192.168.100.254): 56 data bytes
64 bytes from 192.168.100.254: icmp_seq=0 ttl=64 time=2.822 ms
64 bytes from 192.168.100.254: icmp_seq=1 ttl=64 time=1.393 ms
^C
nsx-edge1>
--- 192.168.100.254 ping statistics ---
3 packets transmitted, 2 packets received, 33.3% packet loss
round-trip min/avg/max/stddev = 1.393/2.107/2.822/0.715 ms
```

Résultats

Les paquets sont envoyés entre le routeur logique de niveau 0 et le routeur physique pour vérifier la connexion.

Étape suivante

Selon vos besoins réseau, vous pouvez configurer un itinéraire statique ou BGP. Reportez-vous à la section [Configurer un itinéraire statique](#) ou [Configurer BGP sur un routeur logique de niveau 0](#).

Ajouter un port de routeur de bouclage

Vous pouvez ajouter un port de bouclage à un routeur logique de niveau 0.

Le port de bouclage peut être utilisé dans les cas suivants :

- Identifiant de routeur pour protocoles de routage
- NAT
- BFD
- Adresse source pour protocoles de routage

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Sélectionnez le routeur logique de niveau 0.
- 4 Sélectionnez **Configuration > Ports de routeur**
- 5 Cliquez sur **Ajouter**.
- 6 Entrez un nom et éventuellement une description.
- 7 Sélectionnez le type **Bouclage**.
- 8 Sélectionnez un nœud de transport Edge.
- 9 Entrez une adresse IP au format CIDR.

Résultats

Un nouveau port est ajouté pour le routeur de niveau 0.

Ajouter un port VLAN sur un routeur logique de niveau 0 ou de niveau 1

Si vous disposez uniquement de commutateurs logiques reposant sur un VLAN, vous pouvez connecter les commutateurs aux ports VLAN sur un routeur de niveau 0 ou de niveau 1 de sorte que NSX-T Data Center puisse fournir des services de niveau 3.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Cliquez sur le nom d'un routeur.
- 4 Cliquez sur l'onglet **Configuration** et sélectionnez **Ports de routeur**.

- 5 Cliquez sur **Ajouter**.
- 6 Entrez un nom pour le port de routeur et éventuellement une description.
- 7 Dans le champ **Type**, sélectionnez **Centralisé**.
- 8 Pour **Mode URPF**, sélectionnez **Strict** ou **Aucun**.
URPF (Unicast Reverse Path Forwarding) est une fonctionnalité de sécurité.
- 9 (Requis) Sélectionnez un commutateur logique.
- 10 Indiquez si cette association crée un port de commutateur ou met à jour un port de commutateur existant.

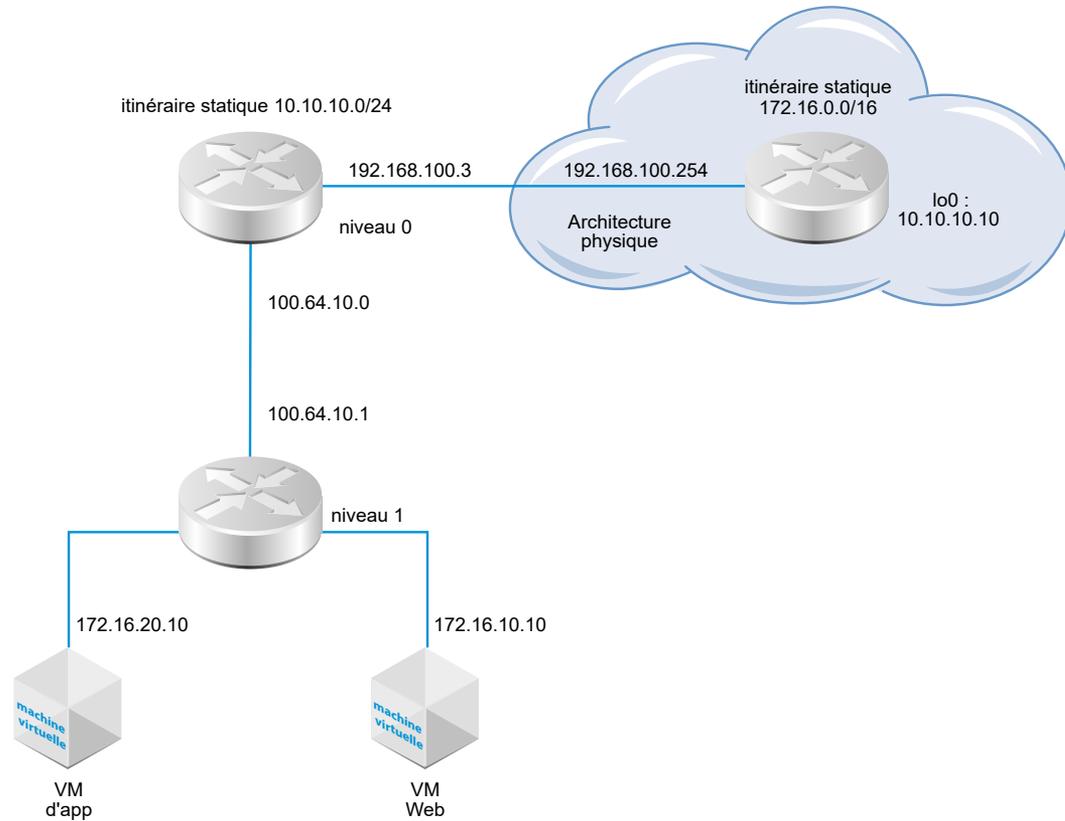
Si l'association est destinée à un port de commutateur existant, sélectionnez le port dans le menu déroulant.
- 11 Entrez l'adresse IP du port de routeur dans la notation CIDR.
- 12 Cliquez sur **Ajouter**.

Configurer un itinéraire statique

Vous pouvez configurer un itinéraire statique sur le routeur de niveau 0 vers des réseaux externes. Une fois que vous avez configuré un itinéraire statique, il n'est pas nécessaire d'annoncer l'itinéraire de niveau 0 à niveau 1, car les routeurs de niveau 1 disposent automatiquement d'un itinéraire par défaut statique vers leur routeur de niveau 0 connecté.

La topologie d'itinéraire statique montre un routeur logique de niveau 0 avec un itinéraire statique vers le préfixe 10.10.10.0/24 dans l'architecture physique. À des fins de test, l'adresse 10.10.10.10/32 est configurée sur l'interface de boucle de routeur externe. Le routeur externe dispose d'un itinéraire statique vers le préfixe 172.16.0.0/16 pour atteindre les VM d'application et Web.

Figure 5-2. Topologie d'itinéraire statique



Conditions préalables

- Vérifiez que le routeur physique et le routeur logique de niveau 0 sont connectés. Reportez-vous à la section [Vérifier le routeur logique de niveau 0 et la connexion ToR](#).
- Vérifiez que le routeur de niveau 1 est configuré pour annoncer des itinéraires connectés. Reportez-vous à la section [Créer un routeur logique de niveau 1](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Sélectionnez le routeur logique de niveau 0.
- 4 Cliquez sur l'onglet **Routage** et sélectionnez **Itinéraire statique** dans le menu déroulant.
- 5 Sélectionnez **Ajouter**.
- 6 Entrez une adresse réseau au format CIDR.
Par exemple, 10.10.10.0/24.

7 Cliquez sur **+ Ajouter** pour ajouter une adresse IP de tronçon suivant.

Par exemple, 192.168.100.254. Vous pouvez également spécifier un itinéraire nul en cliquant sur l'icône de crayon et en sélectionnant **NULL** dans la liste déroulante.

8 Spécifiez la distance administrative.

9 Sélectionnez un port de routeur logique dans la liste déroulante.

La liste inclut les ports IPsec VTI (Virtual Tunnel Interface).

10 Cliquez sur le bouton **Ajouter**.

Étape suivante

Vérifiez que l'itinéraire statique est configuré correctement. Reportez-vous à la section [Vérifier l'itinéraire statique](#).

Vérifier l'itinéraire statique

Utilisez l'interface de ligne de commande pour vérifier que l'itinéraire statique est connecté. Vous devez également vérifier que le routeur externe peut effectuer un test ping sur les VM internes et que les VM internes peuvent effectuer un test ping sur le routeur externe.

Conditions préalables

Vérifiez qu'un itinéraire statique est configuré. Reportez-vous à la section [Configurer un itinéraire statique](#).

Procédure

1 Connectez-vous à l'interface de ligne de commande de NSX Manager.

2 Vérifiez l'itinéraire statique.

- a Obtenez les informations UUID du routeur de service.

```
get logical-routers
```

```
nsx-edge1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 2
type       : TUNNEL

Logical Router
UUID       : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf        : 4
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf        : 5
type       : DISTRIBUTED_ROUTER

Logical Router
UUID       : a6ee6316-2212-4171-99cc-930c98bcad7f
vrf        : 6
type       : DISTRIBUTED_ROUTER
```

- b Localisez les informations UUID à partir du résultat.

```
Logical Router
UUID       : d40bbfa4-3e3d-4178-8615-6f42ea335037
vrf        : 4
type       : SERVICE_ROUTER_TIER0
```

- c Vérifiez que l'itinéraire statique fonctionne.

```
get logical-router d40bbfa4-3e3d-4178-8615-6f42ea335037 static
```

```
Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

s    10.10.10.0/24      [1/1]      via 192.168.100.254
rl   100.64.1.0/31     [0/0]      via 169.0.0.1
ns   172.16.10.0/24    [3/3]      via 169.0.0.1
ns   172.16.20.0/24   [3/3]      via 169.0.0.1
```

- 3 À partir du routeur externe, effectuez un test ping sur les VM internes pour vérifier qu'elles sont accessibles via la superposition NSX-T Data Center.

- a Connectez-vous au routeur externe.

```
ping 172.16.10.10
```

```
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=62 time=127 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=62 time=1.96 ms
^C
--- 172.16.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.966/64.793/127.620/62.827 ms
```

- b Testez la connectivité réseau.

```
tracert 172.16.10.10
```

```
tracert to 172.16.10.10 (172.16.10.10), 30 hops max, 60 byte packets
 1 192.168.100.3 (192.168.100.3) 0.640 ms 0.575 ms 0.696 ms
 2 100.64.1.1 (100.64.1.1) 0.656 ms 0.604 ms 0.578 ms
 3 172.16.10.10 (172.16.10.10) 3.397 ms 3.703 ms 3.790 ms
```

- 4 Depuis les VM, effectuez un test ping sur l'adresse IP externe.

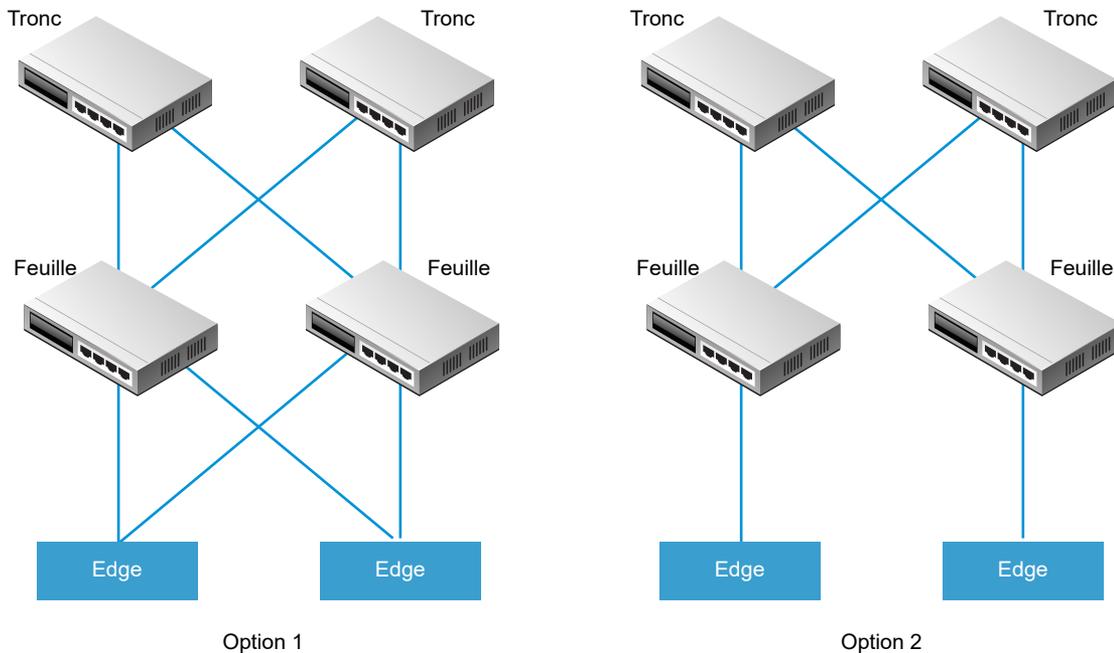
```
ping 10.10.10.10
```

```
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_req=1 ttl=62 time=119 ms
64 bytes from 10.10.10.10: icmp_req=2 ttl=62 time=1.93 ms
^C
--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.936/60.865/119.795/58.930 ms
```

Options de configuration de BGP

Pour bénéficier entièrement du routeur logique de niveau 0, la topologie doit être configurée avec une redondance et une symétrie avec BGP entre les routeurs de niveau 0 et les homologues ToR externes. Cette conception permet d'assurer la connectivité en cas d'échecs du lien et du nœud.

Il existe deux modes de configuration : actif-actif et actif-veille. Le schéma suivant montre deux options pour une configuration symétrique. Deux nœuds NSX Edge sont indiqués dans chaque topologie. Dans le cas d'une configuration actif-actif, lorsque vous créez des ports de liaison montante de niveau 0, vous pouvez associer chaque port de liaison montante à huit nœuds de transport NSX Edge au maximum. Chaque nœud NSX Edge peut disposer de deux liaisons montantes.



Pour l'option 1, lorsque les routeurs feuille-nœud physiques sont configurés, ils doivent disposer de voisins BGP avec les dispositifs NSX Edge. La redistribution d'itinéraire doit inclure les mêmes préfixes de réseau avec des mesures BGP égales à tous les voisins BGP. Dans la configuration du routeur logique de niveau 0, tous les routeurs feuille-nœud doivent être configurés en tant que voisins BGP.

Lorsque vous configurez les voisins BGP du routeur de niveau 0, si vous ne spécifiez pas une adresse locale (l'adresse IP source), la configuration du voisin BGP est envoyée à tous les nœuds NSX Edge associés aux liaisons montantes du routeur logique de niveau 0. Si vous configurez une adresse locale, la configuration passe au nœud NSX Edge avec la liaison montante possédant cette adresse IP.

Dans le cas de l'option 1, si les liaisons montantes se trouvent sur le même sous-réseau sur les nœuds NSX Edge, il est judicieux d'omettre l'adresse locale. Si les liaisons montantes sur les nœuds NSX Edge se trouvent dans des sous-réseaux différents, l'adresse locale doit être spécifiée dans la configuration du voisin BGP du routeur de niveau 0 afin d'éviter que la configuration n'aille à tous les nœuds NSX Edge associés.

Pour l'option 2, vérifiez que la configuration du routeur logique de niveau 0 inclut l'adresse IP locale du routeur de service de niveau 0. Les routeurs feuille-nœud sont configurés uniquement avec les dispositifs NSX Edge auxquels ils sont directement connectés en tant que voisin BGP.

Configurer BGP sur un routeur logique de niveau 0

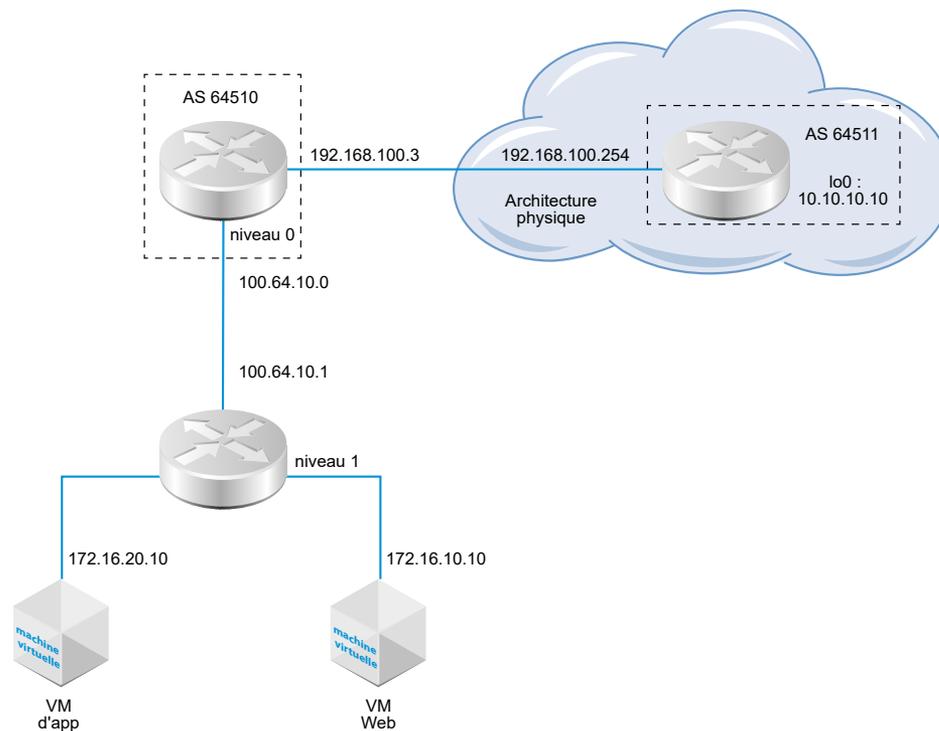
Pour activer l'accès entre vos VM et le monde extérieur, vous pouvez configurer une connexion BGP externe (eBGP) entre un routeur logique de niveau 0 et un routeur dans votre infrastructure physique.

Lors de la configuration de BGP, vous devez configurer un nombre AS (Autonomous System) local pour le routeur logique de niveau 0. Par exemple, la topologie suivante indique que le nombre AS local est 64510. Vous devez également configurer le nombre AS distant du routeur physique. Dans cet exemple, le nombre AS distant est 64511. L'adresse IP du voisin distant est 192.168.100.254. Le voisin doit se trouver dans le même sous-réseau IP que la liaison montante sur le routeur logique de niveau 0. Les tronçons multiples de BGP sont pris en charge.

À des fins de test, l'adresse 10.10.10.10/32 est configurée sur l'interface de boucle de routeur externe.

Note L'ID de routeur pour former des sessions BGP sur un nœud Edge est sélectionné automatiquement à partir des adresses IP configurées sur les liaisons montantes d'un routeur logique de niveau 0. Les sessions BGP sur un nœud Edge peuvent bagoter lorsque l'ID de routeur change. Cela peut se produire lorsque l'ID de routeur sélectionné automatiquement à partir des adresses IP est supprimé ou si le port du routeur logique sur lequel cette adresse IP est attribuée est supprimé.

Figure 5-3. Topologie de connexion BGP



Conditions préalables

- Vérifiez que le routeur de niveau 1 est configuré pour annoncer des itinéraires connectés. Reportez-vous à la section [Configurer l'annonce d'itinéraires sur un routeur logique de niveau 1](#). Il ne s'agit pas strictement d'une condition préalable pour la configuration de BGP, mais si vous disposez d'une topologie à deux niveaux et que vous prévoyez de redistribuer vos réseaux de niveau 1 dans BGP, cette étape est obligatoire.
- Vérifiez qu'un routeur de niveau 0 est configuré. Reportez-vous à la section [Créer un routeur logique de niveau 0](#).
- Assurez-vous que le routeur logique de niveau 0 a appris les itinéraires du routeur logique de niveau 1. Reportez-vous à la section [Vérifier qu'un routeur de niveau 0 a appris des itinéraires d'un routeur de niveau 1](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Sélectionnez le routeur logique de niveau 0.
- 4 Cliquez sur l'onglet **Routage** et sélectionnez **BGP** dans le menu déroulant.
- 5 Cliquez sur **Modifier**.
 - a Configurez le nombre AS local.
Par exemple, 64510.
 - b Cliquez sur le bouton bascule **État** pour activer BGP.
Le bouton État doit apparaître comme étant Activé.
 - c (Facultatif) Cliquez sur le bouton bascule **ECMP** pour activer ECMP.
 - d (Facultatif) Cliquez sur le bouton bascule **Redémarrage normal** pour activer le redémarrage normal.
 - e (Facultatif) Configurez l'agrégation de route, activez le redémarrage normal et activez ECMP.
Le redémarrage normal n'est pris en charge que si le cluster NSX Edge associé au routeur de niveau 0 ne dispose que d'un seul nœud Edge.
 - f Cliquez sur **Enregistrer**.
- 6 Cliquez sur **Ajouter** pour ajouter un voisin BGP.
- 7 Saisissez l'adresse IP du voisin.
Par exemple, 192,168,100,254.
- 8 (Facultatif) Spécifiez la limite maximale de tronçon.
La valeur par défaut est 1.

9 Entrez le nombre AS distant.

Par exemple, 64511.

10 (Facultatif) Configurez les temporisateurs (durée de survie et durée de retenue) et un mot de passe.

11 (Facultatif) Cliquez sur l'onglet **Adresse locale** pour sélectionner une adresse locale.

a (Facultatif) Décochez **Toutes les liaisons montantes** pour voir les ports de bouclage, ainsi que les ports de liaison montante.

12 (Facultatif) Cliquez sur l'onglet **Familles d'adresses** pour ajouter une famille d'adresses.

13 (Facultatif) Cliquez sur l'onglet **Configuration BFD** pour activer BFD.

14 Cliquez sur **Enregistrer**.

Étape suivante

Testez si BGP fonctionne correctement. Reportez-vous à la section [Vérifier les connexions BGP à partir d'un routeur de service de niveau 0](#).

Vérifier les connexions BGP à partir d'un routeur de service de niveau 0

Utilisez l'interface de ligne de commande pour vérifier à partir du routeur de service de niveau 0 qu'une connexion BGP à un voisin est établie.

Conditions préalables

Vérifiez que BGP est configuré. Reportez-vous à la section [Configurer BGP sur un routeur logique de niveau 0](#).

Procédure

- 1 Connectez-vous à l'interface de ligne de commande de NSX Manager.
- 2 Sur le dispositif NSX Edge, exécutez la commande `get logical-routers` pour rechercher le numéro VRF du routeur de service de niveau 0.

```
nsx-edge-1> get logical-routers
Logical Router
UUID       : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf        : 0
type       : TUNNEL

Logical Router
UUID       : 421a2d0d-f423-46f1-93a1-2f9e366176c8
vrf : 5
type       : SERVICE_ROUTER_TIER0

Logical Router
UUID       : f3ce9d7d-7123-47d6-aba6-45cf1388ca7b
vrf        : 6
```

```

type      : DISTRIBUTED_ROUTER

Logical Router
UUID      : c8e64eff-02b2-4462-94ff-89f3788f1a61
vrf       : 7
type      : SERVICE_ROUTER_TIER1

Logical Router
UUID      : fb6c3f1f-599f-4421-af8a-99692dff3dd4
vrf       : 8
type      : DISTRIBUTED_ROUTER

```

- 3 Exécutez la commande `vrf <number>` pour entrer le contexte du routeur de service de niveau 0.

```

nsx-edge-1> vrf 5
nsx-edge1(tier0_sr)>

```

- 4 Vérifiez que l'état de BGP est Established, up.

```
get bgp neighbor
```

```

BGP neighbor: 192.168.100.254   Remote AS: 64511
BGP state: Established, up
Hold Time: 180s   Keepalive Interval: 60s
Capabilities:
  Route Refresh: advertised and received
  Address Family: IPv4 Unicast:advertised and received
  Graceful Restart: none
  Restart Remaining Time: 0
Messages: 28 received, 31 sent
Minimum time between advertisements: 30s (default)
For Address Family IPv4 Unicast:advertised and received
  Route Refresh: 0 received, 0 sent
  Prefixes: 2 received, 2 sent, 2 advertised
1 Connections established, 2 dropped
Local host: 192.168.100.3, Local port: 179
Remote host: 192.168.100.254, Remote port: 33044

```

Étape suivante

Vérifiez la connexion de BGP à partir du routeur externe. Reportez-vous à la section [Vérifier la connectivité nord-sud et la redistribution d'itinéraires](#).

Configurer BFD sur un routeur logique de niveau 0

BFD (Bidirectional Forwarding Detection) est un protocole pouvant détecter les échecs de transfert de chemin d'accès.

Note Dans cette version, BFD sur les ports VTI (Virtual Tunnel Interface) n'est pas pris en charge.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Sélectionnez le routeur logique de niveau 0.
- 4 Cliquez sur l'onglet **Routage** et sélectionnez **BFD** dans le menu déroulant.
- 5 Cliquez sur **Modifier** pour configurer BFD.
- 6 Cliquez sur le bouton bascule **État** pour activer BFD.

En option, vous pouvez modifier les propriétés BFD globales **Recevoir un intervalle**, **Transmettre un intervalle** et **Déclarer un intervalle d'inactivité**.

- 7 (Facultatif) Cliquez sur **Ajouter** sous Homologues BFD pour les tronçons suivants d'itinéraire statique afin d'ajouter un homologue BFD.

Spécifiez l'adresse IP homologue et définissez le statut administratif sur **Activé**. En option, vous pouvez remplacer les propriétés BFD globales **Recevoir un intervalle**, **Transmettre un intervalle** et **Déclarer un intervalle d'inactivité**.

Activer la redistribution d'itinéraire sur le routeur logique de niveau 0

Lorsque vous activez la redistribution d'itinéraire, le routeur logique de niveau 0 commence le partage d'itinéraires spécifiés avec son routeur ascendant.

Conditions préalables

- Vérifiez que les routeurs logiques de couche 0 et de couche 1 sont connectés, de manière à ce qu'ils puissent indiquer aux réseaux du routeur logique de niveau 1 de redistribuer les itinéraires sur le routeur logique de niveau 0. Reportez-vous à la section [Attacher le niveau 0 et le niveau 1](#).
- Si vous souhaitez filtrer des adresses IP spécifiques à partir de la redistribution des routes, vérifiez que des cartes de route sont configurées. Reportez-vous à la section [Créer une carte de route](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Sélectionnez le routeur logique de niveau 0.
- 4 Cliquez sur l'onglet **Routage** et sélectionnez **Redistribution d'itinéraire** dans le menu déroulant.

- 5 Cliquez sur **Ajouter** pour remplir les critères de redistribution des itinéraires.

Option	Description
Nom et description	Attribuez un nom à la redistribution d'itinéraire. Vous pouvez éventuellement fournir une description. Exemple de nom : advertise-to-bgp-neighbor.
Sources	Cochez les cases en regard des itinéraires sources à redistribuer. Statique : itinéraires statiques de niveau 0. Connecté à NSX : itinéraires connectés de niveau 1. NSX statique : itinéraires statiques de niveau 1. Ces itinéraires statiques sont créés automatiquement. NAT de niveau 0 : itinéraires générés si la NAT est configurée sur le routeur logique de niveau 0. NAT de niveau 1 : itinéraires générés si la NAT est configurée sur le routeur logique de niveau 1.
Carte de route	(Facultatif) Attribuez une carte de route pour filtrer une séquence d'adresses IP à partir de la redistribution d'itinéraire.

- 6 Cliquez sur **Enregistrer**.
- 7 Cliquez sur le bouton **État** pour activer la redistribution des itinéraires.
Le bouton État apparaît comme Activé.

Vérifier la connectivité nord-sud et la redistribution d'itinéraires

Utilisez l'interface de ligne de commande pour vérifier que les itinéraires BGP sont connus. Auprès du routeur, vous pouvez vérifier que les machines connectées via NSX-T Data Center sont accessibles.

Conditions préalables

- Vérifiez que BGP est configuré. Reportez-vous à la section [Configurer BGP sur un routeur logique de niveau 0](#).
- Vérifiez que les itinéraires statiques NSX-T Data Center sont configurés pour être redistribués. Reportez-vous à la section [Activer la redistribution d'itinéraire sur le routeur logique de niveau 0](#).

Procédure

- 1 Connectez-vous à l'interface de ligne de commande de NSX Manager.
- 2 Afficher les itinéraires appris dans le voisinage BGP externe

```
nsx-edge1(tier0_sr)> get route bgp

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT
```

```
b 10.10.10.0/24 [20/0] via 192.168.100.254
```

- 3 À partir du routeur externe, vérifiez que les itinéraires BGP sont connus et que les machines virtuelles sont accessibles via la superposition NSX-T Data Center.

- a Dressez la liste des itinéraires BGP.

```
user@router# run show ip route bgp
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route

B>* 172.16.10.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
B>* 172.16.20.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
B>* 172.16.30.0/24 [20/0] via 192.168.100.2, eth2, 00:00:48
```

- b Depuis le routeur externe, envoyez une requête Ping aux machines virtuelles connectées via NSX-T Data Center.

```
ping 172.16.10.10
```

```
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=62 time=127 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=62 time=1.96 ms
^C
--- 172.16.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.966/64.793/127.620/62.827 ms
```

- c Vérifiez le chemin via la superposition NSX-T Data Center.

```
traceroute 172.16.10.10
```

```
traceroute to 172.16.10.10 (172.16.10.10), 30 hops max, 60 byte packets
 1 192.168.100.3 (192.168.100.3) 0.640 ms 0.575 ms 0.696 ms
 2 100.91.176.1 (100.91.176.1) 0.656 ms 0.604 ms 0.578 ms
 3 172.16.10.10 (172.16.10.10) 3.397 ms 3.703 ms 3.790 ms
```

- 4 Depuis les machines virtuelles internes, envoyez une requête Ping vers l'adresse IP externe.

```
ping 10.10.10.10
```

```
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_req=1 ttl=62 time=119 ms
64 bytes from 10.10.10.10: icmp_req=2 ttl=62 time=1.93 ms
```

```

^C
--- 10.10.10.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.936/60.865/119.795/58.930 ms
    
```

Étape suivante

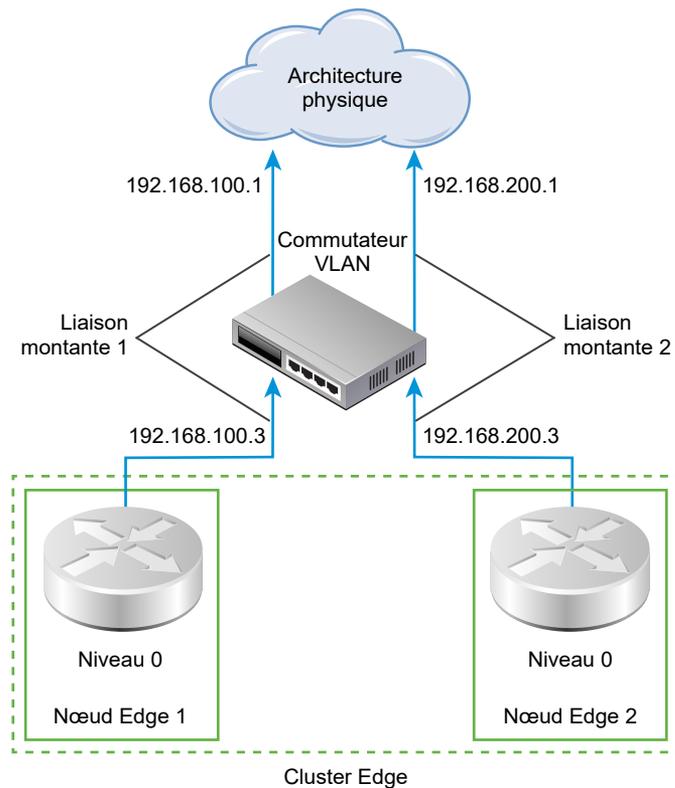
Configurez la fonctionnalité de routage supplémentaire, par exemple ECMP.

Comprendre le routage ECMP

Le protocole de routeur logique ECMP (Equal cost multi-path) augmente la bande passante de communication nord-sud en ajoutant une liaison montante au routeur logique de niveau 0 et en la configurant pour chaque nœud Edge dans un cluster NSX Edge. Les chemins de routage ECMP sont utilisés pour équilibrer la charge du trafic et pour fournir la tolérance de panne pour les chemins en échec.

Les chemins ECMP sont automatiquement créés à partir des VM attachées à des commutateurs logiques sur les nœuds Edge sur lesquels le routeur logique de niveau 0 est instancié. Un maximum de huit chemins ECMP sont pris en charge.

Figure 5-4. Topologie du routage ECMP



Par exemple, la topologie montre deux routeurs logiques de niveau 0 dans un cluster NSX Edge. Chaque routeur logique de niveau 0 se trouve dans un nœud Edge et ces nœuds font partie du cluster. Les ports de liaison montante 192.168.100.3 et 198.168.200.3 définissent comment le nœud de transport se connecte au commutateur logique pour pouvoir accéder au réseau physique. Lorsque les chemins de routage ECMP sont activés, ces chemins connectent les VM attachées à des commutateurs logiques et les deux nœuds Edge dans le cluster NSX Edge. Les chemins de routage ECMP multiples augmentent le débit et la résilience du réseau.

Ajouter un port de liaison montante pour le second nœud Edge

Avant d'activer ECMP, vous devez configurer une liaison montante pour connecter le routeur logique de niveau 0 au commutateur logique VLAN.

Conditions préalables

- Vérifiez qu'une zone de transport et deux nœuds de transport sont configurés. Reportez-vous à *Guide d'installation de NSX-T Data Center*.
- Vérifiez que deux nœuds Edge et un cluster Edge sont configurés. Reportez-vous à *Guide d'installation de NSX-T Data Center*.
- Vérifiez qu'un commutateur logique VLAN pour la liaison montante est disponible. Reportez-vous à la section [Créer un commutateur logique VLAN pour la liaison montante NSX Edge](#).
- Vérifiez qu'un routeur logique de niveau 0 est configuré. Reportez-vous à la section [Créer un routeur logique de niveau 0](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Sélectionnez le routeur logique de niveau 0.
- 4 Cliquez sur l'onglet **Configuration** pour ajouter un port de routeur.
- 5 Cliquez sur **Ajouter**.
- 6 Renseignez les détails du port de routeur.

Option	Description
Nom	Attribuez un nom au port de routeur.
Description	Fournissez une description supplémentaire indiquant que le port est destiné à la configuration ECMP.
Type	Acceptez le type par défaut Liaison montante .
Nœud de transport	Attribuez le nœud de transport hôte à partir du menu déroulant.
Commutateur logique	Attribuez le commutateur logique VLAN à partir du menu déroulant.

Option	Description
Port de commutateur logique	Attribuez un nouveau nom de port de commutateur. Vous pouvez également utiliser un port de commutateur existant.
Adresse IP/Masque	Entrez une adresse IP qui se trouve dans le même sous-réseau que le port connecté sur le commutateur ToR.

7 Cliquez sur **Enregistrer**.

Résultats

Un nouveau port de liaison montante est ajouté au routeur de niveau 0 et au commutateur logique VLAN. Le routeur logique de niveau 0 est configuré sur les deux nœuds Edge.

Étape suivante

Créez une connexion BGP pour le second voisin et activez le routage ECMP. Reportez-vous à la section [Ajouter un second voisin BGP et activer le routage ECMP](#).

Ajouter un second voisin BGP et activer le routage ECMP

Avant d'activer le routage ECMP, vous devez ajouter un voisin BGP et le configurer avec les informations de liaison montante qui viennent d'être ajoutées.

Conditions préalables

Vérifiez que le second nœud Edge dispose d'un port de liaison montante configuré. Reportez-vous à la section [Ajouter un port de liaison montante pour le second nœud Edge](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Sélectionnez le routeur logique de niveau 0.
- 4 Cliquez sur l'onglet **Routage** et sélectionnez **BGP** dans le menu déroulant.
- 5 Cliquez sur **Ajouter** sous la section Voisins pour ajouter un voisin BGP.
- 6 Saisissez l'adresse IP du voisin.
Par exemple, 192,168,200,254.
- 7 (Facultatif) Spécifiez la limite maximale de tronçon.
La valeur par défaut est 1.
- 8 Entrez le nombre AS distant.
Par exemple, 64511.

- 9 (Facultatif) Cliquez sur l'onglet **Adresse locale** pour sélectionner une adresse locale.
 - a (Facultatif) Décochez **Toutes les liaisons montantes** pour voir les ports de bouclage, ainsi que les ports de liaison montante.
- 10 (Facultatif) Cliquez sur l'onglet **Familles d'adresses** pour ajouter une famille d'adresses.
- 11 (Facultatif) Cliquez sur l'onglet **Configuration BFD** pour activer BFD.
- 12 Cliquez sur **Enregistrer**.

Le voisin BGP qui vient d'être ajouté s'affiche.
- 13 Cliquez sur **Modifier** en regard de la section Configuration de BGP.
- 14 Cliquez sur le bouton bascule **ECMP** pour activer ECMP.

Le bouton État doit apparaître comme étant Activé.
- 15 Cliquez sur **Enregistrer**.

Résultats

Plusieurs chemins de routage ECMP connectent les VM attachées à des commutateurs logiques et leurs deux nœuds Edge dans le cluster Edge.

Étape suivante

Vérifiez si les connexions de routage ECMP fonctionnent correctement. Reportez-vous à la section [Vérifier la connectivité du routage ECMP](#).

Vérifier la connectivité du routage ECMP

Utilisez l'interface de ligne de commande pour vérifier que la connexion de routage ECMP au voisin est établie.

Conditions préalables

Vérifiez que le routage ECMP est configuré. Reportez-vous aux sections [Ajouter un port de liaison montante pour le second nœud Edge](#) et [Ajouter un second voisin BGP et activer le routage ECMP](#).

Procédure

- 1 Connectez-vous à l'interface de ligne de commande de NSX Manager.
- 2 Obtenez les informations UUID du routeur distribué.

```
get logical-routers
```

```
Logical Router
UUID          : 736a80e3-23f6-5a2d-81d6-bbefb2786666
vrf           : 2
type          : TUNNEL
```

```
Logical Router
UUID          : d40bbfa4-3e3d-4178-8615-6f42ea335037
```

```
vrf      : 4
type    : SERVICE_ROUTER_TIER0

Logical Router
UUID    : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf     : 5
type    : DISTRIBUTED_ROUTER

Logical Router
UUID    : a6ee6316-2212-4171-99cc-930c98bcad7f
vrf     : 6
type    : DISTRIBUTED_ROUTER
```

- 3 Localisez les informations UUID à partir du résultat.

```
Logical Router
UUID    : d0289ba4-250e-41b4-8ffc-7cab4a46c3e4
vrf     : 5
type    : DISTRIBUTED_ROUTER
```

- 4 Tapez le VRF pour le routeur distribué de niveau 0.

```
vrf 5
```

- 5 Vérifiez que le routeur distribué de niveau 0 est connecté aux nœuds Edge.

```
get forwarding
```

Par exemple, edge-node-1 et edge-node-2.

- 6 Entrez **exit** pour quitter le contexte vrf.
- 7 Ouvrez le contrôleur actif pour le routeur logique de niveau 0.
- 8 Vérifiez que le routeur distribué de niveau 0 sur le nœud de contrôleur est connecté.

```
get logical-router <UUID> route
```

Le type d'itinéraire pour l'UUID doit être NSX_CONNECTED.

- 9 Démarrez une session SSH sur les deux nœuds Edge.

- 10 Démarrez une session pour capturer des paquets.

```
set capture session 0 interface fp-eth1 dir tx
```

```
set capture session 0 expression src net <IP_Address>
```

- 11 Accédez au centre de contrôle et double-cliquez sur les scripts httpdata11.bat et httpdata12.bat.

Un grand nombre de demandes HTTP pour les deux VM Web est envoyé et vous voyez le trafic haché sur les deux chemins utilisant les nœuds Edge, ce qui indique qu'ECMP fonctionne.

- 12 Arrêtez la session de capture.

```
del capture session 0
```

- 13 Supprimez les scripts bat.

Créer une liste de préfixes IP

Une liste de préfixes IP contient une ou plusieurs adresses IP auxquelles sont attribuées des autorisations d'accès pour l'annonce de routes. Les adresses IP dans cette liste sont traitées dans l'ordre. Les listes de préfixes IP sont référencées via des filtres de voisin BGP ou des cartes de route avec un sens entrant ou sortant.

Par exemple, vous pouvez ajouter l'adresse IP 192.168.100.3/27 à la liste de préfixes IP et refuser que l'itinéraire soit redistribué au routeur vers le nord. Vous pouvez également ajouter une adresse IP avec des modificateurs inférieur-ou-égal-à (le) et supérieur-ou-égal-à (ge) pour accorder ou limiter la redistribution d'itinéraire. Par exemple, les modificateurs 192.168.100.3/27 ge 24 le 30 correspondent aux masques de sous-réseau supérieur et égal à 24 bits et inférieur ou égal à 30 bits en longueur.

Note L'action par défaut d'un itinéraire est **Refuser**. Lorsque vous créez une liste de préfixes pour refuser ou autoriser des routes spécifiques, veillez à créer un préfixe IP sans adresse réseau spécifique (sélectionnez **Quelconque** dans la liste déroulante) et l'action **Autoriser** si vous voulez autoriser toutes les autres routes.

Conditions préalables

Vérifiez que vous disposez d'un routeur logique de niveau 0 configuré. Reportez-vous à la section [Créer un routeur logique de niveau 0](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Sélectionnez le routeur logique de niveau 0.
- 4 Cliquez sur l'onglet **Routage** et sélectionnez **Listes de préfixes IP** dans le menu déroulant.
- 5 Cliquez sur **Ajouter**.
- 6 Entrez un nom pour la liste de préfixes IP.
- 7 Cliquez sur **Ajouter** pour spécifier un préfixe.
 - a Entrez une adresse IP au format CIDR.
Par exemple, 192.168.100.3/27.
 - b Sélectionnez **Refuser** ou **Autoriser** dans le menu déroulant.
 - c (Facultatif) Définissez une plage de numéros d'adresse IP dans les modificateurs **le** ou **ge**.
Par exemple, définissez le modificateur **le** sur 30 et le modificateur **ge** sur 24.
- 8 Recommencez l'étape précédente pour spécifier des préfixes supplémentaires.
- 9 Cliquez sur **Ajouter** en bas de la fenêtre.

Créer une liste de communauté

Vous pouvez créer des listes de communauté BGP de manière à pouvoir configurer des cartes de route basées sur celles-ci.

Conditions préalables

Vérifiez que vous disposez d'un routeur logique de niveau 0 configuré. Reportez-vous à la section [Créer un routeur logique de niveau 0](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Sélectionnez le routeur logique de niveau 0.
- 4 Cliquez sur l'onglet **Routage** et sélectionnez **Listes de communauté** dans le menu déroulant.
- 5 Cliquez sur **Ajouter**.
- 6 Entrez le nom de la liste de communauté.
- 7 Spécifiez une communauté à l'aide du format aa:nn, par exemple, 300:500 et appuyez sur Entrée. Répétez ces étapes pour ajouter d'autres communautés.

En outre, vous pouvez cliquer sur la flèche de liste déroulante et sélectionner une ou plusieurs des options suivantes :

- NO_EXPORT_SUBCONFED : ne pas annoncer aux homologues EBGp.
- NO_ADVERTISE : n'annoncer à aucun homologue.
- NO_EXPORT : ne pas annoncer en dehors de la confédération BGP.

- 8 Cliquez sur **Ajouter**.

Créer une carte de route

Une carte de route se compose d'une séquence de listes de préfixes IP, d'attributs de chemin d'accès BGP et d'une action associée. Le routeur analyse la séquence pour trouver une adresse IP correspondante. S'il existe une correspondance, le routeur effectue l'action et n'analyse plus.

Il est possible de référencer des cartes de route au niveau du voisin BGP et au moment de la redistribution de route. Lorsque des listes de préfixes IP sont référencées dans des cartes de route et que l'action de carte de route « autorisation » ou « refus » s'applique, l'action spécifiée dans la séquence de carte de route remplace la spécification dans la liste de préfixes IP.

Conditions préalables

Vérifiez qu'une liste de préfixes IP est configurée. Reportez-vous à la section [Créer une liste de préfixes IP](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Sélectionnez le routeur logique de niveau 0.
- 4 Sélectionnez **Routage > Cartes de route**.
- 5 Cliquez sur **Ajouter**.
- 6 Entrez un nom et une description facultative pour la carte de route.
- 7 Cliquez sur **Ajouter** pour ajouter une entrée dans la carte de route.
- 8 Modifiez la colonne **Faire correspondre la liste de préfixes IP/liste de communauté** pour sélectionner les listes de préfixes IP ou les listes de communautés, mais pas les deux.
- 9 (Facultatif) Définissez des attributs BGP.

Attribut BGP	Description
Préfixe chemin AS	Ajoutez au début d'un chemin d'accès un ou plusieurs nombres AS (Autonomous System) pour que le chemin soit plus long et qu'il ait ainsi moins de chance d'être préféré.
MED	La mesure Multi-Exit Discriminator indique à un homologue externe un chemin d'accès préféré vers un AS.
Poids	Définissez un poids pour influencer la sélection du chemin d'accès. La plage est comprise entre 0 et 65 535.
Communauté	Spécifiez une communauté à l'aide du format aa:nn, par exemple, 300:500. Ou utilisez le menu déroulant pour sélectionner l'une des options suivantes : <ul style="list-style-type: none"> ■ NO_EXPORT_SUBCONFED : ne pas annoncer aux homologues EBGp. ■ NO_ADVERTISE : n'annoncer à aucun homologue. ■ NO_EXPORT : ne pas annoncer en dehors de la confédération BGP.

- 10 Dans la colonne Action, sélectionnez **Autoriser** ou **Refuser**.

Vous pouvez autoriser ou refuser l'annonce de leurs adresses aux adresses IP dans les listes de préfixes IP.

- 11 Cliquez sur **Enregistrer**.

Configurer le temporisateur d'activation du transfert

Vous pouvez configurer le temporisateur d'activation du transfert pour un routeur logique de niveau 0.

Le temporisateur d'activation du transfert définit le temps en secondes que le routeur doit attendre avant d'envoyer la notification d'activation après l'établissement de la première session BGP. Ce temporisateur (anciennement retard de transfert) réduit les interruptions de service en cas de basculements pour des configurations active-active ou active-en veille de routeurs logiques sur NSX Edge qui utilisent le routage dynamique (BGP). Il doit être défini sur le nombre de secondes qu'un routeur externe (TOR) prend pour

annoncer tous les itinéraires à ce routeur après la première session BGP/BFD. La valeur du temporisateur doit être directement proportionnelle au nombre d'itinéraires dynamiques ascendants que le routeur doit apprendre. Ce temporisateur doit être défini sur 0 sur les configurations de nœud Edge uniques.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur *https://<adresse-ip-nsx-manager>*.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Sélectionnez le routeur logique de niveau 0.
- 4 Sélectionnez **Routage > Configuration globale**
- 5 Cliquez sur **Modifier**.
- 6 Entrez une valeur pour le temporisateur d'activation du transfert.
- 7 Cliquez sur **Enregistrer**.

Traduction d'adresse réseau

6

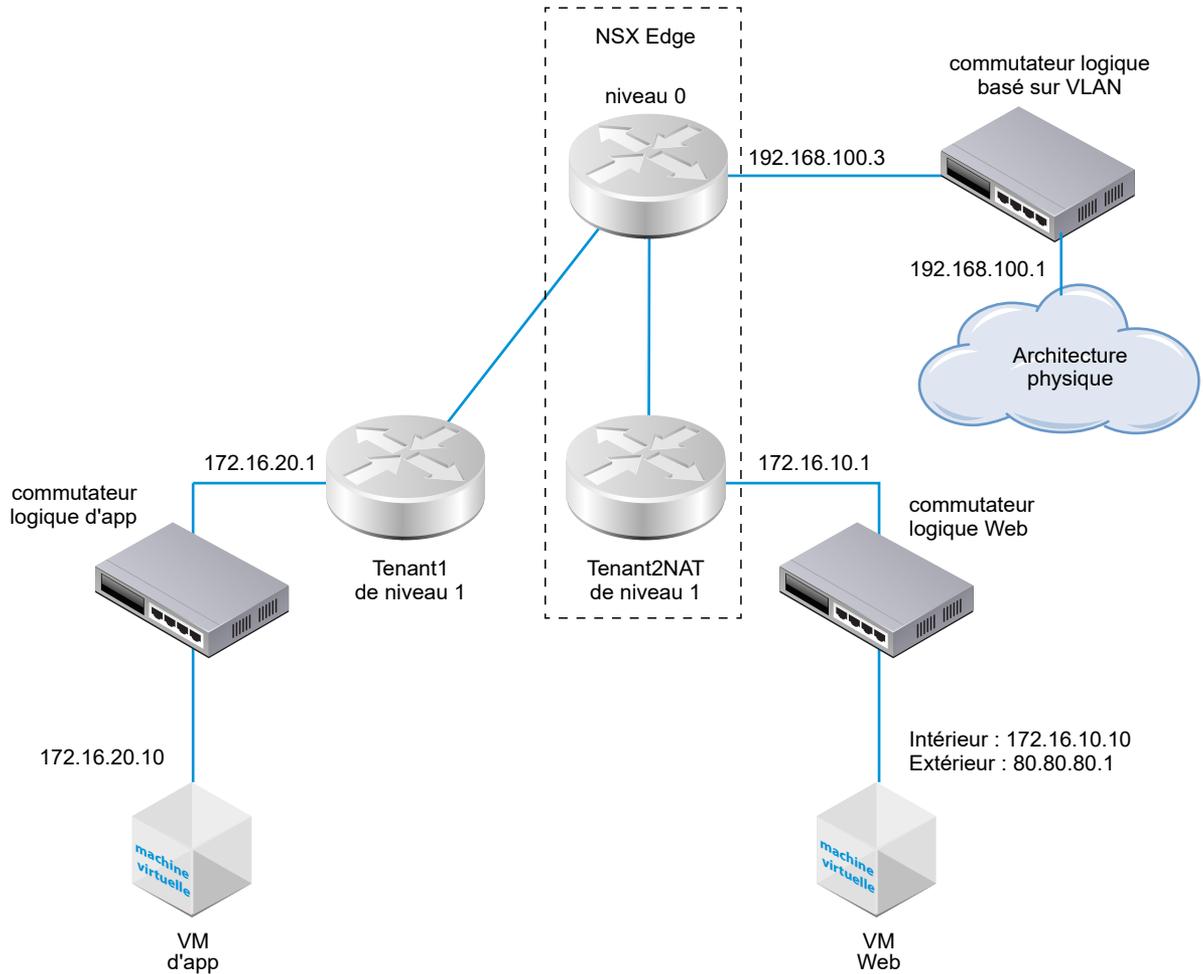
La traduction d'adresse réseau (NAT) dans NSX-T Data Center peut être configurée sur des routeurs logiques de niveau 0 et de niveau 1.

Par exemple, le schéma suivant montre deux routeurs logiques de niveau 1 avec la NAT configurée sur Tenant2NAT. La VM Web est simplement configurée pour utiliser 172.16.10.10 comme adresse IP et 172.16.10.1 comme passerelle par défaut.

La NAT est appliquée au niveau de la liaison montante du routeur logique Tenant2NAT sur sa connexion au routeur logique de niveau 0.

Pour activer la configuration de la NAT, Tenant2NAT doit disposer d'un composant de service sur un cluster NSX Edge. Par conséquent, Tenant2NAT est indiqué à l'intérieur du dispositif NSX Edge. En comparaison, Tenant1 peut se trouver à l'extérieur du dispositif NSX Edge, car il n'utilise aucun service Edge.

Figure 6-1. Topologie de la NAT



Ce chapitre contient les rubriques suivantes :

- [NAT de niveau 1](#)
- [NAT de niveau 0](#)
- [NAT réflexive](#)

NAT de niveau 1

Les routeurs logiques de niveau 1 prennent en charge la NAT source et la NAT de destination.

Configurer la NAT source sur un routeur de niveau 1

La NAT source (SNAT) change l'adresse source dans l'en-tête Adresse IP d'un paquet. Elle peut également changer le port source dans les en-têtes TCP/UDP. L'utilisation classique consiste à changer une adresse/un port privé (rfc1918) en adresse/port public pour des paquets quittant votre réseau.

Vous pouvez créer une règle pour activer ou désactiver la NAT source.

Dans cet exemple, les paquets étant reçus depuis la machine virtuelle Web, le routeur de niveau 1 Tenant2NAT remplace l'adresse IP source des paquets 172.16.10.10 par l'adresse IP 80.80.80.1. Disposer d'une adresse IP source publique permet à des destinations extérieures au réseau privé de revenir à la source d'origine.

Conditions préalables

- Le routeur de niveau 0 doit disposer d'une liaison montante connectée à un commutateur logique basé sur VLAN. Reportez-vous à la section [Connecter un routeur logique de niveau 0 à un commutateur logique VLAN pour la liaison montante NSX Edge](#).
- Le routage (statique ou BGP) et la redistribution d'itinéraire du routeur de niveau 0 doivent être configurés sur sa liaison montante vers l'architecture physique. Reportez-vous à [Configurer un itinéraire statique](#), [Configurer BGP sur un routeur logique de niveau 0](#), et [Activer la redistribution d'itinéraire sur le routeur logique de niveau 0](#).
- Une liaison montante vers un routeur de niveau 0 doit être configurée sur chaque routeur de niveau 1. Tenant2NAT doit être sauvegardé par un cluster NSX Edge. Reportez-vous à la section [Attacher le niveau 0 et le niveau 1](#).
- Des ports de liaison descendante et l'annonce d'itinéraires doivent être configurés sur les routeurs de niveau 1. Reportez-vous aux sections [Ajouter un port de liaison descendante sur un routeur logique de niveau 1](#) et [Configurer l'annonce d'itinéraires sur un routeur logique de niveau 1](#).
- Les machines virtuelles doivent être attachées aux commutateurs logiques corrects.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Cliquez sur un routeur logique de niveau 1 sur lequel vous voulez configurer la NAT.
- 4 Sélectionnez **Services > NAT**.
- 5 Cliquez sur **AJOUTER**.
- 6 Spécifiez une valeur de priorité.
Une valeur inférieure signifie une priorité plus élevée pour cette règle.
- 7 Pour **Action**, sélectionnez **SNAT** pour activer la NAT source ou **NO_SNAT** pour désactiver la NAT source.
- 8 Sélectionnez le type de protocole.
Par défaut, **N'importe quel protocole** est sélectionné.
- 9 (Facultatif) Pour **Adresse IP Source**, spécifiez une adresse IP ou une plage d'adresses IP au format CIDR.
Si vous laissez ce champ vide, toutes les sources sur les ports de liaison descendante du routeur sont traduites. Dans cet exemple, l'adresse IP source est 172.16.10.10.

10 (Facultatif) Pour **Adresse IP de Destination**, spécifiez une adresse IP ou une plage d'adresses IP au format CIDR.

Si vous laissez ce champ vide, la NAT s'applique à toutes les destinations extérieures du sous-réseau local.

11 Si **Action** a la valeur **SNAT**, pour **Adresse IP traduite**, spécifiez une adresse IP ou une plage d'adresses IP au format CIDR.

Dans cet exemple, l'adresse IP traduite est 80.80.80.1.

12 (Facultatif) Pour **Appliqué à**, sélectionnez un port de routeur.

13 (Facultatif) Définissez le statut de la règle.

La règle est activée par défaut.

14 (Facultatif) Modifiez l'état de la journalisation.

La journalisation est désactivée par défaut.

15 (Facultatif) Modifiez le paramètre de contournement de pare-feu.

Ce paramètre est activé par défaut.

Résultats

La nouvelle règle est répertoriée sous NAT. Par exemple :

ID	Action	Correspondance				Traduit		Appliqué à	Statut
		Protocole	IP source	Ports source	Adresse IP de destination	Ports de destination	IP		
1033	SNAT	Quelcon...	172.16.10.10	Quelcon...	Quelconque	Quelconque	80.80.80.1	Q...	

Étape suivante

Configurez le routeur de niveau 1 pour annoncer des itinéraires NAT.

Pour annoncer les itinéraires NAT en amont, du routeur de niveau 0 à l'architecture physique, configurez le routeur de niveau 0 pour qu'il annonce les itinéraires NAT de niveau 1.

Configurer la NAT de destination sur un routeur de niveau 1

La NAT de destination modifie l'adresse de destination dans l'en-tête IP d'un paquet. Elle peut également modifier le port de destination dans les en-têtes TCP/UDP. Le but est généralement de rediriger les paquets entrants dont la destination est une adresse ou un port public vers une adresse ou un port IP à l'intérieur de votre réseau.

Vous pouvez créer une règle pour activer ou désactiver la NAT de destination.

Dans cet exemple, les paquets étant reçus de la machine virtuelle d'application, le routeur de niveau 1 Tenant2NAT remplace l'adresse IP de destination des paquets 172.16.10.10 par l'adresse IP 80.80.80.1. L'utilisation d'une adresse de destination publique permet à une destination à l'intérieur du réseau privé d'être contactée depuis l'extérieur de ce réseau.

Conditions préalables

- Le routeur de niveau 0 doit disposer d'une liaison montante connectée à un commutateur logique basé sur VLAN. Reportez-vous à la section [Connecter un routeur logique de niveau 0 à un commutateur logique VLAN pour la liaison montante NSX Edge](#).
- Le routage (statique ou BGP) et la redistribution d'itinéraire du routeur de niveau 0 doivent être configurés sur sa liaison montante vers l'architecture physique. Reportez-vous à [Configurer un itinéraire statique](#), [Configurer BGP sur un routeur logique de niveau 0](#), et [Activer la redistribution d'itinéraire sur le routeur logique de niveau 0](#).
- Une liaison montante vers un routeur de niveau 0 doit être configurée sur chaque routeur de niveau 1. Tenant2NAT doit être sauvegardé par un cluster NSX Edge. Reportez-vous à la section [Attacher le niveau 0 et le niveau 1](#).
- Des ports de liaison descendante et l'annonce d'itinéraires doivent être configurés sur les routeurs de niveau 1. Reportez-vous aux sections [Ajouter un port de liaison descendante sur un routeur logique de niveau 1](#) et [Configurer l'annonce d'itinéraires sur un routeur logique de niveau 1](#).
- Les machines virtuelles doivent être attachées aux commutateurs logiques corrects.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Cliquez sur un routeur logique de niveau 1 sur lequel vous voulez configurer la NAT.
- 4 Sélectionnez **Services > NAT**.
- 5 Cliquez sur **AJOUTER**.
- 6 Spécifiez une valeur de priorité.
Une valeur inférieure signifie une priorité plus élevée pour cette règle.
- 7 Pour **Action**, sélectionnez **DNAT** pour activer la NAT de destination ou **NO_DNAT** pour désactiver la NAT de destination.
- 8 Sélectionnez le type de protocole.
Par défaut, **N'importe quel protocole** est sélectionné.
- 9 (Facultatif) Pour **Adresse IP Source**, spécifiez une adresse IP ou une plage d'adresses IP au format CIDR.
Si vous ne renseignez pas le champ de l'adresse IP source, la NAT s'applique à toutes les sources extérieures au sous-réseau local.

10 Pour **Adresse IP de Destination**, spécifiez une adresse IP ou une plage d'adresses IP au format CIDR.

Dans cet exemple, l'adresse IP de destination est 80.80.80.1.

11 Si **Action** a la valeur **DNAT**, pour **Adresse IP traduite**, spécifiez une adresse IP ou une plage d'adresses IP au format CIDR.

Dans cet exemple, l'adresse IP interne/traduite est 172.16.10.10.

12 (Facultatif) Si **Action** a la valeur **DNAT**, pour **Ports traduits**, spécifiez les ports traduits.

13 (Facultatif) Pour **Appliqué à**, sélectionnez un port de routeur.

14 (Facultatif) Définissez le statut de la règle.

La règle est activée par défaut.

15 (Facultatif) Modifiez l'état de la journalisation.

La journalisation est désactivée par défaut.

16 (Facultatif) Modifiez le paramètre de contournement de pare-feu.

Ce paramètre est activé par défaut.

Résultats

La nouvelle règle est répertoriée sous NAT. Par exemple :

The screenshot shows the 'Services' tab for 'Tenant2NAT'. It displays a table with one NAT rule. The table has columns for ID, Action, Correspondance (Protocol, IP source, Ports source, Adresse IP de destination, Ports de destination), Traduit (IP, Ports), Appliqué à, and Statistique. The rule has ID 1032, Action DNAT, and is applied to port 1024. The destination IP is 80.80.80.1 and the translated IP is 172.16.10.10.

ID	Action	Correspondance					Traduit		Appliqué à	Statistique
		Protocole	IP source	Ports source	Adresse IP de destination	Ports de destination	IP	Ports		
1032	DNAT	Quelc...	Quelc...	Quelcon...	80.80.80.1	Quelconque	172.16.10.10	Q...		

Étape suivante

Configurez le routeur de niveau 1 pour annoncer des itinéraires NAT.

Pour annoncer les itinéraires NAT en amont, du routeur de niveau 0 à l'architecture physique, configurez le routeur de niveau 0 pour qu'il annonce les itinéraires NAT de niveau 1.

Annoncer des itinéraires NAT de niveau 1 au routeur de niveau 0 en amont

L'annonce d'itinéraires NAT de niveau 1 permet au routeur de niveau 0 en amont d'en savoir plus sur ces itinéraires.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Cliquez sur un routeur logique de niveau 1 sur lequel vous avez configuré la NAT.
- 4 À partir du routeur de niveau 1, sélectionnez **Routage > Annonce d'itinéraires**.
- 5 Modifiez les règles d'annonce d'itinéraires pour activer l'annonce d'itinéraires NAT.

Résultats

Tenant2NAT	
Présentation	Configuration ▾
Routage ▾	Services ▾
Annonce de route MODIFIER	
Etat	● Activé
Annoncer toutes routes connectées à NSX	● Oui
Annoncer toutes les routes NAT	● Oui
Annoncer toutes les routes statiques	● Non
Annoncer toutes les routes VIP de LB	● Non
Annoncer toutes routes IP du SNAT LB	● Non
Réseaux annoncés	5 Réseaux

Étape suivante

Annoncez des itinéraires NAT de niveau 1 à partir du routeur de niveau 0 à l'architecture physique en amont.

Annoncer des itinéraires NAT de niveau 1 à l'architecture physique

L'annonce d'itinéraires NAT de niveau 1 à partir du routeur de niveau 0 permet à l'architecture physique en amont d'en savoir plus sur ces itinéraires.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Routage**.
- 3 Cliquez sur un routeur logique de niveau 0 connecté à un routeur de niveau 1 sur lequel vous avez configuré la NAT.
- 4 À partir du routeur de niveau 0, sélectionnez **Routage > Redistribution d'itinéraire**.
- 5 Modifiez les règles d'annonce d'itinéraires pour activer l'annonce d'itinéraires NAT de niveau 1.

Résultats

Modifier les critères de redistribution - rule1 ? ×

Nom*	rule1
Description	Rule
Sources*	<input type="checkbox"/> Statique <input checked="" type="checkbox"/> NAT de niveau 1 <input checked="" type="checkbox"/> NSX connecté <input type="checkbox"/> VIP d'équilibrage de charge de niveau 1 <input checked="" type="checkbox"/> NSX statique <input type="checkbox"/> SNAT d'équilibrage de charge de niveau 1 <input type="checkbox"/> NAT de niveau 0
Carte de route	× ∨

ANNULER

ENREGISTRER

Étape suivante

Vérifiez que la NAT fonctionne comme prévu.

Vérifier la NAT de niveau 1

Vérifiez que les règles SNAT et DNAT fonctionnent correctement.

Procédure

- 1 Connectez-vous au dispositif NSX Edge.
- 2 Exécutez `get logical-routers` pour déterminer le numéro VRF du routeur de service de niveau 0.
- 3 Entrez le contexte du routeur de service de niveau 0 en exécutant la commande `vrf <number>`.
- 4 Exécutez la commande `get route` et vérifiez que l'adresse de la NAT de niveau 1 s'affiche.

```
nsx-edge(tier0_sr)> get route
```

```
Flags: c - connected, s - static, b - BGP, ns - nsx_static
```

```
nc - nsx_connected, r1 - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT

Total number of routes: 8

t1n 80.80.80.1/32      [3/3]      via 169.0.0.1
...
```

- 5 Si votre VM Web est configurée pour servir de pages Web, vérifiez que vous pouvez ouvrir une page Web à l'adresse `http://80.80.80.1`.
- 6 Vérifiez que le voisin en amont du routeur de niveau 0 dans l'architecture physique peut effectuer un test ping sur `80.80.80.1`.
- 7 Pendant l'exécution du test ping, vérifiez la colonne des statistiques de la règle DNAT.
Il doit y avoir une session active.

NAT de niveau 0

Les routeurs logiques de niveau 0 prennent en charge la NAT source, la NAT de destination et la NAT réflexive.

Configurer la NAT source et de destination sur un routeur de niveau 0

Vous pouvez configurer la NAT source et de destination sur un routeur de niveau 0 exécuté en mode actif-veille.

Vous pouvez également configurer Aucun NAT, Aucun SNAT ou Aucun DNAT pour désactiver la NAT pour une adresse IP ou une plage d'adresses. Si plusieurs règles NAT s'appliquent à une adresse, la règle avec la priorité la plus élevée est appliquée.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Cliquez sur un routeur logique de niveau 0.
- 4 Sélectionnez **Services > NAT**.
- 5 Cliquez sur **AJOUTER** pour ajouter une règle NAT.
- 6 Spécifiez une valeur de priorité.
Une valeur inférieure signifie une priorité plus élevée.
- 7 Pour **Action**, sélectionnez **SNAT**, **DNAT**, **Aucun NAT**, **NO_SNAT** ou **NO_DNAT**.
- 8 Sélectionnez le type de protocole.
Par défaut, **N'importe quel protocole** est sélectionné.

- 9 (Requis) Pour **Adresse IP Source**, spécifiez une adresse IP ou une plage d'adresses IP au format CIDR.

Si vous laissez ce champ vide, la règle NAT s'applique à toutes les sources extérieures au sous-réseau local.

- 10 Pour **Adresse IP de Destination**, spécifiez une adresse IP ou une plage d'adresses IP au format CIDR.

- 11 Pour **Adresse IP traduite**, spécifiez une adresse IP ou une plage d'adresses IP au format CIDR.

- 12 (Facultatif) Si **Action** a la valeur **DNAT**, pour **Ports traduits**, spécifiez les ports traduits.

- 13 (Facultatif) Pour **Appliqué à**, sélectionnez un port de routeur.

- 14 (Facultatif) Définissez le statut de la règle.

La règle est activée par défaut.

- 15 (Facultatif) Modifiez l'état de la journalisation.

La journalisation est désactivée par défaut.

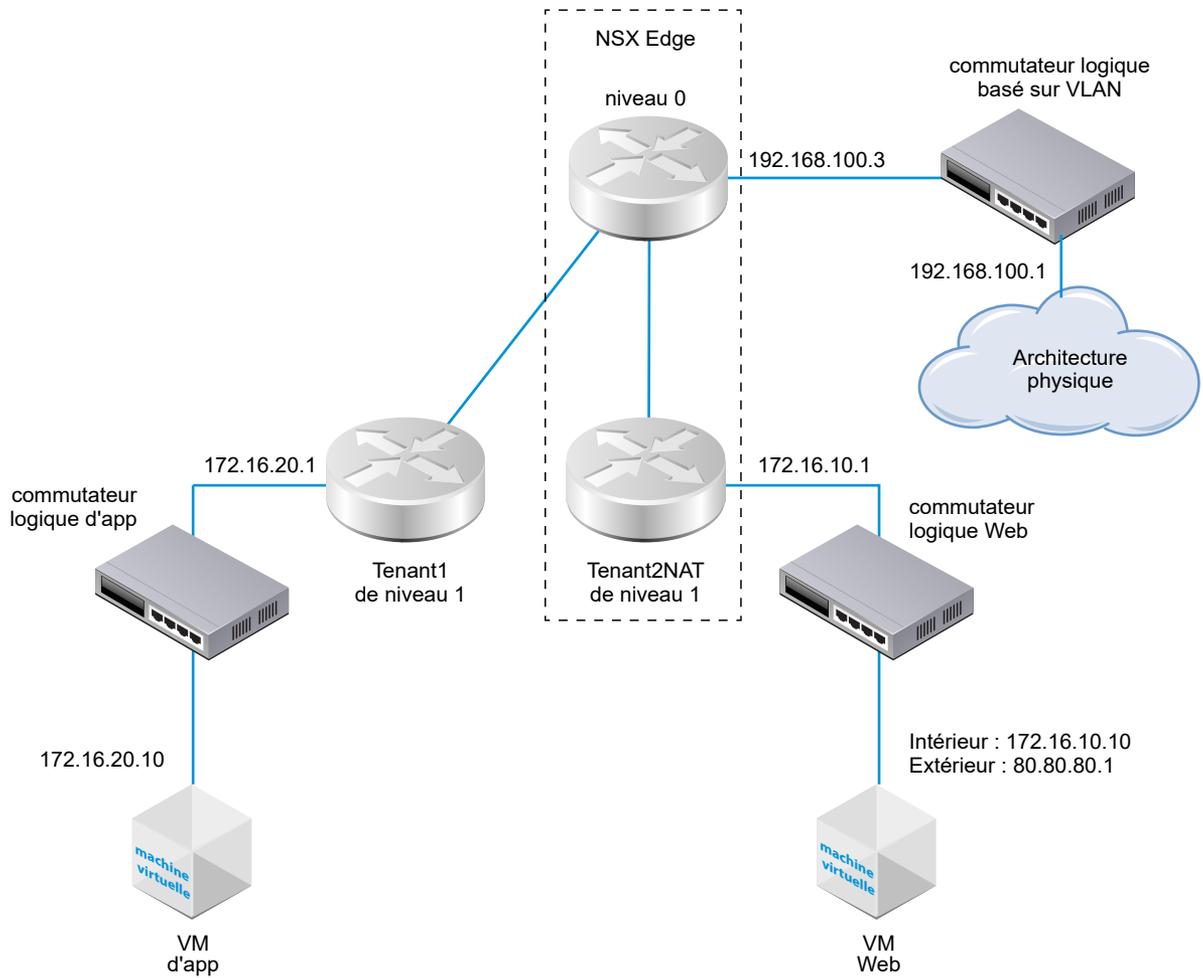
- 16 (Facultatif) Modifiez le paramètre de contournement de pare-feu.

Ce paramètre est activé par défaut.

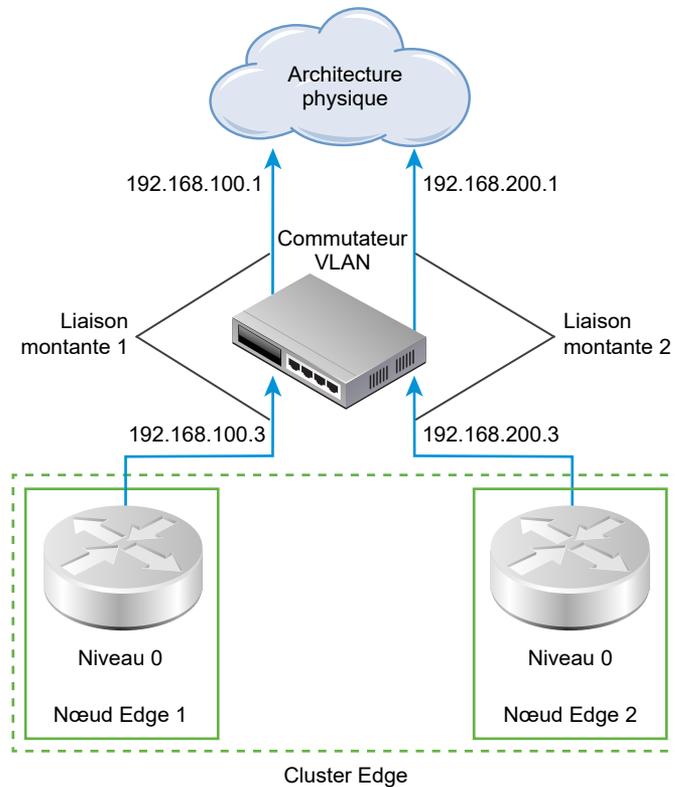
NAT réflexive

Lorsqu'un routeur logique de niveau 0 ou 1 est exécuté en mode Actif-Actif, vous ne pouvez pas configurer une NAT avec état, car des chemins d'accès asymétriques peuvent causer des problèmes. Pour les routeurs en mode Actif-Actif, vous pouvez utiliser une NAT réflexive (parfois appelée NAT sans état).

Dans cet exemple, les paquets étant reçus depuis la machine virtuelle Web, le routeur de niveau 1 Tenant2NAT remplace l'adresse IP source des paquets 172.16.10.10 par l'adresse IP 80.80.80.1. Disposer d'une adresse IP source publique permet à des destinations extérieures au réseau privé de revenir à la source d'origine.



Lorsque deux routeurs de niveau 0 en mode Actif-Actif sont impliqués, comme indiqué ici, la NAT réflexive doit être configurée.



Configurer une NAT réflexive sur un routeur logique de niveau 0 ou 1

Lorsqu'un routeur logique de niveau 0 ou 1 est exécuté en mode Actif-Actif, vous ne pouvez pas configurer une NAT avec état, car des chemins d'accès asymétriques peuvent causer des problèmes. Pour les routeurs en mode Actif-Actif, vous pouvez utiliser une NAT réflexive (parfois appelée NAT sans état).

Pour une NAT réflexive, vous pouvez configurer une adresse source unique à traduire ou une plage d'adresses. Si vous configurez une plage d'adresses source, vous devez également configurer une plage d'adresses traduites. La taille des deux plages doit être identique. La traduction d'adresse est déterministe, ce qui signifie que la première adresse de la plage d'adresses source est traduite vers la première adresse de la plage d'adresses traduites, la deuxième adresse de la plage source est traduite vers la deuxième adresse de la plage traduite et ainsi de suite.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Cliquez sur un routeur logique de niveau 0 ou 1 sur lequel vous voulez configurer une NAT réflexive.
- 4 Sélectionnez **Services > NAT**.
- 5 Cliquez sur **AJOUTER**.

6 Spécifiez une valeur de priorité.

Une valeur inférieure signifie une priorité plus élevée pour cette règle.

7 Pour **Action**, sélectionnez **Réflexive**.

8 Pour **Adresse IP Source**, spécifiez une adresse IP ou une plage d'adresses IP au format CIDR.

9 Pour **Adresse IP traduite**, spécifiez une adresse IP ou une plage d'adresses IP au format CIDR.

10 (Facultatif) Définissez le statut de la règle.

La règle est activée par défaut.

11 (Facultatif) Modifiez l'état de la journalisation.

La journalisation est désactivée par défaut.

12 (Facultatif) Modifiez le paramètre de contournement de pare-feu.

Ce paramètre est activé par défaut.

Résultats

La nouvelle règle est répertoriée sous NAT. Par exemple :

Tier0-LR-1
×

Présentation
Configuration ▾
Routage ▾
Services ▾

NAT
| ACTUALISER

Statistiques du nombre total de règles | Dernière mise à jour : 6 mars 2019 18:12:03

0 Sessions actives
0 Nombre de paquets
0 Octets Données

+ AJOUTER
MODIFIER
SUPPRIMER

ID	Action	Correspondance				Traduit		Appliqué à	Statistiques
		Protocole	IP source	Ports source	Adresse IP de destinat	Ports de destinati	IP		
▼ Priorité: 1024									
2048	Réflexif	Quelconque	80.80.80.1	Quelconque	Quelconque	Quelconque	172.16.10.10	Quelconque	

Sections de pare-feu et règles de pare-feu



Les sections de pare-feu sont utilisées pour grouper un ensemble de règles de pare-feu.

Une section de pare-feu est composée d'une ou plusieurs règles de pare-feu individuelles. Chaque règle de pare-feu individuelle contient des instructions qui déterminent si un paquet doit être autorisé ou bloqué, quels protocoles elle est autorisée à utiliser, quels ports elle est autorisée à utiliser, etc. Les sections sont utilisées pour l'architecture mutualisée, telle que des règles spécifiques pour les services de vente et d'ingénierie dans des sections séparées.

Une section peut être définie comme l'application de règles avec état ou sans état. Les règles sans état sont traitées comme des listes de contrôle d'accès (ACL) sans état traditionnelles. Les ACL réflexives ne sont pas prises en charge pour les sections sans état. Il n'est pas recommandé de mélanger des règles sans état et des règles avec état sur un port de commutateur logique, car cela pourrait entraîner un comportement non défini.

Il est possible de monter et de descendre des règles dans une section. Pour le trafic tentant de passer par le pare-feu, les informations sur le paquet sont soumises aux règles dans l'ordre indiqué dans la section, en commençant par le haut jusqu'à la règle par défaut en bas. La première règle qui correspond au paquet voit son action configurée appliquée, le traitement spécifié dans les options configurées de la règle est exécuté et toutes les règles suivantes sont ignorées (même si une règle ultérieure est une meilleure correspondance). Par conséquent, vous devez placer des règles spécifiques au-dessus de règles plus générales afin de garantir que ces règles ne sont pas ignorées. La règle par défaut, située en bas du tableau de règles, est une règle générique ; les paquets ne correspondant à aucune autre règle seront appliqués par la règle par défaut.

Note Un commutateur logique dispose d'une propriété appelée mode N-VDS. Cette propriété provient de la zone de transport à laquelle appartient le commutateur. Si le mode N-VDS est ENS (également appelé Enhanced Datapath), vous ne pouvez pas créer de règle de pare-feu ou de section avec le commutateur ou ses ports dans les champs Source, Destination ou Applied To.

Ce chapitre contient les rubriques suivantes :

- [Ajouter une section de règles de pare-feu](#)
- [Supprimer une section de règles de pare-feu](#)
- [Activer et désactiver des règles de section](#)

- [Activer et désactiver des journaux de sections](#)
- [À propos des règles de pare-feu](#)
- [Ajouter une règle de pare-feu](#)
- [Suppression d'une règle de pare-feu](#)
- [Modifier la règle du pare-feu distribué par défaut](#)
- [Modifier l'ordre d'une règle de pare-feu](#)
- [Filtrer les règles de pare-feu](#)
- [Configurer le pare-feu pour un port de pont de commutateur logique](#)
- [Configurer une liste d'exclusion de pare-feu](#)
- [Activer et désactiver le pare-feu](#)
- [Ajouter ou supprimer une règle de pare-feu à un routeur logique](#)

Ajouter une section de règles de pare-feu

Une section de règles de pare-feu est modifiée et enregistrée indépendamment et est utilisée pour appliquer une configuration de pare-feu distincte aux locataires.

Procédure

- 1 Sélectionnez **Sécurité > Pare-feu distribué** dans le panneau de navigation.
- 2 Cliquez sur l'onglet **Général** pour les règles de la couche 3 (L3) ou sur l'onglet **Ethernet** pour les règles de la couche 2 (L2).
- 3 Cliquez sur une section ou une règle existante.
- 4 Cliquez sur l'icône de section sur la barre de menus et sélectionnez **Ajouter la section ci-dessus** ou **Ajouter la section ci-dessous**.

Note Pour le trafic tentant de passer par le pare-feu, les informations sur le paquet sont soumises aux règles dans l'ordre indiqué dans le tableau Règles, en commençant par le haut jusqu'aux règles par défaut en bas. Dans certains cas, l'ordre de priorité de deux règles ou plus peut être important pour déterminer la disposition d'un paquet.

- 5 Entrez le nom de la section.
- 6 Pour rendre le pare-feu sans état, sélectionnez **Activer le pare-feu sans état**. Cette option est uniquement applicable à L3.

Les pare-feu sans état observent le trafic réseau, et limitent ou bloquent les paquets en fonction des adresses source et de destination ou d'autres valeurs statiques. Les pare-feu avec état peuvent

observer les flux de trafic d'une extrémité à l'autre. Les pare-feu sans état sont en général plus rapides et ont de meilleures performances sous des charges de trafic plus lourdes. Les pare-feu avec état sont plus efficaces pour identifier les communications non autorisées et falsifiées. Il n'y a pas de basculement entre le mode avec état et le mode sans état une fois qu'il est défini.

- 7 Sélectionnez un ou plusieurs objets pour appliquer la section.

Les types d'objet sont des ports logiques, des commutateurs logiques et des NSGroups. Si vous sélectionnez un NSGroup, il doit contenir un ou plusieurs commutateurs logiques ou ports logiques. Si le NSGroup contient uniquement les ensembles d'adresses IP ou les ensembles d'adresses MAC, il sera ignoré.

Note Le paramètre **Appliqué à** d'une section remplacera tous les paramètres **Appliqué à** des règles de cette section.

- 8 Cliquez sur **OK**.

Étape suivante

Ajoutez des règles de pare-feu à la section.

Supprimer une section de règles de pare-feu

Une section de règles de pare-feu peut être supprimée lorsqu'elle n'est plus utilisée.

Lorsque vous supprimez une section de règles de pare-feu, toutes les règles dans cette section sont supprimées. Vous ne pouvez pas supprimer une section et la rajouter ailleurs dans la table du pare-feu. Pour ce faire, vous devez supprimer la section et publier la configuration. Ensuite, ajoutez la section supprimée à la table de pare-feu et republiez la configuration.

Procédure

- 1 Sélectionnez **Sécurité > Pare-feu distribué** dans le panneau de navigation.
- 2 Cliquez sur l'onglet **Général** pour les règles L3 ou **Ethernet** pour les règles L2.
- 3 Cliquez sur l'icône du menu dans la première colonne de la section, puis sélectionnez **Supprimer la section**.

Vous pouvez également sélectionner la section et cliquer sur l'icône de suppression dans la barre de menus.

Activer et désactiver des règles de section

Vous pouvez activer ou désactiver toutes les règles dans une section de règles de pare-feu.

Procédure

- 1 Sélectionnez **Sécurité > Pare-feu distribué** dans le panneau de navigation.
- 2 Cliquez sur l'onglet **Général** pour les règles L3 ou **Ethernet** pour les règles L2.

- 3 Cliquez sur l'icône du menu dans la première colonne de la section et sélectionnez **Activer toutes les règles** ou **Désactiver toutes les règles**.
- 4 Cliquez sur **Publier**.

Activer et désactiver des journaux de sections

L'activation de journaux pour des règles de section enregistre des informations sur les paquets pour toutes les règles dans une section. En fonction du nombre de règles dans une section, une section de pare-feu classique générera de grandes quantités d'informations de journal et peut affecter les performances.

Les journaux sont stockés dans le fichier `/var/log/dfwpklogs.log` sur des hôtes vSphere ESXi et KVM.

Procédure

- 1 Sélectionnez **Sécurité > Pare-feu distribué** dans le panneau de navigation.
- 2 Cliquez sur l'onglet **Général** pour les règles L3 ou **Ethernet** pour les règles L2.
- 3 Cliquez sur l'icône du menu dans la première colonne de la section et sélectionnez **Activer les journaux** ou **Désactiver les journaux**.
- 4 Cliquez sur **Publier**.

À propos des règles de pare-feu

NSX-T Data Center utilise des règles de pare-feu pour spécifier le traitement du trafic vers et en dehors du réseau.

Le pare-feu offre plusieurs ensembles de règles configurables : règles de couche 3 (onglet Général) et règles de couche 2 (onglet Ethernet). Les règles de pare-feu de couche 2 sont traitées avant les règles de couche 3. Vous pouvez configurer une liste d'exclusion qui contient des commutateurs logiques, des ports logiques ou des groupes qui doivent être exclus de l'application du pare-feu.

Les règles de pare-feu s'appliquent comme suit :

- Les règles sont traitées de haut en bas.
- Chaque paquet est analysé en fonction de la règle définie sur la première ligne du tableau de règles. Les règles suivantes sont ensuite appliquées dans l'ordre descendant.
- La première règle de la table correspondant aux paramètres du trafic est appliquée.

Aucune règle suivante ne peut être appliquée, car la recherche est ensuite terminée pour ce paquet. En raison de ce comportement, il est toujours recommandé de placer les stratégies les plus granulaires en haut du tableau de règles. Ainsi, vous êtes assuré qu'elles seront appliquées avant des règles plus spécifiques.

La règle par défaut, située en bas du tableau de règles, est une règle générique ; les paquets ne correspondant à aucune autre règle seront appliqués par la règle par défaut. Après l'opération de préparation de l'hôte, la règle par défaut est définie pour autoriser l'action. Cela garantit que la communication entre VM n'est pas rompue lors des phases de transfert ou de migration. Il est vivement conseillé de modifier par la suite cette règle par défaut afin de bloquer l'action et d'appliquer un contrôle de l'accès via un modèle de contrôle positif (c'est-à-dire que seul le trafic défini dans la règle de pare-feu est autorisé sur le réseau).

Note Pour le protocole TCP, la vérification stricte est automatiquement activée pour une règle avec état. Cela signifie qu'un paquet est mis en correspondance avec la règle TCP uniquement si la connexion réseau a été démarrée avec un paquet SYN.

Tableau 7-1. Propriétés d'une règle de pare-feu

Propriété	Description
Nom	Nom de la règle de pare-feu.
ID	ID système unique généré pour chaque règle.
Source	La source de la règle peut être une adresse IP ou MAC ou un objet autre qu'une adresse IP. La source correspondra à n'importe laquelle si elle n'est pas définie. IPv6 n'est pas pris en charge pour la plage source ou de destination.
Destination	Masque de réseau/adresse IP ou MAC de destination de la connexion concernée par la règle. La destination correspondra à n'importe laquelle si elle n'est pas définie. IPv6 n'est pas pris en charge pour la plage source ou de destination.
Service	Le service peut être une combinaison de protocoles de port prédéfinie pour L3. Pour L2, il peut être de type ether. Pour L2 et L3, vous pouvez définir manuellement un nouveau service ou groupe de services. Le service correspondra à n'importe lequel, s'il n'est pas spécifié.
Appliqué à	Définit l'étendue à laquelle la règle s'applique. Si elle n'est pas définie, l'étendue sera tous les ports logiques. Si vous avez ajouté « Appliqué à » dans une section, elle remplacera la règle.
Journal	La journalisation peut être désactivée ou activée. Les journaux sont stockés dans le fichier <code>/var/log/dfwpklogs.log</code> sur des hôtes ESX et KVM.
Action	L'action appliquée par la règle peut être Autoriser , Abandonner ou Refuser . La valeur par défaut est Autoriser .
Protocole IP	Les options sont IPv4 , IPv6 et IPv4_IPv6 . La valeur par défaut est IPv4_IPv6 . Pour accéder à cette propriété, cliquez sur l'icône Paramètres avancés .
Direction	Les options sont Entrant , Sortant et Entrant/Sortant . La valeur par défaut est Entrant/Sortant . Ce champ fait référence à la direction du trafic selon le point de vue de l'objet de destination. Entrant signifie que seul le trafic vers l'objet est vérifié, Sortant signifie que seul le trafic provenant de l'objet est vérifié et Entrant/Sortant signifie que le trafic dans les deux sens est vérifié. Pour accéder à cette propriété, cliquez sur l'icône Paramètres avancés .

Tableau 7-1. Propriétés d'une règle de pare-feu (suite)

Propriété	Description
Balises de règle	Balises qui ont été ajoutées à la règle. Pour accéder à cette propriété, cliquez sur l'icône Paramètres avancés .
Statistiques sur les flux	Champ en lecture seule qui affiche le nombre d'octets, le nombre de paquets et les sessions. Pour accéder à cette propriété, cliquez sur l'icône de graphique.

Note Si Spoofguard n'est pas activé, les liaisons d'adresse découvertes automatiquement ne peuvent pas être garanties comme étant dignes de confiance, car une machine virtuelle malveillante peut demander l'adresse d'une autre machine virtuelle. Si Spoofguard est activé, il vérifie chaque liaison découverte afin que seules les liaisons approuvées soient présentées.

Ajouter une règle de pare-feu

Un pare-feu est un système de sécurité réseau qui surveille et contrôle le trafic réseau entrant et sortant en fonction de règles de pare-feu prédéterminées.

Des règles de pare-feu sont ajoutées à l'étendue de NSX Manager. Le champ Appliqué à vous permet d'affiner le niveau auquel vous souhaitez appliquer la règle. Vous pouvez ajouter plusieurs objets aux niveaux source et destination de chaque règle, de sorte à réduire le nombre total de règles de pare-feu à ajouter.

Note Par défaut, une règle correspond à la valeur par défaut d'éléments source, de destination et de règle de service, qui correspondent à toutes les interfaces et tous les sens du trafic. Si vous voulez limiter l'effet de la règle à des interfaces ou des sens du trafic particuliers, vous devez spécifier la limite dans la règle.

Conditions préalables

Pour utiliser un groupe d'adresses, commencez par associer manuellement les adresses IP et MAC de chaque VM à leur commutateur logique.

Procédure

- 1 Sélectionnez **Sécurité > Pare-feu distribué** dans le panneau de navigation.
- 2 Cliquez sur l'onglet **Général** pour les règles L3 ou **Ethernet** pour les règles L2.
- 3 Cliquez sur une section ou une règle existante.

- 4 Cliquez sur l'icône du menu dans la première colonne d'une règle et sélectionnez **Ajouter la règle ci-dessus** ou **Ajouter la règle ci-dessous**.

Une nouvelle ligne s'affiche pour définir une règle de pare-feu.

Note Pour le trafic tentant de passer par le pare-feu, les informations sur le paquet sont soumises aux règles dans l'ordre indiqué dans le tableau Règles, en commençant par le haut jusqu'aux règles par défaut en bas. Dans certains cas, l'ordre de priorité de deux règles ou plus peut être important pour déterminer la disposition d'un paquet.

- 5 Dans la colonne **Nom**, entrez le nom de la règle.
- 6 Dans la colonne **Source**, cliquez sur l'icône de modification et sélectionnez la source de la règle. La source correspondra à n'importe laquelle si elle n'est pas définie.

Option	Description
Adresses IP	Entrez plusieurs adresses IP ou MAC dans une liste en les séparant par une virgule. La liste peut comporter jusqu'à 255 caractères. Les formats IPv4 et IPv6 sont pris en charge.
Objets de conteneur	Les objets disponibles sont Ensemble d'IP, Port logique, Commutateur logique et Groupe NS. Sélectionnez les objets et cliquez sur OK .

- 7 Dans la colonne **Destination**, cliquez sur l'icône de modification et sélectionnez la destination. La destination correspondra à n'importe laquelle si elle n'est pas définie.

Option	Description
Adresses IP	Vous pouvez entrer plusieurs adresses IP ou MAC dans une liste en les séparant par une virgule. La liste peut comporter jusqu'à 255 caractères. Les formats IPv4 et IPv6 sont pris en charge.
Objets de conteneur	Les objets disponibles sont Ensemble d'IP, Port logique, Commutateur logique et Groupe NS. Sélectionnez les objets et cliquez sur OK .

- 8 Dans la colonne **Service**, cliquez sur l'icône de modification et sélectionnez les services. Le service correspondra à n'importe lequel s'il n'est pas défini.
- 9 Pour sélectionner un service prédéfini, sélectionnez un ou plusieurs des services disponibles.
- 10 Pour définir un nouveau service, cliquez sur l'onglet **Port brut-Protocole** et cliquez sur **Ajouter**.

Option	Description
Type de service	<ul style="list-style-type: none"> ■ ALG ■ ICMP ■ IGMP ■ IP ■ Ensemble de ports L4
Protocole	Sélectionnez l'un des protocoles disponibles.
Ports source	Entrez le port source.
Ports de destination	Sélectionnez le port de destination.

- 11 Dans la colonne **Appliqué à**, cliquez sur l'icône de modification et sélectionnez des objets.

12 Dans la colonne **Journal**, définissez l'option de journalisation.

Les journaux sont stockés dans le fichier `/var/log/dfwpktLogs.log` sur les hôtes ESXi et KVM. L'activation de la journalisation peut affecter les performances.

13 Dans la colonne **Action**, sélectionnez une action.

Option	Description
Autoriser	Autorise le trafic L3 ou L2 avec la source, la destination et le protocole spécifiés à passer par le contexte de pare-feu actuel. Les paquets qui correspondent à la règle, et qui sont acceptés, traversent le système comme si le pare-feu n'était pas présent.
Annuler	Abandonne des paquets avec la source, la destination et le protocole spécifiés. L'abandon d'un paquet est une action silencieuse sans notification aux systèmes source ou de destination. L'abandon d'un paquet entraîne une nouvelle tentative de connexion jusqu'à ce que le seuil de nouvelles tentatives soit atteint.
Refuser	Rejette des paquets avec la source, la destination et le protocole spécifiés. Le refus d'un paquet est une manière plus appropriée de refuser un paquet, car il envoie un message de destination inaccessible à l'expéditeur. Si le protocole est TCP, un message TCP RST est envoyé. Les messages ICMP avec du code interdit par l'administrateur sont envoyés pour les connexions UDP, ICMP et autres connexions IP. L'avantage d'utiliser Refuser est que l'application d'envoi est informée après une seule tentative que la connexion ne peut pas être établie.

14 Cliquez sur l'icône **Paramètres avancés** pour spécifier le protocole IP, la direction, les balises de règle et les commentaires.

15 Cliquez sur **Publier**.

Suppression d'une règle de pare-feu

Un pare-feu est un système de sécurité réseau qui surveille et contrôle le trafic réseau entrant et sortant en fonction de règles de pare-feu prédéterminées. Des règles définies personnalisées peuvent être ajoutées et supprimées.

Procédure

- 1 Sélectionnez **Sécurité > Pare-feu distribué** dans le panneau de navigation.
- 2 Cliquez sur l'onglet **Général** pour les règles L3 ou **Ethernet** pour les règles L2.
- 3 Cliquez sur l'icône du menu dans la première colonne de la règle, puis sélectionnez **Supprimer la règle**.
- 4 Cliquez sur **Publier**.

Modifier la règle du pare-feu distribué par défaut

Vous pouvez modifier les paramètres de pare-feu par défaut qui s'appliquent au trafic qui ne correspond à aucune règle de pare-feu définie par l'utilisateur.

Les règles de pare-feu par défaut s'appliquent au trafic qui ne correspond à aucune règle de pare-feu définie par l'utilisateur. La règle de couche 3 par défaut s'affiche sous l'onglet **Général** et la règle de couche 2 par défaut s'affiche sous l'onglet **Ethernet**.

Les règles de pare-feu par défaut permettent à tout le trafic de couche 3 et de couche 2 d'emprunter tous les clusters préparés de votre infrastructure. La règle par défaut se situe toujours en bas de la table des règles et il est impossible de l'en supprimer. Toutefois, pour l'élément **Action** de la règle, vous pouvez remplacer **Autoriser** par **Annuler** ou par **Refuser** (non recommandé) et indiquer si le trafic de cette règle doit être journalisé.

La règle de pare-feu de couche 3 par défaut s'applique à tout le trafic, y compris au trafic DHCP. Si vous remplacez **Action** par **Annuler** ou **Refuser**, le trafic DHCP sera bloqué. Vous devrez créer une règle pour autoriser le trafic DHCP.

Procédure

- 1 Sélectionnez **Sécurité > Pare-feu distribué** dans le panneau de navigation.
- 2 Cliquez sur l'onglet **Général** pour les règles L3 ou **Ethernet** pour les règles L2.
- 3 Dans la colonne **Nom**, entrez un nouveau nom.
- 4 Dans la colonne **Action**, sélectionnez une des options.
 - Autoriser : autorise le trafic de couche 3 ou de couche 2 avec la source, la destination et le protocole spécifiés à passer par le contexte de pare-feu actuel. Les paquets qui correspondent à la règle, et qui sont acceptés, traversent le système comme si le pare-feu n'était pas présent.
 - Bloquer : annule des paquets avec la source, la destination et le protocole spécifiés. L'abandon d'un paquet est une action silencieuse sans notification aux systèmes source ou de destination. L'abandon d'un paquet entraîne une nouvelle tentative de connexion jusqu'à ce que le seuil de nouvelles tentatives soit atteint.
 - Refuser : refuse des paquets avec la source, la destination et le protocole spécifiés. Le refus d'un paquet est une manière plus appropriée de refuser un paquet, car il envoie un message de destination inaccessible à l'expéditeur. Si le protocole est TCP, un message TCP RST est envoyé. Les messages ICMP avec du code interdit par l'administrateur sont envoyés pour les connexions UDP, ICMP et autres connexions IP. L'avantage d'utiliser Refuser est que l'application d'envoi est informée après une seule tentative que la connexion ne peut pas être établie.

Note Il n'est pas recommandé de sélectionner **Refuser** comme action pour la règle par défaut.

- 5 Dans **Journal**, activez ou désactivez la journalisation.
L'activation de la journalisation peut affecter les performances.
- 6 Cliquez sur **Publier**.

Modifier l'ordre d'une règle de pare-feu

Les règles sont traitées de haut en bas. Vous pouvez modifier l'ordre des règles dans la liste.

Pour le trafic tentant de passer par le pare-feu, les informations sur le paquet sont soumises aux règles dans l'ordre indiqué dans le tableau Règles, en commençant par le haut jusqu'aux règles par défaut en bas. Dans certains cas, l'ordre de priorité de deux règles ou plus peut être important pour déterminer le flux de trafic.

Vous pouvez déplacer une règle personnalisée vers le haut ou vers le bas du tableau ; la règle par défaut se trouve toujours en bas du tableau et ne peut pas être déplacée.

Procédure

- 1 Sélectionnez **Sécurité > Pare-feu distribué** dans le panneau de navigation.
- 2 Cliquez sur l'onglet **Général** pour les règles L3 ou **Ethernet** pour les règles L2.
- 3 Sélectionnez la règle et cliquez sur l'icône **Monter** ou **Descendre** dans la barre de menus.
- 4 Cliquez sur **Publier**.

Filtrer les règles de pare-feu

Lorsque vous accédez à la section de pare-feu, toutes les règles sont affichées au départ. Vous pouvez appliquer un filtre pour contrôler les données affichées afin de ne voir qu'un sous-ensemble des règles. Cela peut faciliter la gestion des règles.

Procédure

- 1 Sélectionnez **Sécurité > Pare-feu distribué** dans le panneau de navigation.
- 2 Cliquez sur l'onglet **Général** pour les règles L3 ou **Ethernet** pour les règles L2.
- 3 Dans le champ de recherche sur le côté droit de la barre de menus, sélectionnez un objet ou entrez les premiers caractères d'un nom d'objet pour limiter la liste des objets à sélectionner.

Lorsque vous sélectionnez un objet, le filtre est appliqué et la liste des règles est mise à jour, ce qui affiche uniquement les règles qui contiennent l'objet dans l'une des colonnes suivantes :

- Sources
- Destinations
- Appliqué à
- Services

- 4 Pour supprimer le filtre, supprimez le nom de l'objet dans le champ de texte.

Configurer le pare-feu pour un port de pont de commutateur logique

Vous pouvez configurer des sections de pare-feu et les règles de pare-feu pour le port de pont d'un commutateur logique de couche 2 sauvegardé par pont. Le pont doit être créé à l'aide de nœuds NSX Edge.

Conditions préalables

Vérifiez que le commutateur est associé à un profil de pont. Reportez-vous à la section [Créer un commutateur logique sauvegardé par pont de couche 2](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Sécurité > Pare-feu de pont** dans le panneau de navigation.
- 3 Sélectionnez un commutateur logique.
Le commutateur doit être associé à un profil de pont.
- 4 Suivez les mêmes étapes que dans les sections précédentes pour configurer un pare-feu de couche 2 ou de couche 3.

Configurer une liste d'exclusion de pare-feu

Un port logique, un commutateur logique ou un NSGroup peuvent être exclus d'une règle de pare-feu.

Après avoir créé une section comportant des règles de pare-feu, vous pouvez choisir d'exclure un port du dispositif NSX-T Data Center des règles de pare-feu.

Procédure

- 1 Sélectionnez **Sécurité > Pare-feu distribué** dans le panneau de navigation.
- 2 Cliquez sur l'onglet **Liste d'exclusion**.
- 3 Cliquez sur **Ajouter**.
- 4 Sélectionnez un type et un objet.
Les types disponibles sont **Port logique**, **Commutateur logique** et **NSGroup**.
- 5 Cliquez sur **OK**.
- 6 Pour supprimer un objet dans la liste d'exclusion, sélectionnez l'objet et cliquez sur **Supprimer** dans la barre de menus.

Activer et désactiver le pare-feu

Vous pouvez activer ou désactiver la fonctionnalité de pare-feu distribué. Si la fonctionnalité est désactivée, aucune règle ne sera appliquée.

Procédure

- 1 Sélectionnez **Sécurité > Pare-feu distribué** dans le panneau de navigation.
- 2 Cliquez sur l'onglet **Paramètres**.
- 3 Cliquez sur **Modifier**.

- 4 Dans la boîte de dialogue, définissez l'état du pare-feu sur vert (activé) ou gris (désactivé).
- 5 Cliquez sur **Enregistrer**.

Ajouter ou supprimer une règle de pare-feu à un routeur logique

Vous pouvez ajouter des règles de pare-feu à un routeur logique de niveau 0 ou de niveau 1 afin de contrôler la communication dans le routeur.

Conditions préalables

Familiarisez-vous avec les paramètres d'une règle de pare-feu. Reportez-vous à la section [Ajouter une règle de pare-feu](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Routeurs** s'il n'est pas déjà sélectionné.
- 4 Cliquez sur le nom d'un routeur logique.
- 5 Sélectionnez **Services > Pare-feu Edge**.
- 6 Cliquez sur une section ou une règle existante.
- 7 Pour ajouter une règle, cliquez sur **Ajouter une règle** dans la barre de menus et sélectionnez **Ajouter la règle ci-dessus** ou **Ajouter la règle ci-dessous**, ou cliquez sur l'icône du menu dans la première colonne d'une règle et sélectionnez **Ajouter la règle ci-dessus** ou **Ajouter la règle ci-dessous**, puis spécifiez les paramètres de règle.

Le champ Appliqué à n'est pas affiché, car cette règle s'applique uniquement au routeur logique.
- 8 Pour supprimer une règle, sélectionnez-la, cliquez sur **Supprimer** dans la barre de menus ou cliquez sur l'icône du menu dans la première colonne et sélectionnez **Supprimer**.

Résultats

Note Si vous ajoutez une règle de pare-feu à un routeur logique de niveau 0 et que le cluster NSX Edge sauvegardant le routeur est en cours d'exécution en mode actif-actif, le pare-feu peut uniquement s'exécuter en mode sans état. Si vous configurez la règle de pare-feu avec des services avec état tels qu'HTTP, SSL, TCP et ainsi de suite, la règle de pare-feu ne fonctionnera pas comme prévu. Pour éviter ce problème, configurez le cluster NSX Edge afin qu'il s'exécute en mode actif-veille.

Réseaux privés virtuels

8

NSX-T Data Center prend en charge les VPN IPSec et les VPN de couche 2 (L2VPN) sur NSX Edge.

Note Les VPN IPSec et L2VPN ne sont pas pris en charge dans la version NSX-T Data Center avec exportation limitée.

VPN IPSec

Un VPN IPSec sécurise le trafic circulant entre deux réseaux connectés via un réseau public par le biais de passerelles IPSec appelées points de terminaison. NSX Edge prend uniquement en charge un mode tunnel qui utilise la mise en tunnel IP avec ESP (Encapsulating Security Payload).

Le VPN IPSec utilise le protocole IKE pour négocier les paramètres de sécurité. Le port UDP par défaut est défini à 500. Si NAT est détectée dans la passerelle, le port est défini sur 4500.

Note Le VPN IPSec est pris en charge uniquement sur le routeur logique de niveau 0.

NSX Edge prend en charge deux types de VPN, le VPN basé sur des stratégies et le VPN basé sur une route.

Les VPN basés sur des stratégies exigent qu'une stratégie soit appliquée aux paquets transférés au service IPSec. Ce type de VPN est considéré comme statique, car lorsque la topologie et la configuration du réseau local changent, les paramètres de stratégie doivent également être mis à jour pour prendre en charge les modifications.

Un VPN basé sur une route fournit un tunnel sur le trafic en fonction des itinéraires appris dynamiquement sur une interface spéciale appelée interface de tunnel virtuel (VTI) qui utilise BGP, par exemple, comme protocole. IPSec sécurise tout le trafic circulant à travers l'interface de tunnel virtuel (VTI).

VPN L2

La connectivité L2VPN permet d'étendre les réseaux de couche 2 d'un centre de données sur site au cloud, tel que VMware Cloud sur Amazon (VMC). Cette connexion est sécurisée avec le tunnel IPSec basé sur une route.

Le réseau étendu est un sous-réseau unique avec un seul domaine de diffusion, de sorte que vous pouvez migrer les machines virtuelles entre le centre de données sur site et cloud public sans avoir à modifier leurs adresses IP.

En plus de prendre en charge la migration de centre de données, un réseau sur site étendu avec un L2VPN est utile pour la récupération d'urgence et l'implication dynamique des ressources de calcul hors site pour répondre à une augmentation de la demande appelée « cloud bursting ».

Chaque session L2VPN dispose d'un tunnel GRE. La redondance du tunnel n'est pas prise en charge. Une session L2VPN peut s'étendre sur jusqu'à 4094 réseaux de couche 2.

Note L2VPN est pris en charge entre NSX-T Data Center et un dispositif NSX Edge qui est non géré ou géré dans une instance de NSX Data Center for vSphere.

Ce chapitre contient les rubriques suivantes :

- [Configuration du VPN IPSec](#)
- [Configuration de VPN L2](#)

Configuration du VPN IPSec

Vous pouvez uniquement créer un VPN basé sur une route et une session VPN basée sur des stratégies à l'aide de l'API.

Note Le VPN IPSec n'est pas pris en charge dans la version NSX-T Data Center avec exportation limitée.

Vous ne pouvez pas utiliser NAT et VPN IPSec simultanément sur le même profil réseau. Assurez-vous de placer NAT et VPN IPSec sur différents profils réseau.

Conditions préalables

Familiarisez-vous avec le VPN IPSec. Reportez-vous à la section [VPN IPSec](#).

Procédure

- 1 Configurez un service VPN IPSec sur le routeur logique de niveau 0.

Utilisez l'appel de POST `/api/v1/vpn/ipsec/services`.

```
POST /api/v1/vpn/ipsec/services
{
  "display_name": "IPSec VPN service",
  "logical_router_id": "f81f220f-3072-4a6e-9f53-ad3b8bb8af57"
}
```

- 2 Configurez le profil DPD (Dead Peer Detection).

Utilisez l'appel de POST `/api/v1/vpn/ipsec/dpd-profiles`.

Le profil par défaut est provisionné avec un intervalle de sonde DPD de 60 secondes.

```
POST /api/v1/vpn/ipsec/dpd-profiles
{
  "enabled": "true",
  "dpd_probe_interval": 60,
  "description": "DPD profile",
  "display_name": "DPD profile"
}
```

3 Configurez les paramètres de profil IKE.

Utilisez l'appel de POST `/api/v1/vpn/ipsec/ike-profiles`.

```
POST /api/v1/vpn/ipsec/ike-profiles
{
  "digest_algorithms": ["SHA2_256"],
  "description": "IKEProfile for site1",
  "display_name": "IKEProfile site1",
  "encryption_algorithms": ["AES_128"],
  "ike_version": "IKE_V2",
  "dh_groups": ["GROUP14"],
  "sa_life_time": 21600
}
```

4 Configurez un profil de tunnel pour le VPN IPsec.

Utilisez l'appel de POST `/api/v1/vpn/ipsec/tunnel-profiles`.

```
POST /api/v1/vpn/ipsec/tunnel-profiles/
{
  "digest_algorithms": ["SHA1", "SHA2_256"],
  "description": "Tunnel Profile for site 1",
  "display_name": "Tunnel Profile for site 1",
  "encapsulation_mode": "TUNNEL_MODE",
  "encryption_algorithms": ["AES_128", "AES_256"],
  "enable_perfect_forward_secrecy": true,
  "dh_groups": ["GROUP14"],
  "transform_protocol": "ESP",
  "sa_life_time": 3600,
  "df_policy": "CLEAR"
}
```

5 Configurez un point de terminaison homologue pour communiquer avec l'homologue VPN IPsec.

Utilisez l'appel de POST `/api/v1/vpn/ipsec/peer-endpoints`.

```
POST /api/v1/vpn/ipsec/peer-endpoints
{
  "display_name": "Peer endpoint for site 1",
  "connection_initiation_mode": "INITIATOR",
  "authentication_mode": "PSK",
  "ipsec_tunnel_profile_id": "640607f3-bb83-4e54-a153-57939965881c",
  "dpd_profile_id": "4808d04e-572d-480d-8182-61ddaa146461",
  "psk": "6721b9f1f5936956c0a8b4ed95286b452db04dae721edd0f264f0fcc6e94882b",
}
```

```
"ike_profile_id": "a4db6863-b6f0-45bd-967e-a2e22c260329",
"peer_address": "10.14.24.4",
"peer_id": "10.14.24.4"
}
```

6 Configurez un point de terminaison local pour le point de terminaison VPN.

Utilisez l'appel de POST `/api/v1/vpn/ipsec/local-endpoints`.

```
POST /api/v1/vpn/ipsec/local-endpoints
{
  "local_address": "1.1.1.12",
  "local_id": "1.1.1.12",
  "display_name": "Local endpoint",
  "ipsec_vpn_service_id": {
    "target_id": "81388ec0-b5e3-4a9e-b551-e372e700772c"
  }
}
```

7 Configurez une session VPN basée sur une route.

Utilisez l'appel de POST `/api/v1/vpn/ipsec/sessions`.

```
POST /api/v1/vpn/ipsec/sessions
{
  "resource_type": "RouteBasedIPSecVPNSession",
  "display_name": "RouteSession1",
  "ipsec_vpn_service_id": "657bcb55-48ce-4e0f-bfc7-a5a91b2990ae",
  "peer_endpoint_id": "cfc70ab5-16d1-4292-9391-fcee23ccea96",
  "local_endpoint_id": "9d4b44f1-0bfa-4705-ac67-09244a17d42e",
  "enabled": true,
  "tunnel_ports": [
    {
      "ip_subnets": [
        {
          "ip_addresses": [
            "192.168.50.1"
          ],
          "prefix_length": 24
        }
      ]
    }
  ]
}
```

8 Configurez une session VPN basée sur des stratégies.

Utilisez l'appel de POST `/api/v1/vpn/ipsec/sessions`.

```
POST /api/v1/vpn/ipsec/sessions
{
  "resource_type": "PolicyBasedIPSecVPNSession",
  "display_name": "PolicySession1",
  "ipsec_vpn_service_id": "ea071856-9e91-4826-a841-9ec7ee9ea534",
  "peer_endpoint_id": "0c2447d2-8890-4b55-bf02-8c6b1a94d1ce",
}
```

```

"local_endpoint_id": "161acb63-c3f2-438d-9e5c-cb655e6a1099",
"enabled": true,
"policy_rules": [
  {
    "sources": [
      {
        "subnet": "2.2.2.0/24"
      }
    ],
    "logged": true,
    "destinations": [
      {
        "subnet": "3.3.3.0/24"
      }
    ],
    "action": "PROTECT",
    "enabled": true
  }
]
}

```

Configuration de VPN L2

Vous pouvez uniquement créer un service et une session L2VPN à l'aide de l'API.

Note L2VPN n'est pas pris en charge dans la version NSX-T Data Center avec exportation limitée.

Conditions préalables

- Familiarisez-vous avec L2VPN. Reportez-vous à la section [VPN L2](#).
- Vérifiez qu'un routeur logique de niveau 0 est configuré avec des profils de liaison montante. Reportez-vous à *Guide d'installation de NSX-T Data Center*.
- Vérifiez qu'un commutateur logique est configuré. Reportez-vous à la section [Créer un commutateur logique](#).
- Vérifiez qu'un NSX Edge non géré est disponible dans NSX Data Center for vSphere.
- Assurez-vous que le VPN IPSec est configuré. [Configuration du VPN IPSec](#)

Procédure

1 Configurez un service L2VPN.

Utilisez l'appel de POST `/api/v1/vpn/l2vpn/services`.

```

POST /api/v1/vpn/l2vpn/services
{
  "logical_router_id": "b6fe5455-619b-4030-b5f8-8575749f4404",
  "logical_tap_ip_pool" : [ "169.254.64.0/28" ],
  "enable_full_mesh" : true
}

```

2 Configurez une session L2VPN.

Utilisez l'appel de POST `/api/v1/vpn/l2vpn/sessions`.

```
POST /api/v1/vpn/l2vpn/sessions
{
  "l2vpn_service_id" : "421de3a2-c6ec-4c42-a891-5bde3b5feb68",
  "transport_tunnels" : [
    {
      "target_id" : "801e5140-6da8-4e78-ab44-f966de75f311"
    }
  ]
}
```

3 Configurez un port logique avec connexion.

Utilisez l'appel de POST `/api/v1/vpn/logical-ports`.

```
POST /api/v1/logical-ports/
{
  "resource_type": "LogicalPort",
  "display_name": "Extend logicaSwitch, port for service",
  "logical_switch_id": "f52abcee-27a7-426c-a128-037db2283582",
  "admin_state" : "UP",
  "attachment": {
    "attachment_type": "L2VPN_SESSION",
    "id": "6806c4ea-3b77-4b8a-8af2-ccc47b1ba8a9",
    "context" : {
      "resource_type" : "L2VpnAttachmentContext",
      "tunnel_id" : 10
    }
  }
}
```

4 Téléchargez la configuration de code homologue L2VPN.

GET `/api/v1/vpn/l2vpn/sessions/<L2VPN-session-ID>/peer-codes`

5 Connectez-vous à la CLI de NSX Edgenon géré de NSX Data Center for vSphere sur site.

6 Collez la configuration de code homologue L2VPN.

7 (Facultatif) Surveillez la session L2VPN.

- Récapitulatif de la session L2VPN GET `/api/v1/vpn/l2vpn/sessions/summary`.
- Statistiques de la session L2VPN GET `/api/v1/vpn/l2vpn/sessions/<L2VPN-session-ID>/statistics`.

Gestion d'objets, de groupes, de services et de machines virtuelles

9

Vous pouvez créer des ensembles d'IP, des pools d'IP, des ensembles MAC, des NSGroups et des NSServices. Vous pouvez également gérer des balises pour les machines virtuelles.

Ce chapitre contient les rubriques suivantes :

- [Créer un ensemble d'adresses IP](#)
- [Créer un pool d'adresses IP](#)
- [Créer un ensemble d'adresses MAC](#)
- [Créer un NSGroup](#)
- [Configuration de services et de groupes de services](#)
- [Gérer les balises d'une machine virtuelle](#)

Créer un ensemble d'adresses IP

Un ensemble d'adresses IP est un groupe d'adresses IP que vous pouvez utiliser comme sources et destinations dans des règles de pare-feu.

Un ensemble d'adresses IP peut contenir une combinaison d'adresses IP individuelles, de plages d'adresses IP et de sous-réseaux. Vous pouvez spécifier des adresses IPv4 ou IPv6, ou les deux. Un ensemble d'adresses IP peut être un membre de groupes NSGroup.

Note IPv6 n'est pas pris en charge pour les plages source ou de destination pour les règles de pare-feu.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Inventaire > Groupes** dans le panneau de navigation.
- 3 Sélectionnez **Ensembles d'adresses IP** en haut du panneau principal.
- 4 Cliquez sur **Ajouter**.
- 5 Entrez un nom.

- 6 (Facultatif) Entrez une description.
- 7 Entrez des adresses individuelles ou une plage d'adresses.
- 8 Cliquez sur **Enregistrer**.

Créer un pool d'adresses IP

Vous pouvez utiliser un pool d'adresses IP pour allouer des adresses IP ou des sous-réseaux lorsque vous créez des sous-réseaux L3.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Inventaire > Groupes** dans le panneau de navigation.
- 3 Sélectionnez **Pools d'adresses IP** en haut du panneau principal.
- 4 Cliquez sur **Ajouter**.
- 5 Entrez un nom.
- 6 (Facultatif) Entrez une description.
- 7 Cliquez sur **Ajouter**.
- 8 Entrez des plages d'adresses IP.

Passez le curseur de la souris sur le coin supérieur droit de chaque cellule et cliquez sur l'icône de crayon pour la modifier.
- 9 (Facultatif) Entrez une passerelle.
- 10 Entrez une adresse IP CIDR avec un suffixe.
- 11 (Facultatif) Entrez des serveurs DNS.
- 12 (Facultatif) Entrez un suffixe DNS.
- 13 Cliquez sur **Enregistrer**.

Créer un ensemble d'adresses MAC

Un ensemble d'adresses MAC est un groupe d'adresses MAC que vous pouvez utiliser comme sources et destinations dans des règles de pare-feu de couche 2 et comme membre d'un groupe NS.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Inventaire > Groupes** dans le panneau de navigation.
- 3 Sélectionnez **Ensembles d'adresses MAC** en haut du panneau principal.

- 4 Cliquez sur **Ajouter**.
- 5 Entrez un nom.
- 6 (Facultatif) Entrez une description.
- 7 Entrez les adresses MAC.
- 8 Cliquez sur **Enregistrer**.

Créer un NSGroup

Vous pouvez configurer un NSGroup pour qu'il contienne une combinaison d'ensembles d'IP, d'ensembles MAC, de ports logiques, de commutateurs logiques et d'autres NSGroups. Vous pouvez spécifier des NSGroups comme des sources et destinations, ainsi que dans le champ `Applied To`, dans des règles de pare-feu.

Remarques concernant NSX Cloud Si vous utilisez NSX Cloud, reportez-vous à la section [Comment utiliser des fonctionnalités NSX-T Data Center avec le cloud public](#) pour obtenir la liste des entités logiques générées automatiquement, les fonctionnalités prises en charge et les configurations requises pour NSX Cloud.

Un NSGroup a les caractéristiques suivantes :

- Vous pouvez spécifier des membres directs, qui peuvent être des ensembles d'IP, des ensembles MAC, des commutateurs logiques, des ports logiques et des NSGroups.
- Vous pouvez spécifier jusqu'à cinq critères d'appartenance qui s'appliquent à des commutateurs logiques, des ports logiques ou des machines virtuelles. Pour un critère qui s'applique à des commutateurs logiques ou des ports logiques, vous pouvez spécifier une balise et éventuellement une étendue. Pour un critère qui s'applique à des machines virtuelles, vous pouvez spécifier un nom qui commence par, est égal à ou contient une chaîne donnée.
- Un NSGroup dispose de membres directs et de membres effectifs. Les membres effectifs incluent des membres que vous spécifiez à l'aide de critères d'appartenance, ainsi que tous les membres directs et effectifs qui appartiennent aux membres de ce NSGroup. Par exemple, supposons que NSGroup-1 dispose du membre direct LogicalSwitch-1. Vous ajoutez NSGroup-2 et spécifiez NSGroup-1 et LogicalSwitch-2 comme membres. Maintenant, NSGroup-2 dispose des membres directs NSGroup-1 et LogicalSwitch-2, ainsi qu'un membre effectif, LogicalSwitch-1. Ensuite, vous ajoutez NSGroup-3 et spécifiez NSGroup-2 comme membre. Maintenant, NSGroup-3 dispose du membre direct NSGroup-2 et des membres effectifs LogicalSwitch-1 et LogicalSwitch-2.
- Un NSGroup peut disposer d'un maximum de 500 membres directs.
- La limite recommandée pour le nombre de membres effectifs dans un NSGroup est de 5 000. Dépasser cette limite n'affecte pas la fonctionnalité, mais peut avoir un impact négatif sur les performances. Sur NSX Manager, lorsque le nombre de membres effectifs d'un NSGroup dépasse 80 % de 5 000, le message d'avertissement `Le NSGroup xyz est sur le point de dépasser la limite de membres maximale. Le nombre total dans le NSGroup est de ...` s'affiche dans le fichier journal, et lorsque le nombre dépasse 5 000, le message d'avertissement `Le NSGroup`

xyz a atteint la limite de nombres maximale. Nombre total dans le NSGroup = ... s'affiche. Sur NSX Controller, lorsque le nombre de VIF/IP/MAC traduits dans un NSGroup dépasse 5 000, le message d'avertissement Le conteneur xyz a atteint la limite de traductions maximale d'IP/MAC/VIF. Nombre de traduction actuel dans le conteneur – IP :..., MAC :..., VIF :... s'affiche dans le fichier journal. NSX Manager et NSX Controller vérifient sur les NSGroups la limite deux fois par jour, à 7h et à 19h.

- Le nombre maximal pris en charge de machines virtuelles est de 10 000.

Pour tous les objets que vous pouvez ajouter à un NSGroup en tant que membres, c'est-à-dire des commutateurs logiques, des ports logiques, des ensembles d'IP, des ensembles MAC, des machines virtuelles et des NSGroups, vous pouvez accéder à l'écran pour n'importe lequel des objets et sélectionner **Éléments associés > NSGroups** pour voir tous les NSGroups qui ont directement ou indirectement cet objet comme membre. Par exemple, dans l'exemple ci-dessus, lorsque vous avez accédé à l'écran pour LogicalSwitch-1, la sélection de **Éléments associés > NSGroups** indique NSGroup-1, NSGroup-2 et NSGroup-3, car tous les trois ont LogicalSwitch-1 comme membre, directement ou indirectement.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Inventaire > Groupes** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Groupes** s'il n'est pas déjà sélectionné.
- 4 Cliquez sur **Ajouter**.
- 5 Entrez un nom pour le NSGroup.
- 6 (Facultatif) Entrez une description.
- 7 (Facultatif) Cliquez sur **Critères d'appartenance**.

Un critère peut s'appliquer à des commutateurs logiques, des ports logiques ou des machines virtuelles. Pour chaque critère, vous pouvez spécifier jusqu'à cinq règles qui sont combinées avec l'opérateur logique AND. Pour une règle qui s'applique à des commutateurs logiques ou des ports logiques, vous pouvez spécifier une balise et éventuellement une étendue. Pour une règle qui s'applique à des machines virtuelles, vous pouvez spécifier un nom qui commence par, est égal à ou contient une chaîne donnée.

Vous pouvez spécifier jusqu'à cinq critères qui sont combinés avec l'opérateur logique OR.

- 8 (Facultatif) Cliquez sur **Membres** pour sélectionner des membres.

Les types disponibles sont **Ensemble d'IP**, **Ensemble MAC**, **Commutateur logique**, **Port logique** et **NSGroup**.

- 9 Cliquez sur **Enregistrer**.

Configuration de services et de groupes de services

Vous pouvez configurer un NSService et spécifier des paramètres de correspondance du trafic réseau, tels qu'un couplage port/protocole. Vous pouvez également utiliser un NSService pour autoriser ou bloquer certains types de trafic dans les règles de pare-feu.

Un NSService peut être de l'un des types suivants :

- Ether
- IP
- IGMP
- ICMP
- ALG
- Ensemble de ports L4

Un ensemble de ports L4 prend en charge l'identification de ports source et de ports de destination. Vous pouvez spécifier des ports individuels ou une plage de ports, jusqu'à un maximum de 15 ports.

Un NSService peut également être un groupe d'autres NSServices. Un NSService qui est un groupe peut être de l'un des types suivants :

- Couche 2
- Couche 3 et au-dessus

Vous ne pouvez pas modifier le type après la création d'un NSService. Certains NSServices sont prédéfinis. Vous ne pouvez pas les modifier ou les supprimer.

Créer un NSService

Vous pouvez créer un NSService pour spécifier les caractéristiques que la correspondance de réseau utilise ou pour définir le type de trafic à bloquer ou à autoriser dans les règles de pare-feu.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur *https://<adresse-ip-nsx-manager>*.
- 2 Sélectionnez **Inventaire > Services** dans le panneau de navigation.
- 3 Cliquez sur **Ajouter**.
- 4 Entrez un nom.
- 5 (Facultatif) Entrez une description.
- 6 Sélectionnez **Spécifier un protocole** pour configurer un service individuel ou sélectionnez **Grouper des services existants** pour configurer un groupe de NSServices.
- 7 Pour un service individuel, sélectionnez un type et un protocole.

Les types disponibles sont **Ether**, **IP**, **IGMP**, **ICMP**, **ALG** et **Ensemble de ports L4**

- 8 Pour un groupe de services, sélectionnez un type et des membres pour le groupe.
Les types disponibles sont **Couche 2** et **Couche 3 et au-dessus**.
- 9 Cliquez sur **Enregistrer**.

Gérer les balises d'une machine virtuelle

Vous pouvez consulter la liste des machines virtuelles dans l'inventaire. Vous pouvez ajouter des balises à une machine virtuelle pour faciliter la recherche.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur *https://<adresse-ip-nsx-manager>*.
- 2 Sélectionnez **Inventaire > Machines virtuelles** dans le panneau de navigation.

La liste des machines virtuelles affiche 4 colonnes : Machine virtuelle, ID externe, Source et Balise. Vous pouvez cliquer sur l'icône de filtre dans l'en-tête des trois premières colonnes pour filtrer la liste. Entrez une chaîne de caractères pour une correspondance partielle. Si la chaîne dans la colonne contient la chaîne que vous avez entrée, l'entrée s'affiche. Entrez une chaîne de caractères placée entre guillemets doubles pour une correspondance exacte. Si la chaîne dans la colonne correspond exactement à la chaîne que vous avez entrée, l'entrée s'affiche.
- 3 Sélectionnez une machine virtuelle.
- 4 Cliquez sur **GÉRER LES BALISES**.
- 5 Ajoutez ou supprimez des balises.

Option	Action
Ajouter une balise	Cliquez sur AJOUTER pour spécifier une balise et éventuellement une étendue.
Supprimer une balise	Sélectionnez une balise existante et cliquez sur SUPPRIMER .

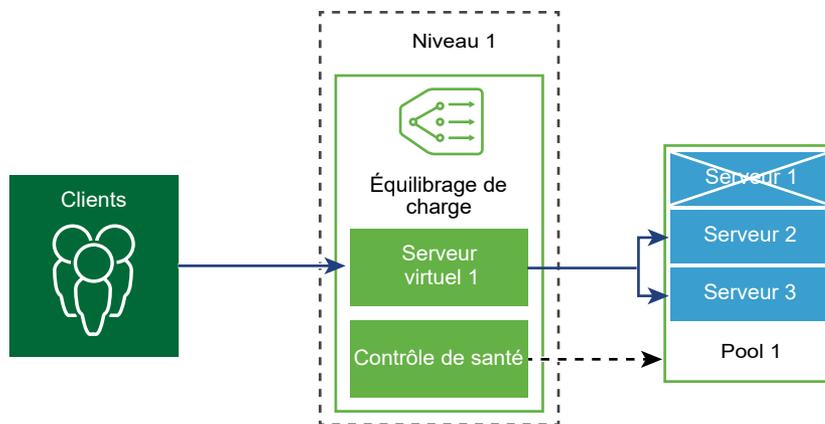
Une machine virtuelle peut contenir un maximum de 15 balises.

- 6 Cliquez sur **Enregistrer**.

Équilibrage de charge logique

10

L'équilibrage de charge logique NSX-T Data Center offre un service de haute disponibilité pour les applications et distribue la charge du trafic réseau entre plusieurs serveurs.



L'équilibrage de charge distribue les demandes de service entrantes uniformément entre plusieurs serveurs de telle sorte que la distribution de la charge est transparente pour les utilisateurs. Il contribue à obtenir une utilisation optimale des ressources, à optimiser le débit, à réduire les temps de réponse et à éviter la surcharge.

Vous pouvez mapper une adresse IP virtuelle à un ensemble de serveurs de pool pour l'équilibrage de charge. L'équilibrage de charge accepte les demandes TCP, UDP, HTTP ou HTTPS sur l'adresse IP virtuelle et décide du serveur de pool à utiliser.

En fonction des besoins de votre environnement, vous pouvez adapter les performances de l'équilibrage de charge en augmentant le nombre de serveurs virtuels et de membres du pool existants pour gérer un trafic réseau intense.

Note L'équilibrage de charge logique est uniquement pris en charge sur un routeur logique de niveau 1. Un seul équilibreur de charge peut être attaché par un routeur logique de niveau 1.

Ce chapitre contient les rubriques suivantes :

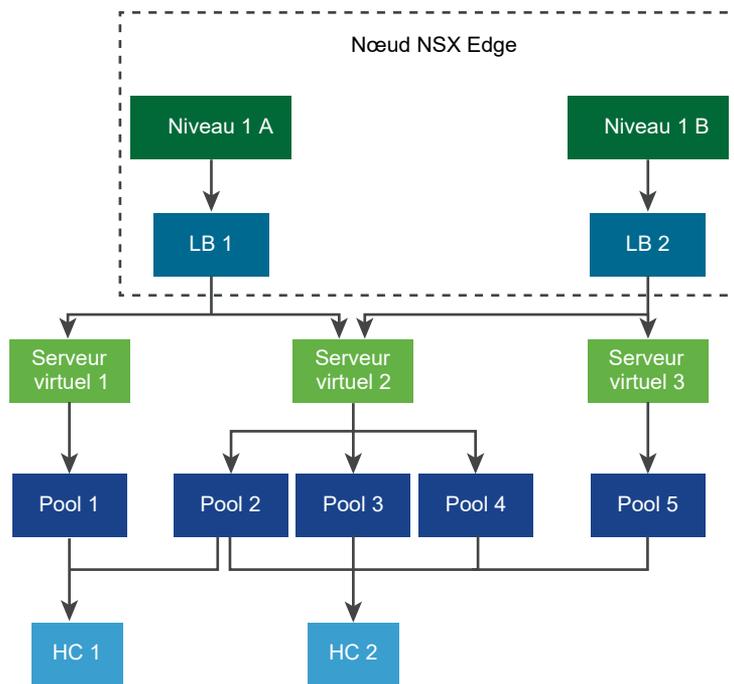
- [Concepts clés de l'équilibrage de charge](#)
- [Configuration des composants d'équilibrage de charge](#)

Concepts clés de l'équilibrage de charge

L'équilibrage de charge inclut des serveurs virtuels, des pools de serveurs et des moniteurs de contrôle de santé.

Un équilibrage de charge est connecté à un routeur logique de niveau 1. Il héberge un ou plusieurs serveurs virtuels. Un serveur virtuel est un résumé d'un service d'application, représenté par la combinaison unique d'une adresse IP, d'un port et d'un protocole. Le serveur virtuel est associé à un ou plusieurs pools de serveurs. Un pool de serveurs se compose d'un groupe de serveurs. Les pools de serveurs incluent des membres de pool de serveurs individuels.

Pour vérifier que chaque serveur exécute correctement l'application, vous pouvez ajouter des moniteurs de contrôle de santé qui vérifient l'état de santé d'un serveur.



Évolutivité des ressources d'équilibrage de charge

Les équilibres de charge sont disponibles en différentes tailles : petit, moyen et grand. En fonction de la taille de l'équilibrage de charge, celui-ci peut héberger différents serveurs virtuels et membres du pool.

Un équilibrage de charge est attaché à un routeur logique de niveau 1. Ce routeur logique de niveau 1 est hébergé sur les nœuds NSX Edge. NSX Edge comprend des dispositifs de VM de différents facteurs de forme : bare metal, petit, moyen et grand. Selon le format, le nœud NSX Edge peut héberger un nombre différent d'équilibres de charge.

Tableau 10-1. Échelle d'équilibrage de charge pour le service d'équilibrage de charge

Service d'équilibrage de charge	Petit équilibrage de charge	Équilibrage de charge moyen	Grand équilibrage de charge
Nombre de serveurs virtuels par équilibrage de charge	10	100	1 000
Nombre de pools par équilibrage de charge	20	200	2 000
Nombre de membres du pool par équilibrage de charge	200	2 000	10 000

Tableau 10-2. Échelle d'équilibrage de charge pour le nœud NSX Edge

Équilibrage de charge par nœud NSX Edge	Petit équilibrage de charge	Équilibrage de charge moyen	Grand équilibrage de charge	Nombre maximal de membres du pool
VM de NSX Edge - petite	S/O	S/O	S/O	S/O
VM de NSX Edge - moyenne	1	S/O	S/O	200
VM de NSX Edge - grande	40	4	S/O	5 000
VM de NSX Edge - bare metal	750	75	7	20 000

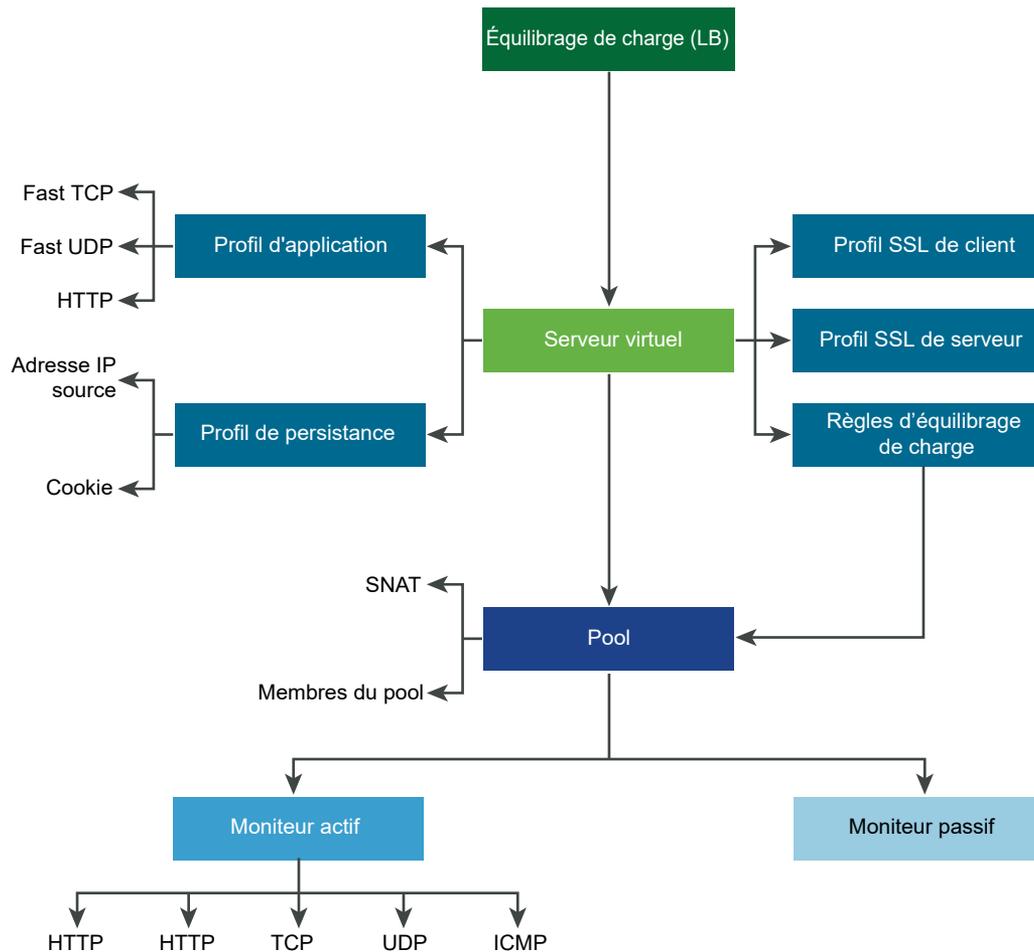
Fonctionnalités d'équilibrage de charge prises en charge

L'équilibrage de charge NSX-T Data Center prend en charge les fonctionnalités suivantes.

- Couche 4 : TCP et UDP
- Couche 7 : HTTP et HTTPS avec prise en charge des règles d'équilibrage de charge
- Pools de serveurs : statiques et dynamiques avec NSGroup
- Persistance : mode de persistance de l'adresse IP source et des cookies
- Moniteurs de contrôle de santé : moniteur actif (HTTP, HTTPS, TCP, UDP et ICMP) et moniteur passif
- SNAT : transparent, routage automatique et liste des adresses IP
- Mise à niveau HTTP - pour les applications qui utilisent la mise à niveau HTTP telles que WebSocket, les demandes de mise à niveau HTTP prise en charge du client ou du serveur. Par défaut, NSX-T Data Center prend en charge et accepte les demandes de mise à niveau HTTPS du client à l'aide du profil d'application HTTP.

Pour détecter une communication client ou serveur inactive, l'équilibrage de charge utilise la fonctionnalité de délai d'attente de réponse du profil d'application HTTP définie sur 60 secondes. Si le serveur n'envoie pas de trafic pendant l'intervalle de 60 secondes, NSX-T Data Center met fin à la connexion côté client et serveur.

Remarque : le mode d'arrêt SSL et le mode proxy SSL ne sont pas pris en charge dans la version Limited Export de NSX-T Data Center 2.2.

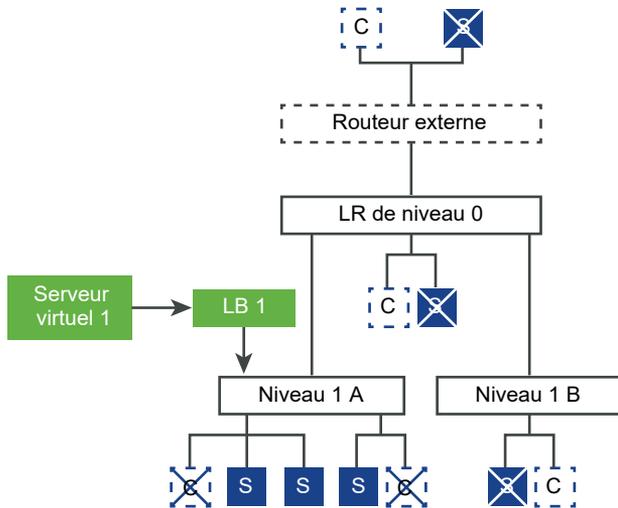


Topologies d'équilibrage de charge

Les équilibres de charge sont généralement déployés en mode en ligne ou en mode manchot.

Topologie en ligne

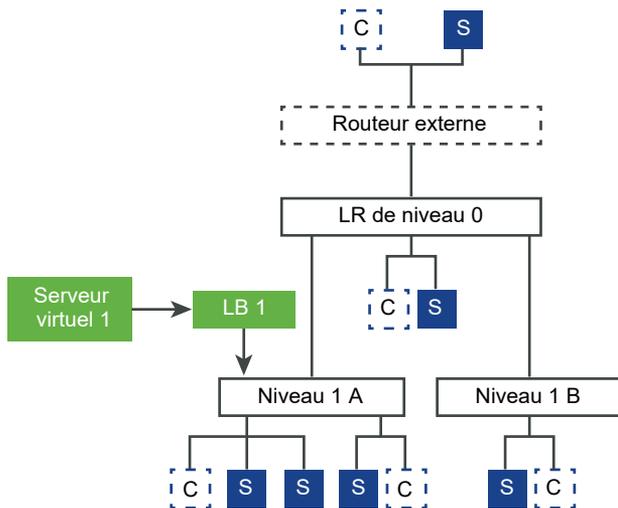
Dans le mode en ligne, l'équilibrage de charge se trouve sur le chemin du trafic entre le client et le serveur. Les clients et les serveurs ne doivent pas être connectés au même routeur logique de niveau 1. Cette topologie ne nécessite pas de serveur virtuel SNAT.



Topologie manchot

Dans le mode manchot, l'équilibrage de charge ne se trouve pas sur le chemin du trafic entre le client et le serveur. Dans ce mode, le client et le serveur peuvent être à n'importe quel emplacement. L'équilibrage de charge utilise un NAT source (SNAT) pour forcer le trafic de retour du serveur destiné au client à passer par l'équilibrage de charge. Dans cette topologie, un serveur virtuel SNAT doit être activé.

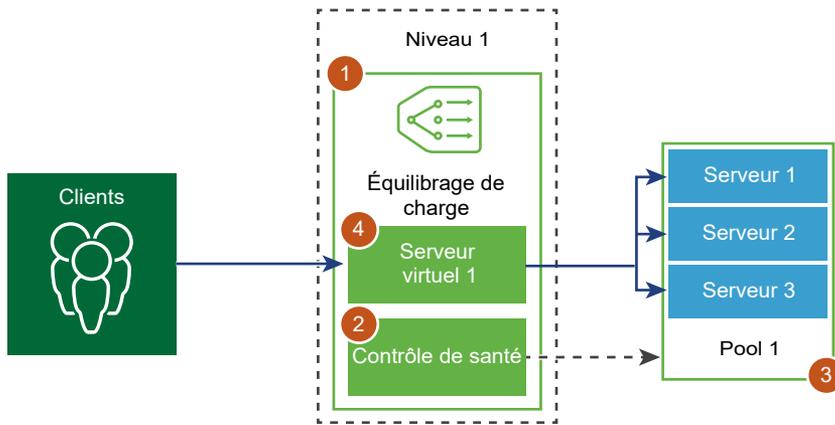
Lorsque l'équilibrage de charge reçoit le trafic client vers l'adresse IP virtuelle, l'équilibrage de charge sélectionne un membre du pool de serveurs et y achemine le trafic client. En mode manchot, l'équilibrage de charge remplace l'adresse IP du client par l'adresse IP de l'équilibrage de charge afin que la réponse du serveur soit toujours envoyée à l'équilibrage de charge et que celui-ci transmette la réponse au client.



Configuration des composants d'équilibrage de charge

Pour utiliser des équilibrages de charge logiques, vous devez commencer par configurer un équilibrage de charge et l'attacher à un routeur logique de niveau 1.

Vous pouvez ensuite configurer le contrôle de santé de vos serveurs, puis configurer des pools de serveurs pour l'équilibrage de charge. Enfin, vous devez créer un serveur virtuel de couche 4 ou de couche 7 pour l'équilibrage de charge.

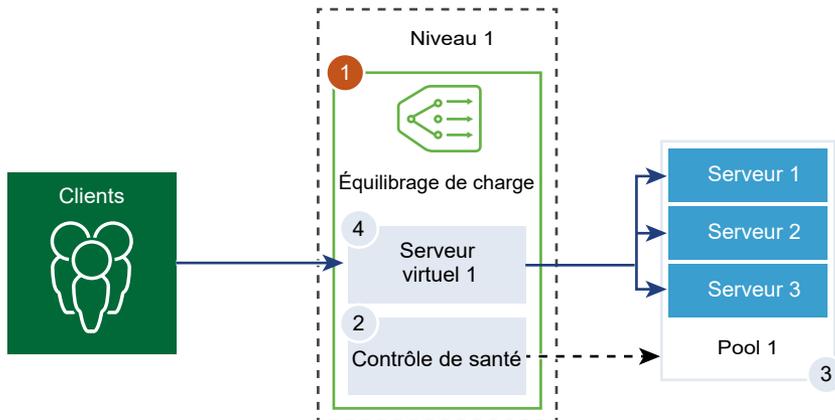


Créer un équilibrage de charge

Un équilibrage de charge est créé et attaché au routeur logique de niveau 1.

Vous pouvez configurer le niveau des messages d'erreur que vous souhaitez que l'équilibrage de charge ajoute au journal des erreurs.

Note Évitez de définir le niveau de journalisation sur DÉBOGAGE sur les équilibrages de charge avec un trafic significatif, car le grand nombre de messages enregistrés dans le journal peut affecter les performances.



Conditions préalables

Vérifiez qu'un routeur logique de niveau 1 est configuré. Reportez-vous à la section [Créer un routeur logique de niveau 1](#) .

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Équilibrage de charge > Ajouter**.
- 3 Entrez un nom et une description pour l'équilibrage de charge.
- 4 Sélectionnez la taille du serveur virtuel d'équilibrage de charge et le nombre de membres du pool en fonction des ressources disponibles.
- 5 Définissez le niveau de gravité du journal d'erreur dans le menu déroulant.

L'équilibrage de charge collecte des informations sur les problèmes de différents niveaux de gravité rencontrés dans le journal d'erreur.

- 6 Cliquez sur **OK**.
- 7 Associez l'équilibrage de charge créé à un serveur virtuel.
 - a Sélectionnez l'équilibrage de charge et cliquez sur **Actions > Attacher à un serveur virtuel**.
 - b Sélectionnez un serveur virtuel existant dans le menu déroulant.
 - c Cliquez sur **OK**.
- 8 Attachez l'équilibrage de charge créé à un routeur logique de niveau 1.
 - a Sélectionnez l'équilibrage de charge et cliquez sur **Actions > Attacher à un routeur logique**.
 - b Sélectionnez un routeur logique de niveau 1 existant dans le menu déroulant.

Le routeur de niveau 1 doit être en mode Actif-En veille.

- c Cliquez sur **OK**.

- 9 (Facultatif) Supprimez l'équilibrage de charge.

Si vous ne souhaitez plus utiliser l'équilibrage de charge, vous devez d'abord le détacher du serveur virtuel et du routeur logique de niveau 1.

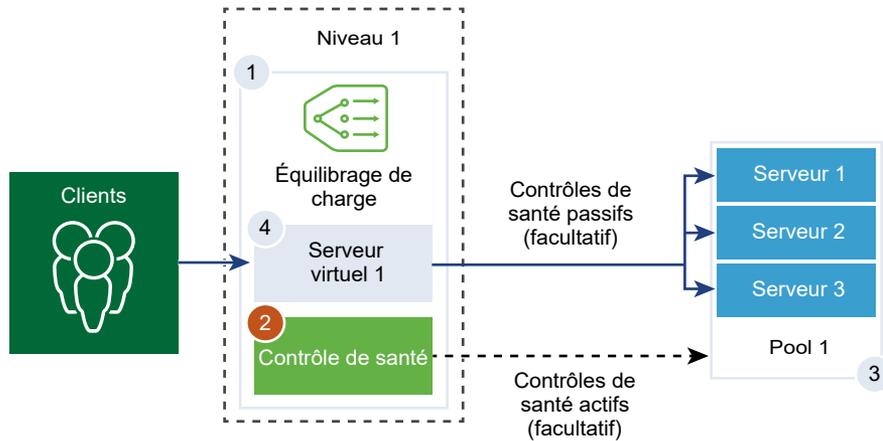
Configurer un moniteur de santé actif

Le moniteur de santé actif est utilisé pour tester la disponibilité d'un serveur. Pour cela, il utilise plusieurs types de tests, notamment l'envoi d'une commande ping aux serveurs ou de demandes HTTP avancées pour surveiller la santé de l'application.

Les serveurs qui ne répondent pas après un certain temps ou qui répondent avec des erreurs, sont exclus des futures connexions jusqu'à ce qu'un contrôle de santé périodique ultérieur détermine que ces serveurs sont sains.

Les contrôles de santé actifs sont effectués sur les membres du pool de serveurs une fois que le membre du pool est associé à un serveur virtuel et que le serveur virtuel est attaché à un routeur logique de niveau 1. L'adresse IP de liaison montante de niveau 1 est utilisée pour le contrôle de santé.

Note Un moniteur de santé actif peut être configuré par pool de serveurs.



Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
 - 2 Sélectionnez **Équilibrage de charge > Mise en réseau > Moniteurs > Moniteurs de santé actifs > Ajouter**.
 - 3 Entrez un nom et une description pour le moniteur de santé actif.
 - 4 Sélectionnez un protocole de contrôle de santé pour le serveur dans le menu déroulant.
- Vous pouvez également utiliser des protocoles prédéfinis dans NSX Manager ; http-monitor, https-monitor, Icmp-monitor, Tcp-monitor et Udp-monitor.
- 5 Définissez la valeur du port de surveillance.
 - 6 Configurez les valeurs pour surveiller un pool de services.

Vous pouvez également accepter les valeurs de contrôle de santé actif par défaut.

Option	Description
Intervalle de surveillance	Définissez le délai en secondes après lequel le moniteur envoie une autre demande de connexion au serveur.
Nombre d'échecs	Définissez le nombre d'échecs consécutifs avant que le serveur ne soit considéré comme temporairement indisponible.
Nombre de reconnections	Définissez un délai d'expiration après lequel une nouvelle tentative de connexion au serveur est effectuée afin de déterminer s'il est disponible.
Délai d'expiration	Définissez le nombre de fois que le serveur est testé avant qu'il ne soit considéré comme INACTIF.

Par exemple, si l'intervalle de surveillance est défini sur 5 secondes et le délai d'expiration sur 15 secondes, l'équilibrage de charge envoie des demandes au serveur toutes les 5 secondes. À chaque interrogation, si la réponse attendue est reçue du serveur sous 15 secondes, le contrôle de santé est OK. Dans le cas contraire, le résultat est CRITIQUE. Si les trois récents résultats de contrôle de santé sont tous ACTIF, le serveur est considéré comme ACTIF.

- 7 Si vous sélectionnez HTTP en tant que protocole de contrôle de santé, renseignez les détails suivants.

Option	Description
Méthode HTTP	Sélectionnez la méthode de détection de l'état du serveur dans le menu déroulant : GET, OPTIONS, POST, HEAD et PUT.
URL de demande HTTP	Entrez l'URI de la demande pour la méthode.
Version de la demande HTTP	Sélectionnez la version de la demande prise en charge dans le menu déroulant. Vous pouvez également accepter la version par défaut, HTTP_VERSION_1_1.
Corps de la demande HTTP	Entrez le corps de la demande. Valide pour les méthodes POST et PUT.
Code de réponse HTTP	Entrez la chaîne à laquelle le moniteur doit correspondre dans la ligne d'état du corps de la réponse HTTP. Le code de réponse est une liste de valeurs séparées par des virgules. Par exemple, 200,301,302,401.
Corps de la réponse HTTP	Si la chaîne du corps de la réponse HTTP et le corps de la réponse du contrôle de santé HTTP correspondent, le serveur est considéré comme sain.

- 8 Si vous sélectionnez HTTPS en tant que protocole de contrôle de santé, renseignez les détails suivants.

- a Sélectionnez la liste de protocoles SSL.

Les versions TLS 1.1 et TLS 1.2 sont prises en charge et activées par défaut. TLS 1.0 est pris en charge, mais désactivé par défaut.

- b Cliquez sur la flèche et déplacez les protocoles dans la section des éléments sélectionnés.

- c Attribuez un chiffrement SSL par défaut ou créez un chiffrement SSL personnalisé.
- d Renseignez les détails suivants pour le protocole HTTP en tant que protocole de contrôle de santé.

Option	Description
Méthode HTTP	Sélectionnez la méthode de détection de l'état du serveur dans le menu déroulant : GET, OPTIONS, POST, HEAD et PUT.
URL de demande HTTP	Entrez l'URI de la demande pour la méthode.
Version de la demande HTTP	Sélectionnez la version de la demande prise en charge dans le menu déroulant. Vous pouvez également accepter la version par défaut, HTTP_VERSION_1_1.
Corps de la demande HTTP	Entrez le corps de la demande. Valide pour les méthodes POST et PUT.
Code de réponse HTTP	Entrez la chaîne à laquelle le moniteur doit correspondre dans la ligne d'état du corps de la réponse HTTP. Le code de réponse est une liste de valeurs séparées par des virgules. Par exemple, 200,301,302,401.
Corps de la réponse HTTP	Si la chaîne du corps de la réponse HTTP et le corps de la réponse du contrôle de santé HTTP correspondent, le serveur est considéré comme sain.

- 9 Si vous sélectionnez ICMP en tant que protocole de contrôle de santé, entrez la taille des données du paquet de contrôle de santé ICMP en octets.
- 10 Si vous sélectionnez TCP en tant que protocole de contrôle de santé, vous pouvez laisser les paramètres vides.

Si le protocole d'envoi et le protocole de réception ne sont pas répertoriés, une connexion TCP d'établissement de liaison tridirectionnelle est établie pour valider la santé du serveur. Aucune donnée n'est envoyée. Si un protocole figure dans la liste, les données attendues doivent se présenter sous la forme d'une chaîne et peuvent se situer n'importe où dans la réponse. Les expressions régulières ne sont pas prises en charge.

- 11 Si vous sélectionnez UDP en tant que protocole de contrôle de santé, renseignez les détails suivants.

Option requise	Description
Données UDP envoyées	Entrez la chaîne à envoyer à un serveur une fois la connexion établie.
Données UDP attendues	Entrez la chaîne devant être reçue du serveur. Le serveur est considéré comme actif uniquement lorsque la chaîne reçue correspond à cette définition.

- 12 Cliquez sur **Terminer**.

Étape suivante

Associez le moniteur de santé actif à un pool de serveurs. Reportez-vous à la section [Ajouter un pool de serveurs pour l'équilibrage de charge](#).

Configurer les moniteurs de santé passifs

Les équilibrages de charge effectuent des contrôles de santé passifs pour surveiller les échecs des connexions client et marquer les serveurs à l'origine d'échecs réguliers comme étant INACTIF.

Un contrôle de santé passif surveille le trafic client sur l'équilibrage de charge et identifie les échecs. Par exemple, si un membre du pool envoie une réinitialisation TCP (RST) en réponse à une connexion client, l'équilibrage de charge détecte cet échec. Si plusieurs échecs consécutifs se produisent, l'équilibrage de charge considère que ce membre du pool de serveurs n'est temporairement pas disponible et arrête de lui envoyer des demandes de connexion pendant un certain temps. Après une certaine période, l'équilibrage de charge envoie une demande de connexion pour vérifier si le membre du pool a récupéré. Si la connexion réussie, le membre du pool est alors considéré comme sain. Dans le cas contraire, l'équilibrage de charge attend pendant un certain temps avant de réessayer.

Le contrôle de santé passif considère les scénarios suivants comme des échecs du trafic client :

- En cas d'échec de la connexion à un membre du pool de serveurs associés aux serveurs virtuels de couche 7. Par exemple, lorsque l'équilibrage de charge tente de se connecter ou d'effectuer un établissement de liaison SSL et que le membre du pool échoue, ce dernier envoie une demande RST TCP.
- Pour les pools de serveurs associés aux serveurs virtuels TCP de couche 4, si le membre du pool envoie un message RST TCP en réponse à une demande SYN TCP du client ou ne répond pas du tout.
- Pour les pools de serveurs associés aux serveurs virtuels UDP de couche 4, si un port n'est pas accessible ou un message d'erreur ICMP indiquant que la destination est inaccessible est reçu en réponse à un paquet UDP client.

Pour les pools de serveurs associés aux serveurs virtuels de couche 7, le nombre d'échecs de connexion est incrémenté lorsque des erreurs de connexion TCP se produisent (par exemple, échec RST TCP de l'envoi des données ou échecs d'établissement de liaison SSL).

Pour les pools de serveurs associés aux serveurs virtuels de couche 4, si aucune réponse à un message SYN TCP envoyé au membre du pool de serveurs de couche 4 n'est reçue ou si un message RST TCP est reçu en réponse à une demande SYN TCP, le membre du pool de serveurs est considéré comme INACTIF. Le nombre d'échecs est incrémenté.

Pour les serveurs virtuels UDP de couche 4, si une erreur ICMP (par exemple, port ou destination inaccessible) est reçue en réponse au trafic client, le serveur est considéré comme INACTIF.

Note Un moniteur de santé passif peut être configuré pour chaque pool de serveurs.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Équilibrage de charge > Moniteurs > Moniteurs de santé actifs > Ajouter**.

- 3 Entrez un nom et une description pour le moniteur de santé passif.
- 4 Configurez les valeurs pour surveiller un pool de services.

Vous pouvez également accepter les valeurs de contrôle de santé actif par défaut.

Option	Description
Nombre d'échecs	Définissez le nombre d'échecs consécutifs avant que le serveur ne soit considéré comme temporairement indisponible.
Délai d'expiration	Définissez le nombre de fois que le serveur est testé avant qu'il ne soit considéré comme INACTIF.

Par exemple, lorsque les échecs consécutifs atteignent la valeur configurée de 5, le membre est considéré comme temporairement indisponible pendant 5 secondes. Après cette période, une nouvelle connexion est tentée afin de déterminer s'il est disponible. Si la connexion est établie, le membre est considéré comme disponible et le nombre d'échecs est défini sur zéro. Toutefois, si la connexion échoue, il n'est pas utilisé pendant un autre intervalle de 5 secondes.

- 5 Cliquez sur **OK**.

Étape suivante

Associez le moniteur de santé passif à un pool de serveurs. Reportez-vous à la section [Ajouter un pool de serveurs pour l'équilibrage de charge](#).

Ajouter un pool de serveurs pour l'équilibrage de charge

Un pool de serveurs est constitué d'un ou de plusieurs serveurs configurés qui exécutent la même application. Un seul pool peut être associé à des serveurs virtuels de couche 4 et de couche 7.

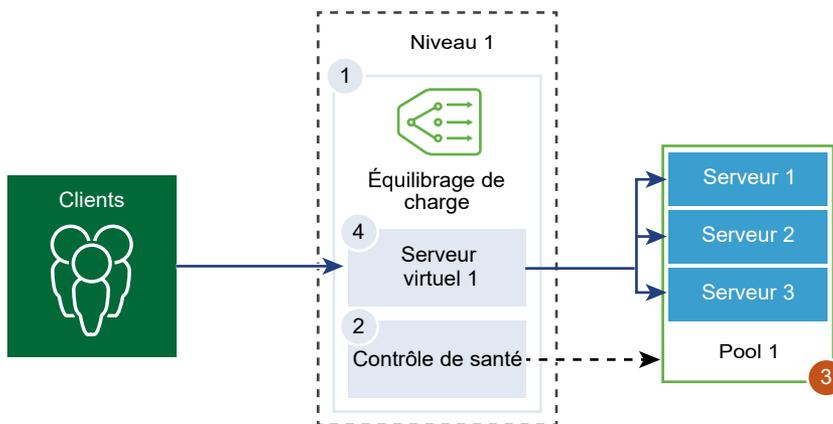
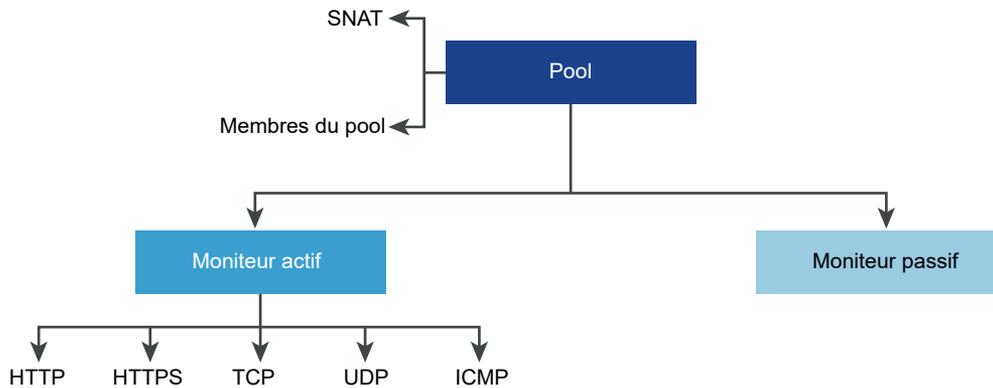


Figure 10-1. Configuration des paramètres du pool de serveurs**Conditions préalables**

- Si vous utilisez des membres de pool dynamique, vous devez configurer un NSGroup. Reportez-vous à la section [Créer un NSGroup](#).
- En fonction de la surveillance utilisée, vérifiez que des moniteurs de santé actifs ou passifs sont configurés. Reportez-vous à la section [Configurer un moniteur de santé actif](#) ou [Configurer les moniteurs de santé passifs](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Équilibrage de charge > Pools de serveurs > Ajouter**.
- 3 Entrez un nom et une description pour le pool d'équilibrage de charge.
Vous pouvez éventuellement décrire les connexions gérées par le pool de serveurs.
- 4 Sélectionnez un algorithme d'équilibrage pour le pool de serveurs.

L'algorithme d'équilibrage de charge contrôle la manière dont les connexions entrantes sont distribuées sur les membres. Il peut être utilisé sur un pool de serveurs ou directement sur un serveur.

Tous les algorithmes d'équilibrage de charge ignorent les serveurs qui remplissent l'une des conditions suivantes :

- L'état d'administration est défini sur DISABLED.
- L'état d'administration est défini sur GRACEFUL_DISABLED et aucune entrée de persistance ne correspond.
- L'état de contrôle de santé actif ou passif est INACTIF.

- La limite maximale de connexions simultanées pour le pool de serveurs a été atteinte.

Option	Description
ROUND_ROBIN	<p>Les demandes entrantes des clients sont analysées en fonction d'une liste de serveurs disponibles capables de les traiter.</p> <p>Les pondérations des membres du pool de serveurs sont ignorées, même si elles sont configurées.</p>
WEIGHTED_ROUND_ROBIN	<p>Une pondération qui qualifie les performances d'un serveur par rapport aux autres serveurs du pool, est attribuée à chaque serveur. Cette valeur détermine le nombre de demandes client envoyées à un serveur par rapport aux autres serveurs du pool.</p> <p>L'algorithme d'équilibrage de charge est conçu pour répartir équitablement la charge entre les ressources de serveur disponibles.</p>
LEAST_CONNECTION	<p>Diffuse les requêtes client à plusieurs serveurs en se basant sur le nombre de connexions déjà sur le serveur.</p> <p>Les nouvelles connexions sont envoyées au serveur avec les connexions les moins nombreuses. Les pondérations des membres du pool de serveurs sont ignorées, même si elles sont configurées.</p>
WEIGHTED_LEAST_CONNECTION	<p>Une pondération qui qualifie les performances d'un serveur par rapport aux autres serveurs du pool, est attribuée à chaque serveur. Cette valeur détermine le nombre de demandes client envoyées à un serveur par rapport aux autres serveurs du pool.</p> <p>Cet algorithme d'équilibrage de charge se concentre sur l'utilisation de la valeur pondérée pour distribuer équitablement la charge sur les ressources disponibles du serveur.</p> <p>Par défaut, la pondération est 1 si la valeur n'est pas configurée et si le démarrage lent est activé.</p>
IP-HASH	<p>Sélectionne un serveur en fonction d'un hachage de l'adresse IP source et du poids total des serveurs en cours d'exécution.</p>

- 5 Faites basculer le bouton Multiplexage TCP pour activer cet élément de menu.

Le multiplexage TCP vous permet d'utiliser la même connexion TCP entre un équilibrage de charge et le serveur pour l'envoi de plusieurs demandes client à partir de différentes connexions TCP client.

- 6 Définissez le nombre maximal de connexions de multiplexage TCP par pool qui sont conservées pour l'envoi de demandes client ultérieures.

7 Sélectionnez le mode NAT source (SNAT).

Selon la topologie, le mode SNAT peut être nécessaire pour que l'équilibrage de charge reçoive le trafic du serveur destiné au client. Ce mode peut être activé pour chaque pool de serveurs.

Mode	Description
Mode transparent	L'équilibrage de charge utilise l'adresse IP du client et l'usurpation de port lors de l'établissement des connexions aux serveurs. Le mode SNAT n'est pas requis.
Mode de mappage automatique	L'équilibrage de charge utilise l'adresse IP de l'interface et un port éphémère pour continuer la communication avec un client initialement connecté à l'un des ports d'écoute établis du serveur. Le mode SNAT est requis. Activez la surcharge de port pour permettre l'utilisation de la même adresse IP et du même port SNAT pour les connexions multiples si le tuple (adresse IP source, port source, adresse IP de destination, port de destination et protocole IP) est unique une fois le processus SNAT effectué. Vous pouvez également définir le facteur de surcharge de port pour permettre le nombre maximal d'utilisations simultanées d'un port pour les connexions multiples.
Mode de liste des adresses IP	Spécifiez une plage d'adresses IP unique, par exemple, 1.1.1.1-1.1.1.10 pour le mode SNAT lors de la connexion aux serveurs du pool. Par défaut, la plage de ports de 4 000 à 64 000 est utilisée pour toutes les adresses IP SNAT configurées. La plage de ports de 1 000 à 4 000 est réservée à différentes fins, notamment pour les contrôles de santé et les connexions initiées à partir d'applications Linux. Si plusieurs adresses IP sont présentes, elles sont sélectionnées selon la méthode de répétition alternée. Activez la surcharge de port pour permettre l'utilisation de la même adresse IP et du même port SNAT pour les connexions multiples si le tuple (adresse IP source, port source, adresse IP de destination, port de destination et protocole IP) est unique une fois le processus SNAT effectué. Vous pouvez également définir le facteur de surcharge de port pour permettre le nombre maximal d'utilisations simultanées d'un port pour les connexions multiples.

8 Sélectionnez les membres du pool de serveurs.

Un pool de serveurs est constitué d'un ou de plusieurs membres du pool. Chaque membre du pool a une adresse IP et un port.

Chaque membre du pool de serveurs peut être configuré avec une pondération pour une utilisation dans l'algorithme d'équilibrage de charge. Cette pondération indique la charge plus ou moins importante qu'un membre de pool donné peut gérer par rapport aux autres membres du pool.

La désignation d'un membre du pool comme membre de sauvegarde fonctionne avec le moniteur de santé pour fournir un état actif/en veille. Le basculement du trafic se produit pour les membres de sauvegarde si les membres actifs ne réussissent pas un contrôle de santé.

Option	Description
Statique	Cliquez sur Ajouter pour inclure un membre de pool statique. Vous pouvez également cloner un membre de pool statique existant.
Dynamique	Sélectionnez le NSGroup dans le menu déroulant. Les critères d'appartenance au pool de serveurs sont définis dans le groupe. Vous pouvez éventuellement définir la liste d'adresses IP maximales du groupe.

- 9 Entrez le nombre minimal de membres actifs que le pool de serveurs doit toujours comprendre.
- 10 Sélectionnez un moniteur de santé actif et passif pour le pool de serveurs dans le menu déroulant.
- 11 Cliquez sur **Terminer**.

Configuration des composants de serveur virtuel

Les serveurs virtuels comprennent plusieurs composants que vous pouvez configurer, notamment les profils d'application, les profils persistants et les règles d'équilibrage de charge.

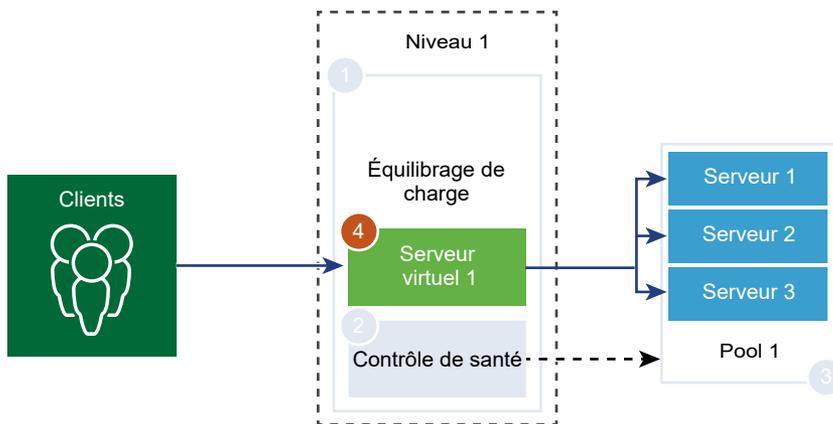
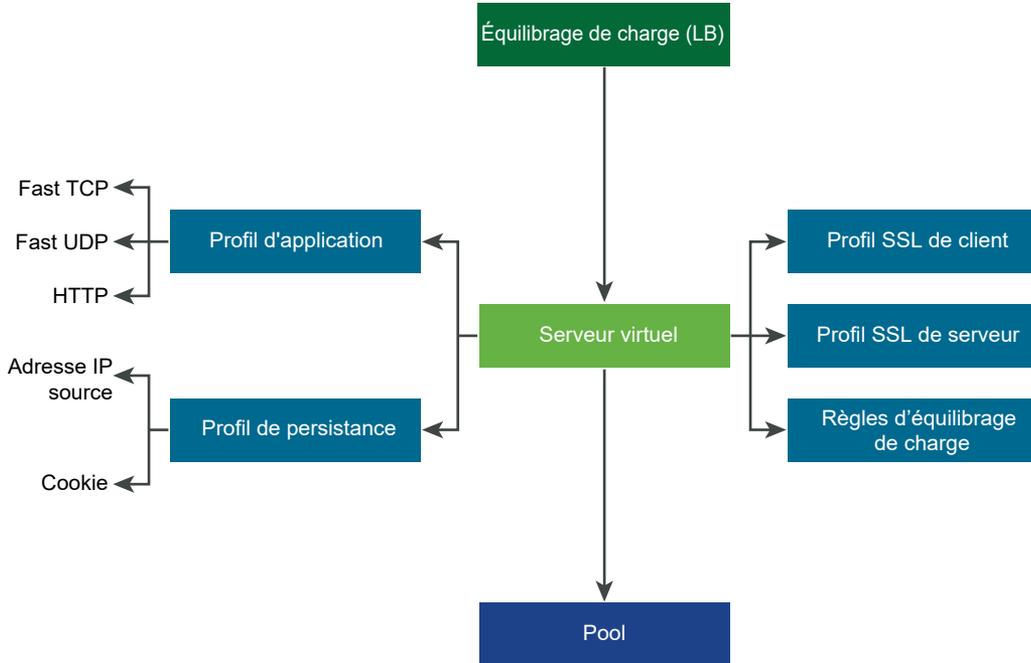


Figure 10-2. Composants de serveur virtuel



Configurer des profils d'application

Les profils d'application sont associés à des serveurs virtuels afin d'améliorer le trafic réseau d'équilibrage de charge et de simplifier les tâches de gestion du trafic.

Les profils d'application définissent le comportement d'un type particulier de trafic réseau. Le serveur virtuel associé traite le trafic réseau conformément aux valeurs spécifiées dans un profil d'application. Les profils d'application pris en charge sont TCP rapide, UDP rapide et HTTP.

Le profil d'application TCP est utilisé par défaut lorsqu'aucun profil d'application n'est associé à un serveur virtuel. Les profils d'application TCP et UDP sont utilisés lorsqu'une application s'exécute sur un protocole TCP ou UDP, et ne nécessite aucun équilibrage de charge au niveau de l'application (par exemple, un équilibrage de charge d'URL HTTP). Ces profils sont également utilisés lorsque vous souhaitez uniquement appliquer un équilibrage de charge de couche 4, qui fournit de meilleures performances et prend en charge la mise en miroir de la connexion.

Le profil d'application HTTP est utilisé pour les applications HTTP et HTTPS lorsque l'équilibrage de charge doit effectuer des actions basées sur la couche 7, telles que l'équilibrage de charge de toutes les demandes d'images envoyées à un membre du pool de serveurs spécifique ou l'arrêt d'une connexion HTTPS pour décharger les connexions SSL des membres du pool. Contrairement au profil d'application TCP, le profil d'application HTTP met fin à la connexion TCP client avant la sélection du membre du pool de serveurs.

Figure 10-3. Profil d'application TCP et UDP de couche 4

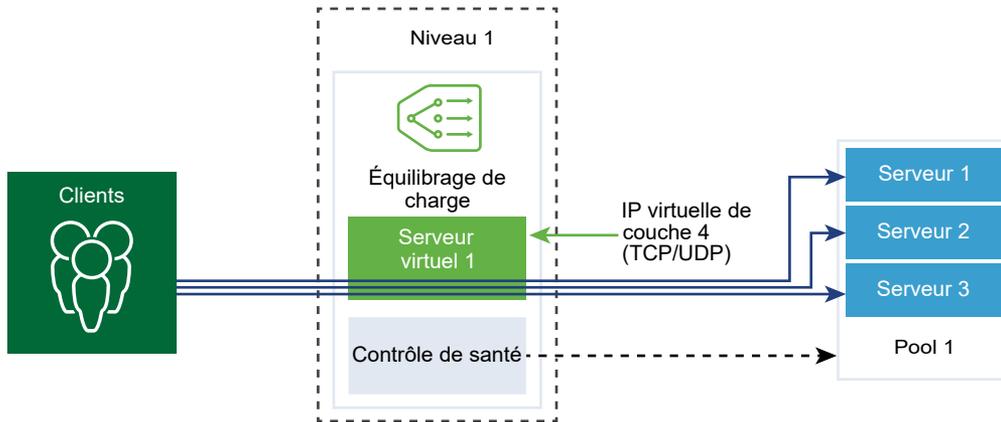
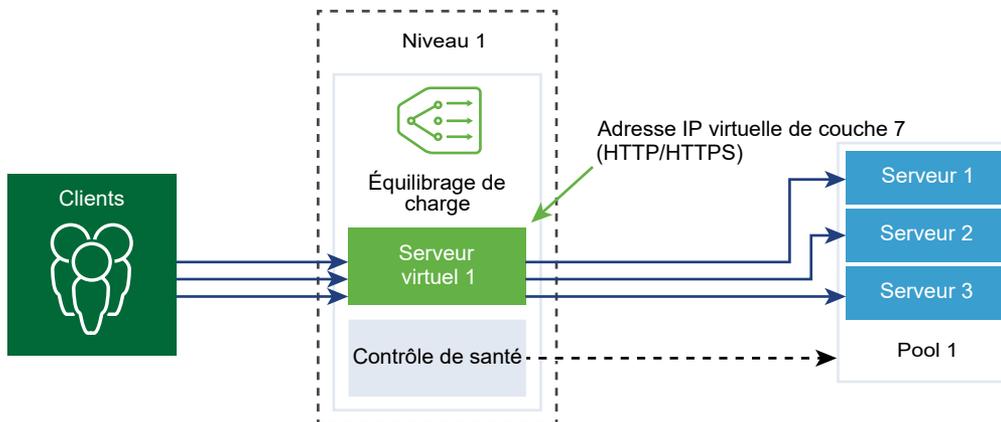


Figure 10-4. Profil d'application HTTPS de couche 7



Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Mise en réseau > Équilibrage de charge > Profils > Profils d'application**.
- 3 Créez un profil d'application TCP rapide.
 - a Sélectionnez **Ajouter > Profil TCP rapide** dans le menu déroulant.
 - b Entrez un nom et une description pour le profil d'application TCP rapide.

- c Renseignez les détails du profil d'application.

Vous pouvez également accepter les paramètres du profil TCP rapide par défaut.

Option	Description
Délai d'inactivité de la connexion	Entrez la durée en secondes pendant laquelle le serveur peut rester inactif après l'établissement d'une connexion TCP. Définissez un délai qui comprend le délai d'inactivité de l'application plus quelques secondes afin que l'application puisse fermer les connexions avant que l'équilibrage de charge ne le fasse.
Délai de fermeture de la connexion	Entrez la durée en secondes pendant laquelle les FIN ou RST de la connexion TCP doivent être conservés pour une application avant la fermeture de la connexion. Définissez un délai de fermeture court pour permettre des vitesses de connexion rapides.
Mise en miroir de flux HA	Faites basculer ce bouton pour mettre en miroir tous les flux du serveur virtuel associé sur le nœud de secours HA.

- d Cliquez sur **OK**.

4 Créez un profil d'application UDP rapide.

Vous pouvez également accepter les paramètres du profil UDP par défaut.

- a Sélectionnez **Ajouter > Profil UDP rapide** dans le menu déroulant.
- b Entrez un nom et une description pour le profil d'application UDP rapide.
- c Renseignez les détails du profil d'application.

Option	Description
Délai d'inactivité	Entrez la durée en secondes pendant laquelle le serveur peut rester inactif après l'établissement d'une connexion UDP. UDP est un protocole sans connexion. Dans le cadre de l'équilibrage de charge, tous les paquets UDP avec la même signature de flux, c'est-à-dire avec les mêmes adresses IP ou ports source et de destination, et le protocole IP reçus pendant la période d'inactivité, sont considérés comme appartenant à la même connexion et envoyés vers le même serveur. Si aucun paquet n'est reçu pendant la période d'inactivité, la connexion, qui est une association entre la signature de flux et le serveur sélectionné, est fermée.
Mise en miroir de flux HA	Faites basculer ce bouton pour mettre en miroir tous les flux du serveur virtuel associé sur le nœud de secours HA.

- d Cliquez sur **OK**.

5 Créez un profil d'application HTTP.

Vous pouvez également accepter les paramètres du profil HTTP par défaut.

Le profil d'application HTTP est utilisé pour les applications HTTP et HTTPS.

- a Sélectionnez **Ajouter > Profil HTTP rapide** dans le menu déroulant.
- b Entrez un nom et une description pour le profil d'application HTTP.

c Renseignez les détails du profil d'application.

Option	Description
<p>Redirection</p>	<ul style="list-style-type: none"> ■ Aucun : si un site Web est temporairement hors service, l'utilisateur reçoit un message d'erreur indiquant que la page est introuvable. ■ Redirection HTTP : si un site Web est temporairement hors service ou a été déplacé, les demandes entrantes pour le serveur virtuel peuvent être redirigées temporairement vers l'URL spécifiée par cette option. Une seule redirection statique est prise en charge. <p>Par exemple, si la redirection HTTP est définie sur <code>http://sitedown.abc.com/sorry.html</code> et qu'une demande <code>http://original_app.site.com/home.html</code> ou <code>http://original_app.site.com/somepage.html</code> est effectuée, celle-ci est redirigée vers l'URL spécifiée lorsque le site Web d'origine est hors service.</p> <ul style="list-style-type: none"> ■ Redirection HTTP vers HTTPS : certaines applications sécurisées peuvent appliquer une connexion SSL, mais au lieu de refuser les connexions non-SSL, elles peuvent rediriger la demande client afin d'utiliser une connexion SSL. La redirection HTTP vers HTTPS vous permet de conserver les chemins d'hôte et d'URI, et de rediriger la demande client afin d'utiliser une connexion SSL. <p>Pour la redirection HTTP vers HTTPS, le serveur virtuel HTTPS doit avoir le port 443 et la même adresse IP de serveur virtuel doit être configurée sur le même équilibrage de charge.</p> <p>Par exemple, une demande client pour <code>http://app.com/path/page.html</code> est redirigée vers <code>https://app.com/path/page.html</code>. Si le nom d'hôte ou l'URI doit être modifié lors de la redirection, par exemple, vers <code>https://secure.app.com/path/page.html</code>, des règles d'équilibrage de charge doivent être utilisées.</p>
<p>X-Forwarded-For (XFF)</p>	<ul style="list-style-type: none"> ■ INSERT : si l'en-tête HTTP XFF ne figure pas dans la demande entrante, l'équilibrage de charge insère un nouvel en-tête XFF comprenant l'adresse IP du client. ■ REPLACE : si l'en-tête HTTP XFF est déjà présent dans la demande entrante, l'équilibrage de charge peut remplacer l'en-tête. <p>Les serveurs Web enregistrent dans des journaux chaque demande qu'ils gèrent avec l'adresse IP du client demandeur. Ces journaux sont utilisés à des fins de débogage et d'analyse. Si la topologie de déploiement nécessite le mode SNAT sur l'équilibrage de charge, le serveur utilise l'adresse IP SNAT et la journalisation n'a plus lieu d'être.</p> <p>Pour résoudre ce problème, l'équilibrage de charge peut être configuré pour insérer un en-tête HTTP XFF avec l'adresse IP du client d'origine. Les serveurs peuvent être configurés pour enregistrer l'adresse IP dans l'en-tête XFF au lieu de l'adresse IP source de la connexion.</p>
<p>Délai d'inactivité de la connexion</p>	<p>Entrez la durée en secondes pendant laquelle une application HTTP peut rester inactive, au lieu du paramètre de socket TCP qui doit être configuré dans le profil d'application TCP.</p>
<p>Taille de l'en-tête de la demande</p>	<p>Spécifiez la taille maximale de tampon en octets utilisée pour stocker les en-têtes de demande HTTP.</p>
<p>Authentification NTLM</p>	<p>Faites basculer ce bouton pour que l'équilibrage de charge désactive le multiplexage TCP et active les connexions HTTP persistantes.</p>

Option	Description
	<p>NTLM est un protocole d'authentification qui peut être utilisé sur HTTP. Pour l'équilibrage de charge avec l'authentification NTLM, le multiplexage TCP doit être désactivé pour les pools de serveurs hébergeant des applications NTLM. Dans le cas contraire, une connexion côté serveur établie avec les informations d'identification d'un client peut être potentiellement utilisée afin de servir les demandes d'un autre client.</p> <p>Si l'authentification NTLM est activée dans le profil et associée à un serveur virtuel, et que le multiplexage TCP est activé dans le pool de serveurs, l'authentification NTLM est prioritaire. Le multiplexage TCP n'est pas effectué pour ce serveur virtuel. Toutefois, si le même pool est associé à un autre serveur virtuel non-NTLM, le multiplexage TCP est disponible pour les connexions vers ce serveur.</p> <p>Si le client utilise des connexions HTTP/1.0, l'équilibrage de charge les met à niveau vers le protocole HTTP/1.1 et les connexions HTTP persistantes sont définies. Toutes les demandes HTTP reçues sur la même connexion TCP côté client sont envoyées vers le même serveur via une seule connexion TCP afin de s'assurer qu'aucune nouvelle autorisation n'est requise.</p>

- d Cliquez sur **OK**.

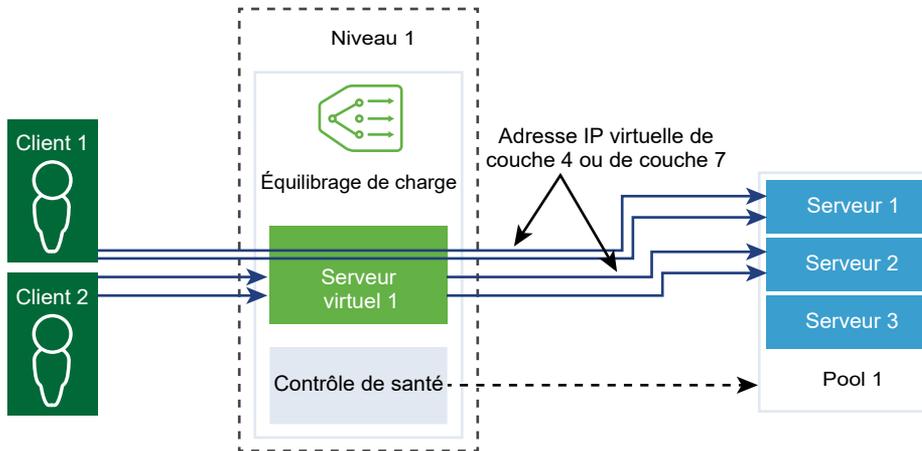
Configurer des profils persistants

Pour garantir la stabilité des applications avec état, les équilibres de charge implémentent la persistance qui dirige toutes les connexions associées au même serveur. Différents types de persistance sont pris en charge pour répondre à différents types de besoins d'application.

Certaines applications conservent l'état du serveur, par exemple, les paniers d'achat. Cet état peut être par client et identifié par l'adresse IP du client ou par la session HTTP. Les applications peuvent accéder à cet état ou le modifier lors du traitement des connexions suivantes liées à partir du même client ou de la même session HTTP.

Le profil de persistance de l'adresse IP source effectue le suivi des sessions en fonction de l'adresse IP source. Lorsqu'un client demande une connexion à un serveur virtuel prenant en charge la persistance de l'adresse source, l'équilibrage de charge vérifie si ce client s'est précédemment connecté, et si c'est le cas, renvoie le client au même serveur. Si ce n'est pas le cas, vous pouvez sélectionner un membre du pool de serveurs en fonction de l'algorithme d'équilibrage de charge du pool. Le profil de persistance de l'adresse IP source est utilisé par les serveurs virtuels de couche 4 et de couche 7.

Le profil de persistance des cookies insère un cookie unique afin d'identifier la session la première fois qu'un client accède au site. Le cookie HTTP est transmis par le client dans les demandes suivantes et l'équilibrage de charge utilise ces informations pour permettre la persistance des cookies. Le profil de persistance des cookies peut uniquement être utilisé par les serveurs virtuels de couche 7.



Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Mise en réseau > Équilibrage de charge > Profils > Profils de persistance**.
- 3 Créez un profil de persistance de l'adresse IP source.
 - a Sélectionnez **Ajouter > Persistance de l'adresse IP source** dans le menu déroulant.
 - b Entrez un nom et une description pour le profil de persistance de l'adresse IP source.

- c Renseignez les détails du profil de persistance.

Vous pouvez également accepter les paramètres du profil de persistance de l'adresse IP source par défaut.

Option	Description
Partager la persistance	<p>Faites basculer ce bouton pour partager la persistance afin que tous les serveurs virtuels auxquels ce profil est associé puissent partager la table de persistance.</p> <p>Si le partage de persistance n'est pas activé dans le profil de persistance de l'adresse IP source associé à un serveur virtuel, chaque serveur virtuel auquel le profil est associé maintient une table de persistance privée.</p>
Délai d'expiration de l'entrée de persistance	<p>Entrez la durée d'expiration de la persistance en secondes.</p> <p>La table de persistance d'équilibrage de charge conserve les entrées pour enregistrer que les demandes des clients sont dirigées vers le même serveur.</p> <ul style="list-style-type: none"> ■ Si aucune nouvelle demande de connexion n'est reçue de la part du même client pendant le délai d'expiration, l'entrée de persistance expire et est supprimée. ■ Si une nouvelle demande de connexion est reçue de la part du même client pendant le délai d'expiration, le temporisateur est réinitialisé et la demande du client est envoyée à un membre du pool rémanent. <p>Lorsque le délai est expiré, les nouvelles demandes de connexion sont envoyées à un serveur alloué par l'algorithme d'équilibrage de charge. Pour le scénario de persistance d'adresse IP source TCP d'équilibrage de charge L7, l'entrée de persistance expire si aucune nouvelle connexion TCP n'est établie pendant une certaine période, même si les connexions existantes sont toujours actives.</p>
Mise en miroir de la persistance HA	<p>Faites basculer ce bouton pour synchroniser les entrées de persistance avec l'homologue HA.</p>
Purger les entrées (table pleine)	<p>Purgez les entrées lorsque la table de persistance est pleine.</p> <p>Un délai d'expiration élevé peut entraîner le remplissage rapide de la table de persistance si le trafic est intense. Lorsque le tableau de persistance se remplit, l'entrée la plus ancienne est supprimée pour accepter l'entrée la plus récente.</p>

- d Cliquez sur **OK**.

4 Créer un profil de persistance des cookies.

- a Sélectionnez **Ajouter > Persistance des cookies** dans le menu déroulant.
- b Entrez un nom et une description pour le profil de persistance des cookies.

- c Faites basculer le bouton **Partager la persistance** pour partager la persistance entre plusieurs serveurs virtuels associés aux mêmes membres du pool.

Le profil de persistance des cookies insère un cookie au format `<nom>.<ID de profil>.<ID de pool>`.

Si la persistance partagée n'est pas activée dans le profil de persistance des cookies associé à un serveur virtuel, la persistance des cookies privée de chaque serveur virtuel est utilisée et certifiée par le membre du pool. L'équilibrage de charge insère un cookie au format `<nom>.<ID du serveur virtuel>.<ID du pool>`.

- d Cliquez sur **Suivant**.
- e Renseignez les détails du profil de persistance.

Option	Description
Mode de cookie	Sélectionnez un mode dans le menu déroulant. <ul style="list-style-type: none"> ■ INSERT : ajoute un cookie unique afin d'identifier la session. ■ PREFIX : ajoute des informations aux informations du cookie HTTP existantes. ■ REWRITE : réécrit les informations du cookie HTTP existantes.
Nom du cookie	Entrez le nom du cookie.
Domaine de cookie	Entrez le nom du domaine. Un domaine de cookie HTTP peut être configuré uniquement en mode INSERT.
Chemin d'accès au cookie	Entrez le chemin d'URL du cookie. Un chemin d'accès au cookie HTTP peut être défini uniquement en mode INSERT.
Chiffrement de cookie	Chiffrez l'adresse IP et le port du serveur de cookie. Faites basculer le bouton pour désactiver le chiffrement. Lorsque le chiffrement est désactivé, ces informations sont en texte brut.
Option de secours de cookie	Sélectionnez un nouveau serveur qui traitera la demande client si le cookie pointe vers un serveur dont l'état est DÉSACTIVÉ ou INACTIF. Faites basculer le bouton afin que la demande client soit refusée si le cookie pointe vers un serveur dont l'état est DÉSACTIVÉ ou INACTIF.

- f Renseignez les détails d'expiration du cookie.

Option	Description
Type de durée de cookie	Sélectionnez un type de durée de cookie dans le menu déroulant. Les types de cookie de session et de persistance expirent lors de la fermeture du navigateur.
Durée d'inactivité maximale	Entrez la durée en secondes pendant laquelle le cookie peut être inactif avant son expiration.

- g Cliquez sur **Terminer**.

Configurer un profil SSL

Les profils SSL configurent des propriétés SSL indépendantes des applications, notamment des listes de chiffrement qui peuvent être réutilisées sur plusieurs applications. Les propriétés SSL sont différentes lorsque l'équilibrage de charge est utilisé en tant que client ou en tant que serveur, et par conséquent, des profils SSL distincts sont pris en charge pour le côté client et le côté serveur.

Note Le profil SSL n'est pas pris en charge dans la version Limited Export de NSX-T Data Center.

Le profil SSL côté client fait référence à l'équilibrage de charge utilisé en tant que serveur SSL et à l'arrêt de la connexion SSL client. Le profil SSL côté serveur fait référence à l'équilibrage de charge utilisé en tant que client et à l'établissement d'une connexion avec le serveur.

Vous pouvez spécifier une liste de chiffrement sur les profils SSL côté client et côté serveur.

La mise en cache de session SSL permet au client et au serveur SSL de réutiliser les paramètres de sécurité précédemment négociés en évitant l'opération de clé publique coûteuse au cours de l'établissement de liaison SSL. Cette mise en cache est désactivée par défaut côté client et côté serveur.

Les tickets de session SSL constituent un autre mécanisme qui permet au client et au serveur SSL de réutiliser les paramètres de session précédemment négociés. Dans ces tickets, le client et le serveur négocient s'ils prennent en charge les tickets de session SSL lors de l'établissement de liaison. S'ils sont pris en charge des deux côtés, le serveur peut envoyer un ticket SSL, qui inclut des paramètres de session SSL chiffrés, au client. Le client peut utiliser ce ticket dans les connexions suivantes afin de réutiliser la session. Les tickets de session SSL sont activés côté client et désactivés côté serveur.

Figure 10-5. Déchargement SSL

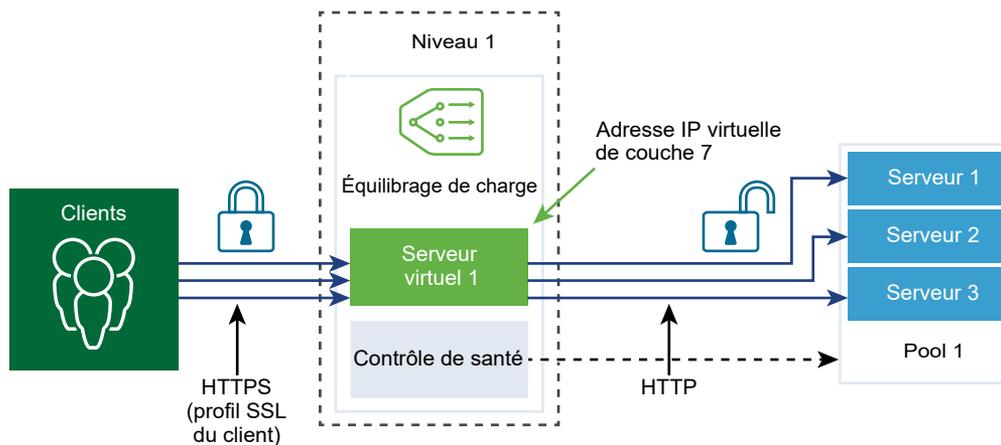
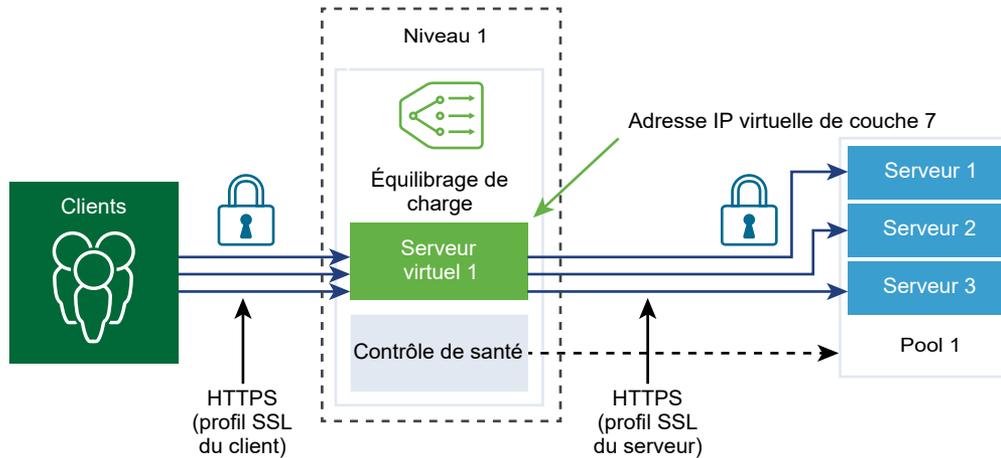


Figure 10-6. SSL de bout en bout



Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Équilibrage de charge > Profils > Profils SSL**.
- 3 Créez un profil SSL client.
 - a Sélectionnez **Ajouter > SSL côté client** dans le menu déroulant.
 - b Entrez un nom et une description pour le profil SSL client.
 - c Sélectionnez les chiffrements SSL à inclure dans le profil SSL client.
Vous pouvez également créer des chiffrements SSL personnalisés.
 - d Cliquez sur la flèche pour déplacer les chiffrements vers la section des éléments sélectionnés.
 - e Cliquez sur l'onglet **Protocoles et sessions**.
 - f Sélectionnez les protocoles SSL à inclure dans le profil SSL client.
Les versions de protocole SSL TLS 1.1 et TLS 1.2 sont activées par défaut. TLS 1.0 est également prise en charge, mais désactivée par défaut.
 - g Cliquez sur la flèche pour déplacer les protocoles vers la section des éléments sélectionnés.

- h Indiquez les détails du protocole SSL.

Vous pouvez également accepter les paramètres du profil SSL par défaut.

Option	Description
Mise en cache de session	La mise en cache de session SSL permet au client et au serveur SSL de réutiliser les paramètres de sécurité précédemment négociés en évitant l'opération de clé publique coûteuse au cours de l'établissement de liaison SSL.
Délai d'expiration de l'entrée de cache de session	Entrez le délai d'expiration du cache en secondes pour spécifier la durée pendant laquelle les paramètres de session SSL sont conservés et peuvent être réutilisés.
Chiffrement de serveur préféré	Faites basculer ce bouton pour que le serveur puisse sélectionner le premier chiffrement pris en charge dans la liste. Lors de l'établissement de liaison SSL, le client envoie une liste ordonnée des chiffrements pris en charge au serveur.

- i Cliquez sur **OK**.

4 Créer un profil SSL de serveur.

- a Sélectionnez **Ajouter > SSL côté serveur** dans le menu déroulant.
- b Entrez un nom et une description pour le profil SSL de serveur.
- c Sélectionnez les chiffrements SSL à inclure dans le profil SSL de serveur.

Vous pouvez également créer des chiffrements SSL personnalisés.

- d Cliquez sur la flèche pour déplacer les chiffrements vers la section des éléments sélectionnés.
- e Cliquez sur l'onglet **Protocoles et sessions**.
- f Sélectionnez les protocoles SSL à inclure dans le profil SSL de serveur.

Les versions de protocole SSL TLS 1.1 et TLS 1.2 sont activées par défaut. TLS 1.0 est également prise en charge, mais désactivée par défaut.

- g Cliquez sur la flèche pour déplacer les protocoles vers la section des éléments sélectionnés.
- h Acceptez le paramètre de mise en cache de session par défaut.

La mise en cache de session SSL permet au client et au serveur SSL de réutiliser les paramètres de sécurité précédemment négociés en évitant l'opération de clé publique coûteuse au cours de l'établissement de liaison SSL.

- i Cliquez sur **OK**.

Configurer des serveurs virtuels de couche 4

Les serveurs virtuels reçoivent toutes les connexions client et les distribuent entre les serveurs. Un serveur virtuel dispose d'une adresse IP, d'un port et d'un protocole. Pour les serveurs virtuels de couche 4, des listes de plages de ports peuvent être spécifiées au lieu d'un seul port TCP ou UDP pour prendre en charge les protocoles complexes à l'aide de ports dynamiques.

Un serveur virtuel de couche 4 doit être associé à un pool de serveurs principal, également appelé pool par défaut.

Si l'état d'un serveur virtuel est Désactivé, toute tentative de nouvelle connexion au serveur virtuel est refusée via l'envoi d'un RST TCP pour une connexion TCP ou d'un message d'erreur ICMP pour la connexion UDP. Les nouvelles connexions sont refusées, même si des entrées de persistance correspondent. Le traitement des connexions actives se poursuit. Si un serveur virtuel est supprimé ou dissocié d'un équilibrage de charge, les connexions actives à ce serveur échouent.

Conditions préalables

- Vérifiez que les profils d'application sont disponibles. Reportez-vous à la section [Configurer des profils d'application](#).
- Vérifiez que les profils persistants sont disponibles. Reportez-vous à la section [Configurer des profils persistants](#).
- Vérifiez que les profils SSL pour le client et le serveur sont disponibles. Reportez-vous à la section [Configurer un profil SSL](#).
- Vérifiez que les pools de serveurs sont disponibles. Reportez-vous à la section [Ajouter un pool de serveurs pour l'équilibrage de charge](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Mise en réseau > Équilibrage de charge > Serveurs virtuels > Ajouter**.
- 3 Entrez un nom et une description pour le serveur virtuel de couche 4.
- 4 Dans le menu déroulant, sélectionnez un protocole de couche 4.

Les serveurs virtuels de couche 4 prennent en charge le protocole Fast TCP ou Fast UDP, mais pas les deux. Pour permettre la prise en charge du protocole Fast TCP ou Fast UDP sur la même adresse IP et le même port (par exemple, DNS), un serveur virtuel doit être créé pour chaque protocole.

Selon le type de protocole, le profil d'application existant est automatiquement renseigné.

- 5 Basculez le bouton Journal d'accès pour activer la journalisation pour le serveur virtuel de couche 4.
- 6 Cliquez sur **Suivant**.
- 7 Entrez l'adresse IP et le numéro de port du serveur virtuel.

Vous pouvez entrer le numéro de port ou la plage de ports du serveur virtuel.

8 Renseignez les détails des propriétés avancées.

Option	Description
Nombre maximal de connexions simultanées	Définissez le nombre maximal de connexions simultanées autorisées sur un serveur virtuel afin que celui-ci n'épuise pas les ressources d'autres applications hébergées sur le même équilibrage de charge.
Vitesse maximale de nouvelle connexion	Définissez la vitesse maximale de nouvelle connexion à un membre du pool de serveurs afin qu'un serveur virtuel n'épuise pas ses ressources.
Port de membre du pool par défaut	Entrez un port de membre du pool par défaut si le port de membre du pool pour un serveur virtuel n'est pas défini. Par exemple, si un serveur virtuel est défini avec la plage de ports 2000 - 2999 et que la plage de ports de membre du pool par défaut est définie sur 8000 - 8999, une connexion client entrante sur le port 2500 du serveur virtuel est envoyée à un membre du pool dont le port de destination est défini sur 8500.

9 Sélectionnez un pool de serveurs existant dans le menu déroulant.

Le pool de serveurs est constitué d'un ou de plusieurs serveurs, également appelés membres du pool, qui sont configurés de la même manière et qui exécutent la même application.

10 Sélectionnez un pool de serveurs Désolé existant dans le menu déroulant.

Le pool de serveurs Désolé répond à la demande lorsqu'un équilibrage de charge ne peut pas sélectionner un serveur principal pour répondre à la demande depuis le pool par défaut.

11 Cliquez sur **Suivant**.

12 Sélectionnez le profil de persistance dans le menu déroulant.

Un profil de persistance peut être activé sur un serveur virtuel afin d'autoriser l'envoi de connexions client associées au même serveur.

13 Cliquez sur **Terminer**.

Configurer des serveurs virtuels de couche 7

Les serveurs virtuels reçoivent toutes les connexions client et les distribuent entre les serveurs. Un serveur virtuel dispose d'une adresse IP, d'un port et d'un protocole TCP.

Les règles d'équilibrage de charge sont prises en charge uniquement pour les serveurs virtuels de couche 7 avec un profil d'application HTTP. Différents services d'équilibrage de charge peuvent utiliser les règles d'équilibrage de charge.

Chaque règle d'équilibrage de charge se compose d'une ou de plusieurs conditions de correspondance et d'une ou de plusieurs actions. Si aucune condition de correspondance n'est spécifiée, la règle d'équilibrage de charge correspond toujours et elle est utilisée pour définir des règles par défaut. Si plusieurs conditions de correspondance sont spécifiées, la stratégie de correspondance détermine si toutes les conditions ou quelques conditions doivent correspondre pour que la règle d'équilibrage de charge soit considérée comme une correspondance.

Chaque règle d'équilibrage de charge est mise en œuvre lors d'une phase spécifique du traitement de l'équilibrage de charge : Réécriture de la demande HTTP, Transfert de la demande HTTP et Réécriture de la réponse HTTP. Seules certaines conditions de correspondance et actions sont applicables à chaque phase.

Si l'état d'un serveur virtuel est Désactivé, toute tentative de nouvelle connexion au serveur virtuel est refusée via l'envoi d'un RST TCP pour une connexion TCP ou d'un message d'erreur ICMP pour la connexion UDP. Les nouvelles connexions sont refusées, même si des entrées de persistance correspondent. Le traitement des connexions actives se poursuit. Si un serveur virtuel est supprimé ou dissocié d'un équilibrage de charge, les connexions actives à ce serveur échouent.

Conditions préalables

- Vérifiez que les profils d'application sont disponibles. Reportez-vous à la section [Configurer des profils d'application](#).
- Vérifiez que les profils persistants sont disponibles. Reportez-vous à la section [Configurer des profils persistants](#).
- Vérifiez que les profils SSL pour le client et le serveur sont disponibles. Reportez-vous à la section [Configurer un profil SSL](#).
- Vérifiez que les pools de serveurs sont disponibles. Reportez-vous à la section [Ajouter un pool de serveurs pour l'équilibrage de charge](#).
- Vérifiez que le certificat d'autorité de certification et le certificat client sont disponibles. Reportez-vous à la section [Créer un fichier de demande de signature de certificat](#).
- Vérifiez qu'une liste de révocation des certificats (CRL) est disponible. Reportez-vous à la section [Importer une liste de révocation des certificats](#).
- [Configurer un pool de serveurs virtuels de couche 7 et des règles](#)
Avec les serveurs virtuels de couche 7, vous pouvez éventuellement configurer des règles d'équilibrage de charge et personnaliser le comportement de l'équilibrage de charge à l'aide de règles de correspondance ou d'action.
- [Configurer les profils d'équilibrage de charge de serveur virtuel de couche 7](#)
Avec les serveurs virtuels de couche 7, vous pouvez éventuellement configurer la persistance de l'équilibrage de charge, des profils SSL côté client et des profils SSL côté serveur.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Mise en réseau > Équilibrage de charge > Serveurs virtuels > Ajouter**.
- 3 Entrez un nom et une description pour le serveur virtuel de couche 7.

4 Sélectionnez l'élément de menu **Couche 7**.

Les serveurs virtuels de couche 7 prennent en charge les protocoles HTTP et HTTPS.

Le profil d'application HTTP existant est automatiquement renseigné.

5 (Facultatif) Cliquez sur **Suivant** pour configurer le pool de serveurs et les profils d'équilibrage de charge.

6 Cliquez sur **Terminer**.

Configurer un pool de serveurs virtuels de couche 7 et des règles

Avec les serveurs virtuels de couche 7, vous pouvez éventuellement configurer des règles d'équilibrage de charge et personnaliser le comportement de l'équilibrage de charge à l'aide de règles de correspondance ou d'action.

Les règles d'équilibrage de charge prennent en charge REGEX pour les types de correspondances. Le modèle REGEX de style PCRE est pris en charge avec quelques limitations pour les cas d'utilisation avancés. Lorsque REGEX est utilisé dans des conditions de correspondance, les groupes de capture nommés sont pris en charge.

Les restrictions REGEX sont les suivantes :

- Les unions et intersections de caractères ne sont pas prises en charge. Par exemple, n'utilisez pas `[a-z [0-9]]` et `[a-z&&[aeiou]]` mais plutôt `[a-z0-9]` et `[aeiou]` respectivement.
- Seules 9 références arrière sont prises en charge et `\1` à `\9` peuvent être utilisés pour y faire référence.
- Utilisez le format `\Odd` pour les correspondances avec les caractères au format octal, et non le format `\ddd`.
- Les indicateurs intégrés ne sont pas pris en charge au niveau supérieur, ils sont uniquement pris en charge au sein des groupes. Par exemple, n'utilisez pas « `Case (?i:s)ensitive` » mais plutôt « `Case ((?i:s)ensitive)` ».
- Les opérations de prétraitement `\l`, `\u`, `\L`, `\U` ne sont pas prises en charge. Où `\l` - caractère suivant minuscule `\u` - caractère suivant majuscule `\L` - minuscule jusqu'à `\E` `\U` - majuscule jusqu'à `\E`.
- `(?(condition)X)`, `(?{code})`, `(??{Code})` et `(?#comment)` ne sont pas pris en charge.
- La classe `\X` de caractères Unicode prédéfinie n'est pas prise en charge
- L'utilisation de la construction de caractères nommés n'est pas prise en charge pour les caractères Unicode. Par exemple, n'utilisez pas `\N{nom}` mais plutôt `\u2018`.

Lorsque REGEX est utilisé dans des conditions de correspondance, les groupes de capture nommés sont pris en charge. Par exemple, le modèle de correspondance REGEX `/news/(?<year>\d+)-(?(<month>\d+)-(?(<day>\d+)/?(<article>.*))` peut être utilisé pour correspondre à un URI tel que `/news/2018-06-15/news1234.html`.

Les variables sont ensuite définies comme suit, \$year = "2018" \$month = "06" \$day = "15" \$article = "news1234.html". Une fois les variables configurées, elles peuvent être utilisées dans les actions de règle d'équilibrage de charge. Par exemple, l'URI peut être réécrit en utilisant des variables mises en correspondance, telles que /news.py?year=\$year&month=\$month&day=\$day&article=\$article. Ensuite l'URI est réécrit sous la forme /news.py?year=2018&month=06&day=15&article=news1234.html.

Les actions de réécriture peuvent utiliser une combinaison de groupes de capture nommés et de variables intégrées. Par exemple, l'URI peut être écrit sous la forme /news.py?year=\$year&month=\$month&day=\$day&article=\$article&user_ip=\$_remote_addr. Ensuite l'exemple d'URI est réécrit sous la forme /news.py?year=2018&month=06&day=15&article=news1234.html&user_ip=1.1.1.1.

Note Pour les groupes de capture nommés, le nom ne peut pas commencer par un caractère _.

En plus des groupes de capture nommés, les variables intégrées suivantes peuvent être utilisées dans les actions de réécriture. Tous les noms de variable intégrés commencent par _.

- \$_args - arguments de la demande
- \$_cookie_<nom> - valeur du cookie <nom>
- \$_host - dans l'ordre de priorité - nom d'hôte de la ligne de demande, ou nom d'hôte du champ d'en-tête de demande « Host » ou nom du serveur correspondant à une demande
- \$_hostname - nom d'hôte
- \$_http_<nom> - champ d'en-tête de demande arbitraire, <nom> étant le nom du champ converti en minuscules dans lequel les tirets sont remplacés par des traits de soulignement
- \$_https - "on" si la connexion fonctionne en mode SSL, ou "" dans le cas contraire
- \$_is_args - "?" si une ligne de demande dispose d'arguments, ou "" dans le cas contraire
- \$_query_string - identique à \$_args
- \$_remote_addr - adresse du client
- \$_remote_port - port du client
- \$_request_uri - URI complet de la demande d'origine (avec les arguments)
- \$_scheme - schéma de demande, "http" ou "https"
- \$_server_addr - adresse du serveur qui a accepté une demande
- \$_nom_serveur - nom du serveur qui a accepté une demande
- \$_server_port - port du serveur qui a accepté une demande
- \$_server_protocol - protocole de la demande, généralement « HTTP/1.0 » ou « HTTP/1.1 »
- \$_ssl_client_cert - renvoie le certificat client au format PEM pour une connexion SSL établie, avec chaque ligne, à l'exception de la première, précédée du caractère de tabulation
- \$_ssl_server_name - renvoie le nom du serveur demandé par le biais de SNI
- \$_uri - chemin d'accès URI dans la demande

Conditions préalables

Vérifiez qu'un serveur virtuel de couche 7 est disponible. Reportez-vous à la section [Configurer des serveurs virtuels de couche 7](#).

Procédure

- 1 Ouvrez le serveur virtuel de couche 7.
- 2 Passez à la page Identifiants de serveur virtuel.
- 3 Entrez l'adresse IP et le numéro de port du serveur virtuel.

Vous pouvez entrer le numéro de port ou la plage de ports du serveur virtuel.

- 4 Renseignez les détails des propriétés avancées.

Option	Description
Nombre maximal de connexions simultanées	Définissez le nombre maximal de connexions simultanées autorisées sur un serveur virtuel afin que celui-ci n'épuise pas les ressources d'autres applications hébergées sur le même équilibrage de charge.
Vitesse maximale de nouvelle connexion	Définissez la vitesse maximale de nouvelle connexion à un membre du pool de serveurs afin qu'un serveur virtuel n'épuise pas ses ressources.
Port de membre du pool par défaut	Entrez un port de membre du pool par défaut si le port de membre du pool pour un serveur virtuel n'est pas défini. Par exemple, si un serveur virtuel est défini avec la plage de ports 2000 - 2999 et que la plage de ports de membre du pool par défaut est définie sur 8000 - 8999, une connexion client entrante sur le port 2500 du serveur virtuel est envoyée à un membre du pool dont le port de destination est défini sur 8500.

- 5 (Facultatif) Sélectionnez un pool de serveurs par défaut existant dans le menu déroulant.

Le pool de serveurs est constitué d'un ou de plusieurs serveurs, appelés membres du pool, qui sont configurés de la même manière et qui exécutent la même application.

- 6 Cliquez sur **Ajouter** pour configurer les règles d'équilibrage de charge pour la phase Réécriture de la demande HTTP.

Les types de correspondance prises en charge sont REGEX, STARTS_WITH, ENDS_WITH, etc. et l'option inverse.

Condition de correspondance prise en charge	Description
Méthode de demande HTTP	Correspondance à une méthode de demande HTTP. http_request.method - valeur à faire correspondre
URI de demande HTTP	Correspondance à l'URI d'une demande HTTP sans arguments de requête. http_request.uri - valeur à faire correspondre
Arguments d'URI de demande HTTP	Correspondance à un argument de requête d'URI d'une demande HTTP. http_request.uri_arguments - valeur à faire correspondre

Condition de correspondance prise en charge	Description
Version de la demande HTTP	Correspondance à la version d'une demande HTTP. http_request.version - valeur à faire correspondre
En-tête de demande HTTP	Correspondance à n'importe quel en-tête de demande HTTP. http_request.header_name - nom d'en-tête à faire correspondre http_request.header_value - valeur à faire correspondre
Charge utile de demande HTTP	Correspondance au contenu du corps d'une demande HTTP. http_request.body_value - valeur à faire correspondre
Champs d'en-tête TCP	Correspondance au port TCP source ou de destination. tcp_header.source_port - port source à faire correspondre tcp_header.destination_port - port de destination à faire correspondre
Champs d'en-tête d'adresse IP	Correspondance à une adresse IP source ou de destination. ip_header.source_address - adresse source à faire correspondre ip_header.destination_address - adresse de destination à faire correspondre

Action	Description
Réécriture d'URI de demande HTTP	Modifier un URI. http_request.uri - URI (sans arguments de requête) à écrire http_request.uri_args - arguments de requête d'URI à écrire
Réécriture d'en-tête de demande HTTP	Modifier la valeur d'un en-tête HTTP. http_request.header_name - nom d'en-tête http_request.header_value - valeur à écrire

- 7 Cliquez sur **Ajouter** pour configurer les règles d'équilibrage de charge pour la phase Transfert de la demande HTTP.

Toutes les valeurs de correspondance acceptent des expressions régulières.

Condition de correspondance prise en charge	Description
Méthode de demande HTTP	Correspondance à une méthode de demande HTTP. http_request.method - valeur à faire correspondre
URI de demande HTTP	Correspondance à un URI de demande HTTP. http_request.uri - valeur à faire correspondre
Arguments d'URI de demande HTTP	Correspondance à un argument de requête d'URI d'une demande HTTP. http_request.uri_args - valeur à faire correspondre
Version de la demande HTTP	Correspondance à la version d'une demande HTTP. http_request.version - valeur à faire correspondre
En-tête de demande HTTP	Correspondance à n'importe quel en-tête de demande HTTP. http_request.header_name - nom d'en-tête à faire correspondre http_request.header_value - valeur à faire correspondre

Condition de correspondance prise en charge	Description
Charge utile de demande HTTP	Correspondance au contenu du corps d'une demande HTTP. http_request.body_value - valeur à faire correspondre
Champs d'en-tête TCP	Correspondance au port TCP source ou de destination. tcp_header.source_port - port source à faire correspondre tcp_header.destination_port - port de destination à faire correspondre
Champs d'en-tête d'adresse IP	Correspondance à une adresse IP source. ip_header.source_address - adresse source à faire correspondre

Action	Description
Refuser	Refuser une demande, par exemple, en définissant l'état sur 5xx. http_forward.reply_status - code d'état HTTP utilisé pour le refus http_forward.reply_message - message de refus HTTP
Rediriger	Rediriger une demande. Le code d'état doit être défini sur 3xx. http_forward.redirect_status - code d'état HTTP pour la redirection http_forward.redirect_url - URL de redirection HTTP
Sélectionner un pool	Forcer la demande sur un pool de serveurs spécifique. L'algorithme configuré du membre du pool spécifié (predictor) est utilisé pour sélectionner un serveur dans le pool de serveurs. http_forward.select_pool - UUID du pool de serveurs

- 8 Cliquez sur **Ajouter** pour configurer les règles d'équilibrage de charge pour la phase Réécriture de la réponse HTTP.

Toutes les valeurs de correspondance acceptent des expressions régulières.

Condition de correspondance prise en charge	Description
En-tête de réponse HTTP	Correspondance à n'importe quel en-tête de réponse HTTP. http_response.header_name - nom d'en-tête à faire correspondre http_response.header_value - valeur à faire correspondre

Action	Description
Réécriture de l'en-tête de réponse HTTP	Modifier la valeur d'un en-tête de réponse HTTP. http_response.header_name - nom d'en-tête http_response.header_value - valeur à écrire

- 9 (Facultatif) Cliquez sur **Suivant** pour configurer les profils d'équilibrage de charge.
- 10 Cliquez sur **Terminer**.

Configurer les profils d'équilibrage de charge de serveur virtuel de couche 7

Avec les serveurs virtuels de couche 7, vous pouvez éventuellement configurer la persistance de l'équilibrage de charge, des profils SSL côté client et des profils SSL côté serveur.

Note Les profils SSL ne sont pas pris en charge dans la version Limited Export de NSX-T Data Center 2.2.

Si une liaison de profil SSL côté client est configurée sur un serveur virtuel, mais sans liaison de profil SSL côté serveur, le serveur virtuel fonctionne en mode d'arrêt SSL, ce qui suppose une connexion chiffrée au client et une connexion en texte brut au serveur. Si les liaisons de profils SSL côté client et côté serveur sont configurées, le serveur virtuel fonctionne en mode proxy SSL, ce qui suppose une connexion chiffrée au client et au serveur.

Associer une liaison de profil SSL côté serveur sans associer de liaison de profil SSL côté client n'est actuellement pas pris en charge. Si une liaison de profil SSL côté client et côté serveur n'est pas associée à un serveur virtuel et que l'application est basée sur SSL, le serveur virtuel fonctionne en mode non compatible avec SSL. Dans ce cas, le serveur virtuel doit être configuré pour la couche 4. Par exemple, le serveur virtuel peut être associé à un profil TCP rapide.

Conditions préalables

Vérifiez qu'un serveur virtuel de couche 7 est disponible. Reportez-vous à la section [Configurer des serveurs virtuels de couche 7](#).

Procédure

- 1 Ouvrez le serveur virtuel de couche 7.
- 2 Passez à la page Profils d'équilibrage de charge.
- 3 Faites basculer le bouton Persistance pour activer le profil.

Le profil de persistance autorise l'envoi des connexions client associées au même serveur.

- 4 Sélectionnez le profil Persistance de l'adresse IP source ou Persistance des cookies.
- 5 Sélectionnez le profil de persistance dans le menu déroulant.
- 6 Cliquez sur **Suivant**.
- 7 Faites basculer le bouton SSL côté client pour activer le profil.

La liaison de profil SSL côté client permet d'associer plusieurs certificats au même serveur virtuel pour différents noms d'hôtes.

Le profil SSL côté client associé est automatiquement renseigné.

- 8 Sélectionnez un certificat par défaut dans le menu déroulant.

Ce certificat est utilisé si le serveur n'héberge pas plusieurs noms d'hôte sur la même adresse IP ou si le client ne prend pas en charge l'extension SNI (Server Name Indication, indication de nom de serveur).

- 9 Sélectionnez le certificat SNI disponible et cliquez sur la flèche pour le déplacer vers la section des éléments sélectionnés.
- 10 (Facultatif) Faites basculer le bouton Authentification du client obligatoire pour activer cet élément de menu.
- 11 Sélectionnez le certificat d'autorité de certification disponible et cliquez sur la flèche pour le déplacer vers la section des éléments sélectionnés.
- 12 Définissez la profondeur de la chaîne de certificats pour vérifier la profondeur de la chaîne de certificats du serveur.
- 13 Sélectionnez la liste de révocation des certificats (CRL) disponible et cliquez sur la flèche pour la déplacer vers la section des éléments sélectionnés.

Une CRL peut être configurée pour interdire les certificats de serveur compromis.
- 14 Cliquez sur **Suivant**.
- 15 Faites basculer le bouton SSL côté serveur pour activer le profil.

Le profil SSL côté serveur associé est automatiquement renseigné.
- 16 Sélectionnez un certificat client dans le menu déroulant.

Ce certificat est utilisé si le serveur n'héberge pas plusieurs noms d'hôte sur la même adresse IP ou si le client ne prend pas en charge l'extension SNI.
- 17 Sélectionnez le certificat SNI disponible et cliquez sur la flèche pour le déplacer vers la section des éléments sélectionnés.
- 18 (Facultatif) Faites basculer le bouton Authentification du serveur pour activer cet élément de menu.

La liaison de profil SSL côté serveur indique si le certificat de serveur présenté à l'équilibrage de charge pendant l'établissement de liaison SSL doit être validé. Lorsque la validation est activée, le certificat du serveur doit être signé par une des autorités de certification approuvées dont les certificats autosignés sont spécifiés dans la même liaison de profil SSL côté serveur.
- 19 Sélectionnez le certificat d'autorité de certification disponible et cliquez sur la flèche pour le déplacer vers la section des éléments sélectionnés.
- 20 Définissez la profondeur de la chaîne de certificats pour vérifier la profondeur de la chaîne de certificats du serveur.
- 21 Sélectionnez la liste de révocation des certificats (CRL) disponible et cliquez sur la flèche pour la déplacer vers la section des éléments sélectionnés.

Une CRL peut être configurée pour interdire les certificats de serveur compromis. Le protocole OCSP et l'association OCSP ne sont pas pris en charge côté serveur.
- 22 Cliquez sur **Terminer**.

Le protocole DHCP (Dynamic Host Configuration Protocol) permet aux clients d'obtenir directement la configuration réseau (adresse IP, masque de sous-réseau, passerelle par défaut et configuration DNS) auprès d'un serveur DHCP.

Vous pouvez créer des serveurs DHCP pour gérer vos requêtes DHCP et créer des services de relais DHCP pour relayer le trafic DHCP vers les serveurs DHCP externes. Toutefois, vous ne devez pas configurer un serveur DHCP sur un commutateur logique et configurer un service de relais DHCP sur un port de routeur auquel le même commutateur logique est connecté. Dans ce cas, les demandes DHCP sont uniquement dirigées vers le service de relais DHCP.

Si vous configurez des serveurs DHCP, vous pouvez, pour améliorer la sécurité, configurer une règle DFW qui autorise le trafic sur les ports UDP 67 et 68 uniquement aux adresses IP de serveur DHCP valides.

Note Une règle DFW dont la source est `Logical Switch/Logical Port/NSGroup`, la destination est `Any` et qui est configurée pour rejeter les paquets DHCP pour les ports 67 et 68, ne parviendra pas à bloquer le trafic DHCP. Pour bloquer le trafic DHCP, configurez `Any` à la fois comme source et comme destination.

Ce chapitre contient les rubriques suivantes :

- [Créer un profil de serveur DHCP](#)
- [Créer un serveur DHCP](#)
- [Attacher un serveur DHCP à un commutateur logique](#)
- [Détacher un serveur DHCP d'un commutateur logique](#)
- [Créer un profil de relais DHCP](#)
- [Créer un service de relais DHCP](#)
- [Ajouter un service DHCP à un port de routeur logique](#)

Créer un profil de serveur DHCP

Un profil de serveur DHCP spécifie un cluster NSX Edge ou les membres d'un cluster NSX Edge. Un serveur DHCP doté de ce profil sert les demandes DHCP provenant des machines virtuelles des commutateurs logiques qui sont connectés aux nœuds NSX Edge spécifiés dans le profil.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > DHCP** dans le panneau de navigation.
- 3 Cliquez sur **Profils de serveurs**, puis sur **Ajouter**.
- 4 Entrez un nom et une description facultative.
- 5 Sélectionnez un cluster NSX Edge dans le menu déroulant.
- 6 (Facultatif) Sélectionnez les membres du cluster NSX Edge.
Vous pouvez spécifier jusqu'à 2 membres.

Étape suivante

Créez un serveur DHCP. Reportez-vous à la section [Créer un serveur DHCP](#).

Créer un serveur DHCP

Vous pouvez créer des serveurs DHCP pour servir les demandes DHCP émanant des machines virtuelles connectées aux commutateurs logiques.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > DHCP** dans le panneau de navigation.
- 3 Cliquez sur **Serveurs**, puis sur **Ajouter**.
- 4 Entrez un nom et une description facultative.
- 5 Entrez l'adresse IP du serveur DHCP et son masque de sous-réseau au format CIDR.
Par exemple, entrez 192.168.1.2/24.
- 6 (Requis) Choisissez un profil DHCP dans le menu déroulant.
- 7 (Facultatif) Entrez les options courantes, telles que nom de domaine, passerelle par défaut, serveurs DNS et masque de sous-réseau.
- 8 (Facultatif) Entrez les options d'itinéraire statique sans classe.
- 9 (Facultatif) Entrez les autres options.
- 10 Cliquez sur **Enregistrer**.
- 11 Sélectionnez le serveur DHCP nouvellement créé.
- 12 Développez la section Pools d'adresses IP.

- 13 Cliquez sur **Ajouter** pour ajouter les plages d'adresses IP, la passerelle par défaut, la durée du bail, le seuil d'avertissement, le seuil d'erreur, l'option d'itinéraire statique sans classe, ainsi que d'autres options.
- 14 Développez la section Liaisons statiques.
- 15 Cliquez sur **Ajouter** pour ajouter les liaisons statiques entre les adresses MAC et les adresses IP, la passerelle par défaut, le nom d'hôte, la durée du bail, l'option d'itinéraire statique sans classe, ainsi que d'autres options.

Étape suivante

Attachez un serveur DHCP à un commutateur logique. Reportez-vous à la section [Attacher un serveur DHCP à un commutateur logique](#).

Attacher un serveur DHCP à un commutateur logique

Vous devez attacher un serveur DHCP à un commutateur logique pour que le serveur DHCP puisse traiter les demandes DHCP des VM connectées au commutateur. Le serveur DHCP n'est pas pris en charge sur les commutateurs logiques VLAN.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Commutation** dans le panneau de navigation.
- 3 Cliquez sur le commutateur logique auquel vous prévoyez d'attacher un serveur DHCP.
- 4 Cliquez sur **Actions > Attacher un serveur DHCP**.

Détacher un serveur DHCP d'un commutateur logique

Vous pouvez détacher un serveur DHCP d'un commutateur logique pour reconfigurer votre environnement.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Commutation** dans le panneau de navigation.
- 3 Cliquez sur le commutateur logique duquel vous prévoyez de détacher un serveur DHCP.
- 4 Cliquez sur **Actions > Détacher un serveur DHCP**.

Créer un profil de relais DHCP

Un profil de relais DHCP spécifie un ou plusieurs serveurs DHCP externes. Lorsque vous créez un service de relais DHCP, vous devez spécifier un profil de relais DHCP.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Mise en réseau > DHCP** dans le panneau de navigation.
- 3 Cliquez sur **Profils de relais**, puis sur **Ajouter**.
- 4 Entrez un nom et une description facultative.
- 5 Entrez une ou plusieurs adresses de serveur DHCP externe.

Étape suivante

Créez un service de relais DHCP. Reportez-vous à la section [Créer un service de relais DHCP](#).

Créer un service de relais DHCP

Vous pouvez créer un service de relais DHCP pour relayer le trafic entre des clients DHCP et des serveurs DHCP qui ne sont pas créés dans NSX-T Data Center.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Mise en réseau > DHCP** dans le panneau de navigation.
- 3 Cliquez sur **Services de relais**, puis sur **Ajouter**.
- 4 Entrez un nom et une description facultative.
- 5 Sélectionnez un profil de relais DHCP dans le menu déroulant.

Étape suivante

Ajoutez un service DHCP à un port de routeur logique. Reportez-vous à la section [Ajouter un service DHCP à un port de routeur logique](#).

Ajouter un service DHCP à un port de routeur logique

Lorsque vous ajoutez un service de relais DHCP à un port de routeur logique, des VM sur le commutateur logique attaché à ce port peuvent communiquer avec les serveurs DHCP configurés dans le service de relais.

Conditions préalables

- Vérifiez que vous disposez d'un service de relais DHCP configuré. Reportez-vous à la section [Créer un service de relais DHCP](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur *https://<adresse-ip-nsx-manager>*.
- 2 Sélectionnez **Mise en réseau > Routage** dans le panneau de navigation.
- 3 Sélectionnez le routeur connecté au commutateur logique de votre choix et cliquez sur l'onglet **Configuration**.
- 4 Sélectionnez le port de routeur connecté au commutateur logique de votre choix et cliquez sur **Modifier**.
- 5 Sélectionnez un service de relais DHCP dans la liste déroulante **Service DHCP** et cliquez sur **Enregistrer**.

Le port de routeur logique affiche le service de relais DHCP dans la colonne **Service DHCP**.

Vous pouvez également sélectionner un service de relais DHCP lorsque vous ajoutez un nouveau port de routeur logique.

Proxys de métadonnées

12

Avec un serveur proxy de métadonnées, des instances de VM peuvent récupérer des métadonnées spécifiques d'une instance depuis un serveur API OpenStack Nova.

Les étapes suivantes décrivent comment un proxy de métadonnées fonctionne :

- 1 Une VM envoie une requête HTTP GET à `http://169.254.169.254:80` pour demander certaines métadonnées.
- 2 Le serveur proxy de métadonnées connecté au même commutateur logique que la VM lit la demande, apporte les modifications appropriées aux en-têtes et transfère la demande au serveur API Nova.
- 3 Le serveur API Nova demande et reçoit des informations sur la VM de la part du serveur Neutron.
- 4 Le serveur API Nova recherche les métadonnées et les envoie au serveur proxy de métadonnées.
- 5 Le serveur proxy de métadonnées transfère les métadonnées à la VM.

Un serveur proxy de métadonnées est exécuté sur un nœud NSX Edge. Pour la haute disponibilité, vous pouvez configurer un proxy de métadonnées pour qu'il s'exécute sur deux nœuds NSX Edge ou plus dans un cluster NSX Edge.

Ce chapitre contient les rubriques suivantes :

- [Ajouter un serveur proxy de métadonnées](#)
- [Attacher un serveur proxy de métadonnées à un commutateur logique](#)
- [Détacher un serveur proxy de métadonnées d'un commutateur logique](#)

Ajouter un serveur proxy de métadonnées

Un serveur proxy de métadonnées permet aux machines virtuelles de récupérer les métadonnées à partir d'un serveur d'API OpenStack Nova.

Conditions préalables

Vérifiez que vous avez créé un cluster NSX Edge. Pour plus d'informations, reportez-vous à la section *Guide d'installation de NSX-T Data Center*.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur *https://<adresse-ip-nsx-manager>*.
- 2 Sélectionnez **Mise en réseau > DHCP** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Proxys de métadonnées**.
- 4 Cliquez sur **Ajouter**.
- 5 Entrez un nom pour le serveur proxy de métadonnées.
- 6 (Facultatif) Entrez une description.
- 7 Entrez l'URL et le port du serveur Nova.
La plage de ports valide est 3 000 - 9 000.
- 8 Entrez une valeur pour **Secret**.
- 9 Sélectionnez un cluster NSX Edge dans la liste déroulante.
- 10 (Facultatif) Sélectionnez les membres du cluster NSX Edge.

Exemple

Par exemple :

New Metadata Proxy Server ? ×

Name*	metadata-proxy-1
Description	
Nova Server URL*	https://123.1.1.1:8775
Secret*	*****
Edge Cluster*	edge_cluster_plr1 ▼
Members	53524616-c67f-11e8-837f-020046520048 × ▼

CANCEL
ADD

Étape suivante

Attachez le serveur proxy de métadonnées à un commutateur logique.

Attacher un serveur proxy de métadonnées à un commutateur logique

Pour fournir des services proxy de métadonnées à des VM connectées à un commutateur logique, vous devez attacher un serveur proxy de métadonnées au commutateur.

Conditions préalables

Vérifiez que vous avez créé un commutateur logique. Pour plus d'informations, consultez [Créer un commutateur logique](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > DHCP** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Proxys de métadonnées**.
- 4 Sélectionnez un serveur proxy de métadonnées.
- 5 Sélectionnez l'option de menu **Actions > Attacher à un commutateur logique**
- 6 Sélectionnez un commutateur logique dans la liste déroulante.

Résultats

Vous pouvez également attacher un serveur proxy de métadonnées à un commutateur logique en accédant à **Commutation > Commutateurs**, en sélectionnant un commutateur et en sélectionnant l'option de menu **Actions > Attacher à un proxy de métadonnées**.

Détacher un serveur proxy de métadonnées d'un commutateur logique

Pour interrompre la fourniture de services proxy de métadonnées aux machines virtuelles connectées à un commutateur logique, ou utiliser un autre serveur proxy de métadonnées, vous pouvez détacher le serveur proxy de métadonnées du commutateur logique.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > DHCP** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Proxys de métadonnées**.
- 4 Sélectionnez un serveur proxy de métadonnées.
- 5 Sélectionnez l'option de menu **Actions > Détacher du commutateur logique**
- 6 Sélectionnez un commutateur logique dans la liste déroulante.

Résultats

Vous pouvez également détacher un serveur proxy de métadonnées d'un commutateur logique en accédant à **Commutation > Commutateurs**, en sélectionnant un commutateur, puis en sélectionnant l'option de menu **Actions > Détacher le proxy de métadonnées**.

Gestion des adresses IP

13

Avec la gestion des adresses IP (IPAM), vous pouvez créer des blocs d'adresses IP pour prendre en charge NSX-T Container Plug-in (NCP). Pour plus d'informations sur NCP, consultez le *Guide d'installation et d'administration de NSX-T Container Plug-in for Kubernetes*.

Ce chapitre contient les rubriques suivantes :

- [Gérer des blocs d'adresses IP](#)
- [Gérer des sous-réseaux pour des blocs d'adresses IP](#)

Gérer des blocs d'adresses IP

La configuration de NSX-T Container Plug-in nécessite que vous créiez des blocs d'adresses IP pour les conteneurs.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > IPAM** dans le panneau de navigation.
- 3 Pour ajouter un bloc d'adresses IP, cliquez sur **Ajouter**.
 - a Entrez un nom et éventuellement une description.
 - b Entrez un bloc d'adresses IP au format CIDR. Par exemple, 10.10.10.0/24.
- 4 Pour modifier un bloc d'adresses IP, cliquez sur le nom d'un bloc d'adresses IP.
 - a Dans l'onglet **Présentation**, cliquez sur **Modifier**.

Vous pouvez modifier le nom, la description ou la valeur d'un bloc d'adresses IP.
- 5 Pour gérer les balises d'un bloc d'adresses IP, cliquez sur le nom d'un bloc d'adresses IP.
 - a Dans l'onglet **Présentation**, cliquez sur **Gérer**.

Vous pouvez ajouter ou supprimer des balises.

6 Pour supprimer un ou plusieurs blocs d'adresses IP, sélectionnez les blocs.

a Cliquez sur **Supprimer**.

Vous ne pouvez pas supprimer un bloc d'adresses IP dont le sous-réseau est alloué.

Gérer des sous-réseaux pour des blocs d'adresses IP

Vous pouvez ajouter ou supprimer des sous-réseaux pour des blocs d'adresses IP.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur *https://<adresse-ip-nsx-manager>*.
- 2 Sélectionnez **Mise en réseau > IPAM** dans le panneau de navigation.
- 3 Cliquez sur le nom d'un bloc d'adresses IP.
- 4 Cliquez sur l'onglet **Sous-réseaux**.
- 5 Pour ajouter un sous-réseau, cliquez sur **Ajouter**.
 - a Entrez un nom et éventuellement une description.
 - b Saisissez la taille du sous-réseau.
- 6 Pour supprimer un ou plusieurs sous-réseaux, sélectionnez les sous-réseaux.
 - a Cliquez sur **Supprimer**.

Une stratégie est une combinaison de règles et de services, qui définit les critères d'accès aux ressources et d'utilisation. Les stratégies NSX vous permettent de gérer l'accès aux ressources et l'utilisation sans vous préoccuper des détails.

Ce chapitre contient les rubriques suivantes :

- [Présentation](#)
- [Ajouter un point d'application](#)
- [Ajouter un service](#)
- [Ajouter un domaine](#)
- [Configurer la sauvegarde de NSX Policy Manager](#)
- [Sauvegarder l'instance de NSX Policy Manager](#)
- [Restaurer NSX Policy Manager](#)
- [Associer un hôte vIDM avec NSX Policy Manager](#)
- [Gérer les attributions de rôles](#)

Présentation

Les stratégies NSX vous permettent de spécifier des règles pour les objets, tels que les machines virtuelles, les ports logiques, les adresses IP et les adresses MAC, sans vous préoccuper des mécanismes des règles. Vous gérez les stratégies dans NSX Policy Manager au lieu de l'instance de NSX Manager.

Avant de configurer des stratégies, vous devez installer NSX Policy Manager. Pour plus d'informations, consultez le *Guide d'installation de NSX-T*. Dans NSX Policy Manager, vous devez également ajouter un ou plusieurs points d'application, afin de fournir des informations sur l'instance de NSX Manager sur laquelle les stratégies seront appliquées.

L'exemple suivant décrit comment utiliser une stratégie pour gérer la mise en réseau d'une application.

L'application a trois niveaux (Web, application et base de données) et vous souhaitez que les règles suivantes s'appliquent aux machines virtuelles de l'application :

- Autoriser le trafic entre la couche Web et la couche d'application.

- Autoriser le trafic entre la couche d'application et la couche de base de données.
- Autoriser le trafic entre n'importe quel système et la couche Web.

Dans l'instance de NSX Manager, procédez comme suit :

- Définissez le nom de la charge de travail des machines virtuelles Web comme Web suivi d'une chaîne d'identification.
- Définissez le nom de la charge de travail des machines virtuelles d'application comme App suivi d'une chaîne d'identification.
- Définissez le nom de la charge de travail des machines virtuelles de base de données comme DB suivi d'une chaîne d'identification.

Dans l'instance de NSX Policy Manager, procédez comme suit :

- Créez un domaine et spécifiez les éléments suivants :
 - Créez un groupe appelé WebGroup constitué de machines virtuelles dont le nom de la charge de travail commence par Web.
 - Créez un groupe appelé AppGroup constitué de machines virtuelles dont le nom de la charge de travail commence par App.
 - Créez un groupe appelé DBGroup constitué de machines virtuelles dont le nom de la charge de travail commence par DB.
 - Spécifiez les stratégies de sécurité qui contrôlent la communication entre les groupes.
- Vérifiez la configuration du domaine pour vous assurer qu'il n'y a aucune erreur.
- Sélectionnez les points d'application.

Une fois que vous avez sélectionné les points d'application, le Gestionnaire de stratégie NSX communique avec NSX Manager qui implémentera les stratégies de sécurité au niveau des points d'application.

Contrôle d'accès basé sur les rôles

NSX Policy Manager comprend deux utilisateurs prédéfinis : `admin` et `audit`. Vous pouvez intégrer NSX Policy Manager avec VMware Identity Manager (vIDM) et configurer le contrôle d'accès en fonction du rôle (RBAC) pour les utilisateurs gérés par vIDM.

Pour les utilisateurs gérés par vIDM, la stratégie d'authentification qui s'applique est celle configurée par l'administrateur vIDM et non la stratégie d'authentification de NSX Policy Manager qui s'applique uniquement aux utilisateurs `admin` et `audit`.

Ajouter un point d'application

Un point d'application est l'entité sur laquelle vous souhaitez appliquer les règles d'une stratégie. Dans cette version, le point d'application doit être une installation NSX-T et NSX Policy Manager prend uniquement en charge un seul point d'application.

Procédure

- 1 À partir de votre navigateur, connectez-vous à NSX Policy Manager à l'adresse <https://adresse-IP-nsx-policy-manager>.
- 2 Dans le panneau de navigation, sélectionnez **Système > Points d'application**.
- 3 Cliquez sur **Ajouter**.
- 4 Fournissez les informations suivantes.

Paramètre	Description
Nom	Nom du point d'application.
Informations d'identification	Nom d'utilisateur et mot de passe pour vous connecter à l'instance de NSX Manager.
Adresse d'application	Adresse IP de l'instance de NSX Manager.
Empreinte numérique	Empreinte numérique de certificat de l'instance de NSX Manager.

- 5 Cliquez sur **Enregistrer**.

Ajouter un service

Un service est un protocole ou un composant logiciel de votre environnement. Une stratégie contient des règles qui s'appliquent aux services.

Les services que vous spécifiez peuvent être par exemple des services FTP, HTTP, de serveur Active Directory, de serveur DHCP, de base de données Oracle, etc.

Procédure

- 1 À partir de votre navigateur, connectez-vous à NSX Policy Manager à l'adresse <https://adresse-IP-nsx-policy-manager>.
- 2 Dans le panneau de navigation, sélectionnez **Infrastructure > Services**.
- 3 Cliquez sur **Ajouter un nouveau service**.
- 4 Entrez le nom du service.
- 5 Cliquez sur **Définir les entrées de service** pour ajouter des entrées de service.
 - a Cliquez sur **Ajouter une nouvelle entrée de Service**.
 - b Sélectionnez un type de service.
Les types disponibles sont **IP**, **IGMP**, **ICMP**, **ALG**, **TCP** et **UDP**.
 - c Cliquez sur la liste déroulante **Propriétés supplémentaires** pour sélectionner une propriété. Vous pouvez ajouter des entrées supplémentaires, ou bien modifier ou supprimer des entrées.
- 6 Cliquez sur **Enregistrer**.

Ajouter un domaine

Un domaine est une collection logique de charges de travail qui servent un objectif métier commun et sur lesquelles vous souhaitez appliquer des stratégies. Il contient un ensemble de groupes et leur configuration correspondante en matière de communication.

Si vous prévoyez de créer plusieurs domaines volumineux (chacun avec plus de 200 règles résultantes), veillez à les déployer sur les points d'application de manière séquentielle, en attendant la réalisation de chaque domaine avant de procéder à la suivante. Si vous déployez ces domaines à l'aide de l'API, il est recommandé que les entrées de communication soient créées avant qu'un domaine soit déployé sur un point d'application.

Procédure

- 1 À partir de votre navigateur, connectez-vous à NSX Policy Manager à l'adresse `https://adresse-IP-nsx-policy-manager`.
- 2 Dans le panneau de navigation, sélectionnez **Infrastructure > Domaines**.
- 3 Cliquez sur **Ajouter un domaine** pour ajouter un domaine.
- 4 Spécifiez un nom pour le domaine et une description facultative.
- 5 Cliquez sur **Suivant** pour passer à l'étape Groupes de charges de travail.
- 6 Cliquez sur **Ajouter un groupe** pour ajouter un ou plusieurs groupes de charges de travail. Pour chaque groupe de charges de travail,
 - a Spécifiez un nom.
 - b Cliquez sur le champ **Type des membres** pour sélectionner le type des membres.
Les choix disponibles sont **Machine virtuelle**, **Adresse IP** et **Critères d'appartenance**.
 - c Pour **Machine virtuelle** et **Adresse IP**, spécifiez une valeur.
 - d Pour **Critères d'appartenance**, cliquez sur **Définir les critères d'appartenance** pour spécifier la façon dont les membres sont sélectionnés.
- 7 Cliquez sur **Suivant** pour passer à l'étape Sécurité.
- 8 Cliquez sur **Ajouter une nouvelle section** pour ajouter une section de pare-feu ou **Ajouter une nouvelle règle** pour ajouter une règle de pare-feu.
Vous pouvez ajouter plusieurs sections et règles :
- 9 Cliquez sur **Suivant** pour passer à l'étape Vérifier la configuration du domaine.
Une représentation graphique du domaine s'affiche.
- 10 Cliquez sur **Suivant** pour accéder à l'étape Sélectionner les points d'application.
- 11 Sélectionnez un ou plusieurs points d'application.
- 12 Cliquez sur **Terminer** pour déployer le domaine.

Configurer la sauvegarde de NSX Policy Manager

Vous pouvez sauvegarder NSX Policy Manager afin de protéger les données qu'il stocke. Avant de pouvoir effectuer une sauvegarde, vous devez configurer les propriétés de sauvegarde.

Conditions préalables

Vérifiez que vous disposez de l'empreinte digitale SSH du serveur de fichiers de sauvegarde. Seule une clé ECDSA avec hachage SHA256 est acceptée comme empreinte digitale. Reportez-vous à la section [Rechercher l'empreinte digitale SSH d'un serveur distant](#).

Procédure

- 1 À partir de votre navigateur, connectez-vous à NSX Policy Manager à l'adresse `https://adresse-IP-nsx-policy-manager`.
- 2 Sélectionnez **Système > Utilitaires** dans le panneau de navigation.
- 3 Cliquez sur **Configurer**.
- 4 Cliquez sur le bouton bascule **Sauvegarde automatique** pour activer ou désactiver les sauvegardes automatiques.
- 5 Entrez l'adresse IP ou le nom d'hôte du serveur de fichiers de sauvegarde.
- 6 Modifiez le port par défaut, si nécessaire.
- 7 Entrez le nom d'utilisateur et le mot de passe requis pour vous connecter au serveur de fichiers de sauvegarde.
- 8 Dans le champ **Répertoire de destination**, entrez le chemin de répertoire absolu d'enregistrement des sauvegardes.
Le répertoire doit déjà exister.
- 9 Entrez la phrase secrète utilisée pour chiffrer les données sauvegardées.
Vous aurez besoin de cette phrase secrète pour restaurer une sauvegarde. Si vous oubliez la phrase secrète de sauvegarde, vous ne pouvez restaurer aucune sauvegarde.
- 10 Entrez l'empreinte digitale SSH du serveur qui stocke les sauvegardes. Reportez-vous à la section [Rechercher l'empreinte digitale SSH d'un serveur distant](#).
- 11 Cliquez sur l'onglet **Planification**.
- 12 Sélectionnez la fréquence.
Si vous sélectionnez **Hebdomadaire**, spécifiez le jour de la semaine et l'heure. Si vous sélectionnez **Intervalle**, spécifiez l'intervalle.
- 13 Cliquez sur **Enregistrer**.

Sauvegarder l'instance de NSX Policy Manager

Vous pouvez sauvegarder l'instance de NSX Policy Manager automatiquement ou manuellement.

Si vous avez configuré les sauvegardes automatiques, elles seront effectuées automatiquement. La procédure suivante décrit le démarrage manuel d'une sauvegarde.

Conditions préalables

Vérifiez que vous avez configuré les propriétés de sauvegarde. Reportez-vous à la section [Configurer la sauvegarde de NSX Policy Manager](#).

Procédure

- 1 À partir de votre navigateur, connectez-vous à NSX Policy Manager à l'adresse `https://adresse-IP-nsx-policy-manager`.
- 2 Sélectionnez **Système > Utilitaires** dans le panneau de navigation.
- 3 Cliquez sur **Sauvegarder maintenant**.

Restaurer NSX Policy Manager

Vous pouvez restaurer NSX Policy Manager à un état passé à partir d'une sauvegarde.

Conditions préalables

Vérifiez que vous disposez de l'empreinte digitale SSH du serveur de fichiers de sauvegarde. Seule une clé ECDSA avec hachage SHA256 est acceptée comme empreinte digitale. Reportez-vous à la section [Rechercher l'empreinte digitale SSH d'un serveur distant](#).

Procédure

- 1 À partir de votre navigateur, connectez-vous à NSX Policy Manager à l'adresse `https://adresse-IP-nsx-policy-manager`.
- 2 Sélectionnez **Système > Utilitaires** dans le panneau de navigation.
- 3 Cliquez sur **Restaurer maintenant**.
- 4 Confirmez la réception du message sur les conditions préalables et les risques, puis cliquez sur **Suivant**.
- 5 Entrez l'adresse IP ou le nom d'hôte du serveur de sauvegarde.
- 6 Le cas échéant, modifiez le numéro du port.
La valeur par défaut est 22.
- 7 Entrez le nom d'utilisateur et le mot de passe pour vous connecter au serveur.
- 8 Dans le champ **Répertoire de sauvegarde**, entrez le chemin de répertoire absolu dans lequel les sauvegardes sont stockées.
- 9 Entrez la phrase secrète utilisée pour chiffrer les données sauvegardées.
- 10 Entrez l'empreinte digitale SSH du serveur de sauvegarde.
- 11 Cliquez sur **Suivant**.

12 Sélectionnez une sauvegarde.

13 Cliquez sur **Restaurer**.

L'état de l'opération de restauration s'affiche. Si vous avez supprimé ou ajouté des nœuds d'infrastructure ou des nœuds de transport depuis la sauvegarde, vous serez invité à effectuer certaines actions, par exemple, ouvrir une session sur un nœud et exécuter un script.

Une fois l'opération de restauration terminée, l'écran Restauration terminée s'affiche, indiquant le résultat de la restauration, l'horodatage du fichier de sauvegarde et les heures de début et de fin de l'opération de restauration. Si la restauration échoue, l'écran affiche l'étape où l'échec s'est produit. Pour tenter à nouveau l'opération de restauration, vous devez utiliser un nouveau dispositif Gestionnaire de stratégie et non celui où l'échec s'est produit.

Associer un hôte vIDM avec NSX Policy Manager

Pour activer l'intégration de NSX Policy Manager à vIDM, vous devez fournir des informations sur l'hôte vIDM.

Le serveur vIDM doit disposer d'un certificat signé par une autorité de certification (CA). Dans le cas contraire, il se peut que la connexion à vIDM à partir de NSX Policy Manager ne fonctionne pas avec certains navigateurs, tels que Microsoft Edge ou Internet Explorer 11. Pour plus d'informations sur l'installation d'un certificat signé par une autorité de certification sur vIDM, reportez-vous à la section <https://docs.vmware.com/fr/VMware-Identity-Manager/3.1/vidm-install/GUID-B76761BF-4B12-4CD5-9366-B0A1A2BF2A8B.html>.

Lorsque vous enregistrez NSX Policy Manager auprès de vIDM, vous spécifiez une URI de redirection qui pointe vers NSX Policy Manager. Vous pouvez indiquer le nom de domaine complet ou l'adresse IP. Il est important de se souvenir si vous utilisez le nom de domaine complet ou l'adresse IP. Lorsque vous essayez de vous connecter à Policy Manager via vIDM, vous devez spécifier le nom d'hôte dans l'URL de la même manière, c'est-à-dire, si vous utilisez le nom de domaine complet lors de l'enregistrement du gestionnaire dans vIDM, vous devez utiliser le nom de domaine complet dans l'URL, et si vous utilisez l'adresse IP lors de l'enregistrement du gestionnaire dans vIDM, vous devez utiliser l'adresse IP dans l'URL. Dans le cas contraire, la connexion échouera.

Conditions préalables

- Vérifiez que vous disposez de l'empreinte numérique du certificat de l'hôte vIDM. Reportez-vous à la section [Obtenir l'empreinte numérique de certificat à partir d'un hôte vIDM](#).
- Vérifiez que NSX Policy Manager est enregistré en tant que client OAuth sur l'hôte vIDM. Lors du processus d'enregistrement, notez l'identifiant de client et le secret de client. Pour plus d'informations, consultez la documentation de VMware Identity Manager à l'adresse <https://www.vmware.com/support/pubs/identitymanager-pubs.html>.

Procédure

- 1 À partir de votre navigateur, connectez-vous à NSX Policy Manager à l'adresse `https://adresse-IP-nsx-policy-manager`.

- 2 Sélectionnez **Système > Utilisateurs** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Configuration**.
- 4 Cliquez sur **Modifier**.
- 5 Faites basculer le bouton **Intégration de VMware Identity Manager** sur **Activé**.
- 6 Fournissez les informations suivantes.

Paramètre	Description
Dispositif VMware Identity Manager	Nom de domaine complet (FQDN) de l'hôte vIDM.
ID de client OAuth	ID créé lors de l'enregistrement de NSX Policy Manager sur l'hôte vIDM.
Secret du client OAuth	Code secret créé lors de l'enregistrement de NSX Policy Manager sur l'hôte vIDM.
Empreinte numérique SHA-256	Empreinte numérique du certificat de l'hôte vIDM.
Dispositif de stratégie NSX	Adresse IP ou nom de domaine complet (FQDN) de NSX Policy Manager. Si vous spécifiez un nom de domaine complet, vous devez accéder à NSX Policy Manager à partir d'un navigateur à l'aide du nom de domaine complet du gestionnaire de l'URL, et si vous spécifiez une adresse IP, vous devez utiliser l'adresse IP de l'URL. L'administrateur vIDM peut également configurer le client NSX Policy Manager pour que vous puissiez vous connecter en utilisant le nom de domaine complet ou l'adresse IP.

- 7 Cliquez sur **Enregistrer**.

Gérer les attributions de rôles

Vous pouvez ajouter, modifier et supprimer des attributions de rôles à des utilisateurs ou des groupes d'utilisateurs si VMware Identity Manager est intégré à NSX Policy Manager.

Les rôles suivants sont prédéfinis. Vous ne pouvez pas ajouter de nouveaux rôles.

- Administrateur d'entreprise
- Auditeur
- Ingénieur de fiabilité du site (disponible dans un déploiement cloud de VMware)
- Administrateur de service cloud (disponible dans un déploiement cloud de VMware)
- Auditeur de service cloud (disponible dans un déploiement cloud de VMware)

Conditions préalables

- Vérifiez qu'un hôte vIDM est associé avec NSX Policy Manager. Pour plus d'informations, consultez [Associer un hôte vIDM avec NSX Policy Manager](#).

Procédure

- 1 À partir de votre navigateur, connectez-vous à NSX Policy Manager à l'adresse `https://adresse-IP-nsx-policy-manager`.
- 2 Sélectionnez **Système > Utilisateurs** dans le panneau de navigation.

- 3 Cliquez sur l'onglet **Attributions de rôles** s'il n'est pas déjà sélectionné.
- 4 Ajoutez, modifiez ou supprimez des attributions de rôles.

Option	Actions
Ajouter des attributions de rôles	Cliquez sur Ajouter , sélectionnez des utilisateurs ou des groupes d'utilisateurs et sélectionnez des rôles.
Modifier des attributions de rôles	Sélectionnez un utilisateur ou un groupe d'utilisateurs, et cliquez sur Modifier .
Supprimer des attributions de rôles	Sélectionnez un utilisateur ou un groupe d'utilisateurs, et cliquez sur Supprimer .

Insertion de services

15

Avec l'insertion de services, vous pouvez appliquer des services tiers au trafic nord-sud, ainsi qu'au trafic est-ouest qui passe à travers un routeur. Les services fournissent généralement des fonctionnalités de sécurité avancées comme un système de détection des intrusions (IDS) ou un système de prévention des intrusions (IPS).

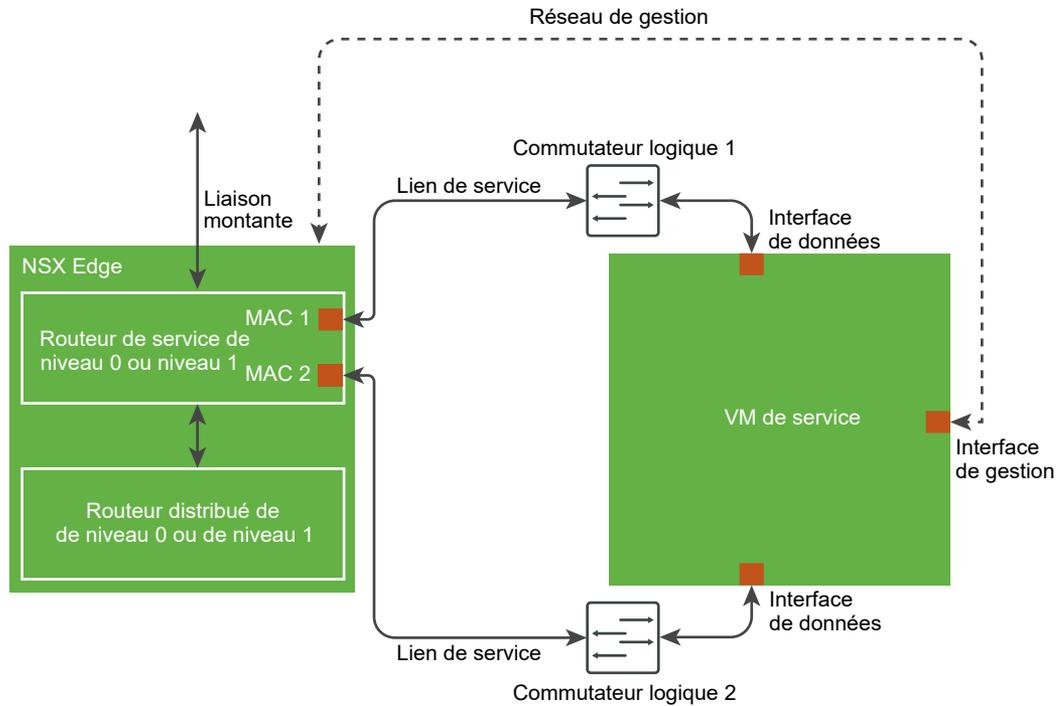
Ce chapitre contient les rubriques suivantes :

- [Présentation](#)
- [Enregistrer un service](#)
- [Déployer une instance de service](#)
- [Configurer la redirection du trafic](#)
- [Surveiller la redirection du trafic](#)

Présentation

Vous pouvez configurer l'insertion de services pour rediriger le trafic nord-sud au niveau d'un routeur de niveau 0 ou le trafic est-ouest au niveau d'un routeur de niveau 1 à une machine virtuelle. Un service en cours d'exécution dans la machine virtuelle peut traiter le trafic et effectuer les actions appropriées.

Le diagramme architectural suivant montre le flux de données avec l'insertion de services configurée.



L'insertion de services prend en charge la haute disponibilité (HA) en mode actif-veille avec deux nœuds Edge et deux machines virtuelles de service. Elle ne prend pas en charge la HA en mode actif-actif. Un routeur ne peut prendre en charge qu'un seul service.

La configuration d'insertion de services implique les étapes suivantes :

- Enregistrer un service.
- Déployer une instance de service.
- Configurer la redirection du trafic.

Enregistrer un service

L'enregistrement d'un service nécessite un appel API. Une fois qu'un service est enregistré, vous pouvez l'afficher dans l'interface utilisateur de NSX Manager.

Vous trouverez des détails sur l'appel API et les paramètres d'entrée dans la *Référence de l'API de NSX-T Data Center*.

Procédure

- 1 Effectuez l'appel API suivant pour enregistrer un service :

```
POST /api/v1/serviceinsertion/services
```

Par exemple,

```
POST https://<nsx-mgr>/api/v1/serviceinsertion/services
{
  "display_name": "NS Service for ABC partner",
  "description": "This service is inserted at T0 router and it provides advanced security",
  "attachment_point": [
    "TIER0_LR"
  ],
  "functionalities": [
    "NG_FW"
  ],
  "implementations": [
    "NORTH_SOUTH"
  ],
  "transports": [
    "L2_BRIDGE"
  ],
  "vendor_id": "ABC_Partner",
  "on_failure_policy": "ALLOW",
  "service_deployment_spec": {
    "deployment_specs": [{
      "ovf_url": "http://server.com/dir1/ABC-Company-HA-OVF/ABC-VM-ESX-2.0.ovf",
      "name": "NS_DepSpec",
      "host_type": "ESXI",
      "service_form_factor": "MEDIUM"
    }],
    "nic_metadata_list": [
      {
        "interface_label": "eth",
        "interface_index": 0,
        "interface_type": "MANAGEMENT"
      },
      {
        "interface_label": "eth",
        "interface_index": 1,
        "interface_type": "DATA1"
      },
      {
        "interface_label": "eth",
        "interface_index": 2,
        "interface_type": "DATA2"
      }
    ],
    "deployment_template": [{
      "name": "NS_DepTemp",
      "attributes": [{
        "attribute_type": "STRING",
        "display_name": "License",
        "key": "LicenseKey"
      }]
    }]
  }
}
```

- 2 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 3 Sélectionnez **Services de partenaires** dans le panneau de navigation.
- 4 Cliquez sur l'onglet **Catalogue** et assurez-vous que le service est enregistré.

Étape suivante

Déployez une instance du service. Reportez-vous à la section [Déployer une instance de service](#).

Déployer une instance de service

Après l'enregistrement d'un service, vous devez déployer une instance de service pour ce service afin de démarrer le traitement du trafic réseau.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Services de partenaires** dans le panneau de navigation.
- 3 Cliquez sur **Déployer**.
- 4 Entrez un nom d'instance et éventuellement une description.
- 5 Cliquez sur le champ **Service de partenaires** et sélectionnez un service.
- 6 Sélectionnez une **Spécification de déploiement**.
- 7 Sélectionnez un routeur logique.
Seuls les routeurs qui ne disposent pas d'insertion de service configurée s'afficheront.
- 8 Cliquez sur **Suivant**.
- 9 Cliquez sur le champ **Gestionnaire de calcul** et sélectionnez un gestionnaire de calcul.
- 10 Cliquez sur le champ **Cluster** et sélectionnez un cluster.
- 11 (Facultatif) Cliquez sur le champ **Pool de ressources** et sélectionnez un pool de ressources s'il a été configuré dans vCenter Server.
- 12 Cliquez sur le champ **Banque de données** et sélectionnez une banque de données.
- 13 Sélectionnez un **Mode de déploiement**.
Les options disponibles sont **Autonome** ou **Haute disponibilité**.
- 14 Sélectionnez une **Stratégie en cas de panne**.
Les options disponibles sont **Autoriser** ou **Bloquer**.
- 15 Entrez l'adresse IP de la machine virtuelle.
- 16 Entrez la passerelle par défaut pour l'adresse IP de la machine virtuelle.

17 Entrez le masque de sous-réseau pour l'adresse IP de la machine virtuelle.

18 Cliquez sur **Suivant**.

19 Sélectionnez un **Modèle de déploiement**.

20 Entrez une licence pour le service de partenaires.

21 Cliquez sur **Terminer**.

Résultats

Le processus de déploiement peut prendre un certain temps, en fonction de la mise en œuvre du fournisseur. Vous pouvez afficher l'état dans l'interface utilisateur du gestionnaire. Lorsque le déploiement réussit, l'état passe à `Déploiement effectué`.

Étape suivante

Configurer la redirection du trafic pour l'instance de service. Reportez-vous à la section [Configurer la redirection du trafic](#).

Configurer la redirection du trafic

Après avoir déployé une instance de service, vous pouvez configurer le type de trafic que le routeur redirige vers le service. La configuration de la redirection du trafic est semblable à la configuration d'un pare-feu.

Pour plus d'informations sur la configuration d'un pare-feu, reportez-vous à la section [Chapitre 7 Sections de pare-feu et règles de pare-feu](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Services de partenaires** dans le panneau de navigation.
- 3 Cliquez sur le nom d'une instance de service.
- 4 Cliquez sur l'onglet **Redirection du trafic**.
- 5 Ajoutez ou supprimez des sections et des règles.

Surveiller la redirection du trafic

Après avoir déployé une instance de service et configuré la redirection du trafic, vous pouvez surveiller la quantité de trafic qui entre dans l'instance de service et qui en sort.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Services de partenaires** dans le panneau de navigation.

3 Cliquez sur le nom d'une instance de service.

L'onglet **Présentation** affiche la configuration et l'état de l'instance de service.

4 Cliquez sur l'onglet **Statistiques**.

Des informations sur le nombre de paquets et la quantité de données qui entre dans l'instance de service et qui en sort s'affichent.

5 Cliquez sur **Actualiser** pour mettre à jour les statistiques.

NSX Cloud vous permet de gérer et de sécuriser l'inventaire de votre cloud public à l'aide de NSX-T Data Center.

Reportez-vous à la section [Architecture et composants de NSX Cloud](#) dans le *Guide d'installation de NSX-T Data Center* pour obtenir la liste et la description des composants de NSX Cloud.

Ce chapitre contient les rubriques suivantes :

- [Cloud Service Manager](#)
- [Gérer la stratégie de mise en quarantaine](#)
- [Présentation de l'intégration et la gestion des machines virtuelles de charge de travail](#)
- [Intégrer les machines virtuelles de charge de travail](#)
- [Gérer les machines virtuelles de charge de travail](#)
- [Utilisation des fonctionnalités avancées de NSX Cloud](#)
- [Dépannage](#)

Cloud Service Manager

Cloud Service Manager (CSM) fournit un point de terminaison de gestion à écran unique pour l'inventaire de votre cloud public.

L'interface CSM est divisée dans les catégories suivantes :

- **Recherche** : vous pouvez utiliser la zone de texte Rechercher pour rechercher des comptes de cloud public ou des constructions associées.
- **Clouds** : votre inventaire de cloud public est géré par le biais des sections sous cette catégorie.
- **Système** : vous pouvez accéder à **Paramètres**, **Utilitaires** et **Utilisateurs** pour Cloud Service Manager depuis cette catégorie.

Vous pouvez effectuer toutes les opérations de cloud public en accédant à la sous-section **Clouds** de CSM.

Pour effectuer des opérations système, telles que sauvegarde, restauration, mise à niveau et gestion des utilisateurs, accédez à la sous-section **Système**.

Clouds

Voici les sections sous **Clouds** :

Clouds > Présentation

Accédez à votre compte de cloud public en cliquant sur **Clouds**.

Présentation : chaque vignette sur cet écran représente votre compte de cloud public avec le nombre de comptes, de régions, de VPC ou de VNet, et d'instances (machines virtuelles de charge de travail) qu'il contient.

Vous pouvez effectuer les tâches suivantes :

Ajouter un compte ou abonnement de cloud public	<p>Vous pouvez ajouter un ou plusieurs comptes ou abonnements de cloud public. Cela vous permet d'afficher votre inventaire de cloud public dans CSM ainsi que le nombre de machines virtuelles gérées par NSX-T Data Center et leur état.</p> <p>Reportez-vous à Ajouter votre compte de cloud public dans le document <i>Guide d'installation de NSX-T Data Center</i> pour obtenir des instructions détaillées.</p>
Déployer/Annuler le déploiement de NSX Public Cloud Gateway	<p>Vous pouvez déployer ou annuler le déploiement d'une ou deux instances de PCG (pour la haute disponibilité). Vous pouvez également annuler le déploiement de PCG à partir de CSM.</p> <p>Pour obtenir des instructions détaillées, reportez-vous à Déployer PCG ou Annuler le déploiement de PCG dans le document <i>Guide d'installation de NSX-T Data Center</i>.</p>
Activer ou désactiver la stratégie de mise en quarantaine	<p>Vous pouvez activer ou désactiver la stratégie de mise en quarantaine. Reportez-vous à Gérer la stratégie de mise en quarantaine pour plus de détails.</p>
Basculer entre la vue de grille et de carte	<p>Les cartes affichent un aperçu de votre inventaire. La grille affiche plus de détails. Cliquez sur les icônes pour basculer entre les types de vues.</p>

CSM fournit une vue globale de tous vos comptes de cloud public que vous avez connectés avec NSX Cloud en présentant votre inventaire de cloud public de différentes manières :

- Vous pouvez afficher le nombre de zones dans lesquelles vous opérez.
- Vous pouvez afficher le nombre de réseaux privés par région.
- Vous pouvez afficher le nombre de machines virtuelles de charge de travail par réseau privé.

Il y a quatre onglets sous **Clouds**.

Consultez aussi [Diagrammes et icônes de CSM](#) pour une description des éléments de l'interface utilisateur.

Clouds > {Votre Cloud Public} > Comptes

La section Comptes de CSM fournit des informations sur les comptes de cloud public que vous avez déjà ajoutés.

Chaque carte représente un compte de cloud public du fournisseur de cloud que vous avez sélectionné dans Clouds.

Vous pouvez effectuer les actions suivantes à partir de cette section :

- Ajouter un compte
- Modifier un compte
- Supprimer un compte
- Resynchroniser un compte

Clouds > {Votre cloud public} > Régions

La section Régions affiche votre inventaire pour une région sélectionnée.

Vous pouvez filtrer les régions selon votre compte de cloud public. Chaque région a des VPC ou des VNet, et des instances. Si vous avez déployé des PCG, vous pouvez les voir ici en tant que passerelles avec un indicateur de la santé des PCG.

Clouds > {Votre Cloud Public}> VPC ou VNet

La section VPC ou VNet affiche l'inventaire de votre cloud privé.

Vous pouvez filtrer l'inventaire par compte et par région.

- Chaque carte représente un VPC ou un VNet.
- Vous pouvez disposer d'une ou deux (pour HA) instances de PCG déployées sur chaque VPC ou VNet.
- Vous pouvez afficher plus de détails pour chaque VPC ou VNet en basculant vers la vue grille.
- Cliquez sur **Actions** pour accéder à ce qui suit :
 - **Modifier la configuration** :
 - Activez ou désactivez la stratégie de quarantaine.
 - Modifiez votre sélection de serveur proxy.
 - **Déployer une passerelle NSX Cloud** : cliquez sur cette option pour démarrer le déploiement de PCG sur ce VPC ou ce VNet. Si une PCG ou une paire HA de PCG est déjà déployée, cette option n'est pas disponible. Reportez-vous à **Déployer PCG** dans le document *Guide d'installation de NSX-T Data Center* pour obtenir des instructions détaillées.

Clouds > {votre Cloud Public} > Instances

La section Instances affiche les détails des instances de votre VPC ou VNet.

Vous pouvez filtrer l'inventaire des instances par compte, par région, et par VPC ou VNet.

Chaque carte représente une instance (machine virtuelle de charge de travail) et affiche un résumé.

Pour plus d'informations sur l'instance, cliquez sur la carte ou basculez vers la vue grille.

Note CSM affiche la valeur de version du système d'exploitation pour les machines virtuelles gérées par NSX, mais pour les machines virtuelles non gérés par NSX, le type du système d'exploitation est indiqué avec le minimum de détails, car il est obtenu à partir des API du fournisseur de cloud.

Diagrammes et icônes de CSM

CSM affiche l'état et la santé de vos constructions de cloud public à l'aide d'icônes descriptives et intuitives.

Note Les workflows de mise en quarantaine s'appliquent uniquement lorsque le paramètre **Activer la mise en quarantaine** est activé. Il est désactivé par défaut.

Réseaux virtuels

Figure 16-1. Réseau virtuel avec des machines virtuelles saines gérées par NSX Cloud

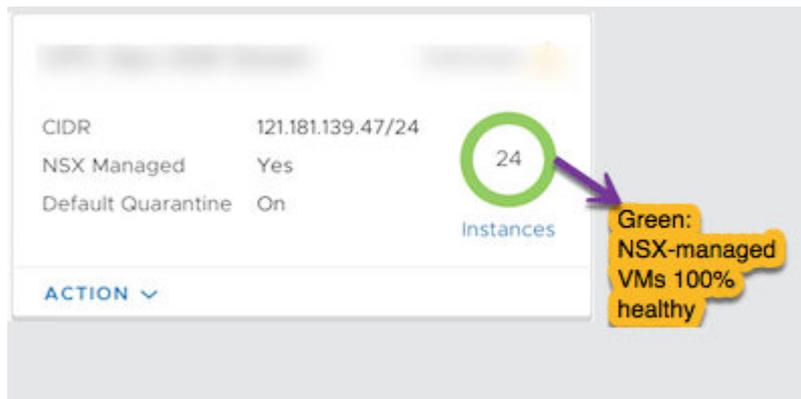


Figure 16-2. Réseau virtuel avec des machines virtuelles gérées par NSX Cloud qui comportent des erreurs

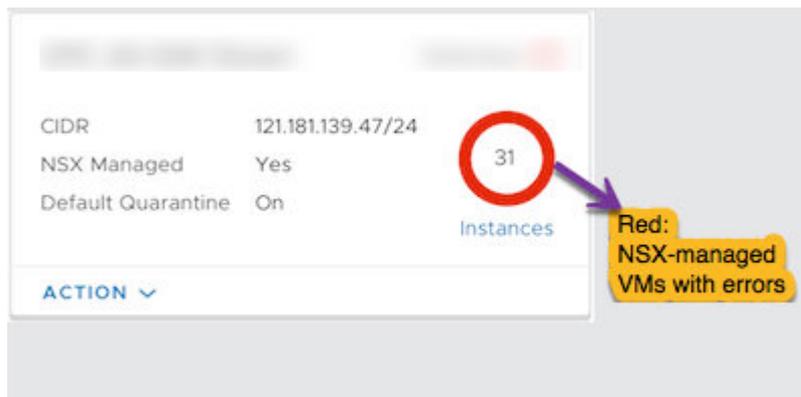


Figure 16-3. Réseau virtuel comportant des machines virtuelles hors tension

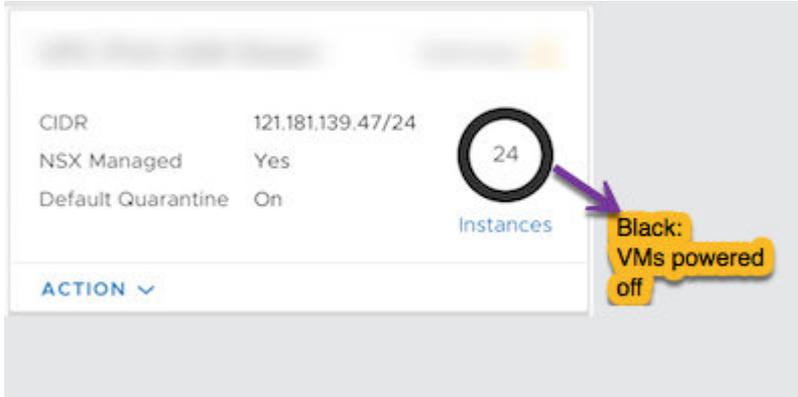


Figure 16-4. Réseau virtuel affichant l'état de mise en quarantaine par défaut

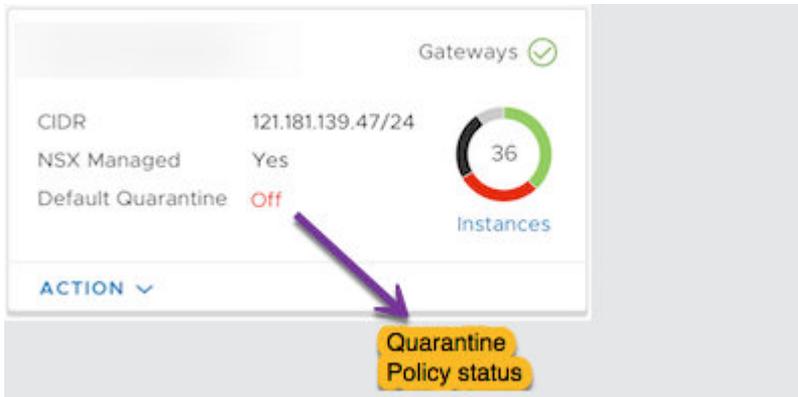
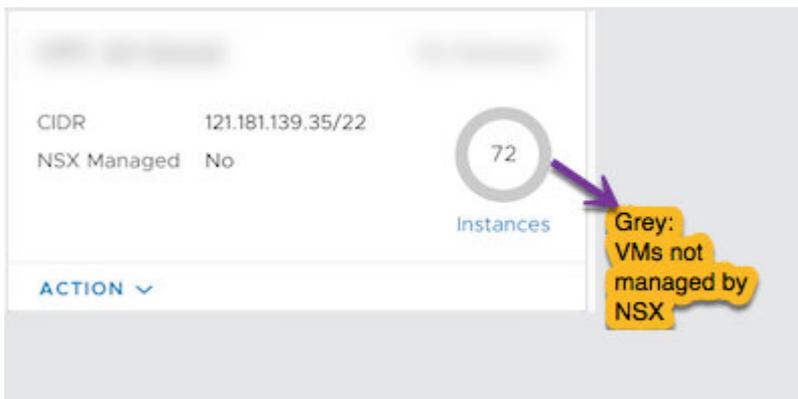


Figure 16-5. Réseau virtuel avec des machines virtuelles non gérées par NSX Cloud



Instances

Instances gérées

Figure 16-6. Instance saine gérée par NSX Cloud

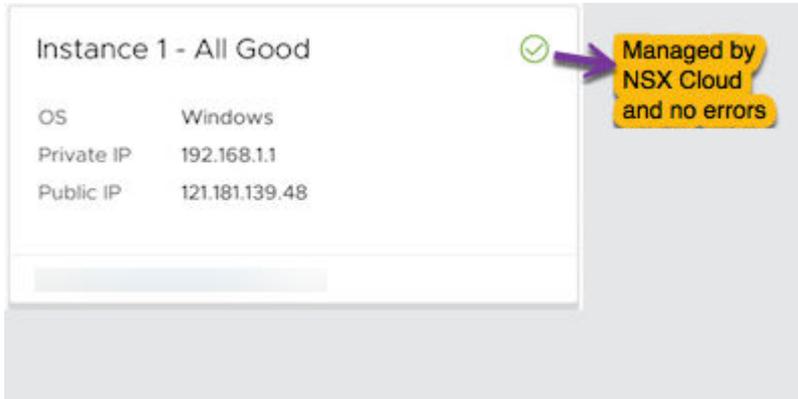


Figure 16-7. Instance gérée par NSX Cloud qui comporte des erreurs

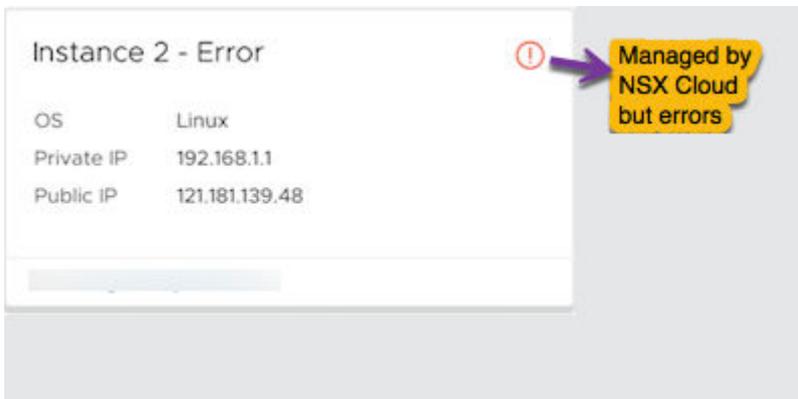


Figure 16-8. Instance gérée par NSX Cloud qui comporte des erreurs et mise en quarantaine

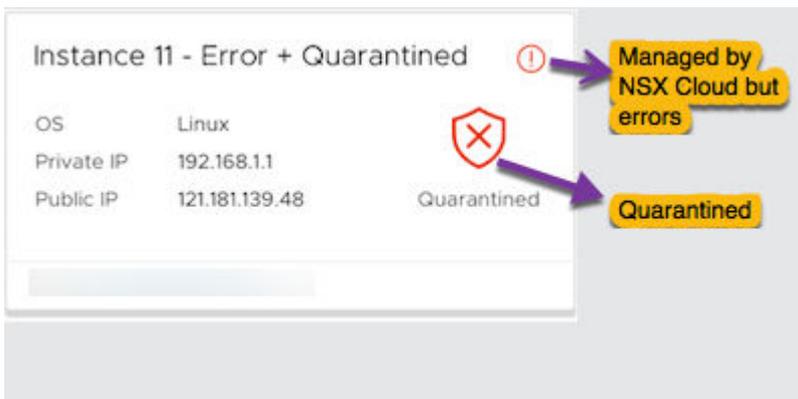


Figure 16-9. Instance gérée par NSX Cloud qui est mise en quarantaine, mais qui est mise sur liste blanche du fait que le groupe de sécurité réseau **vm-override-sg** lui est appliqué

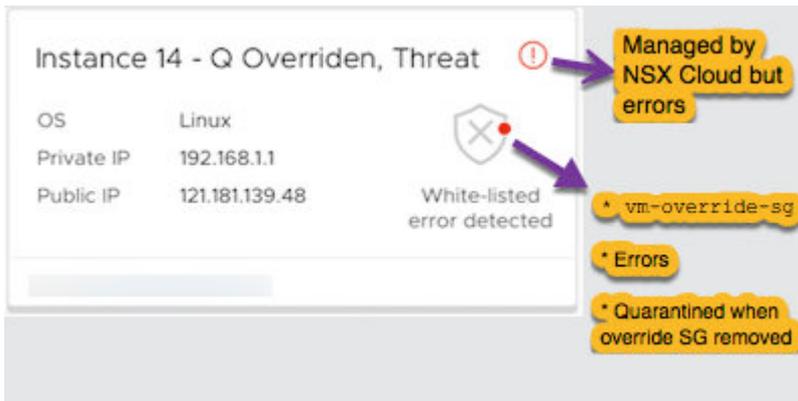
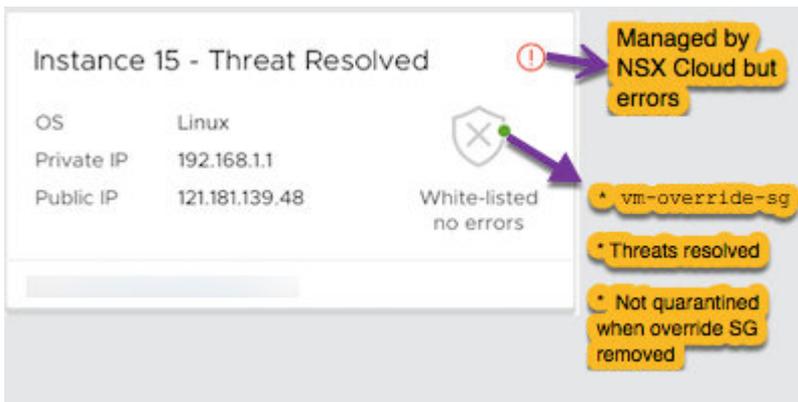


Figure 16-10. Instance gérée par NSX Cloud mise en quarantaine et sur liste blanche avec des erreurs résolues.



Instances non gérées

Figure 16-11. Machine virtuelle non gérée par NSX Cloud et mise en quarantaine par défaut

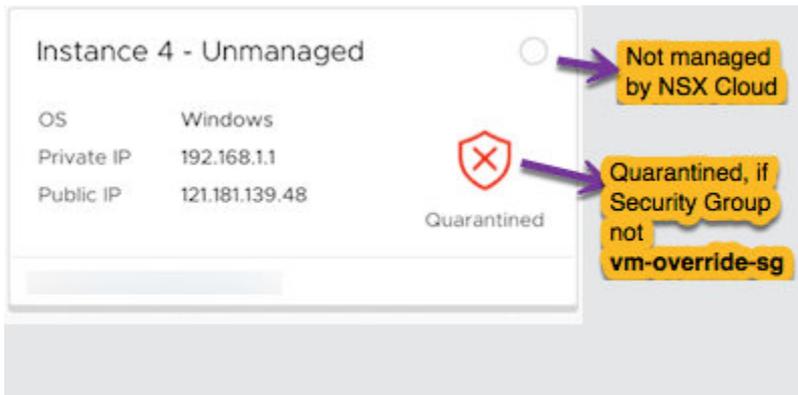
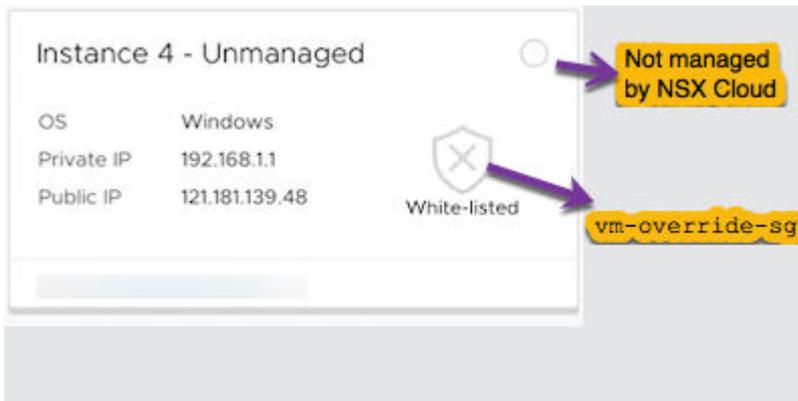


Figure 16-12. VM non gérée par NSX Cloud, mais mise en liste blanche du fait que **vm-override-sg** lui est appliqué



Public Cloud Gateway (PCG)

Figure 16-13. Réseau virtuel dont l'instance de PCG principale et secondaire est active

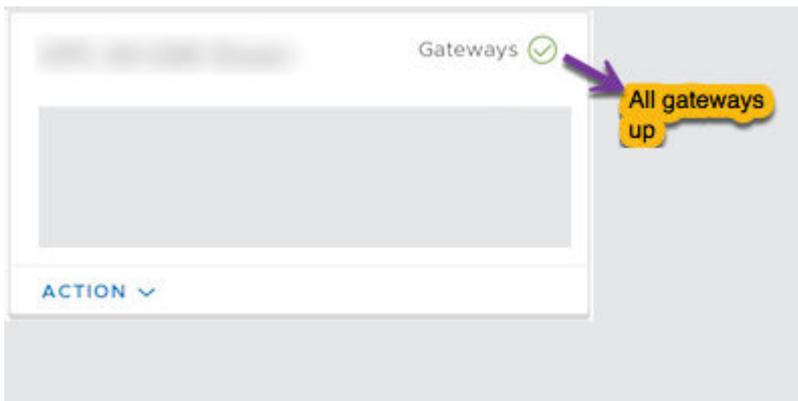


Figure 16-14. Réseau virtuel dont l'instance de PCG principale ou secondaire est inactive

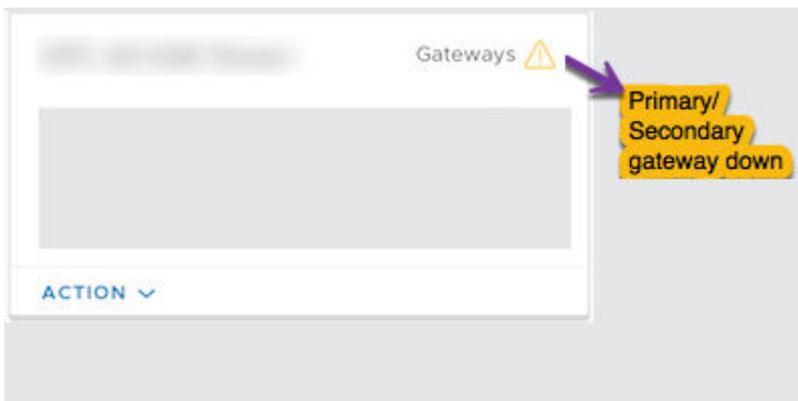
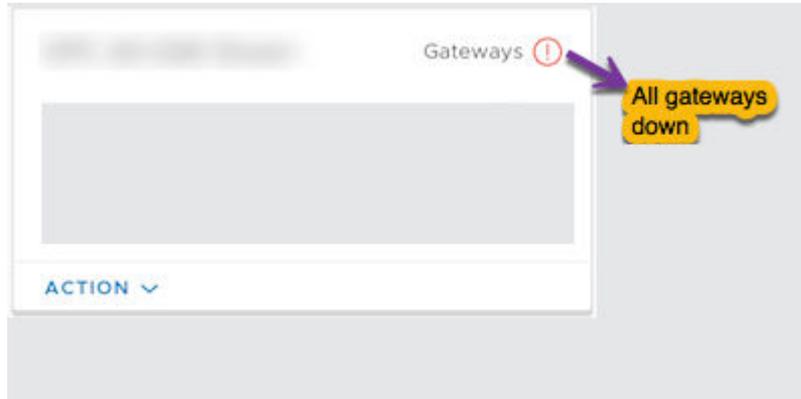


Figure 16-15. Réseau virtuel dont l'instance de PCG principale et secondaire est inactive



Systeme

Voici les sections sous **Systeme** :

Systeme > Parametres

Ces parametres sont configurés pour la première fois lors de l'installation de CSM. Vous pouvez les modifier par la suite.

Joindre CSM avec NSX Manager

Vous devez connecter le dispositif CSM à NSX Manager pour autoriser ces composants à communiquer entre eux.

Conditions préalables

- NSX Manager doit être installé et vous devez disposer des privilèges d'administrateur pour vous connecter à NSX Manager
- CSM doit être installé et vous devez disposer du rôle d'administrateur d'entreprise dans CSM.

Procédure

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

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

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

- 3 Connectez-vous à CSM avec le rôle d'administrateur d'entreprise.
- 4 Cliquez sur **Systeme > Parametres**. Puis, cliquez sur **Configurer** dans le panneau **Nœud NSX associé**.

Note Vous pouvez également fournir ces détails lors de l'utilisation de l'assistant de configuration de CSM qui est disponible lors de l'installation initiale de CSM.

5 Entrez les détails du dispositif NSX Manager.

Option	Description
Nom d'hôte de NSX Manager	Entrez le nom de domaine complet (FQDN) du dispositif NSX Manager, s'il est disponible. Vous pouvez également entrer l'adresse IP de NSX Manager.
Identifiants de l'administrateur	Entrez un nom d'utilisateur disposant du rôle d'administrateur d'entreprise et le mot de passe correspondant.
Empreinte numérique du responsable	Entrez la valeur de l'empreinte numérique du dispositif NSX Manager que vous avez obtenue à l'étape 2.

6 Cliquez sur **Connecter**.

CSM vérifie l'empreinte numérique du dispositif NSX Manager et établit la connexion.

(Facultatif) Configurer les serveurs Proxy

Si vous souhaitez router et surveiller l'ensemble du trafic HTTP/HTTPS dédié à Internet via un proxy HTTP fiable, vous pouvez configurer jusqu'à cinq serveurs proxy dans CSM.

Toutes les communications du cloud public depuis PCG et CSM sont acheminées via le serveur proxy sélectionné.

Les paramètres de proxy de PCG sont indépendants des paramètres de proxy de CSM. Vous pouvez choisir de n'avoir aucun serveur proxy ou un serveur proxy différent pour PCG.

Vous pouvez choisir les niveaux d'authentification suivants :

- Authentification par informations d'identification.
- Authentification par certificat pour l'interception HTTPS.
- Aucune authentification.

Procédure

- 1 Cliquez sur **Système > Paramètres**. Puis, cliquez sur **Configurer** sur le panneau **Serveurs proxy**.

Note Vous pouvez également fournir ces détails lors de l'utilisation de l'assistant de configuration de CSM qui est disponible lors de l'installation initiale de CSM.

- 2 Dans l'écran Configurer les serveurs proxy, entrez les informations suivantes :

Option	Description
Par défaut	Utilisez cette case d'option pour indiquer le serveur proxy par défaut.
Nom du profil	Fournissez un nom de profil de serveur proxy. Cette information est obligatoire.
Serveur proxy	Entrez l'adresse IP du serveur proxy. Cette information est obligatoire.
Port	Entrez le port du serveur proxy. Cette information est obligatoire.
Authentification	Facultative. Si vous souhaitez configurer une authentification supplémentaire, cochez cette case et fournissez un nom d'utilisateur et un mot de passe valides.
Nom d'utilisateur	Ceci est nécessaire si vous cochez la case Authentification.

Option	Description
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.

Systeme > Utilitaires

Les utilitaires suivants sont disponibles.

Sauvegarde et restauration

Suivez les mêmes instructions pour la sauvegarde et la restauration de CSM, comme pour NSX Manager. Reportez-vous à [Sauvegarde et restauration de NSX Manager](#) pour plus de détails.

Bundle de support

Cliquez sur **Télécharger** pour récupérer le bundle de support pour CSM. Cette procédure est utilisée pour le dépannage. Consultez le *Guide de dépannage de NSX-T Data Center* pour plus d'informations.

Systeme > Utilisateurs

Les utilisateurs sont gérés à l'aide du contrôle d'accès basé sur les rôles (RBAC).

Reportez-vous à [Gestion des comptes d'utilisateur et du contrôle d'accès basé sur les rôles](#) pour plus de détails.

Gérer la stratégie de mise en quarantaine

Apprenez à activer ou à désactiver la stratégie de mise en quarantaine et comprenez les implications de ces opérations sur vos machines virtuelles de charge de travail.

NSX Cloud utilise des groupes de sécurité pour la détection des menaces. Par exemple, lorsque la stratégie de mise en quarantaine est activée, si l'agent NSX est arrêté de force sur une machine virtuelle gérée dans un but malveillant, la machine virtuelle compromise est mise en quarantaine à l'aide du groupe de sécurité quarantine (dans Microsoft Azure) ou default (dans AWS).

Recommandation générale :

Démarrez avec l'option *disabled* pour les déploiements dans un **environnement existant** : la stratégie de mise en quarantaine est désactivée par défaut. Lorsque vous avez déjà configuré des machines virtuelles dans votre environnement de cloud public, utilisez le mode désactivé pour la stratégie de mise en quarantaine jusqu'à intégrer vos machines virtuelles de charge de travail. Cela garantit que les machines virtuelles existantes ne sont pas automatiquement mises en quarantaine.

Démarrez avec l'option *activé* pour les déploiements en **environnement vierge** : pour les déploiements en environnement vierge, il est recommandé d'activer la stratégie de mise en quarantaine afin d'autoriser la détection de menaces pour vos machines virtuelles à gérer par NSX Cloud.

Note Lorsque la stratégie de mise en quarantaine est activée, appliquez `vm_override_sg` sur les machines virtuelles de charge de travail afin de pouvoir les intégrer, puis supprimez ce groupe de sécurité, une fois qu'elles sont gérées par NSX Cloud. Les groupes de sécurité appropriés sont appliqués aux machines virtuelles dans les deux minutes qui suivent.

Comment activer ou désactiver la stratégie de mise en quarantaine

Lors du déploiement de PCG, vous pouvez activer ou désactiver la stratégie de mise en quarantaine. Suivez ces étapes pour activer ou désactiver la stratégie de mise en quarantaine.

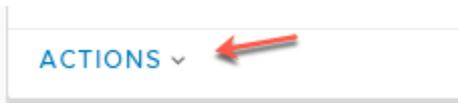
Conditions préalables

Un PCG ou une paire de PCG doit être déployé sur votre VPC ou VNet.

Procédure

- 1 Connectez-vous à CSM et accédez à votre cloud public :
 - a Si vous utilisez AWS, accédez à **Clouds > AWS > VPC**. Cliquez sur le VPC sur lequel un ou une paire de PCG est déployé(e) et en cours d'exécution.
 - b Si vous utilisez Microsoft Azure, accédez à **Clouds > Azure > VNets**. Cliquez sur le réseau virtuel sur lequel un ou une paire de PCG est déployé et en cours d'exécution.
- 2 Activez l'option à l'aide de l'une des options suivantes :

- Dans l'affichage en mosaïque, cliquez sur **ACTIONS > Modifier la configuration**.



- Si vous êtes dans la vue grille, cochez la case en regard du VPC ou du VNet et cliquez sur

ACTIONS > Modifier la configuration. 

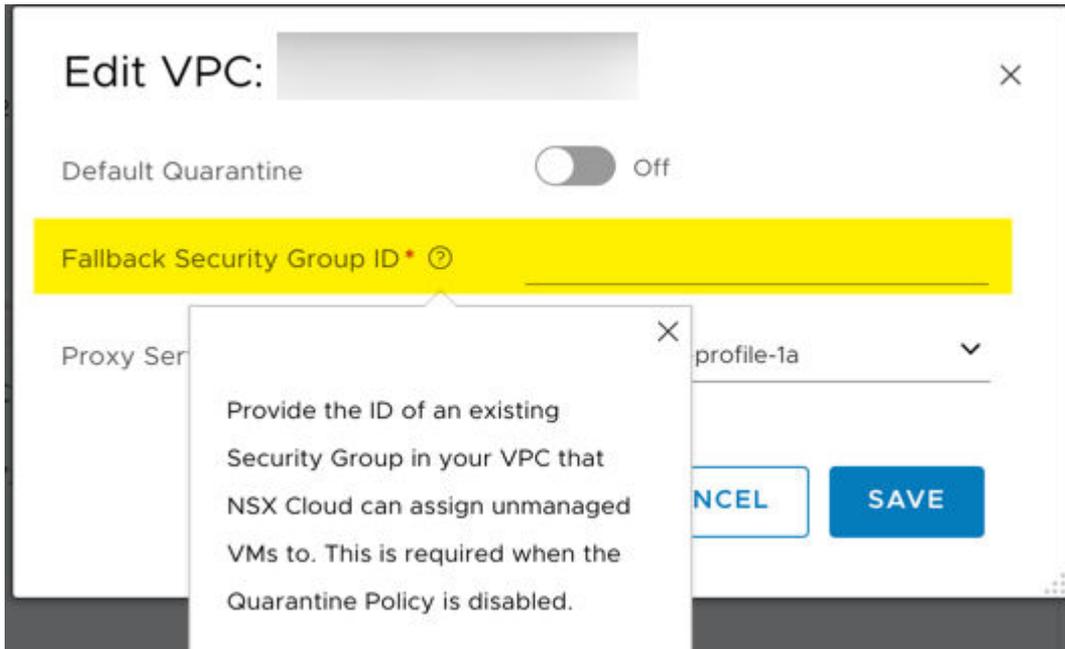
- ◆ Si vous êtes dans la page du VPC ou du VNet, cliquez sur l'icône ACTIONS pour accéder à

Modifier les configurations. 

- 3 Activez ou désactivez la **Mise en quarantaine par défaut**.

- 4 Si vous désactivez la stratégie de mise en quarantaine, vous devez fournir un groupe de sécurité de secours.

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 [Groupes de sécurité NSX Cloud pour le cloud public](#) pour obtenir la liste des groupes de sécurité NSX Cloud.



- Toutes les machines virtuelles non gérées ou en quarantaine dans ce VPC ou VNet obtiendront le groupe de sécurité de secours leur étant attribué lors de la désactivation de la stratégie de mise en quarantaine.
- Toutes les machines virtuelles gérées conservent le groupe de sécurité attribué par NSX Cloud. La première fois que ces machines virtuelles ne sont plus balisées et deviennent non gérées après la désactivation de la stratégie de mise en quarantaine, elles obtiennent également le groupe de sécurité de secours leur étant attribué.

- 5 Cliquez sur **ENREGISTRER**.

Impact de la stratégie de mise en quarantaine lorsqu'elle est désactivée

Stratégie de mise en quarantaine : désactivée

Lorsque la stratégie de mise en quarantaine est désactivée :

- NSX Cloud n'attribue pas de groupes de sécurité aux machines virtuelles lancées dans ce VPC ou réseau virtuel. Vous devez attribuer des groupes de sécurité NSX Cloud appropriés aux machines virtuelles pour activer la détection des menaces.

À partir de la console AWS ou le portail Microsoft Azure :

- ■ Attribuez le groupe `vm-underlay-sg` aux machines virtuelles pour lesquelles vous souhaitez utiliser le réseau de sous-couche fourni par Microsoft Azure ou AWS.

Stratégie de mise en quarantaine : était activée, puis désactivée

Le tableau suivant illustre l'incidence sur les attributions de groupe de sécurité si la stratégie de mise en quarantaine a été activée, puis désactivée :

Tableau 16-1. Incidence sur le groupe de sécurité de la désactivation de la stratégie de mise en quarantaine

ID VM	Géré ?	Groupe de sécurité	Groupe de sécurité pour la machine virtuelle après désactivation de la stratégie de mise en quarantaine
VM 1	Oui	<code>vm-underlay-sg</code>	<code>vm-underlay-sg</code> . Lorsque vous supprimez la balise <code>nsx.network</code> de cette machine virtuelle, pour la retirer de la gestion NSX, le groupe de sécurité de secours est aussi attribué à cette machine virtuelle.
VM 2	Oui	<code>default</code> (AWS) ou <code>quarantine</code> (Microsoft Azure)	Groupe de sécurité de secours que vous spécifiez lors de la désactivation de la stratégie de mise en quarantaine. Reportez-vous à Comment activer ou désactiver la stratégie de mise en quarantaine pour plus de détails.
VM 3	Non	<code>vm-override-sg</code>	Groupe de sécurité de secours que vous spécifiez lors de la désactivation de la stratégie de mise en quarantaine.
VM 4	Non	<code>default</code> (AWS) ou <code>quarantine</code> (Microsoft Azure)	Groupe de sécurité de secours que vous spécifiez lors de la désactivation de la stratégie de mise en quarantaine.

Note La désactivation de la stratégie de mise en quarantaine est requise pour l'annulation du déploiement du PCG. Reportez-vous à la section **Annulation du déploiement du PCG** dans le *Guide d'installation de NSX-T Data Center* pour plus de détails.

Impact de la stratégie de mise en quarantaine lorsqu'elle est activée

Stratégie de mise en quarantaine : activée

Lorsque la stratégie de mise en quarantaine est activée :

- L'attribution de groupe de sécurité ou de groupe de sécurité réseau pour toutes les interfaces des machines virtuelles de charge de travail appartenant à ce VPC ou réseau virtuel est gérée par NSX Cloud comme suit :
 - Les machines virtuelles non gérées se voient attribuer le groupe de sécurité réseau de quarantaine dans Microsoft Azure et le groupe de sécurité default dans AWS et sont mises en quarantaine. Cela limite le trafic sortant et arrête tout le trafic entrant vers ces machines virtuelles.
 - Les machines virtuelles non gérées peuvent devenir des machines virtuelles gérées par NSX lorsque vous installez NSX Agent sur la machine virtuelle et que vous les balisez dans le cloud public avec `nsx.network`. Dans le scénario par défaut, NSX Cloud attribue le groupe `vm-underlay-sg` pour autoriser le trafic entrant/sortant approprié.
 - Une machine virtuelle gérée par NSX peut encore se voir attribuer le groupe de sécurité quarantaine ou default et être mise en quarantaine si une menace est détectée sur la machine virtuelle (par exemple, si NSX Agent est arrêté sur la machine virtuelle).
 - Les modifications manuelles apportées aux groupes de sécurité seront annulées sur le ou les groupes de sécurité déterminés par NSX dans un délai de deux minutes.
 - Si vous souhaitez retirer une machine virtuelle de la quarantaine, attribuez le groupe `vm-override-sg` comme groupe de sécurité unique pour cette machine virtuelle. NSX Cloud ne change pas automatiquement le groupe de sécurité `vm-override-sg` et autorise l'accès SSH et RDP à la machine virtuelle. Supprimer le groupe `vm-override-sg` entraînera à nouveau la restauration du ou des groupes de sécurité de machine virtuelle vers le groupe de sécurité déterminé par NSX.

Note Lorsque la stratégie de mise en quarantaine est activée, affectez le groupe `vm-override-sg` à vos machines virtuelles avant d'installer NSX Agent sur ces dernières. Une fois que vous avez suivi le processus d'installation de NSX Agent et de balisage de la machine virtuelle en tant que machine virtuelle de sous-couche, supprimez le groupe NS `vm-override-sg` de la machine virtuelle. NSX Cloud attribuera automatiquement le groupe de sécurité approprié aux machines virtuelles gérées par NSX par la suite. Cette étape est nécessaire, car elle garantit que le groupe de sécurité quarantaine ou default n'est pas attribué à la machine virtuelle lorsque vous la préparez pour NSX Cloud.

Stratégie de mise en quarantaine : a été désactivée, puis activée

Le tableau suivant illustre l'incidence sur les attributions de groupe de sécurité si la stratégie de mise en quarantaine a été désactivée, puis activée :

Tableau 16-2. Incidence sur le groupe de sécurité de l'activation de la stratégie de mise en quarantaine

ID VM	Géré ?	Menace détectée ?	Groupe de sécurité après activation de la stratégie de mise en quarantaine
VM 1	Oui	Non	vm_underlay_sg .
VM 2	Oui	Oui	default (AWS) ou quarantine (Microsoft Azure)
			Note Vous pouvez attribuer manuellement vm_override_sg aux machines virtuelles gérées. Ces dernières sortent ainsi du mode de quarantaine et vous pouvez résoudre le problème en accédant à ces machines virtuelles via SSH ou RDP. Reportez-vous à la rubrique Stratégie de mise en quarantaine : activée
VM 3	Non	S/O	default (AWS) ou quarantine (Microsoft Azure)

Groupes de sécurité NSX Cloud pour le cloud public

Les groupes de sécurité suivants sont créés par NSX Cloud au moment du déploiement du PCG :

Les groupes de sécurité **gw** sont appliqués aux interfaces PCG respectives.

Tableau 16-3. Groupes de sécurité de cloud public créés par NSX Cloud pour les interfaces PCG

Nom du groupe de sécurité	Disponible dans Microsoft Azure ?	Disponible dans AWS ?	Nom complet
gw-mgmt-sg	Oui	Oui	Groupe de sécurité de gestion de passerelle
gw-uplink-sg	Oui	Oui	Groupe de sécurité de liaison montante de passerelle
gw-vtep-sg	Oui	Oui	Groupe de sécurité de liaison descendante de passerelle

Tableau 16-4. Groupes de sécurité de cloud public créés par NSX Cloud pour les machines virtuelles de charge de travail

Nom du groupe de sécurité	Disponible dans Microsoft Azure ?	Disponible dans AWS ?	Description
quarantine	Oui	Non	Groupe de sécurité de quarantaine pour Microsoft Azure
default	Non	Oui	Groupe de sécurité de quarantaine pour AWS
vm-underlay-sg	Oui	Oui	Groupe de sécurité de non-superposition de VM

Tableau 16-4. Groupes de sécurité de cloud public créés par NSX Cloud pour les machines virtuelles de charge de travail (suite)

Nom du groupe de sécurité	Disponible dans Microsoft Azure ?	Disponible dans AWS ?	Description
vm-override-sg	Oui	Oui	Groupe de sécurité de remplacement de VM
vm-overlay-sg	Oui	Oui	Groupe de sécurité réseau de superposition de VM (non utilisé dans la version actuelle)
vm-outbound-bypass-sg	Oui	Oui	Groupe de sécurité de contournement sortant de VM (non utilisé dans la version actuelle)
vm-inbound-bypass-sg	Oui	Oui	Groupe de sécurité de contournement entrant de VM (non utilisé dans la version actuelle)

Présentation de l'intégration et la gestion des machines virtuelles de charge de travail

Consultez les diagrammes de flux pour obtenir une présentation du workflow d'intégration dans votre cloud public.

Reportez-vous à la section [Installation des composants NSX Cloud](#) dans le *Guide d'installation de NSX-T Data Center* pour obtenir le workflow day-0.

Systèmes d'exploitation pris en charge

Il s'agit de la liste des systèmes d'exploitation actuellement pris en charge par NSX Cloud pour votre machine virtuelle de charge de travail.

Les systèmes d'exploitation suivants sont actuellement pris en charge :

Note Reportez-vous à la section Problèmes connus de NSX Cloud dans le *Notes de mise à jour de NSX-T Data Center* pour les exceptions.

- Red Hat Enterprise Linux (RHEL) 7.2, 7.3, 7.4, 7.5
- CentOS 7.2, 7.3, 7.4, 7.5
- Oracle Enterprise Linux 7.2, 7.3, 7.4 (versions Unbreakable Enterprise Kernel non prises en charge).

Note SE Linux n'est pas pris en charge pour Oracle Enterprise Linux, Red Hat Enterprise Linux et CentOS

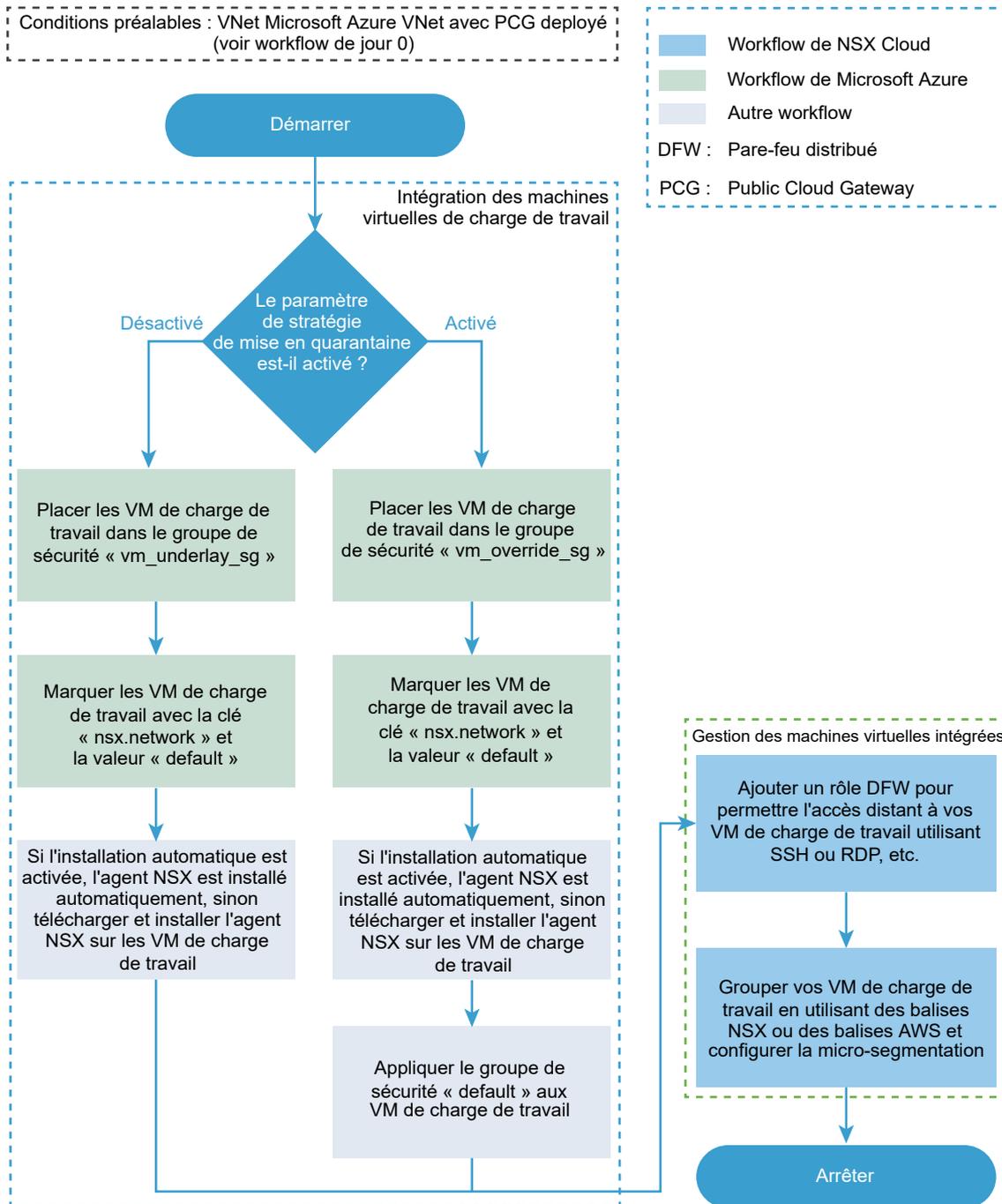
- Ubuntu 14.04, 16.04

- Microsoft Windows Server 2012 R2
- Microsoft Windows Sever 2016

Comment intégrer les machines virtuelles de charge de travail à partir de Microsoft Azure

Reportez-vous à cet organigramme pour obtenir un aperçu des étapes impliquées dans l'intégration des machines virtuelles de charge de travail à partir de Microsoft Azure.

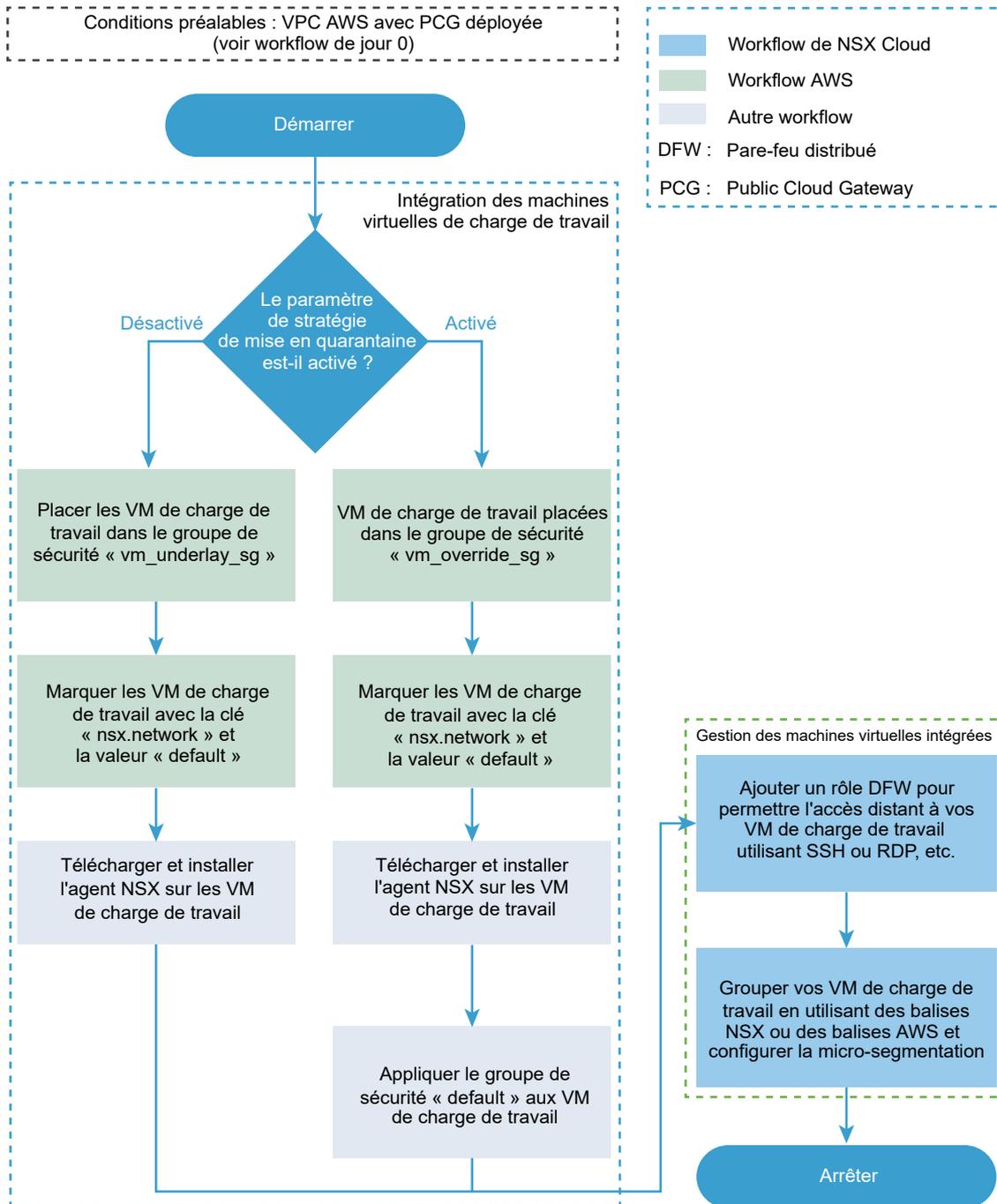
Figure 16-16. Workflow de l'intégration de jour-n pour Microsoft Azure



Comment intégrer des machines virtuelles de charge de travail à partir d'AWS

Reportez-vous à cet organigramme pour un aperçu des étapes impliquées dans l'intégration de machines virtuelles de charge de travail à partir d'AWS.

Figure 16-17. Workflow de l'intégration de jour-n pour AWS



Intégrer les machines virtuelles de charge de travail

Intégration de vos VM de charge de travail pour commencer à les gérer à l'aide de NSX-T Data Center.

Baliser des machines virtuelles dans le cloud public

Appliquez la balise **nsx.network** aux machines virtuelles que vous souhaitez gérer à l'aide de NSX-T Data Center.

Conditions préalables

Le VPC ou le VNet dans lequel les machines virtuelles de charge de travail sont hébergées doit être intégré à NSX Cloud. Pour plus de détails, reportez-vous à la section **Ajout de votre inventaire de cloud public** dans le document *Guide d'installation de NSX-T Data Center*.

Procédure

- 1 Connectez-vous à votre compte de cloud public et accédez à votre VPC ou VNet qui a été intégré à NSX Cloud.
- 2 Sélectionnez les machines virtuelles que vous souhaitez gérer à l'aide de NSX-T Data Center.
- 3 Ajoutez les détails de balise suivants pour les machines virtuelles et enregistrez vos modifications.

```
Name: nsx.network
Value: default
```

Note Vous pouvez appliquer cette balise avec le même effet au niveau de la machine virtuelle comme au niveau de l'interface.

Exemple

Étape suivante

Installez l'agent NSX sur ces machines virtuelles. Reportez-vous à la section [Installer NSX Agent](#).

Si vous utilisez Microsoft Azure, vous avez la possibilité d'installer automatiquement l'agent NSX sur les machines virtuelles balisées. Reportez-vous à [Installer Agent NSX automatiquement](#) pour plus de détails.

Installer NSX Agent

Installez NSX Agent sur vos VM de charge de travail.

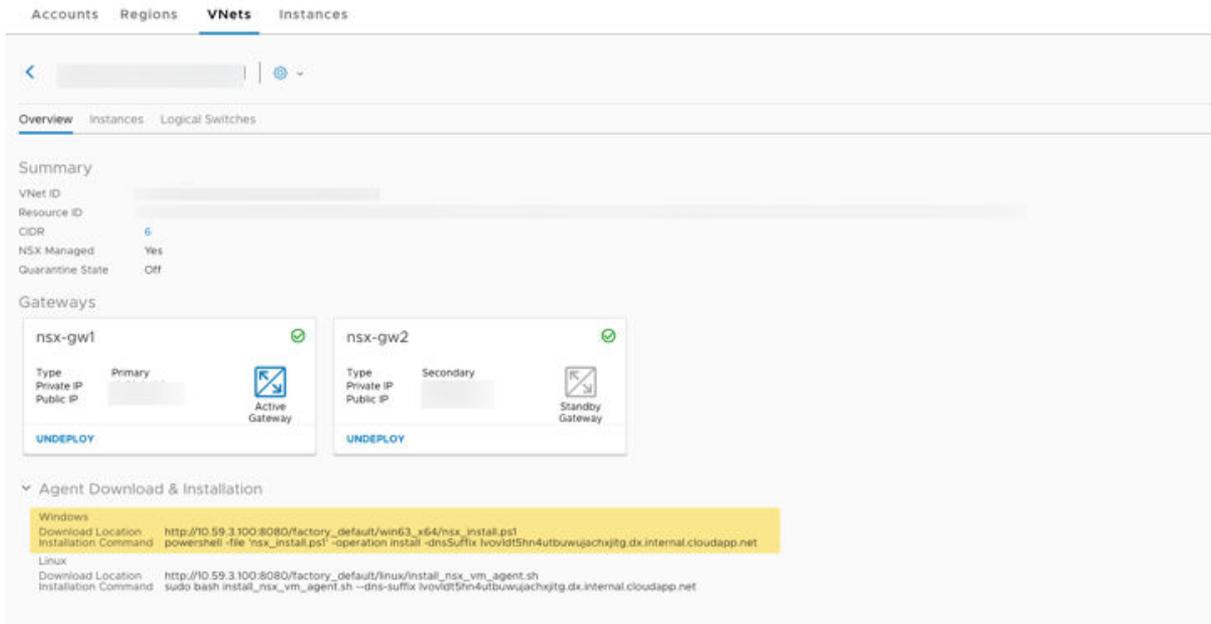
Installer NSX Agent sur des machines virtuelles Windows

Suivez ces instructions pour installer NSX Agent sur votre VM de charge de travail Windows.

Reportez-vous à la section [Systèmes d'exploitation pris en charge](#) pour obtenir la liste des versions de Microsoft Windows prises en charge actuellement.

Procédure

- 1 Connectez-vous à CSM et accédez à votre cloud public :
 - a Si vous utilisez AWS, accédez à **Clouds > AWS > VPC**. Cliquez sur le VPC sur lequel un ou une paire de PCG est déployé(e) et en cours d'exécution.
 - b Si vous utilisez Microsoft Azure, accédez à **Clouds > Azure > VNets**. Cliquez sur le réseau virtuel sur lequel un ou une paire de PCG est déployé et en cours d'exécution.
- 2 À partir de la section **Téléchargement et installation de l'agent** de l'écran, notez l'**emplacement de téléchargement** et la **commande d'installation** sous **Windows**.



Note Le suffixe DNS dans la **commande d'installation** est généré dynamiquement pour correspondre aux paramètres DNS que vous choisissez lors du déploiement de PCG.

- 3 Connectez-vous à votre VM de charge de travail Windows en tant qu'administrateur.
- 4 Téléchargez le script d'installation sur votre machine virtuelle Windows à partir de l'**emplacement de téléchargement** que vous avez noté dans CSM. Vous pouvez télécharger le script à l'aide d'un navigateur, comme Internet Explorer. Le script est téléchargé dans le répertoire de téléchargements par défaut de votre navigateur, par exemple, `C:\Downloads`.
- 5 Ouvrez une invite PowerShell et accédez au répertoire contenant le script téléchargé.

- 6 Utilisez la **commande d'installation** que vous avez notée dans CSM pour exécuter le script téléchargé.

Par exemple :

```
c:\> powershell -file 'nsx_install.ps1' -operation install -dnsSuffix <>
```

Note L'argument de fichier requiert le chemin d'accès complet, sauf si vous vous trouvez dans le même répertoire ou si le script PowerShell est déjà indiqué dans le chemin d'accès. Par exemple, si vous téléchargez le script dans *C:\Downloads* et que vous ne vous trouvez pas dans ce répertoire, le script doit contenir l'emplacement : *powershell -file 'C:\Downloads\nsx_install.ps1' ...*

- 7 Le script s'exécute et lorsqu'il est terminé, un message s'affiche pour indiquer si NSX Agent a été installé correctement.

Note Le script considère l'interface réseau principale comme la valeur par défaut.

Pour obtenir une liste de toutes les options de script et les instructions de désinstallation, reportez-vous à la section [Options du script d'installation de NSX Agent pour les machines virtuelles Windows](#).

Étape suivante

[Gérer les machines virtuelles de charge de travail](#)

Installer NSX Agent sur des machines virtuelles Linux

Suivez ces instructions pour installer NSX Agent sur vos VM de charge de travail Linux.

Reportez-vous à [Systèmes d'exploitation pris en charge](#) pour obtenir la liste des distributions Linux actuellement prises en charge.

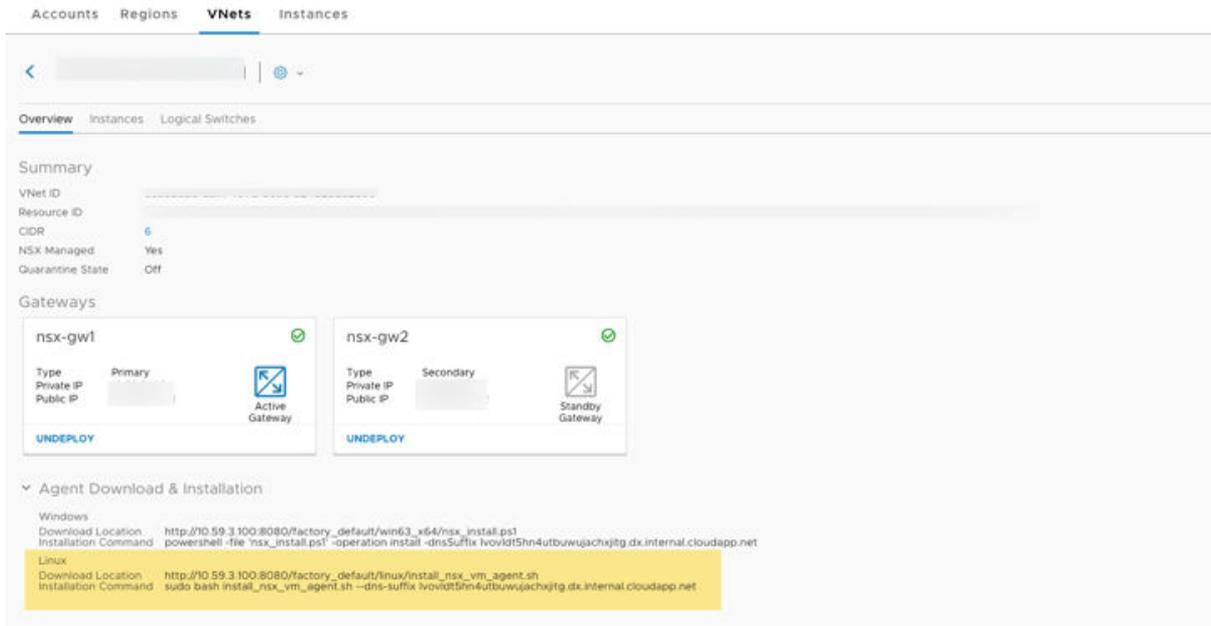
Conditions préalables

Les commandes **wget** et **nslookup** sont nécessaires pour exécuter le script d'installation de NSX Agent.

Procédure

- 1 Connectez-vous à CSM et accédez à votre cloud public :
 - a Si vous utilisez AWS, accédez à **Clouds > AWS > VPC**. Cliquez sur le VPC sur lequel un ou une paire de PCG est déployée et en cours d'exécution.
 - b Si vous utilisez Microsoft Azure, accédez à **Clouds > Azure > VNets**. Cliquez sur le réseau virtuel sur lequel un ou une paire de PCG est déployé(e) et en cours d'exécution.

- 2 À partir de la section **Téléchargement et installation de l'agent** de l'écran, notez l'**emplacement de téléchargement** et la **commande d'installation** sous Linux.



Note Le suffixe DNS dans la commande d'installation est généré dynamiquement pour correspondre aux paramètres DNS que vous choisissez lors du déploiement de PCG.

- 3 Connectez-vous à la VM de charge de travail Linux avec des privilèges de superutilisateur.
- 4 Utilisez wget ou un équivalent pour télécharger le script d'installation sur votre machine virtuelle Linux à partir de l'**emplacement de téléchargement** que vous avez noté dans CSM. Le script d'installation est téléchargé dans le répertoire où vous exécutez la commande wget.
- 5 Modifiez les autorisations sur le script d'installation pour le rendre exécutable, le cas échéant, et exécutez-le :

```
$ sudo chmod +x install_nsx_vm_agent.sh
$ sudo bash install_nsx_vm_agent.sh --dns-suffix <>
```

Remarque : sur Red Hat Enterprise Linux et ses dérivés, SELinux n'est pas pris en charge. Désactivez SELinux pour installer NSX Agent.

- 6 Dès l'instant où l'installation de NSX Agent a commencé, vous perdez la connexion à votre VM Linux. Des messages semblables à ceux-ci s'affichent à l'écran : `Installation completed!!! Starting NSX Agent service. SSH connection will now be lost..` Reconnectez-vous à votre machine virtuelle pour terminer le processus d'intégration.

Résultats

L'agent NSX est installé sur votre ou vos VM de charge de travail.

Note

- Une fois que l'agent NSX a été installé avec succès, le port 8888 apparaît comme étant ouvert sur la machine virtuelle, mais il est bloqué pour les machines virtuelles dans le mode de sous-couche et doit être utilisé uniquement lorsque cela est requis pour un dépannage avancé.
- Le script utilise eth0 comme interface par défaut. Pour obtenir une liste des options de script et les instructions de désinstallation, reportez-vous à la section [Options du script d'installation de NSX Agent pour les machines virtuelles Linux](#).

Étape suivante

[Gérer les machines virtuelles de charge de travail](#)

Options du script d'installation de NSX Agent et désinstallation

Le script d'installation de NSX Agent fournit des options configurables. Le tableau suivant répertorie ces options.

Options du script d'installation de NSX Agent pour les machines virtuelles Windows**Tableau 16-5.**

Option	Description
<code>--gateway <ip dns></code>	<p>IP ou nom DNS de NSX Public Cloud Gateway.</p> <p>Spécifiez cette option si vous souhaitez utiliser une adresse IP pour PCG. Le nom DNS par défaut du PCG est utilisé si ce paramètre n'est pas spécifié.</p> <ul style="list-style-type: none"> ■ Nom DNS du PCG dans AWS : <code>nsx-gw.vmware.local</code> ■ Nom DNS du PCG dans Microsoft Azure : <code>nsx-gw</code> <p>Note En mode HA des PCG, spécifiez l'option "--gateway" avec les deux noms PCG, par exemple, dans une machine virtuelle Microsoft Azure : <code>--gateway "nsx-gw1;nsx-gw2"</code></p>
<code>--noStart true</code>	<p>Vous pouvez créer un disque dur virtuel de la machine virtuelle une fois que l'agent NSX est installé sur celle-ci. Exécutez le script d'installation avec cette option. Créez ensuite un disque dur virtuel de cette machine virtuelle sur le portail Microsoft Azure.</p>
<code>--downloadPath <path></code>	<p>Il s'agit du chemin d'accès au répertoire dans lequel les fichiers doivent être téléchargés. Si le chemin d'accès comporte des caractères d'échappement, placez ces caractères entre guillemets simples.</p> <p>Valeur par défaut = <code>%Temp%</code></p>
<code>--silentInstall <true/false></code>	<p>Si cette option est définie sur <code>true</code>, le script exécute une installation silencieuse.</p> <p>La valeur par défaut est <code>false</code>.</p>
<code>--noSigCheck <true/false></code>	<p>Cela vous permet de spécifier si les signatures sur les fichiers binaires doivent être vérifiées ou non.</p> <p>Valeur par défaut = <code>false</code></p>

Tableau 16-5. (suite)

Option	Description
<code>-logLevel <value></code>	Cela vous permet de spécifier le niveau de journalisation pour les composants NSX. Valeur par défaut = 1 Niveau détaillé = 3
<code>-operation <install/uninstall></code>	Cela vous permet de spécifier l'opération à effectuer : <code>install</code> ou <code>uninstall</code> Valeur par défaut = <code>install</code>
<code>-bundlePath <path></code>	Cela vous permet de spécifier le chemin d'accès local au bundle de l'agent de machine virtuelle NSX. L'option par défaut consiste à télécharger le bundle depuis PCG.

Désinstallation de NSX Agent à partir d'une machine virtuelle Windows

- 1 Connectez-vous à distance à la machine virtuelle via une connexion RDP.
- 2 Exécutez le script d'installation avec l'option `uninstall` :

```
\nsx_install.ps1 -operation uninstall
```

Options du script d'installation de NSX Agent pour les machines virtuelles Linux

Tableau 16-6.

Option	Description
<code>--gateway <ip dns></code>	IP ou nom DNS de NSX Public Cloud Gateway. Spécifiez cette option si vous souhaitez utiliser une adresse IP pour PCG. Le nom DNS par défaut du PCG est utilisé si ce paramètre n'est pas spécifié. <ul style="list-style-type: none"> ■ Nom DNS du PCG dans AWS : <code>nsx-gw.vmware.local</code> ■ Nom DNS du PCG dans Microsoft Azure : <code>nsx-gw</code> <p>Note En mode HA des PCG, spécifiez l'option <code>--gateway</code> avec les deux noms PCG, par exemple, dans une machine virtuelle Microsoft Azure : <code>--gateway "nsx-gw1;nsx-gw2"</code></p>
<code>--no-start</code>	Vous pouvez créer un disque dur virtuel de la machine virtuelle une fois que l'agent NSX est installé sur celle-ci. Exécutez le script d'installation avec cette option. Créez ensuite un disque dur virtuel de cette machine virtuelle sur le portail Microsoft Azure.
<code>--uninstall</code>	Exécutez le script avec cette option pour désinstaller NSX Agent.

Installer Agent NSX automatiquement

Actuellement pris en charge uniquement pour Microsoft Azure.

Dans Microsoft Azure, si les critères suivants sont remplis, NSX Agent est installé automatiquement :

- Extensions de machine virtuelle Azure installées sur les machines virtuelles dans le réseau virtuel ajouté dans NSX Cloud. Pour plus de détails, reportez-vous à la [Documentation Microsoft Azure sur les extensions de machine virtuelle](#).
- Machines virtuelles balisées avec default et la valeur nsx.network.

Pour activer cette fonctionnalité :

- 1 Accédez à **Clouds > Azure > VNets**.
- 2 Sélectionnez le réseau virtuel sur les machines virtuelles dont vous souhaitez installer automatiquement NSX Agent.
- 3 Activez l'option à l'aide de l'une des options suivantes :
 - Dans l'affichage en mosaïque, cliquez sur **ACTIONS > Modifier la configuration**.

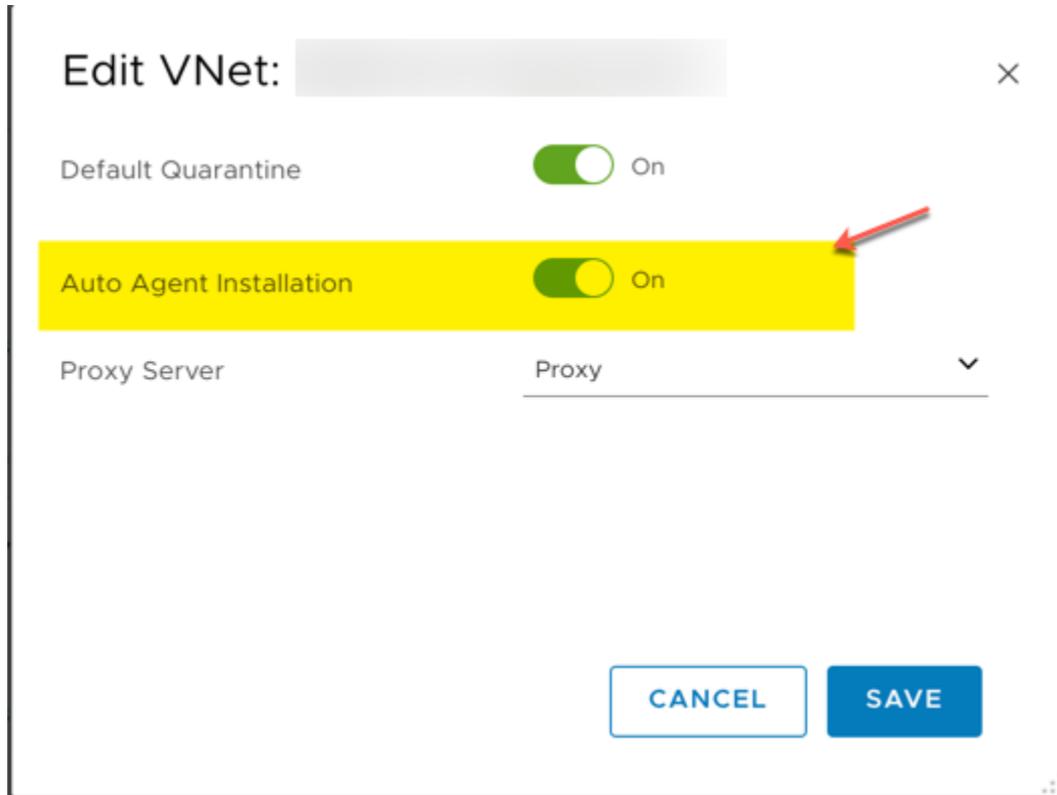


- Si vous êtes dans la vue grille, cochez la case en regard du VNet et cliquez sur **ACTIONS >**

Modifier la configuration. 

- Si vous êtes dans la page du réseau virtuel, cliquez sur l'icône ACTIONS pour accéder à

Modifier les configurations. 



Gérer les machines virtuelles de charge de travail

Après avoir correctement intégré les machines virtuelles de charge de travail, vous pouvez utiliser NSX-T Data Center afin de les gérer.

Accéder aux machines virtuelles de charge de travail gérées

Suivez ce workflow pour accéder aux machines virtuelles gérées dans le mode de sous-couche.

Lors du déploiement de PCG sur votre VPC ou VNet, NSX Cloud crée des règles de pare-feu par défaut afin d'améliorer la sécurité de vos machines virtuelles de charge de travail.

Pour accéder aux machines virtuelles de charge de travail gérées dans le mode de sous-couche, vous devez ajouter une règle de pare-feu distribué (DFW) qui autorise l'accès à la machine virtuelle.

Procédez comme suit :

- 1 Ouvrez la console NSX Manager.
- 2 Accédez à **Pare-feu > Général > Ajouter une règle**.

- 3 Ajoutez une règle avec les configurations suivantes. Reportez-vous à [Ajouter une règle de pare-feu](#) pour obtenir des instructions détaillées.

Tableau 16-7.

Option	Description
Nom	Fournissez un nom pour définir l'objectif de cette règle, par exemple, <code>AllowRemoteAccessToUnderlay</code> .
Source	Sélectionnez Tous .
Destination	Sélectionnez le commutateur logique, le port ou le NSGroup auquel cette VM est associée ou dont elle fait partie.
Services	Sélectionnez les services d'accès à distance pour cette VM de charge de travail, par exemple, SSH pour Linux ou RDP pour Windows.
Action	Sélectionnez Autoriser .

Regrouper les machines virtuelles à l'aide de NSX-T Data Center et de balises de cloud public

NSX Cloud vous permet d'utiliser les balises de cloud public qui sont attribuées à vos machines virtuelles de charge de travail.

NSX Manager utilise ces balises pour regrouper les machines virtuelles, comme le font les clouds publics. Par conséquent, pour simplifier le groupement des machines virtuelles, NSX Cloud insère les balises de cloud public appliquées à vos machines virtuelles de charge de travail, sous réserve qu'elles répondent aux critères de mots réservés et de taille prédéfinis, dans NSX Manager.

Terminologie relatives aux balises

Dans NSX Manager, une **balise** fait référence à ce qui s'appelle une **valeur** dans le contexte d'un cloud public. La **clé** d'une balise de cloud public s'appelle une **portée** dans NSX Manager.

Composants des balises dans NSX Manager	Composants équivalents des balises dans le cloud public
Portée	Clé
Balise	Valeur

Types de balises et limitations

NSX Cloud permet trois types de balises pour les VM de cloud public gérées par NSX.

- **Balises système** : ces balises sont définies par le système et vous ne pouvez pas les ajouter, les modifier ou les supprimer. NSX Cloud utilise les balises système suivantes :
 - `azure:subscription_id`
 - `azure:region`
 - `azure:vm_rg`

- azure:vnet_name
 - azure:vnet_rg
 - aws:vpc
 - aws:availabilityzone
- **Balises découvertes** : les balises que vous avez ajoutées à vos machines virtuelles dans le cloud public sont automatiquement découvertes par NSX Cloud et affichées pour vos machines virtuelles de charge de travail dans l'inventaire de NSX Manager. Ces balises ne sont pas modifiables au sein de NSX Manager. Il n'existe aucune limite quant au nombre de balises découvertes. Ces balises sont précédées de **dis:azure:** pour indiquer qu'elles sont découvertes dans Microsoft Azure.

Lorsque vous apportez des modifications aux balises dans le cloud public, celles-ci sont reflétées dans NSX Manager dans les deux minutes.

Cette fonctionnalité est activée par défaut. Vous pouvez activer ou désactiver la découverte de balises Microsoft Azure ou AWS au moment de l'ajout de l'abonnement Microsoft Azure ou du compte AWS.

- **Balises utilisateur** : vous pouvez créer jusqu'à 25 balises utilisateur. Vous pouvez ajouter, modifier ou supprimer des privilèges pour les balises utilisateur. Pour plus d'informations sur la gestion des balises d'utilisateur, reportez-vous à [Gérer les balises d'une machine virtuelle](#).

Tableau 16-8. Résumé des types de balises et des limitations

Type de balise	Portée de la balise ou préfixe prédéterminé	Limitations	Administrateur d'entreprise Privilèges	Auditeur Privilèges
Définie par le système	Renseignez les balises système : <ul style="list-style-type: none"> ■ azure:subscription_id ■ azure:region ■ azure:vm_rg ■ azure:vnet_name ■ azure:vnet_rg ■ aws:vpc ■ aws:availabilityzone 	Portée (clé) : 20 caractères Balise (valeur) : 65 caractères Nombre maximal possible : 5	Lecture seule	Lecture seule
Découverte	Préfixe des balises Microsoft Azure qui sont importées depuis votre réseau virtuel : dis:azure: Préfixe pour les balises AWS qui sont importées depuis votre VPC : dis:aws:	Portée (clé) : 20 caractères Balise (valeur) : 65 caractères Nombre maximal autorisé : illimité <hr/> Note Les limites de caractères excluent le préfixe dis:<public cloud name> . Les balises qui dépassent ces limites ne sont pas reflétées dans NSX Manager. <hr/> Les balises précédées de nsx sont ignorées.	Lecture seule	Lecture seule
Utilisateur	Les balises utilisateur peuvent avoir n'importe quelle portée (clé) et une valeur comprise dans le nombre de caractères autorisé, sauf : <ul style="list-style-type: none"> ■ le préfixe de l'étendue (clé) dis:azure: ou dis:aws: 	Portée (clé) : 30 caractères Balise (valeur) : 65 caractères Nombre maximal autorisé : 25	Ajouter/modifier/supprimer	Lecture seule

Tableau 16-8. Résumé des types de balises et des limitations (suite)

Type de balise	Portée de la balise ou préfixe prédéterminé	Limitations	Administrateur d'entreprise Privilèges	Auditeur Privilèges
	<ul style="list-style-type: none"> la même portée (clé) que les balises système 			

Exemples de balises découvertes

Note Les balises sont au format **key=value** pour le cloud public et au format **scope=tag** dans NSX Manager.

Tableau 16-9.

Balise de cloud public pour les machines virtuelles de charge de travail	Découverte par NSX Cloud ?	Balise NSX Manager équivalente pour la machine virtuelle de charge de travail
Name=Developer	Oui	dis:azure:Name=Developer
ValidDisTagKeyLength=ValidDisTagValue	Oui	dis:azure:ValidDisTagKeyLength=ValidDisTagValue
Abcdefghijklmnopqrstuvwxyz=value2	Non (la clé dépasse 20 caractères)	aucune
tag3=AbcdefghijklmnopqrstuvwxyzAb2369 Ohgijuytreswqacvbcdefghijklmnopqrstuv wxyz	Non (la valeur dépasse 65 caractères)	aucune
nsx.name=Tester	Non (la clé est précédée de nsx)	aucune

Utilisation des balises dans NSX Manager

- Reportez-vous à la section [Gérer les balises d'une machine virtuelle](#).
- Reportez-vous à la section [Rechercher des objets](#).
- Reportez-vous à la section [Configurer la microsegmentation pour les machines virtuelles de charge de travail](#).

Configurer la microsegmentation pour les machines virtuelles de charge de travail

Vous pouvez configurer une microsegmentation pour les machines virtuelles de charge de travail gérées.

Pour appliquer des règles de pare-feu distribué aux machines virtuelles de charge de travail intégrées, procédez comme suit :

- 1 Créez des groupes NS à l'aide de noms ou de balises de machines virtuelles ou d'autres critères d'appartenance (par exemple, pour les niveaux **web**, **app** et **DB**). Pour trouver des instructions, voir [Créer un NSGroup](#).

Note Vous pouvez utiliser l'une des balises suivantes pour les critères d'appartenance. Reportez-vous à [Regrouper les machines virtuelles à l'aide de NSX-T Data Center et de balises de cloud public](#) pour plus de détails.

- balises définies par le système
 - balises de votre VPC ou VNet découvertes par NSX Cloud
 - ou vos propres balises personnalisées
-

- 2 Créez une section de règles de pare-feu et appliquez-la aux groupes NS, si nécessaire. Reportez-vous à la section [Ajouter une section de règles de pare-feu](#).
- 3 Créez des règles de pare-feu et utilisez des groupes NS pour la source et la destination, comme requis par votre stratégie de sécurité. Reportez-vous à la section [Ajouter une règle de pare-feu](#).

Cette micro-segmentation prend effet lorsque l'inventaire est manuellement resynchronisé à partir de CSM ou dans un délai d'environ deux minutes lorsque les modifications sont intégrées dans CSM à partir de votre cloud public.

Comment utiliser des fonctionnalités NSX-T Data Center avec le cloud public

NSX Cloud crée une topologie réseau pour votre cloud public et vous ne devez pas modifier ou supprimer les entités logiques NSX-T Data Center générées automatiquement.

Utilisez cette liste comme référence rapide indiquant ce qui est généré automatiquement et la manière dont vous devez utiliser les fonctionnalités de NSX-T Data Center appliquées au cloud public.

Configurations de NSX Manager

Les entités suivantes sont automatiquement créées dans NSX Manager :

Important Ne modifiez pas ou ne supprimez pas ces entités créées automatiquement.

- Un nœud Edge nommé **Passerelle de cloud public** (PCG) est créé.
- PCG est ajouté au cluster Edge. Dans un déploiement HA, il y a deux PCG.
- Le PCG (ou les PCG) est enregistré comme nœud de transport avec deux zones de transport créées.
- Deux commutateurs logiques par défaut sont créés.
- Un routeur logique de niveau 0 est créé.
- Un profil de découverte IP est créé. Il est utilisé pour les commutateurs logiques de superposition.

- Un profil DHCP est créé. Il est utilisé pour les serveurs DHCP.

Note Bien que le profil DHCP soit créé, il n'est pas pris en charge dans la version actuelle, car il est utilisé pour la mise en réseau de superposition.

- Un groupe NS par défaut appelé **PublicCloudSecurityGroup** est créé avec les membres suivants :
 - Le commutateur logique VLAN par défaut.
 - Les ports logiques, un pour chacun des ports de liaison montante PCG, si la fonctionnalité HA est activée.
 - Adresse IP
- Trois règles DFW de passerelle distribuées par défaut sont créées :
 - LogicalSwitchToLogicalSwitch
 - LogicalSwitchToAnywhere
 - AnywhereToLogicalSwitch

Note Ces règles DFW (Default Distributed Firewall) bloquent tout le trafic et doivent être ajustées en fonction de vos besoins spécifiques.

Vérifier ces configurations dans NSX Manager :

- 1 Dans le tableau de bord NSX Cloud, cliquez sur **NSX Manager**.
- 2 Accédez à **Infrastructure > Nœuds > Dispositifs Edge**. Vous devez voir **PCG-<votre-nom-VPC-ou-VNet>** comme nœud Edge.

Note Vérifiez que État de déploiement, Gestionnaire de connexion et Connexion du contrôleur sont connectés (l'état indique **Actif** avec un point vert).

- 3 Accédez à **Infrastructure > Nœuds > Clusters Edge** pour vérifier que **PCG-Cluster-<votre-nom-VPC-ou-VNet>** est ajouté.
- 4 Accédez à **Infrastructure > Nœuds > Nœuds de transport** pour vérifier que PCG est enregistré comme nœud de transport et est connecté à deux zones de transport qui ont été créés automatiquement lors du déploiement de PCG :
 - Type de trafic VLAN -- il se connecte à la liaison montante PCG
 - Type de superposition de trafic -- il s'agit de la mise en réseau logique de superposition

Note La superposition n'est pas prise en charge dans la version actuelle.

- 5 Vérifiez que les commutateurs logiques et le routeur logique de niveau 0 ont été créés et que le routeur logique est ajouté au cluster Edge.
 - Accédez à **Mise en réseau > Commutation > Commutateurs**. Vous devez voir les commutateurs **DefaultSwitch-Overlay-<votre-nom-VPC-ou-VNet>** et **DefaultSwitch-VLAN-<votre-nom-VPC-ou-VNet>** créés automatiquement.

- Accédez à **Mise en réseau > Routage > Routeurs**. Vous devez voir le routeur **PCG-Tier0-LR-
<votre-nom-VPC-ou-VNet>** créé automatiquement.

FAQ sur la commutation logique

Tableau 16-10.

Question	Réponse
Est-ce que NSX Cloud crée des commutateurs par défaut lorsqu'un PCG est déployé ?	Oui. NSX Cloud crée deux commutateurs par défaut pour chaque VPC ou VNet sur lequel vous déployez PCG. Les commutateurs sont nommés comme suit : DefaultSwitch-Overlay-<vpc-or-vnet-name> DefaultSwitch-VLAN-<vpc-or-vnet-name>
Puis-je créer un commutateur logique VLAN en plus des commutateurs logiques par défaut créés par NSX Cloud ?	Non. Ne créez pas de commutateur logique VLAN.
Puis-je modifier ou supprimer les commutateurs logiques par défaut créés par NSX Cloud ?	L'interface utilisateur vous permet de modifier ou supprimer les entités logiques par défaut mais il ne faut pas modifier ou supprimer ce qui est créé automatiquement par NSX Cloud.
Dois-je créer des ports ?	Non. Vous n'avez pas besoin de créer des ports. NSX Cloud Crée des ports lorsque vous balisez des machines virtuelles dans AWS ou Microsoft Azure. Ne modifiez pas ou ne supprimez pas les ports créés automatiquement par NSX Cloud.
Dois-je créer des profils de commutation ?	Non. Vous n'avez pas besoin de créer des profils de commutation. Utilisez le PublicCloud-Global-SpoofGuardProfile . Ne modifiez pas ou ne supprimez pas le profil de commutation par défaut.
Où puis-je trouver des informations détaillées sur des commutateurs logiques ?	Reportez-vous à la section Chapitre 1 Commutateurs logiques et configuration d'un attachement de VM .

FAQ sur les routeurs logiques

Tableau 16-11.

Question	Réponse
NSX Cloud crée-t-il automatiquement un routeur logique lorsque PCG est déployé ?	Oui. Un routeur logique de niveau 0 est automatiquement créé par NSX Cloud lorsque PCG est déployé sur un VPC ou un VNet.
Où trouver plus d'informations sur les routeurs logiques ?	Reportez-vous à la section Chapitre 5 Routeur logique de niveau 0 .

FAQ sur IPFIX

Tableau 16-12.

Question	Réponse
Des configurations spécifiques sont-elles requises pour IPFIX pour un fonctionnement correct dans le cloud public ?	Oui : <ul style="list-style-type: none"> ■ IPFIX est pris en charge dans NSX Cloud uniquement sur le port UDP 4739. ■ Le collecteur doit être dans le même VPC ou réseau virtuel que la machine virtuelle sur laquelle le profil IPFIX a été appliqué. ■ Commutateur et DFW IPFIX : si le collecteur se trouve dans le même sous-réseau que la machine virtuelle Windows sur laquelle le profil IPFIX a été appliqué, une entrée ARP statique pour le collecteur sur la machine virtuelle Windows est nécessaire, car Windows ignore silencieusement les paquets UDP lorsqu'aucune entrée ARP n'est trouvée.
Où trouver plus d'informations sur IPFIX ?	Reportez-vous à la section Configurer IPFIX .

FAQ sur la mise en miroir de ports

Tableau 16-13.

Question	Réponse
Des configurations spécifiques sont-elles requises pour la mise en miroir de ports dans le cloud public ?	La mise en miroir de ports est uniquement prise en charge dans AWS dans la version actuelle. <ul style="list-style-type: none"> ■ Pour NSX Cloud, configurez la mise en miroir de ports à partir de Outils > Session de mise en miroir de ports. ■ Seule la mise en miroir de ports L3SPAN est prise en charge. ■ Le collecteur doit se trouver dans le même VPC que la machine virtuelle de charge de travail source.
Où trouver plus d'informations sur la mise en miroir de ports ?	Reportez-vous à la section Surveiller des sessions de mise en miroir de ports .

Autres questions fréquentes

Tableau 16-14.

Question	Réponse
Les balises que j'applique à mes machines virtuelles de charge de travail dans le cloud public sont-elles disponibles dans NSX-T Data Center ?	Oui. Reportez-vous à Regrouper les machines virtuelles à l'aide de NSX-T Data Center et de balises de cloud public pour plus de détails.
Comment puis-je configurer la micro-segmentation pour mes machines virtuelles de charge de travail qui sont gérées par NSX-T Data Center ?	Reportez-vous à la section Configurer la microsegmentation pour les machines virtuelles de charge de travail .

Utilisation des fonctionnalités avancées de NSX Cloud

Activer le transfert Syslog

NSX Cloud prend en charge le transfert Syslog.

Vous pouvez activer le transfert Syslog pour les paquets DFW (Distributed Firewall) sur les machines virtuelles gérées. Pour plus d'informations, reportez-vous à la section **Configurer la journalisation à distance** dans le *Guide de dépannage de NSX-T Data Center*.

Procédez comme suit :

Procédure

- 1 Connectez-vous à PCG à l'aide de l'hôte d'accès direct.
- 2 Tapez `nsxcli` pour ouvrir la CLI NSX-T Data Center.
- 3 Entrez les commandes suivantes pour activer le transfert du journal DFW :

```
nsx-public-cloud-gateway> set gw-controller vm-log-forwarding enabled
nsx-public-cloud-gateway> set logging-server <server-IP-address> proto udp level info messageid
FIREWALL-PKTLOG
```

Une fois ce paramètre défini, les journaux des paquets DFW de NSX Agent sont disponibles sous `/var/log/syslog` sur PCG.

- 4 Pour activer le transfert du journal par VM, entrez la commande suivante :

```
nsx-public-cloud-gateway> set gw-controller vm-log-forwarding enabled <vm-id>
```

Dépannage

Découvrez les options de vérification et de dépannage disponibles dans NSX Cloud.

Vérifier les composants de NSX Cloud

Il est recommandé de vérifier que tous les composants sont en cours d'exécution avant de passer au déploiement dans un environnement de production.

Vérifier que NSX Agent est connecté à PCG

Pour vérifier que l'instance de NSX Agent sur votre machine virtuelle de charge de travail est connecté à PCG, procédez comme suit :

- 1 Entrez la commande `nsxcli` pour ouvrir la CLI de NSX-T Data Center.

- 2 Entrez la commande suivante pour obtenir l'état de connexion de la passerelle, par exemple :

```
get gateway connection status
Public Cloud Gateway : nsx-gw.vmware.com:5555 Connection Status : ESTABLISHED
```

Vérifier le mode interface/réseau de la machine virtuelle

Vérifiez l'interface sur laquelle l'agent NSX est installé, comme suit :

- 1 Entrez la commande `nsxcli` pour ouvrir la CLI de NSX-T Data Center.
- 2 Entrez la commande pour afficher le mode de commutateur, par exemple :

```
get vm-network-mode
Mode réseau de machine virtuelle : interface de sous-couche : eth0
```

Vérifiez la balise d'interface de machine virtuelle dans AWS ou Microsoft Azure

Les machines virtuelles de charge de travail doivent avoir des balises correctes pour se connecter à PCG.

- 1 Connectez-vous à la console AWS ou au portail Microsoft Azure.
- 2 Vérifiez la balise `eth0` ou d'interface de la machine virtuelle.

La clé `nsx.network` doit avoir la valeur `default`.

FAQ de dépannage

Cette liste répertorie les questions fréquemment posées.

J'ai correctement balisé ma machine virtuelle et installé l'agent, mais ma machine virtuelle est mise en quarantaine. Que dois-je faire ?

Si vous rencontrez ce problème, essayez ce qui suit :

- Vérifiez que la balise NSX Cloud: `nsx.managed` et sa valeur : `default` sont correctement entrées. Ces informations sont sensibles à la casse.
- Resynchronisez le compte AWS ou Microsoft Azure à partir de CSM.
 - Connectez-vous à CSM.
 - Accédez à **Clouds > AWS/Azure > Comptes**.
 - Cliquez sur **Actions** depuis la vignette de compte de cloud public et cliquez sur **Resynchroniser le compte**.

Que dois-je faire si je ne peux pas accéder à ma machine virtuelle de charge de travail ?

Dans certains cas rares, vous pouvez perdre la connectivité à vos machines virtuelles de charge de travail Linux ou Windows gérées. Essayez les étapes décrites ci-dessous :

À partir de votre Cloud Public (AWS ou Microsoft Azure)

- Vérifiez que tous les ports sur la machine virtuelle, y compris ceux gérés par NSX Cloud, le pare-feu du système d'exploitation (Microsoft Windows ou IPTables) et NSX-T Data Center sont correctement configurés afin d'autoriser le trafic.

Par exemple, pour autoriser ping pour une machine virtuelle, les éléments suivants doivent être correctement configurés :

- Groupe de sécurité sur AWS ou Microsoft Azure. Pour plus d'informations, reportez-vous à la section [Gérer la stratégie de mise en quarantaine](#).
- Règles DFW de NSX-T Data Center. Reportez-vous à [Accéder aux machines virtuelles de charge de travail gérées](#) pour plus de détails.
- Pare-feu Windows ou IPTables sous Linux.
- Essayez de résoudre le problème en vous connectant à la machine virtuelle à l'aide de SSH ou d'autres méthodes, par exemple, la console série dans Microsoft Azure.
- Vous pouvez redémarrer la machine virtuelle verrouillée.
- Si vous ne pouvez toujours pas accéder à la machine virtuelle, connectez une carte réseau secondaire à la machine virtuelle de charge de travail, à partir de laquelle vous pourrez accéder à cette machine.

Opérations et gestion

17

Il est possible que vous deviez modifier la configuration des dispositifs que vous avez installés, par exemple, ajouter des licences, des certificats et modifier des mots de passe. Il existe également des tâches de maintenance de routine que vous devez effectuer, notamment l'exécution de sauvegardes. De plus, il existe des outils qui vous permettent de rechercher des informations sur les dispositifs qui font partie de l'infrastructure NSX-T Data Center et des réseaux logiques créés par NSX-T Data Center, notamment la journalisation de système distant, Traceflow et les connexions de port.

Ce chapitre contient les rubriques suivantes :

- [Ajouter une clé de licence](#)
- [Gestion des comptes d'utilisateur et du contrôle d'accès basé sur les rôles](#)
- [Configuration de certificats](#)
- [Configuration de dispositifs](#)
- [Ajouter un gestionnaire de calcul](#)
- [Gérer les balises](#)
- [Rechercher des objets](#)
- [Rechercher l'empreinte digitale SSH d'un serveur distant](#)
- [Sauvegarde et restauration de NSX Manager](#)
- [Gestion de dispositifs et de clusters de dispositifs](#)
- [Messages de journal](#)
- [Configurer IPFIX](#)
- [Suivre le chemin d'un paquet avec Traceflow](#)
- [Afficher les informations de connexion du port](#)
- [Surveiller l'activité d'un port de commutateur logique](#)
- [Surveiller des sessions de mise en miroir de ports](#)
- [Surveiller les nœuds d'infrastructure](#)
- [Afficher des données sur les applications exécutées sur des machines virtuelles](#)

- [Collecte des bundles de support](#)
- [Programme d'amélioration du produit](#)

Ajouter une clé de licence

Vous pouvez utiliser l'interface utilisateur de NSX Manager pour ajouter une ou plusieurs clés de licence.

Les types de licence de non-évaluation suivantes sont disponibles :

- Standard
- Avancé
- Enterprise

Lorsque vous installez NSX Manager, une licence d'évaluation préinstallée s'active et est valide pendant 60 jours. La licence d'évaluation fournit toutes les fonctionnalités d'une licence Enterprise. Vous ne pouvez pas installer ou annuler l'attribution d'une licence d'évaluation.

Vous pouvez installer une ou plusieurs des licences de non-évaluation mais, pour chaque type, vous ne pouvez installer qu'une seule clé. Lorsque vous installez une licence standard, avancée ou Enterprise, la licence d'évaluation n'est plus disponible. Vous pouvez également annuler l'attribution de licences de non-évaluation. Si vous annulez l'attribution de toutes les licences de non-évaluation, la licence d'évaluation est restaurée.

Si vous disposez de plusieurs clés du même type de licence et que vous voulez combiner les clés, vous devez accéder à <https://my.vmware.com> et utiliser la fonctionnalité Combiner des clés. L'interface utilisateur de NSX Manager n'offre pas cette fonctionnalité.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur *https://<adresse-ip-nsx-manager>*.
- 2 Sélectionnez **Système > Configuration > Licence** dans le panneau de navigation.
- 3 Cliquez sur **Ajouter** pour entrer la clé de licence.
- 4 Cliquez sur **Enregistrer**.

Gestion des comptes d'utilisateur et du contrôle d'accès basé sur les rôles

Les dispositifs NSX-T Data Center ont deux utilisateurs prédéfinis : administrateur et audit. Vous pouvez intégrer NSX-T Data Center à VMware Identity Manager (vIDM) et configurer le contrôle d'accès basé sur les rôles (RBAC) pour les utilisateurs que vIDM gère.

Pour les utilisateurs gérés par vIDM, la stratégie d'authentification qui s'applique est celle configurée par l'administrateur vIDM et non la stratégie d'authentification de NSX-T Data Center qui s'applique uniquement aux administrateurs et aux auditeurs.

Modifier le mot de passe de l'utilisateur de l'interface de ligne de commande

Chaque dispositif a deux utilisateurs intégrés, admin et audit, que vous pouvez utiliser pour vous connecter et exécuter des commandes d'interface de ligne de commande. Vous pouvez modifier le mot de passe de ces utilisateurs, mais vous ne pouvez pas ajouter ou supprimer des utilisateurs.

Procédure

- 1 Connectez-vous à l'interface de ligne de commande du dispositif.
- 2 Exécutez la commande `set user`. Par exemple,

```
nsx> set user admin
Current password:
New password:
Confirm new password:
nsx>
```

Le mot de passe doit respecter les exigences de complexité suivantes :

- Au moins huit caractères
- Au moins un caractère majuscule
- Au moins un caractère minuscule
- Au moins un caractère numérique
- Au moins un caractère spécial

Paramètres de stratégie d'authentification

Vous pouvez afficher ou modifier les paramètres de stratégie d'authentification via l'interface de ligne de commande.

Vous pouvez voir ou définir la longueur minimale du mot de passe avec les commandes suivantes :

```
get auth-policy minimum-password-length
set auth-policy minimum-password-length <password-length>
```

Les commandes suivantes s'appliquent pour se connecter à l'interface utilisateur de NSX Manager ou pour passer un appel d'API :

```
get auth-policy api lockout-period
get auth-policy api lockout-reset-period
get auth-policy api max-auth-failures
set auth-policy api lockout-period <lockout-period>
set auth-policy api lockout-reset-period <lockout-reset-period>
set auth-policy api max-auth-failures <auth-failures>
```

Les commandes suivantes s'appliquent pour se connecter à l'interface de ligne de commande sur un nœud NSX Manager, NSX Controller ou NSX Edge :

```
get auth-policy cli lockout-period
get auth-policy cli max-auth-failures
set auth-policy cli lockout-period <lockout-period>
set auth-policy cli max-auth-failures <auth-failures>
```

Pour plus d'informations sur les commandes d'interface de ligne de commande, consultez la *Référence de l'interface de ligne de commande NSX-T*.

Par défaut, après cinq tentatives successives infructueuses de connexion à l'interface utilisateur de NSX Manager, le compte d'administrateur est verrouillé pendant 15 minutes. Vous pouvez désactiver le verrouillage de compte avec la commande suivante :

```
set auth-policy api lockout-period 0
```

De même, vous pouvez désactiver le verrouillage de compte pour l'interface de ligne de commande avec la commande suivante :

```
set auth-policy cli lockout-period 0
```

Obtenir l'empreinte numérique de certificat à partir d'un hôte vIDM

Avant de configurer l'intégration de vIDM à NSX-T, vous devez obtenir l'empreinte numérique de certificat de l'hôte vIDM.

Procédure

- 1 Exécutez SSH sur l'hôte vIDM et connectez-vous en tant que **sshuser**.
- 2 Exécutez la commande suivante pour devenir l'utilisateur **racine**.

```
su root
```

- 3 Modifiez le fichier `/etc/ssh/sshd_config` et passez la valeur `PermitRootLogin` sur `yes` et la valeur `StrictModes` sur `no`.

```
PermitRootLogin yes
StrictModes no
```

- 4 Exécutez la commande suivante pour redémarrer le service `sshd`.

```
service sshd restart
```

- 5 Déconnectez-vous et connectez-vous en tant qu'utilisateur **racine**.
- 6 Exécutez la commande suivante pour modifier le directeur.

```
cd /usr/local/horizon/conf
```

7 Exécutez la commande suivante pour obtenir l'empreinte numérique.

```
openssl s_client -connect <FQDN of vIDM host>:443 < /dev/null 2>/dev/null | openssl x509 -
sha256 -fingerprint -noout -in /dev/stdin
```

Par exemple :

```
openssl s_client -connect vidm.corp.local:443 < /dev/null 2>/dev/null | openssl x509 -sha256 -
fingerprint -noout -in /dev/stdin
```

Associer un hôte vIDM à NSX-T

Pour activer l'intégration de NSX-T à vIDM, vous devez fournir des informations sur l'hôte vIDM.

Le serveur vIDM doit disposer d'un certificat signé par une autorité de certification (CA). Dans le cas contraire, la connexion à vIDM à partir de NSX Manager peut ne pas fonctionner avec certains navigateurs, tels que Microsoft Edge ou Internet Explorer 11. Pour plus d'informations sur l'installation d'un certificat signé par une autorité de certification sur vIDM, reportez-vous à la section <https://docs.vmware.com/fr/VMware-Identity-Manager/3.1/vidm-install/GUID-B76761BF-4B12-4CD5-9366-B0A1A2BF2A8B.html>.

Lorsque vous enregistrez NSX Manager auprès de vIDM, vous spécifiez une URI de redirection qui pointe vers NSX Manager. Vous pouvez indiquer le nom de domaine complet ou l'adresse IP. Il est important de se souvenir si vous utilisez le nom de domaine complet ou l'adresse IP. Lorsque vous essayez de vous connecter à NSX Manager via vIDM, vous devez spécifier le nom d'hôte dans l'URL de la même manière, c'est-à-dire, si vous utilisez le nom de domaine complet lors de l'enregistrement du gestionnaire dans vIDM, vous devez utiliser le nom de domaine complet dans l'URL, et si vous utilisez l'adresse IP lors de l'enregistrement du gestionnaire dans vIDM, vous devez utiliser l'adresse IP dans l'URL. Dans le cas contraire, la connexion échouera.

Conditions préalables

- Vérifiez que vous disposez de l'empreinte numérique du certificat de l'hôte vIDM. Reportez-vous à la section [Obtenir l'empreinte numérique de certificat à partir d'un hôte vIDM](#).
- Vérifiez que NSX Manager est enregistré en tant que client OAuth sur l'hôte vIDM. Lors du processus d'enregistrement, notez l'identifiant de client et le secret de client. Pour plus d'informations, consultez la documentation de VMware Identity Manager à l'adresse <https://www.vmware.com/support/pubs/identitymanager-pubs.html>.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Système > Utilisateurs** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Configuration**.
- 4 Cliquez sur **Modifier**.

5 Fournissez les informations suivantes.

Paramètre	Description
Dispositif VMware Identity Manager	Nom de domaine complet (FQDN) de l'hôte vIDM.
ID de client	L'identifiant est créé lors de l'enregistrement de NSX Manager sur l'hôte vIDM.
Secret du client	Code secret créé lors de l'enregistrement de NSX Manager sur l'hôte vIDM.
Empreinte numérique	Empreinte numérique du certificat de l'hôte vIDM.
Dispositif NSX	Adresse IP ou nom de domaine complet (FQDN) de NSX Manager. Si vous spécifiez un nom de domaine complet, vous devez accéder à NSX Manager à partir d'un navigateur à l'aide du nom de domaine complet du responsable dans l'URL, et si vous spécifiez une adresse IP, vous devez utiliser l'adresse IP dans l'URL. L'administrateur vIDM peut également configurer le client NSX Manager pour que vous puissiez vous connecter en utilisant le nom de domaine complet ou l'adresse IP.

6 Cliquez sur **Enregistrer**.

Synchronisation de l'heure entre NSX Manager, vIDM et les composants associés

Pour que l'authentification fonctionne correctement, NSX Manager, vIDM et les autres fournisseurs de service, tels qu'Active Directory, doivent tous être synchronisés. Cette section décrit comment synchroniser l'heure de ces composants.

VMware Infrastructure

Suivez les instructions des articles de la base de connaissances suivants pour synchroniser les hôtes ESXi.

- <https://kb.vmware.com/kb/1003736>
- <https://kb.vmware.com/kb/2012069>

Pour plus d'informations sur la synchronisation des machines virtuelles et de l'hôte, reportez-vous à la section https://docs.vmware.com/fr/VMware-vSphere/6.0/com.vmware.vsphere.vm_admin.doc/GUID-C0D8326A-B6E7-4E61-8470-6C173FDDF656.html. Les machines virtuelles peuvent exécuter NSX Manager, vIDM, Active Directory ou d'autres fournisseurs de services.

Infrastructure de tiers

Suivez les instructions de la documentation du fournisseur pour synchroniser les machines virtuelles et les hôtes.

Configuration de NTP sur le serveur vIDM (non recommandé)

Si vous n'êtes pas en mesure de synchroniser l'heure entre les hôtes, vous pouvez désactiver la synchronisation sur l'hôte et configurer le protocole NTP sur le serveur vIDM. Cette méthode n'est pas recommandée, car elle requiert l'ouverture du port UDP 123 sur le serveur vIDM.

- Vérifiez l'horloge sur le serveur vIDM et assurez-vous qu'elle indique une heure correcte.

```
# hwclock
Tue May 9 12:08:43 2017 -0.739213 seconds
```

- Modifiez le fichier `/etc/ntp.conf` et ajoutez les entrées suivantes si elles n'y figurent pas.

```
server server time.nist.gov
server server pool.ntp.org
server server time.is dynamic
```

- Ouvrez le port UDP 123.

```
# iptables -A INPUT -p udp --dport 123 -j ACCEPT
```

Exécutez la commande suivante pour vérifier que le port est ouvert.

```
# iptables -L -n
```

- Démarrez le service NTP.

```
/etc/init.d/ntp start
```

- Définissez l'exécution automatique de NTP après un redémarrage.

```
# chkconfig --add ntp
# chkconfig ntp on
```

- Vérifiez que le serveur NTP est accessible.

```
# ntpq -p
```

La colonne `reach` ne doit pas indiquer 0. La colonne `st` doit afficher un chiffre différent de 16.

Contrôle d'accès basé sur les rôles

Avec le contrôle d'accès basé sur les rôles (RBAC), vous pouvez limiter l'accès du système aux utilisateurs autorisés. Des rôles sont attribués aux utilisateurs et chaque rôle dispose d'autorisations spécifiques.

Il existe quatre types d'autorisations :

- Accès complet
- Exécution
- Lecture

- Aucun

L'accès complet attribue toutes les autorisations à l'utilisateur. L'autorisation d'exécution inclut l'autorisation de lecture.

NSX-T Data Center comporte les rôles prédéfinis suivants. Vous ne pouvez pas ajouter de nouveaux rôles.

- Administrateur d'entreprise
- Auditeur
- Ingénieur réseau
- Opérations réseau
- Ingénieur sécurité
- Opérations de sécurité
- Administrateur de service Cloud
- Auditeur de service Cloud
- Administrateur d'équilibrage de charge
- Auditeur d'équilibrage de charge

Une fois qu'un rôle est attribué à un utilisateur Active Directory (AD), si le nom d'utilisateur est modifié sur le serveur AD, vous devez attribuer le rôle à nouveau en utilisant le nouveau nom d'utilisateur.

Rôles et autorisations

[Tableau 17-1. Rôles et autorisations](#) affiche les autorisations dont chaque rôle dispose pour différentes opérations. Les abréviations suivantes sont utilisées :

- AE : administrateur d'entreprise
- A : auditeur
- IR : ingénieur réseau
- OR : opérations réseau
- IS : ingénieur sécurité
- OS : opérations de sécurité
- Adm SC : administrateur de service cloud
- Aud SC : auditeur de service cloud
- Adm EC : administrateur d'équilibrage de charge
- Aud EC : auditeur d'équilibrage de charge
- AC : accès complet
- E : Exécution

■ L : Lecture

Tableau 17-1. Rôles et autorisations

Opération	AE	A	IR	OR	IS	OS	Adm SC	Aud SC	Adm EC	Aud EC
Outils > Connexion de port	E	L	E	E	E	E	E	L	E	E
Outils > Traceflow	E	L	E	E	E	E	E	L	E	E
Outils > Mise en miroir de ports	AC	L	AC	AC	AC	AC	AC	L	Aucun	Aucun
Outils > IPFIX	AC	L	AC	L	AC	L	AC	L	Aucun	Aucun
Pare-feu > Général	AC	L	L	L	AC	L	AC	L	Aucun	Aucun
Pare-feu > Configuration	AC	L	L	L	AC	L	AC	L	Aucun	Aucun
Chiffrement	AC	L	AC	L	AC	AC	Aucun	Aucun	Aucun	Aucun
Routage > Routeurs	AC	L	AC	L	L	L	AC	L	L	L
Routage > NAT	AC	L	AC	L	AC	L	AC	L	L	L
DHCP > Profils de serveur	AC	L	AC	L	AC	Aucun	AC	L	Aucun	Aucun
DHCP > Serveurs	AC	L	AC	L	AC	Aucun	AC	L	Aucun	Aucun
DHCP > Profils de relais	AC	L	AC	L	AC	Aucun	AC	L	Aucun	Aucun
DHCP > Services de relais	AC	L	AC	L	AC	Aucun	AC	L	Aucun	Aucun
DHCP > Proxys de métadonnées	AC	L	AC	L	AC	Aucun	Aucun	Aucun	Aucun	Aucun
IPAM	AC	L	AC	L	AC	Aucun	Aucun	Aucun	Aucun	Aucun
Commutation > Commutateurs	AC	L	AC	AC	L	L	AC	L	L	L
Commutation > Ports	AC	L	AC	AC	L	L	AC	L	L	L
Commutation > Profils de commutation	AC	L	AC	AC	AC	AC	AC	L	L	L

Tableau 17-1. Rôles et autorisations (suite)

Opération	AE	A	IR	OR	IS	OS	Adm SC	Aud SC	Adm EC	Aud EC
Équilibrage de charge > Équilibrages de charge	AC	L	Aucun	Aucun	Aucun	Aucun	AC	L	AC	L
Équilibrage de charge > Serveurs virtuels	AC	L	Aucun	Aucun	Aucun	Aucun	AC	L	AC	L
Équilibrage de charge > Profils > Profils d'application	AC	L	Aucun	Aucun	Aucun	Aucun	AC	L	AC	L
Équilibrage de charge > Profils > Profils de persistance	AC	L	Aucun	Aucun	Aucun	Aucun	AC	L	AC	L
Équilibrage de charge > Profils > Profils SSL	AC	L	Aucun	Aucun	AC	L	AC	L	AC	L
Équilibrage de charge > Pools de serveurs	AC	L	Aucun	Aucun	Aucun	Aucun	AC	L	AC	L
Équilibrage de charge > Moniteurs	AC	L	Aucun	Aucun	Aucun	Aucun	AC	L	AC	L
Inventaire > Groupes	AC	L	AC	L	AC	L	AC	L	L	L
Inventaire > Ensembles d'adresses IP	AC	L	AC	L	AC	L	AC	L	L	L
Inventaire > Pools d'adresses IP	AC	L	AC	L	Aucun	L	Aucun	Aucun	L	L
Inventaire > Ensembles d'adresses MAC	AC	L	AC	L	AC	L	AC	L	L	L
Inventaire > Services	AC	L	AC	L	AC	L	AC	L	L	L

Tableau 17-1. Rôles et autorisations (suite)

Opération	AE	A	IR	OR	IS	OS	Adm SC	Aud SC	Adm EC	Aud EC
Inventaire > Machines virtuelles	L	L	L	L	L	L	L	L	L	L
Inventaire > VM > Créer et attribuer des balises	AC	L	AC	AC	AC	AC	AC	L	L	L
Inventaire > VM > Configurer des balises	AC	Aucun	Aucun	Aucun	AC	Aucun	Aucun	Aucun	Aucun	Aucun
Infrastructure > Nœuds > Hôtes	AC	L	L	L	L	L	L	L	Aucun	Aucun
Infrastructure > Nœuds > Nœuds	AC	L	AC	L	AC	L	L	L	Aucun	Aucun
Infrastructure > Nœuds > Dispositifs Edge	AC	L	AC	L	L	L	L	L	Aucun	Aucun
Infrastructure > Nœuds > Clusters Edge	AC	L	AC	L	L	L	L	L	Aucun	Aucun
Infrastructure > Nœuds > Ponts	AC	L	AC	L	L	L	Aucun	Aucun	L	L
Infrastructure > Nœuds > Nœuds de transport	AC	L	L	L	L	L	L	L	L	L
Infrastructure > Nœuds > Tunnels	L	L	L	L	L	L	L	L	L	L
Infrastructure > Profils > Profils de liaison montante	AC	L	L	L	L	L	L	L	L	L
Infrastructure > Profils > Profils de cluster Edge	AC	L	AC	L	L	L	L	L	L	L

Tableau 17-1. Rôles et autorisations (suite)

Opération	AE	A	IR	OR	IS	OS	Adm SC	Aud SC	Adm EC	Aud EC
Infrastructure > Profils > Configuration	AC	L	Aucun	Aucun	Aucun	Aucun	L	L	Aucun	Aucun
Infrastructure > Zones de transport > Zones de transport	AC	L	L	L	L	L	L	L	L	L
Infrastructure > Zones de transport > Profils de zone de transport	AC	L	L	L	L	L	L	L	L	L
Infrastructure > Gestionnaires de calcul	AC	L	L	L	L	L	L	L	Aucun	Aucun
Système > Approuver	AC	L	Aucun	Aucun	AC	L	Aucun	Aucun	AC	L
Système > Configuration	E	L	L	L	L	L	Aucun	Aucun	Aucun	Aucun
Système > Utilitaires > Bundle de support	AC	L	L	L	L	L	L	L	Aucun	Aucun
Système > Utilitaires > Sauvegarde	AC	L	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun
Système > Utilitaires > Restaurer	AC	L	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun
Système > Utilitaires > Mettre à niveau	AC	L	L	L	L	L	Aucun	Aucun	Aucun	Aucun
Système > Utilisateurs > Attributions de rôles	AC	L	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun
Système > Utilisateurs > Configuration	AC	L	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun

Gérer les attributions de rôles

Vous pouvez ajouter, modifier et supprimer des attributions de rôles à des utilisateurs ou des groupes d'utilisateurs si VMware Identity Manager est intégré à NSX-T Data Center.

Conditions préalables

- Vérifiez qu'un hôte vIDM est associé à NSX-T. Pour plus d'informations, reportez-vous à la section [Associer un hôte vIDM à NSX-T](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Système > Utilisateurs** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Attributions de rôles** s'il n'est pas déjà sélectionné.
- 4 Ajoutez, modifiez ou supprimez des attributions de rôles.

Option	Actions
Ajouter des attributions de rôles	Cliquez sur Ajouter , sélectionnez des utilisateurs ou des groupes d'utilisateurs et sélectionnez des rôles.
Modifier des attributions de rôles	Sélectionnez un utilisateur ou un groupe d'utilisateurs, et cliquez sur Modifier .
Supprimer des attributions de rôles	Sélectionnez un utilisateur ou un groupe d'utilisateurs, et cliquez sur Supprimer .

Afficher des identités de principal

Un principal peut être un composant NSX-T Data Center ou une application tierce, telle qu'un produit OpenStack. Avec une identité de principal, un principal peut utiliser le nom d'identité pour créer un objet et s'assurer que seule une entité portant le même nom d'identité peut modifier ou supprimer l'objet.

Une identité de principal possède les propriétés suivantes :

- Nom
- ID de nœud
- Certificat
- Rôle RBAC indiquant les droits d'accès de ce principal
- Indicateur qui signale si les objets créés par ce principal sont protégés

Les utilisateurs (locaux, distants ou avec identité de principal) ayant le rôle d'administrateur d'entreprise peuvent modifier ou supprimer des objets appartenant à des identités de principal. Les utilisateurs (locaux, distants ou avec identité de principal) n'ayant pas le rôle d'administrateur d'entreprise ne peuvent pas modifier ou supprimer des objets appartenant à des identités de principal, mais peuvent modifier ou supprimer les objets non protégés. Un utilisateur administrateur d'entreprise peut uniquement supprimer les objets protégés à l'aide de l'API NSX-T Data Center mais pas de l'interface utilisateur de NSX Manager.

Une identité de principal peut être uniquement créée ou supprimée à l'aide de l'API NSX-T. Pour plus d'informations, reportez-vous à *La référence API de NSX-T Data Center*. Cependant, vous pouvez afficher les identités de principal via l'interface utilisateur de NSX Manager.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Système > Utilisateurs** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Attributions de rôles**.

Les utilisateurs, les groupes d'utilisateurs et des identités de principal sont affichés.

Configuration de certificats

Vous pouvez générer une demande de signature de certificat (CSR) dans NSX Manager et l'envoyer à une autorité de certification afin d'obtenir un certificat de serveur.

La CSR peut également être utilisée pour générer des certificats auto-signés. Si vous disposez d'un certificat existant ou d'un certificat d'autorité de certification, vous pouvez l'importer et l'utiliser. Vous pouvez également importer une liste de révocation des certificats (CRL) qui inclut des certificats révoqués.

Créer un fichier de demande de signature de certificat

Une demande de signature de certificat (CSR) est un texte chiffré qui contient des informations spécifiques telles que le nom de l'organisation, le nom commun, la ville et le pays. Vous envoyez le fichier CSR à une autorité de certification pour demander un certificat d'identité numérique.

Conditions préalables

- Collectez les informations dont vous avez besoin pour remplir le fichier CSR. Vous devez connaître le FQDN du serveur, ainsi que l'unité d'organisation, l'organisation, la ville, l'état et le pays.
- Vérifiez que les paires clé publique/clé privée sont disponibles.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Système > Approbation** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **CSRS**.
- 4 Cliquez sur **Générer une CSR**.

5 Renseignez les détails du fichier CSR.

Option	Description
Nom	Attribuez un nom à votre certificat.
Nom commun	Entrez le nom de domaine complet (FQDN) de votre serveur. Par exemple, test.vmware.com.
Nom de l'organisation	Entrez le nom de votre organisation avec les suffixes applicables. Par exemple, VMware Inc.
Unité de l'organisation	Entrez le service dans votre organisation qui gère ce certificat. Par exemple, service informatique.
Localité	Ajoutez la ville dans laquelle se situe votre organisation. Par exemple, Palo Alto.
État	Ajoutez l'état dans lequel se situe votre organisation. Par exemple, Californie.
Pays	Ajoutez le pays dans lequel se situe votre organisation. Par exemple, États-Unis (US).
Algorithme de message	Définissez l'algorithme de chiffrement pour votre certificat. Chiffrement RSA : utilisé pour les signatures numériques et le chiffrement du message. Par conséquent, il est plus lent que DSA lors de la création d'un jeton chiffré, mais plus rapide pour analyser et valider ce jeton. Ce chiffrement est plus lent pour déchiffrer et plus rapide pour chiffrer. Chiffrement DSA : utilisé pour les signatures numériques. Par conséquent, il est plus rapide que RSA lors de la création d'un jeton chiffré, mais plus lent pour analyser et valider ce jeton. Ce chiffrement est plus rapide pour déchiffrer et plus lent pour chiffrer.
Taille de la clé	Définissez la taille de la clé en bits de l'algorithme de chiffrement. La valeur par défaut, 2048, est adéquate, sauf si vous avez besoin d'une taille de clé différente. Plusieurs autorités de certification requièrent une valeur minimale de 2048. Des tailles de clé supérieures sont plus sûres, mais ont un impact plus important sur les performances.
Description	Entrez des détails spécifiques pour vous aider à identifier ce certificat à une date ultérieure.

6 Cliquez sur **Enregistrer**.

Une CSR personnalisée s'affiche sous forme de lien.

7 Sélectionnez la CSR et cliquez sur **Actions**.

8 Sélectionnez **Télécharger CSR PEM** dans le menu déroulant.

Vous pouvez enregistrer le fichier CSR PEM pour vos dossiers et l'envoi à l'autorité de certification.

9 Utilisez le contenu du fichier CSR pour envoyer une demande de certificat à l'autorité de certification conformément au processus d'inscription de l'autorité de certification.

Résultats

L'autorité de certification crée un certificat de serveur en fonction des informations dans le fichier CSR, le signe avec sa clé privée et vous envoie le certificat. L'autorité de certification vous envoie également un certificat d'autorité de certification racine.

Importer un certificat d'autorité de certification

Vous pouvez importer un certificat d'autorité de certification signé afin de devenir une autorité de certification intermédiaire pour votre entreprise. Une fois que vous avez importé le certificat, vous avez l'autorité pour signer vos propres certificats.

Conditions préalables

Vérifiez qu'un certificat d'autorité de certification est disponible.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Système > Approbation** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Certificats**.
- 4 Sélectionnez **Importer > Importer un certificat d'autorité de certification** et entrez les détails du certificat.

Option	Description
Nom	Attribuez un nom au certificat d'autorité de certification.
Contenu du certificat	Accédez au fichier du certificat d'autorité de certification sur votre ordinateur et ajoutez le fichier.
Description	Entrez un résumé de ce qui est inclus dans ce certificat d'autorité de certification.

- 5 Cliquez sur **Enregistrer**.

Résultats

Vous pouvez désormais signer vos propres certificats.

Importer un certificat

Vous pouvez importer un certificat avec la clé privée pour créer des certificats auto-signés.

Conditions préalables

Vérifiez qu'un certificat est disponible.

Procédure

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

- 2 Sélectionnez **Système > Approbation** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Certificats**.
- 4 Sélectionnez **Importer > Importer un certificat** et entrez les détails du certificat.

Option	Description
Nom	Attribuez un nom au certificat d'autorité de certification.
Contenu du certificat	Accédez au fichier du certificat sur votre ordinateur et ajoutez le fichier.
Clé privée	Accédez au fichier de clé privée sur votre ordinateur et ajoutez le fichier.
Mot de passe	Ajoutez un mot de passe pour ce certificat.
Description	Entrez un résumé de ce qui est inclus dans ce certificat.

- 5 Cliquez sur **Enregistrer**.

Résultats

Vous pouvez maintenant créer vos propres certificats auto-signés.

Créer un certificat auto-signé

L'utilisation de certificats auto-signés peut être moins sûre que l'utilisation de certificats approuvés.

Lorsque vous utilisez un certificat auto-signé, l'utilisateur client reçoit un message d'avertissement tel que *Certificat de sécurité non valide*. L'utilisateur client doit ensuite accepter le certificat auto-signé lorsqu'il se connecte pour la première fois au serveur afin de continuer. Autoriser les utilisateurs clients à sélectionner cette option réduit la sécurité par rapport aux autres méthodes d'authentification.

Conditions préalables

Vérifiez qu'une demande de signature de certificat (CSR) est disponible. Reportez-vous à la section [Créer un fichier de demande de signature de certificat](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur *https://<adresse-ip-nsx-manager>*.
- 2 Sélectionnez **Système > Approbation** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **CSRS**.
- 4 Sélectionnez la CSR existante.
- 5 Cliquez sur **Actions** et sélectionnez **Certificat auto-signé pour la CSR** dans le menu déroulant.
- 6 Entrez le nombre de jours pendant lequel le certificat auto-signé est valide.
La durée par défaut est 10 ans.
- 7 Cliquez sur **Enregistrer**.

Résultats

Le certificat auto-signé s'affiche dans la liste **Certificat**. Le type de certificat est désigné comme auto-signé.

Remplacer un certificat

Lorsque vous devez remplacer un certificat (si votre certificat expire, par exemple), vous pouvez émettre un appel d'API pour remplacer le certificat existant.

Conditions préalables

Vérifiez qu'un certificat est disponible dans le dispositif NSX Manager. Reportez-vous aux sections [Créer un certificat auto-signé](#) et [Importer un certificat](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Système > Approbation** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Certificats**.
- 4 Cliquez sur l'ID du certificat que vous voulez utiliser et copiez l'ID de certificat dans la fenêtre contextuelle.
- 5 Utilisez l'appel d'API POST `/api/v1/node/services/http?action=apply_certificate` pour remplacer le certificat existant. Par exemple,

```
POST https://<nsx-mgr>/api/v1/node/services/http?
action=apply_certificate&certificate_id=e61c7537-3090-4149-b2b6-19915c20504f
```

Pour plus d'informations, reportez-vous à *La référence API de NSX-T*.

Résultats

L'appel d'API redémarre le service HTTP pour qu'il commence à utiliser le nouveau certificat. Lorsque la demande POST est réussie, le code de réponse est 200 `Accepté`.

Importer une liste de révocation des certificats

Une liste de révocation des certificats (CRL) est une liste d'abonnés avec l'état de leur certificat. Lorsqu'un utilisateur potentiel tente d'accéder à un serveur, le serveur autorise ou refuse l'accès en fonction de l'entrée CRL associée à cet utilisateur.

La liste contient les éléments suivants :

- Les certificats révoqués et les motifs de la révocation
- Les dates d'émission des certificats

- Les entités ayant émis les certificats
- Une date proposée pour la prochaine version

Conditions préalables

Vérifiez qu'une liste CRL est disponible.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur *https://<adresse-ip-nsx-manager>*.
- 2 Sélectionnez **Système > Approbation** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **CRLS**.
- 4 Cliquez sur **Importer** et ajoutez les informations de la liste CRL.

Option	Description
Nom	Attribuez un nom à la liste CRL.
Contenu du certificat	<p>Copiez tous les éléments de la liste CRL et collez-les dans cette section.</p> <p>Exemple de liste CRL.</p> <pre style="background-color: #f0f0f0; padding: 10px;">-----BEGIN X509 CRL----- MIIBODCB4zANBgkqhkiG9w0BAQQFADBGMQswCQYDVQQGEwJBVTENMAoGA1UECBM D UUxEMRkwFwYDVQQKEwBNaW5jb20gUHR5LiBMdGQuMQswCQYDVQQLEwJDUzEhMBk G A1UEAxMSU1NMZWZ5IGRlbW8gc2VydMvyFw0wMTAxMTUxNjI2NTdaFw0wMTAyMTQ x NjI2NTdaMFIwEgIBARcNOTUxMDA5MjMzMjA1WjAsAgEDFw05NTEyMDEwMTAwMDEB a MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMA0GCSq G SIb3DQEBAUAA0EAHPjQ3M93Q0j8Ufi+jZM7Y78TfAzG4jJn/ E6MYBPFVQFY0/Gp UZexfjSVo5CIyyS0tYscz8o07avwBxTiMpDEQg== -----END X509 CRL--</pre>
Description	Entrez un résumé de ce qui est inclus dans cette liste CRL.

- 5 Cliquez sur **Enregistrer**.

Résultats

La liste CRL importée apparaît sous forme de lien.

Importer un certificat pour une demande de signature de certificat

Vous pouvez importer un certificat signé pour une demande de signature de certificat.

Lorsque vous utilisez un certificat auto-signé, l'utilisateur client reçoit un message d'avertissement tel que **Certificat de sécurité non valide**. L'utilisateur client doit ensuite accepter le certificat auto-signé lorsqu'il se connecte pour la première fois au serveur afin de continuer. Autoriser les utilisateurs clients à sélectionner cette option réduit la sécurité par rapport aux autres méthodes d'authentification.

Conditions préalables

Vérifiez qu'une demande de signature de certificat (CSR) est disponible. Reportez-vous à la section [Créer un fichier de demande de signature de certificat](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Système > Approbation** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **CSRS**.
- 4 Sélectionnez la CSR existante.
- 5 Cliquez sur **Actions** et sélectionnez **Importer le certificat pour la CSR** dans le menu déroulant.
- 6 Accédez au fichier du certificat signé sur votre ordinateur et ajoutez le fichier.
- 7 Cliquez sur **Enregistrer**.

Résultats

Le certificat auto-signé s'affiche dans la liste **Certificat**. Le type de certificat est désigné comme auto-signé.

Configuration de dispositifs

Certaines tâches de configuration système doivent être effectuées à l'aide de la ligne de commande ou de l'API.

Pour obtenir des informations complètes sur l'interface de ligne de commande, consultez le document *NSX-T Data Center Command-Line Interface Reference* (Référence de l'interface de ligne de commandes de NSX). Pour des informations complètes sur l'API, consultez le document *NSX-T Data Center API Guide* (Guide de l'API de NSX).

Tableau 17-2. Commandes de configuration système et demandes API.

Tâche	Ligne de commande (NSX Manager, NSX Controller, NSX Edge)	Demande API (NSX Manager uniquement)
Définir le fuseau horaire du système	<code>set timezone <timezone></code>	PUT <code>https://<nsx-mgr>/api/v1/node</code>
Définir le serveur NTP	<code>set ntp-server <ntp-server></code>	PUT <code>https://<nsx-mgr>/api/v1/node/services/ntp</code>

Tableau 17-2. Commandes de configuration système et demandes API. (suite)

Tâche	Ligne de commande (NSX Manager, NSX Controller, NSX Edge)	Demande API (NSX Manager uniquement)
Définir le serveur DNS	set name-servers <dns-server>	PUT https://<nsx-mgr>/api/v1/node/network/name-servers
Définir le domaine de recherche DNS	set search-domains <domain>	PUT https://<nsx-mgr>/api/v1/node/network/search-domains

Ajouter un gestionnaire de calcul

Un gestionnaire de calcul, par exemple, vCenter Server, est une application qui gère les ressources, telles que des hôtes et des machines virtuelles. NSX-T Data Center interroge les gestionnaires de calcul pour connaître les modifications, telles que l'ajout ou la suppression d'hôtes ou de machines virtuelles, et met à jour son inventaire en conséquence. L'ajout d'un gestionnaire de calcul est facultatif, NSX-T obtenant des informations d'inventaire, même sans gestionnaire de calcul, comme des machines virtuelles et des hôtes autonomes.

Dans cette version, cette fonctionnalité prend en charge :

- vCenter Server versions 6.5 Update 1, 6.5 Update 2 et 6.7.
- Les communications IPv6 et IPv4 avec vCenter Server.
- Un maximum de 5 gestionnaires de calcul.

Procédure

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

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

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

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

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

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

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

Résultats

Le panneau Gestionnaires de calcul affiche une liste de gestionnaires de calcul. Vous pouvez cliquer sur le nom du gestionnaire pour voir ou modifier ses détails ou pour gérer les balises qui s'appliquent au gestionnaire.

Gérer les balises

Vous pouvez ajouter des balises à des objets pour faciliter la recherche. Lorsque vous spécifiez une balise, vous pouvez également spécifier une étendue.

Remarques concernant NSX Cloud Si vous utilisez NSX Cloud, reportez-vous à la section [Comment utiliser des fonctionnalités NSX-T Data Center avec le cloud public](#) pour obtenir la liste des entités logiques générées automatiquement, les fonctionnalités prises en charge et les configurations requises pour NSX Cloud.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur *https://<adresse-ip-nsx-manager>*.
- 2 Naviguez jusqu'à une catégorie d'objets.
Par exemple, naviguez jusqu'à **Commutation > Commutateurs**.
- 3 Cliquez sur le nom d'un commutateur.
- 4 Sélectionnez l'option de menu **Actions > Gérer les balises** ou cliquez sur **Gérer** en regard de Balises.
- 5 Ajoutez ou supprimez des balises.

Option	Action
Ajouter une balise	Cliquez sur Ajouter pour indiquer une balise et éventuellement sélectionner une étendue.
Supprimer une balise	Sélectionnez une balise et cliquez sur Supprimer .

Un objet peut contenir un maximum de 30 balises. La longueur maximale d'une balise est de 256 caractères. La longueur maximale d'une étendue est de 128 caractères.

- 6 Cliquez sur **Enregistrer**.

Rechercher des objets

Vous pouvez rechercher des objets à l'aide de différents critères tout au long de l'inventaire de NSX-T Data Center.

Les résultats de la recherche sont triés par pertinence et vous pouvez filtrer ces résultats en fonction de votre requête de recherche.

Note Si votre requête de recherche contient des caractères spéciaux qui fonctionnent également comme des opérateurs, vous devez ajouter une barre oblique de début. Les caractères qui fonctionnent comme des opérateurs sont : +, -, =, &&, ||, <, >, !, (,), {, }, [,], ^, ", ~, ?, :, /, \.

Procédure

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

- 2 Sur la page d'accueil, entrez un modèle de recherche pour un objet ou un type d'objet.

Lorsque vous entrez votre modèle de recherche, la fonction de recherche fournit une assistance en indiquant les mots clés applicables.

Recherche	Requête de recherche
Objets avec Logique comme nom ou propriété	Logique
Nom exact du commutateur logique	display_name:LSP-301
Noms contenant des caractères spéciaux tels que !	Logique!

Tous les résultats des recherches connexes sont répertoriés et regroupés par type de ressource dans différents onglets.

Vous pouvez cliquer sur les onglets pour afficher les résultats de recherches spécifiques pour un type de ressource.

- 3 (Facultatif) Dans la barre de recherche, cliquez sur Enregistrer pour enregistrer vos critères de recherche affinés.

- 4 Dans la barre de recherche, cliquez sur l'icône  pour ouvrir la colonne de recherche avancée dans laquelle vous pouvez affiner votre recherche.

- 5 Spécifiez un ou plusieurs critères pour affiner votre recherche.

- Nom
- Type de ressource

- Description
- ID
- Créé par
- Modifié par
- Balises
- Date de création
- Date de modification

Vous pouvez également afficher les résultats de vos recherches récentes et les critères de recherche que vous avez enregistrés.

- 6 (Facultatif) Cliquez sur **Tout effacer** pour réinitialiser vos critères de recherche avancée.

Rechercher l'empreinte digitale SSH d'un serveur distant

Certaines demandes API qui impliquent la copie de fichiers sur ou depuis un serveur distant requièrent que vous fournissiez l'empreinte digitale SSH pour le serveur distant dans le corps de la demande. L'empreinte digitale SSH est dérivée d'une clé hôte sur le serveur distant.

Pour se connecter via SSH, NSX Manager et le serveur distant doivent disposer d'un type de clé hôte en commun. S'il existe plusieurs types de clés hôtes en commun, celle qui est la préférée selon la configuration HostKeyAlgorithm sur NSX Manager est utilisée.

Disposer de l'empreinte digitale d'un serveur distant vous permet de vérifier que vous vous connectez au serveur correct, ce qui vous protège des attaques d'intercepteur. Vous pouvez demander à l'administrateur du serveur distant s'il peut fournir l'empreinte digitale SSH du serveur. Ou vous pouvez vous connecter au serveur distant pour rechercher l'empreinte digitale. Il est plus sûr de se connecter au serveur sur la console que sur le réseau.

Le tableau suivant répertorie les éléments que NSX Manager prend en charge du plus préféré au moins préféré.

Tableau 17-3. Clés hôtes de NSX Manager en ordre de préférence

Types de clés hôtes pris en charge par NSX Manager	Emplacement par défaut de la clé
ECDSA (256 bits)	/etc/ssh/ssh_host_ecdsa_key.pub
ED25519	/etc/ssh/ssh_host_ed25519_key.pub

Procédure

- 1 Connectez-vous au serveur distant en tant que racine.

La connexion à l'aide d'une console est plus sûre que sur le réseau.

- 2 Répertoriez les fichiers de clé publique dans le répertoire `/etc/ssh`.

```
$ ls -al /etc/ssh/*pub
-rw-r--r-- 1 root root 601 Apr  8 18:10 ssh_host_dsa_key.pub
-rw-r--r-- 1 root root  93 Apr  8 18:10 ssh_host_ed25519_key.pub
-rw-r--r-- 1 root root 393 Apr  8 18:10 ssh_host_rsa_key.pub
```

- 3 Comparez les clés disponibles à ce que NSX Manager prend en charge.

Dans cet exemple, ED25519 est la seule clé acceptable.

- 4 Obtenez l'empreinte digitale de la clé.

```
# awk '{print $2}' /etc/ssh/ssh_host_ed25519_key.pub | base64 -d | sha256sum -b | sed 's/ .*$//'
| xxd -r -p | base64 | sed 's/./44g' | awk '{print "SHA256:"$1}'
SHA256:KemgftCfsd/hn7EEflhJ4m1698rRhMmNN2IW8y9iq2A
```

Sauvegarde et restauration de NSX Manager

Si le dispositif NSX Manager devient inopérable, vous pouvez le restaurer à partir de la sauvegarde. Alors que le dispositif NSX Manager est inopérable, le plan de données n'est pas affecté, mais vous ne pouvez pas modifier la configuration.

Il existe trois types de sauvegardes :

Sauvegarde de cluster Cette sauvegarde inclut l'état souhaité du réseau virtuel.

Sauvegarde de nœud Il s'agit d'une sauvegarde du nœud NSX Manager.

Sauvegarde d'inventaire Cette sauvegarde inclut l'ensemble des hôtes ESX et KVM et des dispositifs Edge. Ces informations sont utilisées au cours d'une opération de restauration pour détecter et résoudre les différences entre l'état souhaité du plan de gestion et ces hôtes.

Il existe deux méthodes de sauvegarde :

Sauvegardes manuelles de nœud et de cluster de NSX Manager Les sauvegardes manuelles de nœud et de cluster peuvent être exécutées à tout moment en cas de besoin.

Sauvegarde de nœud, sauvegarde de cluster et sauvegarde d'inventaire automatisées de NSX Manager Les sauvegardes automatisées sont exécutées selon un planning que vous définissez. Les sauvegardes automatisées sont fortement recommandées. Reportez-vous à la section [Planifier des sauvegardes automatisées](#).

Pour vérifier que vous disposez d'une sauvegarde récente, vous devez configurer des sauvegardes automatisées. Il est important d'exécuter régulièrement des sauvegardes de cluster et d'inventaire.

Vous pouvez restaurer une configuration de NSX-T Data Center à l'état dans lequel elle est capturée dans n'importe quelle sauvegarde de cluster. Lors de la restauration d'une sauvegarde, vous devez effectuer la restauration vers un nouveau dispositif NSX Manager exécutant la même version de NSX Manager que le dispositif qui a été sauvegardé.

Sauvegarder la configuration de NSX Manager

La sauvegarde de la configuration de NSX Manager se compose de la sauvegarde de nœud, de la sauvegarde de cluster et de la sauvegarde d'inventaire de NSX Manager.

Procédure

1 Configurer l'emplacement de la sauvegarde

Les sauvegardes sont enregistrées sur un serveur de fichiers auquel NSX Manager peut accéder. Vous devez configurer l'emplacement de ce serveur avant d'effectuer une sauvegarde.

2 Planifier des sauvegardes automatisées

Planifiez des sauvegardes fréquentes pour pouvoir restaurer une instance inopérable de NSX Manager et ses données de configuration. Les sauvegardes automatisées sont désactivées par défaut. Vous pouvez planifier des sauvegardes automatisées pour qu'elles aient lieu certains jours de la semaine ou à un intervalle spécifié. Les sauvegardes planifiées sont fortement recommandées.

Configurer l'emplacement de la sauvegarde

Les sauvegardes sont enregistrées sur un serveur de fichiers auquel NSX Manager peut accéder. Vous devez configurer l'emplacement de ce serveur avant d'effectuer une sauvegarde.

Note De par sa conception, NSX Manager ne supprime pas les fichiers de sauvegarde sur le serveur de fichiers de sauvegarde. Vous devez gérer la rotation des sauvegardes et garantir que le serveur dispose de suffisamment d'espace disque pour les sauvegardes. Vous pouvez envisager d'exécuter un script qui supprime automatiquement les anciennes sauvegardes.

Conditions préalables

Vérifiez que vous disposez de l'empreinte digitale SSH du serveur de fichiers de sauvegarde. Seule une clé ECDSA avec hachage SHA256 est acceptée comme empreinte digitale. Reportez-vous à la section [Rechercher l'empreinte digitale SSH d'un serveur distant](#).

Procédure

- 1 Dans un navigateur, connectez-vous au dispositif NSX Manager en tant qu'administrateur à l'adresse `https://<adresse-ip-nsx-manager>`.
- 2 Cliquez sur **Système > Utilitaires > Sauvegarde**.
- 3 Pour fournir des informations d'identification d'accès à l'emplacement de sauvegarde, cliquez sur **Modifier** dans le coin supérieur droit de la page.
- 4 Cliquez sur le bouton **Sauvegarde automatique** pour activer les sauvegardes automatiques.

- 5 Entrez l'adresse IP ou le nom d'hôte du serveur de fichiers de sauvegarde.
- 6 Modifiez le port par défaut, si nécessaire.
- 7 Entrez le nom d'utilisateur et le mot de passe requis pour vous connecter au serveur de fichiers de sauvegarde.
- 8 Dans le champ **Répertoire de destination**, entrez le chemin de répertoire absolu d'enregistrement des sauvegardes.

Le répertoire doit déjà exister. Si vous disposez de plusieurs déploiements NSX-T Data Center, utilisez un répertoire différent pour chaque déploiement.

- 9 Entrez la phrase secrète utilisée pour chiffrer les données sauvegardées.
Vous aurez besoin de cette phrase secrète pour restaurer une sauvegarde. Si vous oubliez la phrase secrète de sauvegarde, vous ne pouvez restaurer aucune sauvegarde.
- 10 Entrez l'empreinte digitale SSH du serveur qui stocke les sauvegardes. Reportez-vous à la section [Rechercher l'empreinte digitale SSH d'un serveur distant](#).
- 11 Cliquez sur **Enregistrer**.
- 12 Cliquez sur **Sauvegarder maintenant** en bas de la page pour confirmer que les fichiers peuvent être écrits sur le serveur de fichiers de sauvegarde.

Étape suivante

Planifiez des sauvegardes automatisées.

Planifier des sauvegardes automatisées

Planifiez des sauvegardes fréquentes pour pouvoir restaurer une instance inopérable de NSX Manager et ses données de configuration. Les sauvegardes automatisées sont désactivées par défaut. Vous pouvez planifier des sauvegardes automatisées pour qu'elles aient lieu certains jours de la semaine ou à un intervalle spécifié. Les sauvegardes planifiées sont fortement recommandées.

Conditions préalables

- Déterminez un emplacement de sauvegarde adapté. Choisissez un emplacement qui garantisse une protection contre les points de défaillance uniques. Par exemple, ne placez pas les sauvegardes dans le même magasin de fichiers que les dispositifs. Une défaillance du magasin de fichiers pourrait affecter les dispositifs et leurs sauvegardes.
- Recherchez l'empreinte digitale SSH du serveur qui stocke les sauvegardes. Reportez-vous à la section [Rechercher l'empreinte digitale SSH d'un serveur distant](#). Les demandes de sauvegarde et de restauration d'API nécessitent que l'empreinte digitale SSH ne contienne pas de signe deux-points.

Procédure

- 1 Dans un navigateur, connectez-vous au dispositif NSX Manager en tant qu'administrateur à l'adresse `https://<adresse-ip-nsx-manager>`.

- 2 Cliquez sur **Système > Utilitaires > Sauvegarde**.
- 3 Cliquez sur **Modifier** dans le coin supérieur droit de la page.
- 4 Cliquez sur **Serveur de fichiers** et vérifiez que Sauvegarde automatique est activé.
- 5 Cliquez sur **Planifier** en haut de la page.
- 6 Pour la sauvegarde de nœud/cluster, cliquez sur **Hebdomadaire** et définissez le ou les jours et l'heure de la sauvegarde sur le serveur SFTP ou cliquez sur **Intervalle** et définissez une heure de sauvegarde.
- 7 Les sauvegardes d'inventaire sont définies pour se produire toutes les 5 minutes par défaut et doivent se produire fréquemment. Acceptez ou modifiez le paramètre par défaut si nécessaire.
- 8 Cliquez sur **Enregistrer**.

Résultats

Note La première sauvegarde hebdomadaire planifiée se produit le jour de la semaine et à l'heure spécifiés. La première sauvegarde planifiée par intervalle se produit immédiatement après l'enregistrement de la configuration de sauvegarde avec des sauvegardes automatisées activées.

NSX Manager stocke trois fichiers de sauvegarde séparés : niveau de nœud, niveau de cluster et inventaire. Les fichiers de sauvegarde sont enregistrés sur le serveur SFTP dans le répertoire spécifié dans la configuration de sauvegarde. Dans ce répertoire, les fichiers sont enregistrés dans les répertoires suivants :

- /<répertoire spécifié par l'utilisateur>/cluster-node-backups (sauvegardes de cluster et de nœud)
- /<répertoire spécifié par l'utilisateur>/inventory-summary (sauvegardes d'inventaire)

Restauration de la configuration de NSX Manager

Si le dispositif NSX Manager est inopérable, vous pouvez le restaurer à partir d'une sauvegarde. Vous aurez besoin de la phrase secrète spécifiée lorsque la sauvegarde a été créée.

Note La restauration d'une sauvegarde sur le dispositif NSX Manager sur lequel la sauvegarde a été effectuée n'est pas prise en charge.

Procédure

1 [Préparer la restauration d'une sauvegarde NSX Manager](#)

Avant de restaurer une sauvegarde de NSX Manager, vous devez installer un nouveau dispositif NSX Manager. Le nouveau dispositif NSX Manager doit être déployé avec la même adresse IP de gestion que celle du dispositif NSX Manager précédent.

2 Restaurer une sauvegarde

La restauration d'une sauvegarde entraîne la restauration de l'état du réseau au moment de la sauvegarde, la restauration des configurations conservées par l'instance de NSX Manager et l'acceptation des modifications, telles que l'ajout ou la suppression des nœuds, qui ont été apportées à l'infrastructure depuis la sauvegarde.

3 Supprimer l'extension NSX-T Data Center de vCenter Server

Lorsque vous ajoutez un gestionnaire de calcul, le dispositif NSX Manager ajoute son identité en tant qu'extension dans l'instance de vCenter Server. Si vous ne souhaitez pas enregistrer l'instance de vCenter Server dans une installation NSX-T Data Center, vous pouvez supprimer l'extension via le navigateur d'objets gérés (MOB, Managed Object Browser) de l'instance de vCenter Server.

Préparer la restauration d'une sauvegarde NSX Manager

Avant de restaurer une sauvegarde de NSX Manager, vous devez installer un nouveau dispositif NSX Manager. Le nouveau dispositif NSX Manager doit être déployé avec la même adresse IP de gestion que celle du dispositif NSX Manager précédent.

Note La restauration d'une sauvegarde sur le dispositif NSX Manager sur lequel la sauvegarde a été effectuée n'est pas prise en charge.

Conditions préalables

- Vérifiez que vous connaissez la version du dispositif NSX Manager utilisé pour créer les sauvegardes, et que vous disposez d'un fichier d'installation approprié (OVA, OVF ou QCOW2) de la même version disponible.
- Vérifiez que vous connaissez l'adresse IP qui a été attribuée au dispositif NSX Manager utilisé pour créer la sauvegarde de nœud.
- Vérifiez que personne ne tentera d'apporter des modifications de configuration au dispositif NSX Manager tant que le processus de restauration n'est pas terminé.

Procédure

- 1 Si l'ancien dispositif NSX Manager est toujours en cours d'exécution (par exemple, si vous effectuez une restauration pour revenir sur une tentative de mise à niveau), arrêtez-le.
- 2 Installez un nouveau dispositif NSX Manager.
 - La version du nouveau dispositif NSX Manager doit être la même que la version du dispositif utilisé pour créer les sauvegardes.
 - Vous devez configurer ce dispositif avec l'adresse IP qui correspond à la sauvegarde du gestionnaire.

Reportez-vous au *Guide d'installation de NSX-T Data Center* pour obtenir des informations et instructions sur cette procédure.

Étape suivante

Restaurez la sauvegarde.

Restaurer une sauvegarde

La restauration d'une sauvegarde entraîne la restauration de l'état du réseau au moment de la sauvegarde, la restauration des configurations conservées par l'instance de NSX Manager et l'acceptation des modifications, telles que l'ajout ou la suppression des nœuds, qui ont été apportées à l'infrastructure depuis la sauvegarde.

Note La restauration d'une sauvegarde sur le dispositif NSX Manager sur lequel la sauvegarde a été effectuée n'est pas prise en charge.

Conditions préalables

- Vérifiez que vous disposez de l'empreinte digitale SSH du serveur de fichiers de sauvegarde. Seule une clé ECDSA avec hachage SHA256 est acceptée comme empreinte digitale. Reportez-vous à la section [Rechercher l'empreinte digitale SSH d'un serveur distant](#).
- Vérifiez que vous disposez de la phrase secrète des fichiers de sauvegarde du nœud et du cluster.
- Vérifiez que vous disposez d'une nouvelle installation de NSX Manager qui ne contient aucun objet configuré. Reportez-vous à la section [Préparer la restauration d'une sauvegarde NSX Manager](#).

Procédure

- 1 À partir d'un navigateur, connectez-vous à NSX Manager dont vous venez de terminer l'installation.
- 2 Sélectionnez **Système > Utilitaires** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Restaurer**.
- 4 Cliquez sur **Modifier** pour configurer le serveur de fichiers de sauvegarde.
- 5 Entrez l'adresse IP ou le nom d'hôte.
- 6 Le cas échéant, modifiez le numéro du port.
La valeur par défaut est 22.
- 7 Entrez le nom d'utilisateur et le mot de passe pour vous connecter au serveur.
- 8 Dans le champ **Répertoire de destination**, entrez le chemin de répertoire absolu d'enregistrement des sauvegardes.
- 9 Entrez la phrase secrète utilisée pour chiffrer les données sauvegardées.
- 10 Entrez l'empreinte digitale SSH du serveur qui stocke les sauvegardes.
- 11 Cliquez sur **Enregistrer**.
- 12 Sélectionnez une sauvegarde.
- 13 Cliquez sur **Restaurer**.

L'état de l'opération de restauration s'affiche. Si vous avez supprimé ou ajouté des nœuds d'infrastructure ou des nœuds de transport depuis la sauvegarde, vous serez invité à effectuer certaines actions, par exemple, ouvrir une session sur un nœud et exécuter un script.

Une fois l'opération de restauration terminée, l'écran Restauration terminée s'affiche, indiquant le résultat de la restauration, l'horodatage du fichier de sauvegarde et les heures de début et de fin de l'opération de restauration. Si la restauration a échoué, l'écran affiche l'étape où l'échec s'est produit, par exemple, `Current Step: Restoring Cluster (DB)` ou `Current Step: Restoring Node`. Si une restauration de cluster ou de nœud a échoué, l'erreur peut être temporaire. Dans ce cas, il n'est pas nécessaire de cliquer sur **Réessayer**. Vous pouvez relancer ou redémarrer le gestionnaire et la restauration se poursuit.

Vous pouvez également déterminer qu'il y a un échec de la restauration de cluster ou de nœud en exécutant la commande d'interface de ligne de commande suivante pour afficher le fichier journal système et en recherchant les chaînes `Cluster restore failed` (Échec de la restauration de cluster) et `Node restore failed` (Échec de la restauration de nœud).

```
get log-file syslog
```

Pour relancer le gestionnaire, exécutez la commande d'interface de ligne de commande suivante :

```
restart service manager
```

Pour redémarrer le gestionnaire, exécutez la commande d'interface de ligne de commande suivante :

```
reboot
```

Résultats

Note Si vous avez ajouté un gestionnaire de calcul après la sauvegarde et que vous essayez d'ajouter à nouveau le gestionnaire de calcul après la restauration, vous obtenez un message erreur indiquant que l'enregistrement a échoué. Vous pouvez résoudre cette erreur et ajouter le gestionnaire de calcul. Pour plus d'informations, reportez-vous à l'étape 5 de la section [Ajouter un gestionnaire de calcul](#). Si vous souhaitez supprimer les informations sur NSX-T Data Center stockées dans une instance de vCenter Server, suivez la procédure décrite dans la section [Supprimer l'extension NSX-T Data Center de vCenter Server](#).

Supprimer l'extension NSX-T Data Center de vCenter Server

Lorsque vous ajoutez un gestionnaire de calcul, le dispositif NSX Manager ajoute son identité en tant qu'extension dans l'instance de vCenter Server. Si vous ne souhaitez pas enregistrer l'instance de vCenter Server dans une installation NSX-T Data Center, vous pouvez supprimer l'extension via le navigateur d'objets gérés (MOB, Managed Object Browser) de l'instance de vCenter Server.

Procédure

- 1 Connectez-vous à vSphere Web Client en tant qu'administrateur.
- 2 Sélectionnez l'hôte ESXi.
- 3 Cliquez sur l'onglet **Gérer > Paramètres**.
- 4 Dans le menu, sélectionnez **Paramètres système avancés**.

- 5 Activez l'option **Config.HostAgent.plugins.solo.enableMob**.
- 6 Connectez-vous au MOB.
- 7 Cliquez sur le lien de **contenu**, qui est la valeur de la propriété **contenu** dans la table Propriétés.
- 8 Cliquez sur le lien **Gestionnaire d'extensions**, qui est la valeur de la propriété **Gestionnaire d'extensions** dans la table Propriétés.
- 9 Cliquez sur le lien **Annuler l'enregistrement de l'extension** dans la table Méthodes.
- 10 Entrez **com.vmware.nsx.management.nsx** dans le champ de texte **valeur**.
- 11 Cliquez sur le lien **Appeler la méthode** sur le côté droit de la page, sous la table Paramètres.
Le résultat de méthode indique `void`, mais l'extension sera supprimée.
- 12 Pour vérifier que l'extension est supprimée, cliquez sur la méthode **Rechercher l'extension** dans la page précédente et appelez-la en saisissant la même valeur pour l'extension.
Le résultat doit être `void`.

Restaurer un cluster NSX Controller

Si un cluster NSX Controller est irrécupérable, ou si vous avez besoin de remplacer un ou plusieurs contrôleurs en raison de modifications apportées à une appartenance au cluster, vous devez restaurer tout le cluster de contrôleurs.

Avant de restaurer un cluster de contrôleurs, déterminez d'abord si l'appartenance au cluster de contrôle a été modifiée entre ce qui est connu par le plan de gestion et l'appartenance réelle connue par les contrôleurs eux-mêmes. L'appartenance peut différer si des modifications ont été effectuées après une sauvegarde.

- Si tout le cluster est irrécupérable, consultez [Redéployer le cluster NSX Controller](#).
- Suivez les étapes ci-dessous pour déterminer si l'appartenance au cluster a été modifiée et, si c'est le cas, restaurez à partir de la sauvegarde.

Conditions préalables

- Vérifiez que vous disposez d'une sauvegarde récente.
- Effectuez une restauration. Reportez-vous à la section [Restaurer une sauvegarde](#).

Procédure

- 1 Connectez-vous à l'interface de ligne de commande d'une instance de NSX Manager et exécutez la commande `get management-cluster status`.
- 2 Connectez-vous à l'interface de ligne de commande d'une instance de NSX Controller et exécutez la commande `get managers` pour vérifier que le contrôleur est enregistré avec Manager.
- 3 Exécutez la commande `get control-cluster status`.

- 4 Pour déterminer si l'appartenance a été modifiée, comparez les adresses IP du résultat de la commande `get management-cluster status` et le résultat de la commande `get control-cluster status`.

Aucune action n'est nécessaire si l'ensemble d'adresses IP est le même. Si une adresse IP est différente, effectuez les étapes restantes pour restaurer tout le cluster de contrôleur.

- 5 Connectez-vous à l'interface de ligne de commande des instances de NSX Controller pour déterminer le contrôleur maître en exécutant la commande `get control-cluster status`.
Le résultat du contrôleur maître indique `is master: true`.
- 6 Exécutez la commande `stop service <controller>` sur un contrôleur non-maître.
- 7 Connectez-vous au contrôleur maître et exécutez la commande `detach control-cluster <ip-address[:port]>` pour détacher le contrôleur non-maître de l'étape précédente.
- 8 (Facultatif) Exécutez la commande `detach controller <uuid>` sur NSX Manager pour détacher ce contrôleur uniquement si la commande `get management-cluster status` indique ce contrôleur sur NSX Manager.
- 9 Connectez-vous à l'interface de ligne de commande de l'instance de NSX Controller et exécutez la commande `deactivate control-cluster`.
- 10 Supprimez le fichier de démarrage et le fichier `uuid` avec les commandes suivantes : `rm -r /opt/vmware/etc/bootstrap-config` et `rm -r /config/vmware/node-uuid`
- 11 Effectuez les étapes 6 à 10 pour les contrôleurs non-maîtres restants.
- 12 Connectez-vous à l'interface de ligne de commande du contrôleur maître et exécutez la commande `stop service <controller>`.
- 13 Exécutez la commande `detach controller <uuid>` sur NSX Manager pour détacher ce contrôleur.
- 14 Connectez-vous à l'interface de ligne de commande du contrôleur maître et exécutez la commande `deactivate control-cluster`.
- 15 Supprimez le fichier de démarrage et le fichier `uuid` avec les commandes suivantes : `rm -r /opt/vmware/etc/bootstrap-config` et `rm -r /config/vmware/node-uuid`
- 16 Exécutez la commande `get management-cluster status` à partir de NSX Manager. S'il reste des contrôleurs indiqués dans le résultat, exécutez la commande `detach controller <uuid>` pour les détacher.

Étape suivante

Terminez les tâches suivantes dans l'ordre indiqué.

- 1 Terminez la restauration.
- 2 Joignez les NSX Controller avec le plan de gestion, comme documenté dans le *Guide d'installation de NSX-T*.
- 3 Redéployez le cluster NSX Controller, comme documenté dans le *Guide d'installation de NSX-T*.

Gestion de dispositifs et de clusters de dispositifs

Chaque installation de NSX-T Data Center requiert et prend en charge une seule instance de NSX Manager. Les clusters NSX Controller doivent disposer de trois membres. Les clusters NSX Edge doivent disposer d'au moins deux membres.

Si un dispositif dans un NSX Controller ou un cluster NSX Edge devient non opérationnel, ou si vous devez le supprimer pour une raison quelconque, vous pouvez le remplacer par un nouveau dispositif.

Important Si vous apportez des modifications à l'appartenance du cluster NSX Controller ou NSX Edge, vous devez effectuer une sauvegarde de cluster par la suite pour sauvegarder la nouvelle configuration. Reportez-vous à la section [Sauvegarde et restauration de NSX Manager](#).

Gestion de NSX Manager

Vous pouvez vérifier l'état du dispositif NSX Manager et le redémarrer s'il devient inopérable.

Obtenir l'état de NSX Manager

Vous pouvez voir l'état du dispositif NSX Manager via l'interface utilisateur de NSX Manager ou utiliser une commande d'interface de ligne de commande pour obtenir l'état.

Procédure

- 1 Dans un navigateur, connectez-vous à NSX Manager à l'adresse `http://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Système > Composants** dans le panneau de navigation.
L'état de NSX Manager s'affiche.
- 3 Vous pouvez également vous connecter à l'interface de ligne de commande de NSX Manager.
- 4 Exécutez la commande `get management-cluster status`. Par exemple,

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 10.172.121.217 (UUID 42191561-79dc-710a-74f1-d15f10cd2c40) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 10.172.121.91 (UUID ab35851f-e616-4760-8d7a-c4386c537382)
- 10.172.122.187 (UUID d159b758-c320-411f-aa67-1e2fd35f5ef2)
- 10.172.122.138 (UUID 12a3b19d-26a0-492e-836e-e9a3cc25e799)

Control cluster status: DEGRADED
```

Note Même si le résultat indique un cluster de gestion, il ne peut y avoir d'une seule instance de NSX Manager.

Redémarrer NSX Manager

Vous pouvez redémarrer le dispositif NSX Manager avec une commande d'interface de ligne de commande pour une récupération après des erreurs critiques.

Procédure

- 1 Connectez-vous à l'interface de ligne de commande de NSX Manager.
- 2 Exécutez la commande reboot. Par exemple,

```
nsx-manager> reboot
Are you sure you want to reboot (yes/no): y
```

Gérer le cluster NSX Controller

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

Un cluster NSX Controller doit disposer de la majorité pour fonctionner normalement. Si deux membres sur trois sont en ligne, le cluster a toujours la majorité. Vous devez restaurer le cluster à trois membres en activant le NSX Controller hors ligne. Si vous ne pouvez pas l'activer, vous pouvez le remplacer. Reportez-vous à la section [Remplacer un membre du cluster NSX Controller](#).

Si un seul membre sur trois est en ligne, le cluster n'a pas la majorité et il ne fonctionnera pas normalement. Si vous ne pouvez pas activer l'un des membres hors ligne, vous pouvez remplacer les instances de NSX Controller ayant échoué ou redéployer le cluster NSX Controller. Reportez-vous à la section [Redéployer le cluster NSX Controller](#).

Conditions préalables

Vérifiez au moyen d'actions de dépannage que les dispositifs ne sont pas récupérables. Par exemple, cette procédure peut permettre de récupérer les dispositifs et d'éviter leur remplacement.

- Vérifiez la connectivité réseau des dispositifs et établissez-la, le cas échéant.
- Redémarrez les dispositifs.

Étape suivante

Obtenez l'état du cluster NSX Controller. Reportez-vous à la section [Obtenir l'état du cluster NSX Controller](#).

Obtenir l'état du cluster NSX Controller

Vous pouvez rechercher l'état du cluster NSX Controller à partir de NSX Manager. Vous pouvez également vérifier l'état de chaque NSX Controller à partir de son interface de ligne de commande.

L'obtention de l'état du cluster NSX Controller et des membres du cluster vous permet de déterminer la source d'un problème avec le cluster NSX Controller.

Tableau 17-4. État du cluster NSX Controller

	Est-ce qu'au moins un contrôleur est enregistré avec NSX Manager ?	Le cluster NSX Controller a-t-il la majorité ?	Des membres du cluster NSX Controller sont-ils inactifs ?
NO_CONTROLLERS	Non	S/O	S/O
UNAVAILABLE	Inconnu	Inconnu	Inconnu
STABLE	Oui	Oui	Non
DEGRADED	Oui	Oui	Oui
UNSTABLE	Oui	Non	Non

Procédure

- 1 Connectez-vous à l'interface de ligne de commande de NSX Manager.
- 2 Exécutez la commande `get management-cluster status`.

```

nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)

Control cluster status: STABLE
    
```

- 3 Connectez-vous à l'interface de ligne de commande de NSX Controller.
- 4 Exécutez la commande `get control-cluster status`.

```

nsx-controller-1> get control-cluster status
uuid: 03fad907-612f-4068-8109-efdf73002038
is master: true
in majority: true
uuid                address                status
03fad907-612f-4068-8109-efdf73002038 192.168.110.51        active
1228c336-3932-4b5b-b87e-9f66259cebcd 192.168.110.52        active
f5348a2e-2d59-4edc-9618-2c05ac073fd8 192.168.110.53        active
    
```

Redémarrer des membres du cluster NSX Controller

Si vous avez besoin de redémarrer plusieurs membres de votre cluster NSX Controller, vous devez redémarrer un membre à la fois. Un cluster à trois membres peuvent avoir la majorité si un membre est

hors ligne. Si deux membres sont hors ligne, le cluster perdra la majorité et il ne fonctionnera pas normalement.

Procédure

- 1 Connectez-vous à l'interface de ligne de commande d'un dispositif NSX Manager.
- 2 Obtenez l'état des clusters de gestion et de contrôle.

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)

Control cluster status: STABLE
```

- 3 Connectez-vous à l'interface de ligne de commande d'un dispositif NSX Controller que vous devez redémarrer, et redémarrez-le.

```
nsx-controller-2> reboot
Are you sure you want to reboot (yes/no): y
```

- 4 Obtenez de nouveau l'état des clusters de gestion et de contrôle. Attendez que l'état du cluster de contrôle soit STABLE avant de redémarrer des membres supplémentaires.

Dans cet exemple, le dispositif NSX Controller 192.168.110.53 redémarre, et le cluster de contrôle a l'état DEGRADED. Cela signifie que le cluster est en majorité, mais que l'un des membres est inactif. Consultez [Obtenir l'état du cluster NSX Controller](#) pour plus d'informations sur l'état du cluster NSX Controller.

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)

Control cluster status: DEGRADED
```

Une fois que le cluster NSX Controller a l'état STABLE, vous pouvez redémarrer des membres supplémentaires en toute sécurité.

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)

Control cluster status: STABLE
```

- 5 Si vous avez besoin d'informations sur les états d'un dispositif NSX Controller individuel, vous pouvez vous connecter à un dispositif NSX Controller et exécuter la commande `get control-cluster status`.

```
nsx-controller-1> get control-cluster status
uuid: 03fad907-612f-4068-8109-efdf73002038
is master: true
in majority: true
  uuid                address                status
  03fad907-612f-4068-8109-efdf73002038 192.168.110.51        active
  1228c336-3932-4b5b-b87e-9f66259cebcd 192.168.110.52        active
  f5348a2e-2d59-4edc-9618-2c05ac073fd8 192.168.110.53        not active
```

- 6 Répétez les étapes pour redémarrer des dispositifs NSX Controller supplémentaires, si nécessaire.

Remplacer un membre du cluster NSX Controller

Un cluster NSX Controller doit disposer d'au moins trois membres. Si un dispositif NSX Controller devient inopérable ou si vous souhaitez le supprimer du cluster, vous devez d'abord ajouter un nouveau dispositif NSX Controller pour obtenir un cluster à quatre membres. Une fois le quatrième membre ajouté, vous pouvez supprimer un dispositif NSX Controller du cluster.

Conditions préalables

- Vérifiez au moyen d'actions de dépannage que les dispositifs ne sont pas récupérables. Par exemple, cette procédure peut permettre de récupérer les dispositifs et d'éviter leur remplacement.
 - Vérifiez la connectivité réseau des dispositifs et établissez-la, le cas échéant.
 - Redémarrez les dispositifs.
- Vérifiez que vous connaissez la version du dispositif NSX Controller que vous remplacez et que vous disposez d'un fichier d'installation approprié (OVA, OVF ou QCOW2) de la même version disponible.

Procédure

- 1 Installez et configurez un nouveau dispositif NSX Controller.

Reportez-vous au *Guide d'installation de NSX-T Data Center* pour obtenir des informations et instructions sur cette procédure.

- a Installez un nouveau dispositif NSX Controller.

La version du nouveau dispositif NSX Controller doit être la même que celle du dispositif NSX Controller qu'il remplace.

- b Reliez le nouveau dispositif NSX Controller au plan de gestion.
- c Reliez le nouveau dispositif NSX Controller au cluster de contrôle.

- 2 Arrêtez le dispositif NSX Controller que vous voulez supprimer du cluster.
- 3 Connectez-vous à un autre dispositif NSX Controller et vérifiez que le dispositif NSX Controller que vous voulez supprimer présente l'état non actif.

```
nsx-controller-1> get control-cluster status
uuid: e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b
is master: true
in majority: true
  uuid                               address                status
  ----                               -
06996547-f50c-43c0-95c1-8bb644dea498 192.168.110.53         active
471e5ac0-194b-437c-9359-564cea845333 192.168.110.54         active
e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b 192.168.110.51         active
863f9669-509f-4eba-b0ac-61a9702a242b 192.168.110.52         not active
```

- 4 Détachez le contrôleur du cluster.

```
nsx-controller-1> detach control-cluster 192.168.110.52
Successfully detached node from the control cluster.
```

- 5 Détachez le contrôleur du plan de gestion.

```
nsx-manager-1> detach controller 863f9669-509f-4eba-b0ac-61a9702a242b
The detach operation completed successfully
```

- 6 Vérifiez que les contrôleurs sont actifs et que le cluster de contrôle est stable.

À partir d'un dispositif NSX Controller :

```
nsx-controller-1> get control-cluster status
uuid: e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b
is master: true
in majority: true
  uuid                               address                status
  ----                               -
06996547-f50c-43c0-95c1-8bb644dea498 192.168.110.53         active
471e5ac0-194b-437c-9359-564cea845333 192.168.110.54         active
e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b 192.168.110.51         active
```

À partir d'un dispositif NSX Manager :

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 4213216E-F93A-71B2-DA20-AFE5E714644F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.51 (UUID e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b)
- 192.168.110.53 (UUID 06996547-f50c-43c0-95c1-8bb644dea498)
- 192.168.110.54 (UUID 471e5ac0-194b-437c-9359-564cea845333)

Control cluster status: STABLE
```

Résultats

Note Le contrôleur qui a été supprimé avec la commande `detach` conserve certaines informations de configuration. Si vous souhaitez joindre à nouveau le contrôleur à un cluster de contrôleurs, vous devez exécuter la commande CLI suivante sur le contrôleur pour supprimer les informations obsolètes :

```
deactivate control-cluster
```

Redéployer le cluster NSX Controller

Si le remplacement d'un contrôleur n'a pas résolu les problèmes de cluster NSX Controller, ou si plusieurs dispositifs NSX Controller sont irrécupérables, vous pouvez redéployer tout le cluster. Le dispositif NSX Manager contient tout l'état de configuration souhaité et il peut être utilisé pour recréer votre cluster NSX Controller.

Les connexions de chemin d'accès de données ne seront pas interrompues lors de la restauration du cluster NSX Controller.

Conditions préalables

- Vérifiez au moyen d'actions de dépannage que les dispositifs ne sont pas récupérables. Par exemple, cette procédure peut permettre de récupérer les dispositifs et d'éviter leur remplacement.
 - Vérifiez la connectivité réseau des dispositifs et établissez-la, le cas échéant.
 - Redémarrez les dispositifs.
- Vérifiez que vous connaissez la version du dispositif NSX Controller que vous remplacez et que vous disposez d'un fichier d'installation approprié (OVA, OVF ou QCOW2) de la même version disponible.
- Vérifiez que vous connaissez les adresses IP qui ont été attribuées aux dispositifs NSX Controller.

Procédure

- 1 Arrêtez tous les contrôleurs dans le cluster NSX Controller.

2 Détachez les contrôleurs du dispositif NSX Manager.

- a Connectez-vous à l'interface de ligne de commande de NSX Manager.
- b Obtenez une liste des contrôleurs avec la commande `get management-cluster status`.

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 422EC8D8-B43F-D206-5048-781A5AECDC6) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID c28d0ac7-3107-4548-817a-50d76db007ab)
- 192.168.110.51 (UUID 4a0916c7-2f4d-48c2-81b6-29b7b3758ef4)
- 192.168.110.52 (UUID 1a409f24-9b9a-431e-a03a-1929db74bf00)

Control cluster status: UNSTABLE
```

- c Détachez les contrôleurs avec la commande `detach controller`.

```
nsx-manager-1> detach controller 1a409f24-9b9a-431e-a03a-1929db74bf00
The detach operation completed successfully
nsx-manager-1> detach controller 4a0916c7-2f4d-48c2-81b6-29b7b3758ef4
The detach operation completed successfully
nsx-manager-1> detach controller c28d0ac7-3107-4548-817a-50d76db007ab
The detach operation completed successfully
```

3 Installez trois dispositifs NSX Controller et créez un cluster NSX Controller.

Reportez-vous au *Guide d'installation de NSX-T Data Center* pour obtenir des informations et instructions sur cette procédure.

- a Installez trois dispositifs NSX Controller.
 - La version des nouveaux dispositifs NSX Controller doit être la même que celle des dispositifs NSX Controller que vous remplacez.
 - Attribuez aux nouveaux contrôleurs les mêmes adresses IP que celles utilisées sur les anciens contrôleurs.
- b Reliez les dispositifs NSX Controller au plan de gestion.
- c Sur l'un des dispositifs NSX Controller, initialisez le cluster de contrôle.
- d Reliez les deux autres contrôleurs au cluster de contrôle.

Gérer le cluster NSX Edge

Vous pouvez remplacer un dispositif NSX Edge si, par exemple, il devient inopérable ou si vous devez changer de matériel. Une fois que vous avez installé un nouveau dispositif NSX Edge et créé un nœud

de transport, vous pouvez modifier le cluster NSX Edge pour remplacer l'ancien nœud de transport par le nouveau.

Note La suppression d'un cluster NSX Edge de niveau 1 entraîne la brève mise hors service de l'instance du routeur distribué (DR) de niveau 1.

Procédure

- 1 Si le dispositif NSX Edge que vous voulez remplacer fonctionne toujours, vous pouvez le mettre en mode de maintenance pour réduire le temps d'arrêt. Si la haute disponibilité est activée sur les routeurs logiques associés, le passage en mode de maintenance obligera les routeurs logiques à utiliser un membre de cluster NSX Edge différent. Vous n'avez pas à exécuter cette action si le dispositif NSX Edge est inopérable.

- a Obtenez l'ID de nœud d'infrastructure du nœud d'infrastructure échoué.

```
https://192.168.110.201/api/v1/fabric/nodes
...
  "resource_type": "EdgeNode",
  "id": "a0f4fa74-e77c-11e5-8701-005056aeed61",
  "display_name": "edgenode-02a",
  ...
```

- b Mettez le nœud NSX Edge échoué en mode de maintenance.

```
POST https://192.168.110.201/api/v1/fabric/nodes/a0f4fa74-e77c-11e5-8701-005056aeed61?
action=enter_maintenance_mode
```

- 2 Installez un nouveau dispositif NSX Edge.

Reportez-vous au *Guide d'installation de NSX-T Data Center* pour obtenir des informations et instructions sur cette procédure.

- 3 Reliez le nouveau dispositif NSX Edge au plan de gestion avec la commande `join management-plane`.

Reportez-vous au *Guide d'installation de NSX-T Data Center* pour obtenir des informations et instructions sur cette procédure.

- 4 Configurez le dispositif NSX Edge en tant que nœud de transport.

Reportez-vous au *Guide d'installation de NSX-T Data Center* pour obtenir des informations et instructions sur cette procédure.

Vous pouvez obtenir la configuration de nœud de transport du dispositif NSX Edge échoué à partir de l'API et utiliser ces informations pour créer le nœud de transport.

- a Obtenez l'ID de nœud d'infrastructure du nouveau nœud d'infrastructure.

```
https://192.168.110.201/api/v1/fabric/nodes
...
  "resource_type": "EdgeNode",
  "id": "d61c8d86-f4b8-11e5-b1b2-005056ae3c10",
  "display_name": "edgenode-03a",
...

```

- b Obtenez l'ID de nœud de transport du nœud de transport échoué.

```
GET https://192.168.110.201/api/v1/transport-nodes
...
  {
    "resource_type": "TransportNode",
    "description": "",
    "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
    "display_name": "TN-edgenode-01a",
...

```

- c Obtenez la configuration de nœud de transport du nœud de transport échoué.

```
GET https://192.168.110.201/api/v1/transport-nodes/73cb00c9-70d0-4808-abfe-a12a43251133
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
  "display_name": "TN-edgenode-01a",
  "tags": [],
  "transport_zone_endpoints": [
    ...
  ],
  "host_switches": [
    ...
  ],
  "node_id": "a0f4fa74-e77c-11e5-8701-005056aead61",
  "_create_time": 1457696199196,
  "_last_modified_user": "admin",
  "_last_modified_time": 1457696225606,
  "_create_user": "admin",
  "_revision": 2
}
```

- d Créez le nœud de transport avec POST /api/v1/transport-nodes.

Dans le corps de la demande, fournissez les informations suivantes pour le nouveau nœud de transport :

- `description` pour le nouveau nœud de transport (facultatif)
- `display_name` pour le nouveau nœud de transport
- `node_id` du nœud d'infrastructure utilisé pour créer le nœud de transport

Dans le corps de la demande, copiez les informations suivantes à partir du nœud de transport échoué :

- `transport_zone_endpoints`
- `host_switches`
- `tags` (facultatif)

```
POST https://192.168.110.201/api/v1/transport-nodes
{
  "description": "",
  "display_name": "TN-edgenode-03a",
  "tags": [
    ...
  ],
  "transport_zone_endpoints": [
    ...
  ],
  "host_switches": [
```

```
...  
],  
"node_id": "d61c8d86-f4b8-11e5-b1b2-005056ae3c10"  
}
```

5 Modifiez le cluster NSX Edge pour remplacer le nœud de transport ayant échoué par le nouveau nœud.

- a Obtenez l'ID du nouveau nœud de transport et celui du nœud de transport échoué. Le champ `id` contient l'ID du nœud de transport.

```
GET https://192.168.110.201/api/v1/transport-nodes
...
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
  "display_name": "TN-edgenode-01a",
  ...
}
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "890f0e3c-aa81-46aa-843b-8ac25fe30bd3",
  "display_name": "TN-edgenode-03a",
  ...
}
```

- b Obtenez l'ID du cluster NSX Edge. Le champ `id` contient l'ID du cluster NSX Edge. Obtenez les membres du cluster NSX Edge à partir du tableau `members`.

```
GET https://192.168.110.201/api/v1/edge-clusters
....
{
  "resource_type": "EdgeCluster",
  "description": "",
  "id": "9a302df7-0833-4237-af1f-4d826c25ad78",
  "display_name": "Edge-Cluster-1",
  ...
  "members": [
    {
      "member_index": 0,
      "transport_node_id": "73cb00c9-70d0-4808-abfe-a12a43251133"
    },
    {
      "member_index": 1,
      "transport_node_id": "e5d17b14-cdeb-4e63-b798-b23a0757463b"
    }
  ],
}
```

- c Modifiez le cluster NSX Edge pour remplacer le nœud de transport ayant échoué par le nouveau nœud. `member_index` doit correspondre à l'index du nœud de transport échoué.

Attention Si le dispositif NSX Edge fonctionne toujours, il s'agit d'une action perturbatrice. Cela déplacera tous les ports de routeur logique depuis le nœud de transport échoué vers le nouveau nœud de transport.

Dans cet exemple, le nœud de transport TN-edgenode-01a (73cb00c9-70d0-4808-abfe-a12a43251133) a échoué, et il est remplacé par le nœud de transport TN-edgenode-03a (890f0e3c-aa81-46aa-843b-8ac25fe30bd3) dans le cluster NSX Edge Edge-Cluster-1 (9a302df7-0833-4237-af1f-4d826c25ad78).

```
POST http://192.168.110.201/api/v1/edge-clusters/9a302df7-0833-4237-af1f-4d826c25ad78?
action=replace_transport_node
{
  "member_index": 0,
  "transport_node_id" : "890f0e3c-aa81-46aa-843b-8ac25fe30bd3"
}
```

6 (Facultatif) Supprimez le nœud de transport échoué et le nœud NSX Edge.

Messages de journal

Messages de journal de tous les composants de NSX-T Data Center, y compris ceux qui s'exécutent sur les hôtes ESXi, conformes au format syslog, comme spécifié dans RFC 5424. Les messages de journal des hôtes KVM sont au format RFC 3164. Les fichiers journaux se trouvent dans le répertoire /var/log.

Sur les dispositifs NSX-T Data Center, vous pouvez exécuter la commande CLI NSX-T Data Center suivante pour afficher les journaux :

```
get log-file <auth.log | http.log | kern.log | manager.log | node-mgmt.log | syslog> [follow]
```

Sur les hyperviseurs, vous pouvez utiliser des commandes Linux telles que `tail`, `grep` et `more` pour afficher les journaux. Vous pouvez également utiliser ces commandes sur des dispositifs NSX-T Data Center.

Pour plus d'informations sur la norme RFC 5424, reportez-vous à <https://tools.ietf.org/html/rfc5424>. Pour plus d'informations sur la norme RFC 3164, reportez-vous à <https://tools.ietf.org/html/rfc3164>.

La norme RFC 5424 définit le format suivant pour les messages de journal :

```
<facility * 8 + severity> version UTC-TZ hostname APP-NAME procid MSGID [structured-data] msg
```

Exemple de message de journal :

```
<187>1 2016-03-15T22:53:00.114Z nsx-manager NSX - SYSTEM [nsx@6876 comp="nsx-manager"
errorCode="MP4039" subcomp="manager"] Connection verification failed for broker '10.160.108.196'.
Marking broker unhealthy.
```

Chaque message comporte des informations sur le composant (`comp`) et le sous-composant (`subcomp`) pour faciliter l'identification de la source du message.

NSX-T Data Center produit des journaux normaux (installation `local6`, avec la valeur numérique 22) et des journaux d'audit (installation `local7`, avec la valeur numérique 23). Tous les appels API déclenchent un journal d'audit.

Un journal d'audit qui est associé à un appel d'API comporte les informations suivantes :

- Un paramètre d'identifiant d'entité `entId` pour identifier l'objet de l'API.
- Un paramètre d'identifiant de demande `req-id` pour identifier un appel d'API spécifique.
- Un paramètre d'identifiant de demande externe `ereqId` si l'appel d'API contient l'en-tête `X-NSX-EREQID:<string>`.
- Un paramètre d'utilisateur externe `euser` si l'appel d'API contient l'en-tête `X-NSX-EUSER:<string>`.

La norme RFC 5424 définit les niveaux de gravité suivants :

Niveau de gravité	Description
0	Urgence : le système est inutilisable
1	Alerte : une mesure doit être prise immédiatement
2	Critique : conditions critiques
3	Erreur : conditions d'erreur
4	Avertissement : conditions d'avertissement
5	Avis : condition normale mais significative
6	Informatif : messages informatifs
7	Débogage : messages de niveau de débogage

Tous les journaux avec la gravité urgence, alerte, critique ou erreur contiennent un code d'erreur unique dans la partie de données structurée du message de journal. Le code d'erreur se compose d'une chaîne et d'un nombre décimal. La chaîne représente un module spécifique.

Le champ `MSGID` identifie le type de message. Pour obtenir une liste des ID de messages, consultez [ID de messages de journal](#).

Configurer la journalisation à distance

Vous pouvez configurer des dispositifs NSX-T Data Center et des hyperviseurs pour envoyer des messages de journal à un serveur de journalisation distant.

La journalisation à distance est prise en charge sur NSX Manager, NSX Controller, NSX Edge et les hyperviseurs. Vous devez configurer la journalisation à distance sur chaque nœud individuellement.

Sur un hôte KVM, le module d'installation de NSX-T Data Center configure automatiquement le démon `rsyslog` en plaçant les fichiers de configuration dans le répertoire `/etc/rsyslog.d`.

Conditions préalables

- Configurez un serveur de journalisation pour recevoir les journaux.

Procédure

1 Pour configurer la journalisation à distance sur un dispositif NSX-T Data Center :

- a Exécutez la commande suivante pour configurer un serveur de journalisation et les types de messages à envoyer au serveur de journalisation. Plusieurs installations ou ID de message peuvent être spécifiés sous forme d'une liste séparée par des virgules, sans espace.

```
set logging-server <hostname-or-ip-address[:port]> proto <proto> level <level> [facility <facility>] [messageid <messageid>] [certificate <filename>] [structured-data <structured-data>]
```

Pour plus d'informations sur cette commande, reportez-vous à la *Référence CLI de NSX-T*. Vous pouvez exécuter la commande plusieurs fois pour ajouter plusieurs configurations de serveur de journalisation. Par exemple :

```
nsx> set logging-server 192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
nsx> set logging-server 192.168.110.60 proto udp level info facility auth,user
```

- b vous pouvez afficher la configuration de la journalisation à l'aide de la commande `get logging-server`. Par exemple,

```
nsx> get logging-servers
192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
192.168.110.60 proto udp level info facility auth,user
```

2 Pour configurer la journalisation à distance sur un hôte ESXi :

- a Exécutez les commandes suivantes pour configurer syslog et envoyer un message de test :

```
esxcli network firewall ruleset set -r syslog -e true
esxcli system syslog config set --loghost=udp://<log server IP>:<port>
esxcli system syslog reload
esxcli system syslog mark -s "This is a test message"
```

- b Vous pouvez exécuter la commande suivante pour afficher la configuration :

```
esxcli system syslog config get
```

3 Pour configurer la journalisation à distance sur un hôte KVM :

- a Modifiez le fichier `/etc/rsyslog.d/10-vmware-remote-logging.conf` pour votre environnement.

- b Ajoutez la ligne suivante au fichier :

```
*.* @<ip>:514;RFC5424fmt
```

- c Exécutez la commande suivante :

```
service rsyslog restart
```

ID de messages de journal

Dans un message de journal, le champ ID de message identifie le type de message. Vous pouvez utiliser le paramètre `messageid` dans la commande `set logging-server` pour filtrer les messages de journal envoyés à un serveur de journalisation.

Tableau 17-5. ID de messages de journal

ID de message	Exemples
FABRIC	Nœud hôte Préparation de l'hôte Nœud Edge Zone de transport Nœud de transport Profils de liaison montante Profils de cluster Cluster Edge Clusters et points de terminaison de pont
SWITCHING	Commutateur logique Ports de commutateur logique Profils de commutation Fonctionnalités de sécurité de commutateur
ROUTING	Routeur logique Ports de routeur logique Routage statique Routage dynamique NAT
FIREWALL	Règles de pare-feu Sections de règles de pare-feu
FIREWALL-PKTLOG	Journaux de connexion de pare-feu Journaux de paquet de pare-feu
GROUPING	Ensembles d'adresses IP Ensembles MAC NSGroups NSServices Groupes NSService Pool VNI Pool IP
DHCP	relais DHCP

Tableau 17-5. ID de messages de journal (suite)

ID de message	Exemples
SYSTEM	Gestion des dispositifs (Syslog distant, NTP, etc.) Gestion des clusters Gestion de l'approbation Attribution de licences Utilisateur et rôles Gestion des tâches Installation (NSX Manager, NSX Controller) Mise à niveau (NSX Manager, NSX Controller, NSX Edge et mises à niveau des packages d'hôte) Réalisation Balises
MONITORING	SNMP Connexion au port Traceflow
-	Tous les autres messages de journal.

Configurer IPFIX

IPFIX (Internet Protocol Flow Information Export) est une norme pour le format et l'exportation d'informations de flux de réseau. Vous pouvez configurer IPFIX pour des commutateurs et des pare-feu. Pour les commutateurs, le flux de réseau au niveau des VIF (interfaces virtuelles) et des pNIC (cartes réseau physiques) est exporté. Pour les pare-feu, le flux de réseau qui est géré par le composant de pare-feu distribué est exporté.

Remarques concernant NSX Cloud Si vous utilisez NSX Cloud, reportez-vous à la section [Comment utiliser des fonctionnalités NSX-T Data Center avec le cloud public](#) pour obtenir la liste des entités logiques générées automatiquement, les fonctionnalités prises en charge et les configurations requises pour NSX Cloud.

Lorsque IPFIX est activé, tous les nœuds de transport d'hôtes configurés envoient des messages IPFIX aux collecteurs IPFIX via le port 4739. Dans le cas d'ESXi, NSX-T Data Center ouvre automatiquement le port 4739. Dans le cas de KVM, si le pare-feu n'est pas activé, le port 4739 est ouvert, mais si le pare-feu est activé, vous devez vérifier que le port est bien ouvert, car ce dernier n'est pas automatiquement ouvert par NSX-T Data Center.

IPFIX sur ESXi et KVM échantillonnent des paquets de différentes manières. Sur ESXi, le paquet de tunnel est échantillonné sous la forme de deux enregistrements :

- Enregistrement de paquet externe avec certaines informations de paquet interne
 - SrcAddr, DstAddr, SrcPort, DstPort et Protocole font référence au paquet externe.
 - Contient certaines entrées d'entreprise pour décrire le paquet interne.

- Enregistrement de paquet interne
 - SrcAddr, DstAddr, SrcPort, DstPort et Protocole font référence au paquet interne.

Sur KVM, le paquet de tunnel est échantillonné sous la forme d'un enregistrement :

- Enregistrement de paquet interne avec certaines informations du tunnel externe
 - SrcAddr, DstAddr, SrcPort, DstPort et Protocole font référence au paquet interne.
 - Contient certaines entrées d'entreprise pour décrire le paquet externe.

Conditions préalables

- Installez au moins un collecteur IPFIX
- Vérifiez que les connecteurs IPFIX peuvent se connecter aux hyperviseurs via le réseau.
- Vérifiez que les pare-feu, notamment le pare-feu ESXi, autorisent le trafic sur les ports du collecteur IPFIX.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur *https://<adresse-ip-nsx-manager>*.
- 2 Sélectionnez **Outils > IPFIX** dans le panneau de navigation.
- 3 Pour configurer IPFIX de commutateur, cliquez sur l'onglet **Collecteurs IPFIX de commutateur**.
- 4 Cliquez sur **Ajouter**.
- 5 Entrez un nom et éventuellement une description.
- 6 Cliquez sur **Ajouter** et entrez l'adresse IP et le port d'un collecteur.
Vous pouvez ajouter jusqu'à 4 collecteurs.
- 7 Cliquez sur **Enregistrer**.

Configurer des profils IPFIX de commutateur

Vous pouvez configurer des profils IPFIX pour des commutateurs.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur *https://<adresse-ip-nsx-manager>*.
- 2 Sélectionnez **Outils > IPFIX** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Profils IPFIX de commutateur**.

4 Cliquez sur **Ajouter** pour ajouter un profil.

Paramètre	Description
Nom et description	Entrez un nom et éventuellement une description.
Délai d'expiration d'activité (en secondes)	Laps de temps après lequel un flux arrive à expiration, même si d'autres paquets associés au flux sont reçus. La valeur par défaut est 300.
Délai d'expiration d'inactivité (en secondes)	Laps de temps après lequel un flux arrive à expiration, lorsqu'aucun paquet associé au flux n'est reçu (uniquement pour ESXi ; sur KVM, l'expiration de tous les flux est basé sur un délai d'expiration actif). La valeur par défaut est 300.
Flux max.	Nombre maximal de flux mis en mémoire cache sur un pont (pour KVM uniquement, non configurable sur ESXi). La valeur par défaut est 16384.
Probabilité d'échantillonnage (%)	Pourcentage de paquets qui seront échantillonnés (approximativement). L'augmentation de la valeur de ce paramètre peut avoir un impact sur les performances des hyperviseurs et des collecteurs. Si tous les hyperviseurs envoient davantage de paquets au collecteur, ce dernier peut ne pas être en mesure de collecter tous les paquets. En définissant la probabilité sur la valeur par défaut de 0,1 %, l'impact sur les performances restera faible.
ID domaine d'observation	L'ID du domaine d'observation identifie le domaine d'observation d'où proviennent les flux de réseau. Entrez 0 pour n'indiquer aucun domaine d'observation spécifique.
Profil du collecteur	Sélectionnez le collecteur IPFIX de commutateur que vous avez configuré à l'étape précédente.
Priorité	Ce paramètre résout les conflits lorsque plusieurs profils s'appliquent. L'exportateur IPFIX n'utilisera le profil qu'avec la priorité la plus élevée. Une valeur inférieure signifie une priorité plus élevée.

5 Cliquez sur **Appliqué à** pour appliquer le profil à un ou plusieurs objets.

Les types d'objet sont des ports logiques, des commutateurs logiques et des NSGroups. Si vous sélectionnez un NSGroup, il doit contenir un ou plusieurs commutateurs logiques ou ports logiques. Si le NSGroup contient uniquement les ensembles d'adresses IP ou les ensembles d'adresses MAC, il sera ignoré.

6 Cliquez sur **Enregistrer**.

Configurer des collecteurs IPFIX de pare-feu

Vous pouvez configurer des collecteurs IPFIX pour des pare-feu.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Outils > IPFIX** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Collecteurs IPFIX de pare-feu**.
- 4 Entrez un nom et éventuellement une description.
- 5 Cliquez sur **Ajouter** et entrez l'adresse IP et le port d'un collecteur.

Vous pouvez ajouter jusqu'à 4 collecteurs.

6 Cliquez sur **Enregistrer**.

Configurer des profils IPFIX de pare-feu

Vous pouvez configurer des profils IPFIX pour des pare-feu.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur *https://<adresse-ip-nsx-manager>*.
- 2 Sélectionnez **Outils > IPFIX** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Profils IPFIX de pare-feu**.
- 4 Cliquez sur **Ajouter** pour ajouter un profil.

Paramètre	Description
Nom et description	Entrez un nom et éventuellement une description.
Configuration du collecteur	Sélectionnez un collecteur dans la liste déroulante.
Délai d'expiration de l'exportation du flux actif (minutes)	Laps de temps après lequel un flux arrive à expiration, même si d'autres paquets associés au flux sont reçus. La valeur par défaut est 1.
Priorité	Ce paramètre résout les conflits lorsque plusieurs profils s'appliquent. L'exportateur IPFIX n'utilisera le profil qu'avec la priorité la plus élevée. Une valeur inférieure signifie une priorité plus élevée.
ID domaine d'observation	Ce paramètre identifie le domaine d'observation d'où proviennent les flux de réseau. La valeur par défaut est 0. Elle n'indique aucun domaine d'observation spécifique.

- 5 Cliquez sur **Appliqué à** pour appliquer le profil à un ou plusieurs objets.

Les types d'objet sont des ports logiques, des commutateurs logiques et des NSGroups. Si vous sélectionnez un NSGroup, il doit contenir un ou plusieurs commutateurs logiques ou ports logiques. Si le NSGroup contient uniquement les ensembles d'adresses IP ou les ensembles d'adresses MAC, il sera ignoré.

- 6 Cliquez sur **Enregistrer**.

Modèles IPFIX ESXi

Un nœud de transport hôte ESXi prend en charge huit modèles de flux IPFIX.

Modèle IPv4

ID de modèle : 256

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
```

```

IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
// Specify the Interface port- Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()

```

Modèle IPv4 encapsulé

ID de modèle : 257

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourcePort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port - Uplink Port, Access port, N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-Gw or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_END()

```

Modèle IPv4 ICMP

ID de modèle : 258

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ICMP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
// Specify the Interface port - Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 2)
IPFIX_TEMPLATE_END()

```

Modèle IPv4 ICMP encapsulé

ID de modèle : 259

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ICMP_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port- Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.

```

```
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

Modèle IPv6

ID de modèle : 260

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
// Specify the Interface port - Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

Modèle IPv6 encapsulé

ID de modèle : 261

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
```

```

IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
//ENCAP specific
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourcePort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port - Uplink Port, Access Port, or NA
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_END()

```

Modèle IPv6 ICMP

ID de modèle : 262

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ICMP)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(encapId, 8)
// Specify the Interface port - Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 2)
IPFIX_TEMPLATE_END()

```

Modèle IPv6 ICMP encapsulé

ID de modèle : 263

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ICMP_ENCAP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)

```

```

IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_VMW_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
//ENCAP Specific
IPFIX_TEMPLATE_FIELD(encapId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port – Uplink Port, Access Port, or NA
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(encapExportRole, 1)
IPFIX_VMW_TEMPLATE_VAR_LEN_FIELD(virtualObsID, virtualObsDataLen)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()

```

Modèles IPFIX KVM

Un nœud de transport hôte KVM prend en charge 88 modèles de flux IPFIX et un modèle d'options.

Modèles IPFIX KVM Ethernet

Il existe quatre modèles IPFIX KVM Ethernet : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée Ethernet

ID de modèle : 256. Nombre de champs : 27.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)

- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)

Sortie Ethernet

ID de modèle : 257. Nombre de champs : 31.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)

- Unknown(369) (longueur : 8)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)

Entrée Ethernet avec tunnel

ID de modèle : 258. Nombre de champs : 34.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)

- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)

Sortie Ethernet avec tunnel

ID de modèle : 259. Nombre de champs : 38.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)

- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 8)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)

- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)

Modèles IPFIX KVM IPv4

Il existe quatre modèles IPFIX KVM IPv4 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée IPv4

ID de modèle : 276. Nombre de champs : 45.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)

- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie IPv4

ID de modèle : 277. Nombre de champs : 49.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)

- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)

- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Entrée IPv4 avec tunnel

ID de modèle : 278. Nombre de champs : 52.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)

- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)

- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie IPv4 avec tunnel

ID de modèle : 279. Nombre de champs : 56.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))

- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Modèles IPFIX KVM TCP sur IPv4

Il existe quatre modèles IPFIX KVM TCP sur IPv4 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée TCP sur IPv4

ID de modèle : 280. Nombre de champs : 53.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)

- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)
- tcpAckTotalCount (longueur : 8)
- tcpFinTotalCount (longueur : 8)
- tcpPshTotalCount (longueur : 8)
- tcpRstTotalCount (longueur : 8)
- tcpSynTotalCount (longueur : 8)
- tcpUrgTotalCount (longueur : 8)

Sortie TCP sur IPv4

ID de modèle : 281. Nombre de champs : 57.

Les champs sont :

- observationPointId (longueur : 4)

- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)

- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)
- tcpAckTotalCount (longueur : 8)
- tcpFinTotalCount (longueur : 8)
- tcpPshTotalCount (longueur : 8)
- tcpRstTotalCount (longueur : 8)
- tcpSynTotalCount (longueur : 8)
- tcpUrgTotalCount (longueur : 8)

Entrée TCP sur IPv4 avec tunnel

ID de modèle : 282. Nombre de champs : 60.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)

- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)

- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)
- tcpAckTotalCount (longueur : 8)
- tcpFinTotalCount (longueur : 8)
- tcpPshTotalCount (longueur : 8)
- tcpRstTotalCount (longueur : 8)
- tcpSynTotalCount (longueur : 8)
- tcpUrgTotalCount (longueur : 8)

Sortie TCP sur IPv4 avec tunnel

ID de modèle : 283. Nombre de champs : 64.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)

- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)

- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)
- tcpAckTotalCount (longueur : 8)
- tcpFinTotalCount (longueur : 8)
- tcpPshTotalCount (longueur : 8)
- tcpRstTotalCount (longueur : 8)
- tcpSynTotalCount (longueur : 8)
- tcpUrgTotalCount (longueur : 8)

Modèles IPFIX KVM UDP sur IPv4

Il existe quatre modèles IPFIX KVM UDP sur IPv4 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée UDP sur IPv4

ID de modèle : 284. Nombre de champs : 47.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)

- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie UDP sur IPv4

ID de modèle : 285. Nombre de champs : 51.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)

- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)

- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Entrée UDP sur IPv4 avec tunnel

ID de modèle : 286. Nombre de champs : 54.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)

- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)

- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie UDP sur IPv4 avec tunnel

ID de modèle : 287. Nombre de champs : 58.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))

- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)

- postMCastOctetTotalCount (longueur : 8)

Modèles IPFIX KVM SCTP sur IPv4

Il existe quatre modèles IPFIX KVM SCTP sur IPv4 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée SCTP sur IPv4

ID de modèle : 288. Nombre de champs : 47.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)

- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie SCTP sur IPv4

ID de modèle : 289. Nombre de champs : 51.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)

- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)

- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Entrée SCTP sur IPv4 avec tunnel

ID de modèle : 290. Nombre de champs : 54.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)

- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)

- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie SCTP sur IPv4 avec tunnel

ID de modèle : 291. Nombre de champs : 58.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)

- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)

- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Modèles IPFIX KVM ICMPv4

Il existe quatre modèles IPFIX KVM ICMPv4 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée ICMPv4

ID de modèle : 292. Nombre de champs : 47.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- ICMP_IPv4_TYPE (longueur : 1)
- ICMP_IPv4_CODE (longueur : 1)

- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie ICMPv4

ID de modèle : 293. Nombre de champs : 51.

Les champs sont :

- observationPointId (longueur : 4)

- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- ICMP_IPv4_TYPE (longueur : 1)
- ICMP_IPv4_CODE (longueur : 1)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)

- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Entrée ICMPv4 avec tunnel

ID de modèle : 294. Nombre de champs : 54.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)

- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- ICMP_IPv4_TYPE (longueur : 1)
- ICMP_IPv4_CODE (longueur : 1)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)

- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie ICMPv4 avec tunnel

ID de modèle : 295. Nombre de champs : 58.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)

- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- ICMP_IPv4_TYPE (longueur : 1)
- ICMP_IPv4_CODE (longueur : 1)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)

- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Modèles IPFIX KVM IPv6

Il existe quatre modèles IPFIX KVM IPv6 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée IPv6

ID de modèle : 296. Nombre de champs : 46.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)

- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie IPv6

ID de modèle : 297. Nombre de champs : 50.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)

- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Entrée IPv6 avec tunnel

ID de modèle : 298. Nombre de champs : 53.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)

- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)

- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie IPv6 avec tunnel

ID de modèle : 299. Nombre de champs : 57.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)

- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)

- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Modèles IPFIX KVM TCP sur IPv6

Il existe quatre modèles IPFIX KVM TCP sur IPv6 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée TCP sur IPv6

ID de modèle : 300. Nombre de champs : 54.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)

- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)

- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)
- tcpAckTotalCount (longueur : 8)
- tcpFinTotalCount (longueur : 8)
- tcpPshTotalCount (longueur : 8)
- tcpRstTotalCount (longueur : 8)
- tcpSynTotalCount (longueur : 8)
- tcpUrgTotalCount (longueur : 8)

Sortie TCP sur IPv6

ID de modèle : 301. Nombre de champs : 58.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)

- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

- tcpAckTotalCount (longueur : 8)
- tcpFinTotalCount (longueur : 8)
- tcpPshTotalCount (longueur : 8)
- tcpRstTotalCount (longueur : 8)
- tcpSynTotalCount (longueur : 8)
- tcpUrgTotalCount (longueur : 8)

Entrée TCP sur IPv6 avec tunnel

ID de modèle : 302. Nombre de champs : 61.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))

- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)

- postMCastOctetTotalCount (longueur : 8)
- tcpAckTotalCount (longueur : 8)
- tcpFinTotalCount (longueur : 8)
- tcpPshTotalCount (longueur : 8)
- tcpRstTotalCount (longueur : 8)
- tcpSynTotalCount (longueur : 8)
- tcpUrgTotalCount (longueur : 8)

Sortie TCP sur IPv6 avec tunnel

ID de modèle : 303. Nombre de champs : 65.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)

- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)

- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)
- tcpAckTotalCount (longueur : 8)
- tcpFinTotalCount (longueur : 8)
- tcpPshTotalCount (longueur : 8)
- tcpRstTotalCount (longueur : 8)
- tcpSynTotalCount (longueur : 8)
- tcpUrgTotalCount (longueur : 8)

Modèles IPFIX KVM UDP sur IPv6

Il existe quatre modèles IPFIX KVM UDP sur IPv6 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée UDP sur IPv6

ID de modèle : 304. Nombre de champs : 48.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)

- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)

- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie UDP sur IPv6

ID de modèle : 305. Nombre de champs : 52.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)

- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Entrée UDP sur IPv6 avec tunnel

ID de modèle : 306. Nombre de champs : 55.

Les champs sont :

- observationPointId (longueur : 4)

- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)

- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie UDP sur IPv6 avec tunnel

ID de modèle : 307. Nombre de champs : 59.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)

- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)

- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Modèles IPFIX KVM SCTP sur IPv6

Il existe quatre modèles IPFIX KVM SCTP sur IPv6 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée SCTP sur IPv6

ID de modèle : 308. Nombre de champs : 48.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)

- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)

- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie SCTP sur IPv6

ID de modèle : 309. Nombre de champs : 52.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)

- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)

- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Entrée SCTP sur IPv6 avec tunnel

ID de modèle : 310. Nombre de champs : 55.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))

- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie SCTP sur IPv6 avec tunnel

ID de modèle : 311. Nombre de champs : 59.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))

- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Modèles IPFIX KVM ICMPv6

Il existe quatre modèles IPFIX KVM ICMPv6 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée ICMPv6

ID de modèle : 312. Nombre de champs : 48.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- ICMP_IPv6_TYPE (longueur : 1)
- ICMP_IPv6_CODE (longueur : 1)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)

- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie ICMPv6

ID de modèle : 313. Nombre de champs : 52.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)

- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- ICMP_IPv6_TYPE (longueur : 1)
- ICMP_IPv6_CODE (longueur : 1)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)

- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Entrée ICMPv6 avec tunnel

ID de modèle : 314. Nombre de champs : 55.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)

- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- ICMP_IPv6_TYPE (longueur : 1)
- ICMP_IPv6_CODE (longueur : 1)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)

- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie ICMPv6 avec tunnel

ID de modèle : 315. Nombre de champs : 59.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)

- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- ICMP_IPv6_TYPE (longueur : 1)
- ICMP_IPv6_CODE (longueur : 1)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)

- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Modèles IPFIX VLAN KVM Ethernet

Il existe quatre modèles IPFIX VLAN KVM Ethernet : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée Ethernet VLAN

ID de modèle : 316. Nombre de champs : 30.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)

- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)

Sortie Ethernet VLAN

ID de modèle : 317. Nombre de champs : 34.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 8)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)

- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)

Entrée Ethernet VLAN avec tunnel

ID de modèle : 318. Nombre de champs : 37.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)

- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)

Sortie Ethernet VLAN avec tunnel

ID de modèle : 319. Nombre de champs : 41.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 8)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)

- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)

Modèles IPFIX VLAN KVM IPv4

Il existe quatre modèles IPFIX VLAN KVM IPv4 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée IPv4 VLAN

ID de modèle : 336. Nombre de champs : 48.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)

- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie IPv4 VLAN

ID de modèle : 337. Nombre de champs : 52.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)

- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Entrée IPv4 VLAN avec tunnel

ID de modèle : 338. Nombre de champs : 55.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)

- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)

- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie IPv4 VLAN avec tunnel

ID de modèle : 339. Nombre de champs : 59.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)

- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)

- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Modèles IPFIX VLAN KVM TCP sur IPv4

Il existe quatre modèles IPFIX VLAN KVM TCP sur IPv4 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée TCP sur IPv4 VLAN

ID de modèle : 340. Nombre de champs : 56.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)

- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)

- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)
- tcpAckTotalCount (longueur : 8)
- tcpFinTotalCount (longueur : 8)
- tcpPshTotalCount (longueur : 8)
- tcpRstTotalCount (longueur : 8)
- tcpSynTotalCount (longueur : 8)
- tcpUrgTotalCount (longueur : 8)

Sortie TCP sur IPv4 VLAN

ID de modèle : 341. Nombre de champs : 60.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)

- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)

- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)
- tcpAckTotalCount (longueur : 8)
- tcpFinTotalCount (longueur : 8)
- tcpPshTotalCount (longueur : 8)
- tcpRstTotalCount (longueur : 8)
- tcpSynTotalCount (longueur : 8)
- tcpUrgTotalCount (longueur : 8)

Entrée TCP sur IPv4 VLAN avec tunnel

ID de modèle : 342. Nombre de champs : 63.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)

- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)

- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)
- tcpAckTotalCount (longueur : 8)
- tcpFinTotalCount (longueur : 8)
- tcpPshTotalCount (longueur : 8)
- tcpRstTotalCount (longueur : 8)
- tcpSynTotalCount (longueur : 8)
- tcpUrgTotalCount (longueur : 8)

Sortie TCP sur IPv4 VLAN avec tunnel

ID de modèle : 343. Nombre de champs : 67.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)

- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)

- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)
- tcpAckTotalCount (longueur : 8)
- tcpFinTotalCount (longueur : 8)
- tcpPshTotalCount (longueur : 8)
- tcpRstTotalCount (longueur : 8)
- tcpSynTotalCount (longueur : 8)
- tcpUrgTotalCount (longueur : 8)

Modèles IPFIX VLAN KVM UDP sur IPv4

Il existe quatre modèles IPFIX VLAN KVM UDP sur IPv4 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée UDP sur IPv4 VLAN

ID de modèle : 344. Nombre de champs : 50.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)

- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie UDP sur IPv4 VLAN

ID de modèle : 345. Nombre de champs : 54.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)

- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)

- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Entrée UDP sur IPv4 VLAN avec tunnel

ID de modèle : 346. Nombre de champs : 57.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)

- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)

- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie UDP sur IPv4 VLAN avec tunnel

ID de modèle : 347. Nombre de champs : 61.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)

- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)

- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

modèles IPFIX VLAN KVM SCTP sur IPv4

Il existe quatre modèles IPFIX VLAN KVM SCTP sur IPv4 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée SCTP sur IPv4 VLAN

ID de modèle : 348. Nombre de champs : 50.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)

- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)

- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie SCTP sur IPv4 VLAN

ID de modèle : 349. Nombre de champs : 54.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)

- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Entrée SCTP sur IPv4 VLAN avec tunnel

ID de modèle : 350. Nombre de champs : 57.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))

- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie SCTP sur IPv4 VLAN avec tunnel

ID de modèle : 351. Nombre de champs : 61.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))

- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Modèles IPFIX VLAN KVM ICMPv4

Il existe quatre modèles IPFIX VLAN KVM ICMPv4 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée ICMPv4 VLAN

ID de modèle : 352. Nombre de champs : 50.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- ICMP_IPv4_TYPE (longueur : 1)
- ICMP_IPv4_CODE (longueur : 1)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)

- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie ICMPv4 VLAN

ID de modèle : 353. Nombre de champs : 54.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)

- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- ICMP_IPv4_TYPE (longueur : 1)
- ICMP_IPv4_CODE (longueur : 1)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)

- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Entrée ICMPv4 VLAN avec tunnel

ID de modèle : 354. Nombre de champs : 57.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)

- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- ICMP_IPv4_TYPE (longueur : 1)
- ICMP_IPv4_CODE (longueur : 1)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)

- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie ICMPv4 VLAN avec tunnel

ID de modèle : 355. Nombre de champs : 61.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)

- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IP_SRC_ADDR (longueur : 4)
- IP_DST_ADDR (longueur : 4)
- ICMP_IPv4_TYPE (longueur : 1)
- ICMP_IPv4_CODE (longueur : 1)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)

- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Modèles IPFIX VLAN KVM IPv6

Il existe quatre modèles IPFIX VLAN KVM IPv6 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée IPv6 VLAN

ID de modèle : 356. Nombre de champs : 49.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)

- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)

- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie IPv6 VLAN

ID de modèle : 357. Nombre de champs : 53.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)

- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Entrée IPv6 VLAN avec tunnel

ID de modèle : 358. Nombre de champs : 56.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))

- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie IPv6 VLAN avec tunnel

ID de modèle : 359. Nombre de champs : 60.

Les champs sont :

- observationPointId (longueur : 4)

- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))

- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

modèles IPFIX VLAN KVM TCP sur IPv6

Il existe quatre modèles IPFIX VLAN KVM TCP sur IPv6 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée TCP sur IPv6 VLAN

ID de modèle : 360. Nombre de champs : 57.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)

- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)
- tcpAckTotalCount (longueur : 8)
- tcpFinTotalCount (longueur : 8)
- tcpPshTotalCount (longueur : 8)
- tcpRstTotalCount (longueur : 8)
- tcpSynTotalCount (longueur : 8)
- tcpUrgTotalCount (longueur : 8)

Sortie TCP sur IPv6 VLAN

ID de modèle : 361. Nombre de champs : 61.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)

- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)
- tcpAckTotalCount (longueur : 8)
- tcpFinTotalCount (longueur : 8)
- tcpPshTotalCount (longueur : 8)
- tcpRstTotalCount (longueur : 8)
- tcpSynTotalCount (longueur : 8)
- tcpUrgTotalCount (longueur : 8)

Entrée TCP sur IPv6 VLAN avec tunnel

ID de modèle : 362. Nombre de champs : 64.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))

- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)
- tcpAckTotalCount (longueur : 8)
- tcpFinTotalCount (longueur : 8)
- tcpPshTotalCount (longueur : 8)

- tcpRstTotalCount (longueur : 8)
- tcpSynTotalCount (longueur : 8)
- tcpUrgTotalCount (longueur : 8)

Sortie TCP sur IPv6 VLAN avec tunnel

ID de modèle : 363. Nombre de champs : 68.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)

- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)

- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)
- tcpAckTotalCount (longueur : 8)
- tcpFinTotalCount (longueur : 8)
- tcpPshTotalCount (longueur : 8)
- tcpRstTotalCount (longueur : 8)
- tcpSynTotalCount (longueur : 8)
- tcpUrgTotalCount (longueur : 8)

modèles IPFIX VLAN KVM UDP sur IPv6

Il existe quatre modèles IPFIX VLAN KVM UDP sur IPv6 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée UDP sur IPv6 VLAN

ID de modèle : 364. Nombre de champs : 51.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)

- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)

- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie UDP sur IPv6 VLAN

ID de modèle : 365. Nombre de champs : 55.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)

- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Entrée UDP sur IPv6 VLAN avec tunnel

ID de modèle : 366. Nombre de champs : 58.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))

- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie UDP sur IPv6 VLAN avec tunnel

ID de modèle : 367. Nombre de champs : 62.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))

- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Modèles IPFIX VLAN KVM SCTP sur IPv6

Il existe quatre modèles IPFIX VLAN KVM SCTP sur IPv6 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée SCTP sur IPv6 VLAN

ID de modèle : 368. Nombre de champs : 51.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)

- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie SCTP sur IPv6 VLAN

ID de modèle : 369. Nombre de champs : 55.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)

- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)

- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Entrée SCTP sur IPv6 VLAN avec tunnel

ID de modèle : 370. Nombre de champs : 58.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)

- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)

- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie SCTP sur IPv6 VLAN avec tunnel

ID de modèle : 371. Nombre de champs : 62.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)

- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- L4_SRC_PORT (longueur : 2)
- L4_DST_PORT (longueur : 2)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)

- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Modèles IPFIX VLAN KVM ICMPv6

Il existe quatre modèles IPFIX KVM ICMPv6 : entrée, sortie, entrée avec tunnel et sortie avec tunnel.

Entrée ICMPv6

ID de modèle : 372. Nombre de champs : 51.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)

- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- ICMP_IPv6_TYPE (longueur : 1)
- ICMP_IPv6_CODE (longueur : 1)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)

- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie ICMPv6

ID de modèle : 373. Nombre de champs : 55.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)

- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- ICMP_IPv6_TYPE (longueur : 1)
- ICMP_IPv6_CODE (longueur : 1)
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)

- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Entrée ICMPv6 avec tunnel

ID de modèle : 374. Nombre de champs : 58.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)
- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)

- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- ICMP_IPv6_TYPE (longueur : 1)
- ICMP_IPv6_CODE (longueur : 1)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)
- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)

- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP_LENGTH_MINIMUM (longueur : 8)
- IP_LENGTH_MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Sortie ICMPv6 avec tunnel

ID de modèle : 375. Nombre de champs : 62.

Les champs sont :

- observationPointId (longueur : 4)
- DIRECTION (longueur : 1)
- SRC_MAC (longueur : 6)
- DESTINATION_MAC (longueur : 6)
- ethernetType (longueur : 2)
- ethernetHeaderLength (longueur : 1)
- INPUT_SNMP (longueur : 4)
- Unknown(368) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- OUTPUT_SNMP (longueur : 4)
- Unknown(369) (longueur : 4)
- IF_NAME (longueur : variable)
- IF_DESC (longueur : variable)
- SRC_VLAN (longueur : 2)
- dot1qVlanId (longueur : 2)
- dot1qPriority (longueur : 1)
- IP_PROTOCOL_VERSION (longueur : 1)
- IP_TTL (longueur : 1)
- PROTOCOL (longueur : 1)
- IP_DSCP (longueur : 1)
- IP_PRECEDENCE (longueur : 1)

- IP_TOS (longueur : 1)
- IPV6_SRC_ADDR (longueur : 4)
- IPV6_DST_ADDR (longueur : 4)
- FLOW_LABEL (longueur : 4)
- ICMP_IPv6_TYPE (longueur : 1)
- ICMP_IPv6_CODE (longueur : 1)
- 893 (longueur : 4, PEN : VMware Inc. (6876))
- 894 (longueur : 4, PEN : VMware Inc. (6876))
- 895 (longueur : 1, PEN : VMware Inc. (6876))
- 896 (longueur : 2, PEN : VMware Inc. (6876))
- 897 (longueur : 2, PEN : VMware Inc. (6876))
- 891 (longueur : 1, PEN : VMware Inc. (6876))
- 892 (longueur : variable, PEN : VMware Inc. (6876))
- 898 (longueur : variable, PEN : VMware Inc. (6876))
- flowStartDeltaMicroseconds (longueur : 4)
- flowEndDeltaMicroseconds (longueur : 4)
- DROPPED_PACKETS (longueur : 8)
- DROPPED_PACKETS_TOTAL (longueur : 8)
- PKTS (longueur : 8)
- PACKETS_TOTAL (longueur : 8)
- Unknown(354) (longueur : 8)
- Unknown(355) (longueur : 8)
- Unknown(356) (longueur : 8)
- Unknown(357) (longueur : 8)
- Unknown(358) (longueur : 8)
- MUL_DPKTS (longueur : 8)
- postMCastPacketTotalCount (longueur : 8)
- Unknown(352) (longueur : 8)
- Unknown(353) (longueur : 8)
- flowEndReason (longueur : 1)
- DROPPED_BYTES (longueur : 8)
- DROPPED_BYTES_TOTAL (longueur : 8)

- BYTES (longueur : 8)
- BYTES_TOTAL (longueur : 8)
- BYTES_SQUARED (longueur : 8)
- BYTES_SQUARED_PERMANENT (longueur : 8)
- IP LENGTH MINIMUM (longueur : 8)
- IP LENGTH MAXIMUM (longueur : 8)
- MUL_DOCTETS (longueur : 8)
- postMCastOctetTotalCount (longueur : 8)

Modèles IPFIX d'options KVM

Il existe un modèle d'options KVM, basé sur la RFC 7011, section 3.4.2 de l'IETF.

Modèle d'options

ID de modèle : 462. Nombre d'étendues : 1. Nombre de données : 1.

Suivre le chemin d'un paquet avec Traceflow

Utilisez Traceflow pour inspecter le chemin d'un paquet lorsqu'il se déplace d'un port logique sur le réseau logique à un autre port logique sur le même réseau. Traceflow suit le chemin de niveau nœud de transport d'un paquet injecté sur un port logique. Le paquet suivi traverse la superposition du commutateur logique, mais il n'est pas visible pour les interfaces attachées au commutateur logique. Autrement dit, aucun paquet n'est vraiment remis aux destinataires prévus du paquet de test.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Accédez à l'écran Traceflow. Deux options s'offrent à vous.
 - Sélectionnez **Outils > Traceflow** dans le panneau de navigation.
 - Sélectionnez **Commutation** dans le panneau de navigation, cliquez sur l'onglet **Ports**, sélectionnez un port attaché à un VIF et cliquez sur **Actions > Traceflow**
- 3 Sélectionnez un type de trafic.
Les choix sont Monodiffusion, Multidiffusion et Diffusion.

4 Spécifiez les informations sur la source et la destination en fonction du type de trafic.

Type de trafic	Spécifier des informations sur la source	Spécifier des informations sur la destination
Monodiffusion	<p>Sélectionnez une VM et une interface virtuelle.</p> <p>L'adresse IP et l'adresse MAC sont affichées si VMtools est installé dans la VM ou si la VM est déployée à l'aide du plug-in OpenStack (des liaisons d'adresse seront utilisées dans ce cas). Si la VM dispose de plusieurs adresses IP, sélectionnez-en une dans le menu déroulant.</p> <p>Si l'adresse IP et l'adresse MAC ne sont pas affichées, entrez-les dans les zones de texte.</p> <p>Cela s'applique également à Multidiffusion et Diffusion.</p>	<p>Choisissez Nom de VM ou IP-MAC dans le menu déroulant Type.</p> <ul style="list-style-type: none"> ■ Si Nom de VM est sélectionné, sélectionnez une VM et une interface virtuelle. Sélectionnez ou entrez une adresse IP et une adresse MAC. ■ Si IP-MAC est sélectionné, sélectionnez le type de suivi (couche 2 ou couche 3). Si le type de suivi est Couche 2, entrez une adresse IP et une adresse MAC. Si le type de suivi est Couche 3, entrez une adresse IP.
Multidiffusion	Même chose que ci-dessus.	Entrez une adresse IP. Il doit s'agir d'une adresse multidiffusion comprise entre 224.0.0.0 et 239.255.255.255.
Diffusion	Même chose que ci-dessus.	Entrez une longueur de préfixe de sous-réseau.

5 (Facultatif) Cliquez sur **Avancé** pour voir les options avancées.

6 (Facultatif) Dans la colonne de gauche, entrez les valeurs souhaitées pour les champs suivants :

Option	Description
Taille de la trame	Par exemple, 128
TTL	Par exemple, 64
Délai d'expiration (ms)	Par exemple, 10 000
EtherType	Par exemple, 2048
Type de charge utile	Sélectionnez une option dans le menu déroulant.
Données relatives à la charge utile	Charge utile formatée en fonction du type de charge utile sélectionné (Base64, Hex, Texte brut, Binaire ou Décimal)

7 (Facultatif) Dans la colonne de gauche sous Protocole, sélectionnez un protocole dans le menu déroulant Type.

8 (Facultatif) En fonction du protocole sélectionné, exécutez les étapes associées dans le tableau suivant.

Protocole	Étape 1	Étape 2	Étape 3
TCP	Entrez un port source.	Entrez un port de destination.	Sélectionnez les indicateurs TCP souhaités dans le menu déroulant.
UDP	Entrez un port source.	Entrez un port de destination.	S/O
ICMP	Entrez un ID ICMP.	Entrez une valeur de séquence.	S/O

9 Cliquez sur **Trace**.

Des informations sur les connexions, les composants et les couches sont affichées. La sortie inclut un tableau répertoriant le type d'observation (Livré, Abandonné, Reçu, Transféré), le nœud de transport et le composant, ainsi qu'une carte graphique de la topologie si la monodiffusion et un commutateur logique comme destination sont sélectionnés. Vous pouvez appliquer un filtre (**Tout**, **Livré**, **Abandonné**) sur les observations qui s'affichent. S'il existe des observations abandonnées, le filtre **Abandonné** est appliqué par défaut. Sinon, le filtre **Tout** est appliqué. La carte graphique affiche le fond de panier et les liens du routeur. Notez que les informations de pontage ne sont pas affichées.

Afficher les informations de connexion du port

Vous pouvez utiliser l'outil de connexion du port pour visualiser et dépanner rapidement la connexion entre deux VM.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Outils > Connexion au port** dans le panneau de navigation.
- 3 Sélectionnez une VM dans le menu déroulant **Machine virtuelle source**.
- 4 Sélectionnez une VM dans le menu déroulant **Machine virtuelle de destination**.
- 5 Cliquez sur **Aller à**.

Une carte visuelle de la topologie de connexion du port s'affiche. Vous pouvez cliquer sur n'importe quel composant de la carte pour afficher davantage d'informations le concernant.

Surveiller l'activité d'un port de commutateur logique

Vous pouvez surveiller l'activité du port logique pour, par exemple, dépanner la surcharge du réseau et des paquets abandonnés.

Conditions préalables

Vérifiez qu'un port de commutateur logique est configuré. Reportez-vous à la section [Connexion d'une machine virtuelle à un commutateur logique](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Mise en réseau > Commutation** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Ports**.
- 4 Cliquez sur le nom d'un port.

5 Cliquez sur l'onglet **Surveiller**.

L'état du port et les statistiques sont affichés.

6 Pour télécharger un fichier CSV des adresses MAC apprises par l'hôte, cliquez sur **Télécharger la table MAC**.**7** Pour contrôler l'activité sur le port, cliquez sur **Commencer le suivi**.

Une page de suivi du port s'ouvre. Vous pouvez voir le trafic de port bidirectionnel et identifier les paquets abandonnés. La page de suivi du port répertorie également les profils de commutation attachés au port de commutateur logique.

Résultats

Par exemple, si vous remarquez des paquets abandonnés en raison d'une surcharge du réseau, vous pouvez configurer un profil de commutation QoS pour le port de commutateur logique afin d'éviter toute perte de données sur les paquets préférés. Reportez-vous à la section [Comprendre le profil de commutation QoS](#).

Surveiller des sessions de mise en miroir de ports

Vous pouvez surveiller des sessions de mise en miroir de ports à des fins de dépannage ou autre.

Remarques concernant NSX Cloud Si vous utilisez NSX Cloud, reportez-vous à la section [Comment utiliser des fonctionnalités NSX-T Data Center avec le cloud public](#) pour obtenir la liste des entités logiques générées automatiquement, les fonctionnalités prises en charge et les configurations requises pour NSX Cloud.

Cette fonctionnalité présente les restrictions suivantes :

- Un port de miroir source ne peut pas se trouver dans plusieurs sessions de miroir.
- Un port de destination ne peut recevoir que du trafic de miroir.
- Avec KVM, plusieurs cartes réseau peuvent être attachées au même port OVS. La mise en miroir se produit au niveau du port de liaison montante OVS, ce qui signifie que le trafic sur tous les pNIC attachés au port OVS est mis en miroir.
- Les ports source et de destination de session de miroir doivent se trouver sur le même vSwitch hôte. Par conséquent, si vous migrez par vMotion la VM avec le port source ou de destination vers un autre hôte, le trafic sur ce port ne peut plus être mis en miroir.
- Sur ESXi, lorsque la mise en miroir est activée sur la liaison montante, des paquets TCP de production brute sont encapsulés à l'aide du protocole Geneve par VDL2 dans des paquets UDP. Une carte réseau physique prenant en charge TSO (TCP Segmentation Offload) peut modifier les paquets et les marquer avec l'indicateur MUST_TSO. Sur une VM de moniteur avec des vNIC VMXNET3 ou E1000, le pilote traite les paquets comme des paquets UDP normaux. Il ne peut pas traiter l'indicateur MUST_TSO et il abandonne les paquets.

Si une grande partie du trafic est mise en miroir vers une VM de moniteur, il existe un risque que l'anneau de tampon du pilote sature et que des paquets soient abandonnés. Pour régler le problème, vous pouvez prendre une ou plusieurs des mesures suivantes :

- Augmentez la taille de l'anneau de tampon rx.
- Attribuez plus de ressources de CPU à la VM.
- Utilisez le DPDK (Data Plane Development Kit) pour améliorer les performances du traitement des paquets.

Note Vérifiez que le paramètre MTU de la VM de moniteur (dans le cas de KVM, également le paramètre MTU du périphérique de carte réseau virtuelle de l'hyperviseur) est suffisamment élevé pour traiter les paquets. Cela est particulièrement important pour les paquets encapsulés, car l'encapsulation augmente la taille des paquets. Sinon, les paquets peuvent être abandonnés. Ce n'est pas un problème avec les VM ESXi avec des cartes réseau VMXNET3, mais il s'agit d'un risque potentiel avec les autres types de cartes réseau sur les VM ESXi et KVM.

Note Dans une session de mise en miroir de ports L3 impliquant des VM sur des hôtes KVM, vous devez définir une taille MTU suffisamment grande pour traiter les octets supplémentaires requis par l'encapsulation. Le trafic de miroir passe par une interface OVS et une liaison montante OVS. Vous devez définir une taille MTU de l'interface OVS d'au moins 100 octets de plus que la taille du paquet d'origine (avant l'encapsulation et la mise en miroir). Si vous voyez des paquets abandonnés, augmentez le paramètre MTU pour la carte réseau virtuelle de l'hôte et l'interface OVS. Utilisez la commande suivante pour définir le paramètre MTU pour une interface OVS :

```
ovs-vsctl -- set interface <ovs_Interface> mtu_request=<MTU>
```

Note Lorsque vous surveillez le port logique d'une VM et le port de liaison montante d'un hôte sur lequel réside la VM, vous verrez différents comportements selon si l'hôte est ESXi ou KVM. Pour ESXi, les paquets de miroir de port logique et les paquets de miroir de liaison montante sont étiquetés avec le même ID VLAN et ils sont semblables pour la VM de moniteur. Pour KVM, les paquets de miroir de port logique ne sont pas étiquetés avec un ID VLAN, mais les paquets de miroir de liaison montante sont étiquetés. Ils sont différents pour la VM de moniteur.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Outils > Session de mise en miroir de ports** dans le panneau de navigation.
- 3 Cliquez sur **Ajouter** et sélectionnez un type de session.
Les types disponibles sont **SPAN local**, **SPAN distant**, **SPLAN L3 distant** et **SPAN logique**.
- 4 Entrez un nom de session et éventuellement une description.

5 Fournissez les paramètres supplémentaires.

Type de session	Paramètres
SPAN local	<ul style="list-style-type: none"> ■ Nœud de transport - sélectionnez un nœud de transport. ■ Direction - sélectionnez Bidirectionnel, Entrée ou Sortie. ■ Troncation des paquets - sélectionnez une valeur de troncation des paquets.
SPAN distant	<ul style="list-style-type: none"> ■ Type de session - sélectionnez Session source RSPAN ou Session de destination RSPAN. ■ Nœud de transport - sélectionnez un nœud de transport. ■ Direction - sélectionnez Bidirectionnel, Entrée ou Sortie. ■ Troncation des paquets - sélectionnez une valeur de troncation des paquets. ■ ID de VLAN d'encapsulation - spécifiez un ID de VLAN d'encapsulation. ■ Conserver le VLAN d'origine - indiquez si vous voulez conserver l'ID de VLAN d'origine.
SPAN L3 distant	<ul style="list-style-type: none"> ■ Encapsulation - sélectionnez GRE, ERSPAN TWO ou ERSPAN THREE. ■ Clé GRE - spécifiez une clé GRE si l'encapsulation est GRE. ■ Nœud de transport - spécifiez un nœud de transport si l'encapsulation est ERSPAN TWO ou ERSPAN THREE. ■ ID ERSPAN - spécifiez un ID ERSPAN si l'encapsulation est ERSPAN TWO ou ERSPAN THREE. ■ Direction - sélectionnez Bidirectionnel, Entrée ou Sortie. ■ Troncation des paquets - sélectionnez une valeur de troncation des paquets.
SPAN logique	<ul style="list-style-type: none"> ■ Commutateur logique - sélectionnez un commutateur logique. ■ Direction - sélectionnez Bidirectionnel, Entrée ou Sortie. ■ Troncation des paquets - sélectionnez une valeur de troncation des paquets.

6 Cliquez sur **Suivant**.

7 Fournissez des informations sur la source.

Type de session	Paramètres
SPAN local	<ul style="list-style-type: none"> ■ Sélectionnez un N-VDS. ■ Sélectionnez des interfaces physiques. ■ Activez ou désactivez le paquet encapsulé. ■ Sélectionnez les machines virtuelles. ■ Sélectionnez les interfaces virtuelles.
SPAN distant	<ul style="list-style-type: none"> ■ Sélectionnez les machines virtuelles. ■ Sélectionnez les interfaces virtuelles.
SPAN L3 distant	<ul style="list-style-type: none"> ■ Sélectionnez les machines virtuelles. ■ Sélectionnez les interfaces virtuelles. ■ Sélectionnez un commutateur logique.
SPAN logique	<ul style="list-style-type: none"> ■ Sélectionnez les ports logiques.

8 Cliquez sur **Suivant**.

9 Fournissez les informations sur la destination.

Type de session	Paramètres
SPAN local	<ul style="list-style-type: none"> ■ Sélectionnez les machines virtuelles. ■ Sélectionnez les interfaces virtuelles.
SPAN distant	<ul style="list-style-type: none"> ■ Sélectionnez un N-VDS. ■ Sélectionnez des interfaces physiques.
SPAN L3 distant	<ul style="list-style-type: none"> ■ Spécifiez une adresse IPv4.
SPAN logique	<ul style="list-style-type: none"> ■ Sélectionnez les ports logiques.

10 Cliquez sur **Enregistrer**.

Vous ne pouvez pas modifier la source ou la destination après l'enregistrement de la session de mise en miroir de ports.

Surveiller les nœuds d'infrastructure

Vous pouvez surveiller les nœuds d'infrastructure tels que des hôtes, des dispositifs Edge, des clusters NSX Edge, des ponts et des nœuds de transport à partir de l'interface utilisateur de NSX Manager.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<adresse-ip-nsx-manager>`.
- 2 Sélectionnez **Infrastructure > Nœuds** dans le panneau de navigation.
- 3 Sélectionnez l'un des onglets suivants.
 - Hôtes
 - Dispositifs Edge
 - Clusters Edge
 - Ponts
 - Nœuds de transport

Résultats

Note Sur l'écran Hôtes, si l'état de Connectivité MPA est Inactive ou Inconnue pour un hôte, ignorez l'état de Connectivité LCP, car il peut être inexact.

Afficher des données sur les applications exécutées sur des machines virtuelles

Vous pouvez afficher des informations sur les applications exécutées sur des machines virtuelles qui sont membres d'un NSGroup. Il s'agit d'une fonctionnalité de la version d'évaluation technique.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur *https://<adresse-ip-nsx-manager>*.
- 2 Sélectionnez **Inventaire > Groupes** dans le panneau de navigation.
- 3 Cliquez sur le nom d'un NSGroup.
- 4 Cliquez sur l'onglet **Applications**.
- 5 Cliquez sur **COLLECTER DES DONNÉES D'APPLICATION**.

Ce processus peut prendre quelques minutes. Lorsque le processus est terminé, les informations suivantes s'affichent :

- Le nombre total de processus.
 - Des cercles représentant divers niveaux, par exemple, couche Web, couche de base de données et couche d'application. Le nombre de processus de chaque niveau est également affiché.
- 6 Cliquez sur un cercle pour voir plus d'informations sur les processus dans cette couche.

Collecte des bundles de support

Vous pouvez collecter des bundles de support sur des nœuds de cluster et d'infrastructure enregistrés et télécharger les bundles sur votre machine ou sur un serveur de fichiers.

Si vous choisissez de télécharger les bundles sur votre machine, vous obtenez un fichier d'archive composé d'un fichier manifeste et de bundles de support pour chaque nœud. Si vous choisissez de télécharger les bundles sur un serveur de fichiers, le fichier manifeste et les bundles individuels sont téléchargés sur le serveur de fichiers séparément.

Remarque concernant NSX Cloud Si vous souhaitez collecter le bundle de support pour CSM, connectez-vous à CSM, accédez à **Système > Utilitaires > Bundle de support**, puis cliquez sur **Télécharger**. Le bundle de support pour PCG est disponible à partir de NSX Manager en suivant les instructions suivantes. Le bundle de support pour PCG contient également des journaux de toutes les machines virtuelles de charge de travail.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à NSX Manager sur *https://nsx-manager-ip-address*.
- 2 Sélectionnez **Système > Utilitaires** dans le panneau de navigation.
- 3 Cliquez sur l'onglet **Bundle de support**.
- 4 Sélectionnez les nœuds cibles.

Les types de nœuds disponibles sont les nœuds de gestion, les nœuds de contrôleur, les dispositifs Edge, les hôtes et les passerelles PCG.

- 5 (Facultatif) Spécifiez l'âge de journal en jours pour exclure les journaux antérieurs au nombre de jours spécifié.
- 6 (Facultatif) Basculez le commutateur qui indique s'il faut inclure ou exclure les fichiers noyaux et les journaux d'audit.

Note Les fichiers noyaux et les journaux d'audit peuvent contenir des informations sensibles, telles que des mots de passe ou des clés de chiffrement.

- 7 (Facultatif) Cochez une case pour télécharger les bundles sur un serveur de fichiers.
- 8 Cliquez sur **Démarrer la collecte des bundles** pour démarrer la collecte des bundles de support.
En fonction du nombre de fichiers journaux existants, chaque nœud peut prendre plusieurs minutes.
- 9 Surveillez l'état du processus de collecte.
Le champ d'état indique le pourcentage de nœuds ayant terminé la collecte des bundles de support.
- 10 Cliquez sur **Télécharger** pour télécharger le bundle si l'option pour envoyer le bundle à un serveur de fichiers n'a pas été définie.

Programme d'amélioration du produit

NSX-T Data Center participe au Programme d'amélioration du produit de VMware (CEIP).

Les détails concernant les données recueillies via le CEIP et les fins auxquelles elles sont utilisées par VMware sont définis dans le Centre d'approbation et d'assurance à l'adresse <https://www.vmware.com/solutions/trustvmware/ceip.html>.

Pour joindre ou quitter le CEIP pour NSX-T Data Center ou pour modifier les paramètres du programme, reportez-vous à la section [Modifier la configuration du Programme d'amélioration du produit](#).

Modifier la configuration du Programme d'amélioration du produit

Lorsque vous installez ou mettez à niveau NSX Manager, vous pouvez décider de participer au programme CEIP et configurer les paramètres de collecte de données.

Vous pouvez également modifier la configuration CEIP existante pour rejoindre ou quitter le programme, définir la fréquence et les jours où les informations sont collectées ainsi que la configuration du serveur proxy.

Conditions préalables

- Vérifiez que NSX Manager est connecté et peut se synchroniser avec votre hyperviseur.
- Vérifiez que NSX-T Data Center est connecté à un réseau public pour télécharger les données.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<adresse-ip-nsx-manager>>.
- 2 Sélectionnez **Système > Configuration > Propriétés**.

- 3 Cliquez sur **Modifier** dans la section État et statistiques.
- 4 Basculez l'élément de menu **Collecte de données** .
- 5 Cliquez sur **Modifier** dans la section Programme d'amélioration du produit.
- 6 Basculez l'élément de menu **Prendre part au programme d'amélioration de l'expérience utilisateur de VMware**.
- 7 (Facultatif) Configurez les paramètres de collecte de données et de récurrence du téléchargement.
- 8 (Facultatif) Cliquez sur l'onglet **Proxy**.
- 9 Basculez l'élément de menu **Proxy** pour configurer les paramètres du serveur proxy pour envoyer des données.

Option	Description
Nom d'hôte	Entrez le nom de domaine complet ou l'adresse IP du serveur proxy.
Port	Entrez le port du serveur proxy.
Nom d'utilisateur	(Facultatif) Entrez le nom d'utilisateur utilisé pour s'authentifier auprès du serveur proxy.
Mot de passe	(Facultatif) Entrez le mot de passe utilisé pour s'authentifier auprès du serveur proxy.
Schéma	Définissez le schéma HTTP ou HTTPS accepté par le serveur proxy dans le menu déroulant.

- 10 Cliquez sur **Enregistrer**.