

Guide d'administration de NSX-T Data Center

Modifié le 6 mai 2022

VMware NSX-T Data Center 2.5

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

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

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

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

Copyright © 2022 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 13

1 Présentation de NSX Manager 14

2 Passerelles de niveau 0 17

Ajouter une passerelle de niveau 0 18

Créer une liste de préfixes IP 21

Créer une liste de communauté 23

Configurer un itinéraire statique 24

Créer une carte de route 24

Utilisation d'expressions régulières pour faire correspondre les listes de communauté lors de l'ajout de mappages de route 27

Configurer BGP 28

Configurer BFD 32

Configurer le transfert de couche 3 IPv6 32

Créer des profils SLAAC et DAD pour l'attribution d'adresses IPv6 33

3 Passerelle de niveau 1 36

Ajouter une passerelle de niveau 1 36

4 Segments 39

Profils de segments 39

Comprendre le profil de segment QoS 40

Comprendre le profil de segment de découverte d'adresses IP 43

Comprendre le profil de segment SpoofGuard 45

Comprendre le profil de segmentation de sécurité de segment 47

Comprendre le profil de segment de découverte d'adresses MAC 49

Ajouter un segment 50

5 VPN (Virtual Private Network) 53

Comprendre le VPN IPSec 54

Utilisation d'un VPN IPSec basé sur les stratégies 54

Utilisation du VPN IPSec basé sur une route 55

Présentation de VPN de couche 2 57

Ajout de services VPN 58

Ajouter un service VPN IPSec 60

Ajouter un service VPN L2 62

Ajout de sessions VPN IPSec 65

Ajouter une session IPSec basée sur les stratégies	65
Ajout d'une session IPSec basée sur une route	69
À propos des suites de conformité prises en charge	73
Présentation de la restriction MSS TCP	74
Ajout de sessions VPN L2	74
Ajouter une session de serveur VPN L2	75
Ajouter une session client VPN de couche 2	77
Télécharger le fichier de configuration du VPN de couche 2 côté distant	79
Ajouter des points de terminaison locaux	80
Ajout de profils	81
Ajouter des profils IKE	82
Ajouter des profils IPSec	85
Ajouter des profils DPD	88
Ajouter un dispositif Edge autonome en tant que client VPN L2	89
Vérifier l'état réalisé d'une session VPN IPSec	92
Surveiller et dépanner des sessions VPN	95
6 Traduction d'adresse réseau	96
Configurer la NAT sur une passerelle	96
7 Équilibrage de charge	99
Concepts clés de l'équilibreur de charge	100
Évolutivité des ressources d'équilibreur de charge	100
Fonctionnalités d'équilibrage de charge prises en charge	101
Topologies d'équilibreur de charge	102
Configuration des composants d'équilibrage de charge	104
Ajouter des équilibrages de charge	104
Ajouter un moniteur actif	106
Ajouter un moniteur passif	110
Ajouter un pool de serveurs	111
Configuration des composants de serveur virtuel	116
Groupes créés pour les pools de serveurs et les serveurs virtuels	140
8 Stratégies de transfert	142
Ajouter ou modifier des stratégies de transfert	143
9 IP Address Management (IPAM)	145
Ajouter une zone DNS	145
Ajouter un service de transfert DNS	146
Ajouter un serveur DHCP	147
Configurer un serveur de relais DHCP pour une passerelle de niveau 0 ou de niveau 1	148

- Ajouter un pool d'adresses IP 149
- Ajouter un bloc d'adresses IP 150

10 Sécurité 151

- Présentation de la configuration de la sécurité 151
- Terminologie de la sécurité 152
- Pare-feu d'identité 152
 - Workflow d'Identity Firewall 154
- Profil de contexte de couche 7 156
 - Workflow de règles de pare-feu de couche 7 158
 - Attributs 159
- Pare-feu distribué 163
 - Brouillons de pare-feu 163
 - Ajouter un pare-feu distribué 166
 - Journaux de paquet de pare-feu distribué 171
 - Sélectionner une stratégie de connectivité par défaut 173
 - Gérer une liste d'exclusion de pare-feu 174
 - Filtrage de domaines spécifiques (noms de domaine complets/URL) 174
 - Extension des stratégies de sécurité aux charges de travail physiques 176
 - Ensembles d'adresses partagées 183
- Sécurité du réseau est-ouest : chaînage des services tiers 184
 - Concepts clés de la protection de réseau horizontal 184
 - Exigences de NSX-T Data Center pour le trafic est-ouest 185
 - Tâches de haut niveau de la sécurité réseau est-ouest 186
 - Déployer un service pour l'inspection horizontale du trafic 186
 - Ajouter un profil de service 188
 - Ajouter une chaîne de services 188
 - Ajouter des règles de redirection pour le trafic horizontal 189
- Configuration d'un pare-feu de passerelle 192
 - Ajouter une règle ou une stratégie de pare-feu de passerelle 192
- Sécurité du réseau nord-sud : insertion de service tiers 196
 - Tâches de haut niveau de la sécurité réseau nord-sud 196
 - Déployer un service pour l'inspection verticale du trafic 196
 - Configurer la redirection du trafic 198
 - Ajouter des règles de redirection pour le trafic nord-sud 200
 - Surveiller la redirection du trafic 201
- Protection de point de terminaison 202
 - Comprendre la protection du point de terminaison 202
 - Configurer la protection du point de terminaison 207
 - Gérer la protection du point de terminaison 223
- Profil de sécurité 237

- Créer un temporisateur de session 237
- Protection de propagation 239
- Configurer la sécurité DNS 242
- Gérer la priorité des groupes sur les profils 244

11 Inventaire 245

- Ajouter un service 245
- Ajouter un groupe 246
- Ajouter un profil de contexte 248

12 Surveillance 250

- Ajouter un profil IPFIX de pare-feu 250
- Ajouter un profil IPFIX de commutateur 251
- Ajouter un collecteur IPFIX 252
- Ajouter un profil de mise en miroir de ports 253
- Protocole de gestion de réseau simple (SNMP) 254
- Utilisation de vRealize Log Insight pour la surveillance du système 255
- Utilisation de vRealize Operations Manager pour la surveillance du système 256
- Utilisation de vRealize Network Insight Cloud pour la surveillance du système 260
- Outils de surveillance avancés 273
 - Afficher les informations de connexion au port 273
 - Traceflow 273
 - Surveiller des sessions de mise en miroir de ports 276
 - Configurer des filtres pour une session de mise en miroir de ports 280
 - Configurer IPFIX 281
 - Surveiller l'activité d'un port de commutateur logique 451

13 Commutateurs logiques 453

- Comprendre les modes de répllication de trame BUM 455
- Créer un commutateur logique 456
- Connexion d'une machine virtuelle à un commutateur logique 457
 - Attacher une VM hébergée sur vCenter Server à un commutateur logique NSX-T Data Center 458
 - Attacher une machine virtuelle autonome hébergée sur un hôte ESXi autonome à un commutateur logique NSX-T Data Center 459
 - Attacher une VM hébergée sur KVM à un commutateur logique NSX-T Data Center 465
- Créer un port de commutateur logique 466
- Tester la connectivité de couche 2 467
- Créer un commutateur logique VLAN pour la liaison montante NSX Edge 470
- Basculement des profils pour commutateurs logiques et ports logiques 472
 - Comprendre le profil de commutation QoS 474
 - Comprendre le profil de commutation de mise en miroir de ports 476

Comprendre le profil de commutation de découverte d'adresses IP	479
Comprendre SpoofGuard	482
Comprendre le profil de commutation de sécurité de commutateur	484
Comprendre le profil de commutation de gestion MAC	486
Associer un profil personnalisé à un commutateur logique	488
Associer un profil personnalisé à un port logique	489
Pile de mise en réseau améliorée	490
Attribuer automatiquement des cœurs logiques ENS	490
Configurer le routage inter-VLAN d'invité	491
Pontage de couche 2	493
Créer un profil de pont Edge	494
Configurer le pontage basé sur Edge	495
Créer un commutateur logique sauvegardé par pont de couche 2	498

14 Routeurs logiques 500

Routeur logique de niveau 1	500
Créer un routeur logique de niveau 1	502
Ajouter un port de liaison descendante sur un routeur logique de niveau 1	503
Ajouter un port VLAN sur un routeur logique de niveau 0 ou de niveau 1	504
Configurer l'annonce d'itinéraires sur un routeur logique de niveau 1	505
Configurer l'itinéraire statique d'un routeur logique de niveau 1	507
Créer un routeur logique de niveau 1 autonome	509
Routeur logique de niveau 0	511
Créer un routeur logique de niveau 0	512
Attacher le niveau 0 et le niveau 1	513
Connecter un routeur logique de niveau 0 à un commutateur logique VLAN pour la liaison montante NSX Edge	516
Ajouter un port de routeur de bouclage	520
Ajouter un port VLAN sur un routeur logique de niveau 0 ou de niveau 1	520
Configurer un itinéraire statique	521
Options de configuration de BGP	525
Configurer BFD sur un routeur logique de niveau 0	532
Activer la redistribution d'itinéraire sur le routeur logique de niveau 0	532
Comprendre le routage ECMP	535
Créer une liste de préfixes IP	539
Créer une liste de communauté	540
Créer une carte de route	541
Configurer le temporisateur d'activation du transfert	542

15 NAT avancé 544

Traduction d'adresse réseau	544
NAT de niveau 1	546

NAT de niveau 0 553

NAT réflexive 554

16 Regroupement d'objets avancé 558

Créer un ensemble d'adresses IP 558

Créer un pool d'adresses IP 559

Créer un ensemble d'adresses MAC 560

Créer un NSGroup 560

Configuration de services et de groupes de services 562

Créer un NSService 563

Gérer les balises d'une machine virtuelle 563

17 DHCP avancé 565

DHCP 565

Créer un profil de serveur DHCP 566

Créer un serveur DHCP 566

Attacher un serveur DHCP à un commutateur logique 567

Détacher un serveur DHCP d'un commutateur logique 567

Créer un profil de relais DHCP 568

Créer un service de relais DHCP 568

Ajouter un service de relais DHCP à un port de routeur logique 568

Supprimer un bail DHCP 569

Proxys de métadonnées 569

Ajouter un serveur proxy de métadonnées 570

Attacher un serveur proxy de métadonnées à un commutateur logique 571

Détacher un serveur proxy de métadonnées d'un commutateur logique 571

18 Gestion avancée des adresses IP 573

Gérer des blocs d'adresses IP 573

Gérer des sous-réseaux pour des blocs d'adresses IP 574

19 Équilibrage de charge avancé 575

Concepts clés de l'équilibreur de charge 576

Configuration des composants d'équilibreur de charge 577

Créer un équilibrage de charge 577

Configurer un moniteur de santé actif 578

Configurer les moniteurs de santé passifs 582

Ajouter un pool de serveurs pour l'équilibrage de charge 583

Configuration des composants de serveur virtuel 587

20 Pare-feu avancé 611

Ajouter ou supprimer une règle de pare-feu à un routeur logique	611
Configurer le pare-feu pour un port de pont de commutateur logique	612
Sections de pare-feu et règles de pare-feu	613
Activer et désactiver un pare-feu distribué	613
Ajouter une section de règles de pare-feu	614
Supprimer une section de règles de pare-feu	615
Activer et désactiver des règles de section	615
Activer et désactiver des journaux de sections	616
Configurer une liste d'exclusion de pare-feu	616
À propos des règles de pare-feu	616
Ajouter une règle de pare-feu	618
Suppression d'une règle de pare-feu	621
Modifier la règle du pare-feu distribué par défaut	621
Modifier l'ordre d'une règle de pare-feu	622
Filtrer les règles de pare-feu	622

21 Opérations et gestion 624

Afficher les tableaux de bord de surveillance	625
Afficher l'utilisation et la capacité des catégories d'objets	627
Vérification de l'état réalisé d'un changement de configuration	629
Rechercher des objets	633
Filtrer par attributs d'objet	635
Ajouter un gestionnaire de calcul	635
Ajout d'Active Directory	638
Ajouter un serveur LDAP	639
Synchroniser Active Directory	640
Gestion des comptes d'utilisateur et du contrôle d'accès basé sur les rôles	641
Gérer le mot de passe d'un utilisateur	641
Réinitialisation des mots de passe d'un dispositif	642
Paramètres de stratégie d'authentification	644
Obtenir l'empreinte numérique de certificat à partir d'un hôte vIDM	645
Configurer l'intégration de VMware Identity Manager	645
Valider les fonctionnalités de VMware Identity Manager	648
Synchronisation de l'heure entre NSX Manager, vIDM et les composants associés	650
Contrôle d'accès basé sur les rôles	651
Ajouter une attribution de rôle ou une identité de principal	663
Sauvegarde et restauration de NSX Manager	665
Configurer des sauvegardes	666
Suppression d'anciennes sauvegardes	668
Liste des sauvegardes disponibles	668
Restaurer une sauvegarde	669

Sauvegarde et restauration pendant la mise à niveau	672
Supprimer l'extension NSX-T Data Center de vCenter Server	672
Gestion du cluster NSX Manager	673
Afficher la configuration et l'état du cluster NSX Manager	674
Arrêter et mettre sous tension le cluster NSX Manager	676
Redémarrer NSX Manager	677
Modifier l'adresse IP d'un NSX Manager	677
Redimensionner un nœud NSX Manager	679
Ajout et suppression d'un nœud de transport d'hôte ESXi vers et depuis des serveurs vCenter	680
Remplacement d'un nœud de transport NSX Edge dans un cluster NSX Edge	681
Remplacer un nœud de transport NSX Edge à l'aide de l'interface utilisateur de NSX Manager	681
Remplacer un nœud de transport NSX Edge à l'aide de l'API	682
Récupération de NSX-T lorsque vCenter Server est perdu et ne peut pas être récupéré	683
Déploiement multisite de NSX-T Data Center	685
Configuration de dispositifs	692
Ajouter une clé de licence et générer un rapport d'utilisation de licence	693
Configuration de certificats	694
Importer un certificat	695
Créer un fichier de demande de signature de certificat	695
Importer un certificat d'autorité de certification	697
Créer un certificat auto-signé	698
Remplacer le certificat d'un nœud NSX Manager ou l'adresse IP virtuelle d'un cluster NSX Manager	699
Importer une liste de révocation des certificats	700
Configuration de NSX Manager pour récupérer une liste de révocation des certificats	701
Importer un certificat pour une demande de signature de certificat	702
Stockage des certificats publics et des clés privées	702
Configuration basée sur la conformité	702
Afficher le rapport sur l'état de conformité	703
Codes de rapport d'état de conformité	704
Configurer le mode de conformité FIPS global pour l'équilibreur de charge	707
Collecter des bundles de support	710
Messages de journal et codes d'erreur	711
Configurer la journalisation à distance	713
ID de messages de journal	720
Résolution des problèmes de Syslog	722
Configurer la journalisation série sur une machine virtuelle de dispositif	722
Programme d'amélioration du produit	723
Modifier la configuration du Programme d'amélioration du produit	723
Ajouter des balises à un objet	724

- Rechercher l'empreinte digitale SSH d'un serveur distant 725
- Afficher des données sur les applications exécutées sur des machines virtuelles 726
- Configuration d'un équilibreur de charge externe 727

22 Utilisation de NSX Cloud 729

- Présentation rapide de Cloud Service Manager 729
 - Clouds 730
 - Système 734
- Détection des menaces à l'aide de la stratégie de mise en quarantaine de NSX Cloud 737
 - Stratégie de mise en quarantaine dans le Mode d'application NSX 738
 - Stratégie de mise en quarantaine dans le Mode d'application du Cloud natif 744
 - Mise sur liste blanche de machines virtuelles 745
- Mode d'application NSX 746
 - Systèmes d'exploitation actuellement pris en charge pour les machines virtuelles de charge de travail 747
 - Intégration de machines virtuelles dans le Mode d'application NSX 748
 - Gestion des machines virtuelles dans le Mode d'application NSX 757
- Mode d'application du Cloud natif 759
 - Gestion des machines virtuelles dans le Mode d'application du Cloud natif 759
- Fonctionnalités de NSX-T Data Center prises en charge avec NSX Cloud 763
 - Regrouper les machines virtuelles à l'aide de NSX-T Data Center et de balises de cloud public 765
 - Utiliser les services cloud natifs 768
 - Insertion de services pour votre cloud public 770
 - Activer la fonctionnalité NAT sur les machines virtuelles gérées par NSX 777
 - Activer le transfert Syslog 778
 - Configurer le VPN en mode NSX appliqué 778
- Questions fréquemment posées (FAQ) 783

23 Utilisation de NSX Intelligence 787

- Démarrage avec NSX Intelligence 787
 - Découverte de la page d'accueil de NSX Intelligence 788
 - Familiarisation avec les éléments graphiques de NSX Intelligence 790
- Présentation des vues et des flux de NSX Intelligence 792
 - Utilisation de la vue Groupes 792
 - Utilisation de la vue VM 797
 - Utilisation des flux de trafic 800
- Utilisation des recommandations de NSX Intelligence 801
 - Comprendre les recommandations de NSX Intelligence 802
 - Générer une nouvelle recommandation de NSX Intelligence 802
 - Vérifier et publier une recommandation générée 804
- Sauvegarde et restauration de NSX Intelligence 806

Configurer des sauvegardes NSX Intelligence	807
Sauvegarder NSX Intelligence	808
Restaurer des sauvegardes de NSX Intelligence	809
Dépannage des problèmes liés à NSX Intelligence	810
Vérifier l'état du dispositif NSX Intelligence	810
Collecter des bundles de support NSX Intelligence	815

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, la NAT, les pare-feu, SpoofGuard, le regroupement et DHCP. Il décrit également comment configurer NSX Cloud.

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

Présentation de NSX Manager

1

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

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

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

Quand utiliser la stratégie ou les interfaces avancées

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

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

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


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

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

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

Utilisation de l'interface de stratégie

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

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

Où trouver les interfaces de stratégie et les interfaces avancées

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

Tableau 1-2. Interfaces de stratégie et interfaces avancées

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

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

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

Noms des objets créés dans la stratégie et les interfaces avancées

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

Tableau 1-3. Noms des objets

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

Passerelles de niveau 0

2

Une passerelle de niveau 0 exécute les fonctions d'un routeur logique de niveau 0. Elle traite le trafic entre les réseaux logiques et physiques.

NSX Cloud Note Si vous utilisez NSX Cloud, consultez [Fonctionnalités de NSX-T Data Centerprises en charge avec NSX Cloud](#) pour obtenir la liste des entités logiques générées automatiquement, des fonctionnalités prises en charge et des configurations requises pour NSX Cloud.

Un nœud Edge ne peut prendre en charge qu'une seule passerelle de niveau 0 ou un seul routeur logique. Lorsque vous créez une passerelle de niveau 0 ou un routeur logique, assurez-vous de ne pas créer plus de passerelles de niveau 0 ou de routeurs logiques que le nombre de nœuds Edge dans le cluster NSX Edge.

Note Dans l'onglet **Sécurité et mise en réseau avancées**, le terme « routeur logique de niveau 0 » est utilisé pour faire référence à une passerelle de niveau 0.

Ce chapitre contient les rubriques suivantes :

- [Ajouter une passerelle de niveau 0](#)
- [Créer une liste de préfixes IP](#)
- [Créer une liste de communauté](#)
- [Configurer un itinéraire statique](#)
- [Créer une carte de route](#)
- [Utilisation d'expressions régulières pour faire correspondre les listes de communauté lors de l'ajout de mappages de route](#)
- [Configurer BGP](#)
- [Configurer BFD](#)
- [Configurer le transfert de couche 3 IPv6](#)
- [Créer des profils SLAAC et DAD pour l'attribution d'adresses IPv6](#)

Ajouter une passerelle de niveau 0

Une passerelle de niveau 0 dispose de connexions de liaison descendante vers les passerelles de niveau 1 et de connexions de liaison montante vers les réseaux physiques.

Vous pouvez configurer le mode HA (haute disponibilité) d'une passerelle de niveau 0 pour qu'il soit actif-actif ou actif-en veille. Les services suivants sont pris en charge uniquement en mode actif-en veille :

- NAT
- Équilibrage de charge
- Pare-feu avec état
- VPN

Les passerelles de niveau 0 et de niveau 1 prennent en charge les configurations d'adressage suivantes pour toutes les interfaces (liaisons montantes, ports de service et liaisons descendantes) dans les topologies à un seul niveau et à plusieurs niveaux :

- IPv4 uniquement
- IPv6 uniquement
- Double pile : IPv4 et IPv6

Pour utiliser l'adressage IPv6 ou double pile, activez **IPv4 et IPv6** en tant que mode de transfert L3 dans **Mise en réseau > Paramètres de mise en réseau > Configuration de mise en réseau globale**.

Si vous configurez la redistribution de routes pour la passerelle de niveau 0, vous pouvez choisir parmi deux groupes de sources : les sous-réseaux de niveau 0 et les sous-réseaux de niveau 1 annoncés. Les sources dans le groupe de sous-réseaux de niveau 0 sont :

Type de source	Description
Interfaces et segments connectés	Il s'agit des sous-réseaux de l'interface externe, des sous-réseaux de l'interface de service et des sous-réseaux de segments connectés à la passerelle de niveau 0.
Routes statiques	Routes statiques que vous avez configurées sur la passerelle de niveau 0.
Adresse IP NAT	Adresses IP NAT appartenant à la passerelle de niveau 0 et découvertes à partir de règles NAT qui sont configurées sur la passerelle de niveau 0.
Adresse IP locale IPSec	Adresse IP locale du point de terminaison IPSec pour établir des sessions VPN.
Adresse IP du redirecteur DNS	Adresse IP de l'écouteur pour les requêtes DNS des clients et également utilisée comme adresse IP source pour transférer les requêtes DNS vers le serveur DNS en amont.

Les sources dans le groupe de sous-réseaux de niveau 1 annoncés sont :

Type de source	Description
Interfaces et segments connectés	Il s'agit des sous-réseaux de segments connectés aux sous-réseaux de passerelle de niveau 1 et de l'interface de service configurés sur la passerelle de niveau 1.
Routes statiques	Routes statiques que vous avez configurées sur la passerelle de niveau 1.

Type de source	Description
Adresse IP NAT	Adresses IP NAT appartenant à la passerelle de niveau 1 et découvertes à partir de règles NAT qui sont configurées sur la passerelle de niveau 1.
VIP D'ÉQUILIBREUR DE CHARGE	Adresse IP du serveur virtuel d'équilibrage de charge.
Adresse IP du SNAT d'équilibreur de charge	Adresse IP ou plage d'adresses IP utilisée pour la NAT source par l'équilibreur de charge.
Adresse IP du redirecteur DNS	Adresse IP de l'écouteur pour les requêtes DNS des clients et également utilisée comme adresse IP source pour transférer les requêtes DNS vers le serveur DNS en amont.
Point de terminaison local IPSec	Adresse IP du point de terminaison local IPSec.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Passerelles de niveau 0**.
- 3 Cliquez sur **Ajouter une passerelle de niveau 0**.
- 4 Entrez un nom pour la passerelle.
- 5 Sélectionnez un mode HA (haute disponibilité).

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

Important Après la création de la passerelle, le mode HA ne peut pas être modifié.

- 6 Si le mode HA est actif-en veille, 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.
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 (Facultatif) Sélectionnez un cluster NSX Edge.
- 8 (Facultatif) Ajoutez une ou plusieurs balises.

9 (Facultatif) Cliquez sur **Paramètres supplémentaires**.

- a Dans le champ **Sous-réseau de transit interne**, entrez un sous-réseau.

Il s'agit du sous-réseau utilisé pour la communication entre les composants dans cette passerelle. La valeur par défaut est 169.254.0.0/28.

- b Dans le champ **Sous-réseaux de transit T0-T1**, entrez un ou plusieurs sous-réseaux.

Ces sous-réseaux sont utilisés pour la communication entre cette passerelle et toutes les passerelles de niveau 1 qui y sont liées. Une fois que vous avez créé cette passerelle et lié une passerelle de niveau 1, vous verrez l'adresse IP réelle attribuée au lien du côté de la passerelle de niveau 0 et du côté de la passerelle de niveau 1. L'adresse s'affiche dans **Paramètres supplémentaires > Liens de routeur** sur la page de la passerelle de niveau 0 et de la passerelle de niveau 1. La valeur par défaut est 100.64.0.0/16.

- c Sélectionnez un **Profil ND** et un **Profil DAD** pour la configuration d'adresse IPv6.

Ces profils sont utilisés pour configurer SLAAC (Stateless Address Autoconfiguration) et DAD (Duplicate Address Detection) pour les adresses IPv6. Le profil par défaut est créé.

10 Cliquez sur **Enregistrer**.

11 Pour configurer la redistribution de routes, cliquez sur **Redistribution de routes** et sur **Définir**.

Sélectionnez une ou plusieurs des sources :

- Sous-réseaux de niveau 0 : **Routes statiques, Adresse IP NAT, Adresse IP locale IPSec, Adresse IP du redirecteur DNS, Interfaces et segments connectés.**

Sous **Interfaces et segments connectés**, vous pouvez sélectionner une ou plusieurs des options suivantes : **Sous-réseau de l'interface de service, Sous-réseau de l'interface externe, Sous-réseau de l'interface de bouclage, Segment connecté.**

- Sous-réseaux de niveau 1 annoncés : **Adresse IP du redirecteur DNS, Routes statiques, VIP d'équilibreur de charge, Adresse IP NAT, Adresse IP du SNAT d'équilibreur de charge, Point de terminaison local IPSec Interfaces et segments connectés.**

Sous **Interfaces et segments connectés**, vous pouvez sélectionner **Sous-réseau de l'interface de service** et/ou **Segment connecté**.

12 Pour configurer les interfaces, cliquez sur **Interfaces** et sur **Définir**.

- a Cliquez sur **Ajouter une interface**.

- b Entrez un nom.

- c Sélectionnez un type.

Si le mode HA est actif-en veille, les choix sont **Externe, Service** et **Bouclage**. Si le mode HA est actif-actif, les choix sont **Externe** et **Bouclage**.

- d Entrez une adresse IP au format CIDR.

- e Sélectionnez un segment.

- f Si le type d'interface n'est pas **Service**, sélectionnez un nœud NSX Edge.

- g (Facultatif) Si le type d'interface n'est pas **Bouclage**, entrez une valeur de MTU.
 - h (Facultatif) Ajoutez des balises et sélectionnez un profil ND.
- 13** (Facultatif) Si le mode HA est actif-en veille, cliquez sur **Définir** en regard de **Configuration de l'adresse IP virtuelle HA** pour configurer VIP HA.

Lorsque l'adresse IP virtuelle HA est configurée, la passerelle de niveau 0 est opérationnelle même si une liaison montante est inactive. Le routeur physique interagit uniquement avec la VIP HA. L'adresse IP virtuelle HA est conçue pour fonctionner avec le routage statique et non avec BGP.

- a Cliquez sur **Ajouter une adresse IP virtuelle HA**.
 - b Entrez une adresse IP et un masque de sous-réseau.
Le sous-réseau VIP HA doit être le même que le sous-réseau de l'interface à laquelle il est lié.
 - c Sélectionnez deux interfaces de deux nœuds Edge différents.
- 14** Cliquez sur **Routage** pour ajouter des listes de préfixes IP, des listes de communauté, des routes statiques et des cartes de route.
- 15** Cliquez sur **BGP** pour configurer BGP.
- 16** Cliquez sur **Configuration avancée** pour accéder à la page **Mise en réseau et sécurité avancées > Routeurs** afin d'effectuer des configurations supplémentaires.
- a Pour configurer le mode de transfert de couche 3, cliquez sur l'onglet **Configuration globale**.
 - b Cliquez sur **Modifier**.
 - c Sélectionnez **IPv4** ou **IPv4 et IPv6**.
La valeur par défaut est IPv4 uniquement. IPv6 uniquement n'est pas pris en charge. Pour activer IPv6, sélectionnez **IPv4 et IPv6**.
 - d Cliquez sur **Enregistrer**.

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 de routes. 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'une passerelle de niveau 0 configurée. 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Passerelles de niveau 0**.
- 3 Pour modifier une passerelle de niveau 0, cliquez sur l'icône de menu (trois points) et sélectionnez **Modifier**.
- 4 Cliquez sur **Routage**.
- 5 Cliquez sur **Définir** en regard de la **Liste de préfixes IP**.
- 6 Cliquez sur **Ajouter une liste de préfixes IP**.
- 7 Entrez un nom pour la liste de préfixes IP.
- 8 Cliquez sur **Définir** pour ajouter des préfixes IP.
- 9 Cliquez sur **Ajouter un préfixe**.
 - a Entrez une adresse IP au format CIDR.
Par exemple, 192.168.100.3/27.
 - b (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.
 - c Sélectionnez **Refuser** ou **Autoriser** dans le menu déroulant.
 - d Cliquez sur **Ajouter**.
- 10 Recommencez l'étape précédente pour spécifier des préfixes supplémentaires.
- 11 Cliquez sur **Enregistrer**.

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.

Les listes de communauté sont des listes définies par l'utilisateur de valeurs d'attributs de communauté. Ces listes peuvent être utilisées pour faire correspondre ou manipuler l'attribut de communautés dans les messages de mise à jour BGP.

L'attribut de communautés BGP (RFC 1997) et l'attribut de grandes communautés BGP (RFC 8092) sont pris en charge. L'attribut de communautés BGP est une valeur de 32 bits fractionnée en deux valeurs de 16 bits. L'attribut de grandes communautés BGP possède 3 composants, chacun de 4 octets de longueur.

Dans les cartes de route, il est possible de faire correspondre ou de définir l'attribut de communautés ou de grandes communautés BGP. À l'aide de cette fonctionnalité, les opérateurs de réseau peuvent implémenter une stratégie réseau basée sur l'attribut de communautés BGP.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Passerelles de niveau 0**.
- 3 Pour modifier une passerelle de niveau 0, cliquez sur l'icône de menu (trois points) et sélectionnez **Modifier**.
- 4 Cliquez sur **Routage**.
- 5 Cliquez sur **Définir** en regard de **Liste de communauté**.
- 6 Cliquez sur **Ajouter une liste de communauté**.
- 7 Entrez le nom de la liste de communauté.
- 8 Spécifiez une liste de communautés. Pour une communauté normale, utilisez le format aa:nn, par exemple, 300:500. Pour une grande communauté, utilisez le format aa:bb:cc, par exemple, 11:22:33. Notez que la liste ne peut pas contenir à la fois des communautés normales et des grandes communautés. Elle doit contenir uniquement des communautés normales ou uniquement des grandes communautés.

Par ailleurs, vous pouvez sélectionner une ou plusieurs des communautés normales suivantes. Notez que vous ne pouvez pas les ajouter si la liste contient des grandes communautés.
 - 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.
- 9 Cliquez sur **Enregistrer**.

Configurer un itinéraire statique

Vous pouvez configurer une route statique sur la passerelle de niveau 0 vers des réseaux externes. Une fois que vous avez configuré une route statique, il n'est pas nécessaire de l'annoncer du niveau 0 au niveau 1, car les passerelles de niveau 1 disposent automatiquement d'une route statique par défaut vers leur passerelle de niveau 0 connectée.

Les itinéraires statiques récurrents sont pris en charge.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau > Passerelles de niveau 0**.
- 3 Pour modifier une passerelle de niveau 0, cliquez sur l'icône de menu (trois points) et sélectionnez **Modifier**.
- 4 Cliquez sur **Routage**.
- 5 Cliquez sur **Définir** en regard de **Routes statiques**.
- 6 Cliquez sur **Ajouter une route statique**.
- 7 Entrez un nom et une adresse réseau au format CIDR. Les routes statiques basées sur IPv6 sont prises en charge. Les préfixes IPv6 ne peuvent comporter qu'un saut suivant de type IPv6.
- 8 Cliquez sur **Définir les sauts suivants** pour ajouter des informations sur les sauts suivants.
- 9 Cliquez sur **Ajouter un saut suivant**.
- 10 Entrez une adresse IP.
- 11 Spécifiez la distance administrative.
- 12 Sélectionnez une interface dans la liste déroulante.
- 13 Cliquez sur le bouton **Ajouter**.

Étape suivante

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

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 pour la redistribution de routes.

Conditions préalables

- Vérifiez qu'une liste de préfixes IP ou une liste de communauté est configurée. Reportez-vous à la section [Créer une liste de préfixes IP](#) ou [Créer une liste de communauté](#).
- Pour plus d'informations sur l'utilisation d'expressions régulières pour définir les critères de correspondance d'un mappage de route pour les listes de communauté, reportez-vous à la section [Utilisation d'expressions régulières pour faire correspondre les listes de communauté lors de l'ajout de mappages de route](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Passerelles de niveau 0**.
- 3 Pour modifier une passerelle de niveau 0, cliquez sur l'icône de menu (trois points) et sélectionnez **Modifier**.
- 4 Cliquez sur **Routage**.
- 5 Cliquez sur **Définir** en regard de **Cartes de route**.
- 6 Cliquez sur **Ajouter une carte de route**.
- 7 Entrez un nom et cliquez sur **Définir** pour ajouter des critères de correspondance.
- 8 Cliquez sur **Ajouter les critères de correspondance** pour ajouter un ou plusieurs critères de correspondance.

9 Pour chaque critère, sélectionnez **Préfixe IP** ou **Liste de communauté** et cliquez sur **Définir** pour spécifier une ou plusieurs expressions de correspondance.

a Si vous avez sélectionné **Liste de communautés**, spécifiez les expressions de correspondance qui définissent la correspondance des membres des listes de communautés. Pour chaque liste de communautés, les options de correspondance suivantes sont disponibles :

- **FAIRE CORRESPONDRE À N'IMPORTE QUEL** - effectuez l'action de définition dans la carte de route si n'importe quelle communauté de la liste de communauté est mise en correspondance.
- **FAIRE CORRESPONDRE À TOUS LES** - effectuez l'action de définition dans la carte de route si toutes les communautés de la liste de communauté sont mises en correspondance quel que soit l'ordre.
- **FAIRE CORRESPONDRE EXACTEMENT À** - effectuez l'action de définition dans la carte de route si toutes les communautés de la liste de communautés sont mises en correspondance dans le même ordre.
- **FAIRE CORRESPONDRE À LA VALEUR REGEX DE COMMUNAUTÉ** : effectuez l'action de définition dans la carte de route si toutes les communautés régulières associées au NRLI correspondent à l'expression régulière.
- **FAIRE CORRESPONDRE À LA VALEUR REGEX DE GRANDE COMMUNAUTÉ** : effectuez l'action de définition dans la carte de route si toutes les grandes communautés associées au NRLI correspondent à l'expression régulière.

Vous devez utiliser le critère de filtrage `MATCH_COMMUNITY_REGEX` pour faire correspondre les routes aux communautés standard et utiliser le critère de correspondance `MATCH_LARGE_COMMUNITY_REGEX` pour faire correspondre les routes aux grandes communautés. Si vous souhaitez autoriser des routes contenant soit la valeur de communauté standard, soit la valeur de grande communauté, vous devez créer deux critères de correspondance. Si les expressions de correspondance sont présentées dans le même critère de correspondance, seules les routes contenant à la fois les communautés standard et les grandes communautés seront autorisées.

Pour tous les critères de correspondance, les expressions de correspondance sont appliquées dans une opération AND, ce qui signifie que toutes les expressions de correspondance doivent être satisfaites pour qu'une correspondance se produise. S'il existe plusieurs critères de correspondance, ils sont appliqués dans une opération OR, ce qui signifie qu'une correspondance se produit si un critère de correspondance est satisfait.

10 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 liste de communautés. Pour une communauté normale, utilisez le format aa:nn, par exemple, 300:500. Pour une grande communauté, utilisez le format aa:bb:cc, par exemple, 11:22:33. 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.
Préférence locale	Utilisez cette valeur pour choisir le chemin d'accès BGP externe sortant. Le chemin d'accès ayant la valeur la plus élevée est privilégié.

11 Dans la colonne Action, sélectionnez **Autoriser** ou **Refuser**.

Vous pouvez autoriser ou refuser l'annonce des adresses IP filtrées par les listes de préfixes IP ou les listes de communauté.

12 Cliquez sur **Enregistrer**.

Utilisation d'expressions régulières pour faire correspondre les listes de communauté lors de l'ajout de mappages de route

Vous pouvez utiliser des expressions régulières pour définir les critères de correspondance de mappage de route pour les listes de communauté. Les expressions régulières BGP sont basées sur les expressions régulières POSIX 1003.2.

Les expressions suivantes sont un sous-ensemble des expressions régulières POSIX.

Expression	Description
.	Correspond à n'importe quel caractère unique.
*	Correspond à 0 ou plusieurs occurrences du modèle.
+	Correspond à 1 ou plusieurs occurrences du modèle.
?	Correspond à 0 ou 1 occurrence du modèle.
^	Correspond au début de la ligne.

Expression	Description
\$	Correspond à la fin de la ligne.
–	Ce caractère a des significations spéciales dans les expressions régulières BGP. Il correspond à un espace, une virgule, des délimiteurs d'ensemble AS { and } et des délimiteurs de confédération AS (and). Il correspond également au début de la ligne et à la fin de la ligne. Par conséquent, ce caractère peut être utilisé pour une correspondance de limites de valeurs AS. Ce caractère est techniquement évalué à (^ [,{}])!\$).

Voici quelques exemples d'utilisation d'expressions régulières dans les mappages de route :

Expression	Description
^101	Fait correspondre les routes dont l'attribut de communauté commence par 101.
^[0-9]+	Fait correspondre les routes dont l'attribut de communauté commence par un nombre compris entre 0 et 9 et comporte une ou plusieurs instances d'un tel nombre.
.*	Correspond à des routes ayant un attribut de communauté Quelconque ou Non.
.*+	Correspond aux routes ayant une valeur de communauté Quelconque.
^\$	Correspond aux routes ayant une valeur de communauté non/nulle.

Configurer BGP

Pour activer l'accès entre vos VM et le monde extérieur, vous pouvez configurer une connexion BGP externe ou interne (eBGP ou iBGP) entre une passerelle 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 la passerelle de niveau 0. Vous devez également configurer le nombre AS distant. Les voisins EBGP doivent être connectés directement et se trouver dans le même sous-réseau que la liaison montante de niveau 0. S'ils ne se trouvent pas dans le même sous-réseau, une traversée de tronçons multiples BGP doit être utilisée.

BGPv6 est pris en charge pour les tronçons uniques et multiples. Un voisin BGPv6 prend uniquement en charge les adresses IPv6. La redistribution, la liste de préfixes et les cartes de route sont pris en charge avec des préfixes IPv6.

Une passerelle de niveau 0 en mode actif-actif prend en charge iBGP inter-SR (routeur de service). Si la passerelle 1 ne parvient pas à communiquer avec un routeur physique ascendant, le trafic est réacheminé vers la passerelle 2 dans le cluster actif-actif. Si la passerelle 2 est capable de communiquer avec le routeur physique, le trafic entre la passerelle 1 et le routeur physique n'est pas affecté.

L'implémentation d'ECMP sur NSX Edge est basée sur les 5 tuples du numéro de protocole, des adresses source et de destination, ainsi que des ports source et de destination.

La fonctionnalité iBGP présente les capacités et restrictions suivantes :

- La redistribution, les listes de préfixes et les cartes d'itinéraire sont prises en charge.
- Les réflecteurs d'itinéraire ne sont pas pris en charge.

- La confédération BGP n'est pas prise en charge.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Passerelles de niveau 0**.
- 3 Pour modifier une passerelle de niveau 0, cliquez sur l'icône de menu (trois points) et sélectionnez **Modifier**.
- 4 Cliquez sur **BGP**.
 - a Entrez le nombre AS local.

En mode actif-actif, la valeur ASN par défaut, 65 000, est déjà renseignée. En mode actif-veille, il n'existe pas de valeur ASN par défaut.
 - b Cliquez sur le bouton bascule **BGP** pour activer ou désactiver BGP.

En mode actif-actif, **BGP** est activé par défaut. En mode actif-veille, **BGP** est désactivé par défaut.
 - c Si cette passerelle est en mode actif-actif, cliquez sur le bouton bascule **iBGP Inter SR** pour activer ou désactiver iBGP inter-SR. iBGP inter-SR est activé par défaut.

Si la passerelle est en mode actif-veille, cette fonctionnalité n'est pas disponible.
 - d Cliquez sur le bouton bascule **ECMP** pour activer ou désactiver ECMP.

- e Cliquez sur le bouton bascule **Alléger les chemins multiples** pour activer ou désactiver le partage de charge sur plusieurs chemins qui diffèrent uniquement par les valeurs d'attribut de chemin AS, mais qui ont la même longueur de chemin AS.

Note ECMP doit être activé pour que **Alléger les chemins multiples** fonctionne.

- f Dans le champ **Redémarrage normal**, sélectionnez **Désactiver**, **Assistance uniquement** ou **Redémarrage normal et assistance**.

Vous pouvez éventuellement modifier les options **Temporisateur de redémarrage normal** et **Temporisateur caduc de redémarrage normal**.

Par défaut, le mode Redémarrage normal est défini sur **Assistance uniquement**. Le mode Assistance est utile pour éliminer et/ou réduire l'interruption du trafic associé aux routes apprises par un voisin capable de redémarrer normalement. Le voisin doit pouvoir conserver sa table de transfert lorsqu'il est en cours de redémarrage.

Il n'est pas recommandé d'activer la fonctionnalité de redémarrage normal sur les passerelles de niveau 0, car les homologations BGP de toutes les passerelles sont toujours actives. Lors d'un basculement, la capacité de redémarrage normal augmente la durée nécessaire à un voisin distant pour sélectionner une autre passerelle de niveau 0. Cela retardera la convergence basée sur BFD.

Remarque : sauf si la configuration spécifique au voisin est remplacée, la configuration de niveau 0 s'applique à tous les voisins BGP.

- 5 Configurez **Agrégation de route** en ajoutant des préfixes d'adresses IP.

- a Cliquez sur **Ajouter un préfixe**.
- b Entrez un préfixe d'adresse IP au format CIDR.
- c Pour l'option **Résumé uniquement**, sélectionnez **Oui** ou **Non**.

- 6 Cliquez sur **Enregistrer**.

Vous devez enregistrer la configuration globale de BGP avant de pouvoir configurer les voisins BGP.

- 7 Configurez **Voisins BGP**.

- a Entrez l'adresse IP du voisin.
- b Activez ou désactivez **BFD**.
- c Entrez une valeur pour **Nombre d'AS distants**.

Pour iBGP, entrez le même nombre AS que celui de l'étape 4a. Pour eBGP, entrez le nombre AS du routeur physique.

- d Configurez **Filtre sortant**.
- e Configurez **Filtre entrant**.

- f Activez ou désactivez la fonctionnalité **Allowas-in**.

Elle est désactivée par défaut. Avec cette fonctionnalité activée, les voisins BGP peuvent recevoir des routes avec le même AS, par exemple, lorsque vous avez deux emplacements interconnectés à l'aide du même fournisseur de services. Cette fonctionnalité s'applique à toutes les familles d'adresses et ne peut pas être appliquée à des familles d'adresses spécifiques.

- g Dans le champ **Adresses source**, vous pouvez sélectionner une adresse source pour établir une session d'homologation avec un voisin à l'aide de cette adresse source spécifique. Si vous n'en sélectionnez aucune, la passerelle en choisira une automatiquement.
- h Dans le champ **Famille d'adresses IP**, sélectionnez **IPv4**, **IPv6** ou **Désactivé**.
- i Entrez une valeur pour **Limite de tronçon maximale**.
- j Dans le champ **Redémarrage normal**, vous pouvez sélectionner **Désactiver**, **Assistance uniquement** ou **Redémarrage normal et assistance**.

Option	Description
Aucune sélection	Le redémarrage normal de ce voisin suivra la configuration BGP de la passerelle de niveau 0.
Désactiver	<ul style="list-style-type: none"> ■ Si BGP de passerelle de niveau 0 est configuré avec Désactiver, le redémarrage normal sera désactivé pour ce voisin. ■ Si BGP de passerelle de niveau 0 est configuré avec Assistance uniquement, le redémarrage normal sera désactivé pour ce voisin. ■ Si BGP de passerelle de niveau 0 est configuré avec Redémarrage normal et assistance, le redémarrage normal sera désactivé pour ce voisin.
Assistance uniquement	<ul style="list-style-type: none"> ■ Si BGP de passerelle de niveau 0 est configuré avec Désactiver, le redémarrage normal sera configuré comme Assistance uniquement pour ce voisin. ■ Si BGP de passerelle de niveau 0 est configuré avec Assistance uniquement, le redémarrage normal sera configuré comme Assistance uniquement pour ce voisin. ■ Si BGP de passerelle de niveau 0 est configuré avec Redémarrage normal et assistance, le redémarrage normal sera configuré comme Assistance uniquement pour ce voisin.
Redémarrage normal et assistance	<ul style="list-style-type: none"> ■ Si BGP de passerelle de niveau 0 est configuré avec Désactiver, le redémarrage normal sera configuré comme Redémarrage normal et assistance pour ce voisin. ■ Si BGP de passerelle de niveau 0 est configuré avec Assistance uniquement, le redémarrage normal sera configuré comme Redémarrage normal et assistance pour ce voisin. ■ Si BGP de passerelle de niveau 0 est configuré avec Redémarrage normal et assistance, le redémarrage normal sera configuré comme Redémarrage normal et assistance pour ce voisin.

- k Cliquez sur **Temporisateurs et mot de passe**.

- l Entrez une valeur pour **Intervalle BFD**.

L'unité est en millisecondes. Pour un nœud Edge en cours d'exécution dans une machine virtuelle, la valeur minimale est de 1 000. Pour un nœud Edge Bare Metal, la valeur minimale est de 300.

- m Entrez une valeur pour **Multiplicateur BFD**.
- n Entrez une valeur pour **Durée de retenue**.
- o Entrez une valeur pour **Durée de survie**.
- p Entrez un mot de passe.

Ceci est nécessaire si vous configurez l'authentification MD5 entre des homologues BGP.

- 8 Cliquez sur **Enregistrer**.

Configurer BFD

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

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau > Passerelles de niveau 0**.
- 3 Pour modifier une passerelle de niveau 0, cliquez sur l'icône de menu (trois points) et sélectionnez **Modifier**.
- 4 Cliquez sur **Configuration avancée**.

Vous accédez ainsi à la page **Mise en réseau et sécurité avancées > Routeurs**. La passerelle s'affichera comme l'un des routeurs logiques. Suivez les instructions de la section [Configurer BFD sur un routeur logique de niveau 0](#).

Configurer le transfert de couche 3 IPv6

Le transfert de couche 3 IPv4 est activé par défaut. Vous pouvez également configurer le transfert de couche 3 IPv6.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau > Passerelles de niveau 0**.
- 3 Modifiez une passerelle de niveau 0 en cliquant sur l'icône de menu (trois points) et sélectionnez **Modifier**.

4 Cliquez sur **Configuration avancée**.

Vous accédez ainsi à la page **Mise en réseau et sécurité avancées > Routeurs**. La passerelle s'affichera comme l'un des routeurs logiques.

5 Cliquez sur l'onglet **Configuration globale**.

6 Dans le champ **Mode de transfert L3**, sélectionnez **IPv4 et IPv6**.

IPv6 uniquement n'est pas pris en charge.

7 Modifiez de nouveau la passerelle en accédant à l'onglet **Mise en réseau**.

8 Accédez à **Paramètres supplémentaires**.

a Il n'existe aucune adresse IPv6 configurable pour **Sous-réseau de transit interne**. Le système utilise automatiquement les adresses locales de liaison IPv6.

b Entrez un sous-réseau IPv6 pour **Sous-réseaux de transit T0-T1**.

9 Accédez à **Interfaces** et ajoutez une interface pour IPv6.

Créer des profils SLAAC et DAD pour l'attribution d'adresses IPv6

Lorsque vous utilisez IPv6 sur une interface de routeur logique, vous pouvez configurer la configuration automatique d'adresse sans état (SLAAC) pour l'attribution d'adresses IP. SLAAC active l'adressage d'un hôte, en fonction d'un préfixe réseau annoncé à partir d'un routeur réseau local, via les annonces du routeur. La détection d'adresse en double (DAD) garantit l'unicité des adresses IP.

Conditions préalables

Accédez à **Mise en réseau et sécurité avancées > Routeurs > Configuration globale** et sélectionnez **IPv4 et IPv6** comme **Mode de transfert L3**

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Passerelles de niveau 0**.
- 3 Pour modifier une passerelle de niveau 0, cliquez sur l'icône de menu (trois points) et sélectionnez **Modifier**.
- 4 Cliquez sur **Paramètres supplémentaires**.

- 5 Pour créer un **profil ND** (profil SLAAC), cliquez sur l'icône du menu (trois points) et sélectionnez **Créer un**.
 - a Entrez le nom du profil.
 - b Sélectionnez un mode :
 - **Désactivé** : les messages d'annonce du routeur sont désactivés.
 - **SLAAC avec DNS via RA** : l'adresse et les informations DNS sont générées avec le message d'annonce du routeur.
 - **SLAAC avec DNS via DHCP** : l'adresse est générée avec le message d'annonce du routeur et les informations DNS sont générées par le serveur DHCP.
 - **DHCP avec adresse et DNS via DHCP** : l'adresse et les informations DNS sont générées par le serveur DHCP.
 - **SLAAC avec adresse et DNS via DHCP** : l'adresse et les informations DNS sont générées par le serveur DHCP. Cette option est uniquement prise en charge par NSX Edge et non par les hôtes KVM ou ESXi.
 - c Entrez l'heure d'accessibilité et l'intervalle de retransmission pour le message d'annonce du routeur.
 - d Entrez le nom du domaine et spécifiez une durée de vie pour celui-ci. Entrez ces valeurs uniquement pour le mode **SLAAC avec DNS via RA**.
 - e Entrez un serveur DNS et spécifiez une durée de vie pour celui-ci. Entrez ces valeurs uniquement pour le mode **SLAAC avec DNS via RA**.
 - f Entrez les valeurs pour l'annonce du routeur :
 - **Intervalle RA** : intervalle de temps entre la transmission des messages d'annonce du routeur consécutifs.
 - **Limite de tronçon** : durée de vie des routes annoncées.
 - **Durée de vie du routeur** : durée de vie du routeur.
 - **Durée de vie du préfixe** : durée de vie du préfixe en secondes.
 - **Délai de préfixe préféré** : heure à laquelle une adresse valide est préférée.
- 6 Pour créer un **profil DAD**, cliquez sur l'icône du menu (trois points) et sélectionnez **Créer un**.
 - a Entrez le nom du profil.
 - b Sélectionnez un mode :
 - **Libre** : une notification d'adresse en double est reçue, mais aucune action n'est effectuée lorsqu'une adresse en double est détectée.
 - **Strict** : une notification d'adresse en double est reçue et l'adresse en double n'est plus utilisée.

- c Entrez le **temps d'attente (en secondes)** qui spécifie l'intervalle de temps entre les paquets NS.
- d Entrez le **nombre de nouvelles tentatives de NS** qui spécifie le nombre de paquets NS pour détecter les adresses en double à des intervalles définis dans le champ **Temps d'attente (en secondes)**

Passerelle de niveau 1

3

Une passerelle de niveau 1 exécute les fonctions d'un routeur logique de niveau 1. Il dispose de connexions à liaison descendante pour les segments et de connexions à liaison montante pour les passerelles de niveau 0.

Note Dans l'onglet **Mise en réseau avancée et sécurité**, le routeur logique de terme de niveau 1 est utilisé pour faire référence à une passerelle de niveau 1.

Vous pouvez configurer des annonces de routes et des routes statiques sur une passerelle de niveau 1. Les itinéraires statiques récurrents sont pris en charge.

Ce chapitre contient les rubriques suivantes :

- [Ajouter une passerelle de niveau 1](#)

Ajouter une passerelle de niveau 1

Une passerelle de niveau 1 est généralement connectée à une passerelle de niveau 0 dans le sens ascendant et à des segments dans le sens descendant.

Les passerelles de niveau 0 et de niveau 1 prennent en charge les configurations d'adressage suivantes pour toutes les interfaces (liaisons montantes, ports de service et liaisons descendantes) dans les topologies à un seul niveau et à plusieurs niveaux :

- IPv4 uniquement
- IPv6 uniquement
- Double pile : IPv4 et IPv6

Pour utiliser l'adressage IPv6 ou double pile, activez **IPv4 et IPv6** en tant que mode de transfert L3 dans **Mise en réseau > Paramètres de mise en réseau > Configuration de mise en réseau globale** .

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Passerelles de niveau 1**.
- 3 Cliquez sur **Ajouter la passerelle de niveau 1**.

- 4 Entrez un nom pour la passerelle.
- 5 (Facultatif) Sélectionnez une passerelle de niveau 0 pour vous connecter à cette passerelle de niveau 1 afin de créer une topologie à plusieurs niveaux.
- 6 Sélectionnez un mode de basculement.

Option	Description
Préemptif	Si le nœud NSX Edge préféré échoue, puis se rétablit, il prévaut sur son homologue et devient le nœud actif. L'homologue modifie son état sur veille.
Non préemptif	Si le nœud NSX Edge préféré échoue, puis se rétablit, 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. Il s'agit de l'option par défaut.

- 7 (Facultatif) Sélectionnez un cluster NSX Edge si vous voulez que cette passerelle de niveau 1 héberge des services avec état (NAT, équilibreur de charge, pare-feu).

Si un cluster NSX Edge est sélectionné, un routeur de service est toujours créé (même si vous ne configurez pas les services avec état), ce qui affecte le modèle de trafic Vertical.

- 8 (Facultatif) Sélectionnez un nœud NSX Edge.
- 9 (Facultatif) Cliquez sur le bouton bascule **Activer le déplacement en veille** pour activer ou désactiver le déplacement en veille.

Le déplacement en veille signifie que si le nœud Edge sur lequel le routeur logique actif ou en veille est en cours d'exécution échoue, un nouveau routeur logique en veille est créé sur un autre nœud Edge pour maintenir la haute disponibilité. Si le nœud Edge qui échoue exécute le routeur logique actif, le routeur logique de secours initial devient le routeur logique actif et un nouveau routeur logique en veille est créé. Si le nœud Edge qui a échoué exécute le routeur logique en veille, le nouveau routeur logique en veille le remplace.

- 10 Cliquez sur **Enregistrer**.
- 11 (Facultatif) Cliquez sur **Annonce de route**.

Sélectionnez une ou plusieurs des options suivantes :

- Toutes les routes statiques
- Toutes les adresses IP NAT
- Toutes les routes du redirecteur DNS
- Toutes les routes d'équilibreur de charge VIP
- Tous les segments et ports de service connectés
- Toutes les routes IP d'équilibreur de charge SNAT
- Tous les points de terminaison locaux IPSec

Dans le champ **Définir des règles d'annonce de route**, cliquez sur **Définir** pour ajouter des règles d'annonce de route.

- 12 (Facultatif) Cliquez sur **Interfaces de service** et **Définir** pour configurer les connexions à des segments. Requis dans certaines topologies, telles que les segments supportés par VLAN ou l'équilibrage de charge à un bras.
- a Cliquez sur **Ajouter une interface**.
 - b Entrez un nom et une adresse IP au format CIDR.
 - c Sélectionnez un segment.
 - d Dans le champ **MTU**, entrez une valeur entre 64 et 9 000.
 - e Dans le champ **Profil ND**, sélectionnez un profil.
 - f Cliquez sur **Enregistrer**.
- 13 (Facultatif) Cliquez sur **Routes statiques** et **Définir** pour configurer des routes statiques.
- a Cliquez sur **Ajouter une route statique**.
 - b Entrez un nom et une adresse réseau au format CIDR ou CIDR IPv6.
 - c Cliquez sur **Définir les tronçons suivants** pour ajouter des informations sur les tronçons suivants.
 - d Cliquez sur **Enregistrer**.

Segments

4

Un segment exécute les fonctions d'un commutateur logique.

Note Dans l'onglet **Mise en réseau avancée et sécurité**, le commutateur logique de terme est utilisé pour faire référence à un segment.

Ce chapitre contient les rubriques suivantes :

- [Profils de segments](#)
- [Ajouter un segment](#)

Profils de segments

Les profils de segments incluent des détails de configuration de mise en réseau de couche 2 pour les segments et les ports de segments. NSX Manager prend en charge plusieurs types de profils de segments.

Les types de segments de profils suivants sont disponibles :

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

Note Vous ne pouvez pas modifier ni supprimer les profils de segments par défaut. Si vous avez besoin de paramètres supplémentaires dans le profil de segment par défaut, vous pouvez créer un profil de segment personnalisé. Par défaut, tous les profils de segments personnalisés, à l'exception du profil de sécurité du segment, héritent des paramètres du profil de segment par défaut approprié. Par exemple, un profil de segment de détection IP personnalisé par défaut aura les mêmes paramètres que le profil de segment de détection IP par défaut.

Chaque profil de segment par défaut ou personnalisé dispose d'un identifiant unique. Cet identifiant est utilisé pour associer le profil de segment à un segment ou à un port de segment.

Un segment ou un port de segment ne peut être associé qu'à un seul profil de segment de chaque type. Par exemple, vous ne pouvez pas avoir deux profils de segment QoS associés à un segment ou à un port de segment.

Si vous n'associez pas un profil de segment lorsque vous créez un segment, NSX Manager associe un profil de segment par défaut correspondant défini par le système. Les ports de segment enfants héritent du segment parent le profil de segment par défaut défini par le système.

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

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

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

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

Comprendre le profil de segment 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 segment 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 segment. Dans chaque cas, la valeur DSCP est propagée vers l'en-tête IP externe des 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 segment 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 segment et sont hérités par le port de segment enfant.

Créer un profil de segment QoS

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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau > Segments > Profils de segments**.
- 3 Cliquez sur **Ajouter un profil de segment** et sélectionnez **QoS**.

4 Renseignez les détails du profil de commutation QoS.

Option	Description
Nom	Nom du profil.
Mode	<p>Sélectionnez l'option Approuvé ou Non approuvé dans le menu déroulant Mode.</p> <p>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 taille de rafale est basée sur la durée avec la bande passante maximale. Vous définissez la durée de rafale dans le paramètre de taille de rafale. Vous ne pouvez pas garantir la bande passante. Toutefois, vous pouvez utiliser les paramètres Moyenne, Maximale et Taille de rafale pour limiter la bande passante réseau.</p> <p>Par exemple, si la bande passante moyenne est de 30 Mbit/s, la bande passante maximale de 60 Mbit/s et la durée autorisée de 0,1 seconde, alors la taille de rafale est de $60 * 1\,000\,000 * 0,10/8 = 750\,000$ octets.</p> <p>La valeur par défaut de 0 désactive la limitation du taux sur le trafic d'entrée.</p>

Option	Description
Diffusion d'entrée	<p>Définissez des valeurs personnalisées pour le trafic réseau sortant de la VM vers le réseau logique en fonction de la diffusion.</p> <p>Par exemple, lorsque vous définissez la bande passante moyenne pour un commutateur logique sur 3 000 Kbit/s, que la bande passante maximale est de 6 000 Kbit/s et la durée autorisée de 0,1 seconde, alors la taille de rafale est de $6\,000 * 1\,000 * 0,10/8 = 75\,000$ octets.</p> <p>La valeur par défaut de 0 désactive la limitation du taux sur le trafic de diffusion d'entrée.</p>
Sortie	<p>Définissez des valeurs personnalisées pour le trafic réseau entrant du réseau logique vers la VM.</p> <p>La valeur par défaut de 0 désactive la limitation du taux sur le trafic de sortie.</p>

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

5 Cliquez sur **Enregistrer**.

Comprendre le profil de segment de découverte d'adresses IP

La découverte d'adresses IP utilise l'écoute DHCP et DHCPv6, l'écoute ARP (Address Resolution Protocol), l'écoute ND (Neighbor-Discovery) et VM Tools pour découvrir les adresses MAC et IP.

Note Les méthodes de détection d'adresses IP pour IPv6 sont désactivées dans le profil de segment de détection d'IP par défaut. Pour activer la détection d'adresses IP pour IPv6 pour des segments, vous devez créer un profil de détection d'adresses IP avec les options IPv6 activées et associer le profil aux segments. En outre, assurez-vous que le pare-feu distribué autorise les paquets de détection de voisin IPv6 entre toutes les charges de travail (autorisé par défaut).

Les adresses MAC et IP découvertes sont utilisées pour obtenir la suppression ARP/ND, ce qui réduit le trafic entre les machines virtuelles connectées à un même segment. Les adresses sont également utilisées par SpoofGuard et les composants du pare-feu distribué (DFW). DFW utilise les liaisons d'adresse pour déterminer l'adresse IP des objets dans les règles de pare-feu.

L'écoute DHCP/DHCPv6 inspecte les paquets DHCP/DHCPv6 échangés entre le client et le serveur DHCP/DHCPv6 pour apprendre les adresses IP et MAC.

L'écoute ARP inspecte les paquets ARP et GARP (ARP gratuits) sortants d'une 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 MAC et IP ou IPv6. Cette méthode de découverte d'adresses IP est disponible pour les machines virtuelles en cours d'exécution sur les hôtes ESXi uniquement.

L'écoute ND est l'équivalent IPv6 de l'écoute ARP. Elle inspecte les messages Neighbor Solicitation (NS) et Neighbor Advertisement (NA) pour découvrir les adresses IP et MAC.

La détection d'adresses en double vérifie si une adresse IP qui vient d'être découverte est déjà présente dans la liste de liaison réalisée pour un port différent. Cette vérification est effectuée pour les ports se trouvant sur le même segment. Si une adresse en double est détectée, l'adresse qui vient d'être découverte est ajoutée à la liste découverte, mais n'est pas ajoutée à la liste de liaison réalisée. Toutes les adresses IP en double ont un horodatage de découverte associé. Si l'adresse IP qui se trouve sur la liste des liaisons réalisées est supprimée, soit en l'ajoutant à la liste Ignorer la liaison, soit en désactivant l'écoute, l'adresse IP en double avec l'horodatage le plus ancien est déplacée vers la liste des liaisons réalisées. Les informations d'adresse en double sont disponibles via un appel d'API.

Par défaut, les méthodes de découverte par écoute ARP et écoute ND fonctionnent dans un mode appelé TOFU (Trust On First Use). En mode TOFU, lorsqu'une adresse est découverte et ajoutée à la liste de liaison réalisée, cette liaison reste indéfiniment dans la liste réalisée. TOFU s'applique aux « n » premières liaisons uniques <IP, MAC, VLAN> découvertes à l'aide de l'écoute ARP/ND, où « n » représente la limite de liaison que vous pouvez configurer. Vous pouvez désactiver le mode TOFU pour l'écoute ARP/ND. Les méthodes fonctionneront ensuite en mode TOEU (Trust On Every Use). En mode TOEU, lorsqu'une adresse est découverte, elle est ajoutée à la liste de liaison réalisée et lorsqu'elle est supprimée ou expirée, elle est supprimée de cette liste. L'écoute DHCP et VMTools fonctionnent toujours dans le mode TOEU.

Note TOFU n'est pas identique à SpoofGuard et ne bloque pas le trafic de la même manière que SpoofGuard. Pour plus d'informations, reportez-vous à la section [Comprendre le profil de segment SpoofGuard](#).

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>.

Pour chaque port, NSX Manager conserve une liste Ignorer les liaisons, qui contient les adresses IP qui ne peuvent pas être liées au port. En accédant à **Mise à niveau avancée et sécurité > Commutation > Ports** et en sélectionnant un port, vous pouvez ajouter des liaisons découvertes à la liste des liaisons ignorées. Vous pouvez également supprimer une liaison existante découverte ou réalisée en la copiant vers **Ignorer les liaisons**.

Créer un profil de segment pour la découverte d'adresses IP

NSX-T Data Center dispose de plusieurs profils de commutation de découverte d'adresses IP par défaut. Vous pouvez également en créer de nouveaux.

Conditions préalables

Familiarisez-vous avec les concepts 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://<nsx-manager-ip-address>>.

- 2 Sélectionnez **Mise en réseau > Segments > Profils de segments**.
- 3 Cliquez sur **Ajouter un profil de segment** et sélectionnez **Découverte d'adresses IP**.
- 4 Indiquez les détails du profil de commutation de découverte d'adresses IP.

Option	Description
Nom	Entrez un nom.
Écoute ARP	Pour un environnement IPv4. Applicable si les machines virtuelles ont des adresses IP statiques.
Limite de liaison ARP	Nombre maximal d'adresses IP IPv4 pouvant être liées à un port. La valeur minimale autorisée est 1 (valeur par défaut) et la valeur maximale est 256.
Délai d'expiration de limite de liaison ARP ND	Valeur du délai d'expiration, en minutes, des adresses IP dans la table de liaison ARP/ND si TOFU est désactivé. Si une adresse arrive à expiration, une adresse qui vient d'être découverte la remplace.
Écoute DHCP	Pour un environnement IPv4. Applicable si les machines virtuelles ont des adresses IPv4.
Écoute DHCP V6	Pour un environnement IPv6. Applicable si les machines virtuelles ont des adresses IPv6.
VM Tools	Disponible pour les machines virtuelles hébergées par ESXi uniquement.
VM Tools pour IPv6	Disponible pour les machines virtuelles hébergées par ESXi uniquement.
Écoute dans le cadre de la découverte de voisin	Pour un environnement IPv6. Applicable si les machines virtuelles ont des adresses IP statiques.
Limite de liaison pour la découverte de voisin	Nombre maximal d'adresses IPv6 pouvant être liées à un port.
Approuver à la première utilisation	Applicable à l'écoute ARP et ND.
Détection d'adresses IP en double	Pour toutes les méthodes d'écoute, et les environnements IPv4 et IPv6.

- 5 Cliquez sur **Enregistrer**.

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

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

Créer un profil de segment 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/segment 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Segments > Profils de segments**.
- 3 Cliquez sur **Ajouter un profil de segment** et sélectionnez **SpoofGuard**.
- 4 Entrez un nom.
- 5 Pour activer SpoofGuard de niveau port, définissez **Liaisons de port** sur **Activé**.
- 6 Cliquez sur **Enregistrer**.

Comprendre le profil de segmentation de sécurité de segment

La sécurité du segment offre une sécurité de couche 2 et de couche 3 sans état en vérifiant le trafic d'entrée vers le segment 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 du segment pour protéger l'intégrité du segment en éliminant les attaques malveillantes sur les VM du réseau.

Notez que le profil de sécurité de segment par défaut dispose des paramètres `DHCP Server Block` et `Server Block - IPv6` activés. Cela signifie qu'un segment qui utilise le profil de sécurité de segment par défaut bloque le trafic d'un serveur DHCP vers un client DHCP. Si vous souhaitez qu'un segment autorise le trafic du serveur DHCP, vous devez créer un profil de sécurité de segment personnalisé pour le segment.

Créer un profil de segment de sécurité de segment

Vous pouvez créer un profil de segment de sécurité de segment 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 segment de sécurité de segment. 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Segments > Profils de segments**.
- 3 Cliquez sur **Ajouter un profil de segment** et sélectionnez **Sécurité du segment**.

4 Renseignez les détails du profil de sécurité de segment.

Option	Description
Nom	Nom du profil.
Filtre BPDU	<p>Basculez le bouton Filtre BPDU pour activer le filtrage BPDU. Désactivé par défaut.</p> <p>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.</p>
Liste d'autorisation de filtre BPDU	<p>Cliquez sur l'adresse MAC de destination dans la liste d'adresses MAC de destination du BPDU pour autoriser le trafic vers la destination autorisée. Vous devez activer Filtre BPDU pour pouvoir le sélectionner dans cette liste.</p>
Filtre DHCP	<p>Basculez les boutons Bloc de serveur et Bloc de client pour activer le filtrage DHCP. Les deux valeurs sont désactivées par défaut.</p> <p>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.</p> <p>Bloc de client DHCP empêche une VM d'acquérir une adresse IP DHCP en bloquant les demandes DHCP.</p>
Filtre DHCPv6	<p>Basculez les boutons Bloc de serveur - IPv6 et Bloc de client - IPv6 pour activer le filtrage DHCP. Les deux valeurs sont désactivées par défaut.</p> <p>Le blocage de serveur DHCPv6 bloque le trafic allant d'un serveur DHCPv6 vers un client DHCPv6. Notez qu'il ne bloque pas le trafic allant d'un serveur DHCP vers un agent du relais DHCP. Les paquets dont le numéro de port source UDP est 547 sont filtrés.</p> <p>Le blocage de client DHCPv6 empêche une machine virtuelle d'acquérir une adresse IP DHCP en bloquant les demandes DHCP. Les paquets dont le numéro de port source UDP est 546 sont filtrés.</p>
Bloquer le trafic non-IP	<p>Basculez le bouton Bloquer le trafic non-IP pour autoriser uniquement le trafic IPv4, IPv6, ARP et BPDU.</p> <p>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.</p> <p>Par défaut, cette option est désactivée pour autoriser la gestion du trafic non-IP comme trafic normal.</p>
Protection contre les annonces du routeur	<p>Basculez le bouton Protection contre les annonces du routeur pour filtrer les annonces du routeur IPv6 en entrée. Les paquets ICMPv6 de type 134 sont filtrés. Cette option est activée par défaut.</p>
Limites de débit	<p>Définissez une limite de débit pour le trafic de diffusion et de multidiffusion. Cette option est activée par défaut.</p> <p>Des limites de débit peuvent être utilisées pour protéger le commutateur logique ou les machines virtuelles d'événements, tels que les tempêtes de diffusion.</p> <p>Pour éviter tout problème de connectivité, la valeur minimale du débit maximal doit être ≥ 10 pps.</p>

5 Cliquez sur **Enregistrer**.

Comprendre le profil de segment de découverte d'adresses MAC

Le profil de segment de gestion MAC prend en charge deux fonctionnalités : l'apprentissage MAC et le 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 machine virtuelle ESXi se connecte à un port de segment, 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 période n'est pas configurable. Le champ **Durée de vieillissement d'apprentissage MAC** affiche la valeur prédéfinie, qui est 600.

L'apprentissage MAC prend également en charge la propagation monodiffusion inconnue. Normalement, lorsqu'un paquet reçu par un port présente une adresse MAC de destination inconnue, il est abandonné. Lorsque la propagation monodiffusion inconnue est activée, le port propage le trafic de monodiffusion inconnue à chaque port du commutateur sur lequel l'apprentissage MAC et la propagation monodiffusion inconnue sont activés. Cette propriété est activée par défaut, mais uniquement si l'apprentissage MAC est activé.

Le nombre d'adresses MAC pouvant être apprises est configurable. La valeur maximale est 4 096, qui est la valeur par défaut. Vous pouvez également définir la stratégie pour le moment auquel la limite est atteinte. Les options sont les suivantes :

- **Annuler** : les paquets provenant d'une adresse MAC source inconnue sont annulés. Les paquets entrants sur cette adresse MAC seront traités comme des monodiffusions inconnues. Le port recevra les paquets uniquement si la propagation monodiffusion inconnue est activée.
- **Autoriser** : les paquets provenant d'une adresse MAC source inconnue sont transférés bien que l'adresse ne soit pas apprise. Les paquets entrants sur cette adresse MAC seront traités comme des monodiffusions inconnues. Le port recevra les paquets uniquement si la propagation monodiffusion inconnue est activée.

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

Créer un profil de segment de détection MAC

Vous pouvez créer un profil de segment de détection MAC pour gérer les adresses MAC.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Segments > Profils de segments**.
- 3 Cliquez sur **Ajouter un profil de segment** et sélectionnez **Détection d'adresses MAC**.
- 4 Renseignez les détails du profil de détection d'adresses MAC.

Option	Description
Nom	Nom du profil.
Modification de MAC	Activez ou désactivez la fonctionnalité de changement d'adresse MAC. La valeur par défaut est Désactivé.
Apprentissage MAC	Activez ou désactivez la fonctionnalité d'apprentissage MAC. La valeur par défaut est Désactivé.
Stratégie de limite MAC	Sélectionnez Autoriser ou Annuler . La valeur par défaut est Autoriser . Cette option est disponible si vous activez l'apprentissage MAC
Propagation monodiffusion inconnue	Activez ou désactivez la fonctionnalité de propagation monodiffusion inconnue. La valeur par défaut est Activé. Cette option est disponible si vous activez l'apprentissage MAC
Limite MAC	Définissez le nombre maximal d'adresses MAC. La valeur par défaut est 4 096. Cette option est disponible si vous activez l'apprentissage MAC
Durée de vieillissement d'apprentissage MAC	Uniquement pour informations. Cette valeur n'est pas configurable. La valeur prédéfinie est 600.

- 5 Cliquez sur **Enregistrer**.

Ajouter un segment

Un segment se connecte à des passerelles et à des machines virtuelles. Un segment exécute les fonctions d'un commutateur logique.

Pour plus d'informations sur la recherche de l'ID VIF d'une VM, reportez-vous à la section [Connexion d'une machine virtuelle à un commutateur logique](#).

Note Un commutateur N-VDS configuré en mode Chemin de données optimisé prend en charge la découverte d'adresses IP, SpoofGuard et les profils IPFIX.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Segments**.
- 3 Cliquez sur **Ajouter un segment**.
- 4 Entrez un nom pour le segment.

5 Sélectionnez une passerelle connectée.

Vous pouvez sélectionner une passerelle de niveau 0 ou 1 existante ou **Aucune**. La valeur par défaut est **Aucune**, ce qui signifie que le segment est simplement un commutateur logique. Avec un sous-réseau configuré, il peut s'associer à une passerelle de niveau 0 ou 1.

6 Si la passerelle connectée est de niveau 1, sélectionnez un type, **Flexible** ou **Fixe**.

Un segment flexible peut être dissocié de passerelles. Un segment fixe peut être supprimé, mais ne peut pas être dissocié d'une passerelle.

7 Pour spécifier un sous-réseau, cliquez sur **Définir les sous-réseaux**.

8 Sélectionnez une zone de transport, qui peut être une superposition ou un VLAN.

9 Si la zone de transport est de type VLAN, dressez une liste des ID VLAN.

10 Si vous souhaitez utiliser un VPN de couche 2 pour étendre le segment, cliquez sur la zone de texte **VPN de couche 2** et sélectionnez une session de client ou de serveur VPN de couche 2.

Vous pouvez en sélectionner plusieurs.

11 Dans **ID de tunnel VPN**, entrez une valeur unique utilisée pour identifier le segment.

12 Cliquez sur **Enregistrer**.

13 Pour ajouter des ports de segment, cliquez sur **Oui** lorsque vous y êtes invité si vous souhaitez continuer à configurer le segment.

a Cliquez sur **Ports** et sur **Ensemble**.

b Cliquez sur **Ajouter un port de segment**.

c Entrez un nom de port.

d Pour **ID**, entrez l'UUID VIF de la machine virtuelle ou du serveur qui se connecte à ce port.

e Sélectionnez un type : **Parent**, **Enfant** ou **Indépendant**.

Laissez cette zone de texte vide, à l'exception des cas d'utilisation, tels que des conteneurs ou VMware HCX. Si ce port est destiné au conteneur d'une machine virtuelle, sélectionnez **Enfant**. Si ce port est destiné à une machine virtuelle hébergeant un conteneur, sélectionnez **Parent**. Si ce port est destiné à un conteneur ou serveur bare metal, sélectionnez **Indépendant**.

f Entrez un ID de contexte.

Entrez l'ID VIF du parent si le **Type** est **Enfant**, ou l'ID du nœud de transport si le **Type** est **Indépendant**.

g Entrez une balise de trafic.

Entrez l'ID VLAN dans un conteneur et d'autres cas d'utilisation.

h Sélectionnez une méthode d'allocation d'adresse : **Pool d'adresses IP**, **Pool d'adresses MAC**, **Les deux** ou **Aucune**.

i Spécifiez des balises.

- j Appliquez la liaison d'adresse en spécifiant l'adresse IP (adresse IPv4, adresse IPv6 ou sous-réseau IPv6) et l'adresse MAC du port logique auquel vous souhaitez appliquer la liaison d'adresse. Par exemple, pour IPv6, 2001 ::/64 est un sous-réseau IPv6, 2001 ::1 est une adresse IP d'hôte, alors que 2001 ::1/64 est une entrée non valide. Vous pouvez également spécifier un ID VLAN.

Les liaisons d'adresses manuelles, si elles sont spécifiées, remplacent les liaisons d'adresse découvertes automatiquement.

- k Sélectionnez des profils de segment pour ce port.

14 Pour sélectionner des profils de segments, cliquez sur **Profils de segments**.

15 Cliquez sur **Enregistrer**.

VPN (Virtual Private Network)

5

NSX-T Data Center prend en charge le réseau privé virtuel IPsec (VPN IPsec) et le VPN de couche 2 (VPN L2) sur un nœud NSX Edge. Le VPN IPsec offre la connectivité de site à site entre un nœud NSX Edge et des sites distants. Avec le VPN L2, vous pouvez étendre votre centre de données en autorisant les machines virtuelles à conserver leur connectivité réseau au-delà de limites géographiques tout en utilisant la même adresse IP.

Note Les VPN IPsec et L2 ne sont pas pris en charge dans la version NSX-T Data Center avec exportation limitée.

Vous devez disposer d'un nœud NSX Edge opérationnel, doté d'au moins une passerelle de niveau 0 ou de niveau 1 configurée, pour pouvoir configurer un service VPN. Pour plus d'informations, reportez-vous à la section « Installation de NSX Edge » du *Guide d'installation de NSX-T Data Center*.

À partir de NSX-T Data Center 2.4, vous pouvez également configurer de nouveaux services VPN en utilisant l'interface utilisateur de NSX Manager. Dans les versions antérieures de NSX-T Data Center, vous pouvez configurer les services VPN uniquement en utilisant les appels REST API.

Important Lorsque vous utilisez NSX-T Data Center 2.4 ou une version ultérieure pour configurer des services VPN, vous devez utiliser de nouveaux objets, comme des passerelles de niveau 0, qui ont été créés à l'aide de l'interface utilisateur NSX Manager ou d'API de stratégie incluses dans NSX-T Data Center 2.4 ou une version ultérieure. Pour utiliser les routeurs logiques de niveau 0 ou de niveau 1 existants qui ont été configurés avant la version 2.4 de NSX-T Data Center, vous devez continuer à utiliser des appels API pour configurer un service VPN.

Des profils de configuration système par défaut avec des valeurs et des paramètres prédéfinis sont mis à disposition de manière à être utilisés lors de la configuration d'un service VPN. Vous pouvez également définir de nouveaux profils avec des paramètres différents et les sélectionner lors de la configuration du service VPN.

Ce chapitre contient les rubriques suivantes :

- [Comprendre le VPN IPsec](#)
- [Présentation de VPN de couche 2](#)
- [Ajout de services VPN](#)
- [Ajout de sessions VPN IPsec](#)

- [Ajout de sessions VPN L2](#)
- [Ajouter des points de terminaison locaux](#)
- [Ajout de profils](#)
- [Ajouter un dispositif Edge autonome en tant que client VPN L2](#)
- [Vérifier l'état réalisé d'une session VPN IPSec](#)
- [Surveiller et dépanner des sessions VPN](#)

Comprendre le VPN IPSec

Un VPN de sécurité du protocole Internet (Internet Protocol Security, IPSec) sécurise le trafic circulant entre deux réseaux connectés via un réseau public par le biais de passerelles IPSec appelées des points de terminaison. NSX Edge prend uniquement en charge un mode tunnel qui utilise la mise en tunnel IP avec ESP (Encapsulating Security Payload). ESP fonctionne directement au-dessus d'IP en utilisant le numéro de protocole IP 50.

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

NSX Edge prend en charge un VPN IPSec basé sur une stratégie ou sur une route.

Les services VPN IPSec sont uniquement pris en charge sur les passerelles de niveau 0 qui doivent être en mode haute disponibilité *Active-Standby*. Consultez [Ajouter une passerelle de niveau 0](#) pour plus d'informations. À partir de la version NSX-T Data Center 2.5, VPN IPSec est également pris en charge sur les passerelles de niveau 1. Vous pouvez utiliser les segments connectés à des passerelles de niveau 0 ou 1 lors de la configuration d'un service VPN IPSec.

Le service VPN IPSec dans NSX-T Data Center utilise la fonctionnalité de basculement au niveau de la passerelle pour prendre en charge un service haute disponibilité. Des tunnels sont rétablis sur le basculement et les données de configuration VPN sont synchronisées. L'état du VPN IPSec n'est pas synchronisé lors du rétablissement des tunnels.

L'authentification en mode de clé prépartagée et le trafic de monodiffusion IP sont pris en charge entre le nœud NSX Edge et les sites VPN distants. En outre, l'authentification par certificat est prise en charge à partir de NSX-T Data Center 2.4. Seuls les types de certificat signés par l'un des algorithmes de hachage de signature suivants sont pris en charge.

- SHA256withRSA
- SHA384withRSA
- SHA512withRSA

Utilisation d'un VPN IPSec basé sur les stratégies

Un VPN IPSec basé sur les stratégies nécessite qu'une stratégie VPN soit appliquée aux paquets pour déterminer quel trafic doit être protégé par IPSec avant d'être transmis via le tunnel VPN.

Ce type de VPN est considéré comme statique, car lorsque la topologie et la configuration du réseau local changent, les paramètres de stratégie du VPN doivent également être mis à jour pour prendre en charge les modifications.

Lorsque vous utilisez un VPN IPSec basé sur les stratégies avec NSX-T Data Center, les tunnels IPSec vous permettent de connecter un ou plusieurs sous-réseaux locaux derrière le nœud NSX Edge aux sous-réseaux homologues sur le site VPN distant.

Vous pouvez déployer un nœud NSX Edge derrière un périphérique NAT. Dans ce type de déploiement, le périphérique NAT convertit l'adresse VPN d'un nœud NSX Edge en une adresse accessible publiquement sur Internet. Les sites VPN distants utilisent cette adresse publique pour accéder au nœud NSX Edge.

Vous pouvez aussi placer des sites VPN distants derrière un périphérique NAT. Vous devez fournir l'adresse IP publique du site VPN distant, ainsi que son ID (adresse de nom de domaine complet ou adresse IP) pour configurer le tunnel IPSec. Des deux côtés, une conversion NAT statique bijective est indispensable pour l'adresse du VPN.

Note DNAT n'est pas pris en charge sur une passerelle de niveau 1 où un VPN IPSec basé sur les stratégies est configuré.

La taille du nœud NSX Edge détermine le nombre maximal de tunnels pris en charge, comme indiqué dans le tableau suivant.

Tableau 5-1. Nombre de tunnels IPSec pris en charge

Taille du nœud Edge	Nombre de tunnels IPSec par session VPN (basée sur les stratégies)	Nombre de sessions par service VPN	Nombre de tunnels IPSec par service VPN (16 tunnels par session)
Petite	S/o (POC/Lab uniquement)	S/o (POC/Lab uniquement)	S/o (POC/Lab uniquement)
Moyenne	128	128	2048
Grande	128 (limite logicielle)	256	4096
Bare Metal	128 (limite logicielle)	512	6000

Restriction L'architecture inhérente d'un VPN IPSec basé sur les stratégies vous empêche de configurer la redondance d'un tunnel VPN.

Pour plus d'informations sur la configuration d'un VPN IPSec basé sur les stratégies, consultez la section [Ajouter un service VPN IPSec](#).

Utilisation du VPN IPSec basé sur une route

Un VPN IPSec basé sur l'itinéraire fournit un tunnel sur le trafic en fonction des itinéraires statiques ou des itinéraires appris de façon dynamique 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).

Note

- Le routage dynamique OSPF n'est pas pris en charge pour le routage via des tunnels VPN IPSec.
 - Le routage dynamique de la VTI n'est pas pris en charge sur un VPN basé sur des passerelles de niveau 1.
-

VPN IPSec basé sur le routage est similaire à GRE (Generic Routing Encapsulation) sur IPSec, à la différence près qu'aucune encapsulation supplémentaire n'est ajoutée au paquet avant l'application du traitement IPSec.

Dans cette approche de tunneling VPN, des VTI sont créées sur le nœud NSX Edge. Chaque VTI est associée à un tunnel IPSec. Le trafic crypté est acheminé d'un site à un autre site au moyen des interfaces VTI. Le traitement IPSec se produit uniquement sur les VTI.

Redondance de tunnel VPN

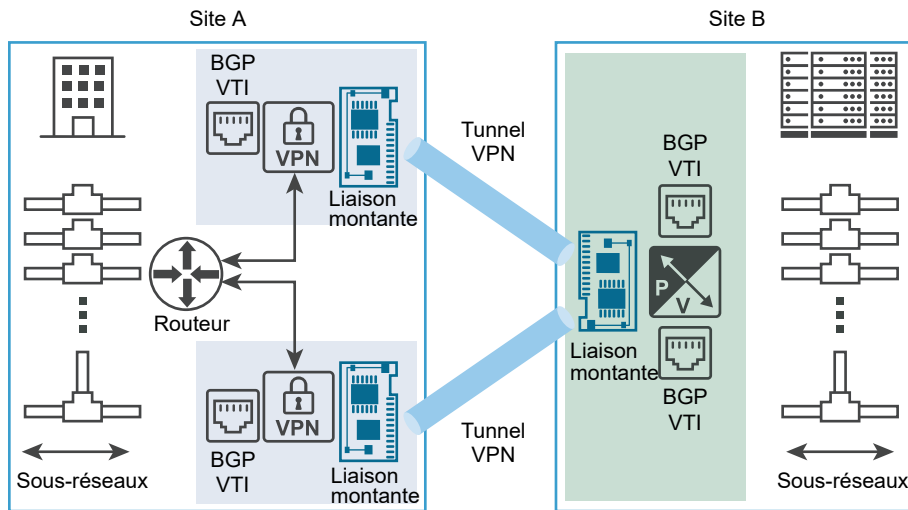
Vous pouvez configurer la redondance de tunnel VPN avec une session VPN IPSec basée sur l'itinéraire qui est configurée sur une passerelle de niveau 0. Avec la redondance de tunnel, plusieurs tunnels peuvent être configurés entre deux sites, un tunnel étant utilisé comme principal avec basculement vers les autres tunnels lorsque le tunnel principal devient indisponible. Cette fonctionnalité est très utile lorsqu'un site dispose de plusieurs options de connectivité, par exemple avec différents FAI pour la redondance de liaison.

Important

- Dans NSX-T Data Center, la redondance de tunnel VPN IPSec est prise en charge uniquement à l'aide de BGP.
 - N'utilisez pas de routage statique pour les tunnels VPN IPSec basés sur le routage pour obtenir la redondance de tunnel VPN.
-

La figure suivante illustre une représentation logique de la redondance de tunnel VPN IPSec entre deux sites. Dans cette figure, le Site A et le Site B représentent deux centres de données. Pour cet exemple, supposez que NSX-T Data Center ne gère pas les passerelles VPN Edge sur le site A et que NSX-T Data Center gère un dispositif virtuel de passerelle Edge sur le site B.

Figure 5-1. Redondance de tunnel dans un VPN IPSec basé sur l'itinéraire



Comme illustré dans la figure, vous pouvez configurer deux tunnels VPN IPSec indépendants en utilisant des VTI. Le routage dynamique est configuré à l'aide du protocole BGP pour obtenir la redondance de tunnel. Si les deux tunnels VPN IPSec sont disponibles, ils restent en service. Tout le trafic destiné à aller du Site A au Site B via le nœud NSX Edge est acheminé via la VTI. Le trafic de données subit un traitement IPSec et sort de son interface de liaison montante de nœud NSX Edge associée. Tout le trafic IPSec entrant reçu de la passerelle VPN du Site B sur l'interface de liaison montante de nœud NSX Edge est transféré vers la VTI après déchiffrement, puis le routage habituel a lieu.

Vous devez configurer les temporisateurs de durée de retenue et de durée de survie du protocole BGP pour détecter toute perte de connectivité avec l'homologue dans le délai de basculement requis. Reportez-vous à la section [Configurer BGP](#).

Présentation de VPN de couche 2

Grâce à VPN de couche 2 (VPN L2), vous pouvez étendre les réseaux de couche 2 (VNI ou VLAN) sur plusieurs sites dans le même domaine de diffusion. Cette connexion est sécurisée avec un tunnel IPSec basé sur l'itinéraire entre le serveur VPN de couche 2 et le client VPN de couche 2.

Note Cette fonctionnalité VPN L2 est uniquement disponible pour NSX-T Data Center et n'offre aucune interopérabilité tiers.

Le réseau étendu est un sous-réseau unique avec un seul domaine de diffusion, de telle sorte que les machines virtuelles demeurent sur le même sous-réseau lorsqu'elles sont déplacées entre des sites et leurs adresses IP ne changent pas. Par conséquent, les entreprises peuvent migrer des machines virtuelles de manière transparente entre les sites réseau. Les machines virtuelles peuvent s'exécuter sur des réseaux VNI ou VLAN. Pour les fournisseurs de cloud, VPN L2 fournit un mécanisme permettant d'intégrer des locataires sans modifier les adresses IP existantes utilisées par leurs charges de travail et leurs applications.

Outre la prise en charge de la migration de centre de données, un réseau sur site étendu avec un VPN de couche 2 est utile pour un plan de récupération d'urgence et l'engagement dynamique de ressources de calcul pour répondre à l'augmentation de la demande.

Chaque session VPN L2 dispose d'un tunnel GRE (Generic Routing Encapsulation). La redondance du tunnel n'est pas prise en charge. Une session VPN de couche 2 peut inclure jusqu'à 4 094 segments de couche 2.

Dans NSX-T Data Center, les services VPN de couche 2 sont uniquement pris en charge sur les passerelles de niveau 0. Les segments peuvent être connectés à des passerelles de niveau 0 ou de niveau 1, et utilisent des services VPN L2.

À partir de la version NSX-T Data Center 2.5, les segments VLAN peuvent être étendus à l'aide du service VPN de couche 2 sur un NSX Edge qui est géré dans un environnement NSX-T Data Center. Cette prise en charge permet d'étendre les réseaux de couche 2 du VLAN au VNI, du VLAN au VLAN et du VNI au VNI.

Le protocole VLAN Trunking est également pris en charge à l'aide d'un commutateur virtuel distribué (N-VDS) géré par NSX ESX. Si les ressources de calcul et d'E/S le permettent, le protocole VLAN Trunking permet à un cluster NSX Edge d'étendre plusieurs réseaux VLAN sur une interface unique.

La prise en charge du service VPN de couche 2 est assurée dans les scénarios suivants.

- Entre un serveur VPN de couche 2 NSX-T Data Center et un client VPN de couche 2 hébergé sur un NSX Edge géré dans un environnement NSX Data Center for vSphere. Un client VPN L2 géré prend en charge les VLAN et les VNI.
- Entre un serveur VPN L2 NSX-T Data Center et un client VPN L2 hébergé sur une instance autonome ou non gérée de NSX Edge. Un client VPN L2 non géré ne prend en charge que les VLAN.
- Entre un serveur VPN L2 NSX-T Data Center et un client VPN L2 hébergé sur une instance autonome de NSX Edge. Un client VPN L2 autonome ne prend en charge que les VLAN.
- À partir de NSX-T Data Center 2.4, la prise en charge du service VPN L2 est disponible entre un serveur VPN L2 NSX-T Data Center et des clients VPN L2 NSX-T Data Center. Dans ce scénario, vous pouvez étendre les segments logiques de couche 2 entre deux centres de données software-defined (SDDC) sur site

Ajout de services VPN

Vous pouvez ajouter un VPN IPsec (basé sur les stratégies ou basé sur le routage) ou un VPN de couche 2 à l'aide de l'interface utilisateur de NSX Manager.

Les sections suivantes fournissent des informations sur les workflows requis pour configurer le service VPN dont vous avez besoin. Les rubriques qui suivent ces sections fournissent des détails sur l'ajout d'un VPN IPsec ou un VPN de couche 2 à l'aide de l'interface utilisateur de NSX Manager.

Workflow de configuration de VPN IPSec basé sur les stratégies

La configuration d'un workflow de service VPN IPSec basé sur les stratégies nécessite les étapes de haut niveau suivantes.

- 1 Créez et activez un service VPN IPSec à l'aide d'une passerelle de niveau 0 ou de niveau 1 existante. Reportez-vous à la section [Ajouter un service VPN IPSec](#).
- 2 Créez un profil de détection des homologues inactifs (DPD), si vous préférez ne pas utiliser le profil par défaut du système. Reportez-vous à la section [Ajouter des profils DPD](#).
- 3 Pour utiliser un profil IKE par défaut non système, définissez un profil IKE (Internet Key Exchange). Reportez-vous à la section [Ajouter des profils IKE](#).
- 4 Configurez un profil IPSec à l'aide de la section [Ajouter des profils IPSec](#).
- 5 Utilisez [Ajouter des points de terminaison locaux](#) pour créer un serveur VPN hébergé sur NSX Edge.
- 6 Configurez une session VPN IPSec basée sur les stratégies, appliquez les profils et attachez le point de terminaison local à cette session. Reportez-vous à la section [Ajouter une session IPSec basée sur les stratégies](#). Spécifiez les sous-réseaux locaux et homologues à utiliser pour le tunnel. Le trafic d'un sous-réseau local destiné au sous-réseau homologue est protégé à l'aide du tunnel défini dans la session.

Workflow de configuration de VPN IPSec basé sur le routage

Un workflow de configuration VPN IPSec basé sur le routage nécessite les étapes de haut niveau suivantes.

- 1 Configurez et activez un service VPN IPSec à l'aide d'une passerelle de niveau 0 ou de niveau 1 existante. Reportez-vous à la section [Ajouter un service VPN IPSec](#).
- 2 Définissez un profil IKE si vous préférez ne pas utiliser le profil IKE par défaut. Reportez-vous à la section [Ajouter des profils IKE](#).
- 3 Si vous décidez de ne pas utiliser le profil IPSec par défaut du système, créez-en un à l'aide de la section [Ajouter des profils IPSec](#).
- 4 Créez un profil DPD si vous ne souhaitez pas utiliser le profil DPD par défaut. Reportez-vous à la section [Ajouter des profils DPD](#).
- 5 Ajoutez un point de terminaison local à l'aide de la section [Ajouter des points de terminaison locaux](#).
- 6 Configurez une session VPN IPSec basée sur l'itinéraire, appliquez les profils et attachez le point de terminaison local à cette session. Saisissez une adresse IP VTI dans la configuration et utilisez la même adresse IP pour configurer le routage. Les itinéraires peuvent être statiques ou dynamiques (à l'aide de BGP). Reportez-vous à la section [Ajout d'une session IPSec basée sur une route](#).

Workflow de configuration de VPN de couche 2

La configuration d'un VPN de couche 2 nécessite de configurer un service VPN de couche 2 en mode serveur, puis un autre service VPN de couche 2 en mode client. Vous devez également configurer les sessions pour le serveur VPN de couche 2 et le client VPN de couche 2 à l'aide du code homologue généré par le serveur VPN de couche 2. Voici un workflow de haut niveau pour la configuration d'un service VPN de couche 2.

- 1 Créez un service VPN de couche 2 en mode serveur.
 - a Configurez un tunnel VPN IPSec basé sur le routage avec une passerelle de niveau 0 et un service serveur VPN de couche 2 à l'aide de ce tunnel IPSec basé sur le routage. Reportez-vous à la section [Ajouter un service serveur VPN de couche 2](#).
 - b Configurez une session serveur VPN de couche 2, ce qui lie le nouveau service VPN IPSec basé sur le routage et le service serveur VPN de couche 2 et alloue automatiquement des adresses IP GRE. Reportez-vous à la section [Ajouter une session de serveur VPN L2](#).
 - c Ajoutez des segments aux sessions serveur VPN de couche 2. Cette étape est également décrite dans la section [Ajouter une session de serveur VPN L2](#).
 - d Utilisez la section [Télécharger le fichier de configuration du VPN de couche 2 côté distant](#) pour obtenir le code homologue pour la session du service serveur VPN de couche 2, qui doit être appliquée sur le site distant et utilisée pour configurer automatiquement la session client VPN de couche 2.
- 2 Créez un service VPN de couche 2 en mode client.
 - a Configurez un autre service VPN IPSec basé sur le routage à l'aide d'une autre passerelle de niveau 0 et configurez un service client VPN de couche 2 à l'aide de la passerelle de niveau 0 que vous venez de configurer. Consultez [Ajouter un service client VPN L2](#) pour plus d'informations.
 - b Définissez les sessions client VPN de couche 2 en important le code homologue généré par le service serveur VPN de couche 2. Reportez-vous à la section [Ajouter une session client VPN de couche 2](#).
 - c Ajoutez des segments aux sessions client VPN de couche 2 définies dans l'étape précédente. Cette étape est décrite dans la section [Ajouter une session client VPN de couche 2](#).

Ajouter un service VPN IPSec

NSX-T Data Center prend en charge l'établissement d'un service VPN IPSec site à site entre une passerelle de niveau 0 ou de niveau 1 et des sites distants. Vous pouvez créer un service VPN IPSec basé sur des stratégies ou sur une route. Vous devez d'abord créer le service VPN IPSec avant de pouvoir configurer une session VPN IPSec basée sur des stratégies ou sur une route.

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

Le VPN IPSec n'est pas pris en charge lorsque l'adresse IP du point de terminaison local passe par NAT dans le même routeur logique sur lequel la session VPN IPSec est configurée.

Conditions préalables

- Familiarisez-vous avec le VPN IPSec. Reportez-vous à la section [Comprendre le VPN IPSec](#).
- Vous devez avoir configuré au moins une passerelle de niveau 0 ou de niveau 1 et celle-ci doit être disponible. Pour plus d'informations, reportez-vous à la section [Ajouter une passerelle de niveau 0](#) ou [Ajouter une passerelle de niveau 1](#).

Procédure

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

2 Accédez à **Mise en réseau > VPN > Services VPN**.

3 Sélectionnez **Ajouter un service > IPSec**.

4 Entrez le nom du service IPSec.

Ce nom est obligatoire.

5 Dans le menu déroulant **Passerelle**, sélectionnez la passerelle de niveau 0 ou de niveau 1 à associer à ce service VPN IPSec.

6 Activez ou désactivez **Statut administratif**.

Par défaut, la valeur est définie sur `Enabled`, ce qui signifie que le service VPN IPSec est activé sur la passerelle de niveau 0 ou de niveau 1 une fois le nouveau service VPN IPSec configuré.

7 Définissez la valeur pour **Niveau de journal IKE**.

Par défaut, il est défini sur le niveau `Info`.

8 Entrez une valeur pour **Balises** si vous souhaitez inclure ce service dans un groupe de balises.

9 Cliquez sur **Règles de contournement global** si vous voulez autoriser l'échange de paquets de données entre les adresses IP locales et distantes spécifiées sans protection IPSec, même si les adresses IP sont spécifiées dans les règles de session IPSec. Dans les zones de texte **Réseaux locaux** et **Réseaux distants**, entrez la liste des sous-réseaux locaux et distants entre lesquels les règles de contournement sont appliquées.

Par défaut, la protection IPSec est utilisée lorsque les données sont échangées entre les sites locaux et distants. Ces règles s'appliquent à toutes les sessions VPN IPSec créées au sein de ce service VPN IPSec.

10 Cliquez sur **Enregistrer**.

Une fois que le nouveau service VPN IPSec a été correctement créé, il vous est demandé si vous souhaitez poursuivre le reste de la configuration VPN IPSec. Si vous cliquez sur **Oui**, vous revenez au panneau Ajouter un service VPN IPSec. Le lien **Sessions** est à présent activé et vous pouvez cliquer dessus pour ajouter une session VPN IPSec.

Étape suivante

Utilisez les informations de la rubrique [Ajout de sessions VPN IPSec](#) pour vous guider lors de l'ajout d'une session VPN IPSec. Vous fournissez également des informations pour les profils et le point de terminaison local qui sont requises pour terminer la configuration VPN IPSec.

Ajouter un service VPN L2

Vous configurez un service VPN L2 sur une passerelle de niveau 0. Pour activer le service VPN L2, vous devez d'abord créer un service VPN IPSec sur la passerelle de niveau 0, s'il n'existe pas encore. Vous configurez ensuite un tunnel VPN L2 entre un serveur VPN L2 (passerelle de destination) et un client VPN L2 (passerelle source).

Pour configurer un service VPN L2, utilisez les informations données dans les rubriques suivantes de cette section.

Conditions préalables

- Familiarisez-vous avec les réseaux VPN IPSec et VPN L2. Reportez-vous aux sections [Comprendre le VPN IPSec](#) et [Présentation de VPN de couche 2](#).
- Vous devez disposer d'au moins une passerelle de niveau 0 configurée et disponible pour l'utilisation. Reportez-vous à la section [Ajouter une passerelle de niveau 0](#).

Procédure

1 [Ajouter un service serveur VPN de couche 2](#)

Pour configurer un service serveur VPN de couche 2, vous devez configurer le service VPN de couche 2 en mode serveur sur le dispositif NSX Edge de destination auquel le client VPN de couche 2 doit être connecté.

2 [Ajouter un service client VPN L2](#)

Après avoir configuré le service de serveur VPN L2, configurez le service VPN L2 en mode client sur une autre instance de NSX Edge.

Ajouter un service serveur VPN de couche 2

Pour configurer un service serveur VPN de couche 2, vous devez configurer le service VPN de couche 2 en mode serveur sur le dispositif NSX Edge de destination auquel le client VPN de couche 2 doit être connecté.

Procédure

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

- 2 (Facultatif) Si un service VPN IPSec n'existe pas encore sur la passerelle de niveau 0 que vous souhaitez configurer en tant que serveur VPN L2, créez le service en procédant comme suit.
 - a Accédez à l'onglet **Mise en réseau > VPN > Services VPN** et sélectionnez **Ajouter un service > IPSec**.
 - b Entrez un nom pour le service VPN IPSec.
 - c Dans le menu déroulant **Passerelle de niveau 0**, sélectionnez une passerelle de niveau 0 à utiliser avec le serveur VPN de couche 2.
 - d Si vous souhaitez utiliser des valeurs différentes de celles du système, définissez le reste des propriétés dans le volet Ajouter un service IPSec, si nécessaire.
 - e Cliquez sur **Enregistrer** et sélectionnez **Non** lorsqu'il vous est demandé si vous souhaitez continuer à configurer le service VPN IPSec.
- 3 Accédez à l'onglet **Mise en réseau > VPN > Services VPN** et sélectionnez **Ajouter un service > Serveur VPN de couche 2** pour créer un serveur VPN de couche 2.
- 4 Entrez le nom du serveur VPN de couche 2.
- 5 Dans le menu déroulant **Passerelle de niveau 0**, sélectionnez la même passerelle de niveau 0 que vous avez utilisée avec le service IPSec que vous venez de créer.
- 6 Entrez une description facultative pour ce serveur VPN de couche 2.
- 7 Entrez une valeur pour **Balises** si vous souhaitez inclure ce service dans un groupe de balises.
- 8 Activez ou désactivez la propriété **Hub and spoke**.

Par défaut, la valeur est définie sur `Disabled`, ce qui signifie que le trafic reçu à partir des clients VPN L2 est répliqué uniquement vers les segments connectés au serveur VPN L2. Si cette propriété est définie sur `Enabled`, le trafic à partir de n'importe quel client VPN de couche 2 est répliqué vers tous les autres clients VPN de couche 2.

- 9 Cliquez sur **Enregistrer**.

Une fois que le nouveau service VPN de couche 2 a été correctement créé, il vous est demandé si vous souhaitez poursuivre le reste de la configuration du service VPN de couche 2. Si vous cliquez sur **Oui**, vous êtes redirigé vers le volet Ajouter un serveur VPN de couche 2 et le lien **Session** est activé. Vous pouvez utiliser ce lien pour créer une session serveur VPN de couche 2 ou utiliser l'onglet **Mise en réseau > VPN > Sessions VPN de couche 2**.

Étape suivante

Configurez une session serveur VPN de couche 2 pour le serveur VPN de couche 2 que vous avez configuré à l'aide des informations de la section [Ajouter une session de serveur VPN L2](#) pour vous guider.

Ajouter un service client VPN L2

Après avoir configuré le service de serveur VPN L2, configurez le service VPN L2 en mode client sur une autre instance de NSX Edge.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 (Facultatif) S'il n'en existe pas encore, créez un service VPN IPSec pour le service client VPN L2 en procédant comme suit.
 - a Accédez à l'onglet **Mise en réseau > VPN > Services VPN** et sélectionnez **Ajouter un service > IPSec**.
 - b Entrez un nom pour le service VPN IPSec.
 - c Dans le menu déroulant **Passerelle de niveau 0**, sélectionnez une passerelle de niveau 0 à utiliser avec le client VPN L2.
 - d Si vous souhaitez utiliser des valeurs différentes de celles du système, définissez le reste des propriétés dans le volet Ajouter un service IPSec, si nécessaire.
 - e Cliquez sur **Enregistrer** et sélectionnez **Non** lorsqu'il vous est demandé si vous souhaitez continuer à configurer le service VPN IPSec.
- 3 Accédez à l'onglet **Mise en réseau > VPN > Services VPN** et sélectionnez **Ajouter un service > Client VPN de couche 2**.
- 4 Entrez un nom pour le service du client VPN L2.
- 5 Dans le menu déroulant **Passerelle de niveau 0**, sélectionnez la même passerelle de niveau 0 que celle que vous avez utilisée avec le tunnel IPSec basé sur le routage que vous venez de créer.
- 6 Vous pouvez éventuellement définir les valeurs pour **Description** et **Balises**.
- 7 Cliquez sur **Enregistrer**.

Une fois le nouveau service du client VPN L2 créé, vous êtes invité à poursuivre la configuration du client VPN L2. Si vous cliquez sur **Oui**, vous êtes redirigé vers le volet Ajouter un client VPN L2 et le lien **Session** est activé. Vous pouvez utiliser ce lien pour créer une session de client VPN L2 ou utiliser l'onglet **Mise en réseau > VPN > Sessions VPN de couche 2**.

Étape suivante

Configurez une session de client VPN L2 pour le service du client VPN L2 que vous avez configuré. Utilisez les informations de la section [Ajouter une session client VPN de couche 2](#) pour y parvenir.

Ajout de sessions VPN IPSec

Après avoir configuré un service VPN IPSec, vous devez ajouter une session VPN IPSec basée sur les stratégies ou une session VPN IPSec basée sur le routage, selon le type de VPN IPSec vous souhaitez configurer. Vous devez également fournir les informations pour le point de terminaison local et les profils à utiliser afin de terminer la configuration du service VPN IPSec.

Ajouter une session IPSec basée sur les stratégies

Lorsque vous ajoutez un VPN IPSec basé sur les stratégies, les tunnels IPSec sont utilisés pour connecter plusieurs sous-réseaux locaux qui se trouvent derrière le nœud NSX Edge, tandis que les sous-réseaux homologues sont sur le site VPN distant.

Les étapes suivantes utilisent l'onglet **Sessions IPSec** sur l'interface utilisateur de NSX Manager pour créer une session IPSec basée sur des stratégies. Vous ajoutez également des informations pour les profils de tunnel, IKE et DPD, puis sélectionnez un point de terminaison local existant à utiliser avec le VPN IPSec basé sur les stratégies.

Note Vous pouvez également ajouter les sessions VPN IPSec immédiatement après avoir correctement configuré le service VPN IPSec. Vous cliquez sur **Oui** lorsque vous êtes invité à poursuivre la configuration du service VPN IPSec et sélectionnez **Sessions > Ajouter des sessions** dans le panneau Ajouter un service IPsec. Les premières étapes de la procédure suivante supposent que vous avez sélectionné **Non** en réponse à l'invite vous proposant de poursuivre la configuration du service VPN IPSec. Si vous sélectionnez **Oui**, passez à l'étape 3 dans les étapes suivantes pour être guidé dans le reste de la configuration de la session VPN IPSec basée sur les stratégies.

Conditions préalables

- Vous devez avoir configuré un service VPN IPSec avant de continuer. Reportez-vous à la section [Ajouter un service VPN IPSec](#).
- Obtenez les informations pour le point de terminaison local, l'adresse IP pour le site homologue, le sous-réseau du réseau local et le sous-réseau du réseau distant à utiliser avec la session VPN IPSec basée sur les stratégies que vous ajoutez. Pour créer un point de terminaison local, reportez-vous à la section [Ajouter des points de terminaison locaux](#).
- Si vous utilisez une clé prépartagée (PSK) pour l'authentification, obtenez la valeur PSK.
- Si vous utilisez un certificat pour l'authentification, assurez-vous que les certificats de serveur nécessaires et les certificats signés par l'autorité de certification correspondants sont déjà importés. Reportez-vous à la section [Configuration de certificats](#).
- Si vous ne souhaitez pas utiliser les valeurs par défaut pour les profils de tunnel IPSec, IKE ou de détection des homologues inactifs (DPD) fournis par NSX-T Data Center, configurez les profils que vous souhaitez utiliser à la place. Pour plus d'informations, reportez-vous à la section [Ajout de profils](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Accédez à l'onglet **Mise en réseau > VPN > Sessions IPSec**.
- 3 Sélectionnez **Ajouter une session IPSec > Basé sur la stratégie**.
- 4 Entrez un nom pour la session VPN IPSec basée sur les stratégies.
- 5 Dans le menu déroulant **Service VPN**, sélectionnez le service VPN IPSec auquel vous souhaitez ajouter cette nouvelle session IPSec.

Note Si vous ajoutez cette session IPSec à partir de la boîte de dialogue **Ajouter les sessions IPSec**, le nom du service VPN est déjà indiqué au-dessus du bouton **Ajouter une session IPSec**.

- 6 Sélectionnez un point de terminaison local existant dans le menu déroulant.
 Cette valeur de point de terminaison local est requise et identifie le nœud NSX Edge local. Si vous souhaitez créer un point de terminaison local différent, cliquez sur le menu à trois points (⋮) et sélectionnez **Ajouter un point de terminaison local**.
- 7 Dans la zone de texte **Adresse IP distante**, entrez l'adresse IP requise du site distant.
 Cette valeur est requise.
- 8 Entrez une description facultative pour cette session VPN IPSec basée sur les stratégies.
 La longueur maximale est de 1 024 caractères.
- 9 Pour activer ou désactiver la session VPN IPSec, cliquez sur **Statut administratif**.
 Par défaut, la valeur est définie sur `Enabled`, ce qui signifie que la session VPN IPSec doit être configurée jusqu'au nœud NSX Edge.
- 10 (Facultatif) Dans le menu déroulant **Suite de conformité**, sélectionnez une suite de conformité de sécurité.

Note La prise en charge de la suite de conformité est garantie à partir de la version NSX-T Data Center 2.5. Pour plus d'informations, reportez-vous à la section [À propos des suites de conformité prises en charge](#).

La valeur par défaut sélectionnée est `None`. Si vous sélectionnez une suite de conformité, le **mode d'authentification** est défini sur `Certificate` et dans la section **Propriétés avancées**, les valeurs de **Profil IKE** et **Profil IPSec** sont définies sur les profils définis par le système pour la suite de conformité de sécurité sélectionnée. Il n'est pas possible de modifier ces profils définis par le système.

- 11 Si la **Suite de conformité** est définie sur `None`, sélectionnez un mode dans le menu déroulant **Mode d'authentification**.

Le mode d'authentification par défaut utilisé est `PSK`, ce qui signifie qu'une clé secrète partagée entre NSX Edge et le site distant doit être utilisée pour la session VPN IPSec. Si vous sélectionnez `Certificate`, le certificat de site utilisé pour configurer le point de terminaison local est utilisé pour l'authentification.

- 12 Dans les zones de texte Réseaux locaux et Réseaux distants, entrez au moins une adresse de sous-réseau IP à utiliser pour cette session VPN IPSec basée sur les stratégies.

Ces sous-réseaux doivent être au format CIDR.

- 13 Si le paramètre **Mode d'authentification** est défini sur `PSK`, entrez la valeur de clé dans la zone de texte **Clé prépartagée**.

La clé secrète peut être une chaîne d'une longueur maximale de 128 caractères.

Attention Soyez prudent lorsque vous partagez et stockez une valeur PSK, car elle contient des informations sensibles.

- 14 Pour identifier le site homologue, entrez une valeur dans **ID distant**.

Pour les sites homologues qui utilisent l'authentification PSK, cette valeur d'ID doit être l'adresse IP publique ou le nom de domaine complet du site homologue. Pour les sites homologues utilisant l'authentification par certificat, cette valeur d'ID doit être le nom commun (CN) ou le nom unique (DN) figurant dans le certificat du site homologue.

Note Si le certificat du site homologue contient une adresse e-mail dans la chaîne DN, par exemple,

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123/emailAddress=user1@mycompany.com
```

entrez la valeur **ID distant** en utilisant le format suivant comme exemple.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, MAILTO=user1@mycompany.com"
```

Si le certificat du site local contient une adresse e-mail dans la chaîne DN et que le site homologue utilise l'implémentation IPsec strongSwan, entrez la valeur d'ID du site local dans ce site homologue. Vous en trouverez ci-dessous un exemple.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, E=user1@mycompany.com"
```

- 15 Pour modifier les profils, le mode d'initialisation, le mode de restriction MSS TCP et les balises utilisées par la session VPN IPsec basée sur les stratégies, cliquez sur **Propriétés avancées**.

Par défaut, les profils générés par le système sont utilisés. Sélectionnez un autre profil disponible si vous ne souhaitez pas utiliser la valeur par défaut. Pour utiliser un profil qui n'est pas encore configuré, cliquez sur le menu à trois points (⋮) pour créer un autre profil. Reportez-vous à la section [Ajout de profils](#).

- a Si le menu déroulant **Profils IKE** est activé, sélectionnez le profil IKE.
- b Sélectionnez le profil de tunnel IPsec, si le menu déroulant **Profils IPsec** n'est pas désactivé.
- c Sélectionnez le profil DPD préféré dans le menu déroulant **Profils DPD** est activé.
- d Sélectionnez le mode préféré à partir du menu déroulant **Mode d'initialisation de la connexion**.

Le mode d'initialisation de la connexion définit la stratégie utilisée par le point de terminaison local au cours du processus de création du tunnel. La valeur par défaut est **Initiateur**. Le tableau suivant décrit les différents modes d'initialisation de la connexion disponibles.

Tableau 5-2. Modes d'initialisation de la connexion

Mode d'initialisation de la connexion	Description
Initiator	Valeur par défaut. Dans ce mode, le point de terminaison local lance la création du tunnel VPN IPsec et répond aux demandes de configuration de tunnel entrantes provenant de la passerelle homologue.
On Demand	Dans ce mode, le point de terminaison local lance la création du tunnel VPN IPsec après que le premier paquet correspondant à la règle de stratégie est reçu. Il répond également à la demande d'initialisation entrante.
Respond Only	Le VPN IPsec ne lance jamais une connexion. Le site homologue initie toujours la demande de connexion et le point de terminaison local répond à celle-ci.

- e Pour réduire la charge utile de taille maximale de segment (MSS) de la session TCP pendant la connexion IPsec, activez **Restriction MSS TCP**, sélectionnez la valeur de **Direction de MSS TCP** et définissez éventuellement la **valeur de MSS TCP**.

Pour plus d'informations, reportez-vous à la section [Présentation de la restriction MSS TCP](#).

- f Si vous souhaitez inclure cette session dans le cadre d'un groupe spécifique, entrez le nom de la balise dans **Balises**.

- 16 Cliquez sur **Enregistrer**.

Résultats

Lorsque la nouvelle session VPN IPSec basée sur les stratégies est correctement configurée, elle est ajoutée à la liste des sessions VPN IPSec disponibles. Elle est en mode de lecture seule.

Étape suivante

- Vérifiez que l'état du tunnel VPN IPSec est Actif. Pour plus d'informations, reportez-vous à la section [Surveiller et dépanner des sessions VPN](#).
- Si nécessaire, gérez les informations de la session VPN IPSec en cliquant sur le menu à trois points (⋮) à gauche de la ligne de la session. Sélectionnez l'une des actions que vous êtes autorisé à effectuer.

Ajout d'une session IPSec basée sur une route

Lorsque vous ajoutez un VPN IPSec basé sur une route, la tunnellation est fournie sur le trafic qui est basé sur les routes qui ont été apprises dynamiquement via une interface de tunnel virtuel (VTI) à l'aide d'un protocole préféré, tel que BGP. IPSec sécurise tout le trafic circulant à travers l'interface de tunnel virtuel (VTI).

Les étapes décrites dans cette rubrique utilisent l'onglet **Sessions IPSec** pour créer une session IPSec basée sur une route. Vous ajoutez également des informations pour le tunnel, IKE et les profils DPD, et sélectionnez un point de terminaison local existant à utiliser avec le VPN IPSec basé sur une route.

Note Vous pouvez également ajouter les sessions VPN IPSec immédiatement après avoir correctement configuré le service VPN IPSec. Vous cliquez sur **Oui** lorsque vous êtes invité à poursuivre la configuration du service VPN IPSec et sélectionnez **Sessions > Ajouter des sessions** dans le panneau Ajouter un service IPsec. Les premières étapes de la procédure suivante supposent que vous avez sélectionné **Non** en réponse à l'invite vous proposant de poursuivre la configuration du service VPN IPSec. Si vous avez sélectionné **Oui**, passez à l'étape 3 dans les étapes suivantes, qui vous guideront dans la suite de la configuration de la session VPN IPSec basée sur une route.

Conditions préalables

- Vous devez avoir configuré un service VPN IPSec avant de continuer. Reportez-vous à la section [Ajouter un service VPN IPSec](#).
- Obtenez les informations pour le point de terminaison local, l'adresse IP pour le site homologue et l'adresse de sous-réseau IP du service de tunnel à utiliser avec la session IPSec basée sur une route que vous ajoutez. Pour créer un point de terminaison local, reportez-vous à la section [Ajouter des points de terminaison locaux](#).
- Si vous utilisez une clé prépartagée (PSK) pour l'authentification, obtenez la valeur PSK.
- Si vous utilisez un certificat pour l'authentification, assurez-vous que les certificats de serveur nécessaires et les certificats signés par l'autorité de certification correspondants sont déjà importés. Reportez-vous à la section [Configuration de certificats](#).

- Si vous ne souhaitez pas utiliser les valeurs par défaut pour le tunnel IPSec, IKE ou les profils DPD (Dead Peer Detection) fournis par NSX-T Data Center, configurez les profils que vous souhaitez utiliser à la place. Pour plus d'informations, reportez-vous à la section [Ajout de profils](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Accédez à **Mise en réseau > VPN > Sessions IPSec**.
- 3 Sélectionnez **Ajouter une session IPSec > Basé sur la route**.
- 4 Entrez le nom de la session IPSec basée sur une route.
- 5 Dans le menu déroulant **Service VPN**, sélectionnez le service VPN IPSec auquel vous souhaitez ajouter cette nouvelle session IPSec.

Note Si vous ajoutez cette session IPSec à partir de la boîte de dialogue **Ajouter les sessions IPSec**, le nom du service VPN est déjà indiqué au-dessus du bouton **Ajouter une session IPSec**.

- 6 Sélectionnez un point de terminaison local existant dans le menu déroulant.
 Cette valeur de point de terminaison local est requise et identifie le nœud NSX Edge local.
 Pour créer un point de terminaison local différent, cliquez sur le menu à trois points (⋮) et sélectionnez **Ajouter un point de terminaison local**.
- 7 Dans la zone de texte **Adresse IP distante**, entrez l'adresse IP du site distant.
 Cette valeur est requise.
- 8 Entrez une description facultative pour cette session VPN IPSec basé sur une route.
 La longueur maximale est de 1 024 caractères.
- 9 Pour activer ou désactiver la session IPSec, cliquez sur **Statut administratif**.
 Par défaut, la valeur est définie sur `Enabled`, ce qui signifie que la session IPSec doit être configurée jusqu'au nœud NSX Edge.
- 10 (Facultatif) Dans le menu déroulant **Suite de conformité**, sélectionnez une suite de conformité de sécurité.

Note La prise en charge de la suite de conformité est garantie à partir de la version NSX-T Data Center 2.5. Pour plus d'informations, reportez-vous à la section [À propos des suites de conformité prises en charge](#).

La valeur par défaut est définie sur `None`. Si vous sélectionnez une suite de conformité, le **mode d'authentification** est défini sur `Certificate` et dans la section **Propriétés avancées**, les valeurs de **Profil IKE** et **Profil IPSec** sont définies sur les profils définis par le système pour la suite de conformité sélectionnée. Il n'est pas possible de modifier ces profils définis par le système.

- 11 Entrez une adresse de sous-réseau IP dans **Interface de tunnel** selon la notation CIDR.

Cette adresse est requise.

- 12 Si la **Suite de conformité** est définie sur `None`, sélectionnez un mode dans le menu déroulant **Mode d'authentification**.

Le mode d'authentification par défaut utilisé est `PSK`, ce qui signifie qu'une clé secrète partagée entre NSX Edge et le site distant doit être utilisée pour la session VPN IPSec. Si vous sélectionnez `Certificate`, le certificat de site utilisé pour configurer le point de terminaison local est utilisé pour l'authentification.

- 13 Si vous avez sélectionné `PSK` pour le mode d'authentification, entrez la valeur de la clé dans la zone de texte **Clé prépartagée**.

La clé secrète peut être une chaîne d'une longueur maximale de 128 caractères.

Attention Soyez prudent lorsque vous partagez et stockez une valeur PSK, car elle contient des informations sensibles.

- 14 Entrez une valeur dans **ID distant**.

Pour les sites homologues qui utilisent l'authentification PSK, cette valeur d'ID doit être l'adresse IP publique ou le nom de domaine complet du site homologue. Pour les sites homologues utilisant l'authentification par certificat, cette valeur d'ID doit être le nom commun (CN) ou le nom unique (DN) figurant dans le certificat du site homologue.

Note Si le certificat du site homologue contient une adresse e-mail dans la chaîne DN, par exemple,

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123/emailAddress=user1@mycompany.com
```

entrez la valeur **ID distant** en utilisant le format suivant comme exemple.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, MAILTO=user1@mycompany.com"
```

Si le certificat du site local contient une adresse e-mail dans la chaîne DN et que le site homologue utilise l'implémentation IPsec strongSwan, entrez la valeur d'ID du site local dans ce site homologue. Vous en trouverez ci-dessous un exemple.

```
C=US, ST=California, O=MyCompany, OU=MyOrg, CN=Site123, E=user1@mycompany.com"
```

- 15 Si vous souhaitez inclure cette session IPSec dans le cadre de la balise d'un groupe spécifique, entrez le nom de la balise dans **Balises**.

- 16 Pour modifier les profils, le mode d'initialisation, le mode de restriction MSS TCP et les balises utilisées par la session VPN IPsec basée sur une route, cliquez sur **Propriétés avancées**.

Par défaut, les profils générés par le système sont utilisés. Sélectionnez un autre profil disponible si vous ne souhaitez pas utiliser la valeur par défaut. Pour utiliser un profil qui n'est pas encore configuré, cliquez sur le menu à trois points (⋮) pour créer un autre profil. Reportez-vous à la section [Ajout de profils](#).

- a Si le menu déroulant **Profils IKE** est activé, sélectionnez le profil IKE.
- b Sélectionnez le profil de tunnel IPsec, si le menu déroulant **Profils IPsec** n'est pas désactivé.
- c Sélectionnez le profil DPD préféré dans le menu déroulant **Profils DPD** est activé.
- d Sélectionnez le mode préféré à partir du menu déroulant **Mode d'initialisation de la connexion**.

Le mode d'initialisation de la connexion définit la stratégie utilisée par le point de terminaison local au cours du processus de création du tunnel. La valeur par défaut est **Initiateur**. Le tableau suivant décrit les différents modes d'initialisation de la connexion disponibles.

Tableau 5-3. Modes d'initialisation de la connexion

Mode d'initialisation de la connexion	Description
Initiator	Valeur par défaut. Dans ce mode, le point de terminaison local lance la création du tunnel VPN IPsec et répond aux demandes de configuration de tunnel entrantes provenant de la passerelle homologue.
On Demand	Ne pas utiliser avec le VPN basé sur une route. Ce mode s'applique uniquement au VPN basé sur les stratégies.
Respond Only	Le VPN IPsec ne lance jamais une connexion. Le site homologue initie toujours la demande de connexion et le point de terminaison local répond à celle-ci.

- 17 Pour réduire la charge utile de la taille de segment maximale (MSS) de la session TCP pendant la connexion IPsec, activez **Restriction MSS TCP**, sélectionnez la valeur de Direction **MSS TCP** et définissez éventuellement la **Valeur MSS TCP**. []

Pour plus d'informations, reportez-vous à la section [Présentation de la restriction MSS TCP](#).

- 18 Si vous souhaitez inclure cette session IPsec dans le cadre de la balise d'un groupe spécifique, entrez le nom de la balise dans **Balises**.
- 19 Cliquez sur **Enregistrer**.

Résultats

Lorsque la nouvelle session VPN IPsec basée sur une route est correctement configurée, elle est ajoutée à la liste des sessions VPN IPsec disponibles. Elle est en mode de lecture seule.

Étape suivante

- Vérifiez que l'état du tunnel VPN IPsec est Actif. Pour plus d'informations, reportez-vous à la section [Surveiller et dépanner des sessions VPN](#).
- Configurez le routage à l'aide d'une route statique ou d'un BGP. Voir [Configurer un itinéraire statique](#) ou [Configurer BGP](#).
- Si nécessaire, gérez les informations de la session VPN IPsec en cliquant sur le menu à trois points (⋮) à gauche de la ligne de la session. Sélectionnez l'une des actions que vous pouvez effectuer.

À propos des suites de conformité prises en charge

À partir de la version NSX-T Data Center 2.5, vous pouvez spécifier une suite de conformité de sécurité à utiliser pour configurer les profils de sécurité utilisés pour une session VPN IPsec.

Une suite de conformité de sécurité comprend des valeurs prédéfinies qui sont utilisées pour différents paramètres de sécurité et qui ne peuvent pas être modifiées. Lorsque vous sélectionnez une suite de conformité, les valeurs prédéfinies sont automatiquement utilisées pour le profil de sécurité de la session VPN IPsec que vous configurez.

Le tableau suivant répertorie les suites de conformité prises en charge pour les profils IKE dans NSX-T Data Center et les valeurs prédéfinies pour chacun.

Nom de la suite de conformité	Version IKE	Algorithme de chiffrement	Algorithme Digest	Groupe Diffie Hellman
CNSA	IKEv2	AES 256	SHA 2 384	Groupe 15, groupe 20
FIPS	IKE-Flex	AES 128	SHA 2 256	Groupe 20
Foundation	IKEv1	AES 128	SHA 2 256	Groupe 14
PRIME	IKEv2	AES GCM 128	Non défini	Groupe 19
Suite-B-GCM-128	IKEv2	AES 128	SHA 2 256	Groupe 19
Suite-B-GCM-256	IKEv2	AES 256	SHA 2 384	Groupe 20

Le tableau suivant répertorie les suites de conformité prises en charge pour les profils IPsec dans NSX-T Data Center et les valeurs prédéfinies pour chacun.

Nom de la suite de conformité	Algorithme de chiffrement	Algorithme Digest	Groupe PFS	Groupe Diffie-Hellman
CNSA	AES 256	SHA 2 384	Activé	Groupe 15, groupe 20
FIPS	AES GCM 128	Non défini	Activé	Groupe 20

Nom de la suite de conformité	Algorithme de chiffrement	Algorithme Digest	Groupe PFS	Groupe Diffie-Hellman
Foundation	AES 128	SHA 2 256	Activé	Groupe 14
PRIME	AES GCM 128	Non défini	Activé	Groupe 19
Suite-B-GCM-128	AES GCM 128	Non défini	Activé	Groupe 19
Suite-B-GCM-256	AES GCM 256	Non défini	Activé	Groupe 20

Présentation de la restriction MSS TCP

La restriction MSS TCP vous permet de réduire la valeur de taille maximale de segment (MSS) utilisée par une session TCP lors de l'établissement de la connexion via un tunnel IPsec. Cette fonctionnalité est prise en charge à partir de la version NSX-T Data Center 2.5.

MSS TCP représente la quantité maximale de données en octets qu'un hôte est disposé à accepter dans un segment TCP unique. Chaque extrémité d'une connexion TCP envoie la valeur MSS souhaitée à son homologue pendant une liaison à trois voies, où MSS est l'une des options d'en-tête TCP utilisées dans un paquet TCP SYN. MSS TCP est calculé en fonction de l'unité de transmission maximale (MTU) de l'interface de sortie de l'hôte émetteur.

Lorsqu'un trafic TCP passe par un VPN IPsec ou tout type de tunnel VPN, des en-têtes supplémentaires sont ajoutés au paquet d'origine pour en garantir la sécurité. Pour le mode tunnel IPsec, les en-têtes supplémentaires utilisés sont IP, ESP et éventuellement UDP (si la traduction du port est présente sur le réseau). En raison de ces en-têtes supplémentaires, la taille du paquet encapsulé est supérieure à celle de la MTU de l'interface VPN. Le paquet peut être fragmenté ou abandonné en fonction de la stratégie DF.

Pour éviter la fragmentation ou l'abandon des paquets, vous pouvez ajuster la valeur MSS pour la session IPsec en activant la fonctionnalité de restriction MSS TCP. Accédez à **Mise en réseau > VPN > Sessions IPsec**. Lorsque vous ajoutez une session IPsec ou que vous modifiez une session existante, développez la section **Propriétés avancées** et activez **Restriction MSS TCP**.

Vous pouvez configurer la valeur MSS précalculée adaptée à la session IPsec en définissant les paramètres **Direction MSS TCP** et **Valeur MSS TCP**. La valeur MSS configurée est utilisée pour la restriction MSS. Vous pouvez, si vous le souhaitez, utiliser le calcul MSS dynamique en définissant le paramètre **Direction MSS TCP** et en laissant le paramètre **Valeur MSS TCP** vide. La valeur MSS est calculée automatiquement en fonction de la MTU de l'interface VPN, de la capacité supplémentaire du VPN et de la MTU de chemin (PMTU) lorsqu'elle est déjà déterminée. La valeur MSS effective est recalculée pendant chaque liaison TCP pour gérer les modifications de MTU ou de PMTU de façon dynamique.

Ajout de sessions VPN L2

Une fois que vous avez configuré un serveur VPN L2 et un client VPN L2, vous devez ajouter des sessions VPN L2 pour les deux afin de terminer la configuration du service VPN L2.

Ajouter une session de serveur VPN L2

Après avoir créé un service de serveur VPN L2, vous devez ajouter une session VPN L2 et l'associer à un segment existant.

Les étapes suivantes utilisent l'onglet **Sessions VPN de couche 2** dans l'interface utilisateur de NSX Manager pour créer une session de serveur VPN L2. Vous sélectionnez également un point de terminaison local et un segment existants à attacher à la session de serveur VPN L2.

Note Vous pouvez également ajouter une session de serveur VPN L2 immédiatement après avoir correctement configuré le service de serveur VPN L2. Vous cliquez sur **Oui** lorsque vous êtes invité à poursuivre la configuration du serveur VPN L2, puis sélectionnez **Sessions > Ajouter des sessions** dans le panneau Ajouter un serveur VPN L2. Les premières étapes de la procédure suivante supposent que vous avez sélectionné **Non** à l'invite vous demandant de poursuivre la configuration du serveur VPN L2. Si vous avez sélectionné **Oui**, passez à l'étape 3 dans les étapes suivantes, qui vous guideront dans le reste de la configuration d'une session de serveur VPN L2.

Conditions préalables

- Vous devez avoir configuré un service de serveur VPN L2 avant de continuer. Reportez-vous à la section [Ajouter un service serveur VPN de couche 2](#).
- Obtenez les informations pour le point de terminaison local et l'adresse IP distante à utiliser avec la session de serveur VPN L2 que vous ajoutez. Pour créer un point de terminaison local, reportez-vous à la section [Ajouter des points de terminaison locaux](#).
- Obtenez les valeurs de la clé prépartagée (PSK) et du sous-réseau d'interface de tunnel à utiliser avec la session du serveur VPN L2.
- Obtenez le nom du segment existant que vous souhaitez associer à la session de serveur VPN L2 que vous créez. Pour plus d'informations, reportez-vous à la section [Ajouter un segment](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Accédez à l'onglet **Mise en réseau > VPN > Sessions VPN de couche 2**.
- 3 Sélectionnez **Ajouter une session VPN de couche 2 > Serveur VPN de couche 2**.
- 4 Entrez un nom pour la session du serveur VPN L2.
- 5 Dans le menu déroulant **Service VPN de couche 2**, sélectionnez le service du serveur VPN L2 pour lequel la session VPN L2 est créée.

Note Si vous ajoutez cette session de serveur VPN L2 à partir de la boîte de dialogue Définir des sessions de serveur L2VPN, le service du serveur VPN L2 est déjà indiqué au-dessus du bouton **Ajouter une session de couche 2**.

- 6 Sélectionnez un point de terminaison local existant dans le menu déroulant.

Si vous souhaitez créer un point de terminaison local différent, cliquez sur le menu à trois points (⋮) et sélectionnez **Ajouter un point de terminaison local**.

- 7 Entrez l'adresse IP du site distant.

- 8 Pour activer ou désactiver la session de serveur VPN de couche 2, cliquez sur **État administratif**.

Par défaut, la valeur est définie sur **Activé**, ce qui signifie que la session de serveur VPN de couche 2 doit être configurée jusqu'au nœud NSX Edge.

- 9 Entrez la valeur de clé secrète dans **Clé prépartagée**.

Attention Soyez prudent lorsque vous partagez et stockez une valeur PSK, car elle contient des informations sensibles.

- 10 Entrez une adresse de sous-réseau IP dans **Interface de tunnel** selon la notation CIDR.

Par exemple, 4.5.6.6/24. Cette adresse de sous-réseau est requise.

- 11 Entrez une valeur dans **ID distant**.

Pour les sites homologues utilisant l'authentification par certificat, cet ID doit être le nom commun figurant dans le certificat du site homologue. Pour les homologues PSK, cet ID peut être une chaîne. Utilisez de préférence l'adresse IP publique du VPN ou un nom de domaine qualifié complet (FQDN) pour les services VPN comme `Remote ID`.

- 12 Si vous souhaitez inclure cette session dans le cadre d'un groupe spécifique, entrez le nom de la balise dans **Balises**.

- 13 Cliquez sur **Enregistrer** et sur **Oui** lorsque vous y êtes invité si vous souhaitez poursuivre avec la configuration du service VPN.

Vous revenez au panneau Ajouter des sessions L2VPN et le lien **Segments** est désormais activé.

- 14 Connectez un segment existant à la session de serveur VPN L2.

- a Cliquez sur **Segments > Définir les segments**.
- b Dans la boîte de dialogue **Définir les segments**, cliquez sur **Définir le segment** pour attacher un segment existant à la session de serveur VPN L2.
- c Dans le menu déroulant **Segment**, sélectionnez le segment VNI ou le segment VLAN que vous souhaitez attacher à la session.
- d Entrez une valeur unique dans **ID de tunnel VPN** ; elle servira à identifier le segment que vous avez sélectionné.
- e Cliquez sur **Enregistrer** et sur **Fermer**.

Dans le volet ou la boîte de dialogue Définir les sessions L2VPN, le système a incrémenté le nombre de **Segments** pour la session de serveur VPN L2.

- 15 Pour terminer la configuration de la session de serveur VPN L2, cliquez sur **Fermer la modification**.

Résultats

Dans l'onglet **Services VPN**, le système a incrémenté le nombre de **Sessions** pour le service de serveur VPN L2 que vous avez configuré.

Étape suivante

Pour terminer la configuration du service VPN L2, vous devez également créer un service VPN L2 en mode Client et une session de client VPN L2. Reportez-vous aux sections [Ajouter un service client VPN L2](#) et [Ajouter une session client VPN de couche 2](#).

Ajouter une session client VPN de couche 2

Vous devez ajouter une session client VPN de couche 2 après la création d'un service client VPN de couche 2 et l'associer à un segment existant.

Les étapes suivantes utilisent l'onglet **Sessions VPN de couche 2** de l'interface utilisateur de NSX Manager pour créer une session client VPN de couche 2. Vous sélectionnez également un point de terminaison local et un segment existants à attacher à la session client VPN de couche 2.

Note Vous pouvez également ajouter une session client VPN de couche 2 immédiatement après avoir configuré correctement le service client VPN de couche 2. Cliquez sur **Oui** lorsque vous êtes invité à poursuivre la configuration du client VPN de couche 2, puis sélectionnez **Sessions > Ajouter des sessions** dans le panneau Ajouter un client VPN de couche 2. Les premières étapes de la procédure suivante supposent que vous avez sélectionné **Non** lorsque vous êtes invité à continuer la configuration du client VPN de couche 2. Si vous sélectionnez **Oui**, passez à l'étape 3 dans les étapes suivantes pour être guidé dans le reste de la configuration de la session client VPN de couche 2.

Conditions préalables

- Vous devez avoir configuré un service client VPN de couche 2 avant de continuer. Reportez-vous à la section [Ajouter un service client VPN L2](#).
- Obtenez les informations des adresses IP pour l'adresse IP locale et l'adresse IP distante à utiliser avec la session client VPN de couche 2 en cours d'ajout.
- Obtenez le code d'homologue qui a été généré lors de la configuration du serveur VPN de couche 2. Reportez-vous à la section [Télécharger le fichier de configuration du VPN de couche 2 côté distant](#).
- Obtenez le nom du segment existant que vous souhaitez joindre à la session client VPN de couche 2 en cours de création. Reportez-vous à la section [Ajouter un segment](#).

Procédure

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

- 2 Sélectionnez **Mise en réseau > VPN > Sessions VPN de couche 2**.
- 3 Sélectionnez **Ajouter une session VPN de couche 2 > Client VPN de couche 2**.
- 4 Entrez le nom de la session client VPN de couche 2.
- 5 Dans le menu déroulant **Service VPN**, sélectionnez le service client VPN de couche 2 avec lequel la session VPN de couche 2 doit être associée.

Note Si vous ajoutez cette session de client VPN de couche 2 à partir de la boîte de dialogue Définir les sessions Client VPN de couche 2, le service client VPN de couche 2 est déjà indiqué au-dessus du bouton **Ajouter une session de couche 2**.

- 6 Dans la zone de texte **Adresse IP locale**, entrez l'adresse IP de la session client VPN de couche 2.
- 7 Entrez l'adresse IP distante du tunnel IPSec à utiliser pour la session client VPN de couche 2.
- 8 Dans la zone de texte **Configuration de l'homologue**, entrez le code d'homologue généré lorsque vous avez configuré le service serveur VPN de couche 2.
- 9 Activez ou désactivez **Statut administratif**.
Par défaut, la valeur est définie sur **Activé**, ce qui signifie que la session de serveur VPN de couche 2 doit être configurée jusqu'au nœud NSX Edge.
- 10 Cliquez sur **Enregistrer** et sur **Oui** lorsque vous y êtes invité si vous souhaitez poursuivre avec la configuration du service VPN.
- 11 Attachez un segment existant à la session client VPN de couche 2.
 - a Sélectionnez **Segments > Ajouter des segments**.
 - b Dans la boîte de dialogue **Définir les segments**, cliquez sur **Ajouter un segment**.
 - c Dans le menu déroulant **Segment**, sélectionnez le segment VNI ou le segment VLAN que vous souhaitez attacher à la session serveur VPN de couche 2.
 - d Entrez une valeur unique dans **ID de tunnel VPN** ; elle servira à identifier le segment que vous avez sélectionné.
 - e Cliquez sur **Fermer**.
- 12 Pour terminer la configuration de la session client VPN de couche 2, cliquez sur **Fermer la modification**.

Résultats

Dans l'onglet **Services VPN**, le nombre de sessions est mis à jour pour le service client VPN de couche 2 que vous avez configuré.

Télécharger le fichier de configuration du VPN de couche 2 côté distant

Pour configurer la session de client VPN L2, vous devez obtenir le code d'homologue qui a été généré lorsque vous avez configuré la session de serveur VPN L2.

Conditions préalables

- Pour continuer, vous devez avoir configuré avec succès un service de serveur VPN L2 et une session. Reportez-vous à la section [Ajouter un service serveur VPN de couche 2](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Accédez à l'onglet **Mise en réseau > VPN > Sessions VPN de couche 2**.
- 3 Dans le tableau des sessions VPN L2, développez la ligne correspondant à la session de serveur VPN L2 que vous prévoyez d'utiliser pour la configuration de session de client VPN L2.
- 4 Cliquez sur **Télécharger la configuration** et cliquez sur **Oui** dans la boîte de dialogue Avertissement.

Un fichier texte portant le nom `L2VPNSession_<nom-de-session-serveur-VPN-L2>_config.txt` est téléchargé. Il contient le code d'homologue pour la configuration du VPN L2 côté distant.

Attention Soyez prudent lorsque vous stockez et partagez le code homologue, car il contient une valeur PSK qui est considérée comme une information sensible.

Par exemple, `L2VPNSession L2VPNServer config.txt` contient la configuration suivante.

```
[
{
    "transport_tunnel_path": "/infra/tier-0s/ServerT0_AS/locale-services/1-policyconnectivity-693/ipsec-vpn-services/Ipservice1/sessions/Routebase1",
    "peer_code":
        "MCw3ZjBjYzdjLHsic2l0ZU5hbWUiOiJSb3V0ZWJhc2UxIiwic3JjVGFWsXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYXBjcCI6IjE2OS4yNTQuNjQuMSIsImlrZU9wdG1vbiI6ImlrZXxyYiwiZW5jYXBQcm90byI6ImdyZS9pcHNlYyIsImRoR3JvdXAiOiJkaDE0IiwizW5jcmlwdEFuZERpZ2VzdCI6ImFlcylnY20vc2hhLTl1NiIsInBzayI6IlZNd2FyZTEyMyIsInRlbm5lbHMiolTI7ImxvY2FsSWQiOiI2MC42MC42MC4xIiwicGVlc2klkIjoINTAuNTAuNTAuMSIsImxvY2FsVnRpSXAIoiIxNjkuMi4yLjMzMzEifV19"
}
]
```

- 5 Copiez le code homologue que vous utilisez pour configurer le service client et la session VPN de couche 2.

À partir de l'exemple de fichier de configuration précédent, le code homologue suivant est celui que vous copiez pour l'utiliser avec la configuration du client VPN de couche 2.

```
MCw3ZjBjYzdjLHsic210ZU5hbWUiOiJSb3V0ZWJhc2UxIiwic3JjVGFwSXAiOiIxNjkuMjU0LjY0LjIiLCJkc3RUYXB  
JcCI6IjE2OS4yNTQuNjQuMSIsImlrZU9wdG1  
vbiI6ImlrZXZyYiwiZW5jYXBQcm90byI6ImdyZS9pcHNlYyIsImRoR3JvdXAiOiJkaDE0IiwiZW5jcnlwdEFuZERpZ2  
VzdCI6ImFlcylnY20vc2hhLTIiNiIsInBzayI  
6IlZNd2FyZTEyMyIsInR1bm5lbHMt7ImxvY2FsSWQiOiI2MC42MC42MC4xIiwicGVlcklkIjoINTAuNTAuNTAuMS  
IsImxvY2FsVnRwSXAiOiIxNjkuMi4yLjMvMzEifV19
```

Étape suivante

Configurez le service et la session de client VPN L2. Reportez-vous aux sections [Ajouter un service client VPN L2](#) et [Ajouter une session client VPN de couche 2](#).

Ajouter des points de terminaison locaux

Vous devez configurer un point de terminaison local qui sera utilisé avec le VPN IPsec que vous configurez.

Les étapes suivantes utilisent l'onglet **Points de terminaison locaux** dans l'interface utilisateur de NSX Manager. Vous pouvez également créer un point de terminaison local lors du processus d'ajout d'une session VPN IPsec en cliquant sur le menu à trois points (⋮) et en sélectionnant **Ajouter un point de terminaison local**. Si vous êtes en cours de configuration d'une session VPN IPsec, passez à l'étape 3 dans les étapes suivantes, qui vous guideront dans la création d'un nouveau point de terminaison local.

Conditions préalables

- Si vous utilisez un mode d'authentification par certificat pour la session VPN IPsec qui doit utiliser le point de terminaison local que vous configurez, obtenez des informations sur le certificat que le point de terminaison local doit utiliser.
- Assurez-vous d'avoir configuré un service VPN IPsec auquel ce point de terminaison local doit être associé.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Accédez à **Mise en réseau > VPN > Points de terminaison locaux** et cliquez sur **Ajouter un point de terminaison local**.
- 3 Entrez le nom du point de terminaison local.
- 4 Dans le menu déroulant **Service VPN**, sélectionnez le service client VPN IPsec auquel le point de terminaison local doit être associé.

5 Entrez une adresse IP pour le point de terminaison local.

Pour un service VPN IPsec exécuté sur une passerelle de niveau 0, l'adresse IP du point de terminaison local doit être différente de l'adresse IP de l'interface de liaison montante de la passerelle de niveau 0. L'adresse IP du point de terminaison local que vous saisissez est associée à l'interface de bouclage pour la passerelle de niveau 0 et est également publiée en tant qu'adresse IP routable sur l'interface de liaison montante. Pour le service VPN IPsec exécuté sur une passerelle de niveau 1, l'annonce de route pour les points de terminaison locaux IPsec doit être activée dans la configuration de la passerelle de niveau 1 pour que l'adresse IP du point de terminaison local soit routable. Pour plus d'informations, reportez-vous à la section [Ajouter une passerelle de niveau 1](#).

6 Si vous utilisez un mode d'authentification par certificat pour la session VPN IPsec, dans le menu déroulant **Certificat de site**, sélectionnez le certificat qui doit être utilisé par le point de terminaison local.

7 (Facultatif) Vous pouvez éventuellement ajouter une description dans **Description**.

8 Entrez la valeur **ID local** qui est utilisée pour identifier l'instance locale de NSX Edge.

Cet ID local est l'ID homologue sur le site distant. L'ID local doit être l'adresse IP publique ou le nom de domaine complet du site distant. Pour les sessions VPN basées sur des certificats définies à l'aide du point de terminaison local, l'ID local est dérivé du certificat associé au point de terminaison local. L'ID spécifié dans la zone de texte **ID local** est ignoré. L'ID local dérivé du certificat pour une session VPN dépend des extensions présentes dans le certificat.

- Si l'extension X509v3 `X509v3 Subject Alternative Name` n'est pas présente dans le certificat, le nom unique (DN) est utilisé comme valeur d'ID locale.
- Si l'extension X509v3 `X509v3 Subject Alternative Name` est trouvée dans le certificat, l'un des autres noms de l'objet est pris comme valeur d'ID locale.

9 Dans **Certificats d'autorité de certification approuvés** et **Liste de révocation de certificats**, sélectionnez les certificats appropriés qui sont nécessaires pour le point de terminaison local.

10 Spécifiez une balise, si nécessaire.

11 Cliquez sur **Enregistrer**.

Ajout de profils

NSX-T Data Center fournit le profil du tunnel IPsec généré par le système et le profil IKE qui sont attribuées par défaut lorsque vous configurez un service VPN IPsec ou un service VPN de couche 2. Un profil DPD généré par le système est créé pour la configuration d'un VPN IPsec.

Les profils IKE et IPsec fournissent des informations sur les algorithmes utilisés pour authentifier, chiffrer et établir un secret partagé entre les sites du réseau. Le profil DPD fournit des informations sur le nombre de secondes à attendre entre chaque sonde.

Si vous décidez de ne pas utiliser les profils par défaut fournis par NSX-T Data Center, vous pouvez configurer votre propre profil à l'aide des informations contenues dans les rubriques qui suivent cette section.

Ajouter des profils IKE

Les profils IKE (Internet Key Exchange) fournissent des informations sur les algorithmes utilisés pour authentifier, chiffrer et établir un secret partagé entre les sites du réseau lorsque vous établissez un tunnel IKE.

NSX-T Data Center fournit des profils IKE générés par le système qui sont attribuées par défaut lorsque vous configurez un service VPN IPSec ou VPN de couche 2. Le tableau suivant répertorie les profils par défaut fournis.

Tableau 5-4. Profils IKE par défaut utilisés pour les services VPN IPSec ou VPN de couche 2

Nom du profil IKE par défaut	Description
nsx-default-l2vpn-ike-profile	<ul style="list-style-type: none"> ■ Utilisé pour la configuration d'un service VPN de couche 2. ■ Configuré avec le protocole IKE V2, un algorithme de chiffrement AES 128, un algorithme SHA2 256 et un algorithme d'échange de clés de groupe 14 de Diffie-Hellman.
nsx-default-l3vpn-ike-profile	<ul style="list-style-type: none"> ■ Utilisé pour la configuration d'un service VPN IPSec. ■ Configuré avec le protocole IKE V2, un algorithme de chiffrement AES 128, un algorithme SHA2 256 et un algorithme d'échange de clés de groupe 14 de Diffie-Hellman.

Au lieu des profils IKE par défaut utilisés, vous pouvez également sélectionner l'une des suites de conformité prises en charge à partir de la version NSX-T Data Center 2.5. Pour plus d'informations, reportez-vous à la section [À propos des suites de conformité prises en charge](#).

Si vous décidez de ne pas utiliser les profils IKE par défaut ou les suites de conformité par défaut fournis, vous pouvez configurer votre propre profil IKE à l'aide de la procédure suivante.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Cliquez sur l'onglet **Mise en réseau > VPN > Profils**.
- 3 Sélectionnez le type de profil **Profils IKE** et cliquez sur **Ajouter un profil IKE**.
- 4 Entrez un nom pour le profil IKE.

- 5 Dans le menu déroulant **Version IKE**, sélectionnez la version IKE à utiliser pour configurer une association de sécurité (SA) dans la suite de protocoles IPSec.

Tableau 5-5. Versions IKE

Version IKE	Description
IKEv1	Lorsqu'il est sélectionné, le VPN IPSec initie et répond au protocole IKEv1 uniquement.
IKEv2	Il s'agit de la version par défaut. Lorsqu'il est sélectionné, le VPN IPSec initie et répond au protocole IKEv2 uniquement.
IKE-Flex	Si cette version est sélectionnée et si l'établissement de tunnel échoue avec le protocole IKEv2, le site source ne se rétablit pas et n'établit pas de connexion avec le protocole IKEv1. En revanche, si le site distant initie une connexion avec le protocole IKEv1, la connexion est acceptée.

- 6 Sélectionnez les algorithmes de chiffrement, Digest et du groupe Diffie-Hellman dans les menus déroulants. Vous pouvez sélectionner plusieurs algorithmes pour les appliquer ou désélectionner tous les algorithmes que vous ne souhaitez pas appliquer.

Tableau 5-6. Algorithmes utilisés

Type d'algorithme	Valeurs valides	Description
Chiffrement	<ul style="list-style-type: none"> ■ AES 128 (par défaut) ■ AES 256 ■ AES GCM 128 ■ AES GCM 192 ■ AES GCM 256 	<p>L'algorithme de chiffrement utilisé lors de la négociation IKE (Internet Key Exchange).</p> <p>Les algorithmes AES-GCM sont pris en charge lorsqu'ils sont utilisés avec IKEv2. Ils ne sont pas pris en charge lorsqu'ils sont utilisés avec IKEv1.</p>
Digest	<ul style="list-style-type: none"> ■ SHA2 256 (par défaut) ■ SHA 1 ■ SHA2 384 ■ SHA2 512 	<p>L'algorithme de hachage sécurisé utilisé lors de la négociation IKE.</p> <p>Si AES-GCM est le seul algorithme de chiffrement sélectionné dans la zone de texte Algorithme de chiffrement, aucun algorithme de hachage ne peut être spécifié dans la zone de texte Algorithme Digest, conformément à la section 8 de RFC 5282. De plus, l'algorithme Pseudo-Random Function (PRF, fonction pseudo-aléatoire) PRF-HMAC-SHA2-256 est implicitement sélectionné et utilisé dans la négociation de l'association de sécurité (SA) IKE. L'algorithme PRF-HMAC-SHA2-256 doit également être configuré sur la passerelle homologue afin que la phase 1 de la négociation de la SA IKE aboutisse.</p> <p>Si d'autres algorithmes sont spécifiés dans la zone de texte Algorithme de chiffrement, en plus de l'algorithme AES-GCM, un ou plusieurs algorithmes de hachage peuvent être sélectionnés dans la zone de texte Algorithme Digest. De plus, l'algorithme PRF utilisé dans la négociation de la SA IKE est implicitement déterminé en fonction des algorithmes de hachage configurés. Au moins l'un des algorithmes PRF correspondants doit également être configuré sur la passerelle homologue pour que la phase 1 de la négociation de la SA IKE aboutisse. Par exemple, si la zone de texte Algorithme de chiffrement contient AES 128 et AES GCM 128. Aussi, SHA1 est spécifié dans la zone de texte Algorithme Digest, puis l'algorithme PRF-HMAC-SHA1 est utilisé lors de la négociation SA IKE. Il doit également être configuré dans la passerelle homologue.</p>
Groupe Diffie-Hellman	<ul style="list-style-type: none"> ■ Groupe 14 (par défaut) ■ Groupe 2 ■ Groupe 5 ■ Groupe 15 ■ Groupe 16 ■ Groupe 19 ■ Groupe 20 	<p>Les schémas de chiffrement utilisés par le site homologue et le dispositif NSX Edge pour établir un secret partagé sur un canal de communication non sécurisé.</p>

Tableau 5-6. Algorithmes utilisés (suite)

Type d'algorithme	Valeurs valides	Description
	■ Groupe 21	

Note Lorsque vous tentez d'établir un tunnel VPN IPSec avec un client VPN GUARD (précédemment client VPN QuickSec) à l'aide de deux algorithmes de chiffrement ou de deux algorithmes Digest, le client VPN GUARD ajoute des algorithmes supplémentaires dans la liste de négociation proposée. Par exemple, si vous avez spécifié AES 128 et AES 256 comme algorithmes de chiffrement et SHA2 256 et SHA2 512 comme algorithmes Digest à utiliser dans le profil IKE que vous utilisez pour établir le tunnel VPN IPSec, le client VPN GUARD propose également AES 192 et SHA2 384 dans la liste de négociation. Dans ce cas, NSX-T Data Center utilise le premier algorithme de chiffrement que vous avez sélectionné lors de l'établissement du tunnel VPN IPSec.

- 7 Entrez une valeur de durée de vie pour l'association de sécurité (SA), en secondes, si vous souhaitez qu'elle soit différente de la valeur par défaut de 86 400 secondes (24 heures).
- 8 Fournissez une description et ajoutez une balise, si nécessaire.
- 9 Cliquez sur **Enregistrer**.

Résultats

Une nouvelle ligne est ajoutée au tableau de profils IKE disponibles. Pour modifier ou supprimer un profil non système, cliquez sur le menu en points de suspension (⋮) et sélectionnez une action dans la liste des actions disponibles.

Ajouter des profils IPSec

Les profils IPSec (Internet Protocol Security) fournissent des informations sur les algorithmes utilisés pour authentifier, chiffrer et établir un secret partagé entre les sites du réseau lorsque vous établissez un tunnel IPSec.

NSX-T Data Center fournit des profils IPSec générés par le système qui sont attribuées par défaut lorsque vous configurez un service VPN IPSec ou VPN de couche 2. Le tableau suivant répertorie les profils IPSec par défaut fournis.

Tableau 5-7. Profils IPSec par défaut utilisés pour les services VPN IPSec ou VPN de couche 2

Nom du profil IPSec par défaut	Description
nsx-default-l2vpn-tunnel-profile	<ul style="list-style-type: none"> ■ Utilisé pour le VPN de couche 2. ■ Configuré avec un algorithme de chiffrement AES GCM 128 et un algorithme d'échange de clés de groupe 14 de Diffie-Hellman.
nsx-default-l3vpn-tunnel-profile	<ul style="list-style-type: none"> ■ Utilisé pour le VPN IPSec. ■ Configuré avec un algorithme de chiffrement AES GCM 128 et un algorithme d'échange de clés de groupe 14 Diffie-Hellman.

Au lieu du profil IPSec par défaut, vous pouvez également sélectionner l'une des suites de conformité prises en charge à partir de la version NSX-T Data Center 2.5. Pour plus d'informations, reportez-vous à la section [À propos des suites de conformité prises en charge](#).

Si vous décidez de ne pas utiliser les profils IPSec ou les suites de conformité par défaut fournis, vous pouvez configurer votre propre profil à l'aide de la procédure suivante.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Accédez à l'onglet **Mise en réseau > VPN > Profils**.
- 3 Sélectionnez le type de profil **Profils IPSec** et cliquez sur **Ajouter un profil IPSec**.
- 4 Entrez un nom pour le profil IPSec.
- 5 Sélectionnez les algorithmes de chiffrement, Digest et Diffie-Hellman dans les menus déroulants. Vous pouvez sélectionner plusieurs algorithmes à appliquer.
Désélectionnez ceux que vous ne voulez pas utiliser.

Tableau 5-8. Algorithmes utilisés

Type d'algorithme	Valeurs valides	Description
Chiffrement	<ul style="list-style-type: none"> ■ AES GCM 128 (par défaut) ■ AES 128 ■ AES 256 ■ AES GCM 192 ■ AES GCM 256 ■ Aucune authentification de chiffrement AES GMAC 128 ■ Aucune authentification de chiffrement AES GMAC 192 ■ Aucune authentification de chiffrement AES GMAC 256 ■ Aucun chiffrement 	L'algorithme de chiffrement utilisé lors de la négociation Internet Protocol Security (IPSec).
Digest	<ul style="list-style-type: none"> ■ SHA 1 ■ SHA 2 256 ■ SHA 2 384 ■ SHA 2 512 	L'algorithme de hachage sécurisé utilisé lors de la négociation IPSec.
Groupe Diffie-Hellman	<ul style="list-style-type: none"> ■ Groupe 14 (par défaut) ■ Groupe 2 ■ Groupe 5 ■ Groupe 15 ■ Groupe 16 ■ Groupe 19 ■ Groupe 20 ■ Groupe 21 	Les schémas de chiffrement utilisés par le site homologue et le dispositif NSX Edge pour établir un secret partagé sur un canal de communication non sécurisé.

- 6 Désélectionnez l'option **Groupe PFS** si vous décidez de ne pas utiliser le protocole de groupe PFS sur votre service VPN.

Cette option est sélectionnée par défaut.

- 7 Dans la zone de texte **Durée de vie de la SA**, modifiez le nombre de secondes par défaut avant que le tunnel IPSec soit rétabli.

Par défaut, une durée de vie de la SA de 24 heures (86 400 secondes) est utilisée.

- 8 Sélectionnez la valeur du **Bit DF** à utiliser avec le tunnel IPSec.

Cette valeur détermine comment gérer le bit « DF (ne pas fragmenter) » inclus dans le paquet de données reçu. Les valeurs acceptées sont décrites dans le tableau suivant.

Tableau 5-9. Valeurs du bit DF

Valeur du bit DF	Description
COPY	Valeur par défaut. Lorsque cette valeur est sélectionnée, NSX-T Data Center copie la valeur du bit DF depuis le paquet reçu vers le paquet transmis. Cette valeur signifie que si le bit DF est défini sur le paquet de données reçu, alors le bit DF est également défini sur le paquet après le chiffrement.
CLEAR	Lorsque cette valeur est sélectionnée, NSX-T Data Center ignore la valeur du bit DF dans le paquet de données reçu et le bit DF est toujours défini sur 0 dans le paquet chiffré.

9 Fournissez une description et ajoutez une balise, si nécessaire.

10 Cliquez sur **Enregistrer**.

Résultats

Une nouvelle ligne est ajoutée au tableau de profils IPsec disponibles. Pour modifier ou supprimer un profil non système, cliquez sur le menu en points de suspension (⋮) et sélectionnez une action dans la liste des actions disponibles.

Ajouter des profils DPD

Un profil DPD (Dead Peer Detection) fournit des informations sur le nombre de secondes nécessaires à la détection de l'activité d'un homologue IPsec entre chaque interrogation.

NSX-T Data Center offre un profil DPD généré par le système, nommé `nsx-default-l3vpn-dpd-profile`, attribué par défaut lorsque vous configurez un service VPN IPsec.

Si vous décidez de ne pas utiliser le profil DPD par défaut fourni, vous pouvez configurer votre profil en exécutant les étapes suivantes.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Accédez à **Mise en réseau > VPN > Profils**.
- 3 Sélectionnez le type de profil **Profils DPD** et cliquez sur **Ajouter un profil DPD**.
- 4 Entrez un nom pour le profil DPD.
- 5 Dans la zone de texte **Intervalle de détection DPD**, entrez le nombre de secondes pendant lesquelles NSX-T Data Center doit attendre avant d'envoyer la détection DPD suivante. La valeur par défaut est de 60 secondes.

Si le nœud NSX Edge reçoit une réponse du site homologue distant, le temporisateur de l'intervalle de détection DPD est redémarré. Si le nœud NSX Edge ne reçoit pas de réponse du site homologue dans les 0,5 seconde après l'envoi de la détection DPD suivante, un temporisateur de retransmission est défini sur 0,5 seconde. Le nœud NSX Edge retransmet la détection DPD suivante après l'expiration du temporisateur de retransmission.

Si le site homologue distant ne répond toujours pas, le temporisateur de retransmission est augmenté de manière exponentielle jusqu'à la limite maximale de 6 secondes. Le nœud NSX Edge continue de retransmettre la détection DPD chaque fois que le temporisateur de retransmission expire. Le nœud NSX Edge retransmet jusqu'à 30 fois maximum avant de déclarer le site homologue inactif et d'annuler l'association de sécurité (SA) sur le lien de l'homologue mort. Le temps total nécessaire pour retransmettre la détection DPD 30 fois est d'environ 2 minutes et 45 secondes.

6 Fournissez une description et ajoutez une balise, si nécessaire.

7 Cliquez sur **Enregistrer**.

Résultats

Une nouvelle ligne est ajoutée au tableau des profils DPD disponibles. Pour modifier ou supprimer un profil non système, cliquez sur le menu en points de suspension (⋮) et sélectionnez une action dans la liste des actions disponibles.

Ajouter un dispositif Edge autonome en tant que client VPN L2

Vous pouvez utiliser un VPN L2 pour étendre vos réseaux de couche 2 à un site qui n'est pas géré par NSX-T Data Center. Un dispositif NSX Edge autonome peut être déployé sur le site en tant que client VPN L2. Le dispositif NSX Edge autonome est simple à déployer, facile à programmer et fournit un VPN haute performance. Le dispositif NSX Edge autonome est déployé à l'aide d'un fichier OVF sur un hôte non géré par NSX-T Data Center. Vous pouvez également activer HA pour la redondance VPN en déployant des clients Edge VPN L2 autonomes principaux et secondaires.

Conditions préalables

- Créez un groupe de ports et liez-le au vSwitch sur votre hôte.
- Créez un groupe de ports pour votre port d'extension L2 interne.
- Obtenez les adresses IP pour l'adresse IP locale et l'adresse IP distante à utiliser avec la session client VPN L2 en cours d'ajout.
- Obtenez le code d'homologue qui a été généré lors de la configuration du serveur VPN de couche 2.

Procédure

- 1 À l'aide de vSphere Web Client, connectez-vous à l'instance de vCenter Server qui gère l'environnement non-NSX.
- 2 Sélectionnez **Hôtes et clusters**, puis développez les clusters pour afficher les hôtes disponibles.
- 3 Cliquez avec le bouton droit sur l'hôte sur lequel vous souhaitez installer le dispositif NSX Edge autonome et sélectionnez **Déployer le modèle OVF**.

- 4 Entrez l'URL pour télécharger et installer le fichier OVF à partir d'Internet ou cliquez sur **Parcourir** pour accéder au dossier de l'ordinateur qui contient le fichier OVF NSX Edge autonome, puis cliquez sur **Suivant**.
- 5 Sur la page **Sélectionner un nom et un dossier**, entrez un nom pour le dispositif NSX Edge autonome et sélectionnez le dossier ou le centre de données dans lequel vous souhaitez effectuer le déploiement. Cliquez ensuite sur **Suivant**.
- 6 Sur la page **Sélectionner une ressource de calcul**, sélectionnez la destination de la ressource de calcul.
- 7 Sur la page Détails de modèle OVF, passez en revue les détails du modèle et cliquez sur **Suivant**.
- 8 Sur la page **Configuration**, sélectionnez une option de configuration de déploiement.
- 9 Sur la page **Sélectionner un stockage**, sélectionnez l'emplacement dans lequel stocker les fichiers disque et les fichiers de configuration.
- 10 Sur la page **Sélectionner les réseaux**, configurez les réseaux que le modèle déployé doit utiliser. Sélectionnez le groupe de ports que vous avez créé pour l'interface de liaison montante, le groupe de ports que vous avez créé pour le port d'extension L2, puis entrez une interface HA. Cliquez sur **Suivant**.
- 11 Sur la page **Personnaliser le modèle**, entrez les valeurs suivantes et cliquez sur **Suivant**.
 - a Composez et confirmez le mot de passe administrateur de l'interface de ligne de commande.
 - b Composez et confirmez le mot de passe d'activation de l'interface de ligne de commande.
 - c Composez et confirmez le mot de passe racine de l'interface de ligne de commande.
 - d Entrez l'adresse IPv4 du réseau de gestion.
 - e Entrez les détails du **Port externe** de l'ID VLAN, de l'interface de sortie, de l'adresse IP et de la longueur du préfixe IP, de sorte que l'interface de sortie soit mappée au réseau avec le groupe de ports de votre interface de liaison montante.

Si l'interface de sortie est connectée à un groupe de ports de jonction, spécifiez un ID VLAN. Par exemple, **20, eth2, 192.168.5.1, 24**. Vous pouvez également configurer votre groupe de ports avec un ID VLAN et utiliser le VLAN 0 pour le **Port externe**.
 - f (Facultatif) Pour configurer la haute disponibilité, entrez les détails du **Port HA** dans lequel l'interface de sortie correspond au réseau HA approprié.
 - g (Facultatif) Lors du déploiement d'un dispositif NSX Edge autonome en tant que nœud secondaire pour HA, sélectionnez **Déployer ce dispositif Edge autonome en tant que nœud secondaire**.

Utilisez le même fichier OVF que le nœud principal et entrez l'adresse IP, le nom d'utilisateur, le mot de passe et l'empreinte numérique du nœud principal.

Pour récupérer l'empreinte numérique du nœud principal, connectez-vous au nœud principal et exécutez la commande suivante :

```
get certificate api thumbprint
```

Assurez-vous que les adresses IP VTEP des nœuds principal et secondaire se trouvent dans le même sous-réseau et qu'ils se connectent au même groupe de ports. Lorsque vous effectuez le déploiement et que vous démarrez le dispositif Edge secondaire, il se connecte au nœud principal pour constituer un cluster Edge.

- 12 Dans la page **Prêt à terminer**, passez en revue les paramètres du dispositif Edge autonome et cliquez sur **Terminer**.

Note Si des erreurs se sont produites pendant le déploiement, un message du jour s'affiche sur l'interface de ligne de commande. Vous pouvez également utiliser un appel d'API pour vérifier les erreurs :

```
GET https://<nsx-mgr>/api/v1/node/status
```

Les erreurs sont classées en tant qu'erreurs logicielles et erreurs matérielles. Utilisez les appels d'API pour résoudre les erreurs logicielles selon les besoins. Vous pouvez effacer le message du jour à l'aide d'un appel d'API :

```
POST /api/v1/node/status?action=clear_bootup_error
```

-
- 13 Mettez sous tension le dispositif NSX Edge autonome.
 - 14 Connectez-vous au client NSX Edge autonome.
 - 15 Sélectionnez **L2VPN > Ajouter une session** et entrez les valeurs suivantes :
 - a Entrez un nom de session.
 - b Entrez l'adresse IP locale et l'adresse IP distante.
 - c Entrez le code homologue à partir de l'instance du serveur L2VPN. Pour plus d'informations sur l'obtention du code homologue, reportez-vous à la section [Télécharger le fichier de configuration du VPN de couche 2 côté distant](#).
 - 16 Cliquez sur **Enregistrer**.
 - 17 Sélectionnez **Port > Ajouter un port** pour créer un port d'extension L2.
 - 18 Entrez un nom, un VLAN et sélectionnez une interface de sortie.
 - 19 Cliquez sur **Enregistrer**.
 - 20 Sélectionnez **L2VPN > Attacher un port** et entrez les valeurs suivantes :
 - a Sélectionnez la session VPN L2 que vous avez créée.
 - b Sélectionnez le port d'extension L2 que vous avez créé.
 - c Entrez un ID de tunnel.

21 Cliquez sur Attacher.

Vous pouvez créer des ports d'extension L2 supplémentaires et les attacher à la session si vous devez étendre plusieurs réseaux L2.

22 Utilisez le navigateur pour vous connecter au dispositif NSX Edge autonome ou utilisez des appels d'API pour afficher l'état de la session L2VPN.

Note Si la configuration du serveur L2VPN change, assurez-vous de télécharger à nouveau le code homologue et de mettre à jour la session avec le nouveau code homologue.

Vérifier l'état réalisé d'une session VPN IPSec

Après l'envoi d'une demande de mise à jour de la configuration d'une session VPN IPSec, vous pouvez vérifier si l'état demandé a été correctement traité dans le plan de contrôle local NSX-T Data Center des nœuds de transport.

Lorsque vous créez une session VPN IPSec, plusieurs entités sont créées : un profil IKE, un profil DPD, un profil de tunnel, un point de terminaison local, un service VPN IPSec et une session VPN IPSec. Ces entités partagent toutes la même étendue `IPSecVPNSession`. Vous pouvez donc obtenir l'état de réalisation de toutes les entités de la session VPN IPSec en profitant d'un même appel d'API `GET`. Vous pouvez vérifier l'état de réalisation en utilisant uniquement l'API.

Conditions préalables

- Familiarisez-vous avec le VPN IPSec. Reportez-vous à la section [Comprendre le VPN IPSec](#).
- Assurez-vous que le VPN IPSec est bien configuré. Reportez-vous à la section [Ajouter un service VPN IPSec](#).
- Vous devez avoir accès à l'API NSX Manager.

Procédure

- 1 Envoyez un appel d'API `POST`, `PUT` ou `DELETE` pour votre demande.

Par exemple :

```
PUT https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/8dd1c386-9b2c-4448-85b8-51ff649fae4f
{
  "resource_type": "PolicyBasedIPSecVPNSession",
  "id": "8dd1c386-9b2c-4448-85b8-51ff649fae4f",
  "display_name": "Test RZ_UPDATED",
  "ipsec_vpn_service_id": "7adfa455-a6fc-4934-a919-f5728957364c",
  "peer_endpoint_id": "17263ca6-dce4-4c29-bd8a-e7d12bd1a82d",
  "local_endpoint_id": "91ebfa0a-820f-41ab-bd87-f0fb1f24e7c8",
  "enabled": true,
  "policy_rules": [
    {
      "id": "1026",
      "sources": [
```



```

        {
            "subnet": "1.1.1.0/24"
        }
    ],
    "logged": true,
    "destinations": [
        {
            "subnet": "2.1.4..0/24"
        }
    ],
    "action": "PROTECT",
    "enabled": true,
    "_revision": 1
}
]
}

```

- 2 Dans l'en-tête de la réponse renvoyée, localisez et copiez la valeur de `x-nsx-requestid`.

Par exemple :

```
x-nsx-requestid    e550100d-f722-40cc-9de6-cf84d3da3ccb
```

- 3 Demandez l'état de réalisation de la session VPN IPsec en utilisant l'appel `GET` suivant.

```
GET https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/<ipsec-vpn-session-id>/state?request_id=<request-id>
```

L'appel d'API suivant utilise les valeurs `id` et `x-nsx-requestid` dans les exemples utilisés lors des étapes précédentes.

```
GET https://<nsx-mgr>/api/v1/vpn/ipsec/sessions/8dd1c386-9b2c-4448-85b8-51ff649fae4f/state?request_id=e550100d-f722-40cc-9de6-cf84d3da3ccb
```

Voici un exemple de réponse que vous recevez lorsque l'état de réalisation est `in_progress`.

```

{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "fe651e63-04bd-43a4-a8ec-45381a3b71b9",
      "state": "in_progress",
      "failure_message": "CCP Id:ab5958df-d98a-468e-a72b-d89dcdae5346, Message:State realization is in progress at the node."
    },
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "ebe174ac-e4f1-4135-ba72-3dd2eb7099e3",
      "state": "in_sync"
    }
  ],
  "state": "in_progress",
  "failure_message": "The state realization is in progress at transport nodes."
}

```

Voici un exemple de réponse que vous recevez lorsque l'état de réalisation est `in_sync`.

```
{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "7046e8f4-a680-11e8-9bc3-020020593f59",
      "state": "in_sync"
    }
  ],
  "state": "in_sync"
}
```

Voici des exemples de réponse possible que vous recevez lorsque l'état de réalisation est `unknown`.

```
{
  "state": "unknown",
  "failure_message": "Unable to get response from any CCP node. Please retry operation after some time."
}
```

```
{
  "details": [
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "3e643776-5def-11e8-94ae-020022e7749b",
      "state": "unknown",
      "failure_message": "CCP Id:ab5958df-d98a-468e-a72b-d89dcdae5346, Message: Unable to get response from the node. Please retry operation after some time."
    },
    {
      "sub_system_type": "TransportNode",
      "sub_system_id": "4784ca0a-5def-11e8-93be-020022f94b73",
      "state": "in_sync"
    }
  ],
  "state": "unknown",
  "failure_message": "The state realization is unknown at transport nodes"
}
```

Après avoir effectué une opération `DELETE` sur l'entité, vous pouvez recevoir l'état `NOT_FOUND`, comme indiqué dans l'exemple suivant.

```
{
  "http_status": "NOT_FOUND",
  "error_code": 600,
  "module_name": "common-services",
  "error_message": "The operation failed because object identifier LogicalRouter/61746f54-7ab8-4702-93fe-6ddeb804 is missing: Object identifiers are case sensitive.."
}
```

Si le service VPN IPSec associé à la session est désactivé, vous recevez la réponse `BAD_REQUEST`, comme indiqué dans l'exemple suivant.

```
{
  "httpStatus": "BAD_REQUEST",
  "error_code": 110199,
  "module_name": "VPN",
  "error_message": "VPN service f9cfe508-05e3-4e1d-b253-fed096bb2b63 associated with the
session 8dd1c386-9b2c-4448-85b8-51ff649fae4f is disabled. Can not get the realization
status."
}
```

Surveiller et dépanner des sessions VPN

Après avoir configuré une session IPSec ou VPN L2, vous pouvez surveiller l'état du tunnel VPN et résoudre les problèmes signalés à l'aide 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://<nsx-manager-ip-address>`.
- 2 Accédez à l'onglet **Mise en réseau > VPN > Sessions IPSec** ou **Mise en réseau > VPN > Sessions VPN de couche 2**.
- 3 Développez la ligne correspondant à la session VPN que vous voulez surveiller ou dépanner.
- 4 Pour afficher l'état du tunnel VPN, cliquez sur l'icône d'informations.
La boîte de dialogue État s'affiche et affiche les états disponibles.
- 5 Pour afficher les statistiques de trafic du tunnel VPN, cliquez sur **Afficher les statistiques** dans la colonne État.
La boîte de dialogue Statistiques affiche les statistiques de trafic du tunnel VPN.
- 6 Pour afficher les statistiques d'erreur, cliquez sur le lien **Plus** dans la boîte de dialogue Statistiques.
- 7 Pour fermer la boîte de dialogue **Statistiques**, cliquez sur **Fermer**.

Traduction d'adresse réseau

6

La traduction d'adresses réseau (NAT) met en correspondance un espace d'adressage IP et un autre. Vous pouvez configurer NAT sur les passerelles de niveau 0 et de niveau 1.

Ce chapitre contient les rubriques suivantes :

- [Configurer la NAT sur une passerelle](#)

Configurer la NAT sur une passerelle

Vous pouvez configurer la NAT source (SNAT), la NAT de destination (DNAT) ou une NAT réflexive sur une passerelle de niveau 0 ou 1.

Lorsqu'une passerelle de niveau 0 est exécutée en mode Actif-Actif, vous ne pouvez pas configurer une SNAT ou une DNAT, les chemins d'accès asymétriques pouvant causer des problèmes. Vous pouvez uniquement configurer une NAT réflexive (parfois appelée NAT sans état). Si une passerelle de niveau 0 est en cours d'exécution en mode Actif-En veille, vous pouvez configurer une SNAT, une DNAT ou une NAT réflexive.

Vous pouvez également désactiver la SNAT ou la DNAT pour une adresse IP ou une plage d'adresses. Si une adresse dispose de plusieurs règles NAT, la règle présentant la priorité la plus élevée est appliquée.

Note DNAT n'est pas pris en charge sur une passerelle de niveau 1 où un VPN IPSec basé sur les stratégies est configuré.

La SNAT configurée sur l'interface externe de la passerelle de niveau 0 traite le trafic provenant d'une passerelle de niveau 1, ainsi que d'une autre interface externe sur la passerelle de niveau 0.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > NAT**.
- 3 Sélectionnez une passerelle.
- 4 Cliquez sur **Ajouter une règle NAT**.

5 Sélectionnez une action.

Pour une passerelle de niveau 1, les actions disponibles sont **SNAT**, **DNAT**, **Réflexive**, **Aucune SNAT** et **Aucune DNAT**.

Pour une passerelle de niveau 0 en mode Actif-En veille, les actions disponibles sont **SNAT**, **DNAT**, **Aucune SNAT** et **Aucune DNAT**.

Pour une passerelle de niveau 0 en mode Actif-Actif, l'action disponible est **Réflexive**.

6 Dans la colonne **Service**, cliquez sur **Définir** pour sélectionner des services.

7 (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.

8 Pour **Adresse IP de Destination**, 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 Entrez une valeur pour **Port traduit**.

11 Sélectionnez un paramètre de pare-feu parmi les options suivantes :

- **Correspond à une adresse externe** : le paquet est traité par des règles de pare-feu qui correspondent à la combinaison de l'adresse IP traduite et du port traduit.
 - Pour SNAT, l'adresse externe est l'adresse source traduite après l'exécution de NAT.
 - Pour DNAT, l'adresse externe est l'adresse de destination d'origine avant l'exécution de NAT.
 - Pour REFLÉXIVE, pour le trafic de sortie, le pare-feu est appliqué à l'adresse source traduite après l'exécution de NAT. Pour le trafic d'entrée, le pare-feu est appliqué à l'adresse de destination d'origine avant l'exécution de NAT.
- **Correspond à une adresse interne** : le paquet est traité par des règles de pare-feu qui correspondent à la combinaison de l'adresse IP d'origine et du port d'origine.
 - Pour SNAT, l'adresse interne est l'adresse source d'origine avant l'exécution de NAT.
 - Pour DNAT, l'adresse interne est l'adresse de destination traduite après l'exécution de NAT.
 - Pour REFLEXIVE, pour le trafic de sortie, le pare-feu est appliqué à l'adresse source d'origine avant l'exécution de NAT. Pour le trafic d'entrée, le pare-feu est appliqué à l'adresse de destination traduite après l'exécution de NAT.
- **Contournement** : le paquet contourne les règles de pare-feu.

12 (Requis) Modifiez l'état de la journalisation.

13 (Requis) Pour **Appliqué à**, sélectionnez les objets auxquels s'applique la règle.

Les objets disponibles sont **Passerelles de niveau 0**, **Interfaces**, **Étiquettes**, **Points de terminaison de l'instance de service** et **Points de terminaison virtuels**.

14 Spécifiez une valeur de priorité.

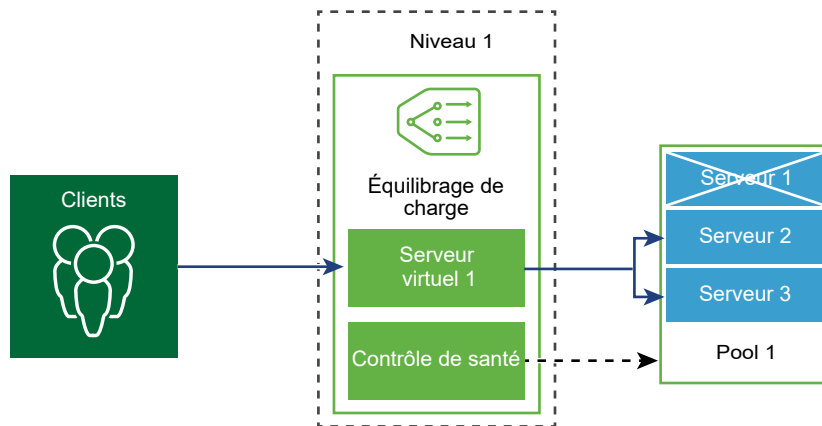
Une valeur inférieure signifie une priorité plus élevée. La valeur par défaut est 100.

15 Cliquez sur **Enregistrer**.

Équilibrage de charge

7

L'équilibreur 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'équilibreur 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'équilibreur 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'équilibreur de charge en augmentant le nombre de serveurs virtuels et de membres du pool existants pour gérer un trafic réseau intense.

Note L'équilibreur de charge logique est uniquement pris en charge sur la passerelle de niveau 1. Un équilibreur de charge ne peut être attaché qu'à une passerelle de niveau 1.

Ce chapitre contient les rubriques suivantes :

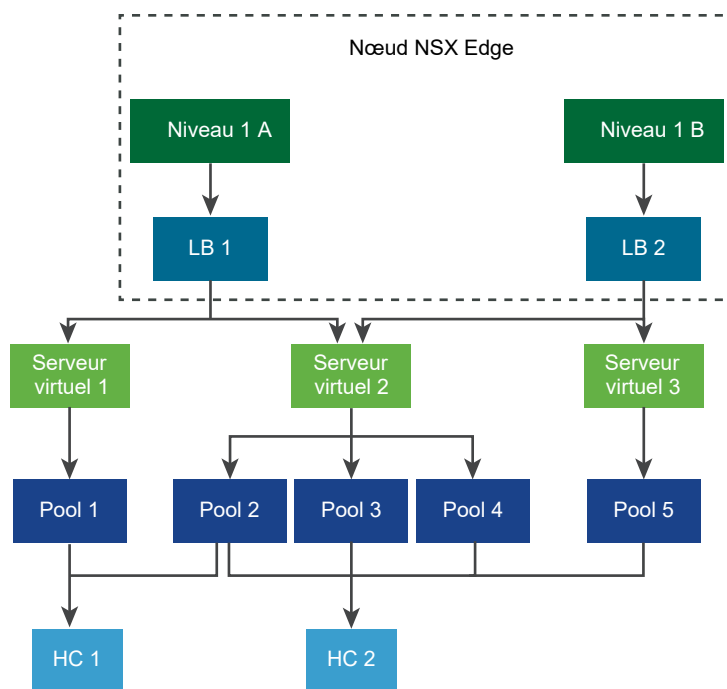
- [Concepts clés de l'équilibreur de charge](#)
- [Configuration des composants d'équilibrage de charge](#)
- [Groupes créés pour les pools de serveurs et les serveurs virtuels](#)

Concepts clés de l'équilibreur de charge

L'équilibreur de charge inclut des serveurs virtuels, des pools de serveurs et des moniteurs de contrôle de santé.

Un équilibreur 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'équilibreur de charge

Lorsque vous configurez un équilibreur de charge, vous pouvez spécifier une taille (petite, moyenne ou grande). La taille détermine le nombre de serveurs virtuels, de pools de serveurs et de membres du pool que l'équilibreur de charge peut prendre en charge.

Un équilibreur de charge s'exécute sur une passerelle de niveau 1, qui doit être en mode actif-en veille. La passerelle s'exécute sur des nœuds NSX Edge. Le facteur de forme du nœud NSX Edge (Bare Metal, petite, moyenne ou grande) détermine le nombre d'équilibreurs de charge que le nœud NSX Edge peut prendre en charge. Dans l'onglet **Mise en réseau et sécurité avancées**, le routeur logique de terme est utilisé pour faire référence à une passerelle.

Pour plus d'informations sur les différentes tailles d'équilibreur de charge et les facteurs de forme que NSX Edge peut prendre en charge, reportez-vous à <https://configmax.vmware.com>.

L'utilisation d'un petit nœud NSX Edge pour exécuter un petit équilibreur de charge n'est pas recommandée dans un environnement de production.

Vous pouvez appeler une API pour obtenir les informations d'utilisation de l'équilibreur de charge d'un nœud NSX Edge : Si vous utilisez l'onglet **Mise en réseau** pour configurer l'équilibrage de charge, exécutez la commande suivante :

```
GET /policy/api/v1/infra/lb-node-usage?node_path=<node-path>
```

Si vous utilisez l'onglet **Mise en réseau et sécurité avancées** pour configurer l'équilibrage de charge, exécutez la commande suivante :

```
GET /api/v1/loadbalancer/usage-per-node/<node-id>
```

Les informations d'utilisation incluent le nombre d'objets d'équilibreur de charge (tels que les services d'équilibreur de charge, les serveurs virtuels, les pools de serveurs et les membres du pool) qui sont configurés sur le nœud Edge. Pour plus d'informations, reportez-vous au *Guide de l'API de NSX-T Data Center*.

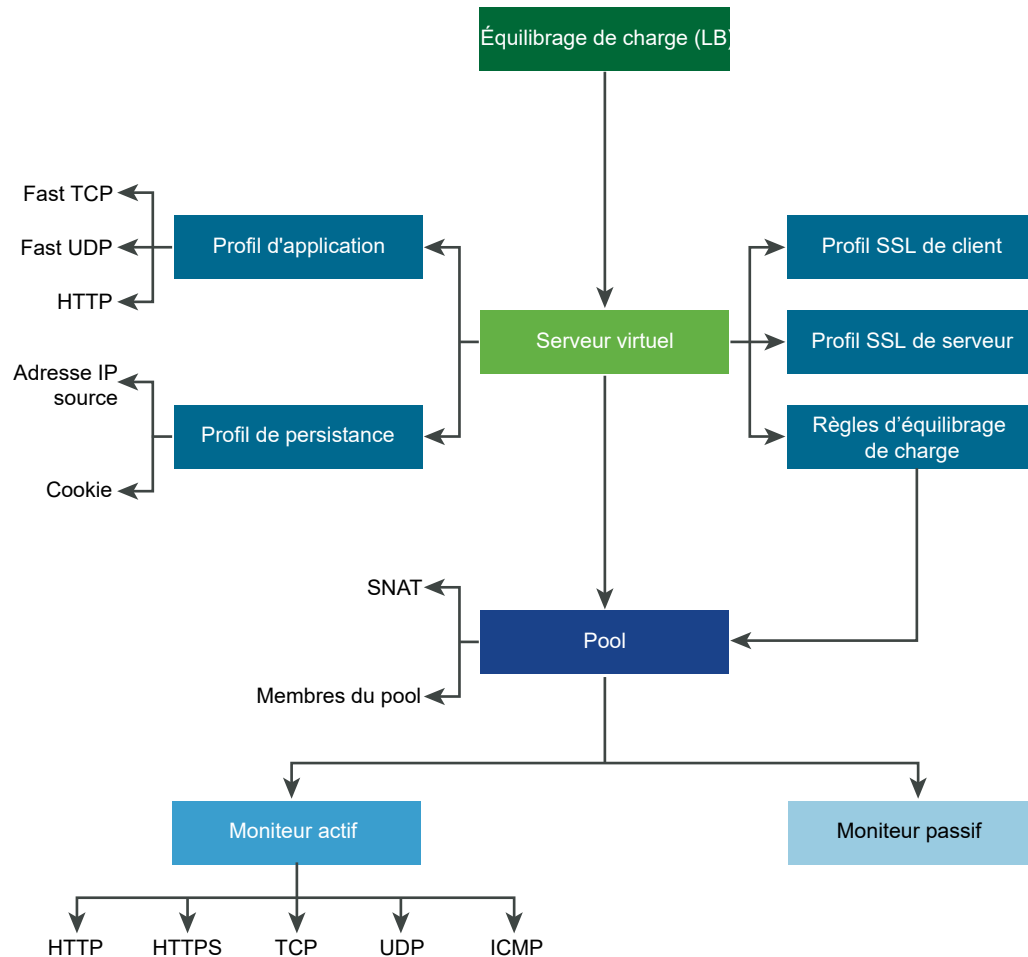
Fonctionnalités d'équilibrage de charge prises en charge

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.

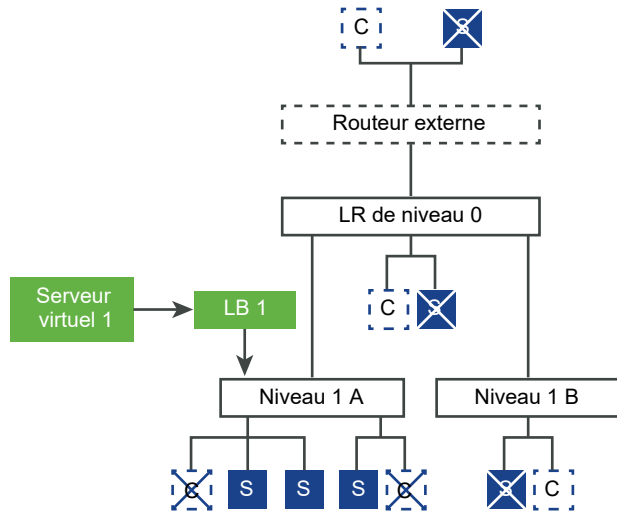


Topologies d'équilibreur de charge

Les équilibreurs de charge sont généralement déployés en mode en ligne ou en mode manchot. Le mode manchot requiert la configuration de la NAT source (SNAT) du serveur virtuel. Le mode en ligne ne la requiert pas.

Topologie en ligne

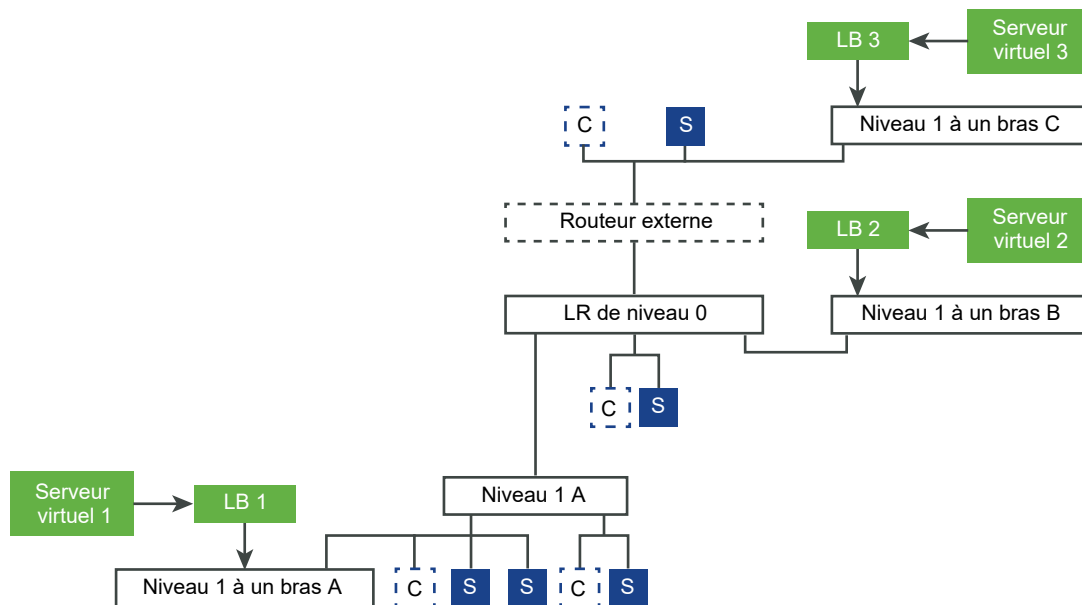
Dans le mode en ligne, l'équilibreur de charge se trouve sur le chemin du trafic entre le client et le serveur. Les clients et les serveurs ne doivent pas être connectés à des segments de superposition sur le même routeur logique de niveau 1 si SNAT sur l'équilibreur de charge n'est pas souhaité. Si des clients et des serveurs sont connectés à des segments de superposition sur le même routeur logique de niveau 1, SNAT est requis.



Topologie manchot

Dans le mode manchot, l'équilibreur 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'équilibreur de charge utilise un NAT source (SNAT) pour forcer le trafic de retour du serveur destiné au client à passer par l'équilibreur de charge. Dans cette topologie, un serveur virtuel SNAT doit être activé.

Lorsque l'équilibreur de charge reçoit le trafic client vers l'adresse IP virtuelle, l'équilibreur de charge sélectionne un membre du pool de serveurs et y achemine le trafic client. En mode manchot, l'équilibreur de charge remplace l'adresse IP du client par l'adresse IP de l'équilibreur de charge afin que la réponse du serveur soit toujours envoyée à l'équilibreur de charge. L'équilibreur de charge transfère la réponse au client.



Chaînage de service de niveau 1

Si une passerelle de niveau 1 ou un routeur logique héberge différents services, tels qu'une NAT, un pare-feu et un équilibreur de charge, les services sont appliqués dans l'ordre suivant :

- Entrée

DNAT - Pare-feu - Équilibreur de charge

Remarque : si DNAT est configuré avec le contournement de pare-feu, le pare-feu est ignoré, mais pas l'équilibreur de charge.

- Sortie

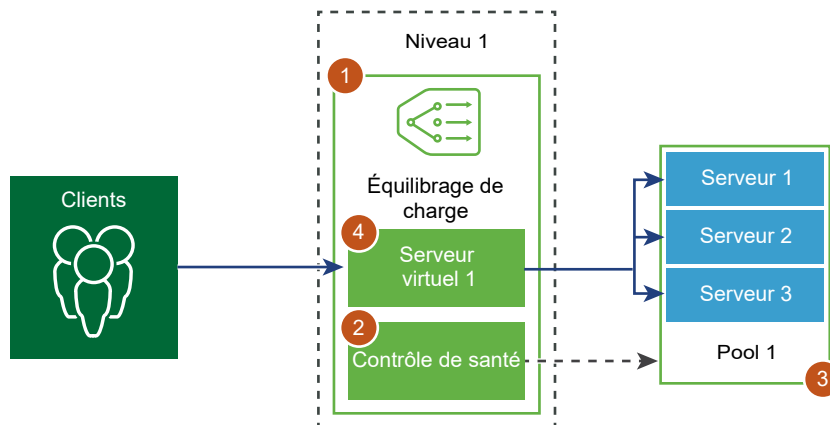
Équilibreur de charge - Pare-feu - SNAT

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 une passerelle de niveau 1.

Note Dans l'onglet **Mise en réseau avancée et sécurité**, le terme routeur logique de niveau 1 est utilisé pour faire référence à une passerelle de niveau 1.

Vous pouvez ensuite configurer la surveillance de 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 votre équilibrage de charge et joindre le nouveau serveur virtuel à l'équilibrage de charge.



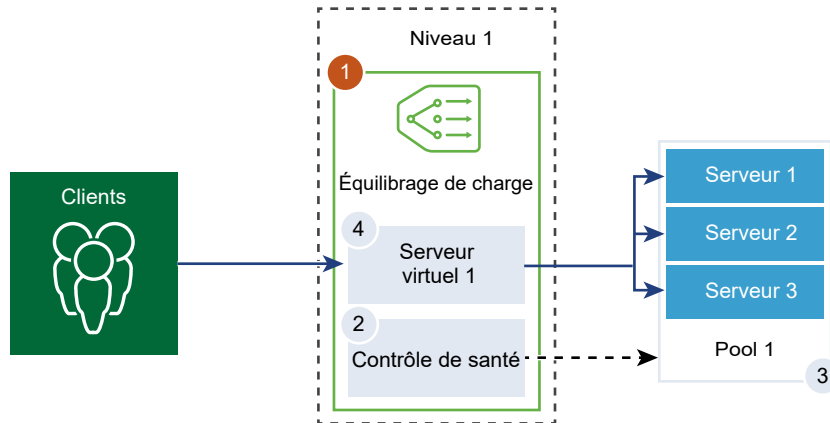
Ajouter des équilibrages de charge

Un équilibrage de charge est créé et attaché à la passerelle de niveau 1.

Note Dans l'onglet **Mise en réseau avancée et sécurité**, le terme routeur logique de niveau 1 est utilisé pour faire référence à une passerelle 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 équilibres de charge avec un trafic significatif, car le grand nombre de messages enregistrés dans le journal peut avoir une incidence sur les performances.



Conditions préalables

Vérifiez qu'une passerelle de niveau 1 est configurée. Reportez-vous à la section [Chapitre 3 Passerelle de niveau 1](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Équilibrage de charge > Ajouter un équilibreur de charge**.
- 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 Dans le menu déroulant, sélectionnez la passerelle de niveau 1 déjà configurée à attacher à cet équilibrage de charge.

La passerelle de niveau 1 doit être en mode Actif-En veille.

- 6 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.

- 7 (Facultatif) Entrez des balises pour faciliter la recherche.

Vous pouvez spécifier une balise pour définir son étendue.

8 Cliquez sur **Enregistrer**.

Environ trois minutes sont nécessaires à la création de l'équilibrage de charge et à sa liaison à la passerelle de niveau 1 (l'état de configuration passe au vert et l'équilibrage de charge est opérationnel).

Si l'état est Hors service, cliquez sur l'icône d'information et résolvez l'erreur avant de continuer.

9 (Facultatif) Supprimez l'équilibrage de charge.

- a Détachez l'équilibrage de charge du serveur virtuel et de la passerelle de niveau 1.
- b Sélectionnez l'équilibrage de charge.
- c Cliquez sur le bouton de sélection verticale.
- d Sélectionnez **Supprimer**.

Ajouter un moniteur actif

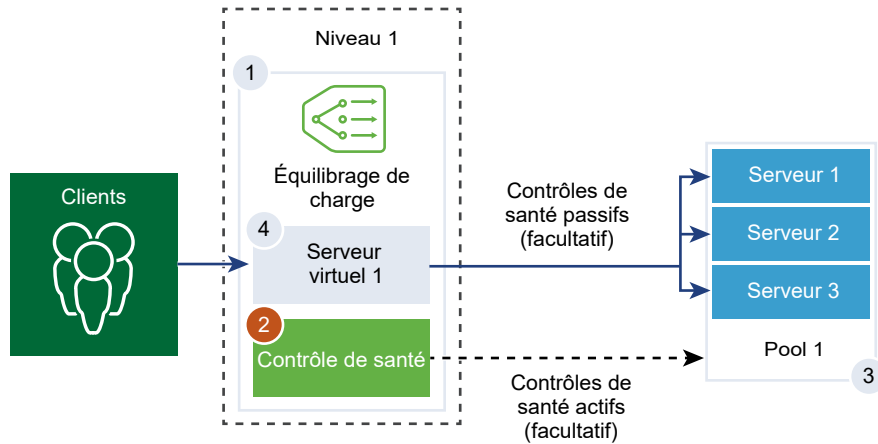
Le moniteur de santé actif est utilisé pour tester la disponibilité d'un serveur. Pour cela, il utilise plusieurs types de tests, notamment l'envoi d'une commande ping de base aux serveurs ou de demandes HTTP avancées pour surveiller la santé d'une application.

Note Dans l'onglet **Mise en réseau avancée et sécurité**, le terme routeur logique de niveau 1 est utilisé pour faire référence à une passerelle de niveau 1.

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 connecté à une passerelle 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Équilibrage de charge > Moniteurs > Actif > Ajouter un moniteur actif**.
- 3 Sélectionnez un protocole pour le serveur dans le menu déroulant.
Vous pouvez également utiliser des protocoles prédéfinis : HTTP, HTTPS, ICMP, TCP et UDP pour NSX Manager.
- 4 Sélectionnez le protocole **HTTP**.
- 5 Configurez les valeurs pour surveiller un pool de services.

Vous pouvez également accepter les valeurs de contrôle de santé actif par défaut.

Option	Description
Nom et description	Entrez un nom et une description pour le moniteur de santé actif.
Port de surveillance	Définissez la valeur du port de surveillance.
Intervalle de surveillance	Définissez le délai en secondes après lequel le moniteur envoie une autre demande de connexion au serveur.
Délai d'expiration	Définissez le nombre de fois que le serveur est testé avant qu'il ne soit considéré comme INACTIF.
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.
Balises	Entrez des balises pour faciliter la recherche. Vous pouvez spécifier une balise pour définir son étendue.

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.

6 Cliquez sur **Configurer**.

7 Entrez les détails de configuration de la demande et de la réponse HTTP.

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.
En-tête de réponse HTTP	Cliquez sur Ajouter et entrez le nom d'en-tête de la réponse HTTP et la valeur correspondante. La valeur d'en-tête par défaut est 4 000. La valeur d'en-tête maximale est 64 000.
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 Sélectionnez le protocole **HTTPS**.

9 Effectuez l'étape 5.

10 Cliquez sur **Configurer**.

11 Entrez les détails de configuration de la demande et de la réponse HTTP, ainsi que ceux de SSL.

Option	Description
Nom et description	Entrez un nom et une description pour le moniteur de santé actif.
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.

Option	Description
En-tête de réponse HTTP	Cliquez sur Ajouter et entrez le nom d'en-tête de la réponse HTTP et la valeur correspondante. La valeur d'en-tête par défaut est 4 000. La valeur d'en-tête maximale est 64 000.
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.
SSL serveur	Faites basculer le bouton pour activer le serveur SSL.
Certificat client	(Facultatif) Sélectionnez, dans le menu déroulant, un certificat qui sera 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 une extension SNI.
Profil SSL serveur	(Facultatif) Attribuez, à partir du menu déroulant, un profil SSL par défaut qui définit les propriétés SSL côté client réutilisables et indépendantes des applications. Cliquez sur les points de suspension verticaux et créez un profil SSL personnalisé.
Certificats d'autorité de certification approuvés	(Facultatif) Vous pouvez exiger que le client dispose d'un certificat d'autorité de certification pour l'authentification.
Authentification du serveur obligatoire	(Facultatif) Faites basculer le bouton pour activer l'authentification du serveur.
Profondeur de la chaîne de certificats	(Facultatif) Définissez la profondeur d'authentification pour la chaîne de certificats du client.
Liste de révocation de certificat	(Facultatif) Définissez une liste de révocation de certificats (CRL) dans le profil SSL côté client pour rejeter les certificats clients compromis.

12 Sélectionnez le protocole **ICMP**.

13 Effectuez l'étape 5 et définissez la taille des données, en octets, du paquet de contrôle de santé ICMP.

14 Sélectionnez le protocole **TCP**.

15 Effectuez l'étape 5 ; vous pouvez laisser les paramètres de données TCP vides.

Si les données envoyées et attendues ne sont pas répertoriées, une connexion TCP d'établissement de liaison tridirectionnelle est établie pour valider la santé du serveur. Aucune donnée n'est envoyée.

Les données attendues, si elles sont répertoriées, doivent se présenter sous la forme d'une chaîne. Les expressions régulières ne sont pas prises en charge.

16 Sélectionnez le protocole **UDP**.

17 Effectuez l'étape 5 et configurez les données UDP.

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.

Étape suivante

Associez le moniteur de santé actif à un pool de serveurs. Reportez-vous à la section [Ajouter un pool de serveurs](#).

Ajouter un moniteur passif

Les équilibres 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'équilibreur 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'équilibreur de charge détecte cet échec. Si plusieurs échecs consécutifs se produisent, l'équilibreur 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'équilibreur de charge envoie une demande de connexion pour s'assurer que le membre du pool a récupéré. Si la connexion réussie, le membre du pool est alors considéré comme sain. Dans le cas contraire, l'équilibreur 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'équilibreur 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Équilibrage de charge > Moniteurs > Passif > Ajouter un moniteur passif**.
- 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.
Balises	Entrez des balises pour faciliter la recherche. Vous pouvez spécifier une balise pour définir son étendue.

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.

Étape suivante

Associez le moniteur de santé passif à un pool de serveurs. Reportez-vous à la section [Ajouter un pool de serveurs](#).

Ajouter un pool de serveurs

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.

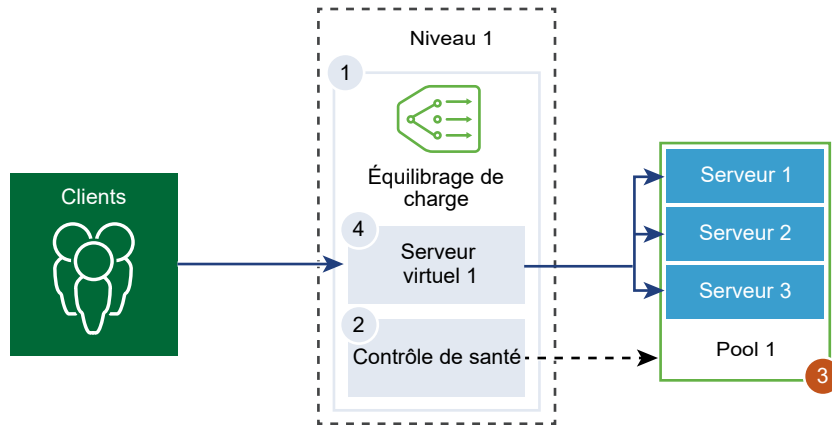
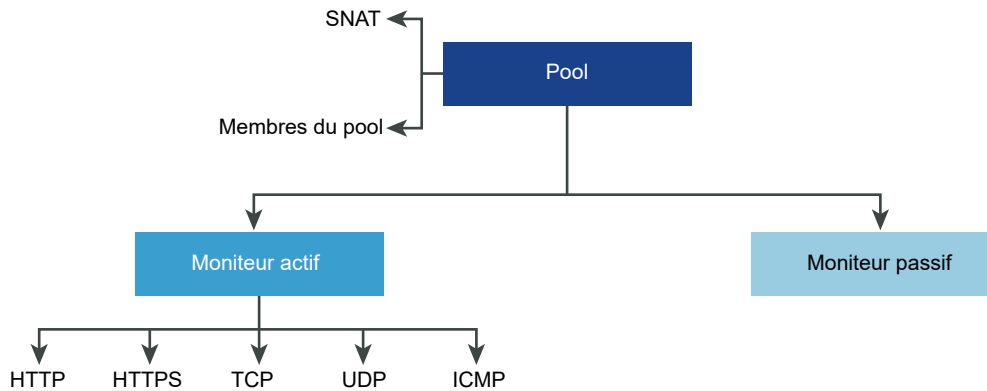


Figure 7-1. Configuration des paramètres du pool de serveurs



Conditions préalables

- Si vous utilisez des membres de pool dynamique, vous devez configurer un NSGroup. Reportez-vous à la section [Créer un NSGroup](#).
- Vérifiez qu'un moniteur de santé passif est configuré. Reportez-vous à la section [Ajouter un moniteur passif](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau > Équilibrage de charge > Pools de serveurs > Ajouter un pool de serveurs**.
- 3 Entrez un nom et une description pour le pool de serveurs 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	Les demandes entrantes des clients sont analysées en fonction d'une liste de serveurs disponibles capables de les traiter. Les pondérations des membres du pool de serveurs sont ignorées, même si elles sont configurées.
WEIGHTED_ROUND_ROBIN	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. L'algorithme d'équilibrage de charge est conçu pour répartir équitablement la charge entre les ressources de serveur disponibles.
LEAST_CONNECTION	Diffuse les requêtes client à plusieurs serveurs en se basant sur le nombre de connexions déjà sur le serveur. 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.
WEIGHTED_LEAST_CONNECTION	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. Cet algorithme d'équilibrage de charge se concentre sur l'utilisation de la valeur pondérée pour distribuer la charge sur les ressources disponibles du serveur. Par défaut, la pondération est 1 si la valeur n'est pas configurée et si le démarrage lent est activé.
IP-HASH	Sélectionne un serveur en fonction d'un hachage de l'adresse IP source et du poids total des serveurs en cours d'exécution.

5 Sélectionnez les membres du pool de serveurs.

Un pool de serveurs est constitué d'un ou de plusieurs membres du pool.

Option	Description
Entrer des membres individuels	<p>Entrez le nom d'un membre du pool, une adresse IP et un port.</p> <p>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.</p> <p>Vous pouvez définir l'état d'administration du pool de serveurs. Par défaut, l'option est activée lorsqu'un membre du pool de serveurs est ajouté.</p> <p>Si l'option est désactivée, les connexions actives sont traitées et le membre du pool de serveurs n'est pas sélectionné pour les nouvelles connexions. Les nouvelles connexions sont attribuées aux autres membres du pool.</p> <p>Si elle est désactivée normalement, elle vous permet de supprimer des serveurs pour la maintenance. Les connexions existantes à un membre du pool de serveurs dans cet état continuent d'être traitées.</p> <p>Faites basculer ce bouton pour désigner un membre du pool comme membre de sauvegarde afin de fonctionner 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. Les membres de sauvegarde sont ignorés lors de la sélection du serveur. Lorsque le pool de serveurs est inactif, les connexions entrantes sont envoyées uniquement aux membres de sauvegarde qui sont configurés avec une page d'erreur indiquant qu'une application n'est pas disponible.</p> <p>La valeur Nombre maximal de connexions simultanées attribue un maximum de connexions afin que les membres du pool de serveurs ne soient pas surchargés et ignorés pendant la sélection du serveur. Si aucune valeur n'est pas spécifiée, la connexion est illimitée.</p>
Sélectionner un groupe	<p>Sélectionnez un groupe préconfiguré de membres du pool de serveurs.</p> <p>Entrez un nom de groupe et une description facultative.</p> <p>Définissez le membre de calcul à partir de la liste existante ou créez-en un.</p> <p>Vous pouvez spécifier les critères d'appartenance, sélectionner les membres du groupe, ajouter des adresses IP et MAC en tant que membres du groupe et ajouter des groupes Active Directory. Les membres d'identité se combinent au membre de calcul pour définir l'appartenance au groupe.</p> <p>Entrez des balises pour faciliter la recherche. Vous pouvez spécifier une balise pour définir son étendue.</p> <p>Vous pouvez éventuellement définir la liste d'adresses IP maximales du groupe.</p>

6 Sélectionnez un moniteur de santé actif pour le pool de serveurs dans le menu déroulant.

L'équilibrage de charge envoie régulièrement une commande ping ICMP vers les serveurs pour vérifier la santé indépendante du trafic de données. Vous ne pouvez configurer qu'un seul moniteur de santé actif par pool de serveurs.

7 Sélectionnez le mode de traduction 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 de mappage automatique	<p>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.</p> <p>Le mode SNAT est requis.</p> <p>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.</p> <p>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.</p>
Désactiver	Désactivez le mode de traduction SNAT.
Pool IP	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>

8 Faites basculer ce bouton pour activer le multiplexage TCP.

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.

9 Définissez le nombre maximal de connexions de multiplexage TCP par pool qui sont conservées pour l'envoi de demandes client ultérieures.

10 Entrez le nombre minimal de membres actifs que le pool de serveurs doit toujours comprendre.

11 Sélectionnez un moniteur de santé passif pour le pool de serveurs dans le menu déroulant.

12 Entrez des balises pour faciliter la recherche.

Vous pouvez spécifier une balise pour définir son étendue.

Configuration des composants de serveur virtuel

Vous pouvez configurer les serveurs virtuels de couche 4 et de couche 7 et configurer plusieurs composants de serveur virtuel, tels les profils d'application, les profils permanents et les règles d'équilibreur de charge.

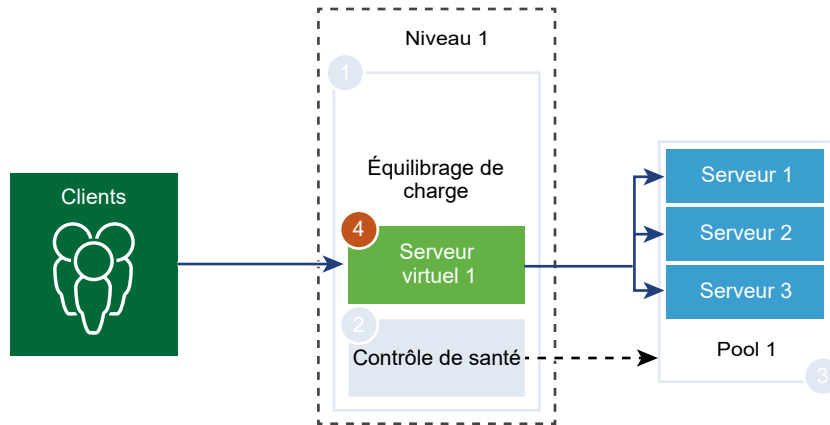
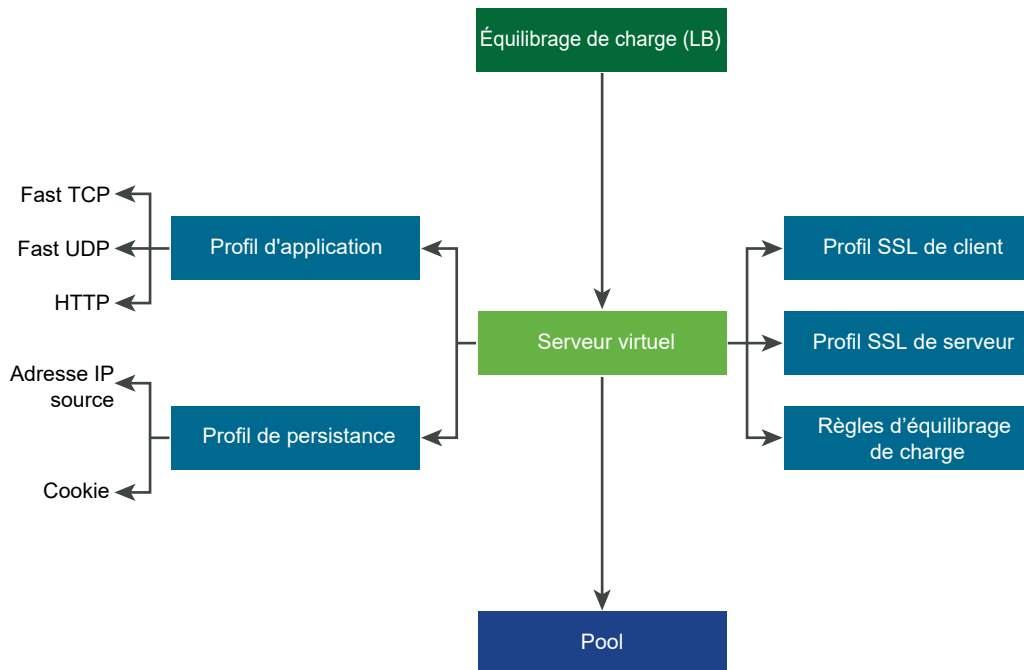


Figure 7-2. Composants de serveur virtuel



Ajouter un profil 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'équilibreur 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 7-3. Profil d'application TCP et UDP de couche 4

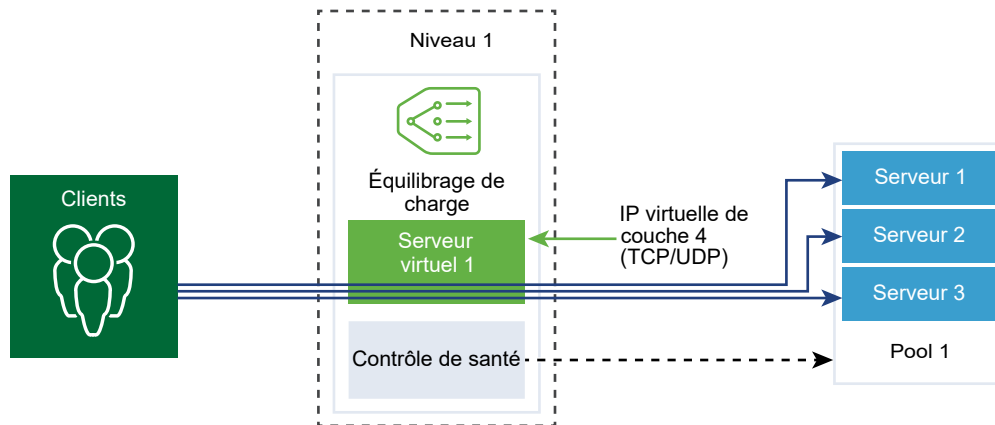
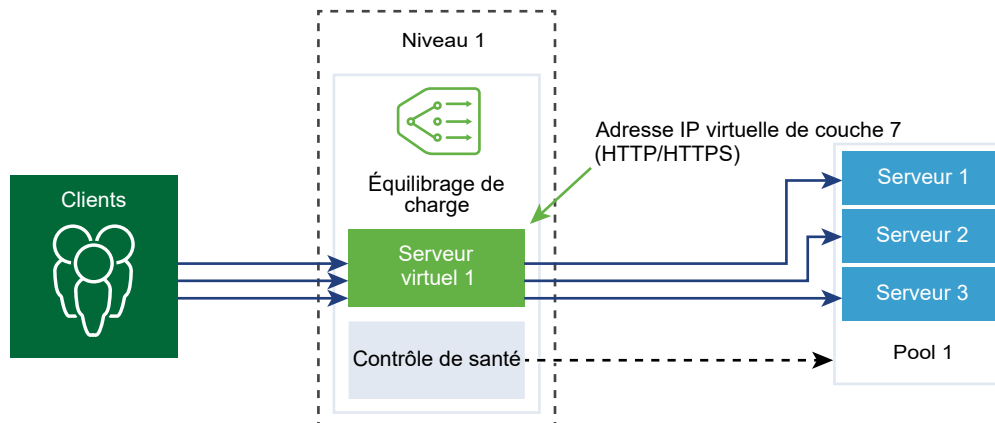


Figure 7-4. Profil d'application HTTPS de couche 7



Procédure

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

- 2 Sélectionnez **Mise en réseau > Équilibrage de charge > Profils > Application > Ajouter des profils d'application**.
- 3 Sélectionnez un profil d'application **TCP rapide** et entrez ses détails.

Vous pouvez également accepter les paramètres du profil TCP rapide par défaut.

Option	Description
Nom et description	Entrez un nom et une description pour le profil d'application TCP rapide.
Délai d'inactivité	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'équilibreur de charge ne le fasse.
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.
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.
Balises	Entrez des balises pour faciliter la recherche. Vous pouvez spécifier une balise pour définir son étendue.

- 4 Sélectionnez un profil d'application **UDP rapide** et entrez ses détails.

Vous pouvez également accepter les paramètres du profil UDP par défaut.

Option	Description
Nom et description	Entrez un nom et une description pour le profil d'application UDP rapide.
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.
Balises	Entrez des balises pour faciliter la recherche. Vous pouvez spécifier une balise pour définir son étendue.

- 5 Sélectionnez un profil d'application **HTTP** et entrez ses détails.

Vous pouvez également accepter les paramètres du profil HTTP par défaut.

Le profil d'application HTTP est utilisé pour les applications HTTP et HTTPS.

Option	Description
Nom et description	Entrez un nom et une description pour le profil d'application HTTP.
Délai d'inactivité	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.
Taille de l'en-tête de la demande	Spécifiez la taille maximale de tampon en octets utilisée pour stocker les en-têtes de demande HTTP.
X-Forwarded-For (XFF)	<ul style="list-style-type: none"> ■ Insert : si l'en-tête HTTP XFF ne figure pas dans la demande entrante, l'équilibreur de charge insère un nouvel en-tête XFF comprenant l'adresse IP du client. Si l'en-tête HTTP XFF figure dans la demande entrante, l'équilibreur de charge insère l'en-tête XFF comprenant l'adresse IP du client. ■ Remplacer : si l'en-tête HTTP XFF est présent dans la demande entrante, l'équilibreur de charge remplace 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'équilibreur 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'équilibreur 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>
Taille du corps de la demande	<p>Entrez une valeur pour la taille maximale de la mémoire tampon utilisée pour stocker le corps de la demande HTTP.</p> <p>Si celle-ci n'est pas spécifiée, la taille du corps de la demande est illimitée.</p>

Option	Description
Redirection	<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 équilibreur 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>
Authentification NTLM	<p>Faites basculer ce bouton pour que l'équilibreur de charge désactive le multiplexage TCP et active les connexions HTTP persistantes.</p> <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'équilibreur 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>
Balises	<p>Entrez des balises pour faciliter la recherche.</p> <p>Vous pouvez spécifier une balise pour définir son étendue.</p>

Ajouter un profil de persistance

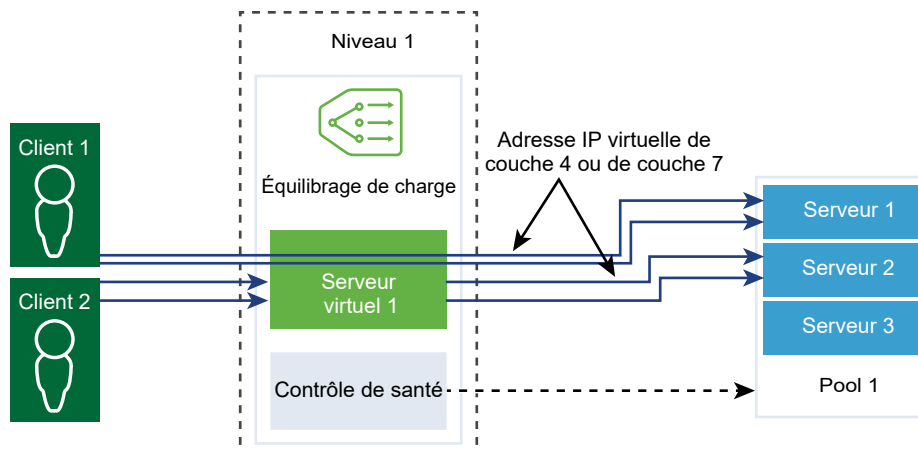
Pour garantir la stabilité des applications avec état, les équilibres de charge implémentent la persistance qui dirige toutes les connexions associées au même serveur. Différents types de persistance sont pris en charge pour répondre à différents types de besoins d'application.

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'équilibreur 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'équilibreur de charge utilise ces informations pour permettre la persistance du cookie. Les serveurs virtuels de la couche 7 ne peuvent utiliser que le profil de persistance du cookie. Notez qu'un espace vide dans un nom de cookie n'est **pas** pris en charge.

Le profil de persistance générique prend en charge la persistance basée sur l'en-tête, le cookie ou l'URL HTTP dans la demande HTTP. Par conséquent, il prend en charge la persistance de session d'application lorsque l'ID de session fait partie de l'URL. Ce profil n'est pas associé directement à un serveur virtuel. Vous pouvez le spécifier lorsque vous configurez une règle d'équilibreur de charge pour le transfert de demande et la réécriture de réponse.



Procédure

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

- 2 Sélectionnez **Mise en réseau > Équilibrage de charge > Profils > Persistance > Ajouter des profils de persistance**.
- 3 Sélectionnez **IP source** pour ajouter un profil de persistance de l'adresse IP source et entrez les détails du profil.

Vous pouvez également accepter les paramètres du profil de persistance de l'adresse IP source par défaut.

Option	Description
Nom et description	Entrez un nom et une description pour le profil de persistance de l'adresse IP source.
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'équilibreur de charge conserve les entrées pour enregistrer que les demandes des clients sont dirigées vers le même serveur.</p> <p>La toute première connexion à partir de l'adresse IP du nouveau client est équilibrée sur un membre du pool en fonction de l'algorithme d'équilibrage de charge. NSX stockera cette entrée de persistance sur la table de persistance de l'équilibrage de charge visible sur le nœud Edge qui héberge l'équilibrage de charge T1 actif via la commande CLI : <code>get load-balancer <LB-UUID> persistence-tables</code>.</p> <ul style="list-style-type: none"> ■ Lorsqu'il y a des connexions de ce client vers l'adresse IP virtuelle, l'entrée de persistance est conservée. ■ Lorsqu'il n'y a plus de connexions de ce client vers l'adresse IP virtuelle, l'entrée de persistance commence le compte à rebours du temporisateur spécifié dans la valeur « Délai d'expiration de l'entrée de persistance ». Si aucune nouvelle connexion de ce client vers l'adresse IP virtuelle n'est effectuée avant l'expiration du temporisateur, l'entrée de persistance de l'adresse IP de ce client est supprimée. Si ce client revient après la suppression de l'entrée, la charge est équilibrée à nouveau sur un membre du pool en fonction de l'algorithme d'équilibrage de charge.
Purger les entrées (table pleine)	<p>Un délai d'expiration élevé peut entraîner le remplissage rapide de la table de persistance si le trafic est intense. Lorsque cette option est activée, l'entrée la plus ancienne est supprimée pour accepter l'entrée la plus récente.</p> <p>Lorsque cette option est désactivée, si la table de persistance IP source est complète, les nouvelles connexions clientes sont rejetées.</p>
Mise en miroir de la persistance HA	Faites basculer ce bouton pour synchroniser les entrées de persistance avec l'homologue HA. Lorsque la mise en miroir de persistance HA est activée, la persistance de l'adresse IP du client est maintenue en cas de basculement de l'équilibreur de charge.
Balises	<p>Entrez des balises pour faciliter la recherche.</p> <p>Vous pouvez spécifier une balise pour définir son étendue.</p>

4 Sélectionnez un profil de persistance de **Cookie** et entrez les détails du profil.

Option	Description
Nom et description	Entrez un nom et une description pour le profil de persistance des cookies.
Partager la persistance	<p>Faites basculer ce bouton pour partager la persistance entre plusieurs serveurs virtuels associés aux mêmes membres du pool.</p> <p>Le profil de persistance des cookies insère un cookie au format <i><nom>.<ID de profil>.<ID de pool></i>.</p> <p>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.</p> <p>L'équilibreur de charge insère un cookie au format <i><nom>.<ID du serveur virtuel>.<ID du pool></i>.</p>
Mode de cookie	<p>Sélectionnez un mode dans le menu déroulant.</p> <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. Un espace vide dans un nom de cookie n'est pas pris en charge.
Domaine de cookie	<p>Entrez le nom du domaine.</p> <p>Un domaine de cookie HTTP peut être configuré uniquement en mode INSERT.</p>
Option de secours de cookie	<p>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.</p> <p>Sélectionne un nouveau serveur qui traitera la demande client si le cookie pointe vers un serveur dont l'état est DÉSACTIVÉ ou INACTIF.</p>
Chemin d'accès au cookie	<p>Entrez le chemin d'URL du cookie.</p> <p>Un chemin d'accès au cookie HTTP peut être défini uniquement en mode INSERT.</p>
Chiffrement de cookie	<p>Faites basculer le bouton pour désactiver le chiffrement.</p> <p>Lorsque le chiffrement est désactivé, ces informations sont en texte brut.</p> <p>Chiffrez l'adresse IP et le port du serveur de cookie.</p>
Type de cookie	<p>Sélectionnez un type de cookie dans le menu déroulant.</p> <p>Cookie de session - non stocké. Sera perdu lors de la fermeture du navigateur.</p> <p>Cookie de persistance - stocké par le navigateur. Ne sera pas perdu lors de la fermeture du navigateur.</p>
Durée d'inactivité max	Entrez la durée en secondes pendant laquelle le type de cookie peut être inactif avant son expiration.
Durée de vie maximale du cookie	Pour le type de cookie de session, entrez la durée en secondes de disponibilité du cookie.
Balises	<p>Entrez des balises pour faciliter la recherche.</p> <p>Vous pouvez spécifier une balise pour définir son étendue.</p>

- 5 Sélectionnez **Générique** pour ajouter un profil de persistance générique et entrez les détails du profil.

Option	Description
Nom et description	Entrez un nom et une description pour le profil de persistance de l'adresse IP source.
Partager la persistance	Faites basculer ce bouton pour partager le profil entre les serveurs virtuels.
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'équilibreur de charge conserve les entrées pour enregistrer que les demandes des clients sont dirigées vers le même serveur.</p> <p>La toute première connexion à partir de l'adresse IP du nouveau client est équilibrée sur un membre du pool en fonction de l'algorithme d'équilibrage de charge. NSX stockera cette entrée de persistance sur la table de persistance de l'équilibrage de charge visible sur le nœud Edge qui héberge l'équilibrage de charge T1 actif via la commande CLI : <code>get load-balancer <LB-UUID> persistence-tables</code>.</p> <ul style="list-style-type: none"> ■ Lorsqu'il y a des connexions de ce client vers l'adresse IP virtuelle, l'entrée de persistance est conservée. ■ Lorsqu'il n'y a plus de connexions de ce client vers l'adresse IP virtuelle, l'entrée de persistance commence le compte à rebours du temporisateur spécifié dans la valeur « Délai d'expiration de l'entrée de persistance ». Si aucune nouvelle connexion de ce client vers l'adresse IP virtuelle n'est effectuée avant l'expiration du temporisateur, l'entrée de persistance de l'adresse IP de ce client est supprimée. Si ce client revient après la suppression de l'entrée, la charge est équilibrée à nouveau sur un membre du pool en fonction de l'algorithme d'équilibrage de charge.
Mise en miroir de la persistance HA	Faites basculer ce bouton pour synchroniser les entrées de persistance avec l'homologue HA.
Balises	<p>Entrez des balises pour faciliter la recherche.</p> <p>Vous pouvez spécifier une balise pour définir son étendue.</p>

Ajouter 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'équilibreur 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'équilibreur 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'équilibreur 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 7-5. Déchargement SSL

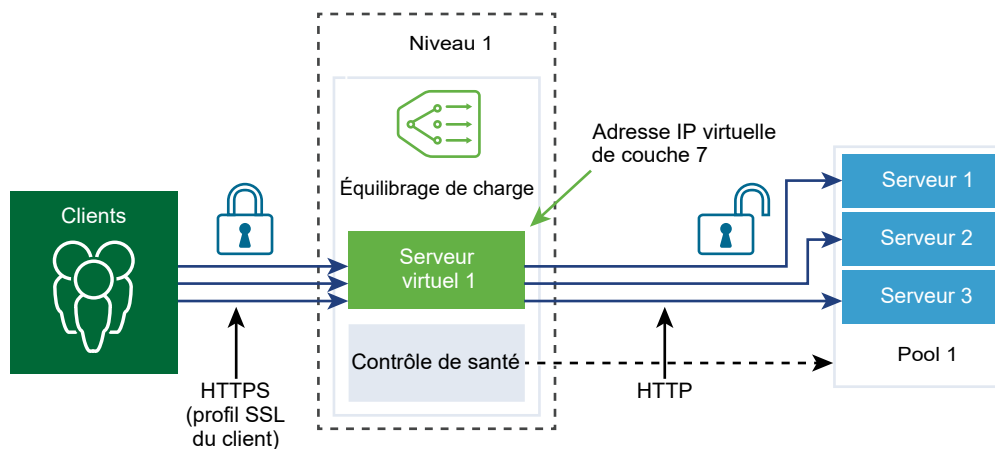
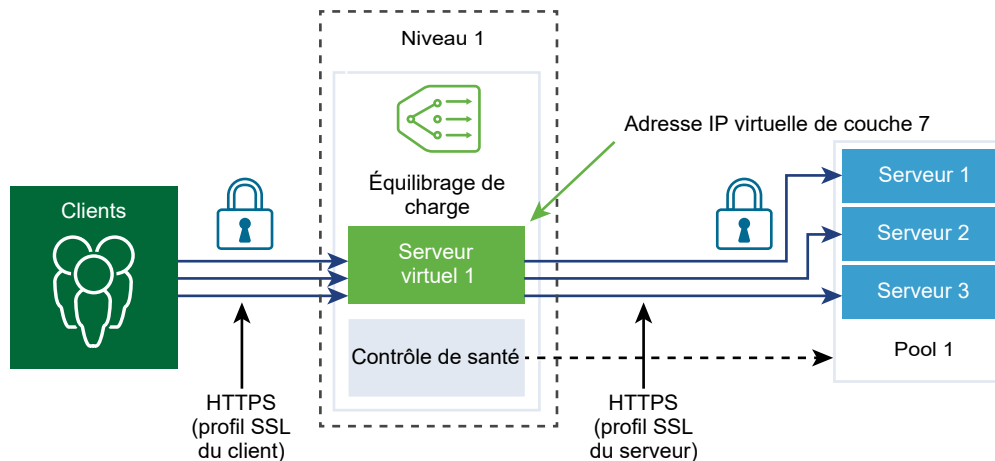


Figure 7-6. SSL de bout en bout



Procédure

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

2 Sélectionnez **Mise en réseau > Équilibrage de charge > Profils > Profil SSL**.

3 Sélectionnez un **profil SSL client** et entrez les détails du profil.

Option	Description
Nom et description	Entrez un nom et une description pour le profil SSL client.
Suite SSL	Sélectionnez le groupe de chiffrement SSL dans le menu déroulant. Les chiffrements et protocoles SSL disponibles à inclure dans le profil SSL client sont renseignés. Le groupe de chiffrement SSL équilibré est le groupe par défaut.
Mise en cache de session	Activez ce bouton pour autoriser le client et le serveur SSL à réutiliser les paramètres de sécurité précédemment négociés en évitant l'opération de clé publique coûteuse au cours de l'établissement de liaison SSL.
Balises	Entrez des balises pour faciliter la recherche. Vous pouvez spécifier une balise pour définir son étendue.
Chiffrements SSL pris en charge	En fonction de la suite SSL, les chiffrements SSL pris en charge sont renseignés ici. Cliquez sur Afficher plus pour afficher la liste complète. Si vous avez sélectionné Personnaliser , vous devez sélectionner les chiffrements SSL dans le menu déroulant.
Protocoles SSL pris en charge	En fonction de la suite SSL, les protocoles SSL pris en charge sont renseignés ici. Cliquez sur Afficher plus pour afficher la liste complète. Si vous avez sélectionné Personnaliser , vous devez sélectionner les chiffrements SSL dans le menu déroulant.
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.

4 Sélectionnez un **profil SSL serveur** et entrez les détails du profil.

Option	Description
Nom et description	Entrez un nom et une description pour le profil SSL de serveur.
Suite SSL	Sélectionnez le groupe de chiffrement SSL dans le menu déroulant. Les chiffrements et protocoles SSL disponibles à inclure dans le profil SSL serveur sont renseignés. Le groupe de chiffrement SSL équilibré est le groupe par défaut.
Mise en cache de session	Activez ce bouton pour autoriser le client et le serveur SSL à réutiliser les paramètres de sécurité précédemment négociés en évitant l'opération de clé publique coûteuse au cours de l'établissement de liaison SSL.
Balises	Entrez des balises pour faciliter la recherche. Vous pouvez spécifier une balise pour définir son étendue.

Option	Description
Chiffrements SSL pris en charge	En fonction de la suite SSL, les chiffrements SSL pris en charge sont renseignés ici. Cliquez sur Afficher plus pour afficher la liste complète. Si vous avez sélectionné Personnaliser , vous devez sélectionner les chiffrements SSL dans le menu déroulant.
Protocoles SSL pris en charge	En fonction de la suite SSL, les protocoles SSL pris en charge sont renseignés ici. Cliquez sur Afficher plus pour afficher la liste complète. Si vous avez sélectionné Personnaliser , vous devez sélectionner les chiffrements SSL dans le menu déroulant.
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.

Ajouter 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 [Ajouter un profil d'application](#).
- Vérifiez que les profils persistants sont disponibles. Reportez-vous à la section [Ajouter un profil de persistance](#).
- Vérifiez que les profils SSL pour le client et le serveur sont disponibles. Reportez-vous à la section [Ajouter un profil SSL](#).
- Vérifiez que les pools de serveurs sont disponibles. Reportez-vous à la section [Ajouter un pool de serveurs](#).
- Vérifiez qu'un équilibrage de charge est disponible. Reportez-vous à la section [Ajouter des équilibres de charge](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Équilibrage de charge > Serveurs virtuels > Ajouter un serveur virtuel**.
- 3 Sélectionnez un protocole **TCP L4** et entrez les détails du protocole.

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.

Option	Description
Nom et description	Entrez un nom et une description pour le serveur virtuel de couche 4.
Adresse IP	Entrez l'adresse IP du serveur virtuel.
Ports	Entrez le numéro de port du serveur virtuel.
Équilibrage de charge	Sélectionnez un équilibrage de charge existant à attacher à ce serveur virtuel de couche 4 dans le menu déroulant.
Pool de serveurs	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. Vous pouvez cliquer sur les points de suspension verticaux pour créer un pool de serveurs.
Profil d'application	Selon le type de protocole, le profil d'application existant est automatiquement renseigné. Vous pouvez cliquer sur les points de suspension verticaux pour créer un profil d'application.
Persistance	Sélectionnez un profil de persistance existant dans le menu déroulant. Un profil de persistance peut être activé sur un serveur virtuel afin d'autoriser l'envoi de connexions client associées à l'adresse IP source au même serveur.
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.
Pool de serveurs Sorry	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. Vous pouvez cliquer sur les points de suspension verticaux pour créer un pool de serveurs.

Option	Description
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.
État de l'administrateur	Faites basculer ce bouton pour désactiver l'état d'administration du serveur virtuel de couche 4.
Journal d'accès	Faites basculer ce bouton pour activer la journalisation pour le serveur virtuel de couche 4.
Balises	Entrez des balises pour faciliter la recherche. Vous pouvez spécifier une balise pour définir son étendue.

4 Sélectionnez un protocole **UDP L4** et entrez les détails du protocole.

Option	Description
Nom et description	Entrez un nom et une description pour le serveur virtuel de couche 4.
Adresse IP	Entrez l'adresse IP du serveur virtuel.
Ports	Entrez le numéro de port du serveur virtuel.
Équilibrage de charge	Sélectionnez un équilibrage de charge existant à attacher à ce serveur virtuel de couche 4 dans le menu déroulant.
Pool de serveurs	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. Vous pouvez cliquer sur les points de suspension verticaux pour créer un pool de serveurs.
Profil d'application	Selon le type de protocole, le profil d'application existant est automatiquement renseigné. Vous pouvez cliquer sur les points de suspension verticaux pour créer un profil d'application.
Persistance	Sélectionnez un profil de persistance existant dans le menu déroulant. Un profil de persistance peut être activé sur un serveur virtuel afin d'autoriser l'envoi de connexions client associées à l'adresse IP source au même serveur.
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.

Option	Description
Pool de serveurs Sorry	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. Vous pouvez cliquer sur les points de suspension verticaux pour créer un pool de serveurs.
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.
État de l'administrateur	Faites basculer ce bouton pour désactiver l'état d'administration du serveur virtuel de couche 4.
Journal d'accès	Faites basculer ce bouton pour activer la journalisation pour le serveur virtuel de couche 4.
Balises	Entrez des balises pour faciliter la recherche. Vous pouvez spécifier une balise pour définir son étendue.

Ajouter des serveurs virtuels HTTP 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'équilibreur de charge sont prises en charge uniquement pour les serveurs virtuels de couche 7 avec un profil d'application HTTP. Différents services d'équilibreur de charge peuvent utiliser les règles d'équilibreur de charge.

Note Le relais SSL de couche 7 est pris en charge dans NSX-T Data Center 3.0 et versions ultérieures.

Chaque règle d'équilibreur 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'équilibreur 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'équilibreur de charge soit considérée comme une correspondance.

Chaque règle d'équilibreur 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 équilibreur de charge, les connexions actives à ce serveur échouent.

Note Le profil SSL n'est pas pris en charge dans la version Limited Export de NSX-T Data Center.

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 que les profils d'application sont disponibles. Reportez-vous à la section [Ajouter un profil d'application](#).
- Vérifiez que les profils persistants sont disponibles. Reportez-vous à la section [Ajouter un profil de persistance](#).
- Vérifiez que les profils SSL pour le client et le serveur sont disponibles. Reportez-vous à la section [Ajouter un profil SSL](#).
- Vérifiez que les pools de serveurs sont disponibles. Reportez-vous à la section [Ajouter un pool de serveurs](#).
- 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](#).
- Vérifiez qu'un équilibreur de charge est disponible. Reportez-vous à la section [Ajouter des équilibrages de charge](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau > Équilibrage de charge > Serveurs virtuels > Ajouter un serveur virtuel**.

3 Sélectionnez un protocole **HTTP L7** et entrez les détails du protocole.

Les serveurs virtuels de couche 7 prennent en charge les protocoles HTTP et HTTPS.

Option	Description
Nom et description	Entrez un nom et une description pour le serveur virtuel de couche 7.
Adresse IP	Entrez l'adresse IP du serveur virtuel.
Ports	Entrez le numéro de port du serveur virtuel.
Équilibreur de charge	Sélectionnez un équilibreur de charge existant à attacher à ce serveur virtuel de couche 4 dans le menu déroulant.
Pool de serveurs	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. Vous pouvez cliquer sur les points de suspension verticaux pour créer un pool de serveurs.
Profil d'application	Selon le type de protocole, le profil d'application existant est automatiquement renseigné. Vous pouvez cliquer sur les points de suspension verticaux pour créer un profil d'application.
Persistance	Sélectionnez un profil de persistance existant dans le menu déroulant. Un profil de persistance peut être activé sur un serveur virtuel afin d'autoriser l'envoi de connexions client associées à l'adresse IP source et aux cookies au même serveur.

4 Cliquez sur **Configurer** pour définir le SSL du serveur virtuel de couche 7.

Vous pouvez configurer le SSL client et le SSL serveur.

5 Configurez le SSL client.

Option	Description
SSL client	Faites basculer ce bouton 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.
Certificat par défaut	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).
Profil SSL client	Sélectionnez le profil SSL côté client dans le menu déroulant.
Certificats SNI	Sélectionnez les certificats SNI disponibles dans le menu déroulant.
Certificats d'autorité de certification approuvés	Sélectionnez le certificat d'autorité de certification disponible.
Authentification de client obligatoire	Faites basculer le bouton pour activer cet élément de menu.

Option	Description
Profondeur de la chaîne de certificats	Définissez la profondeur de la chaîne de certificats pour vérifier la profondeur de la chaîne de certificats du serveur.
Liste de révocation de certificat	Sélectionnez la liste de révocation des certificats (CRL) disponible pour interdire les certificats de serveur compromis.

6 Configurez le SSL serveur.

Option	Description
SSL serveur	Faites basculer ce bouton pour activer le profil.
Certificat client	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 (Server Name Indication, indication de nom de serveur).
Profil SSL serveur	Sélectionnez le profil SSL côté serveur dans le menu déroulant.
Certificats d'autorité de certification approuvés	Sélectionnez le certificat d'autorité de certification disponible.
Authentification du serveur obligatoire	Faites basculer le bouton pour activer cet élément de menu. La liaison de profil SSL côté serveur indique si le certificat de serveur présenté à l'équilibreur 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.
Profondeur de la chaîne de certificats	Définissez la profondeur de la chaîne de certificats pour vérifier la profondeur de la chaîne de certificats du serveur.
Liste de révocation de certificat	Sélectionnez la liste de révocation des certificats (CRL) disponible pour interdire les certificats de serveur compromis. Le protocole OCSP et l'association OCSP ne sont pas pris en charge côté serveur.

7 Configurez les propriétés supplémentaires du serveur virtuel de couche 7.

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 équilibreur 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.
Pool de serveurs Sorry	Sélectionnez un pool de serveurs Désolé existant dans le menu déroulant. Le pool de serveurs Désolé répond à la demande lorsqu'un équilibreur de charge ne peut pas sélectionner un serveur principal pour répondre à la demande depuis le pool par défaut. Vous pouvez cliquer sur les points de suspension verticaux pour créer un pool de serveurs.

Option	Description
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.
État de l'administrateur	Faites basculer ce bouton pour désactiver l'état d'administration du serveur virtuel de couche 7.
Journal d'accès	Faites basculer ce bouton pour activer la journalisation pour le serveur virtuel de couche 7.
Balises	Entrez des balises pour faciliter la recherche. Vous pouvez spécifier une balise pour définir son étendue.

8 Cliquez sur **Enregistrer**.

Ajouter des règles d'équilibreur de charge

Avec les serveurs virtuels HTTP de couche 7, vous pouvez éventuellement configurer des règles d'équilibreur de charge et personnaliser le comportement de l'équilibrage de charge à l'aide de règles de correspondance ou d'action.

Les règles d'équilibreur 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" $article = "news1234.html"`. Une fois les variables configurées, elles peuvent être utilisées dans les actions de règle d'équilibreur de charge. Par exemple, l'URI peut être réécrit en utilisant des variables mises en correspondance, telles que `/news.py?year=$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 `_`.

- `$_args` : arguments de la demande
- `$_arg_<nom>` : argument `<nom>` dans la ligne de demande
- `$_cookie_<nom>` : valeur du cookie `<nom>`
- `$_upstream_cookie_<nom>` : cookie avec le nom spécifié envoyé par le serveur en amont dans le champ d'en-tête de réponse « Set-Cookie »
- `$_upstream_http_<nom>` : champ d'en-tête de demande arbitraire, `<nom>` étant le nom du champ converti en minuscules dans lequel les tirets sont remplacés par des traits de soulignement
- `$_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
- `$_http_<nom>` : champ d'en-tête de demande arbitraire, `<nom>` étant le nom du champ converti en minuscules dans lequel les tirets sont remplacés par des traits de soulignement
- `$_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
- `$_server_protocol` - protocole de la demande, généralement « HTTP/1.0 » ou « HTTP/1.1 »
- (NSX-T Data Center 2.5.0 uniquement) `$_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.
- (NSX-T Data Center 2.5.1 et versions ultérieures) `$_Ssl_client_escaped_cert` : renvoie le certificat client au format PEM pour une connexion SSL établie.
- `$_ssl_server_name` - renvoie le nom du serveur demandé par le biais de SNI
- `$_uri` - chemin d'accès URI dans la demande
- `$_ssl_ciphers` : renvoie les chiffrements SSL du client
- `$_ssl_client_i_dn` : renvoie la chaîne « issuer DN » du certificat client pour une connexion SSL établie conformément à la norme RFC 2253
- `$_ssl_client_s_dn` : renvoie la chaîne « subject DN » du certificat client pour une connexion SSL établie conformément à la norme RFC 2253
- `$_ssl_protocol` : renvoie le protocole d'une connexion SSL établie
- `$_ssl_session_reused` : renvoie « r » si une session SSL a été réutilisée ou « . » sinon

Conditions préalables

Vérifiez qu'un serveur virtuel HTTP de couche 7 est disponible. Reportez-vous à la section [Ajouter des serveurs virtuels HTTP de couche 7](#).

Procédure

- 1 Ouvrez le serveur virtuel HTTP de couche 7.

- 2 Dans la section Règles d'équilibreur de charge, cliquez sur **Définir > Ajouter une règle** pour configurer les règles d'équilibreur de charge pour la phase de 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
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
Cookie de demande HTTP	Correspondance à n'importe quel cookie de demande HTTP. http_request.cookie_value - valeur à faire correspondre
Corps de la demande HTTP	Correspondance au contenu du corps d'une demande HTTP. http_request.body_value - valeur à faire correspondre
SSL client	Correspondance à l'ID de profil SSL du client. ssl_profile_id - valeur à faire correspondre
Port 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
Source d'en-tête 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
Variable	Créez une variable et attribuez une valeur à la variable.
Sensible à la casse	Définissez un indicateur sensible à la casse pour la comparaison des valeurs de l'en-tête HTTP.

Actions	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

Actions	Description
	http_request.header_value - valeur à écrire
Suppression d'en-tête de demande HTTP	Supprimez l'en-tête HTTP. http_request.header_delete - nom d'en-tête http_request.header_delete - valeur à écrire

- 3 Cliquez sur **Transfert de la demande > Ajouter une règle** pour configurer les règles d'équilibreur 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
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
Cookie de demande HTTP	Correspondance à n'importe quel cookie de demande HTTP. http_request.cookie_value - valeur à faire correspondre
Corps de la demande HTTP	Correspondance au contenu du corps d'une demande HTTP. http_request.body_value - valeur à faire correspondre
SSL client	Correspondance à l'ID de profil SSL du client. ssl_profile_id - valeur à faire correspondre
Port 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
Source d'en-tête 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

Condition de correspondance prise en charge	Description
Variable	Créez une variable et attribuez une valeur à la variable.
Sensible à la casse	Définissez un indicateur sensible à la casse pour la comparaison des valeurs de l'en-tête HTTP.
Action	Description
Rejet HTTP	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
Redirection HTTP	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
Inspection de persistance de variable	Sélectionnez un profil de persistance générique et entrez un nom de variable. Vous pouvez également activer le champ Variable de hachage . Si la valeur de la variable est très longue, le hachage de la variable permet de s'assurer qu'elle sera correctement stockée dans le tableau de persistance. Si le champ Variable de hachage n'est pas activé, seule la partie de préfixe fixe de la valeur de la variable est stockée dans le tableau de persistance si la valeur de la variable est très longue. Par conséquent, deux demandes différentes avec des valeurs de variables longues peuvent être envoyées au même serveur principal (car leurs valeurs de variables ont la même partie de préfixe) lorsqu'elles doivent être envoyées à différents serveurs principaux.
Statut de la réponse	Affiche l'état de la réponse.
Message de réponse	Le serveur renvoie un message de réponse qui contient les adresses confirmées et la configuration.

- 4 Cliquez sur **Réécriture de la réponse > Ajouter une règle** pour configurer les règles d'équilibreur 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
Méthode de réponse HTTP	Correspondance à une méthode de réponse HTTP. http_response.method - valeur à faire correspondre
URI de réponse HTTP	Correspondance à un URI de réponse HTTP. http_response.uri - valeur à faire correspondre

Condition de correspondance prise en charge	Description
Arguments d'URI de réponse HTTP	Correspondance à des arguments URI de réponse HTTP. http_response.uri_args - valeur à faire correspondre
Version de réponse HTTP	Correspondance à une version de réponse HTTP. http_response.version - valeur à faire correspondre
Cookie de réponse HTTP	Correspondance à n'importe quel cookie de réponse HTTP. http_response.cookie_value - valeur à faire correspondre
SSL client	Correspondance à l'ID de profil SSL du client. ssl_profile_id - valeur à faire correspondre
Port 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
Source d'en-tête 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
Variable	Créez une variable et attribuez une valeur à la variable.
Sensible à la casse	Définissez un indicateur sensible à la casse pour la comparaison des valeurs de l'en-tête HTTP.
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
Suppression d'en-tête de réponse HTTP	Supprimez l'en-tête HTTP. http_request.header_delete - nom d'en-tête http_request.header_delete - valeur à écrire
Apprentissage de persistance de variable	Sélectionnez un profil de persistance générique et entrez un nom de variable. Vous pouvez également activer le champ Variable de hachage . Si la valeur de la variable est très longue, le hachage de la variable permet de s'assurer qu'elle sera correctement stockée dans le tableau de persistance. Si le champ Variable de hachage n'est pas activé, seule la partie de préfixe fixe de la valeur de la variable est stockée dans le tableau de persistance si la valeur de la variable est très longue. Par conséquent, deux demandes différentes avec des valeurs de variables longues peuvent être envoyées au même serveur principal (car leurs valeurs de variables ont la même partie de préfixe) lorsqu'elles doivent être envoyées à différents serveurs principaux.

Groupes créés pour les pools de serveurs et les serveurs virtuels

NSX Manager crée automatiquement des groupes pour les pools de serveurs d'équilibreur de charge et les ports VIP.

Les groupes d'équilibreur de charge créés sont visibles sous **Inventaire > Groupes**.

Les groupes de pool de serveurs sont créés avec le nom NLB.PoolLB. *Pool_Name LB_Name* avec des adresses IP de membres de groupe attribuées :

- Pool configuré sans LB-SNAT (transparent) : 0.0.0.0/0
- Pool configuré sans mappage automatique LB-SNAT : IP de liaison montante T1 100.64.x.y et IP de l'interface du service T1
- Pool configuré sans pool IP LB-SNAT : Pool IP LB-SNAT

Les groupes d'adresses IP virtuelles sont créés avec le nom NLB.VIP. *Le nom du serveur virtuel* et les adresses IP du membre du groupe d'adresses IP virtuelles sont VIP IP@.

Pour les groupes de pool de serveurs, vous pouvez créer une règle pour autoriser le pare-feu de trafic distribué à partir de l'équilibreur de charge (NLB.PoolLB. *Pool_Name LB_Name*). Pour le pare-feu de passerelle de niveau 1, vous pouvez créer un trafic autorisant les clients vers LB VIP NLB.VIP. *nom du serveur virtuel*.

Stratégies de transfert

8

Cette fonctionnalité se rapporte à NSX Cloud.

Les règles de stratégies de transfert ou de routage basé sur les stratégies définissent la façon dont NSX-T gère le trafic à partir d'une VM gérée par NSX. Ce trafic peut être dirigé vers la superposition NSX-T ou il peut être acheminé via le réseau du fournisseur de cloud (sous-couche).

Note Reportez-vous à la section [Chapitre 22 Utilisation de NSX Cloud](#) pour plus d'informations sur la gestion de vos machines virtuelles de charge de travail de cloud public avec NSX-T Data Center.

Trois stratégies de transfert par défaut sont configurées automatiquement après le déploiement d'une PCG sur un VPC/VNet de transit ou la liaison entre un VPC/VNet de calcul et le transit.

- 1 Une **route vers la sous-couche** pour tout le trafic résolu dans le VPC/VNet de transit et de calcul.
- 2 Une autre **route vers la sous-couche** pour tout le trafic destiné aux services de métadonnées du cloud public.
- 3 Une **route vers la superposition** pour tous les autres trafics, par exemple, le trafic dirigé à l'extérieur du VPC/VNet de transit et de calcul. Ce trafic est acheminé sur le tunnel de superposition NSX-T vers la PCG, puis vers sa destination.

Note Pour le trafic destiné à un autre VPC/VNet géré par la même PCG : le trafic est routé depuis le VPC/VNet géré par NSX source via le tunnel de superposition NSX-T vers la PCG, puis acheminé vers le VPC/VNet de destination.

Pour le trafic destiné à un autre VPC/VNet géré par une PCG différente : le trafic est acheminé d'un VPC/VNet géré par NSX sur le tunnel de superposition NSX vers la PCG du VPC/VNet source et transféré vers la PCG du VPC/VNet géré par NSX de destination.

Si le trafic est dirigé sur Internet, la PCG le dirige vers la destination sur Internet.

Micro-segmentation lors du routage vers la sous-couche

La micro-segmentation est appliquée, même pour les VM de charge de travail dont le trafic est acheminé vers le réseau de sous-couche.

Si vous disposez d'une connectivité directe entre une VM de charge de travail gérée par NSX et une destination en dehors du VPC/VNet géré et que vous voulez contourner la PCG, configurez une stratégie de transfert pour acheminer le trafic de cette VM via la sous-couche.

Lorsque le trafic est acheminé via le réseau de sous-couche, la PCG est contournée et, par conséquent, le pare-feu nord-sud n'est pas rencontré par le trafic. Toutefois, vous devez toujours gérer les règles pour le trafic est-ouest ou le pare-feu distribué (DFW), car ces règles sont appliquées au niveau de la VM avant d'atteindre la PCG.

Stratégies de transfert prises en charge et cas d'utilisation courants

Vous pouvez voir une liste des stratégies de transfert dans le menu déroulant, mais dans cette version, seules les stratégies de transfert suivantes sont prises en charge :

- Route vers la sous-couche
- Route à partir de la sous-couche
- Route vers la superposition

Voici les scénarios courants dans lesquels les stratégies de transfert sont utiles :

- **Route vers la sous-couche** : accédez à un service sur la sous-couche à partir d'une VM gérée par NSX. Par exemple, l'accès au service AWS S3 sur le réseau de sous-couche AWS.
- **Route à partir de la sous-couche** : accédez à un service hébergé sur une VM gérée par NSX à partir du réseau de sous-couche. Par exemple, l'accès à partir d'AWS ELB vers la VM gérée par NSX.

Ce chapitre contient les rubriques suivantes :

- [Ajouter ou modifier des stratégies de transfert](#)

Ajouter ou modifier des stratégies de transfert

Vous pouvez modifier les stratégies de transfert créées automatiquement ou en ajouter de nouvelles.

Par exemple, pour utiliser les services fournis par le cloud public, tels que S3 par AWS, vous pouvez créer manuellement une stratégie pour autoriser un ensemble d'adresses IP à accéder à ce service par routage via la sous-couche.

Conditions préalables

Vous devez disposer d'un VPC ou d'un VNet avec un PCG déployé sur celui-ci.

Procédure

- 1 Cliquez sur **Ajouter une section**. Nommez la section de façon appropriée (par exemple, **Services AWS**).

- 2 Cochez la case en regard de la section et cliquez sur **Ajouter une règle**. Nommez la règle (par exemple, **Règles S3**).
- 3 Dans l'onglet **Sources**, sélectionnez le VPC ou le VNet dans lequel se trouvent les machines virtuelles de charge de travail auxquelles vous souhaitez fournir l'accès au service (par exemple, le VPC AWS). Vous pouvez également créer un **Groupe** ici pour inclure plusieurs machines virtuelles correspondant à un ou plusieurs critères.
- 4 Dans l'onglet **Destinations**, sélectionnez le VPC ou le VNet sur lequel le service est hébergé (par exemple, un **Groupe** qui contient l'adresse IP du service S3 dans AWS).
- 5 Dans l'onglet **Services**, sélectionnez le service dans le menu déroulant. Si le service n'existe pas, vous pouvez l'ajouter. Vous pouvez également laisser la sélection sur **Tous** si vous pouvez fournir les détails de routage sous **Destinations**.
- 6 Dans l'onglet **Action**, sélectionnez la manière dont vous souhaitez que le routage fonctionne. Par exemple, sélectionnez **Route vers la sous-couche** si vous configurez cette stratégie pour le service S3 AWS.
- 7 Cliquez sur **Publier** pour terminer la configuration de la stratégie de transfert.

IP Address Management (IPAM)

9

Pour gérer des adresses IP, vous pouvez configurer le DNS (système de noms de domaine), le DHCP (protocole DHCP), des pools d'adresses IP et des blocs d'adresses IP.

Note Les blocs d'adresses IP sont utilisés par NSX 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 et Cloud Foundry*.

Ce chapitre contient les rubriques suivantes :

- [Ajouter une zone DNS](#)
- [Ajouter un service de transfert DNS](#)
- [Ajouter un serveur DHCP](#)
- [Configurer un serveur de relais DHCP pour une passerelle de niveau 0 ou de niveau 1](#)
- [Ajouter un pool d'adresses IP](#)
- [Ajouter un bloc d'adresses IP](#)

Ajouter une zone DNS

Vous pouvez configurer des zones DNS pour votre service DNS. Une zone DNS est une partie distincte de l'espace de nom de domaine dans le DNS.

Lorsque vous configurez une zone DNS, vous pouvez spécifier une adresse IP source à utiliser par un redirecteur DNS lors du transfert de requêtes DNS vers un serveur DNS en amont. Si vous ne spécifiez pas d'adresse IP source, l'adresse IP source du paquet de requêtes DNS sera l'adresse IP de l'écouteur du redirecteur DNS. La spécification d'une adresse IP source est nécessaire si l'adresse IP de l'écouteur est une adresse interne qui n'est pas accessible depuis le serveur DNS en amont externe. Pour vous assurer que les paquets de réponses DNS sont redirigés vers le redirecteur, une adresse IP source dédiée est requise. Vous pouvez également configurer SNAT sur le routeur logique pour convertir l'adresse IP de l'écouteur en adresse IP publique. Dans ce cas, il n'est pas nécessaire de spécifier une adresse IP source.

Procédure

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

- 2 Sélectionnez **Mise en réseau > Gestion des adresses IP > DNS**.
- 3 Cliquez sur l'onglet **Zones DNS**.
- 4 Pour ajouter une zone par défaut, sélectionnez **Ajouter une zone DNS > Ajouter une zone par défaut**
 - a Entrez un nom et éventuellement une description.
 - b Entrez l'adresse IP de trois serveurs DNS maximum.
 - c (Facultatif) Entrez l'adresse IP dans le champ **Adresse IP source**.
- 5 Pour ajouter une zone de nom de domaine complet, sélectionnez **Ajouter une zone DNS > Ajouter une zone de FQDN**
 - a Entrez un nom et éventuellement une description.
 - b Entrez un nom de domaine complet pour le domaine.
 - c Entrez l'adresse IP de trois serveurs DNS maximum.
 - d (Facultatif) Entrez l'adresse IP dans le champ **Adresse IP source**.
- 6 Cliquez sur **Enregistrer**.

Ajouter un service de transfert DNS

Vous pouvez configurer un redirecteur DNS pour transférer des requêtes DNS à des serveurs DNS externes.

Avant de configurer un redirecteur DNS, vous devez configurer une zone DNS par défaut. Vous pouvez configurer une ou plusieurs zones FQDN DNS. Chaque zone DNS est associée à 3 serveurs DNS au maximum. Lorsque vous configurez une zone FQDN DNS, vous spécifiez un ou plusieurs noms de domaine. Un redirecteur DNS est associé à une zone DNS par défaut et à 5 zones FQDN DNS au maximum. Lorsqu'une requête DNS est reçue, le redirecteur DNS compare le nom de domaine dans la requête avec les noms de domaine dans les zones FQDN DNS. Si une correspondance est trouvée, la requête est transférée aux serveurs DNS spécifiés dans la zone FQDN DNS. Si aucune correspondance n'est trouvée, la requête est transférée aux serveurs DNS spécifiés dans la zone DNS par défaut.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Gestion des adresses IP > DNS**.
- 3 Cliquez sur **Ajouter un service DNS**.
- 4 Entrez un nom et éventuellement une description.
- 5 Sélectionnez une passerelle de niveau 0 ou 1.

6 Entrez l'adresse IP du service DNS.

Les clients envoient des requêtes DNS à cette adresse IP, qui est également appelée IP de l'écouteur du redirecteur DNS.

7 Sélectionnez une zone DNS par défaut.

8 Sélectionnez un niveau de journalisation.

9 Sélectionnez jusqu'à cinq zones de nom de domaine complet.

10 Cliquez sur le bouton bascule **Statut administratif** pour activer ou désactiver le service DNS.

11 Cliquez sur **Enregistrer**.

Ajouter un serveur DHCP

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 les demandes DHCP.

Note Le serveur DHCP créé à l'aide de cette procédure n'est pas pris en charge sur un segment dépendant d'un VLAN. Vous devez utiliser la fonctionnalité DHCP sous **Mise en réseau et sécurité avancées** pour créer un serveur DHCP pris en charge sur un commutateur logique dépendant d'un VLAN.

Procédure

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

2 Sélectionnez **Mise en réseau > Gestion des adresses IP > DHCP**.

3 Cliquez sur **Ajouter un serveur**.

4 Sélectionnez **Serveur DHCP** comme type de serveur.

5 Entrez le nom du serveur.

6 Entrez l'adresse IP du serveur au format CIDR.

Cette étape va créer deux ports logiques (un pour une interface logique et l'autre pour le serveur DHCP lui-même) et connecter le serveur DHCP à un commutateur logique DHCP spécifique. Cette interface apparaîtra sur la passerelle de niveau 0 ou de niveau 1 en tant qu'interface connectée, donc veillez à choisir un sous-réseau qui ne se chevauche pas pour la passerelle de niveau 1 ou de niveau 0 à laquelle vous souhaitez attribuer le serveur DHCP. Vous pouvez spécifier <IP address>/30 à cette fin. La plage de sous-réseau utilisée ici n'est pas annoncée à la passerelle de niveau 0 connectée, mais elle figure dans la table de transfert de la passerelle de niveau 1.

7 Entrez une durée de bail.

- 8 Sélectionnez un cluster NSX Edge.
- 9 Cliquez sur **Enregistrer**.
- 10 Pour attribuer un serveur DHCP à une passerelle de niveau 0 ou de niveau 1 :
 - a Accédez à **Mise en réseau > Passerelles de niveau 0** ou **Mise en réseau > Passerelles de niveau 1**.
 - b Modifiez une passerelle existante.
 - c Dans le champ **Gestion des adresses IP**, cliquez sur **Aucune allocation d'adresses IP**.
 - d Sélectionnez **Serveur DHCP local** dans la liste déroulante Type.
 - e Sélectionnez un serveur DHCP.
 - f Cliquez sur **Enregistrer**.
 - g Cliquez sur **Enregistrer**.
- 11 Pour attribuer un serveur DHCP à un segment :
 - a Accédez à **Mise en réseau > Segments**.
 - b Ajoutez ou modifiez un segment.
Le segment doit être associé à une passerelle de niveau 0 ou de niveau 1.
 - c Cliquez sur **Définir les sous-réseaux** si vous ajoutez un nouveau segment ou cliquez sur le nombre sous **Sous-réseaux** pour ajouter ou modifier un sous-réseau.
 - d Entrez les plages DHCP appropriées.
 - e Cliquez sur **Appliquer**.
 - f Cliquez sur **Enregistrer**.

Configurer un serveur de relais DHCP pour une passerelle de niveau 0 ou de niveau 1

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 un serveur de relais DHCP pour relayer le trafic DHCP vers des serveurs DHCP externes.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Gestion des adresses IP > DHCP**.
- 3 Cliquez sur **Ajouter un serveur**.
- 4 Sélectionnez **Relais DHCP** comme type de serveur.

- 5 Entrez le nom du serveur de relais.
- 6 Entrez une ou plusieurs adresses IP pour le serveur.
- 7 Cliquez sur **Enregistrer**.
- 8 Accédez à **Mise en réseau > Passerelles de niveau 0** ou **Mise en réseau > Passerelles de niveau 1** pour configurer un serveur de relais DHCP pour une passerelle.
- 9 Modifiez la passerelle appropriée.
- 10 Dans le champ **Gestion des adresses IP**, cliquez sur **Aucune allocation d'adresses IP** pour une passerelle de niveau 0 ou sur **Aucune allocation d'adresses IP définie** pour une passerelle de niveau 1.
- 11 Dans le champ **Type**, sélectionnez **Relais DHCP**.
- 12 Dans le champ **Relais DHCP**, sélectionnez le serveur de relais DHCP que vous avez créé précédemment.
- 13 Cliquez sur **Enregistrer**.
- 14 Pour chaque segment connecté à la passerelle qui utilisera ce service de relais DHCP, vous devez spécifier des plages DHCP pour que le relais fonctionne.
 - a Accédez à **Mise en réseau > Segments**.
 - b Ajoutez ou modifiez un segment.
 - c Cliquez sur **Définir les sous-réseaux** si vous ajoutez un nouveau segment ou cliquez sur le nombre sous **Sous-réseaux** pour modifier un sous-réseau.
 - d Spécifiez une ou plusieurs plages DHCP.

Cela est nécessaire pour que le relais fonctionne.
 - e Cliquez sur **Appliquer**.
 - f Cliquez sur **Enregistrer**.

Ajouter un pool d'adresses IP

Vous pouvez configurer des pools d'adresses IP pour une utilisation par composants, comme DHCP.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Gestion des adresses IP > Pools d'adresses IP**.
- 3 Cliquez sur **Ajouter un pool d'adresses IP**.
- 4 Entrez un nom et éventuellement une description.
- 5 Cliquez sur **Définir** dans la colonne **Sous-réseaux** pour ajouter des sous-réseaux.

- 6 Pour indiquer un bloc d'adresses, sélectionnez **Ajouter un sous-réseau > Bloc d'adresses IP**.
 - a Sélectionnez un bloc d'adresses IP.
 - b Indiquez une taille.
 - c Cliquez sur le commutateur **Passerelle d'attribution automatique** pour activer ou désactiver l'attribution automatique d'adresses IP de la passerelle.
 - d Cliquez sur **Ajouter**.
- 7 Pour indiquer des plages d'adresses IP, sélectionnez **Ajouter un sous-réseau > Plages d'adresses IP**.
 - a Entrez des plages d'adresses IPv4 ou IPv6.
 - b Entrez des plages d'adresses IP au format CIDR.
 - c Entrez une adresse pour **Adresse IP de la passerelle**.
 - d Cliquez sur **Ajouter**.
- 8 Cliquez sur **Enregistrer**.

Ajouter un bloc d'adresses IP

Vous pouvez configurer les blocs d'adresses IP pour une utilisation par d'autres composants.

Note Vous pouvez également ajouter un bloc d'adresses IP en accédant à **Mise en réseau avancée et sécurité > Mise en réseau > IPAM**.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau > Gestion des adresses IP > Pools d'adresses IP**.
- 3 Cliquez sur l'onglet **Blocs d'adresses IP**.
- 4 Cliquez sur **Ajouter un bloc d'adresses IP**.
- 5 Entrez un nom et éventuellement une description.
- 6 Entrez un bloc d'adresses IP au format CIDR.
- 7 Cliquez sur **Enregistrer**.

Les rubriques de cette section couvrent la sécurité nord-sud et est-ouest pour les règles de pare-feu distribué, le pare-feu d'identité, l'introspection réseau, le pare-feu de passerelle et les stratégies de protection des points de terminaison.

Ce chapitre contient les rubriques suivantes :

- [Présentation de la configuration de la sécurité](#)
- [Terminologie de la sécurité](#)
- [Pare-feu d'identité](#)
- [Profil de contexte de couche 7](#)
- [Pare-feu distribué](#)
- [Sécurité du réseau est-ouest : chaînage des services tiers](#)
- [Configuration d'un pare-feu de passerelle](#)
- [Sécurité du réseau nord-sud : insertion de service tiers](#)
- [Protection de point de terminaison](#)
- [Profils de sécurité](#)

Présentation de la configuration de la sécurité

Configurez des stratégies de pare-feu horizontal et vertical dans des catégories prédéfinies pour votre environnement.

Le pare-feu distribué (horizontal) et le pare-feu de passerelle (vertical) offrent plusieurs ensembles de règles configurables, divisés en catégories. 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 stratégies de sécurité s'appliquent comme suit :

- Les règles sont traitées par catégorie, de gauche à droite.
- 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, elles seront appliquées avant des règles plus spécifiques.

Terminologie de la sécurité

Les termes suivants sont utilisés dans le pare-feu distribué.

Tableau 10-1. Terminologie liée à la sécurité

Construction	Définition
Stratégie	Une stratégie de sécurité inclut divers éléments de sécurité, notamment des règles de pare-feu et des configurations de service. La stratégie était précédemment appelée une section de pare-feu.
Règle	Ensemble de paramètres auxquels les flux sont comparés et qui déterminent les mesures prises en cas de correspondance. Les règles comprennent des paramètres tels que la source et la destination, le service, le profil de contexte, la journalisation et les balises.
Groupe	<p>Les groupes comprennent différents objets, ajoutés à la fois statiquement et dynamiquement, et pouvant faire office de champs source et de destination pour une règle de pare-feu. Des groupes peuvent être configurés de manière à comporter un ensemble de machines virtuelles, d'adresses IP, d'adresses MAC, de ports logiques, de commutateurs logiques, de groupes d'utilisateurs AD et d'autres groupes imbriqués. L'inclusion dynamique de groupes peut reposer sur une balise, un nom de machine, un nom de système d'exploitation ou un nom d'ordinateur.</p> <p>Lorsque vous créez un groupe, vous devez inclure un domaine auquel il appartient et, par défaut, ce dernier sera le domaine par défaut.</p> <p>Les groupes étaient précédemment appelés NSGroup ou groupe de sécurité.</p>
Service	Définit une combinaison, ou un port et un protocole. Utilisé pour classer le trafic en fonction d'un port et d'un protocole. Des services prédéfinis et des services définis par l'utilisateur peuvent être utilisés dans les règles de pare-feu.
Profil de contexte	Définit des attributs basés sur le contexte, notamment le nom de domaine et l'ID d'application. Comprend également des sous-attributs, comme la version de l'application ou un ensemble de chiffrement. Les règles de pare-feu peuvent inclure un profil de contexte pour activer des règles de pare-feu de couche 7.

Pare-feu d'identité

Les fonctionnalités de pare-feu d'identité (IDFW) permettent à un administrateur NSX de créer des règles de pare-feu distribué (DFW) basées sur l'utilisateur Active Directory.

IDFW peut être utilisé pour des postes de travail virtuels (VDI) ou des sessions de poste de travail distant (prise en charge RDSH), l'activation de connexions simultanées par plusieurs utilisateurs, l'accès aux applications d'utilisateur en fonction de conditions requises et la possibilité de maintenir des environnements utilisateur indépendants. Les systèmes de gestion VDI contrôlent les utilisateurs autorisés à accéder aux machines virtuelles VDI. NSX-T contrôle l'accès aux serveurs de destination à partir de la machine virtuelle (VM) source sur laquelle l>IDFW est activé. Avec RDSH, les administrateurs créent des groupes de sécurité avec différents utilisateurs dans Active Directory (AD) et autorisent ou refusent l'accès à ces utilisateurs à un serveur d'applications selon leur rôle. Par exemple, les ressources humaines et l'ingénierie peuvent se connecter au même serveur RDSH et ont accès à différentes applications à partir de ce serveur.

L>IDFW peut également être utilisé sur les machines virtuelles dont les systèmes d'exploitation sont pris en charge. Reportez-vous à la section [Configurations prises en charge par le pare-feu d'identité](#).

La configuration d>IDFW commence par la préparation de l'infrastructure. Pour cela, l'administrateur installe les composants de préparation de l'hôte sur chaque cluster protégé et configure la synchronisation Active Directory pour que NSX puisse consommer des utilisateurs et des groupes AD. Ensuite, IDFW doit savoir à quel poste de travail un utilisateur Active Directory se connecte pour appliquer des règles IDFW. Lorsque des événements réseau sont générés par un utilisateur, l'agent léger installé avec VMware Tools sur la machine virtuelle rassemble les informations et les transfère au moteur de contexte. Ces informations sont utilisées pour permettre leur application pour le pare-feu distribué.

IDFW traite l'identité de l'utilisateur à la source uniquement dans les règles de pare-feu distribué. Les groupes basés sur l'identité ne peuvent pas être utilisés comme destination dans les règles DFW.

Note IDFW s'appuie sur la sécurité et l'intégrité du système d'exploitation invité. Il existe plusieurs méthodes pour qu'un administrateur local malveillant usurpe son identité pour contourner les règles de pare-feu. Les informations d'identité d'utilisateur sont fournies par l'agent léger NSX Guest Introspection dans les machines virtuelles invitées. Les administrateurs de sécurité doivent s'assurer que l'agent léger est installé et en cours d'exécution sur chaque machine virtuelle invitée. Les utilisateurs connectés ne doivent pas disposer du privilège pour supprimer ou arrêter l'agent.

Pour les configurations d>IDFW prises en charge, reportez-vous à la section [Configurations prises en charge par le pare-feu d'identité](#).

Workflow IDFW :

- 1 Un utilisateur se connecte à une machine virtuelle et démarre une connexion réseau, en ouvrant Skype ou Outlook.
- 2 Un événement de connexion d'utilisateur est détecté par Thin Agent, qui rassemble les informations de connexion et les informations d'identité, et les envoie au moteur de contexte.
- 3 Le moteur de contexte transfère les informations de connexion et d'identité au pare-feu distribué pour l'application de toute règle applicable.

Workflow d'Identity Firewall

IDFW améliore le pare-feu traditionnel en autorisant les règles de pare-feu basées sur l'identité de l'utilisateur. Par exemple, les administrateurs peuvent autoriser le personnel du service client à accéder à une base de données RH avec une stratégie de pare-feu unique, ou le lui interdire.

Les règles de pare-feu basées sur l'identité sont déterminées par appartenance dans une appartenance de groupe Active Directory (AD). Reportez-vous à la section [Configurations prises en charge par le pare-feu d'identité](#).

IDFW traite l'identité de l'utilisateur à la source uniquement dans les règles de pare-feu distribué. Les groupes basés sur l'identité ne peuvent pas être utilisés comme destination dans les règles DFW.

Note Pour l'application des règles de pare-feu d'identité, le service de temps Windows doit être **activé** pour toutes les VM utilisant Active Directory. Cela garantit que la date et l'heure sont synchronisées entre Active Directory et les VM. Les modifications apportées à l'appartenance au groupe AD, y compris l'activation et la suppression d'utilisateurs, ne prennent pas immédiatement effet pour les utilisateurs connectés. Pour que les modifications prennent effet, les utilisateurs doivent fermer puis rouvrir leur session. L'administrateur AD doit forcer la fermeture de session lorsque l'appartenance au groupe est modifiée. Ce comportement est une limite d'Active Directory.

Conditions préalables

Si l'ouverture de session automatique Windows est activée sur les machines virtuelles, accédez à **Stratégie de l'ordinateur local > Configuration ordinateur > Modèles d'administration > Système > Ouverture de session** et activez **Toujours attendre le réseau lors du démarrage de l'ordinateur et de l'ouverture de session**.

Pour les configurations d>IDFW prises en charge, reportez-vous à la section [Configurations prises en charge par le pare-feu d'identité](#).

Procédure

- 1 Activez le pilote d'introspection de fichiers NSX et le pilote d'introspection réseau NSX. L'installation complète de VMware Tools ajoute ces pilotes par défaut.
- 2 Activez IDFW sur un cluster ou un hôte autonome : [Activer le pare-feu d'identité](#).
- 3 Configurez le domaine Active Directory : [Ajout d'Active Directory](#).
- 4 Configurez des opérations de synchronisation Active Directory : [Synchroniser Active Directory](#).
- 5 Créez des groupes de sécurité avec des membres du groupe Active Directory : [Ajouter un groupe](#).
- 6 Attribuez un groupe de sécurité avec des membres du groupe AD à une règle de pare-feu distribué : [Ajouter un pare-feu distribué](#).

Activer le pare-feu d'identité

Le pare-feu d'identité doit être activé afin que les règles de pare-feu IDFW prennent effet.

Procédure

- 1 Sélectionnez **Sécurité > Pare-feu distribué**.
- 2 Dans le coin gauche, cliquez sur **Actions > Paramètres généraux**.
- 3 Faites basculer le bouton **État** pour activer IDFW.
Le pare-feu distribué doit également être activé pour qu'IDFW fonctionne.
- 4 Pour activer IDFW sur des hôtes autonomes ou des clusters, sélectionnez l'onglet **Paramètres du pare-feu d'identité**.
- 5 Faites basculer la barre **Activer** et sélectionnez les hôtes autonomes, ou sélectionnez le cluster sur lequel l'hôte IDFW doit être activé.
- 6 Cliquez sur **Enregistrer**.

Meilleures pratiques du pare-feu d'identité

Les meilleures pratiques suivantes vous aideront à optimiser la réussite des règles de pare-feu d'identité.

- IDFW prend en charge les protocoles suivants ::
 - Prise en charge des cas d'utilisation d'un seul utilisateur (serveur VDI ou non-RDSH) : TCP, UDP, ICMP
 - Prise en charge des cas d'utilisation multi-utilisateur (RDSH) : TCP, UDP
- Un groupe basé sur un seul ID peut être utilisé comme source uniquement dans une règle de pare-feu distribué. Si des groupes basés sur l'adresse IP et l'ID sont nécessaires à la source, créez deux règles de pare-feu distinctes.
- Toute modification apportée à un domaine, y compris un changement de nom de domaine, entraîne une synchronisation complète avec Active Directory. Comme une synchronisation complète peut prendre un certain temps, nous vous recommandons d'effectuer la synchronisation pendant les heures creuses ou hors activité.
- Pour les contrôleurs de domaine local, le port LDAP 389 et le port LDAPS 636 par défaut sont utilisés pour la synchronisation Active Directory et ne doivent pas être modifiés à partir des valeurs par défaut.

Configurations prises en charge par le pare-feu d'identité

Les configurations suivantes sont prises en charge pour le pare-feu d'identité (IDFW) sur les machines virtuelles (VM). L'IDFW pour les périphériques physiques n'est pas pris en charge.

Systèmes d'exploitation clients	Type d'application
Windows 8	Poste de travail - prend en charge le cas d'utilisation des utilisateurs de poste de travail
Windows 10	Poste de travail - prend en charge le cas d'utilisation des utilisateurs de poste de travail
Windows 2012	Serveur - prend en charge le cas d'utilisation des utilisateurs de serveur
Windows 2012R2	Serveur - prend en charge le cas d'utilisation des utilisateurs de serveur
Windows 2016	Serveur - prend en charge le cas d'utilisation des utilisateurs de serveur
Windows 2012R2	RDSH - prend en charge l'hôte de session Bureau à distance
Windows 2016	RDSH - prend en charge l'hôte de session Bureau à distance

Contrôleurs de domaine Active Directory :

- Windows Server 2012
- Windows Server 2012R2
- Windows Server 2016
- Windows Server 2019

Système d'exploitation hôte : ESXi

VMware Tools - Version 11

- Pilote VMCI
- Pilote Introspection de fichiers NSX
- Pilote Introspection réseau NSX

Profil de contexte de couche 7

Les ID d'application de couche 7 sont configurés dans le cadre d'un profil de contexte.

Un profil de contexte peut spécifier un ou plusieurs [Attributs](#) et peut également inclure des sous-attributs, à utiliser dans des règles de pare-feu distribué (DFW) et des règles de pare-feu de passerelle. Lorsqu'un sous-attribut est défini (par exemple, TLS version 1.2), plusieurs attributs d'identité d'application ne sont pas pris en charge. En plus des attributs, DFW prend également en charge un nom de domaine complet (FQDN) ou une URL que vous pouvez spécifier dans un profil de contexte pour la mise sur liste blanche ou sur liste noire de noms de domaine complets. Une liste prédéfinie de domaines est actuellement prise en charge. Le nom de domaine complet peut être configuré avec un attribut dans un profil de contexte ou chaque nom de domaine complet peut être défini dans différents profils de contexte. Une fois qu'un profil de contexte a été défini, il peut être appliqué à une ou plusieurs règles de pare-feu distribué.

Une liste prédéfinie de domaines est actuellement prise en charge. Vous pouvez voir la liste des noms de domaine complets lorsque vous ajoutez un nouveau profil de contexte de type d'attribut *Nom de domaine (FQDN)*. Vous pouvez également voir une liste de noms de domaine complets en exécutant l'appel d'API `/policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME`.

Note

- Les règles de pare-feu de passerelle ne prennent pas en charge l'utilisation d'attributs de nom de domaine complet ou d'autres sous-attributs dans les profils de contexte.
 - Les profils de contexte ne sont pas pris en charge sur la stratégie de pare-feu de passerelle de niveau 0. Les règles de pare-feu de passerelle ne prennent pas en charge l'utilisation d'attributs de nom de domaine complet ou d'autres sous-attributs.
-

Lorsqu'un profil de contexte a été utilisé dans une règle, tout le trafic provenant d'une machine virtuelle est comparé au tableau de règles basées sur 5 tuples. Si la règle correspondant au flux inclut également un profil de contexte de couche 7, ce paquet est redirigé vers un composant de l'espace utilisateur appelé le moteur vDPI. Quelques paquets associés pointent vers ce moteur vDPI pour chaque flux. Une fois l'ID de l'application déterminé, ces informations sont stockées dans la table de contexte du noyau. Lorsque le paquet suivant pour le flux est fourni, les informations contenues dans le tableau de contexte sont de nouveau comparées au tableau de règles et sont mises en correspondance sur 5 tuples et sur l'ID d'application de couche 7. L'action appropriée selon la règle de correspondance totale est effectuée. En cas de règle d'autorisation, tous les paquets associés pour le flux sont traités dans le noyau et comparés au tableau de connexion. Pour une règle d'abandon totalement correspondante, un paquet de rejet est généré. Les journaux générés par le pare-feu incluent l'ID d'application de couche 7 et l'URL applicable, si ce flux pointe vers le moteur DPI.

Traitement des règles pour un paquet entrant :

- 1 Lorsque vous entrez un filtre de pare-feu distribué ou de passerelle, les paquets sont recherchés dans le tableau de flux basé sur 5 tuples.
- 2 Si aucun flux/état n'est trouvé, le flux est comparé au tableau de règles basées sur 5 tuples et une entrée est créée dans le tableau de flux.
- 3 Si le flux correspond à une règle avec un objet de service de couche 7, l'état du tableau de flux est marqué comme « DPI en cours ».
- 4 Le trafic pointe ensuite vers le moteur DPI. Le moteur DPI détermine l'ID d'application.
- 5 Une fois l'ID d'application déterminé, le moteur DPI renvoie l'attribut qui est inséré dans le tableau de contexte pour ce flux. L'indicateur « DPI en cours » est supprimé et le trafic ne pointe plus sur le moteur DPI.

- 6 Le flux (maintenant avec l'ID d'application) est réévalué par rapport à toutes les règles qui correspondent à l'ID d'application, en commençant par la règle d'origine qui a été mise en correspondance en fonction des 5 tuples, puis la première règle L4/L7 totalement correspondante est sélectionnée. La mesure appropriée est prise (autoriser/refuser/rejeter) et l'entrée de tableau de flux est mise à jour en conséquence.

Workflow de règles de pare-feu de couche 7

Les ID d'application de couche 7 sont utilisés dans la création de profils de contexte qui sont utilisés dans des règles de pare-feu distribué ou des règles de pare-feu de passerelle.

L'application de règles basées sur les attributs permet aux utilisateurs d'autoriser les applications à s'exécuter sur n'importe quel port ou de les en empêcher.

NSX-T fournit un [Attributs](#) intégré pour les applications d'infrastructure et d'entreprise communes. Les ID d'application intègrent les versions (SSL/TLS et CIFS/SMB) et la suite de chiffrement (SSL/TLS). Pour le pare-feu distribué, les ID d'application sont utilisés dans les règles via les profils de contexte et peuvent être combinés avec les listes blanches et les listes noires de noms de domaine complets. Les ID d'application sont pris en charge sur les hôtes ESXi et KVM.

Note

- Les règles de pare-feu de passerelle ne prennent pas en charge l'utilisation d'attributs de nom de domaine complet ou d'autres sous-attributs dans les profils de contexte.
 - Les profils de contexte ne sont pas pris en charge sur la stratégie de pare-feu de passerelle de niveau 0. Les règles de pare-feu de passerelle ne prennent pas en charge l'utilisation d'attributs de nom de domaine complet ou d'autres sous-attributs.
-

ID d'application et noms de domaine complets pris en charge:

- Pour le nom de domaine complet, les utilisateurs doivent configurer une règle à priorité élevée avec un ID d'application DNS pour les serveurs DNS spécifiés sur le port 53.
- Les ID d'application ALG (FTP, ORACLE, DCERPC, TFTP) requièrent le service ALG correspondant pour la règle de pare-feu.
- L'ID d'application SYSLOG est détecté uniquement sur les ports standard.

ID d'application et noms de domaine complets pris en charge par KVM :

- Les sous-attributs ne sont pas pris en charge sur KVM.
- Les ID d'application ALG FTP et TFTP sont pris en charge sur KVM.

Notez que si vous utilisez une combinaison de couche 7 et d'ICMP, ou d'autres protocoles, vous devez placer les règles de pare-feu de couche 7 en dernier. Les règles situées au-dessus d'une règle any/any de couche 7 ne sont pas exécutées.

Procédure

- 1 Créez un profil de contexte personnalisé : [Ajouter un profil de contexte](#).

- 2 Utilisez le profil de contexte dans une règle de pare-feu distribué ou une règle de pare-feu de passerelle : [Ajouter un pare-feu distribué](#) ou [Ajouter une règle ou une stratégie de pare-feu de passerelle](#).

Il est possible d'utiliser plusieurs profils de contexte d'ID d'application dans une règle de pare-feu avec des services définis sur **Quelconque**. Pour les profils ALG (FTP, ORACLE, DCERPC, TFTP), un seul profil de contexte est pris en charge par règle.

Attributs

Les attributs de couche 7 (ID d'application) identifient par quelle application un paquet ou un flux particulier est généré, quel que soit le port utilisé.

L'application basée sur les ID d'application permet aux utilisateurs d'autoriser ou de refuser que des applications s'exécutent sur n'importe quel port, ou de forcer l'exécution des applications sur leur port standard. Le vDPI permet de faire correspondre la charge utile des paquets à des modèles définis, généralement appelés signatures. L'identification et l'application basées sur les signatures permettent non seulement aux clients de faire correspondre l'application et le protocole particulier auxquels un flux appartient, mais également la version de ce protocole (par exemple, TLS version 1.0, TLS version 1.2 ou différentes versions du trafic CIFS). Cela permet aux clients d'obtenir une visibilité ou de limiter l'utilisation de protocoles qui présentent des vulnérabilités connues pour toutes les applications déployées et leurs flux E-O dans le centre de données.

Les ID d'application de couche 7 sont utilisés dans les profils de contexte dans des règles de pare-feu de passerelle et de pare-feu distribué et sont pris en charge sur les hôtes ESXi et KVM.

Note NFS version 4 n'est pas un attribut pris en charge.

Note

- Les règles de pare-feu de passerelle ne prennent pas en charge l'utilisation d'attributs de nom de domaine complet ou d'autres sous-attributs dans les profils de contexte.
 - Les profils de contexte ne sont pas pris en charge sur la stratégie de pare-feu de passerelle de niveau 0. Les règles de pare-feu de passerelle ne prennent pas en charge l'utilisation d'attributs de nom de domaine complet ou d'autres sous-attributs.
-

ID d'application et noms de domaine complets pris en charge:

- Pour le nom de domaine complet, les utilisateurs doivent configurer une règle à priorité élevée avec un ID d'application DNS pour les serveurs DNS spécifiés sur le port 53.
- Les ID d'application ALG (FTP, ORACLE, DCERPC, TFTP) requièrent le service ALG correspondant pour la règle de pare-feu.
- L'ID d'application SYSLOG est détecté uniquement sur les ports standard.

ID d'application et noms de domaine complets pris en charge par KVM :

- Les sous-attributs ne sont pas pris en charge sur KVM.

- Les ID d'application ALG FTP et TFTP sont pris en charge sur KVM.

Attribut (ID d'application)	Description	Type
360ANTIV	360 Safeguard est un programme développé par Qihoo 360, une société informatique basée en Chine	Services Web
ACTIVDIR	Microsoft Active Directory	Mise en réseau
AMQP	AMQP (Advanced Messaging Queuing Protocol) est un protocole de couche d'application qui prend en charge la communication de messages d'entreprise entre applications ou organisations.	Mise en réseau
AVAST	Trafic généré par l'exploration sur le site Web officiel Avast.com de téléchargements d'Avast! Antivirus	Services Web
AVG	Téléchargement et mises à jour du logiciel antivirus/sécurité AVG	Transfert de fichiers
AVIRA	Téléchargement et mises à jour du logiciel antivirus/sécurité Avira	Transfert de fichiers
BLAST	Protocole d'accès distant qui compresse, chiffre et code l'ensemble de l'expérience sur ordinateur à un centre de données et la transmet à travers un réseau IP standard pour les postes de travail VMware Horizon.	Accès distant
BDEFENDER	Téléchargement et mises à jour du logiciel antivirus/sécurité BitDefender	Transfert de fichiers
CA_CERT	L'autorité de certification émet des certificats numériques, ce qui certifie la propriété d'une clé publique pour le chiffrement des messages	Mise en réseau
CIFS	CIFS (Common Internet File System) est utilisé pour fournir un accès partagé aux répertoires, fichiers, imprimantes, ports série et diverses communications entre des nœuds sur un réseau	Transfert de fichiers
CLDAP	CLDAP (Connectionless Lightweight Directory Access Protocol) est un protocole d'application conçu pour assurer la maintenance des services d'annuaires distribués sur un réseau IP (Internet Protocol), ainsi que l'accès à ces services, à l'aide d'UDP.	Mise en réseau
CTRXCGP	CTRXCGP (Citrix Common Gateway Protocol) est un protocole d'application conçu pour assurer la maintenance des services d'annuaires distribués sur un réseau IP (Internet Protocol), ainsi que l'accès à ces services, à l'aide d'UDP.	Base de données
CTRKGOTO	Hébergement Citrix GoToMeeting ou sessions similaires basées sur la plate-forme GoToMeeting. Inclut les fonctions de voix, de vidéo et de gestion limitée des foules	Collaboration
CTRICA	ICA (Independent Computing Architecture) est un protocole propriétaire pour un système de serveur d'application, conçu par Citrix Systems	Accès distant
DCERPC	Distributed Computing Environment/Remote Procedure Calls est le système d'appel de procédure distante développé pour DCE (Distributed Computing Environment)	Mise en réseau
DIAMETER	Protocole d'authentification, d'autorisation et de gestion des comptes pour des réseaux d'ordinateurs	Mise en réseau

Attribut (ID d'application)	Description	Type
DHCP	Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole de gestion utilisé pour la distribution d'adresses IP dans un réseau	Mise en réseau
DNS	Interrogation d'un serveur DNS sur TCP ou UDP	Mise en réseau
EPIC	Epic EMR est une application de dossiers médicaux électroniques qui fournit des informations de santé et de soins de patients.	Client serveur
ESET	Téléchargement et mises à jour du logiciel antivirus/sécurité Eset	Transfert de fichiers
FPROT	Téléchargement et mises à jour du logiciel antivirus/sécurité F-Prot	Transfert de fichiers
FTP	FTP (File Transfer Protocol) est utilisé pour transférer des fichiers entre un serveur de fichiers et une machine locale	Transfert de fichiers
GITHUB	GIT basé sur le Web ou service de référentiel de contrôle de version et d'hébergement Internet	Collaboration
HTTP	(HyperText Transfer Protocol) Principal protocole de transport d'Internet	Services Web
HTTP2	Trafic généré par l'exploration de sites Web qui prennent en charge le protocole HTTP 2.0	Services Web
IMAP	IMAP (Internet Message Access Protocol) est un protocole Internet standard pour accéder à une messagerie sur un serveur distant	Messagerie
KASPRSKY	Téléchargement et mises à jour du logiciel antivirus/sécurité Kaspersky	Transfert de fichiers
KERBEROS	Kerberos est un protocole d'authentification réseau conçu pour fournir une authentification forte aux applications client/serveur en utilisant le chiffrement de clé secrète	Mise en réseau
LDAP	LDAP (Lightweight Directory Access Protocol) est un protocole pour lire et modifier des répertoires sur un réseau IP	Base de données
MAXDB	Connexions et requêtes SQL faites à un serveur SQL MaxDB	Base de données
MCAFEE	Téléchargement et mises à jour du logiciel antivirus/sécurité McAfee	Transfert de fichiers
MSSQL	Microsoft SQL Server est une base de données relationnelle.	Base de données
NFS	Permet à un utilisateur sur un ordinateur client d'accéder à des fichiers sur un réseau comme on accède à un stockage local. Note NFS version 4 n'est pas un attribut pris en charge.	Transfert de fichiers
NNTP	Protocole d'application Internet utilisé pour le transport des articles Usenet (« netnews ») entre les serveurs de discussion. Il permet aussi aux utilisateurs finaux de lire et de publier des articles via les applications clientes.	Transfert de fichiers
NTBIOSNS	Service de nom NetBIOS. Pour pouvoir démarrer des sessions ou distribuer des datagrammes, une application doit enregistrer son nom NetBIOS en utilisant le service de nom	Mise en réseau

Attribut (ID d'application)	Description	Type
NTP	NTP (Network Time Protocol) est utilisé pour synchroniser les horloges des systèmes informatiques sur le réseau	Mise en réseau
OCSP	Répondeur OCSP vérifiant que la clé privée d'un utilisateur n'a pas été compromise ou révoquée	Mise en réseau
ORACLE	Système de gestion de base de données relatif aux objets (ORDBMS) produit et commercialisé par Oracle Corporation.	Base de données
PANDA	Téléchargement et mises à jour du logiciel antivirus/sécurité Panda Security	Transfert de fichiers
PCOIP	Protocole d'accès à distance qui compresse, chiffre et code l'ensemble de l'expérience sur ordinateur à un centre de données et la transmet à travers un réseau IP standard.	Accès distant
POP2	POP (Post Office Protocol) est un protocole utilisé par les clients de messagerie locaux afin de récupérer des messages électroniques à partir d'un serveur distant.	Messagerie
POP3	Implémentation Microsoft de NBNS (NetBIOS Name Service), un serveur de nom et un service pour les noms d'ordinateurs NetBIOS.	Messagerie
RADIUS	Fournit une gestion centralisée de l'authentification, l'autorisation et la gestion des comptes à des ordinateurs pour se connecter et utiliser un service réseau	Mise en réseau
RDP	RDP (Remote Desktop Protocol) fournit aux utilisateurs une interface graphique vers un autre ordinateur	Accès distant
RTCP	RTCP (Real-Time Transport Control Protocol) est un protocole frère du protocole RTP (Real-Time Transport Protocol). RTCP fournit des informations de contrôle hors bande pour un flux RTP.	Diffusion multimédia
RTP	RTP (Real-Time Transport Protocol) est utilisé principalement pour fournir l'audio et la vidéo en temps réel	Diffusion multimédia
RTSP	RTSP (Real Time Streaming Protocol) est utilisé pour établir et contrôler des sessions multimédia entre des points de terminaison	Diffusion multimédia
SIP	SIP (Session Initiation Protocol) est un protocole de contrôle commun pour configurer et contrôler les appels vocaux et vidéo	Diffusion multimédia
SMTP	Le protocole SMTP (Simple Mail Transfer Protocol) est une norme Internet pour la transmission de messages électroniques (e-mail) sur des réseaux IP (Internet Protocol).	Messagerie
SNMP	SNMP (Simple Network Management Protocol) est un protocole Internet standard pour gérer des périphériques sur des réseaux IP.	Surveillance du réseau
SSH	SSH (Secure Shell) est un protocole réseau qui permet d'échanger des données à l'aide d'un canal sécurisé entre deux périphériques en réseau.	Accès distant
SSL	SSL (Secure Sockets Layer) est un protocole cryptographique qui fournit une sécurité via Internet.	Services Web

Attribut (ID d'application)	Description	Type
SYMUPDAT	Le trafic Symantec LiveUpdate inclut des définitions de logiciels espions, des règles de pare-feu, des fichiers de signatures antivirus et des mises à jour logicielles.	Transfert de fichiers
SYSLOG	SYSLOG est un protocole qui permet aux périphériques réseau d'envoyer des messages d'événement à un serveur de journalisation.	Surveillance du réseau
TELNET	Protocole réseau utilisé sur Internet ou des réseaux locaux afin de fournir une fonctionnalité de communication orientée texte interactive bidirectionnelle à l'aide d'une connexion de terminal virtuelle.	Accès distant
TFTP	TFTP (Trivial File Transfer Protocol) utilisé pour répertorier, télécharger et charger des fichiers sur un serveur TFTP, comme SolarWinds TFTP Server, à l'aide d'un client tel que le client WinAgents TFTP.	Transfert de fichiers
VNC	Trafic de Virtual Network Computing.	Accès distant
WINS	Implémentation Microsoft de NBNS (NetBIOS Name Service), un serveur de nom et un service pour les noms d'ordinateurs NetBIOS.	Mise en réseau

Pare-feu distribué

Un pare-feu distribué est fourni avec les catégories prédéfinies pour les règles de pare-feu. Les règles sont évaluées de haut en bas et de gauche à droite.

Tableau 10-2. Catégories de règle de pare-feu distribué

Catégorie	Description
Ethernet	Utilisé pour les règles basées sur la couche 2
Urgence	Utilisé pour les règles de mise en quarantaine et d'autorisation
Infrastructure	Définissez l'accès aux services partagés. Règles globales - Serveurs AD, DNS, NTP, DHCP, de sauvegarde, de gestion
Environnement	Règles entre les zones - production contre développement, règles inter unité commerciale
Application	Règles entre applications, niveaux d'application ou règles entre services micro

Brouillons de pare-feu

Un brouillon est une configuration de pare-feu distribué complète avec des sections et des règles de stratégie. Les brouillons peuvent être enregistrés automatiquement ou manuellement, puis publiés ou enregistrés immédiatement pour une publication à une date ultérieure.

Pour enregistrer une configuration manuelle de pare-feu de brouillon, accédez à la partie supérieure droite de l'écran de pare-feu distribué et cliquez sur **Actions > Enregistrer**. Après l'enregistrement, la configuration peut être affichée en sélectionnant **Actions > Afficher**. Les brouillons automatiques sont activés par défaut. Les brouillons automatiques peuvent être désactivés en accédant à **Actions > Paramètres généraux**. Lorsque les brouillons automatiques sont activés, toute modification apportée à une configuration de pare-feu entraîne la création d'un brouillon automatique par le système. Un maximum de 100 brouillons automatiques et 10 brouillons manuels peuvent être enregistrés. Les brouillons automatiques peuvent être modifiés et enregistrés sous forme de brouillon manuel pour une publication immédiate ou ultérieure. Pour empêcher plusieurs utilisateurs d'ouvrir et de modifier le brouillon, les brouillons manuels peuvent être verrouillés. Lorsqu'un brouillon est publié, la configuration actuelle est remplacée par la configuration dans le brouillon.

Enregistrer ou afficher un brouillon de pare-feu

Un brouillon est une configuration de pare-feu distribué qui a été publiée ou enregistrée à des fins de publication à une date ultérieure. Les brouillons sont créés automatiquement et manuellement.

Les brouillons manuels peuvent être modifiés et enregistrés. Les brouillons automatiques peuvent être clonés et enregistrés en tant que brouillons manuels, puis modifiés. Le nombre maximal de brouillons pouvant être enregistrés est de 100 brouillons automatiques et 10 brouillons manuels.

Procédure

- 1 Cliquez sur **Sécurité > Pare-feu distribué**.
- 2 Pour enregistrer manuellement une configuration de pare-feu, accédez à **Actions > Enregistrer**.

Un brouillon manuel peut être enregistré ou modifié, puis enregistré. Après l'enregistrement, vous pouvez restaurer la configuration d'origine.
- 3 **Nommez** la configuration.
- 4 Pour éviter que plusieurs utilisateurs n'ouvrent et ne modifient un brouillon manuel, **verrouillez** la configuration et ajoutez un commentaire.
- 5 Cliquez sur **Enregistrer**.
- 6 Pour afficher la configuration enregistrée, cliquez sur **Actions > Afficher**.

Une chronologie s'ouvre et affiche toutes les configurations enregistrées. Pour voir des détails tels que le nom du brouillon, la date, l'heure et l'auteur de l'enregistrement, pointez sur l'icône en forme de point ou d'étoile de n'importe quel brouillon. Les configurations enregistrées peuvent être filtrées par heure, ce qui affiche tous les brouillons créés au cours du jour précédent, de la semaine précédente, des 30 derniers jours ou du dernier trimestre. Elles peuvent être filtrées par brouillon automatique et enregistrées par l'auteur. Elles peuvent également être filtrées par nom à l'aide de l'outil de recherche en haut à droite.

- 7 Passez le curseur sur un brouillon pour afficher le nom, la date et l'heure de la configuration enregistrée. Cliquez sur le nom pour afficher les détails du brouillon.

La vue détaillée du brouillon affiche les modifications requises à apporter à la configuration de pare-feu actuelle, afin d'être synchronisée avec ce brouillon. Si ce brouillon est publié, toutes les modifications visibles dans cette vue seront appliquées à la configuration actuelle.

Un clic sur la flèche vers le bas développe chaque section et affiche les modifications ajoutées, modifiées et supprimées dans chaque section. La comparaison affiche les règles ajoutées avec une barre verte sur le côté gauche de la zone, les éléments modifiés (tels qu'un changement de nom) ont une barre jaune et les éléments supprimés ont une barre rouge.

- 8 Pour modifier le nom ou la description d'un brouillon sélectionné, cliquez sur l'icône du menu (trois points) dans la fenêtre **Afficher les détails du brouillon** et sélectionnez **Modifier**.

Les brouillons manuels peuvent être verrouillés. S'il est verrouillé, un commentaire pour le brouillon doit être fourni.

Certains rôles, comme Administrateur d'entreprise, disposent d'informations d'identification d'accès complet et ne peuvent pas être verrouillés. Reportez-vous à la section [Contrôle d'accès basé sur les rôles](#).

- 9 Les brouillons automatiques et les brouillons manuels peuvent également être clonés et enregistrés en cliquant sur **Cloner**.

Dans la fenêtre Configurations enregistrées, vous pouvez accepter le nom par défaut ou le modifier. Vous pouvez également verrouiller la configuration. S'il est verrouillé, un commentaire pour le brouillon doit être fourni.

- 10 Pour enregistrer la version clonée de la configuration du brouillon, cliquez sur **Enregistrer**. Le brouillon se trouve maintenant dans la section Configurations enregistrées.

Étape suivante

Après avoir affiché un brouillon, vous pouvez le charger et le publier. Il devient ensuite la configuration du pare-feu active.

Publier ou restaurer un brouillon de pare-feu

Les brouillons automatiques et les brouillons manuels enregistrés peuvent être chargés et publiés pour devenir la configuration active.

Lors de la publication, un nouveau brouillon automatique est créé. Ce brouillon automatique peut être publié pour revenir à la configuration précédente.

Procédure

- 1 Pour afficher la configuration enregistrée, cliquez sur **Actions > Afficher**.

Une chronologie s'ouvre et affiche toutes les configurations enregistrées. Pour voir des détails tels que le nom du brouillon, la date, l'heure et l'auteur de l'enregistrement, pointez sur l'icône en forme de point de n'importe quel brouillon. Les configurations enregistrées sont filtrées par heure, ce qui affiche tous les brouillons créés en 1 jour, 1 semaine, 30 jours ou les 3 derniers mois.

- 2 Cliquez sur le nom d'un brouillon et la fenêtre Afficher les détails du brouillon s'affiche.
- 3 Cliquez sur **Charger**. La nouvelle configuration du pare-feu s'affiche dans la fenêtre principale.

Note Il n'est pas possible de charger un brouillon si des filtres de pare-feu sont utilisés ou si la configuration actuelle contient des modifications non enregistrées.

- 4 Pour valider la configuration de brouillon et la rendre active, cliquez sur **Publier**. Pour revenir à la configuration publiée précédente, cliquez sur **Restaurer**.

Après la publication, les modifications apportées au brouillon seront présentes dans la configuration active.

- 5 Pour modifier le contenu du brouillon sélectionné avant la publication, après avoir cliqué sur **Charger**, modifiez la configuration.

- 6 Pour enregistrer la version modifiée de la configuration de brouillon, cliquez sur **Actions > Enregistrer**.

Les brouillons manuels peuvent être enregistrés en tant que nouvelle configuration ou en tant que mise à jour de la configuration existante. Les brouillons automatiques peuvent uniquement être enregistrés en tant que nouvelle configuration.

- 7 Entrez un **Nom** et une **Description** facultative. Vous pouvez également **Verrouiller** le brouillon. S'il est verrouillé, un commentaire pour le brouillon doit être fourni.

- 8 Cliquez sur **Enregistrer**.

- 9 Pour valider la configuration de brouillon et la rendre active, cliquez sur **Publier** ou, pour revenir à la configuration publiée précédente, cliquez sur **Restaurer**.

Ajouter un pare-feu distribué

Un pare-feu distribué (DFW) permet de surveiller l'ensemble du trafic horizontal sur vos machines virtuelles.

Conditions préalables

Les cartes réseau virtuelles des machines virtuelles invitées devant être protégées par DFW doivent être connectées à un commutateur logique N-VDS associé à une zone de transport.

Si vous créez des règles de pare-feu d'identité, vous devez tout d'abord créer un groupe avec les membres Active Directory. IDFW prend uniquement en charge les règles de pare-feu basées sur TCP.

Note Pour l'application des règles de pare-feu d'identité, le service de temps Windows doit être **activé** pour toutes les VM utilisant Active Directory. Cela garantit que la date et l'heure sont synchronisées entre Active Directory et les VM. Les modifications apportées à l'appartenance au groupe AD, y compris l'activation et la suppression d'utilisateurs, ne prennent pas immédiatement effet pour les utilisateurs connectés. Pour que les modifications prennent effet, les utilisateurs doivent fermer puis rouvrir leur session. L'administrateur AD doit forcer la fermeture de session lorsque l'appartenance au groupe est modifiée. Ce comportement est une limite d'Active Directory.

Notez que si vous utilisez une combinaison de couche 7 et d'ICMP, ou d'autres protocoles, vous devez placer les règles de pare-feu de couche 7 en dernier. Les règles situées au-dessus d'une règle any/any de couche 7 ne sont pas exécutées.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Sécurité > Pare-feu distribué** dans le panneau de navigation.
- 3 Activez le champ Pare-feu distribué en sélectionnant **Actions > Paramètres généraux** et en basculant sur le champ État de pare-feu distribué. Cliquez sur **Enregistrer**.
- 4 Assurez-vous d'être dans la catégorie prédéfinie souhaitée et cliquez sur **Ajouter une stratégie**. Pour en savoir plus sur les catégories, reportez-vous à la section [Pare-feu distribué](#).
- 5 Entrez un **Nom** pour la nouvelle section de stratégie.

- 6 (Facultatif) Pour configurer les paramètres de stratégie suivants, cliquez sur l'icône d'engrenage :

Option	Description
TCP strict	<p>Une connexion TCP commence par l'établissement d'une liaison en trois temps (SYN, SYN-ACK, ACK) et se termine généralement par un échange bidirectionnel (FIN, ACK). Dans certains cas, le pare-feu distribué (DFW) peut ne pas voir l'établissement de liaison à trois voies pour un flux particulier (en raison du trafic asymétrique ou du pare-feu distribué activé lorsqu'il existe un flux). Par défaut, le pare-feu distribué n'impose pas le besoin de voir l'établissement d'une liaison en trois temps et sélectionne les sessions déjà établies. TCP strict peut être activé sur une base par section pour désactiver la prise en charge en milieu de session et pour appliquer la condition requise pour un établissement de liaison à trois voies.</p> <p>Lors de l'activation du mode TCP strict pour une stratégie DFW spécifique et de l'utilisation d'une règle ANY-ANY Block par défaut, les paquets qui ne remplissent pas les conditions requises de connexion d'établissement d'une liaison en trois temps et qui correspondent à une règle TCP dans cette section sont abandonnés. Strict s'applique uniquement aux règles TCP avec état et est activé au niveau de la stratégie du pare-feu distribué. TCP strict n'est pas appliqué pour les paquets qui correspondent à une valeur par défaut ANY-ANY Allow qui n'a aucun service TCP spécifié.</p>
Avec état	Un pare-feu avec état surveille l'état des connexions actives et utilise ces informations pour déterminer les paquets à autoriser via le pare-feu.
Verrouillé	<p>La stratégie peut être verrouillée pour empêcher plusieurs utilisateurs de modifier les mêmes sections. Vous devez inclure un commentaire lors du verrouillage d'une section.</p> <p>Certains rôles, tels Administrateur d'entreprise, disposent d'informations d'identification d'accès complet et ne peuvent pas être verrouillés. Reportez-vous à la section Contrôle d'accès basé sur les rôles.</p>

- 7 Cliquez sur **Publier**. Il est possible d'ajouter plusieurs stratégies à la fois et de les publier ensemble.

La nouvelle stratégie s'affiche à l'écran.

- 8 Sélectionnez une section de stratégie et cliquez sur **Ajouter une règle**.
- 9 Entrez un nom pour la règle.

- 10 Dans la colonne **Sources**, cliquez sur l'icône de modification et sélectionnez la source de la règle. Les groupes avec des membres Active Directory peuvent être utilisés pour le champ source d'une règle IDFW. Pour plus d'informations, reportez-vous à [Ajouter un groupe](#).

Les adresses IPv4, IPv6 et de multidiffusion sont prises en charge.

Remarque : le pare-feu IPv6 doit avoir la détection d'adresses IP pour IPv6 activée sur un segment connecté. Pour plus d'informations, reportez-vous à la section [Comprendre le profil de segment de découverte d'adresses IP](#).

- 11 Dans la colonne **Destinations**, cliquez sur l'icône de modification et sélectionnez la destination de la règle. La destination correspond à **Quelconque** si elle n'est pas définie. Pour plus d'informations, reportez-vous à [Ajouter un groupe](#). Les adresses IPv4, IPv6 et de multidiffusion sont prises en charge.
- 12 Dans la colonne **Services**, cliquez sur l'icône de modification et sélectionnez les services. Le service correspond à **Quelconque** s'il n'est pas défini.
- 13 La colonne **Profils** n'est pas disponible lorsque vous ajoutez une règle à la catégorie Ethernet. Pour toutes les autres catégories de règle de la colonne **Profils**, cliquez sur l'icône de modification et sélectionnez un profil de contexte, ou cliquez sur **Ajouter un nouveau profil de contexte**. Reportez-vous à la section [Ajouter un profil de contexte](#).

Les profils de contexte utilisent les attributs de l'ID d'application de couche 7 pour une utilisation dans des règles de pare-feu distribué et des règles de pare-feu de passerelle. Il est possible d'utiliser plusieurs profils de contexte d'ID d'application dans une règle de pare-feu avec des services définis sur **Quelconque**. Pour les profils ALG (FTP et TFTP), un seul profil de contexte est pris en charge par règle.

- 14 Cliquez sur **Appliquer** pour appliquer le profil de contexte à la règle.
- 15 Par défaut, la colonne **Appliqué à** est définie sur DFW et la règle est appliquée à toutes les charges de travail. Vous pouvez également appliquer la règle ou la stratégie à des groupes sélectionnés. La colonne **Appliqué à** définit la portée de la mise en application pour chaque règle. Elle est utilisée principalement pour l'optimisation ou des ressources sur les hôtes ESXi et KVM. Elle vous aide à définir une stratégie ciblée pour des zones et des locataires spécifiques, sans interférer avec d'autres stratégies définies pour les autres locataires et zones.

Les groupes comprenant uniquement des adresses IP, des adresses MAC ou des groupes Active Directory ne peuvent pas être utilisés dans la zone de texte **Appliqué à**.

- 16 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.

- 17 Cliquez sur le bouton bascule **État** pour activer ou désactiver la règle.

- 18 (Facultatif) Cliquez sur l'icône d'engrenage pour configurer les options de règle suivantes :

Option	Description
Journalisation	La journalisation est désactivée par défaut. Les journaux sont stockés dans le fichier <code>/var/log/dfwpktlogs.log</code> sur des hôtes ESXi et KVM.
Direction	Fait référence à la direction du trafic selon le point de vue de l'objet de destination. IN signifie que seul le trafic vers l'objet est vérifié, OUT signifie que seul le trafic provenant de l'objet est vérifié et In/Out signifie que le trafic dans les deux sens est vérifié.
Protocole IP	Appliquez la règle sur le protocole IPv4, IPv6 ou IPv4-IPv6 à la fois.
Étiquette de journal	L'étiquette de journal est transportée dans le journal du pare-feu lorsque la journalisation est activée.

- 19 Cliquez sur **Publier**. Il est possible d'ajouter plusieurs règles à la fois et de les publier ensemble.
- 20 Sur chaque règle, cliquez sur l'icône **Infos** pour afficher le numéro d'ID de la règle et l'endroit où elle est appliquée.

Cette icône est grisée tant que vous n'avez pas publié la règle. Vous pouvez également spécifier un ID de règle lorsque vous cliquez sur l'icône de filtre pour afficher uniquement les stratégies et les règles qui répondent aux critères de filtre.

- 21 L'API de l'état de réalisation a été optimisée au niveau de la stratégie de sécurité pour fournir des informations supplémentaires sur l'état de réalisation. Pour en bénéficier, spécifiez le paramètre de requête *include_enforced_status=true* avec *intent_path*. Effectuez l'appel d'API suivant.

```
GET https://<nsx>/policy/api/v1/infra/realized-state/status?intent_path=/
infra/domains/default/security-policies/<security-policy-
id>&include_enforced_status=true
```

Journaux de paquet de pare-feu distribué

Si la journalisation est activée pour les règles de pare-feu, vous pouvez consulter les journaux de paquet de pare-feu pour résoudre les problèmes.

Le fichier journal est `/var/log/dfwpktlogs.log` pour les hôtes ESXi et KVM.

Voici un exemple de journal standard pour des règles de pare-feu distribué :

```
2018-07-03T19:44:09.749Z b6507827 INET match PASS mainrs/1024 IN 52 TCP 192.168.4.3/49627-
>192.168.4.4/49153 SEW

2018-07-03T19:46:02.338Z 7396c504 INET match DROP mainrs/1024 OUT 52 TCP 192.168.4.3/49676-
>192.168.4.4/135 SEW

2018-07-06T18:15:49.647Z 028cd586 INET match DROP mainrs/1027 IN 36 PROTO 2 0.0.0.0->224.0.0.1

2018-07-06T18:19:54.764Z 028cd586 INET6 match DROP mainrs/1027 OUT 143 UDP
fe80:0:0:0:68c2:8472:2364:9be/546->ff02:0:0:0:0:1:2/547
```

Les éléments d'un format de fichier journal DFW sont les suivants, séparés par un espace :

- horodatage :
- huit derniers chiffres de l'ID VIF d'interface
- type INET (v4 ou v6)
- motif (correspondance)
- action (PASSER, ANNULER, REJETER)
- ensemble de règles/ID de règle
- direction du paquet (ENTRANT/SORTANT)
- taille du paquet
- protocole (TCP, UDP ou PROTO #)
- direction SVM pour la prochaine correspondance de règle
- adresse IP source/port de destination>adresse IP/port de destination
- indicateurs TCP (SEW)

Pour les paquets TCP transmis, il existe un journal de résiliation lorsque la session est terminée :

```
2018-07-03T19:44:30.585Z 7396c504 INET TERM mainrs/1024 OUT TCP RST 192.168.4.3/49627-
>192.168.4.4/49153 20/16 1718/76308
```

Les éléments d'un journal de terminaison TCP sont les suivants, séparés par un espace :

- horodatage :
- 8 derniers chiffres de l'ID VIF d'interface
- type INET (v4 ou v6)
- action (DURÉE)
- nom de l'ensemble de règles/ID de règle
- direction du paquet (ENTRANT/SORTANT)
- protocole (TCP, UDP ou PROTO #)
- Indicateur RST TCP
- direction SVM pour la prochaine correspondance de règle
- adresse IP source/port de destination>adresse IP/port de destination
- nombre de paquets ENTRANTS/SORTANTS (tous cumulés)
- taille du paquet ENTRANT/taille du paquet SORTANT

Voici un exemple de fichier journal de nom de domaine complet pour les règles de pare-feu distribué :

```
2019-01-15T00:34:45.903Z 7c607b29 INET match PASS 1031 OUT 48 TCP 10.172.178.226/32808-
>23.72.199.234/80 S www.sway.com(034fe78d-5857-0680-81e4-d8da6b28d1b4)
```

Les éléments d'un journal de nom de domaine complet sont les suivants, séparés par un espace :

- horodatage :
- huit derniers chiffres de l'ID VIF d'interface
- type INET (v4 ou v6)
- motif (correspondance)
- action (PASSER, ANNULER, REJETER)
- nom de l'ensemble de règles/ID de règle
- direction du paquet (ENTRANT/SORTANT)
- taille du paquet
- protocole (TCP, UDP ou PROTO #)
- adresse IP source/port de destination>adresse IP/port de destination
- nom de domaine/UUID où UUID est la représentation interne binaire du nom de domaine

Voici un exemple de fichier journal de couche 7 pour les règles de pare-feu distribué :

```
2019-01-15T00:35:07.221Z 82f365ae INET match REJECT 1034 OUT 48 TCP 10.172.179.6/49818-
>23.214.173.202/80 S APP_HTTP

2019-01-15T00:34:46.486Z 7c607b29 INET match PASS 1030 OUT 48 UDP 10.172.178.226/42035-
>10.172.40.1/53 APP_DNS
```

Les éléments d'un journal de couche 7 sont les suivants, séparés par un espace :

- horodatage :
- huit derniers chiffres de l'ID VIF d'interface
- type INET (v4 ou v6)
- motif (correspondance)
- action (PASSER, ANNULER, REJETER)
- nom de l'ensemble de règles/ID de règle
- direction du paquet (ENTRANT/SORTANT)
- taille du paquet
- protocole (TCP, UDP ou PROTO #)
- adresse IP source/port de destination>adresse IP/port de destination
- APP_XXX est l'application détectée

Sélectionner une stratégie de connectivité par défaut

Vous pouvez sélectionner une stratégie de connectivité par défaut pour appliquer votre modèle de sécurité.

La stratégie de connectivité par défaut crée une stratégie « autoriser tout » (liste noire) ou « refuser tout » (liste blanche) au-dessus de toutes les autres règles de pare-feu créées, plutôt que d'avoir à modifier des règles individuelles. Pour définir une stratégie de connectivité par défaut, accédez à **Pare-feu distribué**. En haut de la page, cliquez sur l'état de la connectivité pour sélectionner une autre option.

La stratégie de pare-feu et les règles doivent déjà être créées pour modifier la stratégie de connectivité sélectionnée par défaut et pour qu'elle s'applique immédiatement. Si aucune stratégie ou aucune règle n'est créée, la stratégie de connectivité par défaut reste jusqu'à ce qu'une stratégie et des règles soient créées.

Les options suivantes sont disponibles :

- **Liste noire (avec ou sans journalisation)** : il s'agit de l'option par défaut qui crée une règle « autoriser tout » sur DFW.

- **Liste blanche (avec ou sans journalisation)** : crée une règle de pare-feu de trafic « refuser tout ». Seule la communication à partir de sites ou d'applications qui ont été définis dans des règles de pare-feu est autorisée et l'accès est refusé à toutes les autres communications, y compris le trafic DHCP.
- **Aucune** : sélectionnez cette option pour désactiver la mise sur liste noire ou liste blanche des règles de pare-feu. Cela est utile si vous disposez d'un ensemble de règles déjà configurées à l'aide de versions précédentes de NSX-T Data Center.

Gérer une liste d'exclusion de pare-feu

Les listes d'exclusion de pare-feu sont constituées de groupes qui peuvent être exclus d'une règle de pare-feu basée sur l'appartenance à un groupe.

Les groupes peuvent être exclus des règles de pare-feu et la liste peut contenir un maximum de 100 groupes. Les ensembles d'adresses IP, les ensembles d'adresses MAC et les groupes AD ne peuvent pas être inclus en tant que membres dans un groupe utilisé dans une liste d'exclusion de pare-feu.

Note NSX-T Data Center ajoute automatiquement les machines virtuelles de nœuds NSX Manager et NSX Edge à la liste d'exclusion de pare-feu.

Procédure

- 1 Accédez à **Sécurité > Pare-feu distribué > Actions > Liste d'exclusion**.
Une fenêtre s'affiche répertoriant les groupes disponibles.
- 2 Pour ajouter un groupe à la liste d'exclusion, cochez la case en regard d'un groupe quelconque. Cliquez ensuite sur **Appliquer**.
- 3 Pour créer un groupe, cliquez sur **Ajouter un groupe**. Reportez-vous à la section [Ajouter un groupe](#).
- 4 Pour modifier un groupe, cliquez sur le menu à trois points en regard d'un groupe et sélectionnez **Modifier**.
- 5 Pour supprimer un groupe, cliquez sur le menu à trois points et sélectionnez **Supprimer**.
- 6 Pour afficher les détails du groupe, cliquez sur **Tout développer**.

Filtrage de domaines spécifiques (noms de domaine complets/URL)

Définissez une règle de pare-feu distribué pour filtrer des domaines spécifiques identifiés par des noms de domaine complets ou des URL (par exemple, **.office365.com*).

Une liste prédéfinie de domaines est actuellement prise en charge. Vous pouvez voir la liste des noms de domaine complets lorsque vous ajoutez un nouveau profil de contexte de type d'attribut *Nom de domaine (FQDN)*. Vous pouvez également voir une liste de noms de domaine complets en exécutant l'appel d'API `/policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME`.

Vous devez tout d'abord définir une règle DNS et ensuite la règle de mise sur liste autorisée ou sur liste bloquée du nom de domaine complet en dessous de celle-ci. NSX-T Data Center utilise la durée de vie (TTL) dans la réponse DNS (provenant du serveur DNS vers la machine virtuelle) pour conserver l'entrée de cache de mappage DNS vers IP pour la machine virtuelle (VM). Pour remplacer la durée de vie DNS à l'aide d'un profil de sécurité DNS, reportez-vous à la section [Configurer la sécurité DNS](#). Pour que le filtrage de nom de domaine complet soit efficace, les machines virtuelles doivent utiliser un serveur DNS pour la résolution de domaine (aucune entrée DNS statique) et doivent également respecter le TTL reçu dans la réponse DNS. NSX-T Data Center utilise l'écoute DNS pour obtenir un mappage entre l'adresse IP et le nom de domaine complet. SpoofGuard doit être activé sur le commutateur de tous les ports logiques pour assurer la protection contre le risque d'attaques d'usurpation DNS. Une attaque d'usurpation DNS se fait lorsqu'une machine virtuelle malveillante peut injecter des réponses DNS usurpées pour rediriger le trafic vers des points de terminaison malveillants ou contourner le pare-feu. Pour plus d'informations sur SpoofGuard, reportez-vous à la section [Comprendre le profil de segment SpoofGuard](#).

Cette fonctionnalité fonctionne au niveau de la couche 7 et ne couvre pas ICMP. Si un utilisateur crée une règle Liste bloquée pour tous les services sur `example.com`, la fonctionnalité fonctionne comme prévu si `ping example.com` répond, mais que `curl example.com` ne répond pas.

Il est préférable de sélectionner un nom de domaine complet générique, car il inclut des sous-domaines. Par exemple, la sélection de `*example.com` inclut des sous-domaines tels que `americas.example.com` et `emea.example.com`. `example.com` n'inclut aucun sous-domaine.

Les règles basées sur le nom de domaine complet sont conservées lors du déplacement par vMotion des hôtes ESXi.

Note Les hôtes ESXi et KVM sont pris en charge. Les hôtes KVM ne prennent en charge que la liste autorisée du nom de domaine complet. Le filtrage de noms de domaines complets est disponible uniquement avec le trafic TCP et UDP.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Accédez à **Sécurité > Pare-feu distribué**.
- 3 Ajoutez une section de stratégie de pare-feu en suivant les étapes de la section [Ajouter un pare-feu distribué](#). Une section de stratégie de pare-feu existante peut également être utilisée.
- 4 Sélectionnez une nouvelle section de stratégie de pare-feu ou une section existante et cliquez sur **Ajouter une règle** pour créer tout d'abord la règle de pare-feu DNS.

- 5 Fournissez un nom pour la règle de pare-feu (tel que **Règle DNS**) et indiquez les informations suivantes :

Option	Description
Services	Cliquez sur l'icône de modification et sélectionnez le service DNS ou DNS-UDP pour qu'il s'applique à votre environnement.
Profil	Cliquez sur l'icône de modification et sélectionnez le profil de contexte DNS. Il s'agit d'un profil précréé qui est disponible dans votre déploiement par défaut.
Appliqué à	Sélectionnez un groupe comme requis.
Action	Sélectionnez Autoriser .

- 6 Cliquez à nouveau sur **Ajouter une règle** pour configurer la règle de mise sur liste autorisée ou sur liste bloquée du nom de domaine complet.
- 7 Nommez la règle de façon appropriée (par exemple, **Liste autorisée de noms de domaine complets/d'URL**). Faites glisser la règle sous la règle DNS sous cette section de stratégie.
- 8 Fournissez les détails suivants :

Option	Description
Services	Cliquez sur l'icône de modification et sélectionnez le service que vous souhaitez associer à cette règle (par exemple, HTTP).
Profil	Cliquez sur l'icône de modification et cliquez sur Ajouter un nouveau profil de contexte . Cliquez dans la colonne intitulée Attribut , puis sélectionnez Nom de domaine (FQDN) . Sélectionnez la liste Nom d'attribut/valeurs dans la liste prédéfinie. Cliquez sur Ajouter . Reportez-vous à Ajouter un profil de contexte pour plus de détails.
Appliqué à	Sélectionnez DFW ou un groupe comme requis.
Action	Sélectionnez Autoriser , Abandonner ou Rejeter .

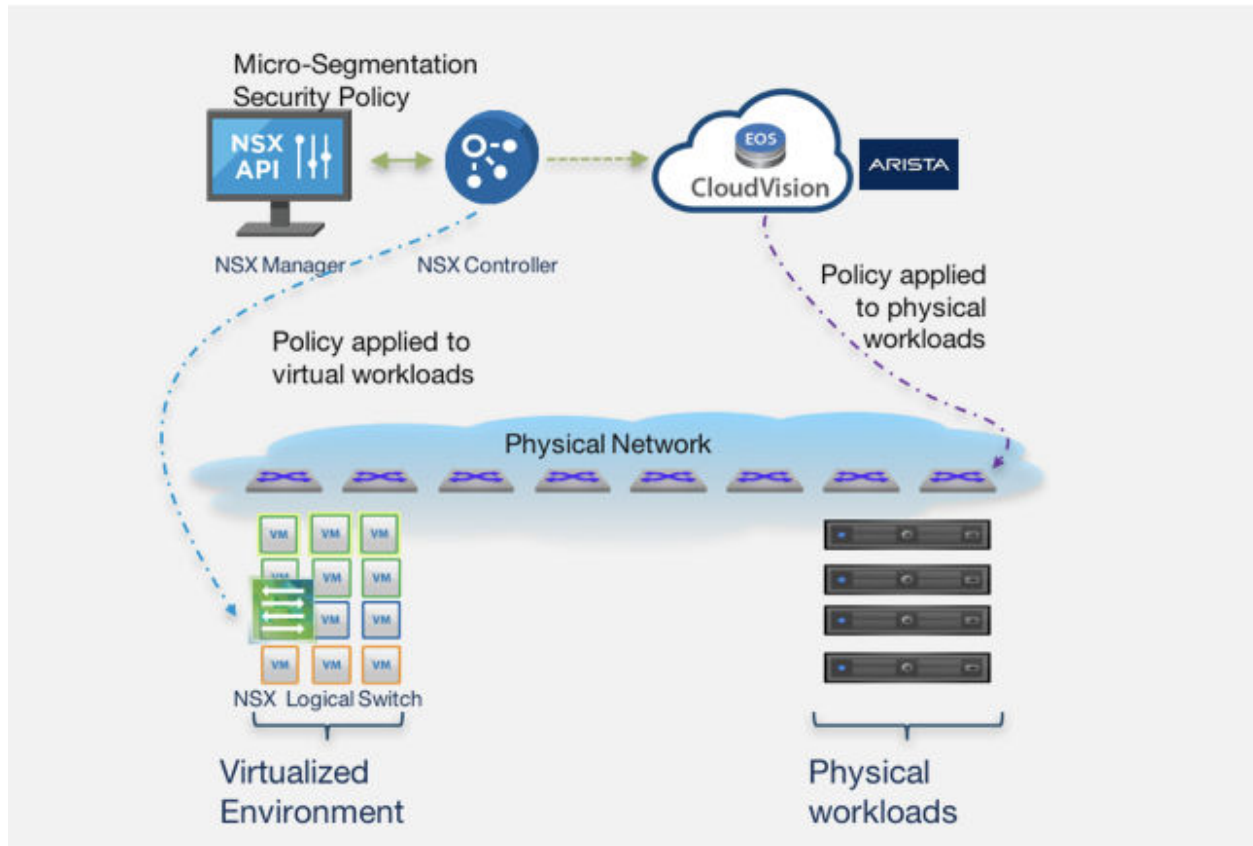
- 9 Cliquez sur **Publier**.

Extension des stratégies de sécurité aux charges de travail physiques

NSX-T Data Center peut agir comme point d'administration unique pour les charges de travail virtuelles et physiques.

À partir de NSX-T Data Center 2.5.1, l'intégration à Arista CloudVision eXchange (CVX) est prise en charge. Cette intégration facilite les services de mise en réseau et de sécurité cohérents sur les charges de travail virtuelles et physiques, indépendamment de vos infrastructures d'application ou de votre infrastructure de réseau physique. NSX-T Data Center ne programme pas directement le commutateur de réseau physique ou le routeur, mais s'intègre au niveau du contrôleur SDN physique. Cela permet de préserver l'autonomie des administrateurs de sécurité et des administrateurs de réseaux physiques.

À partir de NSX-T Data Center 2.5.1, l'intégration à Arista EOS 4.22.1FX-PCS et versions ultérieures est prise en charge.



Limitations

- Les commutateurs Arista exigent que le trafic ARP existe avant l'application des règles de pare-feu à un hôte final connecté à un commutateur Arista. Les paquets peuvent ainsi passer par le commutateur avant de configurer les règles de pare-feu pour bloquer le trafic.
- Le trafic autorisé ne reprend pas lorsqu'un commutateur se bloque ou qu'il est rechargé. Les tables ARP doivent être remplies à nouveau, une fois le commutateur activé, pour appliquer les règles de pare-feu sur le commutateur.
- Vous ne pouvez pas appliquer des règles de pare-feu au commutateur physique Arista, pour les clients passifs FTP qui se connectent au serveur FTP connecté au commutateur physique Arista.
- Dans la configuration HA de CVX qui utilise une adresse IP virtuelle pour le cluster CVX, le mode Promiscuité de dvpg de la machine virtuelle CVX, les fausses transmissions doivent être définies sur Accepter. Si elles sont définies sur la valeur par défaut (Rejeter), l'adresse IP virtuelle HA de CVX n'est pas accessible à partir de NSX Manager.

Configurer Arista CVX pour interagir avec NSX-T Manager

Après avoir configuré NSX-T Data Center, effectuez la procédure de configuration sur Arista CloudVision eXchange (CVX) pour permettre à CVX d'interagir avec NSX-T Data Center.

Conditions préalables

NSX-T Data Center a enregistré CVX en tant que point d'application.

Procédure

- 1 Connectez-vous à NSX Manager en tant qu'utilisateur racine et exécutez la commande suivante pour créer une empreinte numérique pour que CVX communique avec NSX Manager :

```
openssl s_client -connect <IP address of nsx-manager>:443 | openssl x509 -pubkey -noout |
openssl rsa -pubin -outform der | openssl dgst -sha256 -binary | openssl base64
```

Exemple de résultat :

```
depth=0 C = US, ST = CA, L = Palo Alto, O = VMware Inc., OU = NSX, CN = nsx-mgr
verify error:num=18:self signed certificate
verify return:1
depth=0 C = US, ST = CA, L = Palo Alto, O = VMware Inc., OU = NSX, CN = nsx-mgr
verify return:1
writing RSA key
S+zwADluzeNf+dnffDpYvgs4YrS6QBgyeDry40bPgms=
```

- 2 Exécutez les commandes suivantes à partir de l'interface de ligne de commande de CVX :

```
cvx
no shutdown
service pcs
no shutdown
controller <IP address of nsx-manager>
username <NSX administrator user name>
password <NSX administrator password>
enforcement-point cvx-default-ep
pinned-public-key <thumbprint for CVX to communicate with NSX
                    Manager>
notification-id <notification ID created while registering CVX with NSX>
end
```

- 3 Exécutez la commande suivante à partir de l'interface de ligne de commande de CVX pour vérifier la configuration :

```
show running-config
```

Exemple de résultat :

```
cvx
  no shutdown
  source-interface Management1
  !
  service hsc
    no shutdown

  !
  service pcs
    no shutdown
    controller 192.168.2.80
    username admin
    password 7 046D26110E33491F482F2800131909556B
    enforcement-point cvx-default-ep
    pinned-public-key sha256//S+zwADluzeNf+dnffDpYvgs4YrS6QBgyeDry40bPgms=
    notification-id a0286cb6-de4d-41de-99a0-294465345b80
```

- 4 Configurez tag sur l'interface Ethernet du commutateur physique qui se connecte au serveur physique. Exécutez les commandes suivantes sur le commutateur physique géré par CVX.

```
configure terminal
interface ethernet 4
tag phy_app_server
end
copy running-config startup-config
Copy completed successfully.
```

- 5 Exécutez la commande suivante pour vérifier la configuration de la balise pour le commutateur :

```
show running-config section tag
```

Exemple de résultat :

```
interface Ethernet4
  description connected-to-7150s-3
  switchport trunk allowed vlan 1-4093
  switchport mode trunk
  tag sx4_app_server
```

Les adresses IP apprises sur les interfaces balisées, à l'aide d'ARP, sont partagées avec NSX-T Data Center.

- 6 Connectez-vous à NSX Manager pour créer et publier des règles de pare-feu pour les charges de travail physiques gérées par CVX. Pour plus d'informations sur la création de règles, consultez la section [Chapitre 10 Sécurité](#). Par exemple :

+ AJOUTER UNE STRATÉGIE + AJOUTER UNE RÈGLE CLONER ↩️ ANNULER 🗑️ SUPPRIMER ⋮									
	Nom	Sources	Destinations	Services	Profil	Appliqué à	Action		
⋮	Firewall_Services	(2)	Appliqué à	DFW				● Actif	ⓘ ⚙️
⋮	vm_to_phy_server	① 🌐 vm	🌐 phy_server	Quelconque	Aucun	DFW	● Autoriser	🔴	ⓘ ⚙️
⋮	phy_server_to_vm	① 🌐 phy_server	🌐 vm	Quelconque	Aucun	DFW	● Autoriser	🔴	ⓘ ⚙️

Les stratégies et règles de NSX-T Data Center publiées dans NSX-T Data Center s'affichent sous la forme de listes de contrôle d'accès dynamiques sur le commutateur physique géré par CVX.

```
prmh-nsx-tor-7050sx-4#show ip access-lists dynamic
IP Access List et4.v4.in [dynamic]
  10 permit ip host 71.1.1.3 host 27.1.1.11

IP Access List et4.v4.out [dynamic]
  10 permit ip host 27.1.1.11 host 71.1.1.3
```

Pour plus d'informations, reportez-vous aux sections [Configuration HA de CVX](#), [Configuration des adresses IP virtuelles HA de CVX](#) et [Configuration Mlag du commutateur physique](#)

Configurer NSX-T Data Center pour interagir avec Arista CVX

Effectuez la procédure de configuration sur NSX-T Data Center afin d'ajouter CVX en tant que point d'application dans NSX-T Data Center et de faire interagir NSX-T Data Center avec CVX.

Conditions préalables

Obtenez l'adresse IP virtuelle pour le cluster Arista CVX.

Procédure

- 1 Connectez-vous à NSX Manager en tant qu'utilisateur racine et exécutez la commande suivante pour récupérer l'empreinte numérique de CVX :

```
openssl s_client -connect <virtual IP address of CVX cluster> | openssl x509 -noout
-fingerprint -sha256
```

Exemple de résultat :

```
depth=0 CN = self.signed
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = self.signed
```



```
verify return:1
SHA256
Fingerprint=35:C1:42:BC:7A:2A:57:46:E8:72:F4:C8:B8:31:E3:13:5F:41:95:EF:D8:1E:E9:3D:F0:CC:3
B:09:A2:FE:22:DE
```

- 2 Modifiez l'empreinte numérique récupérée pour n'utiliser que des minuscules et exclure les deux-points dans l'empreinte numérique.

Exemple d'empreinte numérique modifiée pour CVX :

```
35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de
```

- 3 Appelez l'API `PATCH /policy/api/v1/infra/sites/default/enforcement-points` et utilisez l'empreinte numérique CVX pour créer un point de terminaison d'application pour CVX. Par exemple :

```
PATCH https://<nsx-manager>/policy/api/v1/infra/sites/default/enforcement-points/cvx-
default-ep
{
  "auto_enforce": "false",
  "connection_info": {
    "enforcement_point_address": "<IP address of CVX>",
    "resource_type": "CvxConnectionInfo",
    "username": "cvpadmin",
    "password": "1q2w3e4rT",
    "thumbprint": "65a9785e88b784f54269e908175ada662be55f156a2dc5f3a1b0c339cea5e343"
  }
}
```

- 4 Appelez l'API `GET /policy/api/v1/infra/sites/default/enforcement-points` pour récupérer les informations de point de terminaison. Par exemple :

```
https://<nsx-manager>/policy/api/v1/infra/sites/default/enforcement-points/cvx-default-ep
{
  "auto_enforce": "false",
  "connection_info": {
    "enforcement_point_address": "<IP address of CVX>",
    "resource_type": "CvxConnectionInfo",
    "username": "admin",
    "password": "1q2w3e4rT",
    "thumbprint": "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de"
  }
}
```

Exemple de résultat :

```
{
  "connection_info": {
    "thumbprint": "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
    "enforcement_point_address": "192.168.2.198",
    "resource_type": "CvxConnectionInfo"
  },
  "auto_enforce": false,
```

```

    "resource_type": "EnforcementPoint",
    "id": "cvx-default-ep",
    "display_name": "cvx-default-ep",
    "path": "/infra/sites/default/enforcement-points/cvx-default-ep",
    "relative_path": "cvx-default-ep",
    "parent_path": "/infra/sites/default",
    "marked_for_delete": false,
    "_system_owned": false,
    "_create_user": "admin",
    "_create_time": 1564036461953,
    "_last_modified_user": "admin",
    "_last_modified_time": 1564036461953,
    "_protection": "NOT_PROTECTED",
    "_revision": 0
  }

```

- 5 Appelez l'API POST `/api/v1/notification-watchers/` et utilisez l'empreinte numérique CVX pour créer un ID de notification. Par exemple :

```

POST https://<nsx-manager>/api/v1/notification-watchers/
{
  "server": "<virtual IP address of CVX cluster>",
  "method": "POST",
  "uri": "/pcs/v1/nsgroup/notification",
  "use_https": true,
  "certificate_sha256_thumbprint":
  "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
  "authentication_scheme": {
    "scheme_name": "BASIC_AUTH",
    "username": "cvpadmin",
    "password": "1q2w3e4rT"
  }
}

```

- 6 Appelez GET `/api/v1/notification-watchers/` pour récupérer l'ID de notification.

Exemple de résultat :

```

{
  "id": "a0286cb6-de4d-41de-99a0-294465345b80",
  "server": "192.168.2.198",
  "port": 443,
  "use_https": true,
  "certificate_sha256_thumbprint":
  "35c142bc7a2a5746e872f4c8b831e3135f4195efd81ee93df0cc3b09a2fe22de",
  "method": "POST",
  "uri": "/pcs/v1/nsgroup/notification",
  "authentication_scheme": {
    "scheme_name": "BASIC_AUTH",
    "username": "cvpadmin"
  },
  "send_timeout": 30,
  "max_send_uri_count": 5000,
  "resource_type": "NotificationWatcher",
}

```

```

    "display_name": "a0286cb6-de4d-41de-99a0-294465345b80",
    "_create_user": "admin",
    "_create_time": 1564038044780,
    "_last_modified_user": "admin",
    "_last_modified_time": 1564038044780,
    "_system_owned": false,
    "_protection": "NOT_PROTECTED",
    "_revision": 0
  }

```

- 7 Appelez l'API PATCH `/policy/api/v1/infra/domains/default/domain-deployment-maps/cvx-default-dmap` pour créer un mappage de déploiement de domaine CVX. Par exemple :

```

PATCH https://<nsx-manager>/policy/api/v1/infra/domains/default/domain-deployment-maps/cvx-default-dmap
{

  "display_name": "cvx-deployment-map",

  "id": "cvx-default-dmap",

  "enforcement_point_path": "/infra/sites/default/enforcement-points/cvx-default-ep"

}

```

- 8 Appelez l'API GET `/policy/api/v1/infra/domains/default/domain-deployment-maps` pour récupérer les informations de mappage de déploiement.

Ensembles d'adresses partagées

Les groupes de sécurité basés sur des objets dynamiques ou logiques peuvent être créés et utilisés dans la zone de texte **Appliqué à** de règles de pare-feu distribué.

Comme les ensembles d'adresses sont renseignés dynamiquement en fonction du nom ou des balises de la machine virtuelle, et doivent être mis à jour sur chaque filtre, ils peuvent épuiser la quantité disponible de mémoire de segment sur les hôtes pour stocker des règles DFW et des ensembles d'adresses IP.

Dans NSX-T Data Center 2.5 et versions ultérieures, une fonctionnalité appelée Ensembles d'adresses globales ou partagées permet de partager les ensembles d'adresses entre tous les filtres. Même si chaque filtre peut avoir des règles différentes, selon **Appliqué à**, les membres des ensembles d'adresses sont constants dans tous les filtres. Cette fonctionnalité est activée par défaut, ce qui réduit l'utilisation de la mémoire de segment. Elle ne peut pas être désactivée.

Dans NSX-T Data Center 2.4 et versions antérieures, la fonctionnalité Ensembles d'adresses globales ou partagées est désactivée, et les environnements avec des règles de pare-feu distribué lourdes peuvent rencontrer des insuffisances de segment de mémoire VSIP.

Sécurité du réseau est-ouest : chaînage des services tiers

Dès que les partenaires ont enregistré leurs services réseau, comme le système de détection des intrusions ou le système de prévention des intrusions (IDS/IPS), auprès de NSX-T Data Center, en tant qu'administrateur, vous pouvez configurer des services réseau pour examiner le trafic horizontal se déplaçant entre les machines virtuelles d'un centre de données sur site.

Conditions préalables

- Les partenaires enregistrent des services auprès de NSX-T Data Center.
- Les hôtes ESXi doivent être préparés comme des nœuds de transport NSX-T Data Center en utilisant des profils de nœud de transport.

Note

- Les machines virtuelles de service sont uniquement prises en charge sur les hôtes ESXi et pas sur les hôtes KVM.
 - NSX-T Data Center protège uniquement les machines virtuelles invitées s'exécutant sur des hôtes ESXi.
 - NSX-T Data Center ne protège pas les machines virtuelles invitées exécutées sur les hôtes KVM.
-

Concepts clés de la protection de réseau horizontal

Le trafic circulant entre les machines virtuelles invitées sur un centre de données sur site est protégé par les services tiers fournis par les partenaires. Quelques concepts facilitent la compréhension du workflow.

- **Service** : les partenaires enregistrent des services auprès de NSX-T Data Center. Un service représente la fonctionnalité de sécurité proposée par le partenaire, les détails de déploiement de service, comme l'URL OVF des machines virtuelles de service, le point de liaison du service et l'état du service.
- **Modèle fournisseur** : il se compose de la fonctionnalité qu'un service peut exécuter sur un trafic réseau. Les partenaires définissent des modèles fournisseur. Par exemple, un modèle fournisseur peut fournir un service d'opération réseau, comme le tunneling avec le service IPSec.
- **Profil de service** : instance d'un modèle fournisseur. Un administrateur de NSX-T Data Center peut créer un profil de service que les machines virtuelles de service doivent utiliser.
- **Machine virtuelle invitée** : source ou destination du trafic dans le réseau. Le trafic entrant ou sortant est examiné par une chaîne de services définie pour une règle exécutant des services de réseau horizontal.
- **Machine virtuelle de service** : machine virtuelle qui exécute le dispositif OVA ou OVF spécifié par un service. Elle est connectée par le biais du plan de service afin de recevoir le trafic redirigé.

- Instance de service : créée lorsqu'un service est déployé sur un hôte. Chaque instance de service comporte une machine virtuelle de service correspondante.
- Segment de service : segment d'un plan de service associé à une zone de transport. Chaque attachement de service est séparé des autres, ainsi que des segments de réseau L2 ou L3 normaux fournis par NSX-T. Le plan de service gère les attachements de service.
- Service Manager : Service Manager partenaire qui pointe vers un ensemble de services.
- Chaîne de services : séquence logique de profils de service, définie par un administrateur. Les profils de service examinent le trafic réseau dans l'ordre défini dans la chaîne de services. Par exemple, le premier profil de service est le pare-feu, le deuxième est le moniteur, etc. Des chaînes de services peuvent spécifier une séquence différente de profils de service pour les différentes directions du trafic (entrée/sortie).
- Stratégie de redirection : garantit que le trafic classé pour une chaîne de services spécifique est redirigé vers cette chaîne de services. Elle repose sur des modèles de trafic qui correspondent au groupe de sécurité NSX-T Data Center et à une chaîne de services. L'ensemble du trafic correspondant au modèle est redirigé le long de la chaîne de services.
- Chemin d'accès aux services : séquence de machines virtuelles de service qui mettent en œuvre les profils de service d'une chaîne de services. Un administrateur définit la chaîne de services, qui se compose d'une commande prédéfinie de profils de service. NSX-T Data Center génère plusieurs chemins d'accès aux services à partir d'une chaîne de services reposant sur le nombre et les emplacements des machines virtuelles invitées et des machines virtuelles de service. Il sélectionne le chemin d'accès aux services optimal pour le flux de trafic à examiner. Chaque chemin d'accès aux services est identifié par un index de chemin d'accès aux services et chaque saut le long d'un chemin porte un index de service unique.

Exigences de NSX-T Data Center pour le trafic est-ouest

Dans le déploiement de NSX-T Data Center, vous devez vous assurer qu'une zone de transport de superposition et des commutateurs logiques basés sur la superposition existent.

L'insertion de services est-ouest est appliquée à l'intégralité d'un déploiement de NSX-T. Vous ne pouvez pas déployer le service au niveau du cluster ou au niveau de l'hôte.

Tous les nœuds de transport doivent être de type Superposition, car le service envoie du trafic sur des commutateurs logiques GENEVE ou supportés par la superposition. Un commutateur logique supporté par la superposition (reposant sur GENEVE) est provisionné en interne et n'est pas visible dans l'interface utilisateur.

Même si vous prévoyez un déploiement à l'aide de commutateurs logiques basés sur VLAN uniquement, le trafic est-ouest passe par des zones de transport de superposition et des commutateurs logiques supportés par la superposition. Par conséquent, assurez-vous de créer une zone de transport de superposition et des commutateurs logiques reposant sur GENEVE. Sans ces exigences, lors d'une opération vMotion, la guestVM sur un hôte ne peut pas être migrée vers un autre nœud de transport. La guestVM passe à l'état Déconnecté, provoquant des erreurs de configuration dans le service est-ouest.

Tâches de haut niveau de la sécurité réseau est-ouest

Suivez ces étapes pour configurer la sécurité réseau du trafic est-ouest.

Tableau 10-3. Liste des tâches de configuration de l'introspection réseau horizontale

Tâches du workflow	Persona	Mise en œuvre
Enregistrer un service	Partenaire	API uniquement
Enregistrer un modèle de fournisseur	Partenaire	API uniquement
Enregistrer Service Manager	Partenaire	API uniquement
Déployer un service pour l'introspection horizontale du trafic	Administrateur	API et interface utilisateur NSX Manager
Ajouter un profil de service	Administrateur	API et interface utilisateur NSX Manager
Ajouter une chaîne de services	Administrateur	API et interface utilisateur NSX Manager
Ajouter des règles de redirection pour le trafic horizontal	Administrateur	API et interface utilisateur NSX Manager

Déployer un service pour l'introspection horizontale du trafic

Une fois que les partenaires ont enregistré leurs services, en tant qu'administrateur, vous devez déployer une instance de ces services sur les hôtes membres d'un cluster.

Déployez les machines virtuelles de service de partenaires qui exécutent le moteur de sécurité partenaire sur tous les hôtes NSX-T Data Center d'un cluster. Après avoir déployé les SVM, vous pouvez créer des règles de stratégie utilisées par les SVM pour protéger les machines virtuelles invitées.

Conditions préalables

- Tous les hôtes sont gérés par un vCenter Server.
- Les services de partenaires doivent être enregistrés auprès de NSX-T Data Center et sont prêts pour le déploiement.
- Les administrateurs de NSX-T Data Center peuvent accéder aux services de partenaires et aux modèles fournisseur.
- La machine virtuelle de service et le Service Manager partenaire (console) doivent être en mesure de communiquer entre eux au niveau du réseau de gestion.
- Déploiement de service basé sur l'hôte : avant de déployer des machines virtuelles de service sur chaque hôte, configurez chaque hôte du cluster avec NSX-T Data Center en appliquant un profil de nœud de transport.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Système > Déploiements de service > Déploiement > Déployer un service**.
- 3 Dans le champ Service de partenaires, sélectionnez le service de partenaires.
- 4 Entrez le nom du déploiement de service.
- 5 Dans le champ Gestionnaire de calcul, sélectionnez l'instance de vCenter Server pour déployer le service.
- 6 Dans le champ Cluster, sélectionnez le cluster dans lequel les services doivent être déployés.
- 7 Dans le menu déroulant Banque de données, sélectionnez une banque de données comme référentiel pour la machine virtuelle de service.
- 8 Dans la colonne Réseau, cliquez sur **Définir**, et accédez à l'interface du réseau de gestion en choisissant le type d'adresse DHCP ou IP statique et le réseau de données.
- 9 Dans le champ Segments de service, sélectionnez un segment de service dans la liste ou cliquez sur l'icône Action pour ajouter ou modifier un segment de service. Les machines virtuelles invitées connectées à un segment de service bénéficient de la protection du trafic réseau est-ouest.
- 10 Dans le champ Type de déploiement, sélectionnez l'une des options de déploiement suivantes : Selon les services enregistrés par le partenaire, plusieurs services peuvent être déployés dans le cadre d'une machine virtuelle de service unique.
 - En cluster : déploie le service sur un hôte ou des hôtes appartenant à un cluster dédié aux machines virtuelles de service de l'hôte.
 - Basé sur l'hôte : déploie le service sur tous les hôtes d'un cluster.
- 11 Dans le champ Modèle de déploiement, sélectionnez le modèle qui fournit des attributs pour protéger la charge de travail que vous souhaitez exécuter sur les groupes de machines virtuelles invitées.
- 12 (Déploiement basé sur cluster uniquement) Dans Nombre de déploiements en cluster, entrez le nombre de machines virtuelles de service à déployer sur le cluster. vCenter Server décide sur quel hôte déployer les machines virtuelles de service.
- 13 Cliquez sur **Enregistrer**.

Résultats

Après le déploiement de service, le Service Manager partenaire est informé de la mise à jour.

Étape suivante

Vous devez connaître les détails du déploiement et l'état de santé des instances de service déployées sur les hôtes. Reportez-vous à la section [Ajouter un profil de service](#).

Ajouter un profil de service

Un profil de service est une instance du modèle de fournisseur d'un partenaire. Les administrateurs peuvent personnaliser les attributs d'un modèle de fournisseur pour créer une instance du modèle.

Note Vous pouvez créer plusieurs profils de service pour un seul fournisseur. Par exemple, le profil de service défini pour le chemin de transfert fournit la protection des ID, tandis que le profil de service défini pour le chemin inverse prend en charge la protection des IP. Cependant, un seul profil de service peut être défini pour les chemins direct et inverse.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Accédez à **Sécurité > Sécurité Est-Ouest > Introspection réseau > Profils de service**.
- 3 Sélectionnez un service dans le champ déroulant Service de partenaire. Vous pouvez créer un profil de service pour le service sélectionné.
- 4 Entrez le nom du profil de service et sélectionnez le modèle de fournisseur.
- 5 Le champ Action de redirection hérite la fonctionnalité du modèle de fournisseur. Par exemple, si COPY est la fonctionnalité fournie par le modèle de fournisseur, par défaut, l'action de redirection lorsque vous créez un profil de service est COPY.
- 6 (Facultatif) Définissez des balises pour filtrer et gérer les profils de service.
- 7 Cliquez sur **Enregistrer**.

Résultats

Un nouveau profil de service est créé pour le service de partenaires.

Étape suivante

Ajoutez une chaîne de service. Reportez-vous à la section [Ajouter une chaîne de services](#).

Ajouter une chaîne de services

Une chaîne de services est une séquence logique de profils de service, définie par l'administrateur réseau.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Sécurité > Sécurité Est-Ouest > Introspection réseau > Chaîne de services > Ajouter une chaîne**.
- 3 Entrez le nom de la chaîne de services.

- 4 Dans le champ Segments de service, sélectionnez le segment de service auquel vous souhaitez appliquer la chaîne de services. Un segment de service est un segment de plan de service qui se connecte à plusieurs machines virtuelles de service d'une zone de transport de superposition. Chaque machine virtuelle de service de la chaîne de services est distincte d'une autre machine virtuelle de service, et des segments de réseau L2 et L3 exécutés par NSX-T Data Center. Le plan de service contrôle l'accès aux machines virtuelles de service.
- 5 Pour définir le chemin de transfert, cliquez sur le champ **Définir le chemin de transfert**, puis sur **Ajouter un profil dans la séquence**.
- 6 Ajoutez le premier profil dans la chaîne de services et cliquez sur **Ajouter**.
- 7 Pour spécifier le profil de service suivant, cliquez sur **Ajouter un profil dans la séquence** et entrez des détails. Vous pouvez également réorganiser l'ordre des profils en utilisant les icônes représentant une flèche vers le haut ou vers le bas.
- 8 Cliquez sur **Enregistrer** pour terminer l'ajout d'un chemin de transfert pour la chaîne de services.
- 9 Dans la colonne Chemin inverse, sélectionnez **Chemin de transfert inverse** pour que le plan de service utilise le profil de service que vous avez défini pour le chemin de transfert.
- 10 Pour définir un nouveau profil de service pour le chemin inverse, cliquez sur **Définir le chemin inverse** et ajoutez un profil de service.
- 11 Cliquez sur **Enregistrer** pour terminer l'ajout d'un chemin inverse pour la chaîne de services.
- 12 Dans le champ Stratégie en cas de panne :
 - Sélectionnez **Autoriser** pour diriger le trafic vers la machine virtuelle de destination en cas de défaillance de la machine virtuelle de service. La défaillance de la machine virtuelle de service est détectée par le mécanisme de détection de réactivité qui ne peut être activé que par des partenaires.
 - Sélectionnez **Bloquer** pour ne pas diriger le trafic vers la machine virtuelle de destination en cas de défaillance de la machine virtuelle de service.
- 13 Cliquez sur **Enregistrer**.

Résultats

Après l'ajout d'une chaîne de services, le Service Manager partenaire est informé de la mise à jour.

Étape suivante

Créez une règle de redirection pour examiner le trafic réseau horizontal. Reportez-vous à la section [Ajouter des règles de redirection pour le trafic horizontal](#).

Ajouter des règles de redirection pour le trafic horizontal

Ajoutez des règles pour rediriger un trafic horizontal à des fins d'introspection du réseau.

Les règles sont définies dans une stratégie. La stratégie en tant que concept est similaire à la notion de sections dans les pare-feu. Lorsque vous ajoutez une stratégie, sélectionnez la chaîne de services afin de rediriger le trafic pour l'inspection par les profils de service de la chaîne de services.


La définition d'une règle comprend la source et la destination du trafic, un service d'inspection, l'objet NSX-T Data Center sur lequel appliquer la règle et la stratégie de redirection du trafic. Une fois la règle publiée, NSX Manager la déclenche lorsqu'un modèle de trafic correspondant est localisé. La règle commence à examiner le trafic. Par exemple, lorsque NSX Manager désigne un flux de trafic devant être examiné, il ne le transfère pas vers le pare-feu distribué habituel, mais le redirige le long de la chaîne de services indiquée dans la stratégie. Les profils de service définis dans la chaîne de services examinent le trafic des services de réseau que le partenaire propose. Si un profil de service termine l'inspection sans détecter de problèmes de sécurité au niveau du trafic, ce dernier est transféré vers le profil de service suivant dans la chaîne de services. À la fin de la chaîne de services, le trafic est transféré vers la cible de destination.

Toutes les notifications sont envoyées aux Service Manager et NSX-T Data Center partenaires.

Conditions préalables

Une chaîne de services est disponible pour rediriger le trafic pour une inspection du réseau.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 **Sécurité > Sécurité Est-Ouest > Inspection réseau > Règles > Ajouter une stratégie.**
Une section de stratégie est semblable à une section de pare-feu dans laquelle vous définissez des règles qui déterminent la circulation du trafic.
- 3 Sélectionnez une chaîne de services.
- 4 Pour ajouter une stratégie, cliquez sur **Publier**.
- 5 Cliquez sur l'icône de sélection verticale  d'une section et cliquez sur **Ajouter une règle**.

- 6 Modifiez le champ **Source** pour ajouter un groupe en définissant des critères d'appartenance, des membres statiques, des adresses IP/MAC ou des groupes Active Directory.
 - a Définissez les critères d'appartenance à l'aide de l'une de ces entités :
 - Machine virtuelle
 - Commutateur logique
 - Port logique
 - Ensemble d'adresses IP
 - b Définissez la liste des membres statiques à l'aide de l'une de ces entités :
 - Groupe
 - Segment
 - Port de segment
 - Interface réseau virtuelle
 - Machine virtuelle
- 7 Cliquez sur **Enregistrer**.
- 8 Pour ajouter un groupe de destination, modifiez le champ **Destination**.
- 9 Dans le champ Appliqué à, vous pouvez effectuer l'une des opérations suivantes :
 - Sélectionnez **DFW** pour appliquer la règle à toutes les cartes réseau virtuelles attachées au commutateur logique.
 - Sélectionnez **Groupe de machines virtuelles** pour appliquer la règle sur des cartes réseau virtuelles des machines virtuelles membres du groupe. Les membres peuvent être sélectionnés dans une liste statique ou en fonction de critères dynamiques. Les objets NSX-T Data Center pris en charge sont les suivants : Machine virtuelle, Commutateur logique, Port logique, Ensemble d'adresses IP, etc.
- 10 Dans le champ Action, sélectionnez **Rediriger** pour rediriger le trafic le long de la chaîne de services ou **Ne pas rediriger** pour ne pas appliquer l'inspection du réseau sur le trafic.
- 11 Cliquez sur **Publier**.
- 12 Pour restaurer une règle publiée, sélectionnez une règle et cliquez sur **Restaurer**.
- 13 Pour ajouter une stratégie, cliquez sur **+ Ajouter une stratégie**.
- 14 Pour cloner une stratégie ou une règle, sélectionnez la stratégie ou une règle, et cliquez sur **Cloner**.
- 15 Pour activer une règle, activez l'icône Activer/Désactiver ou sélectionnez la règle et, dans le menu, cliquez sur **Activer > Activer une règle**.
- 16 Après l'activation ou la désactivation d'une règle, cliquez sur **Publier** pour l'appliquer.

Résultats

Le trafic en direction de la source est redirigé vers la chaîne de services pour l'introspection du réseau. Une fois que les profils de service de la chaîne ont examiné le trafic, il est envoyé à destination.

Pendant le déploiement, il est possible que l'appartenance à un groupe de machines virtuelles d'une stratégie particulière change. NSX-T Data Center informe le Service Manager partenaire de ces mises à jour.

Configuration d'un pare-feu de passerelle

Le pare-feu de passerelle représente les règles appliquées au niveau du pare-feu de périmètre.

La vue **Toutes les règles partagées** comporte des catégories prédéfinies, dans lesquelles les règles appliquées sur l'ensemble des passerelles sont visibles. Les règles sont évaluées de haut en bas et de gauche à droite. Les noms des catégories peuvent être modifiés à l'aide de l'API.

Tableau 10-4. Catégories de règles de pare-feu de passerelle

Catégorie de règles	Objectif
Urgence	Utilisée pour la mise en quarantaine. Peut également être utilisée pour autoriser des règles.
Système	Ces règles sont automatiquement générées par NSX-T Data Center et sont spécifiques du trafic du plan de contrôle interne, comme les règles BFD, les règles VPN, etc. Note Ne modifiez pas les règles du système.
Règles préalables partagées	Ces règles sont appliquées globalement sur les passerelles.
Passerelle locale	Ces règles sont spécifiques d'une passerelle particulière.
Règles de services automatiques	Il s'agit de règles automatiquement raccordées, appliquées au plan de données. Vous pouvez modifier ces règles si nécessaire.
Par défaut	Ces règles définissent le comportement par défaut du pare-feu de passerelle.

Ajouter une règle ou une stratégie de pare-feu de passerelle

Mettez en œuvre des règles de pare-feu de passerelle en les ajoutant sous une section de stratégie de pare-feu appartenant à une catégorie prédéfinie.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Sécurité > Sécurité nord-sud > Pare-feu de passerelle**.

- 3 Pour activer le pare-feu de passerelle, sélectionnez **Actions > Paramètres généraux** et faites basculer le bouton État. Cliquez sur **Enregistrer**.
- 4 Cliquez sur **Ajouter une stratégie**. Pour plus d'informations sur les catégories, reportez-vous à la section [Configuration d'un pare-feu de passerelle](#).
- 5 Entrez un **Nom** pour la nouvelle section de stratégie.
- 6 Sélectionnez la **Destination** de la stratégie.
- 7 Cliquez sur l'icône d'engrenage pour configurer les paramètres de stratégie suivants :

Paramètres	Description
TCP strict	Une connexion TCP commence par un établissement de liaison en trois temps (SYN, SYN-ACK, ACK) et se termine généralement par un échange bidirectionnel (FIN, ACK). Dans certaines circonstances, le pare-feu ne voit pas l'établissement de liaison en trois temps pour un flux particulier (par exemple, en raison du trafic asymétrique). Par défaut, le pare-feu n'impose pas le besoin de voir un établissement de liaison en trois temps et les sessions de collecte déjà établies. TCP strict peut être activé sur une base par section pour désactiver la prise en charge en milieu de session et appliquer la condition requise pour l'établissement d'une liaison en trois temps. Lors de l'activation du mode TCP strict pour une stratégie de pare-feu spécifique et de l'utilisation d'une règle ANY-ANY Block par défaut, les paquets qui ne remplissent pas les conditions requises de connexion d'établissement d'une liaison en trois temps et qui correspondent à une règle TCP dans cette section sont abandonnés. Strict s'applique uniquement aux règles TCP avec état et est activé au niveau de la stratégie du pare-feu de passerelle. TCP strict n'est pas appliqué pour les paquets qui correspondent à une valeur par défaut ANY-ANY Allow qui n'a aucun service TCP spécifié.
Avec état	Un pare-feu avec état surveille l'état des connexions actives et utilise ces informations pour déterminer les paquets à autoriser via le pare-feu.
Verrouillé	La stratégie peut être verrouillée pour empêcher plusieurs utilisateurs d'apporter des modifications à la même section. Vous devez inclure un commentaire lors du verrouillage d'une section.

- 8 Cliquez sur **Publier**. Il est possible d'ajouter plusieurs stratégies à la fois et de les publier ensemble.
La nouvelle stratégie s'affiche à l'écran.
- 9 Sélectionnez une section de stratégie et cliquez sur **Ajouter une règle**.

- 10 Entrez un nom pour la règle. Les adresses IPv4, IPv6 et de multidiffusion sont prises en charge.
- 11 Dans la colonne **Sources**, cliquez sur l'icône de modification et sélectionnez la source de la règle. Pour plus d'informations, reportez-vous à [Ajouter un groupe](#).
- 12 Dans la colonne **Destinations**, cliquez sur l'icône de modification et sélectionnez la destination de la règle. La destination correspond à n'importe laquelle si elle n'est pas définie. Pour plus d'informations, reportez-vous à la section [Ajouter un groupe](#).
- 13 Dans la colonne **Services**, cliquez sur l'icône de crayon et sélectionnez les services. Le service correspond à n'importe lequel s'il n'est pas défini.
- 14 Dans la colonne **Profils**, cliquez sur l'icône de modification et sélectionnez un profil de contexte, ou cliquez sur **Ajouter un nouveau profil de contexte**. Reportez-vous à la section [Ajouter un profil de contexte](#).
 - Les profils de contexte ne sont pas pris en charge sur la stratégie de pare-feu de passerelle de niveau 0.
 - Les règles de pare-feu de passerelle ne prennent pas en charge les profils de contexte avec des attributs de nom de domaine complet ou d'autres sous-attributs.

Les profils de contexte utilisent les attributs de l'ID d'application de couche 7 pour une utilisation dans des règles de pare-feu distribué et des règles de pare-feu de passerelle. Il est possible d'utiliser plusieurs profils de contexte d'ID d'application dans une règle de pare-feu avec des services définis sur **Quelconque**. Pour les profils ALG (FTP et TFTP), un seul profil de contexte est pris en charge par règle.

- 15 Cliquez sur **Appliquer**.
- 16 La colonne **Appliqué à** définit l'étendue de l'application par règle et permet aux utilisateurs d'appliquer de manière sélective des règles à une ou plusieurs interfaces de liaison montante ou à une interface de service. Par défaut, les règles de pare-feu de passerelle sont appliquées à toutes les liaisons montantes et interfaces de service disponibles sur une passerelle sélectionnée.

- 17 Dans la colonne **Action**, sélectionnez une action.

Option	Description
Autoriser	Autorise l'ensemble du trafic 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 rejet d'un paquet 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'application d'envoi est informée après une tentative d'établissement de la connexion.

- 18 Cliquez sur le bouton bascule État pour activer ou désactiver la règle.
- 19 Cliquez sur l'icône représentant un engrenage pour définir la journalisation, la direction, le protocole IP, une balise et des remarques.

Option	Description
Journalisation	La journalisation peut être désactivée ou activée. Les journaux sont stockés dans /var/log/syslog sur le dispositif Edge.
Direction	Les options sont In , Out et In/Out . La valeur par défaut est In/Out . Ce champ fait référence à la direction du trafic selon le point de vue de l'objet de destination. In signifie que seul le trafic vers l'objet est vérifié, Out signifie que seul le trafic provenant de l'objet est vérifié et In/Out signifie que le trafic dans les deux sens est vérifié.
Protocole IP	Les options sont IPv4 , IPv6 et IPv4_IPv6 . La valeur par défaut est IPv4_IPv6 .
Balise	Balise qui a été ajoutée à la règle.

Note Cliquez sur l'icône de graphique pour afficher les statistiques de flux de la règle de pare-feu. Vous pouvez voir des informations telles que le nombre d'octets, le nombre de paquets et les sessions.

- 20 Cliquez sur **Publier**. Il est possible d'ajouter plusieurs règles à la fois et de les publier ensemble.
- 21 Dans chaque section de stratégie, cliquez sur l'icône **Infos** pour afficher l'état actuel des règles de pare-feu Edge qui sont envoyées aux nœuds Edge. Toutes les alarmes générées lorsque des règles ont été transmises à des nœuds Edge sont également affichées.

- 22** Pour afficher l'état consolidé des règles de stratégie appliquées à des nœuds Edge, effectuez l'appel d'API.

```
GET https://<policy-mgr>/policy/api/v1/infra/
realized-state/status?intent_path=/infra/domains/default/gateway-policies/
<GatewayPolicy_ID>&include_enforced_status=true
```

Sécurité du réseau nord-sud : insertion de service tiers

NSX-T Data Center fournit la fonctionnalité permettant d'insérer des services tiers sur un routeur de niveau 0 ou de niveau 1 dans le centre de données pour rediriger le trafic vers le service tiers pour l'introspection. Seuls les hôtes ESXi sont pris en charge pour déployer des machines virtuelles de service nord-sud. Les hôtes KVM ne sont pas pris en charge.

Tâches de haut niveau de la sécurité réseau nord-sud

Suivez ces étapes pour configurer la sécurité réseau du trafic nord-sud.

Tableau 10-5. Liste des tâches de configuration de l'introspection verticale du réseau

Tâches du workflow	Persona	Mise en œuvre
Enregistrer le service auprès de NSX-T Data Center	Partenaire	API uniquement
Déployer un service pour l'introspection verticale du trafic	Administrateur	API et interface utilisateur NSX Manager
Configurer la redirection du trafic	Administrateur	API et interface utilisateur NSX Manager

Déployer un service pour l'introspection verticale du trafic

Après l'enregistrement d'un service, vous devez déployer une instance de service pour ce service afin de démarrer le traitement du trafic réseau.

Déployez la machine virtuelle de service de partenaires sur le routeur logique de niveau 0 ou 1 qui agit comme une passerelle entre le monde physique et le réseau logique sur vCenter Server. Après avoir déployé la SVM comme une instance de service autonome ou une instance de service Actif-En veille, vous pouvez créer des règles de redirection pour rediriger le trafic vers la SVM à des fins d'introspection du réseau.

Conditions préalables

- Tous les hôtes sont gérés par un vCenter Server.
- Les services de partenaires sont enregistrés auprès de NSX-T Data Center et sont prêts pour le déploiement.
- NSX-T Data Center administrateurs peuvent accéder aux services de partenaires.

- Le mode haute disponibilité pour le routeur logique doit être en mode actif-veille.
- Activez l'utilitaire Distributed Resource Scheduler.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Services de partenaires > Instances de service > Catalogue**.
- 3 L'onglet Catalogue affiche les services enregistrés.
- 4 Sélectionnez le service affiché au format OVF et cliquez sur **Déployer** pour commencer le déploiement de l'instance de service.
- 5 Dans la fenêtre Insertion de services de partenaires, cliquez sur **Continuer**.
- 6 Dans la fenêtre Service de partenaires, entrez les détails.

Tableau 10-6. Détails des services de partenaires

Champ	Description
Nom de l'instance	Entrez un nom pour identifier l'instance de service.
Description	Description de l'instance de service.
Service de partenaires	Sélectionnez le service de partenaires enregistré avec NSX-T Data Center.
Spécification de déploiement	Sélectionnez le format à déployer.
Routeur logique	Sélectionnez le routeur logique de niveau 0 sur lequel l'instance de service doit être déployée.

- 7 Cliquez sur **Suivant**.
- 8 Dans la fenêtre Configuration de l'instance, entrez les détails.

Tableau 10-7. Détails de l'instance de service

Champ	Description
Mode de déploiement	Sélectionnez Autonome pour déployer une instance de service unique sur le routeur logique de niveau 0. Sélectionnez Haute disponibilité pour déployer les deux instances de service en mode Actif-En veille sur le routeur logique de niveau 0.
Stratégie en cas de panne	Sélectionnez Autoriser ou Bloquer .
Adresse IP de l'instance de service	Entrez l'adresse IP que l'instance de service doit utiliser.
Passerelle	Entrez une adresse de passerelle.
Masque de sous-réseau	Entrez le masque de sous-réseau.

Tableau 10-7. Détails de l'instance de service (suite)

Champ	Description
ID du réseau	Entrez l'ID du réseau du commutateur logique sur lequel vous souhaitez vous connecter au réseau de gestion.
Gestionnaire de calcul	Sélectionnez l'instance de vCenter Server enregistrée.
Pool de ressources	Sélectionnez le pool de ressources qui fournit des ressources pour le déploiement de l'instance de service.
Banque de données	Sélectionnez le référentiel pour stocker les données de l'instance de service.

9 Cliquez sur **Suivant**.

10 Dans la fenêtre Configuration avancée, entrez les détails.

Tableau 10-8.

Champ	Description
Modèle de déploiement	Sélectionnez le modèle à utiliser lors du déploiement de l'instance de service.
Licence	Entrez la licence du modèle.

11 Cliquez sur **Terminer**.

Résultats

L'onglet Instances de service affiche la progression du déploiement. Le déploiement peut prendre quelques minutes. Vérifiez l'état du déploiement pour vous assurer que l'instance de service est correctement déployée sur le routeur logique de niveau 0.

Sinon, accédez à vCenter Server et vérifiez l'état du déploiement.

Étape suivante

Configurez des règles pour rediriger le trafic vers l'instance de service déployée sur le routeur de niveau 0. Reportez-vous à la rubrique [Configurer la redirection du trafic](#)

Configurer la redirection du trafic

Après avoir déployé une instance de service, configurez 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 [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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Services de partenaires > Instances de service**.
- 3 Cliquez sur l'instance de service.
- 4 Cliquez sur l'onglet **Redirection du trafic**.
- 5 Pour ajouter une section, sélectionnez une section existante et cliquez sur **Ajouter une section**.

- ◆ Dans le menu, sélectionnez **Ajouter une section au-dessus** ou **Ajouter une section au-dessous**.

Une nouvelle section est créée. Le type de trafic à rediriger est défini sur **Redirection L3**, le service est de type **Sans état**, le champ **Appliqué à** est associé à un routeur logique de niveau 0 qui est configuré sur l'hôte. Une fois que vous avez défini des règles, le champ **Règles** est rempli automatiquement.

- 6 Cliquez sur **Publier** pour conserver les détails de configuration de la section.
- 7 Pour ajouter une règle dans cette section, sélectionnez la section et cliquez sur **Ajouter une règle**.
- 8 Dans la ligne règle, entrez les détails suivants :
 - a Entrez un nom de règle.
 - b Entrez la source et la destination du trafic L3. La VM de service de partenaires examine le trafic circulant depuis la source avant de le rediriger vers la VM de destination.
 - c Dans le champ **Appliqué à**, sélectionnez la liaison montante du routeur de niveau 0.
 - d Dans le champ **Action**, sélectionnez **Rediriger** si le trafic doit être examiné par les VM de service ou sélectionnez **Ne pas rediriger** si le trafic n'a pas besoin d'être examiné pour l'inspection nord-sud.
- 9 Chaque règle peut être activée individuellement. Une fois que vous avez activé une règle, elle s'applique au trafic correspondant à la règle.
- 10 Cliquez sur Paramètres avancés pour configurer la direction du trafic et pour activer la journalisation.
- 11 À la fin d'une section contenant des règles, cliquez sur **Publier** pour conserver les règles dans la section ou cliquez sur **Restaurer** pour annuler l'opération.

Résultats

Le trafic est envoyé aux règles d'inspection réseau où les règles de stratégie sont appliquées au trafic.

Étape suivante

Reportez-vous à la section [Ajouter des règles de redirection pour le trafic nord-sud](#).

Ajouter des règles de redirection pour le trafic nord-sud


Utilisez l'interface utilisateur **Mise en réseau et sécurité avancées** pour configurer des règles de redirection nord-sud. La redirection du trafic se produit uniquement pour les services insérés sur le routeur de niveau 0.

Suivez les instructions de la section [Configurer la redirection du trafic](#).

Conditions préalables

- Enregistrez et déployez des services tiers sur NSX-T.
- Configurez le routeur de niveau 0.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 **Sécurité > Pare-feu nord sud > Introspection réseau (N-S) > Ajouter une stratégie.**
Une section de stratégie est semblable à une section de pare-feu dans laquelle vous définissez des règles qui déterminent la circulation du trafic.
- 3 Définissez l'option **Redirection vers** sur l'instance de service enregistrée avec NSX-T pour effectuer l'introspection du réseau du trafic circulant entre les entités source et de destination.
- 4 Pour ajouter une stratégie, cliquez sur **Publier**.
- 5 Cliquez sur l'icône de sélection verticale  d'une section et cliquez sur **Ajouter une règle**.
- 6 Modifiez le champ **Source** pour ajouter un groupe en définissant des critères d'appartenance, des membres statiques, des adresses IP/MAC ou des groupes Active Directory. Voici les types de critère d'appartenance disponibles : Machine virtuelle, Commutateur logique, Port logique, Ensemble d'adresses IP. Vous pouvez sélectionner des membres statiques dans l'une des catégories suivantes : Groupe, Segment, Port de segment, Interface réseau virtuelle ou Machine virtuelle.
- 7 Cliquez sur **Enregistrer**.
- 8 Pour ajouter un groupe de destination, modifiez le champ **Destination**.
- 9 Dans le champ Appliqué à, vous pouvez effectuer l'une des opérations suivantes :
 - Sélectionnez **DFW** pour appliquer la règle à toutes les cartes réseau virtuelles attachées au commutateur logique.

- Sélectionnez **Groupes de machines virtuelles** pour appliquer la règle sur des cartes réseau virtuelles des machines virtuelles membres du groupe. Les membres peuvent être sélectionnés dans une liste statique ou en fonction de critères dynamiques. Les objets NSX-T Data Center pris en charge sont les suivants : Machine virtuelle, Commutateur logique, Port logique, Ensemble d'adresses IP, etc.
- 10 Dans le champ Action, sélectionnez **Rediriger** pour rediriger le trafic le long de l'instance de service ou **Ne pas rediriger** pour ne pas appliquer l'inspection réseau sur le trafic.
 - 11 Cliquez sur **Publier**.
 - 12 Pour restaurer une règle publiée, sélectionnez une règle et cliquez sur **Restaurer**.
 - 13 Pour ajouter une stratégie, cliquez sur **+ Ajouter une stratégie**.
 - 14 Pour cloner une stratégie ou une règle, sélectionnez la stratégie ou une règle, et cliquez sur **Cloner**.
 - 15 Pour activer une règle, activez l'icône Activer/Désactiver ou sélectionnez la règle et, dans le menu, cliquez sur **Activer > Activer une règle**.
 - 16 Après l'activation ou la désactivation d'une règle, cliquez sur **Publier** pour l'appliquer.

Résultats

En fonction des actions définies, le trafic nord-sud est redirigé vers l'instance de service pour l'inspection réseau.

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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Services de partenaires > Instances de service**.
- 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.

Protection de point de terminaison

NSX-T Data Center vous permet d'insérer des services de partenaires tiers en tant que machine virtuelle de service distincte qui fournit des services de protection de point de terminaison. Une machine virtuelle de service de partenaires traite les événements de fichier, de processus et de registre de la machine virtuelle invitée en fonction des règles de stratégie de protection de point de terminaison appliquées par l'administrateur NSX-T Data Center.

Comprendre la protection du point de terminaison

Découvrez le cas d'utilisation, le workflow et les concepts clés de la protection du point de terminaison.

Cas d'utilisation de protection de point de terminaison

Dans un environnement virtuel, utilisez la plate-forme Guest Introspection pour fournir une protection antivirus et anti-logiciels malveillants aux machines virtuelles invitées.

En tant qu'administrateur NSX, vous implémentez une solution antivirus et anti-logiciels malveillants qui est déployée en tant que machine virtuelle de service (Service VM, ou SVM) pour surveiller une activité de fichier, de réseau ou de processus sur une machine virtuelle invitée. À chaque accès d'un fichier (par exemple, une tentative d'ouverture d'un fichier), la VM de service anti-logiciels malveillants est informée de l'événement. La machine virtuelle de service détermine ensuite comment répondre à l'événement. Par exemple, inspecter le fichier à la recherche de signatures de virus.

- Si la VM de service détermine que le fichier ne contient aucun virus, elle permet alors la réussite de l'opération d'ouverture du fichier.
- Si la machine virtuelle de service détecte un virus dans le fichier, elle demande à l'agent léger de la machine virtuelle invitée d'agir de l'une des manières suivantes :
 - Supprimer le fichier infecté ou refuser l'accès au fichier.
 - Les machines virtuelles infectées peuvent se voir attribuer une balise par NSX. Vous pouvez également définir une règle qui déplace automatiquement de telles machines virtuelles invitées balisées vers un groupe de sécurité qui met en quarantaine la machine virtuelle infectée pour une analyse supplémentaire et une isolation du réseau jusqu'à l'éradication complète de l'infection.

Avantages de l'utilisation de la plate-forme Guest Introspection pour protéger les points de terminaison de machines virtuelles invitées :

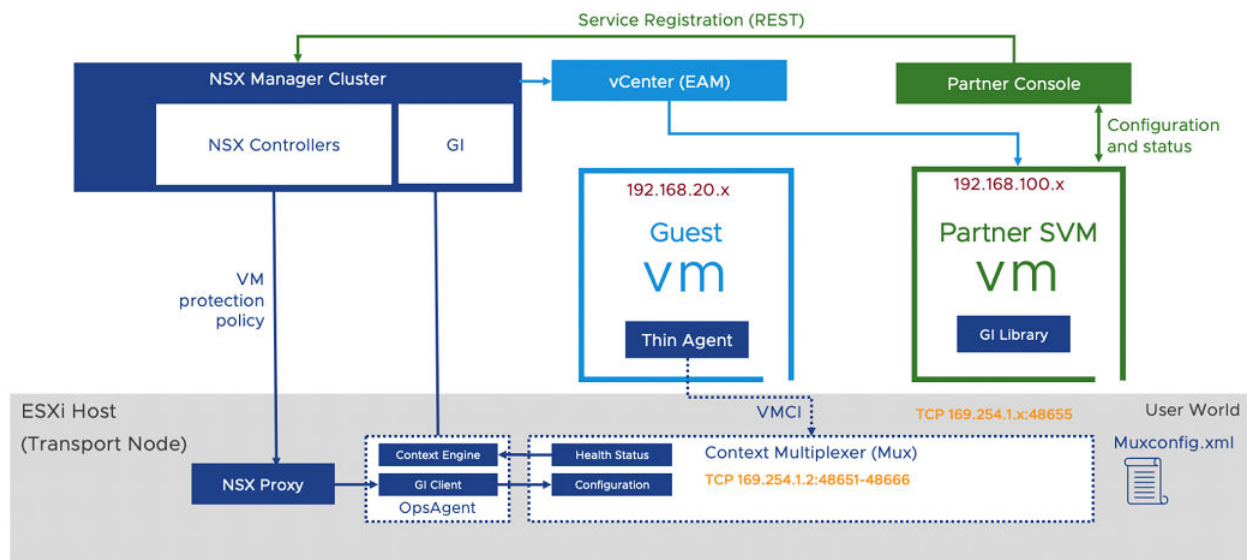
- Réduction de la consommation des ressources de calcul : Guest Introspection décharge les signatures de virus et la logique d'analyse de sécurité de chaque point de terminaison d'un hôte vers une machine virtuelle de service de partenaires tiers de l'hôte. Puisque l'analyse antivirus se produit uniquement sur la machine virtuelle de service, il n'est pas nécessaire de consacrer des ressources de calcul sur des machines virtuelles invitées pour exécuter des analyses antivirus.

- Meilleure gestion : lorsque les analyses de virus sont téléchargées vers une machine virtuelle de service, les signatures de virus doivent être mises à jour sur un seul objet par hôte. Un tel mécanisme fonctionne mieux que la solution basée sur un agent où les mêmes signatures de virus nécessitent des mises à jour sur toutes les machines virtuelles invitées.
- Protection continue antivirus et anti-logiciels malveillants : comme la machine virtuelle de service s'exécute en continu, une machine virtuelle invitée n'est pas mandatée pour exécuter les dernières signatures de virus. Par exemple, une machine virtuelle de snapshot peut exécuter une ancienne version de la signature de virus, ce qui la rend vulnérable dans le mode de protection traditionnel des points de terminaison. Avec la plate-forme Guest Introspection, la machine virtuelle de service exécute en continu les dernières signatures de virus et de logiciels malveillants, ce qui garantit également que toutes les machines virtuelles récemment ajoutées sont protégées par les dernières signatures de virus.
- Signatures de virus téléchargées vers une machine virtuelle de service : le cycle de vie de la base de données antivirus étant en dehors du cycle de vie de la machine virtuelle invitée, la machine virtuelle de service n'est donc pas affectée par les interruptions de machine virtuelle invitée.

Architecture de Guest Introspection

Comprendre l'architecture des composants d'insertion de services et de Guest Introspection dans NSX-T Data Center.

Figure 10-1. Architecture de Guest Introspection



Concepts clés :

- Console de partenaire : il s'agit de l'application Web fournie par le fournisseur de sécurité pour exploiter la plate-forme Guest Introspection.

- **NSX Manager** : il s'agit du dispositif de plan de gestion pour NSX qui fournit une API et une interface utilisateur graphique aux clients et aux partenaires pour la configuration des stratégies de sécurité et de réseau. Pour Guest Introspection, NSX Manager fournit également une API et une interface utilisateur graphique pour déployer et gérer des dispositifs de partenaires.
- **SDK Guest Introspection** : il s'agit de la bibliothèque fournie par VMware qui est utilisée par le fournisseur de sécurité.
- **VM de service** : il s'agit de la machine virtuelle fournie par le fournisseur de sécurité qui consomme le SDK Introspection fourni par VMware. Cette machine virtuelle contient la logique d'analyse des événements de fichier ou de processus permettant de détecter les virus ou les programmes malveillants sur l'invité. Après l'analyse d'une demande, elle renvoie un verdict ou une notification concernant l'action effectuée par la machine virtuelle invitée sur la demande.
- **Agent hôte Guest Introspection (multiplexeur de contexte)** : cet agent traite la configuration des stratégies de protection de point de terminaison. Il multiplexe et transfère également les messages des machines virtuelles protégées vers la machine virtuelle de service. Il signale l'état de santé de la plate-forme Guest Introspection et conserve les enregistrements de la configuration de la machine virtuelle de service dans le fichier `muxconfig.xml`.
- **Agent Ops (moteur de contexte et client Guest Introspection)** : cet agent transfère la configuration Guest Introspection vers l'agent hôte Guest Introspection (multiplexeur de contexte). Il relaie également l'état de santé de la solution à NSX Manager.
- **EAM** : NSX Manager utilise le gestionnaire d'agent ESXi pour déployer une machine virtuelle de service de partenaires sur chaque hôte du cluster configuré pour la protection.
- **Agent léger** : il s'agit de l'agent d'introspection de fichiers ou d'introspection réseau qui est en cours d'exécution dans les machines virtuelles invitées. Il intercepte également les activités de fichier et de réseau qui sont transférées vers la machine virtuelle de service via l'agent hôte. Cet agent fait partie de VMware Tools. Il remplace l'agent traditionnel fourni par les fournisseurs de sécurité antivirus ou anti-programme malveillant. Il s'agit d'un agent générique et léger qui facilite le déchargement des fichiers et des processus pour l'analyse de la machine virtuelle de service fournie par le fournisseur.

Concepts clés de la protection du point de terminaison

Le workflow de la protection du point de terminaison exige des partenaires l'enregistrement de leurs services auprès de NSX-T Data Center et, d'un administrateur, l'utilisation de ces services. Quelques concepts facilitent la compréhension du workflow.

- **Définition de service** : les partenaires définissent des services avec ces attributs : nom, description, formats de formulaire pris en charge, attributs de déploiement qui incluent les interfaces réseau et l'emplacement du module OVF du dispositif à utiliser par la SVM.
- **Insertion de service** : NSX fournit la structure d'insertion de service qui permet aux partenaires d'intégrer des solutions de mise en réseau et de sécurité à la plate-forme NSX. La solution Guest Introspection est une sorte d'insertion de service.

- **Profils de service et modèles fournisseur** : les partenaires enregistrent des modèles fournisseur qui mettent en avant les niveaux de protection pour les stratégies. Par exemple, les niveaux de protection peuvent être or, argent ou platine. Les profils de service peuvent être créés à partir de modèles fournisseur, ce qui permet aux administrateurs NSX de nommer les modèles fournisseur en fonction de leur préférence. Pour les services autres que ceux de Guest Introspection, les profils de service permettent une personnalisation supplémentaire à l'aide d'attributs. Les profils de service peuvent ensuite être utilisés dans les règles de stratégie de protection de point de terminaison pour configurer la protection des groupes de machines virtuelles définis dans NSX. En tant qu'administrateur, vous pouvez créer des groupes en fonction du nom de la machine virtuelle, des balises ou des identifiants. Plusieurs profils de service peuvent être créés en option à partir d'un modèle fournisseur unique.
- **Stratégie de protection de point de terminaison** : une stratégie est un ensemble de règles. Lorsque vous disposez de plusieurs stratégies, organisez-les dans l'ordre de leur exécution. Il en va de même pour les règles définies dans une stratégie. Par exemple, la stratégie A a trois règles, la stratégie B a quatre règles, et elles sont organisées dans une séquence telle que la stratégie A précède la stratégie B. Lorsque Guest Introspection commence à exécuter les stratégies, les règles de la stratégie A sont exécutées en premier avant les règles de la stratégie B.
- **Règle de protection de point de terminaison** : en tant qu'administrateur NSX, vous pouvez créer des règles qui spécifient les groupes de machines virtuelles à protéger et choisir le niveau de protection de ces groupes en spécifiant le profil de service de chaque règle.
- **Instance de service** : elle fait référence à la machine virtuelle de service sur un hôte. Les machines virtuelles de service sont traitées comme des machines virtuelles spéciales par vCenter. Elles sont démarrées avant la mise sous tension des machines virtuelles invitées et arrêtées après la mise hors tension de toutes les machines virtuelles invitées. Il existe une instance de service par service par hôte.

Important Le nombre d'instances de service est égal au nombre d'hôtes sur lesquels le service exécute l'hôte. Par exemple, si vous avez huit hôtes dans un cluster et que le service de partenaires a été déployé sur deux clusters, le nombre total d'instances de service en cours d'exécution est de 16 SVM.

- **Déploiement de service** : en tant qu'admin, vous déployez des machines virtuelles de service de partenaires via NSX-T par cluster. Les déploiements sont gérés au niveau du cluster, de sorte que lorsqu'un hôte est ajouté au cluster, EAM déploie automatiquement la machine virtuelle de service sur celui-ci.

Le déploiement automatique de la SVM est important, car si le service DRS est configuré sur un cluster vCenter, vCenter peut rééquilibrer ou distribuer des machines virtuelles existantes à n'importe quel nouvel hôte qui a été ajouté au cluster après le déploiement et le démarrage de la SVM sur le nouvel hôte. Comme les machines virtuelles du service de partenaires ont besoin d'une plate-forme NSX-T pour fournir la sécurité aux machines virtuelles invitées, l'hôte doit être préparé en tant que nœud de transport.

Important Un déploiement de service fait référence à un cluster sur vCenter Server qui est géré pour le déploiement et la configuration d'un service de partenaires.

- Pilote d'introspection de fichiers : il est installé sur la machine virtuelle invitée et intercepte l'activité de fichier sur la machine virtuelle invitée.
- Pilote d'introspection réseau : il est installé sur la machine virtuelle invitée et intercepte le trafic réseau, l'activité de processus et l'activité de l'utilisateur sur la machine virtuelle invitée.

Tâches de haut niveau de la protection de point de terminaison

Les services de partenaires tiers contenant une logique d'analyse de sécurité sont enregistrés avec NSX-T Data Center pour assurer la protection des machines virtuelles invitées. Le service de partenaires est appliqué lorsque l'administrateur NSX déploie les services enregistrés et applique des stratégies de protection de point de terminaison aux groupes de machines virtuelles invitées.

Le workflow Guest Introspection du cas d'utilisation de protection de point de terminaison est le suivant :

Figure 10-2. Workflow de protection de point de terminaison

Tâches du workflow	Rôle/persona	Mise en œuvre
Enregistrer un service auprès de NSX-T Data Center.	Administrateur partenaire	Console de partenaire
Enregistrer un service auprès de NSX-T Data Center	Administrateur partenaire	Console de partenaire
Enregistrer un service auprès de NSX-T Data Center	Administrateur partenaire	Console de partenaire
Déployer un service	Administrateur NSX	API et interface utilisateur NSX Manager
Afficher les détails de l'instance de service	Administrateur NSX	API et interface utilisateur NSX Manager
Afficher l'instance de service	Administrateur NSX	API et interface utilisateur NSX Manager
Ajouter un profil de service	Administrateur NSX	API et interface utilisateur NSX Manager
Utiliser la stratégie de Guest Introspection	Administrateur NSX	API et interface utilisateur NSX Manager

Tâches du workflow	Rôle/persona	Mise en œuvre
Ajouter et publier des règles de protection de point de terminaison	Administrateur NSX	API et interface utilisateur NSX Manager
Surveiller l'état de la protection de point de terminaison	Administrateur NSX	API et interface utilisateur NSX Manager

Configurer la protection du point de terminaison

Protégez les machines virtuelles invitées s'exécutant dans un environnement NSX-T Data Center à l'aide de services de sécurité partenaires tiers.

Les étapes de haut niveau permettant de configurer des stratégies de protection de point de terminaison sont les suivantes :

- 1 Assurez-vous que les [Conditions préalables à la configuration de la protection de point de terminaison](#) sont remplies avant de configurer la protection de point de terminaison sur les machines virtuelles invitées.
- 2 Logiciels pris en charge. Reportez-vous à la section [Logiciels pris en charge](#).
- 3 Installez le pilote d'introspection de fichiers pour les machines virtuelles Linux. Reportez-vous à la section [Installer l'agent léger Guest Introspection sur les machines virtuelles Linux](#).
- 4 Installez le pilote d'introspection de fichiers pour les machines virtuelles Windows. Reportez-vous à la section [Installer l'agent léger Guest Introspection sur les machines virtuelles Linux](#).
- 5 Installez le pilote d'introspection réseau pour les machines virtuelles Linux. Reportez-vous à la section [Installer l'agent léger Linux pour l'introspection du réseau](#).
- 6 Créez un utilisateur disposant du rôle Administrateur partenaire Guest Introspection. Reportez-vous à la section [Créer un utilisateur disposant du rôle Administrateur partenaire Guest Introspection](#).
- 7 Enregistrez le service de partenaires auprès de NSX-T Data Center Consultez la documentation du partenaire.
- 8 Déployez un service. Reportez-vous à la section [Déployer un service](#).
- 9 Utilisez la stratégie de Guest Introspection. Reportez-vous à la section [Utiliser la stratégie de Guest Introspection](#).
- 10 Ajoutez et publiez des règles de protection de point de terminaison. Reportez-vous à la section [Ajouter et publier des règles de protection de point de terminaison](#).
- 11 Surveillez les règles de protection de point de terminaison. Reportez-vous à la section [Surveiller l'état de la protection de point de terminaison](#).

Conditions préalables à la configuration de la protection de point de terminaison

Avant de configurer la protection de point de terminaison pour les machines virtuelles invitées, assurez-vous que les conditions préalables sont remplies.

Conditions préalables

- NSX Manager est installé sur tous les hôtes.
- Préparez et configurez le cluster NSX-T Data Center en tant que nœuds de transport en appliquant des profils de nœud de transport. Une fois l'hôte configuré en tant que nœud de transport, les composants de Guest Introspection sont installés. Reportez-vous au *Guide d'installation de NSX-T Data Center*.
- La console de partenaire est installée et configurée pour enregistrer les services auprès de NSX-T Data Center.
- Assurez-vous que les machines virtuelles invitées exécutent le fichier de configuration de matériel VM de version 9 ou supérieure.
- Configurez VMware Tools et installez des agents légers.
 - Reportez-vous à la section [Installer l'agent léger Guest Introspection sur les machines virtuelles Linux](#).
 - Reportez-vous à la section [Installer l'agent léger Guest Introspection sur les machines virtuelles Windows](#).
 - Reportez-vous à la section [Installer l'agent léger Linux pour l'introspection du réseau](#).

Installer l'agent léger Guest Introspection sur les machines virtuelles Linux

L'introspection d'invités prend en charge l'introspection de fichiers sous Linux uniquement pour l'antivirus. Pour protéger les machines virtuelles Linux à l'aide d'une solution de sécurité Guest Introspection, vous devez installer l'agent léger Guest Introspection.

L'agent léger Linux est disponible dans le cadre des modules OSP (propres au système d'exploitation). Les modules sont hébergés sur le portail des modules VMware. L'administrateur entreprise ou sécurité (administrateur non NSX) peut installer l'agent sur des machines virtuelles invitées en dehors de NSX.

L'installation de VMware Tools n'est pas nécessaire.

En fonction de votre système d'exploitation Linux, effectuez les étapes suivantes avec les privilèges racine :

Conditions préalables

- Assurez-vous qu'une version de Linux prise en charge est installée sur la machine virtuelle invitée.
 - Red Hat Enterprise Linux (RHEL) 7.4 (64 bits) GA
 - SUSE Linux Enterprise Server (SLES) 12 (64 bits) GA
 - Ubuntu 16.04.5 LTS (64 bits) GA
 - CentOS 7.4 GA
- Vérifiez que Glib 2.0 est installé sur la machine virtuelle Linux.

Procédure**1 Pour les systèmes Ubuntu**

- a Procurez-vous les clés publiques des modules VMware et importez-les à l'aide des commandes suivantes.

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
apt-key add VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b Créez un fichier nommé `vmware.list` sous `/etc/apt/sources.list.d`

- c Modifiez le fichier comme suit :

```
deb [arch=amd64] https://packages.vmware.com/packages/nsx-gi/latest/ubuntu/ xenial main
```

- d Installez le module.

```
apt-get update
apt-get install vmware-nsx-gi-file
```

2 Pour les systèmes RHEL7

- a Procurez-vous les clés publiques des modules VMware et importez-les à l'aide des commandes suivantes.

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b Créez un fichier nommé `vmware.repo` sous `/etc/yum.repos.d`.

- c Modifiez le fichier comme suit :

```
[vmware]
name = VMware
baseurl = https://packages.vmware.com/packages/nsx-gi/latest/rhel7/x86_64
enabled = 1
gpgcheck = 1
metadata_expire = 86400
ui_repoid_vars = basearch
```

3 Installez le module.

```
yum install vmware-nsx-gi-file
```

4 Pour les systèmes SLES

- a Procurez-vous les clés publiques des modules VMware et importez-les à l'aide des commandes suivantes.

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b Ajoutez le référentiel suivant :

```
zypper ar -f "https://packages.vmware.com/packages/nsx-gi/latest/sle12/x86_64/" VMware
```

- c Installez le module.

```
zypper install vmware-nsx-gi-file
```

5 Pour les systèmes CentOS

- a Procurez-vous les clés publiques des modules VMware et importez-les à l'aide des commandes suivantes.

```
curl -O https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
rpm --import VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

- b Créez un fichier nommé `vmware.repo` sous `/etc/yum.repos.d`.

- c Modifiez le fichier comme suit :

```
[vmware]
name = VMware
baseurl = https://packages.vmware.com/packages/nsx-gi/latest/centos7/x86_64
enabled = 1
gpgcheck = 1
metadata_expire = 86400
ui_repoid_vars = basearch
```

Étape suivante

Vérifiez si l'agent léger s'exécute en utilisant la commande de service `vsepd status` avec les privilèges d'administration. L'état doit indiquer en cours d'exécution.

Installer l'agent léger Linux pour l'introspection du réseau

Installez l'agent léger Linux pour l'introspection du trafic réseau.

Important Pour protéger les machines virtuelles invitées contre les antivirus, il n'est pas nécessaire d'installer l'agent léger Linux pour l'introspection réseau.

Le pilote de l'agent léger Linux qui est utilisé pour l'introspection du trafic réseau dépend d'un pilote open source.

Conditions préalables

Installez les modules suivants :

- glib2
- libnetfilter-contrack3/ libnetfilter-contrack
- libnetfilter-queue1/ libnetfilter-queue
- iptables

Procédure

1 Pour installer le pilote open source fourni par Guest Introspection.

a Ajoutez l'URL suivante en tant qu'URL de base pour votre système d'exploitation.

```
deb [arch=amd64] https://packages.vmware.com/guest-introspection-for-vmware-nsx/latest/
```

b Importez la clé de packaging VMware.

```
https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

c Mettez à jour le référentiel et installez le pilote open source.

```
apt-get install Guest-Introspection-for-VMware-NSX
```

2 Pour installer l'agent léger Linux utilisé pour l'introspection de fichier et/ou l'introspection du trafic réseau :

- Pour installer les modules d'introspection de fichiers et d'introspection réseau, sélectionnez le module `vmware-nsx-gi` à l'étape c.
- Pour installer les modules d'introspection réseau, sélectionnez le module `vmware-nsx-gi-net` à l'étape c.

a Ajoutez l'URL suivante en tant qu'URL de base pour votre système d'exploitation.

```
deb [arch=amd64] https://packages.vmware.com/packages/nsx-gi/latest
```

b Importez la clé de packaging VMware.

```
https://packages.vmware.com/packages/nsx-gi/keys/VMWARE-PACKAGING-NSX-GI-GPG-RSA-KEY.pub
```

c Installez l'un des pilotes.

```
vmware-nsx-gi
vmware-nsx-gi-net
```

Installer l'agent léger Guest Introspection sur les machines virtuelles Windows

Pour protéger les machines virtuelles à l'aide d'une solution de sécurité Guest Introspection, vous devez installer sur ces machines l'agent léger Guest Introspection, également appelé Pilotes Guest Introspection. Les pilotes Guest Introspection sont inclus dans VMware Tools for Windows, mais ne font pas partie de l'installation par défaut. Pour installer Guest Introspection sur une machine virtuelle Windows, vous devez effectuer une installation personnalisée et sélectionner les pilotes.

Les machines virtuelles Windows sur lesquelles les pilotes Guest Introspection sont installés sont protégées automatiquement à chaque démarrage sur un hôte ESXi hébergeant la solution de sécurité. Les machines virtuelles protégées conservent la protection de la sécurité lors des arrêts et redémarrages, et même après un déplacement par vMotion sur un autre hôte ESXi hébergeant la solution de sécurité.

- Si vous utilisez vSphere 6.0, reportez-vous à ces instructions. Pour installer VMware Tools, reportez-vous à la section [Installer ou mettre à niveau manuellement VMware Tools sur une machine virtuelle Windows](#).
- Si vous utilisez vSphere 6.5, reportez-vous à ces instructions pour installer VMware Tools : <https://www.vmware.com/support/pubs/vmware-tools-pubs.html>.

Conditions préalables

Assurez-vous qu'une version de Windows prise en charge est installée sur la machine virtuelle invitée. NSX Guest Introspection est compatible avec les systèmes d'exploitation Windows suivants :

- Windows XP SP3 et versions ultérieures (32 bits)
- Windows Vista (32 bits)
- Windows 7 (32/64 bits)
- Windows 8 (32/64 bits)
- Windows 8.1 (32/64) (vSphere 6.0 et versions ultérieures)
- Windows 10
- Windows 2003 SP2 et versions ultérieures (32/64 bits)
- Windows 2003 R2 (32/64 bits)
- Windows 2008 (32/64 bits)
- Windows 2008 R2 (64 bits)
- Win2012 (64)
- Win2012 R2 (64) (vSphere 6.0 et versions ultérieures)
- Windows Server 2016
- Windows Server 2019

Procédure

- 1 Démarrez l'installation de VMware Tools en suivant les instructions de votre version de vSphere. Sélectionnez **Installation personnalisée**.

- 2 Développez la section Pilote VMCI.

Les options disponibles varient selon la version de VMware Tools.

- 3 Sélectionnez le pilote à installer sur la machine virtuelle.

Pilote	Description
Pilote vShield Endpoint	Installe les pilotes d'introspection de fichiers (<code>vsepflt</code>) et d'introspection réseau (<code>vnetflt</code>).
Pilotes Guest Introspection	Installe les pilotes d'introspection de fichiers (<code>vsepflt</code>) et d'introspection réseau (<code>vnetflt</code>).
Pilote NSX File Introspection et pilote NSX Network Introspection	Sélectionnez le pilote NSX File Introspection pour installer <code>vsepflt</code> . (Facultatif) Sélectionnez le pilote d'introspection réseau NSX pour installer <code>vnetflt</code> (<code>vnetWFP</code> sous Windows 10 ou version ultérieure).
Note Sélectionnez le pilote d'introspection réseau NSX uniquement si vous utilisez les fonctionnalités Identity Firewall ou Surveillance des points de terminaison.	

- 4 Dans le menu déroulant en regard des pilotes que vous voulez ajouter, sélectionnez Cette fonctionnalité est installée sur le disque dur local.
- 5 Suivez les autres étapes de la procédure.

Étape suivante

Vérifiez si l'agent léger s'exécute en utilisant la commande `fltmc` avec les privilèges d'administration. La colonne Nom du filtre dans la sortie indique l'agent léger avec une entrée `vsepflt`.

Logiciels pris en charge

Guest Introspection est interopérable avec des versions spécifiques du logiciel.

VMware Tools

VMware Tools 10.3.10 est pris en charge.

Vérifiez l'interopérabilité entre VMware Tools et NSX-T. Consultez les [Matrices d'interopérabilité des produits VMware](#)

Système d'exploitation pris en charge

- Windows 7
- Windows 8/8.1
- Windows 10
- Serveur Windows 2008 R2

- Serveur Windows 2012 R2
- Serveur Windows 2016
- CentOS 7.4 GA
- RHEL 7.4 GA
- Ubuntu 16.04.5 LTS (64 bits)
- SLES 12 GA

Hôtes pris en charge

Pour connaître les hôtes ESXi pris en charge, consultez les [Matrices d'interopérabilité des produits VMware](#).

Créer un utilisateur disposant du rôle Administrateur partenaire Guest Introspection

Attribuez à un utilisateur le rôle Administrateur partenaire Guest Introspection disponible dans NSX-T Data Center.

Remarque : il est recommandé d'enregistrer les services de partenaires par un utilisateur qui est associé au rôle Administrateur partenaire Guest Introspection afin d'éviter tout problème de sécurité.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Système** → **Utilisateur** → **Attributions de rôles**.
- 3 Cliquez sur **Ajouter**.
- 4 Sélectionnez l'utilisateur et attribuez-lui le rôle **Administrateur partenaire GI**.

Étape suivante

Enregistrez les services auprès de NSX-T Data Center. Reportez-vous à la section [Enregistrer un service auprès de NSX-T Data Center](#).

Enregistrer un service auprès de NSX-T Data Center

Enregistrez les services de sécurité tiers auprès de NSX-T Data Center.

Conditions préalables

- Assurez-vous que les conditions préalables sont remplies. Reportez-vous à la section [Conditions préalables à la configuration de la protection de point de terminaison](#).
- Assurez-vous qu'un utilisateur vIDM bénéficie du rôle Administrateur partenaire GI. Ce rôle est utilisé pour enregistrer les services avec NSX-T Data Center.

Procédure

- 1 Connectez-vous avec les privilèges Administrateur partenaire GI à la console de partenaire.
- 2 Enregistrez un service, un modèle de fournisseur et configurez la solution de partenaire auprès de NSX-T Data Center. Consultez la documentation du partenaire.

Étape suivante

Afficher le catalogue des services de partenaires. Reportez-vous à la section [Afficher le catalogue des services de partenaires](#).

Afficher le catalogue des services de partenaires

La page du catalogue affiche tous les partenaires, ainsi que leurs services enregistrés auprès de NSX-T Data Center.

Conditions préalables

- Les partenaires enregistrent des services auprès de NSX-T Data Center.
- Les services sont déployés sur un cluster.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Système > Déploiements de service > Catalogue**.
- 3 Cliquez sur **Afficher** sur un service. La page Déploiement affiche les détails concernant le service, comme l'état du déploiement, les détails du réseau, les détails du cluster, etc.

Étape suivante

Mettez à niveau une machine virtuelle de service de partenaires.

Déployer un 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.

Déployez les machines virtuelles de service de partenaires qui exécutent le moteur de sécurité partenaire sur tous les hôtes NSX-T Data Center d'un cluster. Le service d'ESX Agent Manager (EAM) de vSphere est utilisé pour déployer les machines virtuelles de service de partenaires sur chaque hôte. Après avoir déployé les SVM, vous pouvez créer des règles de stratégie utilisées par les SVM pour protéger les machines virtuelles invitées.

Conditions préalables

- Tous les hôtes sont gérés par un vCenter Server.
- Les services de partenaires sont enregistrés auprès de NSX-T Data Center et sont prêts pour le déploiement.

- Les administrateurs de NSX-T Data Center peuvent accéder aux services de partenaires et aux modèles fournisseur.
- La machine virtuelle de service et le Service Manager partenaire (console) doivent être en mesure de communiquer entre eux au niveau du réseau de gestion.
- Préparez des hôtes en guise de nœuds de transport NSX-T Data Center :
 - Créez une zone de transport.
 - Créez un pool d'adresses IP pour les adresses IP des points de terminaison de tunnel.
 - Créez un profil de liaison montante.
 - Ajoutez un profil de nœud de transport pour préparer un cluster pour le déploiement automatique de nœuds de transport NSX-T Data Center.
 - Configurez un hôte autonome ou géré.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Accédez à l'onglet **Système** et cliquez sur **Déploiement de service**.
- 3 Dans le menu déroulant Service de partenaires, sélectionnez le service à déployer.
- 4 Cliquez sur **Déploiement**, puis sur **Déployer le service**.
- 5 Entrez le nom du déploiement de service.
- 6 Dans le champ Gestionnaire de calcul, sélectionnez la ressource de calcul sur vCenter Server pour déployer le service.
- 7 Dans le champ Cluster, sélectionnez le cluster dans lequel les services doivent être déployés.
- 8 Dans le menu déroulant Banque de données, vous pouvez :
 - a Sélectionner une banque de données comme référentiel de la machine virtuelle de service.
 - b Sélectionnez **Spécifié sur l'hôte**. Ce paramètre signifie que vous n'avez pas besoin de sélectionner un groupe de banques de données et de ports sur cet assistant. Vous pouvez directement configurer les paramètres de l'agent sur EAM dans vCenter Server de manière à ce qu'ils pointent vers un groupe de ports et de banques de données spécifiques à utiliser pour le déploiement du service.

Pour savoir comment configurer EAM, reportez-vous à la documentation de vSphere.
- 9 Dans la colonne Réseau, cliquez sur **Définir**.
- 10 Définissez l'interface du réseau de gestion sur **Spécifié sur l'hôte** ou **DVPG**.
- 11 Définissez le type de réseau sur DHCP ou Pool d'adresses IP statiques. Si vous définissez le type de réseau sur Pool d'adresses IP statiques, effectuez une sélection dans la liste des pools d'adresses IP disponibles.

- 12 Dans le champ Spécification de déploiement, sélectionnez Déploiement basé sur l'hôte pour déployer le service sur tous les hôtes. Selon les services enregistrés par le partenaire, plusieurs services peuvent être déployés dans le cadre d'une machine virtuelle de service unique.
- 13 Dans le champ Modèle de déploiement, sélectionnez le modèle de déploiement enregistré.
- 14 Cliquez sur **Enregistrer**.

Résultats

Lorsqu'un nouvel hôte est ajouté au cluster, EAM déploie automatiquement la machine virtuelle de service sur le nouvel hôte. 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 de NSX Manager. Le service est correctement déployé sur l'hôte lors de l'activation de l'état `Déploiement réussi`.

Pour supprimer un hôte d'un cluster, placez-le d'abord en mode de maintenance. Ensuite, sélectionnez l'option pour migrer les machines virtuelles invitées vers un autre hôte afin de terminer la migration.

Étape suivante

Vous devez connaître les détails du déploiement et l'état de santé des instances de service déployées sur les hôtes. Reportez-vous à la section [Afficher les détails de l'instance de service](#).

Afficher les détails de l'instance de service

Vous devez connaître les détails du déploiement et l'état de santé de l'instance de service déployée sur les hôtes membres d'un cluster.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Système > Déploiements de service > Instances de service**.
- 3 Dans le menu déroulant Service de partenaires, sélectionnez le service de partenaires pour afficher les détails relatifs aux instances de service.

Tableau 10-9.

Champ	Description
Nom de l'instance de service	ID unique identifiant l'instance de service sur un hôte particulier
Nom du déploiement de service	Nom que vous avez entré lors du déploiement du service.
Déployé sur	Adresse IP ou nom de domaine complet de l'hôte
Mode de déploiement	Autonome ou cluster

Tableau 10-9. (suite)

Champ	Description
État du déploiement	État actif pour identifier un déploiement réussi
État de santé	<p>Lorsque l'instance de service est déployée, l'état de santé est <code>Prêt</code>. Pour faire passer l'état de santé de <code>Prêt</code> à <code>Actif</code>, effectuez les modifications de configuration requises. Reportez-vous à la section Afficher l'instance de service.</p> <p>Une fois les paramètres suivants correctement réalisés par NSX-T Data Center, l'état de santé passe de <code>Prêt</code> à <code>Actif</code>.</p> <ul style="list-style-type: none"> ■ État de la solution : actif ■ Connectivité entre l'agent Guest Introspection de NSX-T Data Center et l'agent Ops de NSX-T Data Center : actif ■ État de santé reçu à : <Day, Date, Time>

Étape suivante

Afficher l'instance de service. Reportez-vous à la section [Afficher l'instance de service](#).

Afficher l'instance de service

Après le déploiement de l'instance de service, certains paramètres doivent être réalisés dans NSX-T Data Center pour que l'état de santé soit actif.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Système > Déploiements de service > Instances de service**.
- 3 Dans le menu déroulant Service de partenaires, sélectionnez le service de partenaires pour afficher les détails relatifs aux instances de service.
- 4 La colonne État de santé affiche l'état de l'instance de service comme étant `Prêt`. Cet état indique que l'instance de service est prête à être configurée avec des règles de stratégie de protection de point de terminaison pour protéger les machines virtuelles.
- 5 Les paramètres suivants doivent être réalisés dans NSX-T Data Center pour que l'état de santé passe à `Actif`.
 - Les machines virtuelles invitées doivent être disponibles sur l'hôte.
 - Les machines virtuelles invitées doivent être sous tension.
 - Les règles de protection de point de terminaison doivent être appliquées aux machines virtuelles invitées.

- Les machines virtuelles invitées doivent être configurées avec la version prise en charge de VMTools et des pilotes d'introspection de fichiers.

Étape suivante

Ajoutez un profil de service. Reportez-vous à la section [Ajouter un profil de service](#).

Ajouter un profil de service

Des stratégies Guest Introspection peuvent être mises en œuvre uniquement lorsqu'un profil de service est disponible dans NSX-T Data Center. Les profils de service sont créés à partir d'un modèle fourni par le partenaire. Les profils de service constituent un moyen, pour l'administrateur, de choisir le niveau de protection (stratégie or, argent, platine) d'une machine virtuelle. Il lui suffit, pour cela, de sélectionner les modèles proposés par le fournisseur.

Par exemple, un fournisseur peut proposer des niveaux de stratégie or, platine et argent. Chaque profil créé peut servir à un autre type de charge de travail. Un profil de service or fournit un logiciel anti-programme malveillant complet pour une charge de travail de type PCI, tandis qu'un profil de service argent fournit uniquement une protection de base contre les logiciels malveillants pour une charge de travail normale.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Sécurité > Protection de point de terminaison > Règles de protection de point de terminaison > Profils de service**.
- 3 Dans le champ Service de partenaires, sélectionnez le service pour lequel vous souhaitez créer un profil de service.
- 4 Cliquez sur **Ajouter un profil de service**.
- 5 Entrez le nom du profil de service et sélectionnez le modèle de fournisseur. Vous pouvez éventuellement ajouter des balises et une description.
- 6 Cliquez sur **Enregistrer**.

L'ID du modèle fournisseur utilisé pour créer le profil de service est transmis à la console de partenaire. Les partenaires enregistrent l'ID du modèle fournisseur pour suivre l'utilisation des machines virtuelles invitées protégées par ce modèle.

Résultats

Après avoir créé un profil de service, un administrateur NSX crée des règles pour associer un profil de service à un groupe de machines virtuelles avant la publication de la règle de stratégie.

Étape suivante

Appliquez la stratégie de protection du point de terminaison sur des groupes de machines virtuelles invitées qui doivent être protégées contre les logiciels malveillants. Reportez-vous à la section [Utiliser la stratégie de Guest Introspection](#).

Utiliser la stratégie de Guest Introspection

Pour appliquer une stratégie sur des groupes de machines virtuelles, il suffit de créer des règles qui associent des profils de service à des groupes de machines virtuelles. La protection commence immédiatement après application des règles sur un groupe de machines virtuelles.

La stratégie de protection du point de terminaison est un service de protection proposé par des partenaires pour protéger les machines virtuelles invitées contre les logiciels malveillants en mettant en œuvre des profils de service sur des machines virtuelles invitées. Avec une règle appliquée sur un groupe de machines virtuelles, toutes les machines virtuelles invitées au sein de ce groupe sont protégées par ce profil de service. Lorsqu'un événement d'accès aux fichiers survient sur une machine virtuelle invitée, l'agent léger GI (en cours d'exécution sur chaque machine virtuelle invitée) collecte le contexte du fichier (attributs de fichier, handle de fichier et autres détails de contexte) et signale l'événement à la SVM. Si la SVM souhaite analyser le contenu du fichier, elle demande plus d'informations en utilisant la bibliothèque de l'API EPSec. Dès réception d'un verdict net de la SVM, l'agent léger GI autorise l'utilisateur à accéder au fichier. Si la SVM signale que le fichier est infecté, l'agent léger GI refuse à l'utilisateur l'accès au fichier.

Pour exécuter un service de sécurité sur un groupe de machines virtuelles, vous devez :

Procédure

- 1 Définir une stratégie et des règles.
- 2 Définir des critères d'appartenance pour constituer le groupe de machines virtuelles.
- 3 Définir des règles pour les groupes de machines virtuelles.
- 4 Publier la règle.

Ajouter et publier des règles de protection de point de terminaison

La publication de règles de stratégie sur des groupes de machines virtuelles consiste à associer des groupes de machines virtuelles devant être protégées à un profil de service spécifique.

Procédure

- 1 Dans la section de stratégie, sélectionnez une stratégie.
- 2 Cliquez sur **Ajouter** -> **Ajouter une règle**.
- 3 Dans le champ Nouvelle règle, entrez le nom de la règle.
- 4 Dans le champ Sélectionner des groupes, cliquez sur l'icône Modifier.
- 5 Dans la fenêtre Définir les groupes, effectuez une sélection dans la liste de groupes existante ou ajoutez un nouveau groupe.
 - a Pour ajouter un nouveau groupe, cliquez sur **Ajouter un groupe**, entrez les détails et cliquez sur **Enregistrer**.
Reportez-vous à la section [Ajouter un groupe](#).
- 6 Dans la colonne Groupe, sélectionnez le groupe de machines virtuelles.

- 7 Dans la colonne Profils de service, sélectionnez le profil de service qui fournit le niveau de protection souhaité pour les machines virtuelles invitées du groupe.
 - a Pour ajouter un nouveau profil de service, cliquez sur **Ajouter un profil de service**, entrez les détails et cliquez sur **Enregistrer**.

Reportez-vous à la section [Ajouter un profil de service](#).

- 8 Cliquez sur **Publier**.

Résultats

Les stratégies de protection du point de terminaison protègent des groupes de machines virtuelles.

Étape suivante

Vous souhaitez peut-être modifier l'ordre des règles en fonction du type de protection requis pour différents groupes de machines virtuelles. Reportez-vous à la rubrique [Exécution de la stratégie de protection du point de terminaison par Guest Introspection](#)

Surveiller l'état de la protection de point de terminaison

Surveillez l'état de la configuration des machines virtuelles protégées et non protégées, des problèmes liés à l'agent hôte et aux machines virtuelles de service, et des machines virtuelles configurées avec le pilote d'introspection de fichiers qui a été installé dans le cadre de l'installation de VMTtools.

Vous pouvez afficher :

- L'état du déploiement des services.
- L'état de la configuration de la protection de point de terminaison.
- L'état de la capacité défini pour la protection de point de terminaison.

Afficher l'état des déploiements de services

Affichez les détails des déploiements de services sur le tableau de bord de surveillance.

Affichez l'état de la stratégie EPP à l'échelle du système.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Accédez à **Accueil > Surveillance - Tableaux de bord**.
- 3 Dans le menu déroulant, cliquez sur **Surveillance - Système**.
- 4 Pour afficher l'état du déploiement entre les clusters du système, accédez au widget Protection de point de terminaison, puis cliquez sur le graphique en anneau pour afficher les déploiements réussis ou infructueux.

La page Déploiements de services affiche les détails de déploiement.

Afficher l'état de la configuration de la protection de point de terminaison

Affichez l'état de la configuration du service de protection de point de terminaison.

Affichez l'état de la stratégie EPP à l'échelle du système.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Accédez à **Accueil > Sécurité > Présentation de la sécurité**.
- 3 Pour afficher l'état d'EPP sur les clusters, cliquez sur le widget Sécurité.
- 4 Sur la page Présentation de la sécurité, cliquez sur **Configuration**.



- 5 Dans la section Protection de point de terminaison, consultez les informations suivantes :
 - a Le widget de distribution des VM par profil de service affiche les informations suivantes :
 - 1 Nombre de machines virtuelles protégées par le profil supérieur. Le profil supérieur représente un profil qui protège le nombre maximal de machines virtuelles sur un cluster.
 - 2 Machines virtuelles protégées par les profils de service restants classées sous Autres profils.
 - 3 Machines virtuelles non protégées classées sous Aucun profil.

La page Règles de protection de point de terminaison affiche les machines virtuelles protégées par des stratégies de protection de point de terminaison.
 - b Le widget des composants présentant des problèmes affiche les informations suivantes :
 - 1 Hôte : problèmes liés au multiplexeur de contexte.
 - 2 SVM : problèmes liés aux machines virtuelles de service. Par exemple, l'état de la SVM est inactif, la connexion de la SVM avec la machine virtuelle invitée est en panne.

La colonne État sur la page Déploiement affiche les problèmes de santé.
 - c Le widget de configuration des VM exécutant l'inspection de fichiers affiche les informations suivantes :
 - 1 Machines virtuelles protégées par le pilote d'inspection de fichiers.

- 2 Machines virtuelles dans lesquelles l'état du pilote d'introspection de fichiers est inconnu.

ESXi Agency Manager (EAM) tente de résoudre quelques problèmes liés aux erreurs d'hôtes, de SVM et de configuration. Reportez-vous à la section [Résoudre les problèmes de services de partenaires](#).

Afficher l'état de la capacité défini pour la protection de point de terminaison

Affichez l'état de la capacité du service de protection de point de terminaison.

Affichez l'état de la capacité de la stratégie EPP.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Accédez à **Accueil > Surveillance - Tableaux de bord**.
- 3 Dans le menu déroulant, cliquez sur **Surveillance - Mise en réseau et sécurité**.
- 4 Pour afficher l'état d'EPP sur les clusters, cliquez sur le widget Sécurité.
- 5 Sur la page Présentation de la sécurité, cliquez sur **Capacité** et affichez l'état de la capacité de ces paramètres.

Limite	Capacité maximale	Inventaire actuel (réalisé)	Alerte d'avertissement	Alerte critique
Règles de pare-feu distribué	100 000	2	0 %	70%
Sections de pare-feu à l'échelle du système	10 000	5	0,05 %	70%

- a **Hôtes sur lesquels la protection de point de terminaison à l'échelle du système est activée** : si le nombre d'hôtes protégés atteint le seuil limite, NSX Manager envoie une alerte d'avertissement ou une alerte critique lorsque les seuils limite correspondants sont atteints.
- b **Machines virtuelles sur lesquelles la protection de point de terminaison à l'échelle du système est activée** : si le nombre de machines virtuelles protégées atteint le seuil limite, NSX Manager envoie une alerte d'avertissement ou une alerte critique lorsque les seuils limite correspondants sont atteints.

Note Vous pouvez définir des seuils limite pour ces paramètres, afficher l'état et recevoir des alertes lorsque les paramètres atteignent le seuil limite défini.

Gérer la protection du point de terminaison

Résolvez les conflits de stratégie, les problèmes de santé avec les machines virtuelles de service et apprenez comment fonctionne la stratégie de protection du point de terminaison.

Résoudre les problèmes de services de partenaires

Sans machine virtuelle de service de partenaires fonctionnelle, les machines virtuelles invitées ne sont pas protégées contre les logiciels malveillants.

Sur chaque hôte, vérifiez que le processus ou les services suivants sont opérationnels :

- Le service ESXi Agency Manager (EAM) doit être opérationnel. L'URL suivante doit être accessible.

```
https://<vCenter_Server_IP_Address>/eam/mob
```

Vérifiez que ESXi Agency Manager est en ligne.

```
root> service-control --status vmware-eam
```

- Les groupes de ports des SVM ne doivent pas être supprimés, car ils sont requis pour garantir que SVM continue à protéger les machines virtuelles invitées.

```
https://<vCenter_Server_IP_Address>/ui
```

- Dans vCenter Server, accédez à la machine virtuelle, cliquez sur l'onglet **Réseaux** et vérifiez si **vmervice-vshield-pg** est répertorié.
- Le service du multiplexeur (MUX) de contexte est en cours d'exécution. Vérifiez que VIB `nsx-contexte-mux` est opérationnel sur l'hôte.
- L'interface de gestion sur laquelle NSX-T Data Center communique avec la console du service de partenaires doit être active.
- L'interface de contrôle permettant la communication entre le MUX et la SVM doit être active. Le groupe de ports d'association du MUX avec la SVM doit être créé. L'interface et le groupe de ports sont tous deux nécessaires au fonctionnement du service de partenaires.

Problèmes d' ESXi Agent Manager

Le tableau répertorie les problèmes d' ESXi Agent Manager qui peuvent être résolus à l'aide du bouton Résoudre de l'interface utilisateur de NSX Manager. NSX Manager en est informé et reçoit les détails de l'erreur.

Tableau 10-10. Problèmes d' ESXi Agent Manager

Problème	Catégorie	Description	Résolution
Impossible d'accéder au fichier OVF de l'agent	Machine virtuelle non déployée	Une machine virtuelle d'agent doit être déployée sur un hôte, mais elle ne peut pas être déployée, car ESXi Agent Manager ne parvient pas à accéder au module OVF pour l'agent. Cela peut se produire lorsque le serveur Web fournissant le module OVF est arrêté. Le serveur Web est souvent interne à la solution qui a créé l'agence.	Le service ESXi Agency Manager (EAM) réessaye l'opération de téléchargement du fichier OVF. Vérifiez l'état de la console de gestion de partenaire. Cliquez sur Résoudre .
Version d'hôte incompatible	Machine virtuelle non déployée	Une machine virtuelle d'agent doit être déployée sur un hôte. Cependant, en raison de problèmes de compatibilité, l'agent n'a pas été déployé sur l'hôte.	Mettez à niveau l'hôte ou la solution pour que l'agent soit compatible avec l'hôte. Vérifiez la compatibilité de la SVM. Cliquez sur Résoudre .
Ressources insuffisantes	Machine virtuelle non déployée	Une machine virtuelle d'agent doit être déployée sur un hôte. Cependant, le service ESXi Agency Manager (EAM) n'a pas déployé la machine virtuelle d'agent, car l'hôte dispose de moins de ressources de CPU ou de mémoire.	Le service ESXi Agency Manager (EAM) tente de redéploier la machine virtuelle. Assurez-vous que des ressources de CPU et de mémoire sont disponibles. Vérifiez l'hôte et libérez des ressources. Cliquez sur Résoudre .
Espace insuffisant	Machine virtuelle non déployée	Une machine virtuelle d'agent doit être déployée sur un hôte. Toutefois, la machine virtuelle d'agent n'a pas été déployée, car la banque de données d'agent de l'hôte n'a pas suffisamment d'espace libre.	Le service ESXi Agency Manager (EAM) tente de redéploier la machine virtuelle. Libérez de l'espace sur la banque de données. Cliquez sur Résoudre .
Aucun réseau de machine virtuelle pour l'agent	Machine virtuelle non déployée	Une machine virtuelle d'agent doit être déployée sur un hôte, mais l'agent ne peut pas être déployé, car le réseau d'agent n'a pas été configuré sur l'hôte.	Ajoutez l'un des réseaux répertoriés dans customAgentVmNetwork à l'hôte. Le problème est résolu automatiquement dès que la banque de données est disponible.

Tableau 10-10. Problèmes d' ESXi Agent Manager (suite)

Format OVF non valide	Machine virtuelle non déployée	Une machine virtuelle d'agent doit être provisionnée sur un hôte, mais elle a échoué, car le provisionnement du module OVF a échoué. Le provisionnement est peu susceptible d'aboutir tant que la solution qui fournit le module OVF n'est pas mise à niveau ou corrigée afin de fournir un module OVF valide pour la machine virtuelle d'agent.	Le service ESXi Agency Manager (EAM) tente de redéployer la SVM. Consultez la documentation de la solution de partenaire ou mettez à niveau la solution de partenaire pour obtenir le module OVF valide. Cliquez sur Résoudre .
Pool d'adresses IP d'agent manquant	Machine virtuelle désactivée	Une machine virtuelle d'agent doit être mise sous tension, mais elle est mise hors tension, car il n'y a aucune adresse IP définie sur le réseau de machine virtuelle de l'agent.	Définissez l'adresse IP sur le réseau de la machine virtuelle. Cliquez sur Résoudre .
Aucune banque de données de machine virtuelle pour l'agent	Machine virtuelle désactivée	Une machine virtuelle d'agent doit être déployée sur un hôte, mais l'agent ne peut pas être déployé, car la banque de données d'agent n'a pas été configurée sur l'hôte.	Ajoutez l'une des banques de données répertoriées dans customAgentVmDatastore à l'hôte. Le problème est résolu automatiquement dès que la banque de données est disponible.
Aucun réseau de machine virtuelle personnalisé pour l'agent	Aucun réseau de machine virtuelle pour l'agent	Une machine virtuelle d'agent doit être déployée sur un hôte, mais l'agent ne peut pas être déployé, car le réseau d'agent n'a pas été configuré sur l'hôte.	Ajoutez l'hôte à l'un des réseaux répertoriés dans un réseau de machine virtuelle personnalisé pour l'agent. Le problème est résolu automatiquement dès qu'un réseau de machine virtuelle personnalisé est disponible.
Aucune banque de données de machine virtuelle personnalisée pour l'agent	Aucune banque de données de machine virtuelle pour l'agent	Une machine virtuelle d'agent doit être déployée sur un hôte, mais l'agent ne peut pas être déployé, car la banque de données d'agent n'a pas été configurée sur l'hôte.	Ajoutez l'hôte à l'une des banques de données répertoriées dans une banque de données de machine virtuelle d'agent personnalisée. Le problème est résolu automatiquement.
Agence inactive	Problème d'agence	La solution qui a créé l'agence n'est plus enregistrée auprès de vCenter Server.	Enregistrez la solution auprès de vCenter Server.

Tableau 10-10. Problèmes d' ESXi Agent Manager (suite)

Commutateur DvFilter inactif	Problème d'hôte	Un commutateur dvFilter existe sur un hôte, mais aucun agent sur l'hôte ne dépend de dvFilter. Cela se produit si un hôte est déconnecté lorsque la configuration d'une agence a été modifiée.	Cliquez sur Résoudre . Le service ESXi Agency Manager (EAM) tente de connecter l'hôte avant la mise à jour de la configuration de l'agence.
Machine virtuelle d'agent inconnue	Problème d'hôte	Une machine virtuelle d'agent a été trouvée dans l'inventaire de vCenter Server qui n'appartient pas à aucune agence dans cette instance du serveur vSphere ESX Agent Manager.	Cliquez sur Résoudre . Le service ESXi Agency Manager (EAM) tente de placer la machine virtuelle dans l'inventaire auquel elle appartient.
Propriété OVF non valide	Problème de machine virtuelle	Une machine virtuelle d'agent doit être mise sous tension, mais une propriété OVF est manquante ou a une valeur non valide.	Cliquez sur Résoudre . Le service ESXi Agency Manager (EAM) tente de reconfigurer la propriété OVF appropriée.
Machine virtuelle endommagée	Problème de machine virtuelle	Une machine virtuelle d'agent est endommagée.	Cliquez sur Résoudre . Le service ESXi Agency Manager (EAM) tente de réparer la machine virtuelle.
Machine virtuelle inactive	Problème de machine virtuelle	Une machine virtuelle d'agent est présente sur un hôte, mais l'hôte ne fait plus partie de l'étendue de l'agence. Cela se produit si un hôte est déconnecté lorsque la configuration d'une agence a été modifiée.	Cliquez sur Résoudre . Le service ESXi Agency Manager (EAM) tente de connecter de nouveau l'hôte à la configuration de l'agence.
Machine virtuelle déployée	Problème de machine virtuelle	Une machine virtuelle d'agent doit être supprimée d'un hôte, mais elle ne l'a pas été. La raison particulière pour laquelle vSphere ESX Agent Manager n'a pas pu supprimer la machine virtuelle d'agent peut être que l'hôte est en mode de maintenance, hors tension ou en veille.	Cliquez sur Résoudre . Le service ESXi Agency Manager (EAM) tente de supprimer la machine virtuelle d'agent de l'hôte.
Machine virtuelle désactivée	Problème de machine virtuelle	Une machine virtuelle d'agent doit être mise sous tension, mais elle est hors tension.	Cliquez sur Résoudre . Le service ESXi Agency Manager (EAM) tente de mettre la machine virtuelle sous tension.

Tableau 10-10. Problèmes d' ESXi Agent Manager (suite)

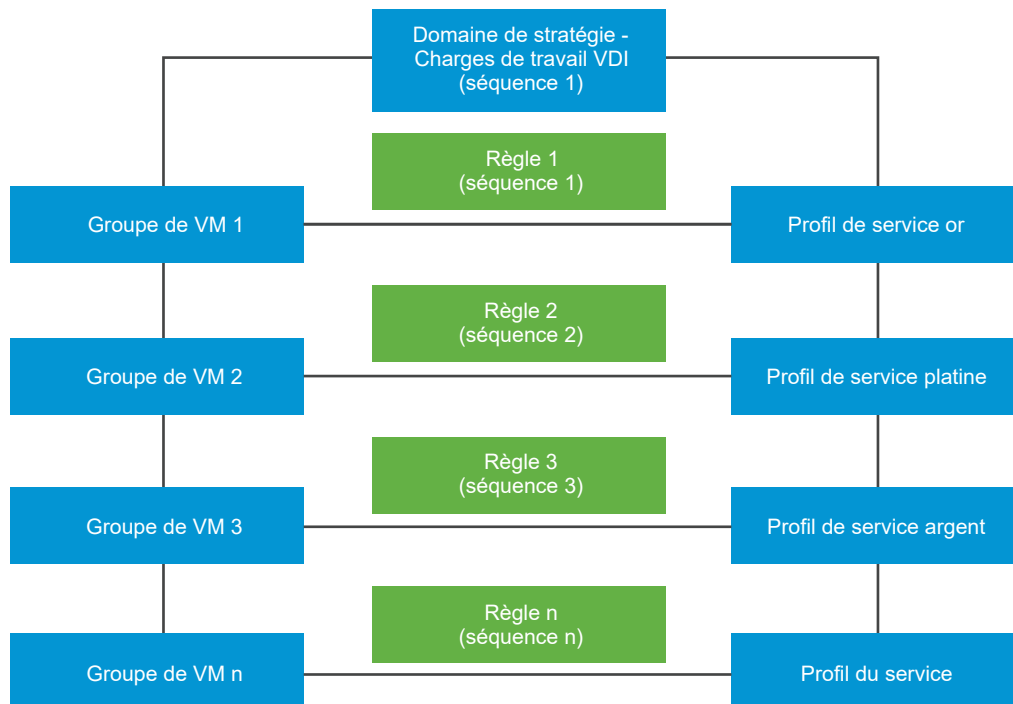
Machine virtuelle activée	Problème de machine virtuelle	Une machine virtuelle d'agent doit être mise hors tension, mais elle est hors tension.	Cliquez sur Résoudre . Le service ESXi Agency Manager (EAM) tente de mettre la machine virtuelle hors tension.
Machine virtuelle interrompue	Problème de machine virtuelle	Une machine virtuelle d'agent doit être mise sous tension, mais elle est interrompue.	Cliquez sur Résoudre . Le service ESXi Agency Manager (EAM) tente de mettre la machine virtuelle sous tension.
Dossier de machine virtuelle incorrect	Problème de machine virtuelle	Une machine virtuelle d'agent doit se trouver dans un dossier de machine virtuelle d'agent désigné, mais se trouve dans un autre dossier.	Cliquez sur Résoudre . Le service ESXi Agency Manager (EAM) tente de placer la machine virtuelle de l'agent dans le dossier désigné.
Pool de ressources de machine virtuelle incorrect	Problème de machine virtuelle	Une machine virtuelle d'agent doit se trouver dans un pool de ressources de machine virtuelle d'agent désigné, mais se trouve dans un pool de ressources différent.	Cliquez sur Résoudre . Le service ESXi Agency Manager (EAM) tente de placer la machine virtuelle d'agent dans un pool de ressources désigné.
Machine virtuelle non déployée	Problème d'agent	Une machine virtuelle d'agent doit être déployée sur un hôte, mais elle n'a pas été déployée. La raison particulière pour laquelle ESXi Agent Manager n'a pas pu déployer l'agent peut être l'impossibilité d'accéder au module OVF pour l'agent ou l'absence d'une configuration d'hôte. Ce problème peut également se produire si la machine virtuelle d'agent est supprimée explicitement de l'hôte.	Cliquez Résoudre pour déployer la machine virtuelle d'agent.

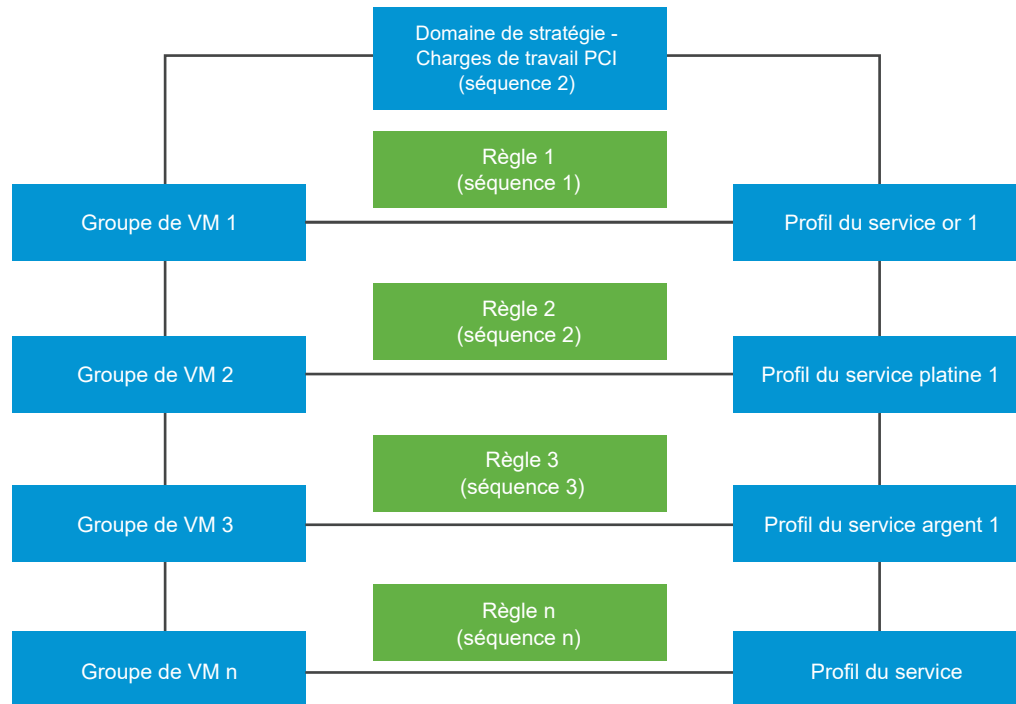
Ensuite, configurez la protection de point de terminaison pour les groupes de machines virtuelles. Reportez-vous à la section [Protection de point de terminaison](#).

Exécution de la stratégie de protection du point de terminaison par Guest Introspection

Les stratégies de protection du point de terminaison sont appliquées dans un ordre spécifique. Lorsque vous concevez des stratégies, prenez en compte le numéro de séquence associé aux règles et les domaines hébergeant les règles.

Scénario : en dehors des nombreuses charges de travail qui s'exécutent dans votre organisation, aux fins de l'illustration, nous envisageons deux types de charges de travail : des machines virtuelles exécutant Virtual Desktop Infrastructure (VDI) et des machines virtuelles exécutant des charges de travail impliquant des normes de sécurité de l'industrie des cartes de paiement (Payment Card Industry Data Security Standard, PCI DSS). Une partie des employés de l'organisation requiert l'accès à un poste de travail distant, ce qui constitue la charge de travail Virtual Desktop Infrastructure (VDI). Cette charge de travail VDI peut exiger une stratégie de protection de niveau or reposant sur des règles de conformité établies par l'organisation. La charge de travail PCI DSS requiert quant à elle le niveau de protection le plus élevé, le niveau platine.





Deux types de charge de travail existant, créez deux stratégies, une pour les charges de travail VDI et l'autre pour les charges de travail serveur. Dans chaque stratégie ou section, définissez un domaine reflétant le type de charge de travail et, dans la section, définissez des règles pour cette charge de travail. Publiez les règles pour démarrer les services GI sur les machines virtuelles invitées. GI utilise en interne les deux numéros de séquence, le numéro de séquence de la stratégie et le numéro de séquence de la règle, pour déterminer la séquence complète des règles à exécuter. Chaque règle a deux objectifs : déterminer quelles machines virtuelles protéger et la stratégie de protection qui doit être appliquée pour protéger les machines virtuelles.

Pour modifier l'ordre de la séquence, dans l'interface utilisateur du gestionnaire de stratégies NSX-T, faites glisser une règle pour en changer l'ordre. Sinon, vous pouvez attribuer explicitement un numéro de séquence pour les règles en utilisant l'API.

Vous pouvez également effectuer un appel d'API NSX-T Data Center pour définir manuellement une règle en associant un profil de service à un groupe de machines virtuelles, et déclarer le numéro de séquence des règles. L'API et les paramètres sont détaillés dans le *guide de l'API* NSX-T Data Center. Effectuez des appels d'API de configuration de service pour appliquer des profils à des entités (groupes de machines virtuelles, etc.).

Tableau 10-11. API NSX-T Data Center utilisées pour définir la règle qui applique le profil de service à des groupes de machines virtuelles

API	Détails
Obtenir tous les détails de configuration de service.	<pre>GET /api/v1/service-configs</pre> <p>L'API de configuration de service renvoie les détails du profil de service appliqué à un groupe de machines virtuelles, le groupe de machines virtuelles protégé et le numéro de séquence ou de priorité qui détermine la priorité de la règle.</p>
Créer une configuration de service.	<pre>POST /api/v1/service-configs</pre> <p>L'API de configuration de service prend les paramètres d'entrée d'un profil de service, le groupe de machines virtuelles à protéger, et le numéro de séquence ou priorité qui doit être appliqué à la règle.</p>
Supprimer une configuration de service.	<pre>DELETE /api/v1/service-configs/ <config-set-id></pre> <p>L'API de configuration de service supprime la configuration appliquée au groupe de machines virtuelles.</p>
Obtenir les détails d'une configuration spécifique.	<pre>GET /api/v1/service-configs/ <config-set-id></pre> <p>Obtenez les détails d'une configuration spécifique.</p>
Mettez à jour une configuration de service.	<pre>PUT /api/v1/service-configs/ <config-set-id></pre> <p>Mettez à jour une configuration de service.</p>
Obtenir des profils efficaces.	<pre>GET /api/v1/service-configs/ effective-profiles?resource_id=<resource-id> &resource_type=<resource-type></pre> <p>L'API de configuration de service renvoie uniquement ce profil qui est appliqué à un groupe de machines virtuelles particulier.</p>

Gérez efficacement les règles en appliquant les recommandations suivantes :

- Définissez un numéro de séquence plus élevé pour une stratégie pour laquelle des règles doivent être exécutées en premier. Dans l'interface utilisateur, vous pouvez faire glisser des stratégies pour en modifier la priorité.
- De même, définissez un numéro de séquence plus élevé pour les règles de chaque stratégie.
- Selon le nombre de règles dont vous avez besoin, vous pouvez espacer ces dernières en fonction de multiples de 2, 3, 4, voire 10. Par conséquent, deux règles consécutives séparées de 10 positions vous donnent davantage de flexibilité pour en modifier l'ordre de la séquence sans avoir à changer l'ordre de la séquence de toutes les règles. Par exemple, si vous ne

prévoyez pas de définir de nombreuses règles, vous pouvez choisir de les positionner de manière à ce qu'elles soient espacées de 10 positions. Par conséquent, la règle 1 reçoit le numéro de séquence 1, la règle 2 le 10, la règle 3 le 20 et ainsi de suite. Cette recommandation permet de gérer efficacement les règles de manière à ce qu'il soit inutile de modifier la séquence de toutes les règles.

En interne, Guest Introspection établit la séquence des règles de stratégie de cette façon.

```
Policy 1 ↔ Sequence Number 1 (1000)

- Rule 1 : Group 1↔ Service Profile ↔ Sequence Number 1 (1001)

- Rule 2 : Group 1↔ Service Profile ↔ Sequence Number 10 (1010)

- Rule 3 : Group 1↔ Service Profile ↔ Sequence Number 20 (1020)

- Rule 4 : Group 1↔ Service Profile ↔ Sequence Number 30 (1030)

Policy 2 ↔ Sequence Number 2 (2000)

- Rule 1 : Group 1↔ Service Profile ↔ Sequence Number 1 (2001)

- Rule 2 : Group 1↔ Service Profile ↔ Sequence Number 10 (2010)

- Rule 3 : Group 1↔ Service Profile ↔ Sequence Number 20 (2020)

- Rule 4 : Group 1↔ Service Profile ↔ Sequence Number 30 (2030)
```

En fonction des numéros de séquence ci-dessus, GI exécute les règles de la stratégie 1 avant d'exécuter les règles de la stratégie 2.

Dans certains cas, cependant, les règles prévues ne sont pas appliquées à un groupe de machines virtuelles ou une machine virtuelle. Ces conflits doivent être résolus pour appliquer les niveaux de protection de stratégie souhaités.

Résolution de conflits de stratégies au niveau du point de terminaison

Envisagez un scénario dans lequel deux domaines de stratégie existent, chacun composé de plusieurs règles. En tant qu'admin, vous n'êtes pas toujours certain des machines virtuelles susceptibles de pouvoir appartenir à un groupe, les machines virtuelles étant associées à un groupe en fonction de critères d'appartenance dynamique, comme le nom du système d'exploitation, le nom de l'ordinateur, l'utilisateur et le marquage.

Des conflits surviennent dans les scénarios suivants :

- Une machine virtuelle fait partie de deux groupes, chacun étant protégé par un profil différent.
- Une machine virtuelle de service de partenaires est associée à plusieurs profils de service.
- Une règle inattendue a été exécutée sur une machine virtuelle invitée ou en l'absence de l'exécution d'une règle sur un groupe de machines virtuelles.

- Aucun numéro de séquence n'est attribué à des domaines ou des règles de stratégie.

Tableau 10-12. Résoudre les conflits de stratégies

Scénario	Flux de protection du point de terminaison attendu	Résolution
<p>Lorsqu'une machine virtuelle parvient à appartenir à plusieurs groupes et que chaque groupe est protégé par un type de profil de service différent.</p> <p>La protection attendue n'a pas été appliquée à la machine virtuelle.</p>	<p>Un groupe de machines virtuelles créé avec des critères d'appartenance implique l'ajout dynamique des machines virtuelles au groupe. Dans ce cas, la même machine virtuelle peut faire partie de plusieurs groupes. Il n'existe aucun moyen de déterminer au préalable à quel groupe une machine virtuelle va appartenir, car les critères d'appartenance ajoutent dynamiquement la machine virtuelle au groupe.</p> <p>Imaginons que la machine virtuelle 1 fait partie du groupe 1 et du groupe 2.</p> <ul style="list-style-type: none"> ■ Règle 1 : le groupe 1 (déterminé par le nom du système d'exploitation) reçoit le profil de service or avec le numéro de séquence 1. ■ Règle 2 : le groupe 2 (déterminé par la balise) reçoit le profil de service platine avec le numéro de séquence 10. <p>La stratégie de protection du point de terminaison exécute le profil de service or sur la machine virtuelle 1, mais n'y exécute pas le profil de service platine.</p>	<p>Modifiez le numéro de séquence de la règle 2 de manière à ce qu'il s'exécute avant la règle 1.</p> <ul style="list-style-type: none"> ■ Dans l'interface utilisateur du gestionnaire de stratégies NSX-T, déplacez la règle 2 avant la règle 1 dans la liste des règles en la faisant glisser. ■ En utilisant l'API du gestionnaire de stratégies NSX-T, ajoutez manuellement un numéro de séquence plus élevé pour la règle 2.
<p>Lorsqu'une règle associe un même profil de service pour protéger deux groupes de machines virtuelles.</p> <p>La protection du point de terminaison n'exécute pas la règle sur le second groupe de machines virtuelles.</p>	<p>La protection du point de terminaison exécute uniquement le premier profil de service sur la machine virtuelle, car un même profil de service ne peut pas être appliqué une nouvelle fois sur une autre règle des stratégies ou du domaine.</p> <p>Imaginons que la machine virtuelle 1 fait partie du groupe 1 et du groupe 2.</p> <p>Règle 1 : le groupe 1 (déterminé par le nom du système d'exploitation) reçoit le profil de service or.</p> <p>Règle 2 : le groupe 2 (déterminé par la balise) reçoit le profil de service or.</p>	<ul style="list-style-type: none"> ■ Ajoutez le groupe 2 à la règle 1. (Règle 1 : le groupe 1 et le groupe 2 reçoivent le profil 1.)

Mettre en quarantaine des machines virtuelles

Une fois les règles appliquées aux groupes de machines virtuelles, selon le niveau de protection et les balises définies par les partenaires, certaines machines virtuelles peuvent être identifiées comme étant infectées et doivent ainsi être mises en quarantaine.

Les partenaires utilisent l'API avec la balise `virus_found=true` pour baliser les machines virtuelles qui sont infectées. La balise `virus_found=true` est attachée aux machines virtuelles affectées.

En tant qu'administrateur, vous pouvez créer un groupe prédéfini de mise en quarantaine selon la valeur de la balise `virus_found=true`, de telle sorte que le groupe se remplit avec les machines virtuelles infectées lorsqu'elles sont balisées. En tant qu'admin, vous pouvez choisir de définir des règles de pare-feu spécifiques pour le groupe de mise en quarantaine. Vous pouvez définir des règles de pare-feu pour le groupe de mise en quarantaine. Par exemple, vous pouvez choisir de bloquer tout le trafic entrant et sortant pour le groupe de mise en quarantaine.

Vérifier l'état de santé des instances de service

L'état de santé d'une instance de service dépend de nombreux facteurs : l'état de la solution de partenaire, la connectivité entre l'agent Guest Introspection (multiplexeur de contexte) et le moteur de contexte (agent Ops) ainsi que la disponibilité des informations de l'agent Guest Introspection et des informations de protocole SVM pour NSX Manager.

Procédure


- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Système > Déploiements de service > Instances de service**.
- 3 Dans la colonne État de santé, cliquez sur  pour connaître la santé de l'instance de service.

Tableau 10-13. État de santé de l'instance de service tiers

Paramètre	Description
État de santé reçu à	Horodatage de la dernière réception par NSX Manager des détails de l'état de santé de l'instance de service.
État de la solution	État de la solution de partenaire en cours d'exécution sur une SVM. L'état ACTIF indique que la solution de partenaire s'exécute correctement.
Connectivité entre l'agent NSX-T Data Center Guest Introspection et l'agent NSX-T Data Center Ops	L'état est ACTIF lorsque l'agent NSX-T Data Center Guest Introspection (multiplexeur de contexte) est connecté avec l'agent Ops (qui inclut le moteur de contexte). Le multiplexeur de contexte transfère les informations de santé des SVM vers le moteur de contexte. Il partage également la configuration de la VM et de la SVM entre chacune d'elle pour savoir quelles VM invitées sont protégées par la SVM.
Version de protocole de VM de service	Version du protocole de transport utilisée en interne pour résoudre des problèmes.
Informations de l'agent NSX-T Data Center Guest Introspection	Il s'agit du protocole de compatibilité de version entre l'agent NSX-T Data Center Guest Introspection et la SVM.

- 4 Lorsque l'état de santé est **Actif** (état affiché en vert) et que la console de partenaire affiche toutes les VM invitées dans un état protégé, l'état de santé de l'instance de service est **Actif**.

- 5 Lorsque l'état de santé est `Actif` (état affiché en vert), mais que la console de partenaire affiche les machines virtuelles invitées dans un état non protégé, procédez comme suit :
 - a Contactez le support VMware pour résoudre le problème. L'état de santé de l'instance de service peut être arrêté, ce qui n'est pas correctement reflété dans l'interface utilisateur de NSX Manager.
- 6 Lorsque l'état de santé est `Inactif` (état affiché en rouge), un ou plusieurs facteurs qui déterminent la santé de l'instance de service sont inactifs.

Tableau 10-14. Dépannage de l'état de santé

Attribut État de santé	Résolution
L'état de la solution est <code>Inactif</code> ou <code>Non disponible</code> .	<ol style="list-style-type: none"> 1 Vérifiez que l'état du déploiement des services est <code>Actif</code> (vert). Si vous rencontrez des erreurs, reportez-vous à la section Résoudre les problèmes de services de partenaires. 2 Assurez-vous qu'au moins une VM invitée dans l'hôte affecté est protégée par une stratégie de protection de point de terminaison. 3 À partir de la console de partenaire, vérifiez si le service de la solution est en cours d'exécution sur la SVM de l'hôte. Pour plus d'informations, consultez la documentation des partenaires. 4 Si aucune des étapes ci-dessus ne résout le problème, contactez le support VMware.
La connectivité entre l'agent NSX-T Data Center Guest Introspection et l'agent NSX-T Data Center Ops est <code>Inactive</code> .	<ol style="list-style-type: none"> 1 Vérifiez que l'état du déploiement des services est <code>Actif</code> (vert). Si vous rencontrez des erreurs, reportez-vous à la section Résoudre les problèmes de services de partenaires. 2 Assurez-vous qu'au moins une VM invitée dans l'hôte affecté est protégée par une stratégie de protection de point de terminaison. 3 À partir de la console de partenaire, vérifiez si le service de la solution est en cours d'exécution sur la SVM de l'hôte. Pour plus d'informations, consultez la documentation des partenaires. 4 Si aucune des étapes ci-dessus ne résout le problème, contactez le support VMware.

Tableau 10-14. Dépannage de l'état de santé (suite)

Attribut État de santé	Résolution
La version de protocole de VM de service est Non disponible.	<ol style="list-style-type: none"> 1 Vérifiez que l'état du déploiement des services est Actif (vert). Si vous rencontrez des erreurs, reportez-vous à la section Résoudre les problèmes de services de partenaires. 2 Assurez-vous qu'au moins une VM invitée dans l'hôte affecté est protégée par une stratégie de protection de point de terminaison. 3 À partir de la console de partenaire, vérifiez si le service de la solution est en cours d'exécution sur la SVM de l'hôte. Pour plus d'informations, consultez la documentation des partenaires. 4 Si aucune des étapes ci-dessus ne résout le problème, contactez le support VMware.
Les informations de l'agent NSX-T Data Center Guest Introspection sont Non disponible.	Contactez le support VMware.

Supprimer des services de partenaires

Pour supprimer des services de partenaires, procédez à un appel d'API. Avant d'effectuer l'appel de l'API pour supprimer des SVM ou des services de partenaires déployés sur un hôte, vous devez effectuer les opérations suivantes à partir de l'interface utilisateur de NSX Manager.

Pour supprimer des services de partenaires :

Procédure

- 1 Supprimez les règles EPP appliquées sur les groupes de machines virtuelles en cours d'exécution sur l'hôte.
- 2 Supprimez la protection de profil de service appliquée sur les groupes de machines virtuelles.
- 3 Pour supprimer des SVM de liaison de solution avec le Service Manager partenaire, soumettez l'appel d'API suivant.

```
/DEL https://<NSX_Manager_IPaddress>/api/v1/serviceinsertion/services/{{service_id}}/
solution-configs/<solution-config-id>
```

- 4 Pour supprimer le déploiement de service, procédez à l'appel d'API suivant.

```
/DEL https://<NSX_Manager_IPaddress>/api/v1/serviceinsertion/services/<service-id>/service-
deployments/<service-deployment-id>
```

Consultez le *guide de l'API NSX-T Data Center* pour plus d'informations sur les paramètres de l'API.

Profils de sécurité

Cette section contient des profils qui affinent les opérations de pare-feu : temporisateurs de session, protection de propagation et sécurité DNS

Créer un temporisateur de session

Les temporisateurs de session définissent la durée pendant laquelle une session est maintenue sur le pare-feu après une période d'inactivité dans la session.

Lorsque le délai d'expiration de la session pour le protocole expire, la session se ferme. Sur le pare-feu, il est possible de spécifier plusieurs délais d'expiration pour les sessions TCP, UDP et ICMP à appliquer à un groupe défini par l'utilisateur ou à une passerelle de niveau 0 ou 1. Les valeurs de session par défaut peuvent être modifiées en fonction des besoins de votre réseau. Notez que la définition d'une valeur trop basse peut entraîner des délais d'expiration fréquents, et la définition d'une valeur trop élevée peut retarder la détection des pannes.

Procédure

- 1 Accédez à **Sécurité > Paramètres > Profils de sécurité > Minuteur de la session**.
- 2 Cliquez sur **Ajouter un profil**.
L'écran **Profil** apparaît, rempli avec les valeurs par défaut.
- 3 Entrez un **nom** et une **description** (facultative) pour le profil de temporisateur.
- 4 Cliquez sur **Définir** pour sélectionner la passerelle ou le groupe de niveau 0 ou 1 afin d'appliquer le profil de temporisateur.
- 5 Sélectionnez le protocole. Acceptez les valeurs par défaut ou entrez vos propres valeurs.

Variables TCP	Description
First Packet	Valeur de délai d'expiration pour la connexion après l'envoi du premier paquet. La valeur par défaut est de 120 secondes.
OPENING	Valeur de délai d'expiration pour la connexion après le transfert d'un second paquet. La valeur par défaut est de 30 secondes.
ESTABLISHED	Valeur de délai d'expiration pour la connexion une fois la connexion établie.
CLOSING	Valeur de délai d'expiration pour la connexion après l'envoi du premier FIN. La valeur par défaut est de 120 secondes.
FIN WAIT	Valeur de délai d'expiration pour la connexion après que les deux FIN ont été échangés et que la connexion a été fermée. La valeur par défaut est de 45 secondes.
CLOSED	Valeur de délai d'expiration pour la connexion une fois qu'un point de terminaison envoie un paquet RST. La valeur par défaut est de 20 secondes.

Variables UDP	Description
First Packet	Valeur de délai d'expiration pour la connexion après l'envoi du premier paquet. Délai d'expiration initial pour le nouveau flux UDP. La valeur par défaut est de 60 secondes.
SINGLE	Valeur de délai d'expiration pour la connexion si l'hôte source envoie plusieurs paquets et que l'hôte de destination n'en a pas renvoyé un. La valeur par défaut est de 30 secondes.
MULTIPLE	Valeur de délai d'expiration pour la connexion si les deux hôtes ont envoyé des paquets. La valeur par défaut est de 60 secondes.
Variables ICMP	Description
First Packet	Valeur de délai d'expiration pour la connexion après l'envoi du premier paquet. Délai d'expiration initial pour le nouveau flux ICMP. La valeur par défaut est de 20 secondes.
Réponse d'erreur	Valeur de délai d'expiration pour la connexion après qu'une erreur ICMP a été renvoyée en réponse à un paquet ICMP. La valeur par défaut est de 10 secondes.

6 Cliquez sur **Enregistrer**.

Étape suivante

Après l'enregistrement, cliquez sur [Gérer la priorité des groupes sur les profils](#) pour gérer la priorité de liaison groupe-profil.

Valeurs du minuteur de la session

Le profil du minuteur de la session applique les valeurs de délai d'expiration aux interfaces de routeur de niveau 0 ou de niveau 1 ou aux groupes contenant des segments. Les valeurs de délai d'expiration déterminent la durée pendant laquelle une session de protocole reste active après la fermeture de la session.

Valeurs du minuteur de la session

- Le profil de minuteur par défaut affiché avec l'API et l'interface utilisateur s'applique uniquement au pare-feu distribué (DFW).
- Les minuteurs de session par défaut de pare-feu de passerelle (GFW) sont différents du minuteur de profil par défaut affiché lors de l'utilisation de l'API et de l'interface utilisateur. Les minuteurs de session par défaut de GFW sont optimisés pour le trafic nord-sud et sont inférieurs par défaut.
- Les minuteurs de session FW peuvent être modifiés pour DFW et GFW à l'aide de l'API et de l'interface utilisateur.
- Le même profil de minuteur non défini par défaut peut être appliqué à DFW et GFW, si nécessaire.

Si vous ne personnalisez pas les valeurs des minuteurs, la passerelle prend les valeurs par défaut. Valeurs de minuteur par défaut du pare-feu de passerelle :

Propriété du minuteur	Edge par défaut (en secondes)	Valeur minimale (en secondes)	Valeur maximale (en secondes)
ICMP Error Reply	6	10	4320000
ICMP First Packet	6	10	4320000
TCP Closed	2	10	4320000
TCP Closing	900	10	4320000
TCP Established	7 200	120	4320000
TCP Fin-wait	4	10	4320000
TCP First Packet	120	10	4320000
TCP Opening	30	10	4320000
UDP First Packet	30	10	4320000
UDP Multiple	30	10	4320000
UDP Single	30	10	4320000

Valeurs de minuteur de session par défaut du pare-feu distribué :

Propriété du minuteur	DFW par défaut (en secondes)	Valeur minimale (en secondes)	Valeur maximale (en secondes)
ICMP Error Reply	10	10	4320000
ICMP First Packet	20	10	4320000
TCP Closed	20	10	4320000
TCP Closing	120	10	4320000
TCP Established	43200	120	4320000
TCP Fin-wait	45	10	4320000
TCP First Packet	120	10	4320000
TCP Opening	30	10	4320000
UDP First Packet	60	10	4320000
UDP Multiple	60	10	4320000
UDP Single	30	10	4320000

Protection de propagation

La protection de propagation permet de se protéger contre les attaques de déni de service (DDoS).

Les attaques DDoS visent à rendre un serveur indisponible pour le trafic légitime en consommant toutes les ressources de serveur disponibles. Le serveur est alors submergé de demandes. La création d'un profil de protection de propagation impose des limites de session active pour les flux TCP ICMP, UDP et semi-ouverts. Le pare-feu distribué peut mettre en cache des entrées de flux qui sont dans les états SYN_SENT et SYN_RECEIVED, et promouvoir chaque entrée à l'état TCP après la réception d'un accusé de réception de la part de l'initiateur, en effectuant l'établissement d'une liaison en trois temps.

Procédure

- 1 Accédez à **Sécurité > Profils de sécurité > Protection de propagation**.
- 2 Cliquez sur **Ajouter un profil** et sélectionnez **Ajouter un profil de passerelle Edge** ou **Ajouter un profil de pare-feu**.
- 3 Renseignez les paramètres du profil de protection de propagation :

Tableau 10-15. Paramètres pour les profils de passerelle Edge et de pare-feu

Paramètre	Valeurs minimales et maximales	Par défaut	
Limite de connexion semi-ouverte TCP : les attaques par saturation TCP SYN sont bloquées en limitant le nombre de flux TCP actifs et non entièrement établis qui sont autorisés par le pare-feu.	1 - 1 000 000	Pare-feu : aucun Passerelle Edge : 1 000 000	Définissez cette zone de texte pour limiter le nombre de connexions semi-ouvertes TCP actives. Si cette zone de texte est vide, cette limite est désactivée sur les nœuds ESX et définie sur la valeur par défaut des passerelles Edge.
Limite de propagation active UDP : les attaques par saturation UDP sont bloquées en limitant le nombre de flux UDP actifs qui sont autorisés par le pare-feu. Une fois la limite de flux UDP définie atteinte, les paquets UDP suivants qui peuvent établir un nouveau flux sont abandonnés.	1 - 1 000 000	Pare-feu : aucun Passerelle Edge : 1 000 000	Définissez cette zone de texte pour limiter le nombre de connexions UDP actives. Si cette zone de texte est vide, cette limite est désactivée sur les nœuds ESX et définie sur la valeur par défaut des passerelles Edge.

Tableau 10-15. Paramètres pour les profils de passerelle Edge et de pare-feu (suite)

Paramètre	Valeurs minimales et maximales	Par défaut	
Limite de propagation active ICMP : les attaques par saturation ICMP sont bloquées en limitant le nombre de flux ICMP actifs qui sont autorisés par le pare-feu. Une fois la limite de flux définie atteinte, les paquets ICMP suivants qui peuvent établir un nouveau flux sont abandonnés.	1 - 1 000 000	Pare-feu : aucun Passerelle Edge - 10 000	Définissez cette zone de texte pour limiter le nombre de connexions ouvertes ICMP actives. Si cette zone de texte est vide, cette limite est désactivée sur les nœuds ESX et définie sur la valeur par défaut des passerelles Edge.
Autre limite de connexion active	1 - 1 000 000	Pare-feu : aucun Passerelle Edge - 10 000	Définissez cette zone de texte pour limiter le nombre de connexions actives autres que les connexions ICMP, TCP et UDP semi-ouvertes. Si cette zone de texte est vide, cette limite est désactivée sur les nœuds ESX et définie sur la valeur par défaut des passerelles Edge.

Tableau 10-15. Paramètres pour les profils de passerelle Edge et de pare-feu (suite)

Paramètre	Valeurs minimales et maximales	Par défaut	
Cache SYN : le cache SYN est utilisé lorsqu'une limite de connexion semi-ouverte TCP a également été configurée. Le nombre de connexions semi-ouvertes actives est appliqué en conservant un cache SYN des sessions TCP non entièrement établies. Ce cache conserve les entrées de flux qui sont dans les états SYN_SENT et SYN_RECEIVED. Chaque entrée du cache SYN sera promue en une entrée complète à l'état TCP après la réception d'un accusé de réception de la part de l'initiateur, en effectuant l'établissement d'une liaison en trois temps.		Disponible uniquement pour les profils de pare-feu.	Bouton bascule d'activation et de désactivation. L'activation du cache SYN n'est efficace que lorsqu'une limite de connexion semi-ouverte TCP est configurée.
Usurpation RST : génère un RST usurpé au serveur lors de la purge d'états semi-ouverts à partir du cache SYN. Permet au serveur de nettoyer les états associés à la saturation SYN (semi-ouverte).		Disponible uniquement pour les profils de pare-feu.	Bouton bascule d'activation et de désactivation. Le cache SYN doit être sélectionné pour que cette option soit disponible

4 Pour appliquer le profil à des passerelles Edge et des groupes de pare-feu, cliquez sur **Définir**.

5 Cliquez sur **Enregistrer**.

Étape suivante

Après l'enregistrement, cliquez sur [Gérer la priorité des groupes sur les profils](#) pour gérer la priorité de liaison groupe-profil.

Configurer la sécurité DNS

La création d'un profil de sécurité DNS permet de se protéger contre les attaques liées à DNS.

Après avoir configuré le profil de sécurité DNS, vous pouvez effectuer les opérations suivantes :

- Écoutez les réponses DNS d'une machine virtuelle ou d'un groupe de machines virtuelles sur le nœud de transport afin d'associer un nom de domaine complet à des adresses IP.
- Ajoutez des informations de serveur DNS globales et par défaut et appliquez-les à toutes les machines virtuelles qui utilisent des règles DFW.
- Spécifiez les informations de serveur DNS sélectionnées pour les machines virtuelles sélectionnées.
- Appliquez des profils DNS à des groupes.

Note Seul ESXi est pris en charge dans la version actuelle.

Procédure

- 1 Accédez à **Sécurité > Paramètres > Profils de sécurité > Sécurité DNS**.
- 2 Cliquez sur **Ajouter un profil**.
- 3 Entrez les valeurs suivantes :

Option	Description
Nom du profil	Fournissez un nom de profil.
TTL	<p>Ce champ capture la durée de vie de l'entrée du cache DNS en secondes. Vous disposez des options suivantes :</p> <p>TTL 0 : l'entrée mise en cache n'expire jamais.</p> <p>TTL 1 à 3 599 : non valide</p> <p>TTL 3 600 à 864 000 : valide</p> <p>TTL laissé vide : TTL automatique, défini à partir du paquet de réponse DNS.</p> <p>Note Le profil de sécurité DNS a un délai d'expiration du cache DNS par défaut de 24 heures.</p>
Appliqué à	<p>Vous pouvez sélectionner un groupe en fonction de n'importe quel critère auquel appliquer le profil de sécurité DNS.</p> <p>Note Un seul profil de serveur DNS est appliqué à une machine virtuelle.</p>
Balises	Facultative. Attribuez une balise et une étendue au profil DNS pour faciliter la recherche. Pour plus d'informations, reportez-vous à la section Ajouter des balises à un objet .

- 4 Cliquez sur **Enregistrer**.

Étape suivante

Après l'enregistrement, cliquez sur [Gérer la priorité des groupes sur les profils](#) pour gérer la priorité de liaison groupe-profil.

Gérer la priorité des groupes sur les profils

Vous pouvez lier plusieurs groupes à un profil de sécurité. NSX-T Data Center applique le profil de sécurité au groupe ayant le niveau de priorité le plus élevé.

Si vous liez un profil de sécurité à plusieurs groupes, NSX-T Data Center attribue la priorité la plus élevée au groupe le plus récent de cette liste. Cependant, vous pouvez modifier le niveau de priorité des groupes.

Pour attribuer une priorité à des groupes :

Conditions préalables

- Les groupes de temporisateurs de session doivent contenir uniquement des segments, des ports de segment et des machines virtuelles en tant que membres. Les autres types de catégories ne sont pas pris en charge.
- Les groupes de sécurité DNS doivent contenir uniquement des machines virtuelles en tant que membres. Les autres types de catégories ne sont pas pris en charge.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Accédez à **Sécurité > Profils de sécurité**.
- 3 Cliquez sur **Gérer la priorité des groupes sur les profils**.
- 4 Pour attribuer le niveau de priorité le plus élevé à un groupe, déplacez le groupe en haut de la liste.
- 5 Cliquez sur **Fermer**.

Résultats

Le profil de sécurité est appliqué au groupe ayant le niveau de priorité le plus élevé.

Vous pouvez configurer les services, les groupes, les profils de contexte et les machines virtuelles pour l'inventaire NSX-T Data Center.

Lorsque vous cliquez sur l'onglet **Inventaire**, une présentation des objets d'inventaire s'affiche, indiquant le nombre de groupes, de services, de machines virtuelles et de profils de contexte qui se trouvent dans l'inventaire. En outre, les informations suivantes sur les groupes sont affichées :

- nombre de groupes utilisés dans les stratégies
- nombre de groupes non utilisés dans les stratégies
- nombre de groupes avec membres
- nombre de groupes sans membres
- nombre de groupes d'identité
- nombre de groupes d'identité utilisés dans les stratégies
- nombre de groupes d'identité non utilisés dans les stratégies

Ce chapitre contient les rubriques suivantes :

- [Ajouter un service](#)
- [Ajouter un groupe](#)
- [Ajouter un profil de contexte](#)

Ajouter un service

Vous pouvez configurer un service et spécifier des paramètres de correspondance du trafic réseau, comme un couplage port/protocole.

Vous pouvez également utiliser un service pour autoriser ou bloquer certains types de trafic dans les règles de pare-feu. Vous ne pouvez pas modifier les types après la création d'un service. Certains services sont prédéfinis, et ne peuvent pas être modifiés ou supprimés.

Procédure

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

- 2 Sélectionnez **Inventaire > Services**.
- 3 Cliquez sur **Ajouter un nouveau service**.
- 4 Entrez un nom.
- 5 Cliquez sur **Définir les entrées de service**. Cliquez sur **Ajouter une nouvelle entrée de service**.
- 6 Pour un nouveau service, sélectionnez un type de service et indiquez des propriétés supplémentaires.

Les types disponibles sont **IP**, **IGMP**, **ICMPv4**, **ICMPv6**, **ALG**, **TCP**, **UDP** et **Ether**.
- 7 Cliquez sur **Enregistrer**.
- 8 (Facultatif) Ajoutez une ou plusieurs balises.
- 9 (Facultatif) Entrez une description.
- 10 Cliquez sur **Enregistrer**.

Ajouter un groupe

Les groupes comprennent différents objets, ajoutés à la fois statiquement et dynamiquement, et pouvant faire office de source et de destination pour une règle de pare-feu.

Des groupes peuvent être configurés de manière à comporter des machines virtuelles, des ensembles d'adresses IP, des ensembles d'adresses MAC, des ports de segment, des segments, des groupes d'utilisateurs AD et d'autres groupes. L'inclusion dynamique de groupes peut reposer sur une balise, un nom de machine, un nom de système d'exploitation ou un nom d'ordinateur. Les groupes basés sur des objets dynamiques ou logiques ne peuvent pas être utilisés dans le champ Appliqué à de règles de pare-feu distribué.

Les balises dans NSX sont sensibles à la casse, mais un groupe basé sur les balises n'est pas « sensible à la casse ». Par exemple, si le critère d'appartenance au groupement dynamique est `vm Tag Equals 'quarantine'`, le groupe comprend toutes les machines virtuelles qui contiennent les balises « mise en quarantaine » ou « MISE EN QUARANTAINE ».

Les groupes peuvent également être exclus des règles de pare-feu et la liste peut contenir un maximum de 100 groupes. Les ensembles d'adresses IP, les ensembles d'adresses MAC et les groupes AD ne peuvent pas être inclus en tant que membres dans un groupe utilisé dans une liste d'exclusion de pare-feu. Pour plus d'informations, reportez-vous à la section [Gérer une liste d'exclusion de pare-feu](#).

Remarque sur NSX Cloud Si vous utilisez NSX Cloud, reportez-vous à la section [Regrouper les machines virtuelles à l'aide de NSX-T Data Center et de balises de cloud public](#) pour plus d'informations sur l'utilisation des balises de cloud public afin de regrouper vos machines virtuelles de charge de travail dans NSX Manager.

Un groupe basé sur un seul ID peut être utilisé comme source uniquement dans une règle de pare-feu distribué. Si des groupes basés sur l'adresse IP et l'ID sont nécessaires à la source, créez deux règles de pare-feu distinctes.

Les groupes comprenant uniquement des adresses IP, des adresses MAC ou des groupes Active Directory ne peuvent pas être utilisés dans la zone de texte **Appliqué à**.

Note Lorsqu'un hôte est ajouté à un serveur vCenter Server ou supprimé de celui-ci, l'ID externe des VM de l'hôte change. Si une VM est un membre statique d'un groupe et que l'ID externe de la VM change, l'interface utilisateur de NSX Manager n'affiche plus la VM en tant que membre du groupe. Toutefois, l'API qui répertorie les groupes indiquera toujours que le groupe contient la VM avec son ID externe d'origine. Si vous ajoutez une VM en tant que membre statique d'un groupe et que l'ID externe de la VM change, vous devez rajouter la VM à l'aide de son nouvel ID externe. Vous pouvez également utiliser des critères d'appartenance dynamique pour éviter ce problème.

Procédure

- 1 Sélectionnez **Inventaire > Groupes** dans le panneau de navigation.
- 2 Cliquez sur **Ajouter un groupe**.
- 3 Entrez un nom de groupe.
- 4 (Facultatif) Cliquez sur **Définir les membres**.

Pour chaque critère d'appartenance, vous pouvez spécifier jusqu'à cinq règles, combinées avec l'opérateur logique AND. Le critère d'appartenance disponible peut s'appliquer aux éléments suivants :

- **Port de segment** : peut spécifier une balise et éventuellement une étendue.
- **Segment** : peut spécifier une balise et éventuellement une étendue.
- **Machine virtuelle** : peut spécifier un nom, une balise, un nom de SE d'ordinateur ou un nom d'ordinateur qui est égal à, contient, commence par, se termine par ou n'est pas égal à une chaîne donnée.
- **Ensemble d'adresses IP** : peut spécifier une balise et éventuellement une étendue.

- 5 (Facultatif) Cliquez sur **Membres** pour sélectionner des membres.

Les types de membres disponibles sont les suivants :

- **Groupe**
- **Segment**
- **Port de segment**
- **Interface réseau virtuelle**
- **Machine virtuelle**

- 6 (Facultatif) Cliquez sur **Adresses IP/MAC** pour ajouter des adresses IP et MAC en tant que membres du groupe.

Les adresses IPv4, IPv6 et de multidiffusion sont prises en charge.

7 (Facultatif) Cliquez sur **Groupes AD** pour ajouter des groupes Active Directory. Les groupes avec des membres Active Directory peuvent être utilisés dans le champ source d'une règle de pare-feu distribué pour Identity Firewall. Les groupes peuvent contenir à la fois des membres AD et des membres de calcul.

8 (Facultatif) Entrez une description et une balise.

9 Cliquez sur **Appliquer**.

Les groupes sont répertoriés, et une option permettant d'en afficher les membres et l'emplacement d'utilisation est mise à disposition.

Ajouter un profil de contexte

Les profils de contexte permettent de créer des paires de valeurs de clés d'attributs telles que l'ID d'application de couche 7 et les noms de domaine. Une fois que vous avez défini un profil de contexte, vous pouvez l'utiliser dans une ou plusieurs règles de pare-feu distribué et règles de pare-feu de passerelle.

Deux attributs sont disponibles à des fins d'utilisation dans les profils de contexte : l'ID d'application et le nom de domaine complet. Sélectionnez les ID d'application qui peuvent avoir un ou plusieurs sous-attributs, comme TLS_Version et CIPHER_SUITE. L'ID d'application et le nom de domaine peuvent être utilisés dans un profil de contexte unique. Plusieurs ID d'application peuvent être utilisés dans un même profil. Il est possible d'utiliser un ID d'application avec sous-attributs. Les sous-attributs sont effacés lorsque plusieurs attributs de type ID d'application sont utilisés dans un seul profil.

Une liste prédéfinie de domaines est actuellement prise en charge. Vous pouvez voir la liste des noms de domaine complets lorsque vous ajoutez un nouveau profil de contexte de type d'attribut *Nom de domaine (FQDN)*. Vous pouvez également voir une liste de noms de domaine complets en exécutant l'appel d'API `/policy/api/v1/infra/context-profiles/attributes?attribute_key=DOMAIN_NAME`.

Note

- Les règles de pare-feu de passerelle ne prennent pas en charge l'utilisation d'attributs de nom de domaine complet ou d'autres sous-attributs dans les profils de contexte.
 - Les profils de contexte ne sont pas pris en charge sur la stratégie de pare-feu de passerelle de niveau 0. Les règles de pare-feu de passerelle ne prennent pas en charge l'utilisation d'attributs de nom de domaine complet ou d'autres sous-attributs.
-

Procédure

- 1 Sélectionnez **Inventaire > Profils de contexte**.
- 2 Cliquez sur **Ajouter un nouveau profil de contexte**.
- 3 Entrez un **nom de profil**.
- 4 Dans la colonne Attributs, cliquez sur **Définir**.

- 5 Sélectionnez un attribut ou cliquez sur **Ajouter un attribut**, puis sélectionnez **ID d'application** ou **Nom de domaine complet**.
- 6 Sélectionne au moins un attribut.
- 7 (Facultatif) Si vous avez sélectionné un attribut avec des sous-attributs tels que SSL ou CIFS, cliquez sur **Définir** dans la colonne Sous-attributs/Valeurs.
 - a Cliquez sur **Ajouter un sous-attribut** et sélectionnez une catégorie de sous-attribut dans le menu déroulant.
 - b Sélectionnez au moins un sous-attribut.
 - c Cliquez sur **Ajouter**. Vous pouvez ajouter un autre sous-attribut en cliquant sur **Ajouter un sous-attribut**.
 - d Cliquez sur **Appliquer**.
- 8 Cliquez sur **Ajouter**.
- 9 (Facultatif) Pour ajouter un autre type d'attribut, cliquez de nouveau sur **Ajouter un attribut**.
- 10 Cliquez sur **Appliquer**.
- 11 (Facultatif) Entrez une description.
- 12 (Facultatif) Entrez un libellé.
- 13 Cliquez sur **Enregistrer**.

Étape suivante

Appliquez ce profil de contexte à une règle de pare-feu distribué de couche 7 (pour la couche 7 ou le nom de domaine) ou à une règle de pare-feu de passerelle (pour la couche 7).

Il existe plusieurs manières de surveiller l'environnement NSX-T ainsi que le trafic réseau.

Ce chapitre contient les rubriques suivantes :

- Ajouter un profil IPFIX de pare-feu
- Ajouter un profil IPFIX de commutateur
- Ajouter un collecteur IPFIX
- Ajouter un profil de mise en miroir de ports
- Protocole de gestion de réseau simple (SNMP)
- Utilisation de vRealize Log Insight pour la surveillance du système
- Utilisation de vRealize Operations Manager pour la surveillance du système
- Utilisation de vRealize Network Insight Cloud pour la surveillance du système
- Outils de surveillance avancés

Ajouter un profil 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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Planifier et dépanner > IPFIX**.
- 3 Cliquez sur l'onglet **Profils IPFIX de pare-feu**.
- 4 Cliquez sur **Ajouter un profil IPFIX de pare-feu**.

5 Renseignez les détails suivants.

Paramètre	Description
Nom et description	Entrez un nom et éventuellement une description. Note Si vous souhaitez créer un profil global, nommez le profil Global . Un profil global ne peut pas être modifié ou supprimé de l'interface utilisateur, mais vous pouvez le faire à l'aide d'API NSX-T Data Center.
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.
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.
Configuration du collecteur	Sélectionnez un collecteur dans le menu déroulant.
Appliqué à	Cliquez sur Définir et sélectionnez un groupe auquel appliquer le filtre ou créez un groupe.
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.

6 Cliquez sur **Enregistrer**, puis sur **Oui** pour continuer la configuration du profil.

7 Cliquez sur **Enregistrer**.

Ajouter un profil IPFIX de commutateur

Vous pouvez configurer des profils IPFIX pour des commutateurs, aussi appelés segments.

La surveillance du réseau basée sur le flux permet aux administrateurs réseau de mieux comprendre le trafic traversant un réseau.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Planifier et dépanner > IPFIX**.
- 3 Cliquez sur l'onglet **Profils IPFIX de commutateur**.
- 4 Cliquez sur **Ajouter un profil IPFIX de commutateur**.

5 Entrez les détails suivants :

Paramètre	Description
Nom et description	Entrez un nom et éventuellement une description. Note Si vous souhaitez créer un profil global, nommez le profil Global . Un profil global ne peut pas être modifié ou supprimé de l'interface utilisateur, mais vous pouvez le faire à l'aide d'API NSX-T Data Center.
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 basée sur un délai d'expiration actif). La valeur par défaut est 300.
Probabilité d'échantillonnage des paquets (%)	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 IPFIX 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.
Configuration du collecteur	Sélectionnez un collecteur dans le menu déroulant.
Appliqué à	Sélectionnez une catégorie : Segment, Port de segment ou Groupes. Le profil IPFIX est appliqué à l'objet sélectionné.
Priorité	Ce paramètre résout les conflits lorsque plusieurs profils s'appliquent. L'exportateur IPFIX n'utilise que le profil avec la priorité la plus élevée. Une valeur inférieure signifie une priorité plus élevée.
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.
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.
Exporter le flux de superposition	Ce paramètre définit s'il faut échantillonner et exporter les flux de superposition sur les ports de liaison montante et de tunnel. Les flux de vNIC et de superposition sont inclus dans l'exemple. La valeur par défaut est activée . Lorsqu'elle est désactivée, seuls les flux de vNIC sont échantillonnés et exportés.
Balises	Entrez une balise pour faciliter la recherche.

6 Cliquez sur **Enregistrer**, puis sur **Oui** pour continuer la configuration du profil.

7 Cliquez sur **Appliqué à** pour appliquer le profil à des objets.

Sélectionnez un ou plusieurs objets.

8 Cliquez sur **Enregistrer**.

Ajouter un collecteur IPFIX

Vous pouvez configurer des collecteurs IPFIX pour des pare-feu et des commutateurs.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Planifier et dépanner > IPFIX**.
- 3 Cliquez sur l'onglet **Collecteurs**.
- 4 Sélectionnez **Ajouter un nouveau collecteur > Commutateur IPFIX** ou **Ajouter un nouveau collecteur > Pare-feu IPFIX**.
- 5 Entrez un nom.
- 6 Entrez l'adresse IP et le port de quatre collecteurs maximum. Les adresses IPv4 et IPv6 sont prises en charge.
- 7 Cliquez sur **Enregistrer**.

Ajouter un profil de mise en miroir de ports

Vous pouvez configurer des profils de mise en miroir de port pour les sessions de mise en miroir de ports.

Notez que SPAN logique est pris en charge uniquement pour les segments de superposition et pas pour les segments VLAN.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Planifier et dépanner > Mise en miroir de ports**.
- 3 Sélectionnez **Ajouter un profil > SPAN L3 distant** ou **Ajouter un profil > SPAN logique**.
- 4 Entrez un nom et éventuellement une description.
- 5 Renseignez les détails de profil suivants.

Type de session	Paramètres
SPAN L3 distant	<ul style="list-style-type: none"> ■ Direction - sélectionnez Bidirectionnel, Entrée ou Sortie. ■ Longueur du snapshot - indiquez le nombre d'octets à capturer à partir d'un paquet. ■ Type d'encapsulation - sélectionnez GRE, ERSPAN TWO ou ERSPAN THREE. ■ Clé GRE - spécifiez une clé GRE si le type d'encapsulation est GRE. ■ ID ERSPAN - spécifiez un ID ERSPAN si le type d'encapsulation est ERSPAN TWO ou ERSPAN THREE.
SPAN logique	<ul style="list-style-type: none"> ■ Direction - sélectionnez Bidirectionnel, Entrée ou Sortie. ■ Longueur du snapshot - indiquez le nombre d'octets à capturer à partir d'un paquet.

- 6 Cliquez sur **Définir** dans la colonne **Source** pour définir une source.

Pour SPAN logique, les sources disponibles sont **Port de segment**, **Groupe de machines virtuelles** et **Groupe d'interfaces réseau virtuelles**.

Pour SPAN L3 distant, les sources disponibles sont **Segment**, **Port de segment**, **Groupe de machines virtuelles** et **Groupe d'interfaces de réseau virtuel**.

- 7 Cliquez sur **Définir** dans la colonne **Destination** pour définir une destination.

- 8 Cliquez sur **Enregistrer**.

Protocole de gestion de réseau simple (SNMP)

Vous pouvez utiliser le protocole SNMP (simple Network Management Protocol) pour surveiller vos composants NSX-T Data Center. Le service SNMP n'est pas démarré par défaut après l'installation.

Procédure

- 1 Connectez-vous à l'interface de ligne de commande NSX Manager ou NSX Edge.
- 2 Exécutez les commandes suivantes

- Pour SNMPv1/SNMPv2 :

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

La limite de caractères maximale pour **chaîne-de-communauté** est de 64.

- Pour SNMPv3

```
set snmp v3-users <nom_utilisateur> auth-password <motdepasse_auth> priv-password
<motdepasse_conf>

start service snmp
```

La limite de caractères maximale pour **nom_utilisateur** est de 32. Assurez-vous que vos mots de passe respectent les contraintes PAM. Si vous souhaitez modifier l'ID de moteur par défaut, utilisez la commande suivante :

```
set snmp v3-engine-id <id_moteur_v3>

start service snmp
```

id_moteur_v3 est une chaîne hexadécimale d'une longueur de 10 à 64 caractères.

NSX-T Data Center prend en charge les protocoles d'authentification et de confidentialité SHA1 et AES128. Vous pouvez également utiliser des appels d'API pour configurer SNMPv3. Pour plus d'informations, reportez-vous au *Guide de l'API de NSX-T Data Center*.

Exemple :

Utilisation de vRealize Log Insight pour la surveillance du système

Vous pouvez surveiller votre environnement NSX-T Data Center à l'aide du pack de contenu Log Insight NSX-T.

Ce pack de contenu comporte les alertes suivantes :

Nom de l'alerte	Description
SysCpuUsage	L'utilisation du CPU est supérieure à 95 % pendant plus de 10 minutes.
SysMemUsage	L'utilisation de la mémoire est supérieure à 95 % pendant plus de 10 minutes.
SysDiskUsage	L'utilisation du disque pour une ou plusieurs partitions est supérieure à 89 % pendant plus de 10 minutes.
PasswordExpiry	Le mot de passe du compte d'utilisateur du dispositif est sur le point d'expirer ou expiré.
CertificateExpiry	Un ou plusieurs certificats signés par une autorité de certification ont expiré.
ClusterNodeStatus	Le nœud du cluster Edge local est inactif.
BackupFailure	Échec de l'opération de sauvegarde planifiée NSX.
VipLeadership	L'adresse IP virtuelle du cluster de gestion NSX est inactive.
ApiRateLimit	L'API client a atteint le seuil configuré.
CorfuQuorumLost	Deux nœuds sont tombés dans le cluster et le quorum corfu a été perdu.
DfwHeapMem	La mémoire du segment de mémoire DFW a dépassé le seuil configuré.
ProcessStatus	L'état du processus critique a été modifié.
ClusterFailoverStatus	État de la haute disponibilité SR modifié ou basculement des services actif/en veille.
DhcpPoolUsageOverloadedEvent	Le pool DHCP a atteint le seuil d'utilisation configuré.
FabricCryptoStatus	Le pilote Edge crypto mux est inactif pour l'échec aux Known_Answer_Tests (KAT).
VpnTunnelState	Le tunnel VPN est inactif
BfdTunnelStatus	L'état du tunnel BFD a changé.
RoutingBgpNeighborStatus	L'état du voisin BGP est inactif.
VpnL2SessionStatus	La session VPN L2 est inactive.
VpnIkeSessionStatus	La session IKE est inactive.
RoutingStatus	Le routage (BGP/BFD) est inactif.
DnsForwarderStatus	L'état d'exécution du redirecteur DNS est inactif.
TnConnDown_15min	La connexion entre le nœud de transport et un contrôleur/gestionnaire est inactive pendant au moins 15 minutes.
TnConnDown_5min	La connexion entre le nœud de transport et le contrôleur/gestionnaire est inactive pendant au moins 5 minutes.

Nom de l'alerte	Description
ServiceDown	Un ou plusieurs services sont inactifs.
IpNotAvailableInPool	Aucune adresse IP n'est disponible dans le pool ou atteint le seuil configuré.
LoadBalancerError	L'état du service d'équilibreur de charge NSX est ERREUR.
LoadBalancerDown	L'état du service d'équilibreur de charge NSX est INACTIF.
LoadBalancerVsDown	État VS : tous les membres du pool sont inactifs.
LoadBalancerPoolDown	État du pool : tous les membres du pool sont inactifs.
ProcessCrash	Un processus ou un démon se bloque dans le chemin données ou d'autres processus d'équilibrage de charge tels que le répartiteur, etc.

Utilisation de vRealize Operations Manager pour la surveillance du système

Vous pouvez surveiller votre environnement NSX-T Data Center à l'aide de vRealize Operations Manager.

Tableau 12-1. Alertes dans le pack de gestion pour NSX-T

Alerte	Description	Recommandation
Le service de gestion de NSX-T a échoué	Déclenchée lorsque le service de gestion sur l'hôte NSX-T Data Center n'est pas en cours d'exécution.	Connectez-vous à NSX-T Manager et redémarrez le service de gestion qui a échoué.
L'état d'administrateur du commutateur logique n'est pas actif	Déclenchée lorsque l'état d'administrateur est désactivé sur le commutateur logique.	Connectez-vous à NSX-T et activez l'état d'administration, le cas échéant.
La connectivité au contrôleur/gestionnaire du nœud Edge n'est pas active	Déclenchée lorsque l'état de connectivité du nœud Edge est inactif dans NSX-T Data Center.	Vérifiez l'état de la connexion du nœud Edge au cluster de contrôleurs et au cluster de gestionnaires et rétablissez la connexion.
Le nœud de l'hôte Edge est en état d'échec/erreur	Déclenchée lorsque le nœud de l'hôte dans NSX-T Data Center est en état d'erreur ou d'échec pour l'une des raisons suivantes : <ul style="list-style-type: none"> ■ Erreur de configuration du dispositif Edge ■ Échec de l'installation ■ Échec de la désinstallation ■ Échec de la mise à niveau ■ Échec du déploiement de la machine virtuelle ■ Échec de la mise hors tension de la machine virtuelle ■ Échec de la mise sous tension de la machine virtuelle ■ Échec de l'annulation du déploiement de la machine virtuelle 	Le nœud de l'hôte Edge est en état d'échec/erreur. Vérifiez l'état du nœud de l'hôte et corrigez le problème.

Tableau 12-1. Alertes dans le pack de gestion pour NSX-T (suite)

Alerte	Description	Recommandation
Le service BFD est désactivé.	Déclenchée lorsque le service BFD n'est pas activé sur le routeur logique.	Le service BFD pour un routeur de niveau 0 n'est pas activé même si les voisins sont configurés. Activez le service BFD si nécessaire.
Règle NAT non configurée	Déclenchée lorsque la règle NAT sur le routeur logique n'est pas configurée.	Connectez-vous à NSX-T Manager et ajoutez les règles NAT pour le routeur logique.
La route statique n'est pas configurée	Déclenchée lorsque la route statique sur le routeur logique n'est pas configurée.	Connectez-vous à NSX-T Manager et ajoutez les routes statiques pour le routeur logique, si nécessaire.
Le service d'annonce de route est désactivé	Déclenchée lorsque le service d'annonce de route n'est pas activé sur le routeur logique.	Le service d'annonce de route pour un routeur de niveau 1 n'est pas activé même si les annonces de route sont configurées. Connectez-vous à NSX-T Manager et activez le service.
Le service de redistribution de route est désactivé	Déclenchée lorsque le service de redistribution de route n'est pas activé sur le routeur logique.	Le service de redistribution de route d'un routeur de niveau 0 n'est pas activé même si les règles de redistribution de route sont configurées. Connectez-vous à NSX-T Manager et activez le service.
Le service ECMP est désactivé pour le routeur logique	Déclenchée lorsque le service ECMP n'est pas activé sur le routeur logique.	Le service ECMP BGP pour un routeur de niveau 0 n'est pas activé même si les voisins sont configurés. Connectez-vous à NSX-T Manager et activez le service.
La connectivité au nœud de contrôleur est interrompue	Déclenchée lorsque l'état de la connexion du nœud de contrôleur est inactif dans NSX-T Data Center	Connectez-vous à NSX-T Manager et vérifiez la connectivité du nœud de contrôleur avec le nœud de gestion et le cluster de contrôleurs et réglez l'état déconnecté.
Moins de 3 nœuds de contrôleur sont déployés	Déclenchée lorsque le serveur NSX-T Data Center dispose de moins de trois nœuds de contrôleur.	Déployez au moins 3 nœuds de contrôleur dans le cluster.
L'état du cluster de contrôleurs n'est pas stable	Déclenchée lorsque tous les nœuds de contrôleur sont inactifs dans NSX-T Data Center.	Vérifiez l'état du cluster de contrôleurs.
L'état de gestion n'est pas stable	Déclenchée lorsque l'état d'un nœud sur le cluster de gestion est inactif.	Vérifiez l'état du cluster de gestion.

Tableau 12-1. Alertes dans le pack de gestion pour NSX-T (suite)

Alerte	Description	Recommandation
L'utilisation du système de fichiers est supérieure à 85 %	Déclenchée lorsque l'utilisation des systèmes de fichiers invités de la machine virtuelle du contrôleur est supérieure à 85 %.	L'utilisation du système de fichiers est supérieure à 85. Vérifiez et nettoyez le système de fichiers pour libérer de l'espace.
L'utilisation du système de fichiers est supérieure à 75 %	Déclenchée lorsque l'utilisation des systèmes de fichiers invités de la machine virtuelle du contrôleur est supérieure à 75 %.	L'utilisation du système de fichiers est supérieure à 75. Vérifiez et nettoyez le système de fichiers pour libérer de l'espace.
L'utilisation du système de fichiers est supérieure à 70 %	Déclenchée lorsque l'utilisation des systèmes de fichiers invités de la machine virtuelle du contrôleur est supérieure à 70 %.	L'utilisation du système de fichiers est supérieure à 70. Vérifiez et nettoyez le système de fichiers pour libérer de l'espace.
L'état du cluster Edge est inactif	Déclenchée lorsque l'état du cluster Edge est inactif.	Vérifiez l'état du cluster Edge et, si nécessaire, suivez les étapes de dépannage standard recommandées par la documentation de NSX-T et la documentation VMware.
L'état du commutateur logique a échoué	Déclenchée lorsque l'état du commutateur logique a échoué.	Vérifiez l'état du commutateur logique et, si nécessaire, suivez les étapes de dépannage standard recommandées par la documentation de NSX-T et la documentation VMware.
L'état opérationnel du service d'équilibreur de charge est inactif	Déclenchée lorsque l'état opérationnel du service d'équilibreur de charge est inactif.	Vérifiez l'état opérationnel du service d'équilibreur de charge et, si nécessaire, suivez les étapes de dépannage standard recommandées par la documentation de NSX-T et la documentation VMware.
Erreur d'état opérationnel du service d'équilibreur de charge	Déclenchée lorsque l'état opérationnel du service d'équilibreur de charge contient une erreur.	Vérifiez l'état opérationnel du service d'équilibreur de charge et, si nécessaire, suivez les étapes de dépannage standard recommandées par la documentation de NSX-T et la documentation VMware.

Tableau 12-1. Alertes dans le pack de gestion pour NSX-T (suite)

Alerte	Description	Recommandation
Le serveur virtuel d'équilibreur de charge est inactif	Déclenchée lorsque l'état opérationnel du serveur virtuel d'équilibreur de charge est inactif	Vérifiez l'état opérationnel du serveur virtuel d'équilibreur de charge et, si nécessaire, suivez les étapes de dépannage standard recommandées par la documentation de NSX-T et la documentation VMware.
État opérationnel du serveur virtuel de l'équilibreur de charge détaché	Déclenchée lorsque l'état opérationnel du serveur virtuel de l'équilibreur de charge est détaché.	Vérifiez l'état opérationnel du serveur virtuel d'équilibreur de charge et, si nécessaire, suivez les étapes de dépannage standard recommandées par la documentation de NSX-T et la documentation VMware.
L'état de configuration du nœud Edge a échoué	Déclenchée lorsque l'état de configuration du nœud Edge a échoué.	Vérifiez l'état de configuration du nœud Edge et, si nécessaire, suivez les étapes de dépannage standard recommandées par la documentation de NSX-T et la documentation VMware.
L'état d'exécution du moniteur du service de gestion a échoué	Déclenchée lorsque l'état d'exécution du moniteur du service de gestion cesse de s'exécuter.	Connectez-vous à NSX-T Manager VA et redémarrez le service de gestion qui a échoué.
L'état de gestion du cluster de gestion n'est pas stable	Déclenchée lorsque l'état de gestion d'un cluster de gestion n'est pas stable.	Vérifiez l'état du cluster de gestion.
Moins de 3 nœuds de gestionnaire sont déployés	Déclenchée lorsque le serveur NSX-T dispose de moins de trois nœuds de gestionnaire déployés.	Déployez au moins 3 nœuds de gestionnaire dans le cluster.
La connectivité au nœud de gestionnaire est interrompue	Déclenchée lorsque l'état de connexion du nœud de gestionnaire est inactif.	Connectez-vous à NSX-T Manager et vérifiez la connectivité du gestionnaire du nœud de gestionnaire puis suivez les étapes de dépannage standard recommandées par la documentation de NSX-T et la documentation VMware.
L'utilisation du système de fichiers du nœud de gestionnaire est supérieure à 85 %	Déclenchée lorsque l'utilisation des systèmes de fichiers invités du nœud de gestionnaire est supérieure à 85 %.	L'utilisation du système de fichiers est supérieure à 85. Vérifiez et nettoyez le système de fichiers pour libérer de l'espace.

Tableau 12-1. Alertes dans le pack de gestion pour NSX-T (suite)

Alerte	Description	Recommandation
L'utilisation du système de fichiers du nœud de gestionnaire est supérieure à 75 %	Déclenchée lorsque l'utilisation des systèmes de fichiers invités du nœud de gestionnaire est supérieure à 75 %.	L'utilisation du système de fichiers est supérieure à 75. Vérifiez et nettoyez le système de fichiers pour libérer de l'espace.
L'utilisation du système de fichiers du nœud de gestionnaire est supérieure à 70 %	Déclenchée lorsque l'utilisation des systèmes de fichiers invités du nœud de gestionnaire est supérieure à 70 %.	L'utilisation du système de fichiers est supérieure à 70. Vérifiez et nettoyez le système de fichiers pour libérer de l'espace.

Utilisation de vRealize Network Insight Cloud pour la surveillance du système

Vous pouvez surveiller votre environnement NSX-T Data Center à l'aide de vRealize Network Insight Cloud.

Tableau 12-2. Événements NSX-T calculés de vRealize Network Insight

OID	Nom de l'événement	Gravité par défaut	Nom de l'interface utilisateur	Description
1.3.6.1.4.1.6876.100.1.0.80205	NSXTNoUplinkConnectivityEvent	Avertissement	Événement de déconnexion du routeur logique NSX-T de niveau 1	Le routeur logique NSX-T de niveau 1 est déconnecté du routeur de niveau 0. Les réseaux sous ce routeur ne sont pas accessibles depuis l'extérieur et vice versa.
1.3.6.1.4.1.6876.100.1.0.80206	NSXTRoutingAdvertisementEvent	Avertissement	Annonce de routage désactivée	L'annonce de routage est désactivée pour le routeur logique NSX-T de niveau 1. Les réseaux sous ce routeur ne sont pas accessibles depuis l'extérieur.
1.3.6.1.4.1.6876.100.1.0.80207	NSXTManagerConnectivityDownEvent	Critique	Le nœud NSX-T Edge n'a pas de connectivité au gestionnaire	Le nœud NSX-T Edge a perdu la connectivité au gestionnaire.

Tableau 12-2. Événements NSX-T calculés de vRealize Network Insight (suite)

OID	Nom de l'événement	Gravité par défaut	Nom de l'interface utilisateur	Description
1.3.6.1.4.1.6876.100.1.0.80208	NSXTControllerConnectivityDegradedEvent	Avertissement	Connectivité du contrôleur dégradée pour le nœud Edge NSX-T	Le nœud NSX-T Edge ne peut pas communiquer avec un ou plusieurs contrôleurs.
1.3.6.1.4.1.6876.100.1.0.80209	NSXTControllerConnectivityDownEvent	Critique	Le nœud NSX-T Edge n'a pas de connectivité du contrôleur	Le nœud NSX-T Edge ne peut communiquer avec aucun des contrôleurs.
1.3.6.1.4.1.6876.100.1.0.80210	NSXTMTuMismatchEvent	Avertissement	Discordance de MTU entre NSX-T niveau 0 et commutateur/routeur de liaison montante	Le MTU configuré sur les interfaces du routeur logique de niveau 0 ne correspond pas aux interfaces du commutateur/routeur de liaison montante du même réseau L2. Cela peut avoir un impact sur les performances du réseau.
1.3.6.1.4.1.6876.100.1.0.80211	NSXTExcludedVmFlowEvent	Infos	Une ou plusieurs machines virtuelles exclues du pare-feu DFW NSX-T.	Une ou plusieurs machines virtuelles ne sont pas protégées par le pare-feu DFW NSX-T. vRealize Network Insight ne recevra pas de flux IPFIX pour ces VM.
1.3.6.1.4.1.6876.100.1.0.80212	NSXTDoubleVlanTaggingEvent	Avertissement	Configuration incorrecte du VLAN de liaison montante	La communication est interrompue, car le VLAN sur le port de liaison montante du routeur de niveau 0 est différent du VLAN sur la passerelle externe.
1.3.6.1.4.1.6876.100.1.0.80213	NSXTNoTzAttachedOnTnEvent	Avertissement	Aucune zone de transport n'est attachée au nœud de transport.	Aucune zone de transport attachée au nœud de transport. Les VM peuvent perdre la connectivité à cause de ce problème.

Tableau 12-2. Événements NSX-T calculés de vRealize Network Insight (suite)

OID	Nom de l'événement	Gravité par défaut	Nom de l'interface utilisateur	Description
1.3.6.1.4.1.6876.100.1.0.80214	NSXTVtepDeleteEvent	Avertissement	Aucun VTEP disponible sur le nœud de transport.	Tous les vtep sont supprimés du nœud de transport. Les VM peuvent perdre la connectivité à cause de ce problème.
1.3.6.1.4.1.6876.100.1.0.80225	NSXTControllerNodeToControlClusterConnectivityEvent	Critique	Le nœud de contrôleur NSX-T n'a pas de connectivité de cluster de contrôle	Le nœud de contrôleur NSX-T a perdu la connectivité du cluster de contrôle.
1.3.6.1.4.1.6876.100.1.0.80226	NSXTControllerNodeToMgmtPlaneConnectivityEvent	Critique	Le nœud de contrôleur NSX-T n'a pas de connectivité de plan de gestion	Le nœud de contrôleur NSX-T a perdu la connectivité de plan de gestion.
1.3.6.1.4.1.6876.100.1.0.80227	NSXTMPNodeToMgmtClusterConnectivityEvent	Critique	Le nœud de gestion NSX-T n'a pas de connectivité de cluster de gestion	Le nœud de gestion NSX-T a perdu la connectivité du cluster de gestion.
1.3.6.1.4.1.6876.100.1.0.80246	NSXTHostNodeMgmtConnectivityStatusDownEvent	Avertissement	Le nœud d'hôte NSX-T n'a pas de connectivité au gestionnaire	Désynchronisation entre l'état de la connectivité de NSX Manager avec les nœuds de transport d'hôte
1.3.6.1.4.1.6876.100.1.0.80247	NSXTEdgeNodeCtrlConnectivityStatusUnknownEvent	Critique	La connectivité au contrôleur pour le nœud NSX-T Edge est Inconnu.	La connectivité du contrôleur de nœuds NSX-T Edge est Inconnu.
1.3.6.1.4.1.6876.100.1.0.80248	NSXTHostNodeCtrlConnectivityStatusDownEvent	Avertissement	Le nœud d'hôte NSX-T n'a pas de connectivité du contrôleur	Le nœud hôte NSX-T ne peut communiquer avec aucun des contrôleurs.
1.3.6.1.4.1.6876.100.1.0.80249	NSXTHostNodeCtrlConnectivityStatusDegradedEvent	Avertissement	Connectivité du contrôleur dégradée pour le nœud d'hôte NSX-T	Le nœud d'hôte NSX-T ne peut pas communiquer avec un ou plusieurs contrôleurs.
1.3.6.1.4.1.6876.100.1.0.80250	NSXTHostNodeCtrlConnectivityStatusUnknownEvent	Avertissement	La connectivité du contrôleur de nœuds d'hôte NSX-T est Inconnu.	La connectivité du contrôleur de nœuds d'hôte NSX-T est Inconnu

Tableau 12-2. Événements NSX-T calculés de vRealize Network Insight (suite)

OID	Nom de l'événement	Gravité par défaut	Nom de l'interface utilisateur	Description
1.3.6.1.4.1.6876.100.1.0.80228	NSXTHostNodePnicStatusDownEvent	Avertissement	L'état de la PNIC du nœud de transport d'hôte NSX-T est « Inactif »	L'état de la PNIC du nœud de transport d'hôte NSX-T est « Inactif »
1.3.6.1.4.1.6876.100.1.0.80229	NSXTHostNodePnicStatusDegradedEvent	Avertissement	L'état de la PNIC du nœud de transport d'hôte NSX-T est « Dégradé »	L'état de la PNIC du nœud de transport d'hôte NSX-T est « Dégradé ».
1.3.6.1.4.1.6876.100.1.0.80230	NSXTHostNodePnicStatusUnknownEvent	Avertissement	L'état de la PNIC du nœud de transport d'hôte NSX-T est « Inconnu ».	L'état de la PNIC du nœud de transport d'hôte NSX-T est « Inconnu ».
1.3.6.1.4.1.6876.100.1.0.80237	NSXTEdgeNodePnicStatusDownEvent	Critique	L'état de la PNIC du nœud de transport NSX-T Edge est « Inactif ».	L'état de la PNIC du nœud de transport NSX-T Edge est « Inactif ».
1.3.6.1.4.1.6876.100.1.0.80238	NSXTEdgeNodePnicStatusDegradedEvent	Critique	L'état de la PNIC du nœud de transport NSX-T Edge est « Dégradé ».	L'état de la PNIC du nœud de transport NSX-T Edge est « Dégradé ».
1.3.6.1.4.1.6876.100.1.0.80239	NSXTEdgeNodePnicStatusUnknownEvent	Critique	L'état de la PNIC du nœud de transport NSX-T Edge est « Inconnu ».	L'état de la PNIC du nœud de transport NSX-T Edge est « Inconnu ».
1.3.6.1.4.1.6876.100.1.0.80231	NSXTHostNodeTunnelStatusDownEvent	Avertissement	L'état du tunnel du nœud de transport d'hôte NSX-T est « Inactif ».	L'état du tunnel du nœud de transport d'hôte NSX-T est « Inactif ».
1.3.6.1.4.1.6876.100.1.0.80232	NSXTHostNodeTunnelStatusDegradedEvent	Avertissement	L'état du tunnel du nœud de transport d'hôte NSX-T est « Dégradé ».	L'état du tunnel du nœud de transport d'hôte NSX-T est « Dégradé ».
1.3.6.1.4.1.6876.100.1.0.80233	NSXTHostNodeTunnelStatusUnknownEvent	Avertissement	L'état du tunnel du nœud de transport d'hôte NSX-T est « Inconnu ».	L'état du tunnel du nœud de transport d'hôte NSX-T est « Inconnu ».
1.3.6.1.4.1.6876.100.1.0.80240	NSXTEdgeNodeTunnelStatusDownEvent	Critique	L'état du tunnel du nœud de transport NSX-T Edge est « Inactif ».	L'état du tunnel du nœud de transport NSX-T Edge est « Inactif ».
1.3.6.1.4.1.6876.100.1.0.80241	NSXTEdgeNodeTunnelStatusDegradedEvent	Critique	L'état du tunnel du nœud de transport NSX-T Edge est « Dégradé ».	L'état du tunnel du nœud de transport NSX-T Edge est « Dégradé ».

Tableau 12-2. Événements NSX-T calculés de vRealize Network Insight (suite)

OID	Nom de l'événement	Gravité par défaut	Nom de l'interface utilisateur	Description
1.3.6.1.4.1.6876.100.1.0.80242	NSXTEdgeNodeTunnelStatusUnknownEvent	Critique	L'état du tunnel du nœud de transport NSX-T Edge est « Inconnu ».	L'état du tunnel du nœud de transport NSX-T Edge est « Inconnu ».
1.3.6.1.4.1.6876.100.1.0.80234	NSXTHostNodeStatusDownEvent	Avertissement	L'état du nœud de transport d'hôte NSX-T est « Inactif ».	L'état du nœud de transport d'hôte NSX-T est « Inactif ».
1.3.6.1.4.1.6876.100.1.0.80235	NSXTHostNodeStatusDegradedEvent	Avertissement	L'état du nœud de transport d'hôte NSX-T est « Dégradé ».	L'état du nœud de transport d'hôte NSX-T est « Dégradé ».
1.3.6.1.4.1.6876.100.1.0.80236	NSXTHostNodeStatusUnknownEvent	Avertissement	L'état du nœud de transport d'hôte NSX-T est « Inconnu ».	L'état du nœud de transport d'hôte NSX-T est « Inconnu ».
1.3.6.1.4.1.6876.100.1.0.80243	NSXTEdgeNodeStatusDownEvent	Critique	L'état du nœud de transport NSX-T Edge est « Inactif ».	L'état du nœud de transport NSX-T Edge est « Inactif ».
1.3.6.1.4.1.6876.100.1.0.80244	NSXTEdgeNodeStatusDegradedEvent	Critique	L'état du nœud de transport NSX-T Edge est « Dégradé ».	L'état du nœud de transport NSX-T Edge est « Dégradé ».
1.3.6.1.4.1.6876.100.1.0.80245	NSXTEdgeNodeStatusUnknownEvent	Critique	L'état du nœud de transport NSX-T Edge est « Inconnu ».	L'état du nœud de transport NSX-T Edge est « Inconnu ».
1.3.6.1.4.1.6876.100.1.0.80252	NSXTLogicalSwitchAdminStatusDownEvent	Avertissement	L'état d'administration du commutateur logique NSX-T est « Inactif ».	L'état d'administration du commutateur logique NSX-T est « Inactif ».
1.3.6.1.4.1.6876.100.1.0.80253	NSXTLogicalPortOperationalStatusDownEvent	Critique	L'état opérationnel du port logique NSX-T est « Inactif »	L'état opérationnel du port logique NSX-T est « Inactif ». Cela peut entraîner un échec de communication entre deux interfaces virtuelles connectées au même commutateur logique. Par exemple, vous ne pouvez pas effectuer un test ping d'une machine virtuelle à partir d'une autre.

Tableau 12-2. Événements NSX-T calculés de vRealize Network Insight (suite)

OID	Nom de l'événement	Gravité par défaut	Nom de l'interface utilisateur	Description
1.3.6.1.4.1.6876.100.1.0.80254	NSXTLogicalPortOperationalStatusUnknownEvent	Avertissement	L'état opérationnel du port logique NSX-T est « Inconnu »	L'état opérationnel du port logique NSX-T est « Inconnu ». Cela peut entraîner un échec de communication entre deux interfaces virtuelles connectées au même commutateur logique. Par exemple, vous ne pouvez pas effectuer un test ping d'une machine virtuelle à partir d'une autre.
1.3.6.1.4.1.6876.100.1.0.80255	NSXTComputeManagerConnectionStatusNotUpEvent	Avertissement	L'état de la connexion du gestionnaire de calcul NSX-T n'est pas actif	L'état de la connexion du gestionnaire de calcul NSX-T n'est pas actif
1.3.6.1.4.1.6876.100.1.0.80256	NSXTClusterBackupDisabledEvent	Avertissement	La sauvegarde de NSX-T Manager n'est pas planifiée.	La sauvegarde de NSX-T Manager n'est pas planifiée
1.3.6.1.4.1.6876.100.1.0.80257	NSXTDFWFirewallDisabledEvent	Critique	Le pare-feu DFW NSX-T est désactivé.	Le pare-feu distribué est désactivé dans NSX-T Manager
1.3.6.1.4.1.6876.100.1.0.80258	NSXTLogicalPortReceivedPacketDropEvent	Avertissement	Les paquets reçus du port logique NSX-T sont abandonnés.	Les paquets reçus sont abandonnés sur le port logique NSX-T ; les entités associées peuvent être affectées
1.3.6.1.4.1.6876.100.1.0.80259	NSXTLogicalPortTransmittedPacketDropEvent	Avertissement	Les paquets transmis du port logique NSX-T sont abandonnés.	Les paquets transmis sont abandonnés sur le port logique NSX-T ; les entités associées peuvent être affectées
1.3.6.1.4.1.6876.100.1.0.80260	NSXTLogicalSwitchReceivedPacketDropEvent	Avertissement	Les paquets reçus du commutateur logique NSX-T sont abandonnés	Les paquets reçus sont abandonnés sur le commutateur logique NSX-T ; les entités associées peuvent être affectées

Tableau 12-2. Événements NSX-T calculés de vRealize Network Insight (suite)

OID	Nom de l'événement	Gravité par défaut	Nom de l'interface utilisateur	Description
1.3.6.1.4.1.6876.100.1.0.80261	NSXTLogicalSwitchTransmittedPacketDropEvent	Avertissement	Les paquets transmis du commutateur logique NSX-T sont abandonnés	Les paquets transmis sont abandonnés sur le commutateur logique NSX-T ; les entités associées peuvent être affectées
1.3.6.1.4.1.6876.100.1.0.80262	NSXTRxPacketDropOnMPNicEvent	Avertissement	Les paquets reçus sont abandonnés sur l'interface réseau du nœud de gestion NSX-T	Les paquets reçus sont abandonnés sur l'interface réseau du nœud de gestion NSX-T. Cela peut avoir un impact sur le trafic réseau lié au cluster de gestion NSX-T.
1.3.6.1.4.1.6876.100.1.0.80263	NSXTRxPacketDropOnEdgeTnNicEvent	Critique	Les paquets reçus sont abandonnés sur l'interface réseau du nœud NSX-T Edge	Les paquets reçus sont abandonnés sur l'interface réseau du nœud NSX-T Edge. Cela peut avoir un impact sur le trafic réseau du cluster Edge.
1.3.6.1.4.1.6876.100.1.0.80264	NSXTRxPacketDropOnHostTnNicEvent	Avertissement	Les paquets reçus sont abandonnés sur l'interface réseau du nœud d'hôte NSX-T	Les paquets reçus sont abandonnés sur l'interface réseau du nœud d'hôte NSX-T. Cela peut affecter le trafic réseau sur l'hôte ESXi.
1.3.6.1.4.1.6876.100.1.0.80265	NSXTTxPacketDropOnMPNicEvent	Avertissement	Les paquets transmis sont abandonnés sur l'interface réseau du nœud de gestion NSX-T	Les paquets transmis sont abandonnés sur l'interface réseau du nœud de gestion NSX-T. Cela peut avoir un impact sur le trafic réseau lié au cluster de gestion NSX-T.
1.3.6.1.4.1.6876.100.1.0.80266	NSXTTxPacketDropOnEdgeTnNicEvent	Critique	Les paquets transmis sont abandonnés sur l'interface réseau du nœud NSX-T Edge	Les paquets transmis sont abandonnés sur l'interface réseau du nœud NSX-T Edge. Cela peut avoir un impact sur le trafic réseau du cluster Edge.

Tableau 12-2. Événements NSX-T calculés de vRealize Network Insight (suite)

OID	Nom de l'événement	Gravité par défaut	Nom de l'interface utilisateur	Description
1.3.6.1.4.1.6876.100.1.0.80267	NSXTTxPacketDropOnHostTnNicEvent	Avertissement	Les paquets transmis sont abandonnés sur l'interface réseau du nœud d'hôte NSX-T	Les paquets transmis sont abandonnés sur l'interface réseau du nœud d'hôte NSX-T. Cela peut affecter le trafic réseau sur l'hôte ESXi.
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeServiceCmlInventoryStatusEvent	Avertissement	Le service d'inventaire CM a cessé de fonctionner	L'état du service d'inventaire CM est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeServiceControllerStatusEvent	Avertissement	Le service de contrôleur a cessé de fonctionner.	L'état du service de contrôleur est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeServiceDataStoreStatusEvent	Avertissement	Le service de banque de données a cessé de fonctionner.	L'état du service de banque de données est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeServiceHttpStatusEvent	Avertissement	Le service HTTP a cessé de fonctionner.	L'état du service HTTP est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeServiceInstallUpgradeEvent	Avertissement	L'installation du service de mise à niveau a cessé de fonctionner.	L'état de l'installation du service de mise à niveau est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeServiceLiagentStatusEvent	Avertissement	Le service Liagent a cessé de fonctionner.	L'état du service Liagent est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeServiceManagerStatusEvent	Avertissement	Le service de gestionnaire a cessé de fonctionner.	L'état du service de gestionnaire est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeServiceMgmtPlaneBusStatusEvent	Avertissement	Le service de plan de gestion a cessé de fonctionner.	L'état du service de gestion est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeServiceMigrationCoordinatorStatusEvent	Avertissement	Le service de coordinateur de migration a cessé de fonctionner.	L'état du service de coordinateur de migration est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeServiceNodeMgmtStatusEvent	Avertissement	Le service de gestion de nœud a cessé de fonctionner.	L'état du service de gestion de nœud est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeServiceNodeStatsStatusEvent	Avertissement	Le service de statistiques du nœud a cessé de fonctionner.	L'état du service de statistiques du nœud est devenu arrêté.

Tableau 12-2. Événements NSX-T calculés de vRealize Network Insight (suite)

OID	Nom de l'événement	Gravité par défaut	Nom de l'interface utilisateur	Description
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeService NSXMessageBusStatusEvent	Avertissement	Le service du bus de messages a cessé de fonctionner.	L'état du service client du bus de messages est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeService NSXPlatformClientStatusEvent	Avertissement	Le service du client de plate-forme s'est arrêté.	L'état du service du client de plate-forme est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeService NSXUpgradeAgentStatusEvent	Avertissement	Le service de mise à niveau de l'agent a cessé de fonctionner.	L'état du service de mise à niveau est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeService NTPStatusEvent	Avertissement	Le service NTP a cessé de fonctionner.	L'état du service NTP est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeService PolicyStatusEvent	Avertissement	Le service de stratégie s'est arrêté.	L'état du service de stratégie est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeService SearchStatusEvent	Avertissement	Le service de recherche s'est arrêté.	L'état du service de recherche est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeService SNMPStatusEvent	Avertissement	Le service SNMP s'est arrêté.	L'état du service SNMP est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeService SSHStatusEvent	Avertissement	Le service SSH s'est arrêté.	L'état du service SSH est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeService SyslogStatusEvent	Avertissement	Le service Syslog s'est arrêté.	L'état du service Syslog est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeService TelemetryStatusEvent	Avertissement	Le service de télémétrie s'est arrêté.	L'état du service de télémétrie est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeService UIServiceStatusEvent	Avertissement	Le service d'interface utilisateur s'est arrêté.	L'état du service d'interface utilisateur est devenu arrêté.
1.3.6.1.4.1.6876.100.1.0.80402	NSXTMPNodeService CmInventoryStatusEvent	Critique	Le service d'inventaire CM s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service d'inventaire CM a cessé de s'exécuter.

Tableau 12-2. Événements NSX-T calculés de vRealize Network Insight (suite)

OID	Nom de l'événement	Gravité par défaut	Nom de l'interface utilisateur	Description
1.3.6.1.4.1.6876.100.1.0.80403	NSXTMPNodeService ControllerStatusEvent	Critique	Le service de contrôleur s'est arrêté.	L'un des services du nœud de gestion NSX-T, à savoir le service de contrôleur a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80404	NSXTMPNodeService DataStoreStatusEvent	Critique	Le service de banque de données s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service de banque de données a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80405	NSXTMPNodeService HttpStatusEvent	Critique	Le service HTTP s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service HTTP a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80406	NSXTMPNodeService InstallUpgradeEvent	Avertissement	Le service de mise à niveau de l'installation s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service de mise à niveau de l'installation a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80407	NSXTMPNodeService LiagentStatusEvent	Avertissement	Le service Liagent s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service LI Agent a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80408	NSXTMPNodeService ManagerStatusEvent	Critique	Le service du gestionnaire s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service du gestionnaire a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80409	NSXTMPNodeService MgmtPlaneBusStatus Event	Avertissement	Le service du plan de gestion s'est arrêté	L'un des services du nœud de gestion de NSX-T, à savoir le service de bus du plan de gestion, a cessé de s'exécuter.

Tableau 12-2. Événements NSX-T calculés de vRealize Network Insight (suite)

OID	Nom de l'événement	Gravité par défaut	Nom de l'interface utilisateur	Description
1.3.6.1.4.1.6876.100.1.0.80410	NSXTMPNodeService MigrationCoordinator StatusEvent	Avertissement	Le service de coordinateur de migration s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service de coordinateur de migration, a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80411	NSXTMPNodeService NodeMgmtStatusEvent	Critique	Le service de gestion des nœuds s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service de gestion des nœuds a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80412	NSXTMPNodeService NodeStatsStatusEvent	Critique	Le service de statistiques de nœud s'est arrêté	L'un des services du nœud de gestion de NSX-T, à savoir le service de statistiques du nœud, a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80413	NSXTMPNodeService NSXMessageBusStatusEvent	Avertissement	Le service du bus de messages s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service de bus de messages a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80414	NSXTMPNodeService NSXPlatformClientStatusEvent	Critique	Le service client de la plate-forme s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service client de la plate-forme a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80415	NSXTMPNodeService NSXUpgradeAgentStatusEvent	Avertissement	Le service de mise à niveau de l'agent s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service de mise à niveau de l'agent a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80416	NSXTMPNodeService NTPStatusEvent	Critique	Le service NTP s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service NTP a cessé de s'exécuter.

Tableau 12-2. Événements NSX-T calculés de vRealize Network Insight (suite)

OID	Nom de l'événement	Gravité par défaut	Nom de l'interface utilisateur	Description
1.3.6.1.4.1.6876.100.1.0.80417	NSXTMPNodeServicePolicyStatusEvent	Critique	Le service de stratégie s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service de stratégie a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80418	NSXTMPNodeServiceSearchStatusEvent	Critique	Le service de recherche s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service de recherche a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80419	NSXTMPNodeServiceSNMPStatusEvent	Avertissement	Le service SNMP s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service SNMP a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80420	NSXTMPNodeServiceSSHStatusEvent	Critique	Le service SSH s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service SSH a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80421	NSXTMPNodeServiceSyslogStatusEvent	Critique	Le service Syslog s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service Syslog a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80422	NSXTMPNodeServiceTelemetryStatusEvent	Avertissement	Le service de télémétrie s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service de télémétrie a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80423	NSXTMPNodeServiceUIServiceStatusEvent	Critique	Le service d'interface utilisateur s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service d'interface utilisateur a cessé de s'exécuter.
1.3.6.1.4.1.6876.100.1.0.80424	NSXTMPNodeServiceClusterManagerStatusEvent	Critique	Le service du gestionnaire de clusters s'est arrêté	L'un des services du nœud de gestion NSX-T, à savoir le service du gestionnaire de clusters a cessé de s'exécuter.

Événements système NSX-T

Voici la liste des événements NSX-T 2.2 à 2.5 pris en charge dans vRealize Network Insight. L'ID d'objet (OID) de tous ces événements système NSX-T est 1.3.6.1.4.1.6876.100.1.0.80203.

Tableau 12-3. Événements système NSX-T

Nom de l'événement	Description
vmwNSXPlatformSysCpuUsage	Utilisation du CPU sur les dispositifs Manager et Edge (NSX-T 2.2).
vmwNSXPlatformSysDiskUsage	Utilisation de l'espace disque sur les dispositifs Manager et Edge pour la partition /var/log (NSX-T 2.2).
vmwNSXPlatformSysMemUsage	Utilisation de la mémoire sur les dispositifs Manager et Edge (NSX-T 2.2).
vmwNSXPlatformSysConfigDiskUsage	Utilisation du disque pour les dispositifs Manager et Edge pour la partition /config (NSX-T 2.4).
vmwNSXPlatformSysVarDumpDiskUsage	Utilisation du disque pour les dispositifs Manager et Edge pour la partition /var/dump (NSX-T 2.5).
vmwNSXPlatformSysRepositoryDiskUsage	Utilisation du disque pour les dispositifs Gestionnaire et Edge pour la partition /repository (NSX-T 2.5).
vmwNSXPlatformSysRootDiskUsage	Utilisation du disque pour les dispositifs Manager et Edge pour la partition racine (NSX-T 2.5).
vmwNSXPlatformSysTmpDiskUsage	Utilisation du disque pour les dispositifs Manager et Edge pour la partition tmp (NSX-T 2.5).
vmwNSXPlatformSysImageDiskUsage	Utilisation du disque pour les dispositifs Manager et Edge pour la partition /image (NSX-T 2.5).
vmwNSXDhcpPoolUsageOverloadedEvent	Pool DHCP surchargé/normal (NSX-T 2.5).
vmwNSXDhcpPoolLeaseAllocationFailedEvent	Échec/réussite de l'allocation du bail de pool DHCP (NSX-T 2.5).
vmwNSXPlatformPasswordExpiryStatus	Expiration du mot de passe de Manager (NSX-T 2.4).
vmwNSXPlatformCertificateExpiryStatus	Expiration du certificat de Manager (NSX-T 2.4).
vmwNSXRoutingBgpNeighborStatus	État du voisin BGP (NSX-T 2.2).
vmwNSXVpnTunnelState	Tunnel VPN actif/inactif (NSX-T 2.2).
vmwNSXVpnL2TunnelStatus	Session VPN L2 active/inactive (NSX-T 2.2).
vmwNSXVpnIkeSessionStatus	Session IKE active/inactive (NSX-T 2.2).
vmwNSXDnsForwarderStatus	État du redirecteur DNS (NSX-T 2.4).
vmwNSXClusterNodeStatus	État du nœud de cluster (NSX-T 2.4).
vmwNSXFabricCryptoStatus	Le pilote Edge crypto mux a échoué/réussi Known_Answer_Tests(KAT) (NSX-T 2.4).
L'utilisation du disque de Manager n'est pas correcte	

Tableau 12-3. Événements système NSX-T (suite)

Nom de l'événement	Description
Le voisin BGP est inactif.	Une alerte est nécessaire lorsque le voisin BGP est inactif.
Voisin BGP actif.	Effacez l'alarme lorsqu'un voisin s'affiche.
Utilisation du stockage sur X	L'alarme de stockage sur X-Event est déclenchée pour toutes les machines virtuelles de dispositif (MP, CCP) ou tous les nœuds de transport (Edge, hôte).
Utilisation de la mémoire sur X	L'alarme de mémoire sur X-Event est déclenchée pour toutes les machines virtuelles de dispositif (MP, CCP) ou tous les nœuds de transport (Edge, hôte).
Utilisation du CPU sur X	L'alarme pour le CPU sur X-Event est déclenchée pour toutes les machines virtuelles de dispositif (MP, CCP) ou tous les nœuds de transport (Edge, hôte).

Outils de surveillance avancés

NSX-T prend en charge les méthodes de surveillance avancées, notamment l'affichage des connexions de port, Traceflow, la mise en miroir de ports, la surveillance des activités, etc.

Afficher les informations de connexion au port

Vous pouvez utiliser l'outil de connexion au 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > 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 au port s'affiche. Vous pouvez cliquer sur n'importe quel composant de la carte pour afficher davantage d'informations le concernant.

Traceflow

Traceflow vous permet d'injecter un paquet dans le réseau et de surveiller son flux sur le réseau. Ce flux vous permet de surveiller votre réseau et d'identifier des problèmes, tels que des goullets d'étranglement ou des interruptions.

Traceflow vous permet d'identifier le ou les chemins empruntés par un paquet pour atteindre sa destination ou, à l'inverse, à quel endroit est déposé un paquet sur le chemin. Chaque entité signale le traitement du paquet en entrée et en sortie, ce qui vous permet de déterminer si des erreurs se produisent à sa réception ou à son transfert.

Traceflow est différent d'une demande/réponse ping qui passe d'une pile de VM invitées à une autre. Traceflow observe un paquet marqué lorsqu'il traverse le réseau de superposition, et chaque paquet est surveillé lorsqu'il traverse le réseau de superposition jusqu'à ce qu'il atteigne une VM invitée de destination ou une liaison montante Edge. Notez que le paquet marqué injecté n'est jamais réellement remis à la VM invitée de destination.

Traceflow peut être utilisé sur des nœuds de transport et prend en charge les protocoles IPV4 et IPV6, notamment : ICMP, TCP, UDP, DHCP, DNS et ARP/NDP.

Vous pouvez créer des paquets avec des champs d'en-tête et des tailles de paquet personnalisés. La source ou la destination de Traceflow peut être un port de commutateur logique, un port de liaison montante de routeur logique, un CSP ou un port DHCP. Le point de terminaison de destination peut être n'importe quel périphérique du réseau NSX superposé ou sous-jacent. Toutefois, vous ne pouvez pas sélectionner une destination à l'extérieur d'un nœud NSX Edge. La destination doit se trouver sur le même sous-réseau ou être accessible via des routeurs logiques distribués NSX.

Si le pontage NSX est configuré, les paquets ayant des adresses MAC de destination inconnues sont toujours envoyés au pont. Généralement, le pont transmet ces paquets à un VLAN et signale que le paquet Traceflow est livré. Un paquet signalé comme livré ne signifie pas nécessairement que le paquet de suivi a été remis à la destination spécifiée.

Les observations de Traceflow peuvent inclure des observations de paquets de Traceflow diffusés. L'hôte ESXi diffuse un paquet Traceflow s'il ne connaît pas l'adresse MAC de l'hôte de destination. Pour le trafic de diffusion, la source est une vNIC de machine virtuelle. L'adresse MAC de destination de couche 2 du trafic de diffusion est FF:FF:FF:FF:FF:FF. Pour créer un paquet valide pour l'inspection de pare-feu, l'opération Traceflow de diffusion nécessite une longueur de préfixe de sous-réseau. Le masque de sous-réseau permet à NSX de calculer une adresse réseau IP pour le paquet.

Suivre le chemin d'un paquet avec Traceflow

Utilisez Traceflow pour inspecter le chemin d'accès d'un paquet. Traceflow suit le chemin d'accès au niveau du nœud de transport d'un paquet. 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Outils > Traceflow**.

3 Sélectionnez un type d'adresse IPv4 ou IPv6.

4 Sélectionnez un type de trafic.

Pour les adresses IPv4, les choix de types de trafic sont Monodiffusion, Multidiffusion et Diffusion. Pour l'adresse IPv6, les choix de type de trafic sont Monodiffusion et Multidiffusion.

Remarque : la multidiffusion et la diffusion ne sont pas prises en charge dans un environnement VMware Cloud (VMC).

5 Spécifiez les informations sur la source et la destination en fonction du type de trafic.

Type de trafic	Source	Destination
Monodiffusion	<p>Sélectionnez une machine virtuelle ou un port logique. Pour une machine virtuelle :</p> <ul style="list-style-type: none"> ■ Sélectionnez une machine virtuelle dans la liste déroulante. ■ Sélectionnez une interface virtuelle. ■ 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'adresses seront utilisées dans ce cas). Si la VM dispose de plusieurs adresses IP, sélectionnez-en une dans la liste déroulante. ■ Si l'adresse IP et l'adresse MAC ne sont pas affichées, entrez-les dans les zones de texte. <p>Pour un port logique :</p> <ul style="list-style-type: none"> ■ Sélectionnez un type d'attachement : VIF, DHCP, Liaison montante Edge ou Service centralisé Edge. ■ Sélectionnez un port. 	<p>Sélectionnez une machine virtuelle, un port logique ou une adresse IP-MAC. Pour une machine virtuelle :</p> <ul style="list-style-type: none"> ■ Sélectionnez une machine virtuelle dans la liste déroulante. ■ Sélectionnez une interface virtuelle. ■ 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'adresses seront utilisées dans ce cas). Si la VM dispose de plusieurs adresses IP, sélectionnez-en une dans la liste déroulante. ■ Si l'adresse IP et l'adresse MAC ne sont pas affichées, entrez-les dans les zones de texte. <p>Pour un port logique :</p> <ul style="list-style-type: none"> ■ Sélectionnez un type d'attachement : VIF, DHCP, Liaison montante Edge ou Service centralisé Edge. ■ Sélectionnez un port. <p>Pour une adresse IP-MAC :</p> <ul style="list-style-type: none"> ■ Sélectionnez le type de suivi (couche 2 ou couche 3). Pour la couche 2, entrez une adresse IP et une adresse MAC. Pour la 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.

6 (Facultatif) Cliquez sur **Avancé** pour voir les options avancées.

- 7 (Facultatif) Dans la colonne de gauche, entrez les valeurs souhaitées pour les champs suivants :

Option	Description
Taille de la trame	La valeur par défaut est 128.
TTL	La valeur par défaut est 64.
Délai d'expiration (ms)	La valeur par défaut est 10000.
EtherType	La valeur par défaut est 2048.
Type de charge utile	Sélectionnez Base64 , Hex , TexteBrut , Binaire ou Décimal .
Données relatives à la charge utile	Charge utile mise en forme en fonction du type sélectionné.

- 8 (Facultatif) Sélectionnez un protocole et fournissez les informations correspondantes.

Protocole	Paramètres
TCP	Spécifiez un port source, un port de destination et des indicateurs TCP.
UDP	Spécifiez un port source et un port de destination.
ICMPv6	Spécifiez un ID ICMP et une séquence.
ICMP	Spécifiez un ID ICMP et une séquence.
DHCPv6	Sélectionnez un type de message DHCP : Solliciter , Annoncer , Demander ou Répondre .
DHCP	Sélectionnez un code OP DHCP : Demande de démarrage ou Réponse de démarrage .
DNS	Spécifiez une adresse et sélectionnez un type de message : Requête ou Réponse .

- 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.

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.

Notez que SPAN logique est pris en charge uniquement pour les commutateurs logiques de superposition et pas pour les commutateurs logiques VLAN.

NSX Cloud Note Si vous utilisez NSX Cloud, consultez [Fonctionnalités de NSX-T Data Center prises en charge avec NSX Cloud](#) pour obtenir la liste des entités logiques générées automatiquement, des fonctionnalités prises en charge et des 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.
- 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.
- Pour une session SPAN locale, les ports source et de destination de la session de mise en miroir doivent se trouver sur le même vSwitch d'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://<nsx-manager-ip-address>>.
- 2 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 3 Sélectionnez **Mise en réseau et sécurité avancées > Outils > Session de mise en miroir de ports**.
- 4 Cliquez sur **Ajouter** et sélectionnez un type de session.
Les types disponibles sont **SPAN local**, **SPAN distant**, **SPLAN L3 distant** et **SPAN logique**.
- 5 Entrez un nom de session et éventuellement une description.

6 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. 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.

7 Cliquez sur **Suivant**.

8 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.

9 Cliquez sur **Suivant**.

10 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.

11 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.

Configurer des filtres pour une session de mise en miroir de ports

Vous pouvez configurer des filtres pour des sessions de mise en miroir de ports afin de limiter la quantité de données qui sont mises en miroir.

Cette fonctionnalité présente les capacités et restrictions suivantes :

- Seuls les nœuds de transport hôtes ESXi et KVM sont pris en charge.
- L'adresse IP, le préfixe d'adresse IP et les plages d'adresses IP sont pris en charge pour la source et la destination.
- IPSet n'est pas pris en charge pour la source ou la destination.
- Les statistiques de mise en miroir sur ESXi ou KVM ne sont pas prises en charge.

Vous devez configurer des filtres à l'aide de l'API. L'utilisation de l'interface utilisateur de NSX Manager n'est pas prise en charge. Pour plus d'informations sur l'API de mise en miroir de ports et le schéma `PortMirroringFilter`, reportez-vous à la section *Référence de l'API NSX-T Data Center*.

Procédure

- 1 Configurez une session de mise en miroir de ports en utilisant l'interface utilisateur ou l'API de NSX Manager.
- 2 Appelez l'API GET `/api/v1/mirror-sessions` pour obtenir des informations sur la session de mise en miroir de ports.
- 3 Appelez l'API GET `/api/v1/mirror-sessions/<mirror-session-id>` pour ajouter un ou plusieurs filtres. Par exemple,

```
PUT https://<nsx-mgr>/api/v1/mirror-sessions/e57e8b2d-3047-4550-b230-dd1ee0e10b49
{
  "resource_type": "PortMirroringSession",
  "id": "e57e8b2d-3047-4550-b230-dd1ee0e10b49",
```

```

"display_name": "port-mirror-session-1",
"description": "Pnic port mirror session 1",
"mirror_sources": [
  {
    "resource_type": "LogicalPortMirrorSource",
    "port_ids": [
      "6a361832-43e4-430d-a48a-b84a6cba73c3"
    ]
  }
],
"mirror_destination": {
  "resource_type": "LogicalPortMirrorDestination",
  "port_ids": [
    "3e42e8b2d-3047-4550-b230-dd1ee0e10b34"
  ]
},
"port_mirroring_filters": [
  {
    "filter_action": "MIRROR",
    "src_ips": {
      "ip-addresses": [
        "192.168.175.250",
        "2001:bd6::c:2957:160:126"
      ]
    },
    "dst_ips": {
      "ip-addresses": [
        "192.168.160.126",
        "2001:bd6::c:2957:175:250"
      ]
    }
  }
],
"session_type": "LogicalPortMirrorSession",
"preserve_original_vlan": false,
"direction": "BIDIRECTIONAL",
"_revision": 0
}

```

- 4 (Facultatif) Vous pouvez appeler la commande d'interface de ligne de commande `get mirroring-session <session-number>` pour afficher les propriétés de la session, y compris les filtres de mise en miroir de ports.

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.

NSX Cloud Note Si vous utilisez NSX Cloud, consultez [Fonctionnalités de NSX-T Data Center prises en charge avec NSX Cloud](#) pour obtenir la liste des entités logiques générées automatiquement, des fonctionnalités prises en charge et des configurations requises pour NSX Cloud.

Cette fonctionnalité est conforme aux normes spécifiées dans RFC 7011 et RFC 7012.

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.

Configurer des collecteurs IPFIX de commutateurs

Vous pouvez configurer des collecteurs IPFIX pour des commutateurs.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Outils > IPFIX**.
- 3 Cliquez sur l'onglet **Collecteurs IPFIX de commutateurs**.
- 4 Cliquez sur **Ajouter** pour ajouter un collecteur.
- 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 **Ajouter**.

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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Outils > IPFIX**.
- 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. Note Si vous souhaitez créer un profil global, nommez le profil Global . Un profil global ne peut pas être modifié ou supprimé de l'interface utilisateur, mais vous pouvez le faire à l'aide d'API NSX-T Data Center.
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.
Exporter le flux de superposition	Paramètre qui contrôle si le résultat de l'exemple inclut des informations de flux de superposition.
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 **Ajouter**.

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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Outils > IPFIX**.
- 3 Cliquez sur l'onglet **Collecteurs IPFIX de pare-feu**.
- 4 Cliquez sur **Ajouter** pour ajouter un collecteur.
- 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 **Ajouter**.

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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Outils > IPFIX**.
- 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. Note Si vous souhaitez créer un profil global, nommez le profil Global . Un profil global ne peut pas être modifié ou supprimé de l'interface utilisateur, mais vous pouvez le faire à l'aide d'API NSX-T Data Center.
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.

Paramètre	Description
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 **Ajouter**.

Modèles IPFIX ESXi

Un nœud de transport d'hôte ESXi prend en charge huit modèles de flux IPFIX de commutateur logique et deux modèles de flux IPFIX de pare-feu distribué.

Le tableau suivant répertorie les éléments spécifiques à VMware dans les paquets IPFIX de commutateurs logiques.

ID d'élément	Nom du paramètre	Type de données	Unité
880	tenantProtocol	unsigned8	1 octet
881	tenantSourceIPv4	ipv4Address	4 octets
882	tenantDestIPv4	ipv4Address	4 octets
883	tenantSourceIPv6	ipv6Address	16 octets
884	tenantDestIPv6	ipv6Address	16 octets
886	tenantSourcePort	unsigned16	2 octets
887	tenantDestPort	unsigned16	2 octets
888	egressInterfaceAttr	unsigned16	2 octets
889	vlanExportRole	unsigned8	1 octet
890	ingressInterfaceAttr	unsigned16	2 octets
898	virtualObsID	string	longueur variable

Le tableau suivant répertorie les éléments spécifiques à VMware dans les paquets IPFIX de pare-feu distribués.

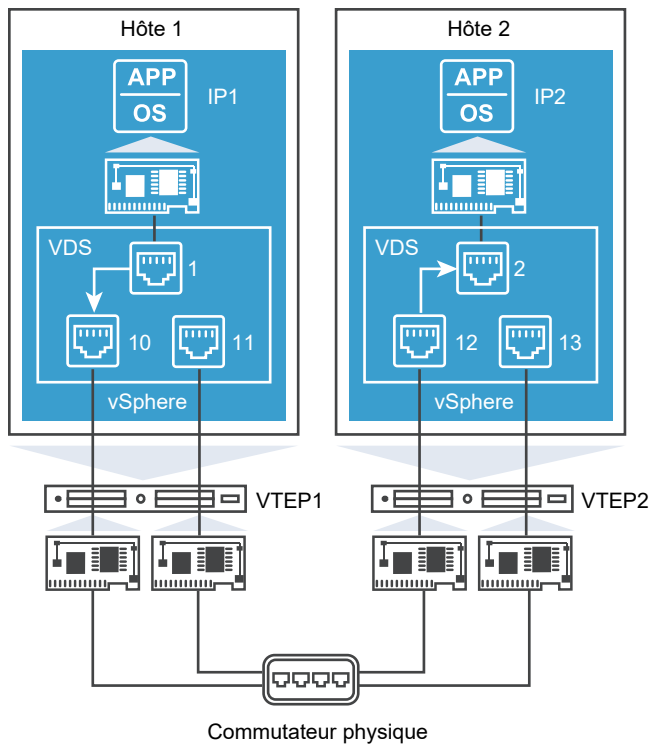
ID d'élément	Nom du paramètre	Type de données	Unité
950	ruleId	unsigned32	4 octets
951	vmUuid	string	16 octets
952	vnidIndex	unsigned32	4 octets
953	sessionFlags	unsigned8	1 octet

ID d'élément	Nom du paramètre	Type de données	Unité
954	flowDirection	unsigned8	1 octet
955	algControlFlowId	unsigned64	8 octets
956	algType	unsigned8	1 octet
957	algFlowType	unsigned8	1 octet
958	averageLatency	unsigned32	4 octets
959	retransmissionCount	unsigned32	4 octets
960	vifUuid	octetArray	16 octets
961	vifId	string	longueur variable

Modèles IPFIX de commutateur logique ESXi

Un nœud de transport hôte ESXi prend en charge huit modèles de flux IPFIX de commutateur logique.

Le diagramme suivant montre le flux du trafic entre les machines virtuelles attachées à des hôtes ESXi surveillés par la fonctionnalité IPFIX :



Le modèle IPv4 encapsulé aura les éléments suivants :

- éléments standard
- SrcAddr : VTEP1

- DstAddr : VTEP2
- tenantSourceIPv4 : IP1
- tenantDestIPv4 : IP2
- tenantSourcePort : 10000
- tenantDestPort : 80
- tenantProtocol : TCP
- ingressInterfaceAttr : 0x03 (port de tunnel)
- egressInterfaceAttr : 0x01
- encapExportRole : 01
- virtualObsID : 89fd5032-2dc9-4fc3-993a-9bb4b616de54 (ID de port logique)

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 de pare-feu distribué ESXi

Un nœud de transport hôte ESXi prend en charge deux modèles de flux IPFIX de pare-feu distribué.

Modèle IPv4

ID de modèle : 288

```
IPFIX_TEMPLATE_FIELD(sourceIPv4Address,4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address,4)
IPFIX_TEMPLATE_FIELD(sourceTransportPort,2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort,2)
IPFIX_TEMPLATE_FIELD(protocolIdentifier,1)
IPFIX_TEMPLATE_FIELD(icmpTypeIPv4,1)
IPFIX_TEMPLATE_FIELD(icmpCodeIPv4,1)
IPFIX_TEMPLATE_FIELD(flowStartSeconds,4)
IPFIX_TEMPLATE_FIELD(flowEndSeconds,4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(firewallEvent,1)
IPFIX_TEMPLATE_FIELD(direction,1)
IPFIX_TEMPLATE_FIELD(ruleId,4)
IPFIX_TEMPLATE_FIELD(vifUuid,16)
IPFIX_TEMPLATE_FIELD(sessionFlags,1)
IPFIX_TEMPLATE_FIELD(flowDirection,1)
IPFIX_TEMPLATE_FIELD(flowId,8)
IPFIX_TEMPLATE_FIELD(algControlFlowId,8)
IPFIX_TEMPLATE_FIELD(algType,1)
IPFIX_TEMPLATE_FIELD(algFlowType,1)
IPFIX_TEMPLATE_FIELD(averageLatency,4)
IPFIX_TEMPLATE_FIELD(retransmissionCount,4)
```

Modèle IPv6

ID de modèle : 289

```
IPFIX_TEMPLATE_FIELD(sourceIPv6Address,16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address,16)
IPFIX_TEMPLATE_FIELD(sourceTransportPort,2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort,2)
IPFIX_TEMPLATE_FIELD(protocolIdentifier,1)
IPFIX_TEMPLATE_FIELD(icmpTypeIPv6,1)
IPFIX_TEMPLATE_FIELD(icmpCodeIPv6,1)
IPFIX_TEMPLATE_FIELD(flowStartSeconds,4)
IPFIX_TEMPLATE_FIELD(flowEndSeconds,4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount,8)
IPFIX_TEMPLATE_FIELD(firewallEvent,1)
IPFIX_TEMPLATE_FIELD(direction,1)
IPFIX_TEMPLATE_FIELD(ruleId,4)
IPFIX_TEMPLATE_FIELD(vifUuid,16)
IPFIX_TEMPLATE_FIELD(sessionFlags,1)
IPFIX_TEMPLATE_FIELD(flowDirection,1)
IPFIX_TEMPLATE_FIELD(flowId,8)
IPFIX_TEMPLATE_FIELD(algControlFlowId,8)
IPFIX_TEMPLATE_FIELD(algType,1)
IPFIX_TEMPLATE_FIELD(algFlowType,1)
IPFIX_TEMPLATE_FIELD(averageLatency,4)
IPFIX_TEMPLATE_FIELD(retransmissionCount,4)
```

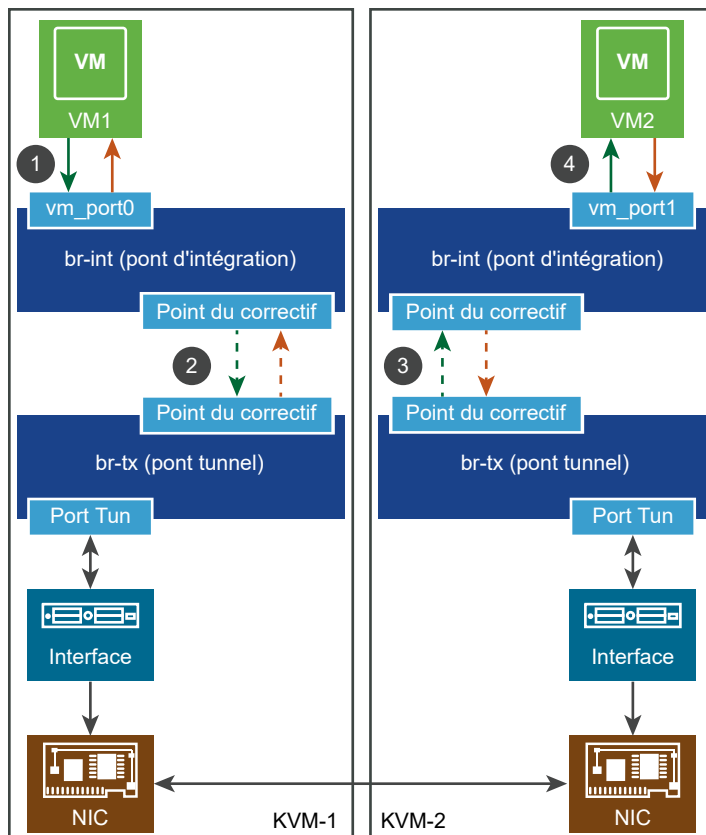

Modèles IPFIX KVM

Un nœud de transport hôte KVM prend en charge 88 modèles de flux IPFIX et un modèle d'options.

Le tableau suivant répertorie les éléments spécifiques à VMware dans les paquets IPFIX KVM.

ID d'élément	Nom du paramètre	Type de données	Unité
891	tunnelType	unsigned8	1 octet
892	tunnelKey	octets	longueur variable
893	tunnelSourceIPv4Address	unsigned32	4 octets
894	tunnelDestinationIPv4Address	unsigned32	4 octets
895	tunnelProtocolIdentifier	unsigned8	1 octet
896	tunnelSourceTransportPort	unsigned16	2 octets
897	tunnelDestinationTransportPort	unsigned16	2 octets
898	virtualObsID	string	longueur variable

Le diagramme suivant montre le flux du trafic entre les machines virtuelles attachées à des hôtes KVM surveillées par la fonctionnalité IPFIX :



Le modèle d'entrée d'IPFIX KVM IPv4 contiendra les éléments suivants :

- éléments standard
- virtualObsID : 6d876a1c-e0ac-4bcf-85ee-bdd42fa7ba34 (ID de port logique)

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.

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://<nsx-manager-ip-address>`.
- 2 Sélectionner un(e) **Mise en réseau et sécurité avancées > Mise en réseau > Commutation > Ports**

- 3 Cliquez sur le nom d'un port.

- 4 Cliquez sur l'onglet **Surveiller**.

L'état du port et les statistiques sont affichés.

- 5 Pour télécharger un fichier CSV des adresses MAC apprises par l'hôte, cliquez sur **Télécharger la table MAC**.

- 6 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](#).

Commutateurs logiques

13

Vous pouvez configurer des commutateurs logiques et des objets associés à partir de l'onglet **Mise en réseau avancée et sécurité**. Un commutateur logique reproduit la fonctionnalité de commutation, le trafic de diffusion, monodiffusion inconnue et multidiffusion (BUM), dans un environnement virtuel dissocié du matériel sous-jacent.

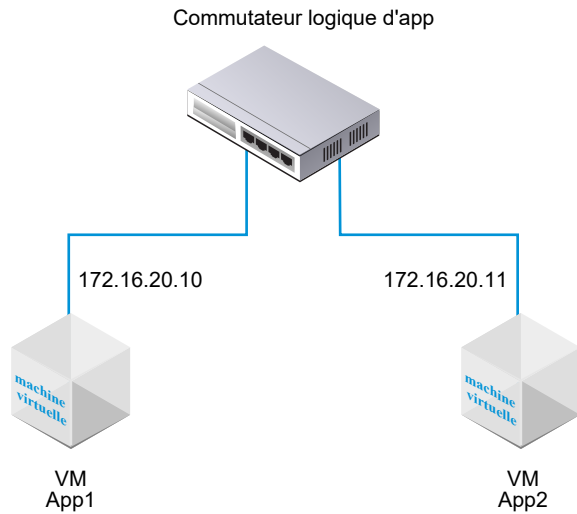
Note Si vous utilisez l'interface utilisateur **Mise en réseau et sécurité avancées** pour modifier des objets créés dans l'interface de stratégie, il se peut que certains paramètres ne soient pas configurables. Cette icône est située à côté de ces paramètres en lecture seule : . Pour plus d'informations, reportez-vous à la section [Chapitre 1 Présentation de NSX Manager](#).

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 planifiiez la topologie que vous créez.

Figure 13-1. Topologie du commutateur logique



Par exemple, la topologie ci-dessus 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.

NSX Cloud Note Si vous utilisez NSX Cloud, consultez [Fonctionnalités de NSX-T Data Centerprises en charge avec NSX Cloud](#) pour obtenir la liste des entités logiques générées automatiquement, des fonctionnalités prises en charge et des configurations requises pour NSX Cloud.

Ce chapitre contient les rubriques suivantes :

- [Comprendre les modes de réplication de trame BUM](#)
- [Créer un commutateur logique](#)
- [Connexion d'une machine virtuelle à un commutateur logique](#)
- [Créer un port de commutateur logique](#)
- [Tester la connectivité de couche 2](#)
- [Créer un commutateur logique VLAN pour la liaison montante NSX Edge](#)
- [Basculement des profils pour commutateurs logiques et ports logiques](#)
- [Pile de mise en réseau améliorée](#)
- [Pontage 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 13 Commutateurs logiques](#) et [Comprendre les modes de réplication de trame BUM](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Commutation > Commutateurs > Ajouter**.
- 3 Entrez un nom pour le commutateur logique et éventuellement une description.

- 4 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.

- 5 Entrez le nom d'une stratégie d'association de liaisons montantes.

- 6 Définissez **Statut administratif** sur **Actif** ou **Inactif**.

- 7 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.

- 8 (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.

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

- 10 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](#).

Connexion d'une machine virtuelle à un commutateur logique

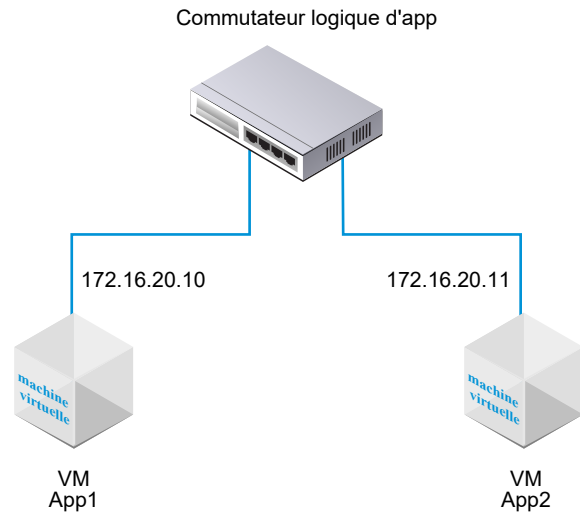
La configuration pour la connexion d'une machine virtuelle à un port logique peut varier en fonction de l'hôte.

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](#).

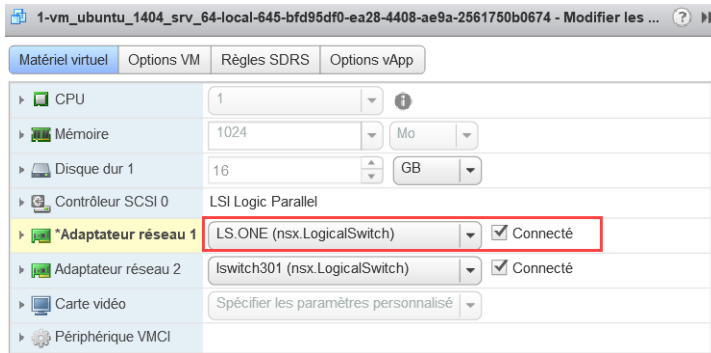
Conditions préalables

- 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 afficher les ports de commutateur logique et l'ID de pièce jointe VIF sur NSX Manager dans **Mise en réseau et sécurité avancées > Mise en réseau > Commutation > Ports**.

Utilisez l'appel API GET `https://<mgr-ip>/api/v1/logical-ports/` pour afficher les détails du port et l'état d'administration de l'ID de pièce jointe VIF correspondant. Pour afficher l'état opérationnel, utilisez l'appel API `https://<mgr-ip>/api/v1/logical-ports/<logical-port-id>/status` avec l'ID de port logique approprié.

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*.

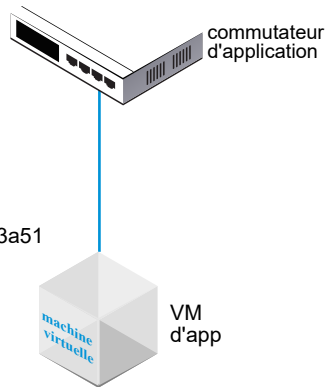
Attacher une machine virtuelle autonome hébergée sur un hôte ESXi autonome à un commutateur logique NSX-T Data Center

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

Matériel virtuel Options VM Règles SDRS

CPU	1	
Mémoire	1024	Mo
Nouveau disque dur	24	GB
Nouveau contrôleur SCSI	LSI Logic SAS	
*Nouveau réseau	VM Network	
Statut	<input checked="" type="checkbox"/> Connecter lors de la mise sous tension	
Type d'adaptateur	VMXNET 3	
DirectPath I/O	<input type="checkbox"/> Activer	
Adresse MAC		Automatique
Nouveau lecteur CD/DVD	Périphérique client	<input type="checkbox"/> Connecter...
Nouvelle disquette	Périphérique client	<input type="checkbox"/> Connecter...

Nouveau périphérique : Réseau Ajouter

- 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-fef7-08c5-5bf7-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 /vmtoolsd/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 /vmtoolsd/power.off 5
Powering off VM:

[user@host:~] vim-cmd /vmtoolsd/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 réplication	Réplication 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 **Mise en réseau et sécurité avancées > Mise en réseau > Commutation > Ports**, retrouvez l'ID d'attachement VIF correspondant à l'externalId de la machine virtuelle, et assurez-vous 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

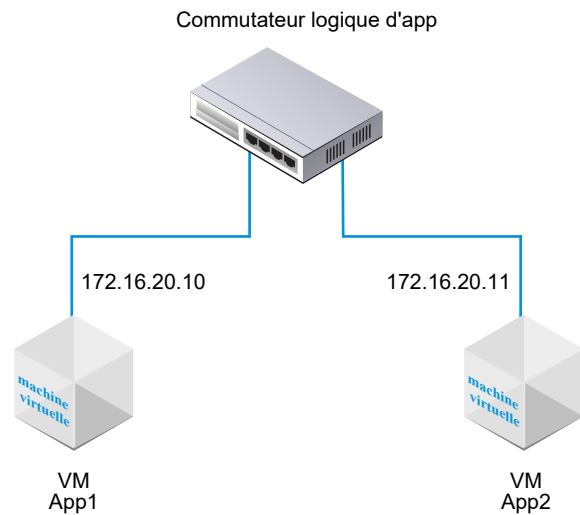
Ajoutez un routeur logique.

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 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 **Mise en réseau et sécurité avancées > Mise en réseau > 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*.

Créer un port de commutateur logique

Un commutateur logique possède plusieurs ports de commutateur. Un port de commutateur logique se connecte à un autre composant réseau, une machine virtuelle ou un conteneur à un commutateur logique.

Si vous connectez une machine virtuelle à un commutateur logique sur un hôte ESXi géré par vCenter Server, un port de commutateur logique est créé automatiquement. 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.

Pour surveiller l'activité sur un port de commutateur logique, reportez-vous à la section [Surveiller l'activité d'un port de commutateur logique](#).

Conditions préalables

Vérifiez qu'un commutateur logique est créé. Reportez-vous à la section [Chapitre 13 Commutateurs logiques](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Commutation > Ports > Ajouter**.

- 3 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 le menu déroulant.
Statut administratif	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.

À l'aide de l'API, vous pouvez définir le type de pièce jointe sur des valeurs supplémentaires (LOGICALROUTER, BRIDGEENDPOINT, DHCP_SERVICE, METADATA_PROXY, L2VPN_SESSION). Si le type de pièce jointe est service DHCP, proxy de métadonnées ou session VPN L2, les profils de commutation du port doivent être ceux par défaut. Vous ne pouvez pas utiliser un profil défini par l'utilisateur.

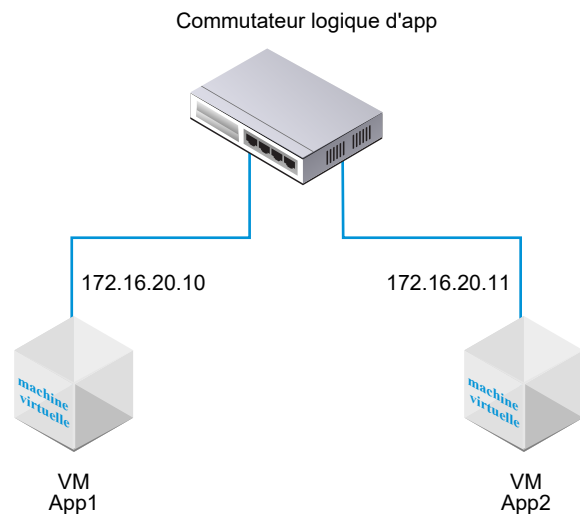
- 4 (Facultatif) Dans l'onglet **Profils de commutation**, sélectionnez des profils de commutation.
- 5 Cliquez sur **Enregistrer**.

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 13-2. 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 le statut administratif du commutateur logique est Actif.
 - d Dans NSX Manager, sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Commutation > Commutateurs**.

- e Cliquez sur le commutateur logique et notez l'UUID et les informations VNI.
- f Exécutez les commandes suivantes pour résoudre le problème.

vdmadmin	Description
get logical-switch <vni-or-uuid> arp-table	<p>Affiche la table ARP du commutateur logique spécifié.</p> <p>Exemple de résultat.</p> <pre>nsx-manager1> 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	<p>Affiche les connexions du commutateur logique spécifié.</p> <p>Exemple de résultat.</p> <pre>nsx-manager1> 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	<p>Affiche la table MAC du commutateur logique spécifié.</p> <p>Exemple de résultat.</p> <pre>nsx-manager1> 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	<p>Affiche des statistiques sur le commutateur logique spécifié.</p> <p>Exemple de résultat.</p> <pre>nsx-manager1> 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	<p>Affiche un résumé de toutes les statistiques du commutateur logique au fil du temps.</p> <p>Exemple de résultat.</p> <pre>nsx-manager1> 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>
get logical-switch <vni-or-uuid> vtep	<p>Affiche tous les points de terminaison de tunnel virtuels liés au commutateur logique spécifié.</p> <p>Exemple de résultat.</p> <pre>nsx-manager1> 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>

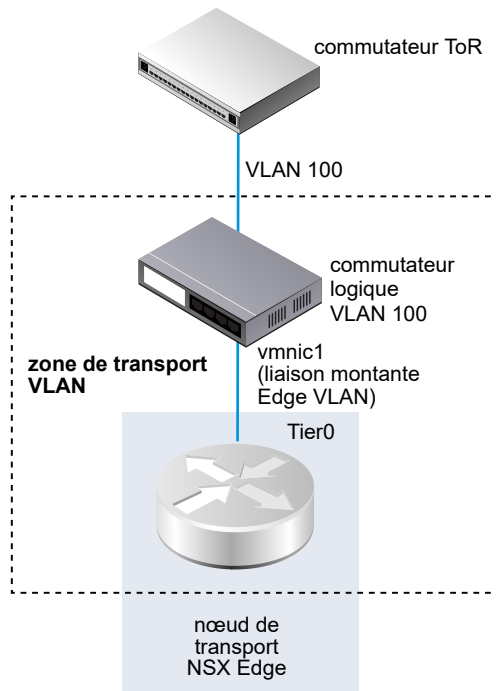
Résultats

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

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 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 et sécurité avancées > Mise en réseau > Commutation > Commutateurs > Ajouter**.
- 3 Tapez un nom pour le commutateur logique.
- 4 Sélectionnez une zone de transport pour le commutateur logique.
- 5 Sélectionnez une stratégie d'association de liaison montante.
- 6 Pour l'état d'administration, sélectionnez **Actif** ou **Inactif**.
- 7 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.
- 8 (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.

Basculement des profils pour commutateurs logiques et ports logiques

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)
- Mise en miroir de ports
- 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.

Avant d'utiliser un profil par défaut, assurez-vous que les paramètres correspondent à vos besoins. Lorsque vous créez un profil personnalisé, certains paramètres ont des valeurs par défaut. Ne partez pas du principe que dans le profil par défaut, ces paramètres auront les valeurs par défaut.

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.

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://<nsx-manager-ip-address>>.
- 2 Sélectionner un(e) **Mise en réseau et sécurité avancées > Mise en réseau > Commutation > Profils de commutation > Ajouter**
- 3 Sélectionnez **QoS** et renseignez les détails du profil de commutation QoS.

Option	Description
Nom et description	Attribuez un nom au profil de commutation QoS personnalisé. En option, vous pouvez décrire le paramètre que vous avez modifié dans le profil.
Mode	<p>Sélectionnez l'option Approuvé ou Non approuvé dans le menu déroulant Mode.</p> <p>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 DSCP.</p> <p>Les valeurs de priorité vont de 0 à 63.</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>

Option	Description
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 taille de rafale est basée sur la durée avec la bande passante maximale. Vous définissez la durée de rafale dans le paramètre de taille de rafale. Vous ne pouvez pas garantir la bande passante. Toutefois, vous pouvez utiliser les paramètres Moyenne, Maximale et Taille de rafale pour limiter la bande passante réseau.</p> <p>Par exemple, si la bande passante moyenne est de 30 Mbit/s, la bande passante maximale de 60 Mbit/s et la durée autorisée de 0,1 seconde, alors la taille de rafale est de $60 * 1\,000\,000 * 0,10/8 = 750\,000$ octets.</p> <p>La valeur par défaut de 0 désactive la limitation du taux sur le trafic d'entrée.</p>
Diffusion d'entrée	<p>Définissez des valeurs personnalisées pour le trafic réseau sortant de la VM vers le réseau logique en fonction de la diffusion.</p> <p>Définissez des valeurs personnalisées pour le trafic réseau sortant de la VM vers le réseau logique en fonction de la diffusion. Par exemple, lorsque vous définissez la bande passante moyenne pour un commutateur logique sur 3 000 Kbit/s, que la bande passante maximale est de 6 000 Kbit/s et la durée autorisée de 0,1 seconde, alors la taille de rafale est de $6\,000 * 1\,000 * 0,10/8 = 75\,000$ octets.</p> <p>La valeur par défaut de 0 désactive la limitation du taux sur le trafic de diffusion d'entrée.</p>
Sortie	<p>Définissez des valeurs personnalisées pour le trafic réseau entrant du réseau logique vers la VM.</p> <p>La valeur par défaut de 0 désactive la limitation du taux sur le trafic de sortie.</p>

Si les options d'entrée, de diffusion d'entrée et de sortie ne sont pas configurées, les valeurs par défaut sont utilisées.

4 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 mise en miroir de ports

La mise en miroir de ports logiques vous permet de répliquer et de rediriger tout le trafic provenant ou sortant d'un port de commutateur logique attaché à un port VIF de VM. Le trafic mis en miroir est envoyé encapsulé dans un tunnel d'encapsulation générique de routage (GRE) à un

collecteur de sorte que toutes les informations du paquet d'origine soient conservées lors de la traversée du réseau vers une destination distante.

Nous vous recommandons d'utiliser la mise en miroir de ports uniquement pour le dépannage.

Note La mise en miroir de ports n'est pas recommandée pour la surveillance, car les performances sont affectées lorsqu'elle est utilisée pendant de longues durées.

Par rapport à la mise en miroir de ports physiques, la mise en miroir de ports logiques garantit que tout le trafic réseau des VM est capturé. Si vous implémentez la mise en miroir de ports uniquement sur le réseau physique, la mise en miroir d'une partie du trafic réseau des VM échoue. Cela se produit car la communication entre les VM résidant sur le même hôte n'entre jamais sur le réseau physique et, par conséquent, elle n'est pas mise en miroir. Avec la mise en miroir de ports logiques, vous pouvez continuer à mettre en miroir le trafic d'une VM même lorsque cette VM est migrée vers un autre hôte.

Le processus de mise en miroir de ports est semblable pour les deux ports de VM dans le domaine NSX-T Data Center et les ports d'applications physiques. Vous pouvez transférer le trafic capturé par une charge de travail connectée à un réseau logique et mettre en miroir ce trafic vers un collecteur. L'adresse IP doit être accessible à partir d'une adresse IP invitée sur laquelle la VM est hébergée. Ce processus est également vrai pour les applications physiques connectées aux nœuds de passerelle.

Configurer un profil de commutation de mise en miroir de ports personnalisé

Vous pouvez créer un profil de commutation de mise en miroir de ports personnalisé avec une valeur de destination et de clé différente.

Conditions préalables

- Familiarisez-vous avec le concept de profil de commutation de mise en miroir de ports. Reportez-vous à la section [Comprendre le profil de commutation de mise en miroir de ports](#).
- Identifiez l'adresse IP de l'ID de port logique de destination vers lequel vous voulez rediriger le trafic réseau.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionner un(e) **Mise en réseau et sécurité avancées > Mise en réseau > Commutation > Profils de commutation > Ajouter**

- 3 Sélectionnez **Mise en miroir de ports** et renseignez le détails du profil de commutation de la mise en miroir de ports.

Option	Description
Nom et description	Attribuez un nom au profil de commutation de mise en miroir de ports personnalisé. En option, vous pouvez décrire le paramètre que vous avez modifié pour personnaliser ce profil.
Direction	Sélectionnez une option dans le menu déroulant pour utiliser cette source pour le trafic Entrée , Sortie ou Bidirectionnel . Entrant est le trafic réseau sortant de la VM vers le réseau logique. Sortant est le trafic réseau entrant du réseau logique vers la VM. Bidirectionnel est le trafic bidirectionnel de la VM vers le réseau logique et du réseau logique vers la VM. Il s'agit de l'option par défaut.
Troncation des paquets	Facultative. La plage est comprise entre 60 et 65 535.
Clé	Entrez une valeur 32 bits aléatoire pour identifier des paquets en miroir provenant du port logique. Cette valeur Clé est copiée dans le champ Clé dans l'en-tête GRE de chaque paquet miroir. Si la valeur Clé est définie sur 0, la définition par défaut est copiée dans le champ Clé dans l'en-tête GRE. La valeur 32 bits par défaut est composée des valeurs suivantes. <ul style="list-style-type: none"> ■ La première valeur 24 bits est une valeur VNI. VNI fait partie de l'en-tête IP des trames encapsulées. ■ Le 25ème bit indique si la première valeur 24 bits est une valeur VNI valide. Un représente une valeur valide et zéro une valeur non valide. ■ Le 26ème bit indique le sens du trafic en miroir. Un représente un sens entrant et zéro un sens sortant. ■ Les six bits restants ne sont pas utilisés.
Destinations	Entrez l'ID de destination du collecteur pour la session de mise en miroir. L'ID de l'adresse IP de destination ne peut qu'être une adresse IPv4 dans le réseau ou une adresse IPv4 distante non gérée par NSX-T Data Center. Vous pouvez ajouter jusqu'à trois adresses IP de destination en les séparant par une virgule.

- 4 Cliquez sur **Enregistrer**.

Résultats

Un profil de commutation de mise en miroir de ports personnalisé 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](#).

Vérifiez que le profil de commutation de mise en miroir de ports personnalisé fonctionne. Reportez-vous à la section [Vérifier le profil de commutation de mise en miroir de ports personnalisé](#).

Vérifier le profil de commutation de mise en miroir de ports personnalisé

Avant de commencer à utiliser le profil de commutation de mise en miroir de ports personnalisé, vérifiez que la personnalisation fonctionne correctement.

Conditions préalables

- Vérifiez que le profil de commutation de mise en miroir de ports personnalisé est configuré. Reportez-vous à la section [Configurer un profil de commutation de mise en miroir de ports personnalisé](#).
- Vérifiez que le profil de commutation de mise en miroir de ports personnalisé est attaché à un commutateur logique. Reportez-vous à la section [Associer un profil personnalisé à un commutateur logique](#).

Procédure

- 1 Localisez deux VM avec des associations de VIF au port logique configuré pour la mise en miroir de ports.

Par exemple, VM1 10.70.1.1 et VM2 10.70.1.2 disposent d'associations de VIF et elles se situent sur le même réseau logique.

- 2 Exécutez la commande `tcpdump` sur une adresse IP de destination.

```
sudo tcpdump -n -i eth0 dst host destination_IP_adress and proto gre
```

Par exemple, l'adresse IP de destination est 10.24.123.196.

- 3 Connectez-vous à la première VM et effectuez un test ping sur la seconde VM pour vérifier que les demandes et les réponses ECHO correspondantes sont reçues à l'adresse de destination.

Étape suivante

Attachez ce profil de commutation de mise en miroir de ports personnalisé à un commutateur 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](#).

Comprendre le profil de commutation de découverte d'adresses IP

La découverte d'adresses IP utilise l'écoute DHCP et DHCPv6, l'écoute ARP (Address Resolution Protocol), l'écoute ND (Neighbor-Discovery) et VM Tools pour découvrir les adresses MAC et IP.

Les adresses MAC et IP découvertes sont utilisées pour permettre la suppression ARP/ND, ce qui réduit le trafic entre les machines virtuelles connectées au même commutateur logique. Les adresses sont également utilisées par SpoofGuard et les composants du pare-feu distribué (DFW). DFW utilise les liaisons d'adresses pour déterminer l'adresse IP des objets dans les règles de pare-feu.

L'écoute DHCP/DHCPv6 inspecte les paquets DHCP/DHCPv6 échangés entre le client et le serveur DHCP/DHCPv6 pour apprendre les adresses IP et MAC.

L'écoute ARP inspecte les paquets ARP et GARP (ARP gratuits) sortants d'une 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 MAC et IP ou IPv6. Cette méthode de découverte d'adresses IP est disponible pour les machines virtuelles en cours d'exécution sur les hôtes ESXi uniquement.

L'écoute ND est l'équivalent IPv6 de l'écoute ARP. Elle inspecte les messages Neighbor Solicitation (NS) et Neighbor Advertisement (NA) pour découvrir les adresses IP et MAC.

La détection d'adresses en double vérifie si une adresse IP qui vient d'être découverte est déjà présente dans la liste des liaisons réalisées pour un port différent. Cette vérification est effectuée pour les ports se trouvant sur le même segment. Si une adresse en double est détectée, l'adresse qui vient d'être découverte est ajoutée à la liste de découverte, mais n'est pas ajoutée à la liste des liaisons réalisées. Toutes les adresses IP en double ont un horodatage de découverte associé. Si l'adresse IP qui se trouve sur la liste des liaisons réalisées est supprimée, soit en l'ajoutant à la liste Ignorer la liaison, soit en désactivant l'écoute, l'adresse IP en double avec l'horodatage le plus ancien est déplacée vers la liste des liaisons réalisées. Les informations d'adresse en double sont disponibles via un appel d'API.

Par défaut, les méthodes de découverte par écoute ARP et écoute ND fonctionnent dans un mode appelé TOFU (Trust On First Use). Dans le mode TOFU, lorsqu'une adresse est découverte et ajoutée à la liste des liaisons réalisées, cette liaison reste indéfiniment dans la liste des liaisons réalisées. TOFU s'applique aux « n » premières liaisons uniques <IP, MAC, VLAN> découvertes à l'aide de l'écoute ARP/ND, où « n » est la limite de liaison que vous pouvez configurer. Vous pouvez désactiver le mode TOFU pour l'écoute ARP/ND. Les méthodes fonctionnent alors dans le mode TOEU (Trust on Every Use). Dans le mode TOEU, lorsqu'une adresse est découverte, elle est ajoutée à la liste des liaisons réalisées et lorsqu'elle est supprimée ou expirée, elle en est supprimée. L'écoute DHCP et VM Tools fonctionnent toujours dans le mode TOEU.

Pour chaque port, NSX Manager conserve une liste Ignorer les liaisons, qui contient les adresses IP qui ne peuvent pas être liées au port. En accédant à **Mise à niveau avancée et sécurité > Commutation > Ports** et en sélectionnant un port, vous pouvez ajouter des liaisons découvertes à la liste des liaisons ignorées. Vous pouvez également supprimer une liaison existante découverte ou réalisée en la copiant vers **Ignorer les liaisons**.

Note TOFU n'est pas identique à SpoofGuard et ne bloque pas le trafic de la même manière que SpoofGuard. Pour plus d'informations, reportez-vous à la section [Comprendre le profil de segment SpoofGuard](#).

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

NSX-T Data Center dispose de plusieurs profils de commutation de découverte d'adresses IP par défaut. Vous pouvez également en créer de nouveaux.

Conditions préalables

Familiarisez-vous avec les concepts 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Commutation > Profils de commutation > Ajouter**.
- 3 Sélectionnez **Découverte d'adresses IP** et spécifiez 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	Pour un environnement IPv4. Applicable si les machines virtuelles ont des adresses IP statiques.
Limite de liaison ARP	Nombre maximal d'adresses IP IPv4 pouvant être liées à un port. La valeur minimale autorisée est 1 (valeur par défaut) et la valeur maximale est 256.
Délai d'expiration de limite de liaison ARP ND	Valeur du délai d'expiration, en minutes, des adresses IP dans la table de liaison ARP/ND si TOFU est désactivé. Si une adresse arrive à expiration, une adresse qui vient d'être découverte la remplace.
Écoute DHCP	Pour un environnement IPv4. Applicable si les machines virtuelles ont des adresses IPv4.
Écoute DHCP V6	Pour un environnement IPv6. Applicable si les machines virtuelles ont des adresses IPv6.
VM Tools	Disponible pour les machines virtuelles hébergées par ESXi uniquement.
VM Tools pour IPv6	Disponible pour les machines virtuelles hébergées par ESXi uniquement.
Écoute dans le cadre de la découverte de voisin	Pour un environnement IPv6. Applicable si les machines virtuelles ont des adresses IP statiques.
Limite de liaison pour la découverte de voisin	Nombre maximal d'adresses IPv6 pouvant être liées à un port.
Approuver à la première utilisation	Applicable à l'écoute ARP et ND.
Détection d'adresses IP en double	Pour toutes les méthodes d'écoute, et les environnements IPv4 et IPv6.

- 4 Cliquez sur **Ajouter**.

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 de modifier leur adresse IP existante. 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 d'autorisation de MAC/VLAN/IP autorisés est fournie via la propriété Liaisons d'adresses 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 d'autorisation de MAC/VLAN/IP autorisés est fournie via la propriété Liaisons d'adresses du commutateur. En général, il s'agit d'une plage d'adresses IP/sous-réseau autorisé 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'adresses de port

Les liaisons d'adresses 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'adresses 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'adresses spécifiées sont appliquées dans le chemin d'accès aux données. En plus de SpoofGuard, les liaisons d'adresses de port sont utilisées pour les traductions de règles DFW.

Procédure

- 1 Dans NSX Manager, sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Commutation > Ports**.
- 2 Cliquez sur le port logique auquel vous voulez appliquer la liaison d'adresse.
Le résumé du port logique s'affiche.
- 3 Dans l'onglet **Présentation**, développez **Liaisons d'adresses > Liaisons manuelles**.
- 4 Cliquez sur **Ajouter**.
La boîte de dialogue Ajouter une liaison d'adresse s'affiche.
- 5 Spécifiez l'adresse IP (adresse IPv4, adresse IPv6 ou sous-réseau IPv6) et l'adresse MAC du port logique auquel vous voulez appliquer la liaison d'adresse. Par exemple, pour IPv6, 2001::/64 est un sous-réseau IPv6, 2001::1 est une adresse IP d'hôte, alors que 2001::1/64 est une entrée non valide. Vous pouvez également spécifier un ID VLAN.
- 6 Cliquez sur **Ajouter**.

Étape suivante

Utilisez les liaisons d'adresses 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Commutation > Profils de commutation > Ajouter**.

- 3 Sélectionnez **SpoofGuard**.
- 4 Entrez un nom et éventuellement une description.
- 5 Pour activer SpoofGuard de niveau port, définissez **Liaisons de port** sur **Activé**.
- 6 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Commutation**.
- 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. Désactivé par défaut. 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 du BPDU pour autoriser le trafic vers la destination autorisée. Vous devez activer Filtre BPDU pour pouvoir le sélectionner dans cette liste.
Filtre DHCP	Basculez les boutons Bloc de serveur et Bloc de client pour activer le filtrage DHCP. Les deux valeurs sont désactivées par défaut. 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'acquérir une adresse IP DHCP en bloquant les demandes DHCP.
Filtre DHCPv6	Basculez les boutons Bloc de serveur V6 et Bloc de client V6 pour activer le filtrage DHCP. Les deux valeurs sont désactivées par défaut. Le blocage de serveur DHCPv6 bloque le trafic allant d'un serveur DHCPv6 vers un client DHCPv6. Notez qu'il ne bloque pas le trafic allant d'un serveur DHCP vers un agent du relais DHCP. Les paquets dont le numéro de port source UDP est 547 sont filtrés. Le blocage de client DHCPv6 empêche une machine virtuelle d'acquérir une adresse IP DHCP en bloquant les demandes DHCP. Les paquets dont le numéro de port source UDP est 546 sont filtrés.
Bloquer le trafic non-IP	Basculez le bouton Bloquer le trafic non-IP pour autoriser uniquement le trafic IPv4, IPv6, ARP 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.
Protection contre les annonces du routeur	Basculez le bouton Protection contre les annonces du routeur pour filtrer les annonces du routeur IPv6 en entrée. Les paquets ICMPv6 de type 134 sont filtrés. Cette option est activée par défaut.
Limites de débit	Définissez une limite de débit pour le trafic de diffusion et de multidiffusion. Cette option est activée par défaut. Des limites de débit peuvent être utilisées pour protéger le commutateur logique ou les machines virtuelles d'événements, tels que les tempêtes 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, sauf lorsque la machine virtuelle invitée est déployée à l'aide de VMware Integrated OpenStack, auquel cas la propriété est activée 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.

L'apprentissage MAC prend également en charge la propagation monodiffusion inconnue. Normalement, lorsqu'un paquet reçu par un port présente une adresse MAC de destination inconnue, il est abandonné. Lorsque la propagation monodiffusion inconnue est activée, le port propage le trafic de monodiffusion inconnue à chaque port du commutateur sur lequel l'apprentissage MAC et la propagation monodiffusion inconnue sont activés. Cette propriété est activée par défaut, mais uniquement si l'apprentissage MAC est activé.

Le nombre d'adresses MAC pouvant être apprises est configurable. La valeur maximale est 4 096, qui est la valeur par défaut. Vous pouvez également définir la stratégie pour le moment auquel la limite est atteinte. Les options sont les suivantes :

- **Annuler** : les paquets provenant d'une adresse MAC source inconnue sont annulés. Les paquets entrants sur cette adresse MAC seront traités comme des monodiffusions inconnues. Le port recevra les paquets uniquement si la propagation monodiffusion inconnue est activée.
- **Autoriser** : les paquets provenant d'une adresse MAC source inconnue sont transférés bien que l'adresse ne soit pas apprise. Les paquets entrants sur cette adresse MAC seront traités comme des monodiffusions inconnues. Le port recevra les paquets uniquement si la propagation monodiffusion inconnue est activée.

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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Commutation > Profils de commutation > Ajouter**.
- 3 Sélectionnez **Gestion MAC** et indiquez 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. La valeur par défaut est Désactivé.
État	Activez ou désactivez la fonctionnalité d'apprentissage MAC. La valeur par défaut est Désactivé.
Propagation monodiffusion inconnue	Activez ou désactivez la fonctionnalité de propagation monodiffusion inconnue. La valeur par défaut est Activé. Cette option est disponible si vous activez l'apprentissage MAC.
Limite MAC	Définissez le nombre maximal d'adresses MAC. La valeur par défaut est 4 096. Cette option est disponible si vous activez l'apprentissage MAC.
Stratégie de limite MAC	Sélectionnez Autoriser ou Annuler . La valeur par défaut est Autoriser . Cette option est disponible si vous activez l'apprentissage MAC.

4 Cliquez sur **Ajouter**.

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 [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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Commutation > Commutateurs**.
- 3 Cliquez sur le commutateur logique pour appliquer le profil de commutation personnalisé.
- 4 Cliquez sur l'onglet **Gérer**.
- 5 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

- 6 Cliquez sur **Modifier**.
- 7 Sélectionnez le profil de commutation personnalisé créé précédemment dans le menu déroulant.
- 8 Cliquez sur **Enregistrer**.
Le commutateur logique est maintenant associé au profil de commutation personnalisé.
- 9 Vérifiez que le nouveau profil de commutation personnalisé avec la configuration modifiée s'affiche dans l'onglet **Gérer**.
- 10 (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 [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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Commutation > Ports**.
- 3 Cliquez sur le port logique pour appliquer le profil de commutation personnalisé.
- 4 Cliquez sur l'onglet **Gérer**.
- 5 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

6 Cliquez sur **Modifier**.

7 Sélectionnez le profil de commutation personnalisé créé précédemment dans le menu déroulant.

8 Cliquez sur **Enregistrer**.

Le port logique est maintenant associé au profil de commutation personnalisé.

9 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*.

Pile de mise en réseau améliorée

Le mode Chemin de données optimisé est un mode de pile de mise en réseau qui, lorsqu'il est configuré, améliore les performances réseau. Il est principalement conçu pour les charges de travail NFV, car elles nécessitent les performances avantageuses fournies par ce mode.

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

Attribuer automatiquement des cœurs logiques ENS

Attribuez automatiquement des cœurs logiques à des cartes réseau virtuelles de telle sorte que les cœurs logiques dédiés gèrent le trafic entrant et sortant des vNIC.

Avec le commutateur N-VDS configuré dans le mode chemin de données optimisé, si un seul cœur logique est associé à un vNIC, ce cœur logique traite le trafic bidirectionnel entrant ou sortant d'un vNIC. Lorsque plusieurs cœurs logiques sont configurés, l'hôte détermine automatiquement le cœur logique devant traiter le trafic d'un vNIC.

Attribuez des cœurs logiques aux vNIC en fonction de l'un des paramètres suivants.

- **vNIC** : l'hôte suppose que la transmission du trafic entrant ou sortant à une direction vNIC nécessite la même quantité de ressources de CPU. Le même nombre de vNIC est attribué à chaque cœur logique en fonction du pool de cœurs logiques disponible. Il s'agit du mode par défaut. Le mode vNIC-count est fiable, mais il n'est pas optimal pour un trafic asymétrique.
- **CPU-usage** : l'hôte prédit l'utilisation du CPU pour transmettre le trafic entrant ou sortant à chaque direction vNIC en se servant des statistiques internes. En fonction de l'utilisation du CPU pour transmettre le trafic, l'hôte modifie les affectations de cœurs logiques pour équilibrer la charge entre les cœurs logiques. Le mode CPU-usage est plus optimal que le mode vNIC-count, mais peu fiable lorsque le trafic n'est pas stable.

Dans le mode CPU-usage, si le trafic transmis change fréquemment, les ressources de CPU prévues requises et l'attribution de vNIC peuvent également changer fréquemment. Des modifications d'attribution trop fréquentes peuvent entraîner des abandons de paquets.

Si les modèles de trafic sont symétriques parmi les vNIC, l'option vNIC-count fournit un comportement fiable, qui est moins vulnérable aux changements fréquents. Cependant, si les modèles de trafic sont asymétriques, le mode vNIC-count peut entraîner des abandons de paquets, car il ne distingue pas la différence de trafic entre les vNIC.

Dans le mode vNIC-count, il est recommandé de configurer un nombre approprié de cœurs logiques afin que chaque cœur logique soit attribué au même nombre de vNIC. Si le nombre de vNIC associés à chaque cœur logique est différent, l'attribution de CPU est abusive et les performances ne sont pas déterministes.

Lorsqu'un vNIC est connecté ou déconnecté ou lorsqu'un cœur logique est ajouté ou supprimé, les hôtes détectent automatiquement les modifications et procèdent à un rééquilibrage.

Procédure

- ◆ Pour passer d'un mode à un autre, exécutez la commande suivante.

```
set ens lcore-assignment-mode <host-switch-name> <ens-lc-mode>
```

Où *<ens-lc-mode>* peut être défini sur le mode **vNIC-count** ou **cpu-usage**.

vNIC-count est une attribution de cœur logique basée sur le nombre de vNIC et sur la direction.

cpu-usage est une attribution de cœur logique basée sur l'utilisation du CPU.

Configurer le routage inter-VLAN d'invité

Sur les réseaux de superposition, NSX-T prend en charge le routage du trafic inter-VLAN sur un domaine L3. Lors du routage, le routeur distribué virtuel (VDR) utilise l'ID VLAN pour acheminer les paquets entre les sous-réseaux VLAN.

Le routage inter-VLAN contourne la limite de 10 vNIC pouvant être utilisées par machine virtuelle. NSX-T prenant en charge le routage inter-VLAN garantit que de nombreuses sous-interfaces VLAN peuvent être créées sur la vNIC et consommées pour différents services de mise en réseau. Par exemple, une vNIC d'une machine virtuelle peut être divisée en plusieurs sous-interfaces. Chaque sous-interface appartient à un sous-réseau, qui peut héberger un service de mise en réseau tel que SNMP ou DHCP. Avec le routage inter-VLAN, par exemple, une sous-interface sur VLAN-10 peut atteindre une sous-interface sur VLAN-10 ou sur tout autre VLAN.

Chaque vNIC d'une machine virtuelle est connectée au N-VDS via le port logique parent, qui gère les paquets non balisés.

Pour créer une sous-interface, sur le commutateur N-VDS amélioré, créez un port enfant en utilisant l'API avec une VIF associée à l'aide de l'appel d'API décrit dans la procédure. La sous-interface balisée avec un ID VLAN est associée à un nouveau commutateur logique. Par exemple, VLAN10 est attaché au commutateur logique LS-VLAN-10. Toutes les sous-interfaces de VLAN10 doivent être attachées à LS-VLAN-10. Ce mappage 1-1 entre l'ID VLAN de la sous-interface et son commutateur logique associé est une condition préalable importante. Par exemple, l'ajout d'un port enfant avec VLAN20 au commutateur logique LS-VLAN-10 mappé à VLAN-10 rend le routage des paquets entre les VLAN non opérationnel. Une telle erreur de configuration rend le routage inter-VLAN non opérationnel.

Conditions préalables

- Avant d'associer une sous-interface VLAN à un commutateur logique, assurez-vous que le commutateur logique n'a pas d'autres associations avec une autre sous-interface VLAN. En cas de discordance, le routage inter-VLAN sur les réseaux de superposition peut ne pas fonctionner.
- Assurez-vous que les hôtes exécutent ESXi v 6.7 U2 ou version ultérieure.

Procédure

- 1 Pour créer des sous-interfaces pour une vNIC, assurez-vous que la vNIC est mise à jour vers un port parent. Effectuez l'appel REST API suivant.

```
PUT https://<nsx-mgr-ip>/api/v1/logical-ports/<Logical-Port UUID-of-the-vNIC>
{
  "resource_type" : "LogicalPort",
  "display_name" : "parentport",
  "attachment" : {
    "attachment_type" : "VIF",
    "context" : {
      "resource_type" : "VifAttachmentContext",
      "vif_type": "PARENT"
    },
    "id" : "<Attachment UUID of the vNIC>"
  },
}
```



```

    "admin_state" : "UP",
    "logical_switch_id" : "UUID of Logical Switch to which the vNIC is connected",
    "_revision" : 0
  }

```

- 2 Pour créer des ports enfants pour un port vNIC parent sur le N-VDS associé aux sous-interfaces sur une machine virtuelle, effectuez l'appel d'API. Avant d'effectuer l'appel d'API, vérifiez qu'un commutateur logique existe pour connecter les ports enfants aux sous-interfaces sur la machine virtuelle.

```

POST https://<nsx-mgr-ip>/api/v1/logical-ports/
{
  "resource_type" : "LogicalPort",
  "display_name" : "<Name of the Child PORT>",
  "attachment" : {
    "attachment_type" : "VIF",
    "context" : {
      "resource_type" : "VifAttachmentContext",
      "parent_vif_id" : "<UUID of the PARENT port from Step 1>",
      "traffic_tag" : <VLAN ID>,
      "app_id" : "<ID of the attachment>", ==> display id(can give any string). Must be
unique.
      "vif_type" : "CHILD"
    },
    "id" : "<ID of the CHILD port>"
  },

  "logical_switch_id" : "<UUID of the Logical switch(not the PARENT PORT's logical switch)
to which Child port would be connected to>",
  "address_bindings" : [ { "mac_address" : "<vNIC MAC address>", "ip_address" : "<IP
address to the corresponding VLAN>", "vlan" : <VLAN ID> } ],
  "admin_state" : "UP"
}

```

Résultats

NSX-T Data Center crée des sous-interfaces sur les machines virtuelles.

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. Ce pont de couche 2 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 Edge et des profils de pont Edge. Vous pouvez configurer le pontage de couche 2 à l'aide de nœuds de transport NSX Edge. Pour utiliser des nœuds de transport NSX Edge pour le pontage, vous créez un profil de pont Edge. Un profil de pont Edge spécifie le cluster Edge à utiliser pour le pontage et le nœud de transport Edge agit en tant que pont principal et de sauvegarde.

Le profil de pont Edge est attaché à un commutateur logique, et le mappage spécifie la liaison montante physique sur le dispositif Edge utilisé pour le pontage et l'ID VLAN à associer au commutateur logique. Un commutateur logique peut être attaché à plusieurs profils de pont.

Créer un profil de pont Edge

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

Lorsque vous créez un profil de pont Edge, si vous définissez le mode de basculement sur préemptif et qu'un basculement se produit, le nœud en veille devient le nœud actif. Après la récupération du nœud ayant échoué, il devient de nouveau le nœud actif. Si vous définissez le mode de basculement sur non-préemptif et qu'un basculement se produit, le nœud en veille devient le nœud actif. Une fois le nœud ayant échoué restauré, il devient le nœud en veille. Vous pouvez définir manuellement le nœud Edge en veille pour qu'il soit le nœud actif en exécutant la commande CLI `set l2bridge-port <uuid> state active` sur le nœud Edge en veille. La commande ne peut être appliquée qu'en mode non-préemptif. Sinon, une erreur se produira. En mode non-préemptif, la commande déclenche un basculement HA lorsqu'elle est appliquée sur un nœud en veille, et elle est ignorée lorsqu'elle est appliquée sur un nœud actif. Pour plus d'informations, reportez-vous à la *référence de l'interface de la ligne de commande de NSX-T Data Center*.

Conditions préalables

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

Procédure

- 1 Sélectionnez **Système > Infrastructure > Profils > Profils de pont Edge > Ajouter**.
- 2 Entrez un nom pour le profil de pont Edge et éventuellement une description.
- 3 Sélectionnez un cluster NSX Edge.
- 4 Sélectionnez un nœud principal.
- 5 Sélectionnez un nœud de secours.
- 6 Sélectionnez un mode de basculement.
Les options sont **Préemptif** et **Non-préemptif**.
- 7 Cliquez sur le bouton **Ajouter**.

Étape suivante

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

Configurer le pontage basé sur Edge

Lorsque vous configurez le pontage basé sur Edge, après la création d'un profil de pont Edge pour un cluster Edge, certaines configurations supplémentaires sont requises.

Notez que le pontage d'un commutateur logique à deux reprises sur le même nœud Edge n'est pas pris en charge. Cependant, vous pouvez relier deux VLAN au même commutateur logique sur deux nœuds Edge différents.

Il existe trois options de configuration.

Option 1 : configurer le mode promiscuité

- Définissez le mode promiscuité sur le groupe de ports.
- Autorisez la fausse transmission sur le groupe de ports.
- Exécutez la commande suivante pour activer le filtre inverse sur l'hôte ESXi sur lequel la machine virtuelle Edge est en cours d'exécution :

```
esxcli system settings advanced set -o /Net/ReversePathFwdCheckPromisc -i 1
```

Ensuite, désactivez et activez le mode Promiscuité dans le groupe de ports en procédant comme suit :

- Modifiez les paramètres du groupe de ports.
- Désactivez le mode Promiscuité et enregistrez les paramètres.
- Modifiez de nouveau les paramètres du groupe de ports.
- Activez le mode Promiscuité et enregistrez les paramètres.
- 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 être réduit, car le trafic VLAN doit être transféré aux deux machines virtuelles en mode promiscuité.

Option 2 : configurer l'apprentissage MAC

Si le dispositif Edge est déployé sur un hôte sur lequel NSX-T est installé, il peut se connecter à un commutateur logique ou à un segment VLAN. Le commutateur logique doit disposer d'un profil de gestion MAC sur lequel l'apprentissage MAC est activé. De même, le segment doit disposer d'un profil de découverte MAC sur lequel l'apprentissage MAC est activé.

Option 3 : configurer un port de réception

- 1 Récupérez le numéro de port de la vNIC de jonction que vous voulez configurer comme port de réception.
 - a Connectez-vous à vSphere Web Client et accédez à **Accueil > Mise en réseau**.

- b Cliquez sur le groupe de ports distribués auquel l'interface de jonction NSX Edge est connectée, puis cliquez sur **Ports** pour afficher les ports et les machines virtuelles connectées. Notez le numéro de port associé à l'interface de jonction. Utilisez ce numéro de port lors de l'extraction et de la mise à jour des données opaques.
- 2 Récupérez la valeur dvsUuid du commutateur vSphere Distributed Switch.
 - a Connectez-vous à l'interface utilisateur de vCenter Mob à l'adresse `https://<vc-ip>/mob`.
 - b Cliquez sur **Contenu**.
 - c Cliquez sur le lien associé à **rootFolder** (par exemple, *group-d1 (Datacenters)*).
 - d Cliquez sur le lien associé à **childEntity** (par exemple, *datacenter-1*).
 - e Cliquez sur le lien associé à **networkFolder** (par exemple, *group-n6*).
 - f Cliquez sur le lien du nom DVS correspondant à l'instance de vSphere Distributed Switch associée aux dispositifs NSX Edge (par exemple, *dvs-1 (Mgmt_VDS)*).
 - g Copiez la valeur de la chaîne uuid. Utilisez cette valeur pour dvsUuid lors de l'extraction et de la mise à jour des données opaques.
- 3 Vérifiez si des données opaques existent pour le port spécifié.
 - a Accédez à `https://<vc-ip>/mob/?moid=DVSManger&vmodl=1`.
 - b Cliquez sur **fetchOpaqueDataEx**.
 - c Dans le champ **selectionSet**, collez l'entrée XML suivante :


```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example
dvsUuid -->
  <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

Utilisez le numéro de port et la valeur dvsUuid que vous avez récupérés pour l'interface de jonction NSX Edge.

 - d Définissez `isRuntime` sur `false`.
 - e Cliquez sur **Appeler la méthode**. Si le résultat affiche des valeurs pour `vim.dvs.OpaqueData.ConfigInfo`, cela signifie que des données opaques sont déjà définies, utilisez l'opération `edit` lorsque vous définissez le port de réception. Si la valeur de `vim.dvs.OpaqueData.ConfigInfo` est vide, utilisez l'opération `add` lorsque vous définissez le port de réception.
- 4 Configurez le port de réception dans le navigateur d'objet géré vCenter (MOB).
 - a Accédez à `https://<vc-ip>/mob/?moid=DVSManger&vmodl=1`.
 - b Cliquez sur **updateOpaqueDataEx**.

- c Dans le champ **selectionSet**, collez l'entrée XML suivante. Par exemple,

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example
dvsUuid -->
  <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

Utilisez la valeur dvsUuid que vous avez récupérée à partir du MOB de vCenter.

- d Dans le champ opaqueDataSpec, collez l'une des entrées XML suivantes.

Utilisez cette entrée pour activer un port de réception si aucune donnée opaque n'est définie (operation est défini sur add) :

```
<opaqueDataSpec>
  <operation>add</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
xsi:type="vmidl.Binary">AAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
</opaqueData>
  </opaqueData>
</opaqueDataSpec>
```

Utilisez cette entrée pour activer un port de réception si des données opaques sont déjà définies (operation est défini sur edit) :

```
<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
xsi:type="vmidl.Binary">AAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
</opaqueData>
  </opaqueData>
</opaqueDataSpec>
```

Utilisez cette entrée pour désactiver un port de réception :

```
<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData
xsi:type="vmidl.Binary">AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
</opaqueData>
  </opaqueData>
</opaqueDataSpec>
```

```

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=
```

- e Définissez `isRuntime` sur `false`.
- f Cliquez sur **Appeler la méthode**.

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.

Conditions préalables

- Vérifiez que vous disposez d'un profil de pont Edge.
- 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 et sécurité avancées > Mise en réseau > Commutation**.
- 3 Cliquez sur le nom d'un commutateur de superposition (type de trafic : superposition).
- 4 Cliquez sur **Éléments associés > Profils de pont Edge**.
- 5 Cliquez sur **Attacher**.
- 6 Pour établir l'association avec un profil de pont Edge, procédez comme suit :
 - a Sélectionnez un profil de pont Edge.
 - b Sélectionnez une zone de transport.
 - c Entrez un ID de VLAN.
 - d Cliquez sur **Enregistrer**.

7 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 profil de pont.

Résultats

Vous pouvez tester la fonctionnalité du pont en effectuant un test ping à partir de la machine virtuelle interne à NSX-T Data Center sur un nœud externe à NSX-T Data Center.

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"
}
```

NSX-T Data Center prend en charge un modèle de routage à deux niveaux.

Le niveau supérieur est le routeur logique de niveau 0. Ascendant, le routeur logique de niveau 0 se connecte à un ou plusieurs routeurs physiques ou commutateurs de couche 3 et sert de passerelle à l'infrastructure physique. Descendant, le routeur logique de niveau 0 se connecte à un ou plusieurs routeurs logiques de niveau 1 ou directement à un ou plusieurs commutateurs logiques.

Le niveau inférieur est le routeur logique de niveau 1. Ascendant, le routeur logique de niveau 1 se connecte à un routeur logique de niveau 0. Descendant, il se connecte à un ou plusieurs commutateurs logiques.

Note Si vous utilisez l'interface utilisateur **Mise en réseau et sécurité avancées** pour modifier des objets créés dans l'interface de stratégie, il se peut que certains paramètres ne soient pas configurables. Cette icône est située à côté de ces paramètres en lecture seule : . Pour plus d'informations, reportez-vous à la section [Chapitre 1 Présentation de NSX Manager](#).

Ce chapitre contient les rubriques suivantes :

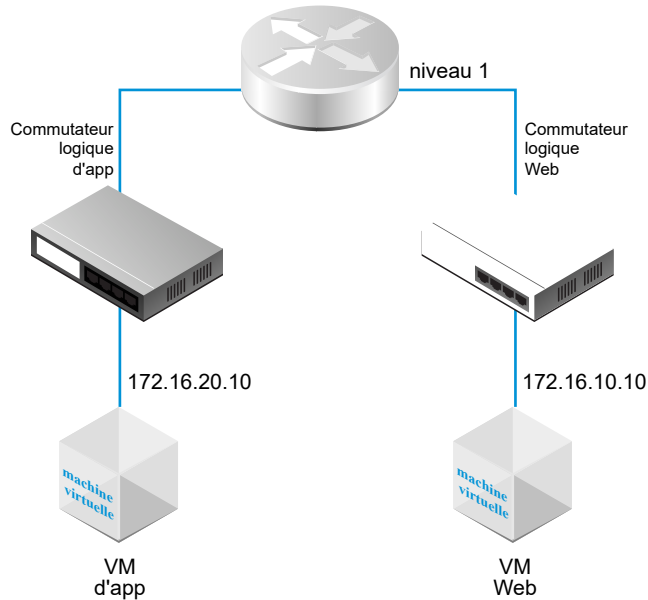
- [Routeur logique de niveau 1](#)
- [Routeur logique de niveau 0](#)

Routeur logique de niveau 1

Les routeurs logiques de niveau 1 disposent de ports de liaison descendante pour se connecter à des commutateurs logiques et des ports de liaison montante pour se connecter à des routeurs logiques de niveau 0.

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

Figure 14-1. 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.

Dans certains scénarios, les clients externes envoient des requêtes ARP pour les adresses MAC liées à des ports d'adresse IP virtuelle pour l'équilibreur de charge. Cependant, ces ports n'ont pas d'adresses MAC et ne peuvent pas traiter ce type de requête. Le proxy ARP est implémenté sur les ports de service centralisés d'un routeur logique de niveau 1 pour traiter les requêtes ARP pour le compte des ports d'adresse IP virtuelle pour l'équilibreur de charge.

Lorsqu'un routeur logique de niveau 1 est configuré avec DNAT, le pare-feu Edge et l'équilibreur de charge, le trafic vers et depuis un autre routeur logique de niveau 1 est traité dans cet ordre : DNAT, le pare-feu Edge, puis l'équilibreur de charge. Le trafic dans le routeur logique de niveau 1 est traité d'abord via DNAT, puis l'équilibreur de charge. Le traitement du pare-feu Edge est ignoré.

Sur un routeur logique de niveau 0 ou de niveau 1, vous pouvez configurer différents types de ports. Un type est appelé port de service centralisé (CSP). Vous devez configurer un CSP sur un routeur logique de niveau 0 en mode actif-en veille ou un routeur logique de niveau 1 pour vous connecter à un commutateur logique supporté par VLAN ou pour créer un routeur logique de niveau 1 autonome. Un CSP prend en charge les services suivants sur un routeur logique de niveau 0 en mode actif-en veille ou un routeur logique de niveau 1 :

- NAT
- Équilibrage de charge

- Pare-feu avec état
- VPN (IPsec et L2VPN)

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 [Routeur logique de niveau 1](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Routeurs > Routeurs > Ajouter**.
- 3 Sélectionnez **Routeur de niveau 1**, et entrez un nom pour le routeur logique et éventuellement une description.
- 4 (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.

- 5 (Facultatif) Sélectionnez un cluster NSX Edge.

Pour désélectionner un cluster que vous avez sélectionné, cliquez sur l'icône **x**. 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.

- 6 (Facultatif) Cliquez sur le bouton bascule **Déplacement en veille** pour activer ou désactiver le déplacement en veille.

Le déplacement en veille signifie que si le nœud Edge sur lequel le routeur logique actif ou en veille est en cours d'exécution échoue, un nouveau routeur logique en veille est créé sur un autre nœud Edge pour maintenir la haute disponibilité. Si le nœud Edge qui échoue exécute le routeur logique actif, le routeur logique de secours initial devient le routeur logique actif et un nouveau routeur logique en veille est créé. Si le nœud Edge qui a échoué exécute le routeur logique en veille, le nouveau routeur logique en veille le remplace.

- 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**.

Résultats

Une fois le routeur logique créé, si vous voulez supprimer le cluster Edge de la configuration du routeur, procédez comme suit :

- Cliquez sur le nom du routeur pour voir les détails de la configuration.
- Sélectionnez **Services > Pare-feu Edge**.
- Cliquez sur **Désactiver le pare-feu**.
- Cliquez dans l'onglet **Présentation**, puis sur **Modifier**.
- Dans le champ **Cluster Edge**, cliquez sur l'icône **x**.
- Cliquez sur **Enregistrer**.

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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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.

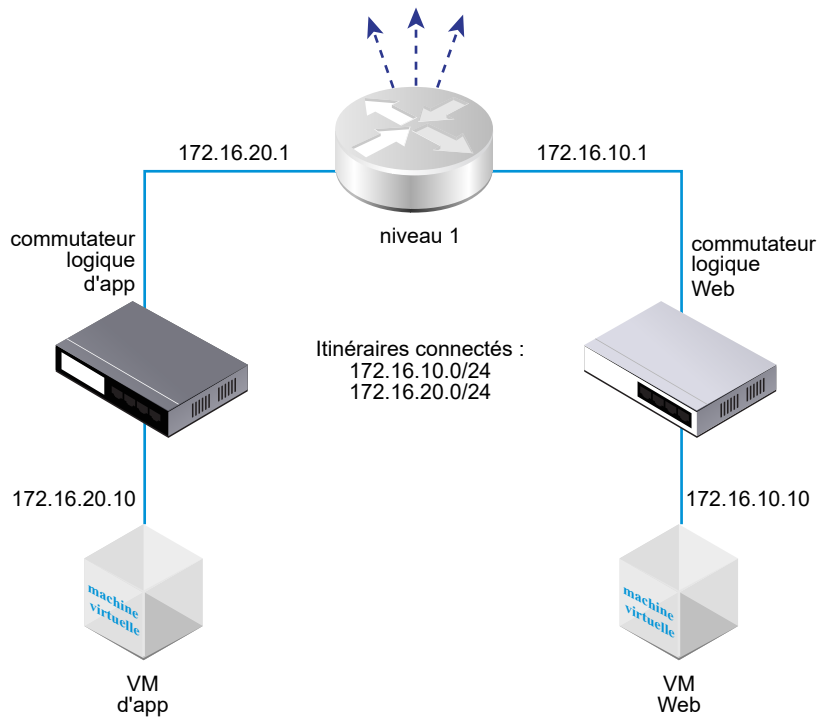
Si l'association est destinée à un port de commutateur existant, sélectionnez le port dans le menu déroulant.
- 11 Entrez l'adresse IP du port de routeur dans la notation CIDR.
- 12 Cliquez sur **Ajouter**.

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 13 Commutateurs logiques](#).
- 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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**
- **Annoncer toutes les routes du redirecteur DNS**

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 [Routeur logique de niveau 0](#).

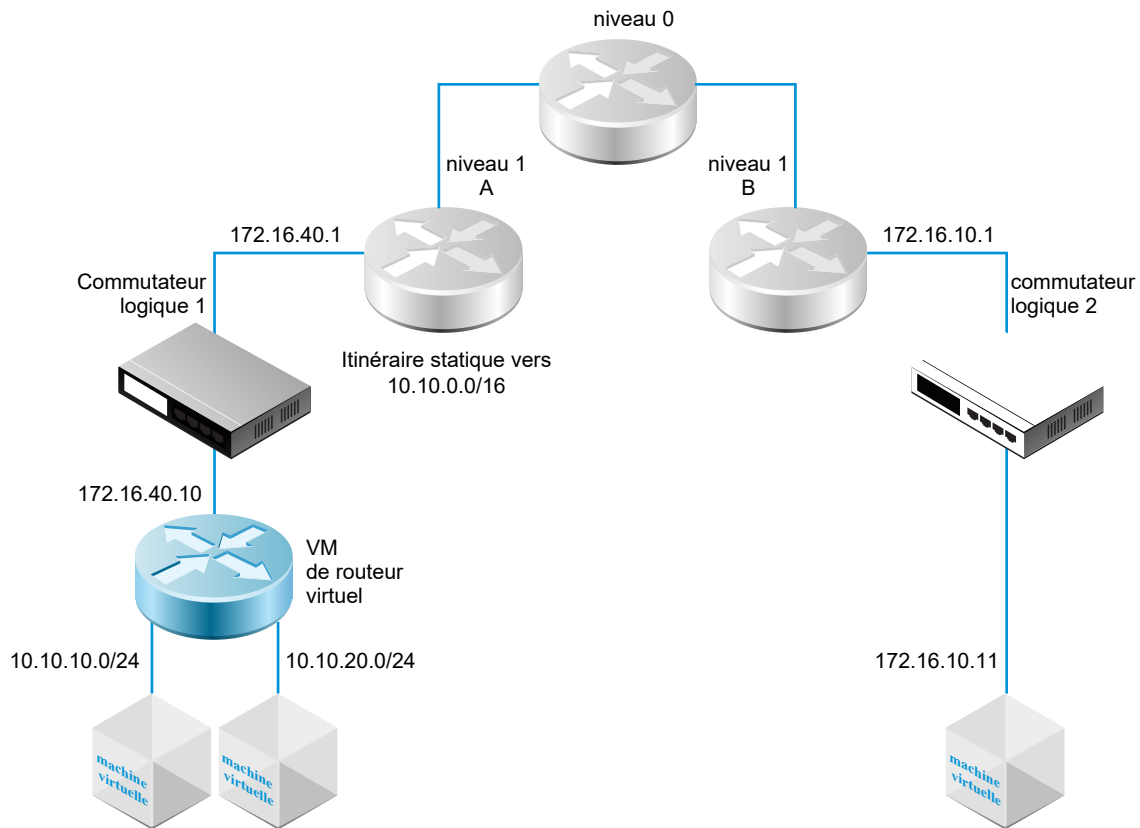
Si vous disposez déjà d'un routeur logique de niveau 0 connecté au routeur logique de niveau 1, vous pouvez vérifier que le routeur de niveau 0 apprend les itinéraires connectés du routeur de niveau 1. Reportez-vous à la section [Vérifier qu'un routeur de niveau 0 a appris des itinéraires d'un routeur 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 14-2. Topologie de l'itinéraire statique du routeur logique de niveau 1



Les itinéraires statiques récurrents sont pris en charge.

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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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.

La route statique basée sur IPv6 est prise en charge. Les préfixes IPv6 ne peuvent comporter qu'un saut suivant de type IPv6.

Par exemple, 10.10.10.0/16 ou une adresse IPv6.

- 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 n'importe quelle combinaison des services IPSec, DNAT, Pare-feu, Équilibrage de charge et Insertion de services. Pour l'entrée, l'ordre de traitement est le suivant : IPSec – DNAT – Pare-feu – Équilibrage de charge – Insertion de services. Pour la sortie, l'ordre de traitement est le suivant : Insertion de services – Équilibrage de charge – Pare-feu – DNAT – IPSec.

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.

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 est pris en charge. Vous pouvez configurer une adresse IP de serveur virtuel d'équilibrage de charge ou une adresse IP SNAT d'équilibrage de charge dans le sous-réseau du CSP. Par exemple, si l'adresse IP du CSP est 1.1.1.1/24, l'adresse IP virtuelle peut être 1.1.1.2. Il peut également s'agir d'une adresse IP dans un autre sous-réseau, telle que 2.2.2.2 si le routage est correctement configuré afin que le trafic pour 2.2.2.2 puisse atteindre le routeur autonome.
- 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.

Procédure

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

- 6 Cliquez sur **Ajouter**.
- 7 Cliquez sur le nom du routeur que vous venez de créer.
- 8 Cliquez sur l'onglet **Configuration** et sélectionnez **Ports de routeur**.
- 9 Cliquez sur **Ajouter**.
- 10 Entrez un nom pour le port de routeur et éventuellement une description.
- 11 Dans le champ **Type**, sélectionnez **Centralisé**.
- 12 Pour **Mode URPF**, sélectionnez **Strict** ou **Aucun**.
URPF (Unicast Reverse Path Forwarding) est une fonctionnalité de sécurité.
- 13 (Requis) Sélectionnez un commutateur logique.
- 14 Indiquez si cette association crée un port de commutateur ou met à jour un port de commutateur existant.
- 15 Entrez l'adresse IP du port de routeur dans la notation CIDR.
- 16 Cliquez sur **Ajouter**.

Routeur logique de niveau 0

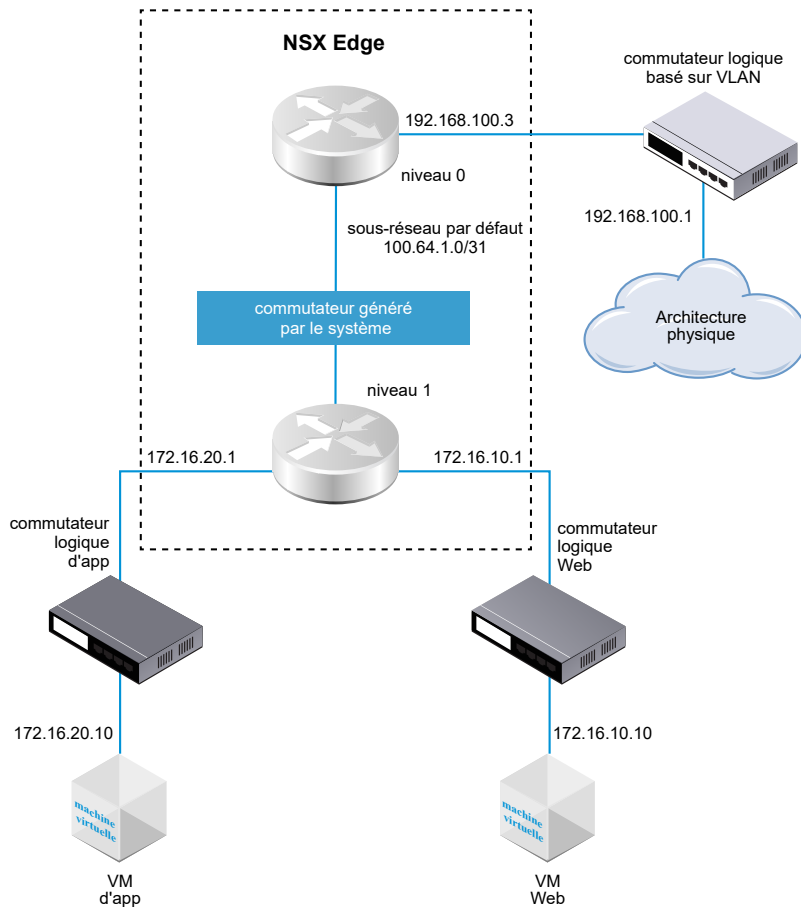
Un routeur logique de niveau 0 fournit un service de passerelle entre le réseau physique et le réseau logique.

NSX Cloud Note Si vous utilisez NSX Cloud, consultez [Fonctionnalités de NSX-T Data Centerprises en charge avec NSX Cloud](#) pour obtenir la liste des entités logiques générées automatiquement, des fonctionnalités prises en charge et des configurations requises pour NSX Cloud.

Un nœud Edge ne peut prendre en charge qu'une seule passerelle de niveau 0 ou un seul routeur logique. Lorsque vous créez une passerelle de niveau 0 ou un routeur logique, assurez-vous de ne pas créer plus de passerelles de niveau 0 ou de routeurs logiques que le nombre de nœuds Edge dans le cluster NSX Edge.

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

Figure 14-3. 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.

Dans certains scénarios, des clients externes envoient des requêtes ARP pour les adresses MAC liées à des ports de bouclage ou IKE IP. Cependant, les ports de bouclage et IKE IP ne possèdent pas d'adresses MAC et ne peuvent pas traiter les requêtes de ce type. Le proxy ARP est implémenté sur la liaison montante et les ports de service centralisés d'un routeur logique de niveau 0 pour traiter les requêtes ARP au nom des ports de bouclage et IKE IP.

Lorsqu'un routeur logique de niveau 0 est configuré avec DNAT, IPsec et le pare-feu Edge, le trafic est traité dans cet ordre : IPsec, DNAT, puis pare-feu Edge.

Sur un routeur logique de niveau 0 ou de niveau 1, vous pouvez configurer différents types de ports. Un type est appelé port de service centralisé (CSP). Vous devez configurer un CSP sur un routeur logique de niveau 0 en mode actif-en veille ou un routeur logique de niveau 1 pour vous connecter à un commutateur logique supporté par VLAN ou pour créer un routeur logique de niveau 1 autonome. Un CSP prend en charge les services suivants sur un routeur logique de niveau 0 en mode actif-en veille ou un routeur logique de niveau 1 :

- NAT
- Équilibrage de charge
- Pare-feu avec état
- VPN (IPsec et L2VPN)

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 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 [Routeur logique de niveau 0](#).

Procédure

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

2 Sélectionnez **Mise en réseau et sécurité avancées > Routeurs > Routeurs > Ajouter**.

3 Sélectionnez **Routeur de niveau 0** dans le menu déroulant.

4 Attribuez un nom au routeur logique de niveau 0.

5 Sélectionnez un cluster NSX Edge existant dans le menu déroulant pour sauvegarder ce routeur logique de niveau 0.

6 (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.

7 (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.

8 (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 100.64.0.0/16. Chaque connexion homologue de niveau 0 à niveau 1 reçoit un sous-réseau /31 dans l'espace d'adressage 100.64.0.0/16.

9 Cliquez sur **Enregistrer**.

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

10 (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.

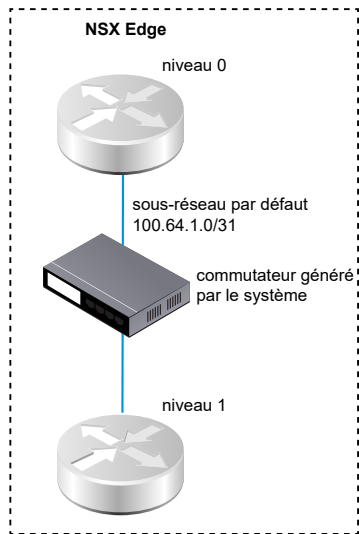
Configurez le routeur logique de niveau 0 pour le connecter à un commutateur logique VLAN afin de créer une liaison montante vers un réseau externe. Reportez-vous à la section [Connecter un routeur logique de niveau 0 à un commutateur logique VLAN pour la liaison montante NSX Edge](#).

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 100.64.0.0/16. Chaque connexion homologue de niveau 0 à niveau 1 reçoit un sous-réseau /31 dans l'espace d'adressage 100.64.0.0/16. 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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

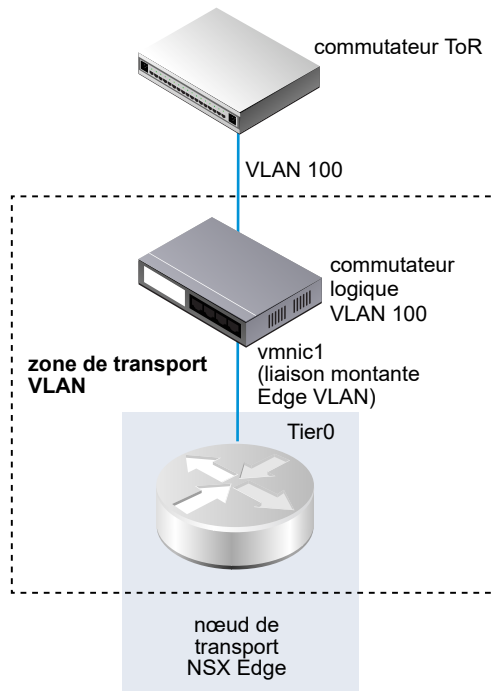
b    10.10.10.0/24      [20/0]      via 192.168.100.254
rl   100.91.176.0/31   [0/0]      via 169.254.0.1
c    169.254.0.0/28    [0/0]      via 169.254.0.2
ns   172.16.10.0/24    [3/3]      via 169.254.0.1
ns   172.16.20.0/24    [3/3]      via 169.254.0.1
c    192.168.100.0/24  [0/0]      via 192.168.100.2

```

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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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.

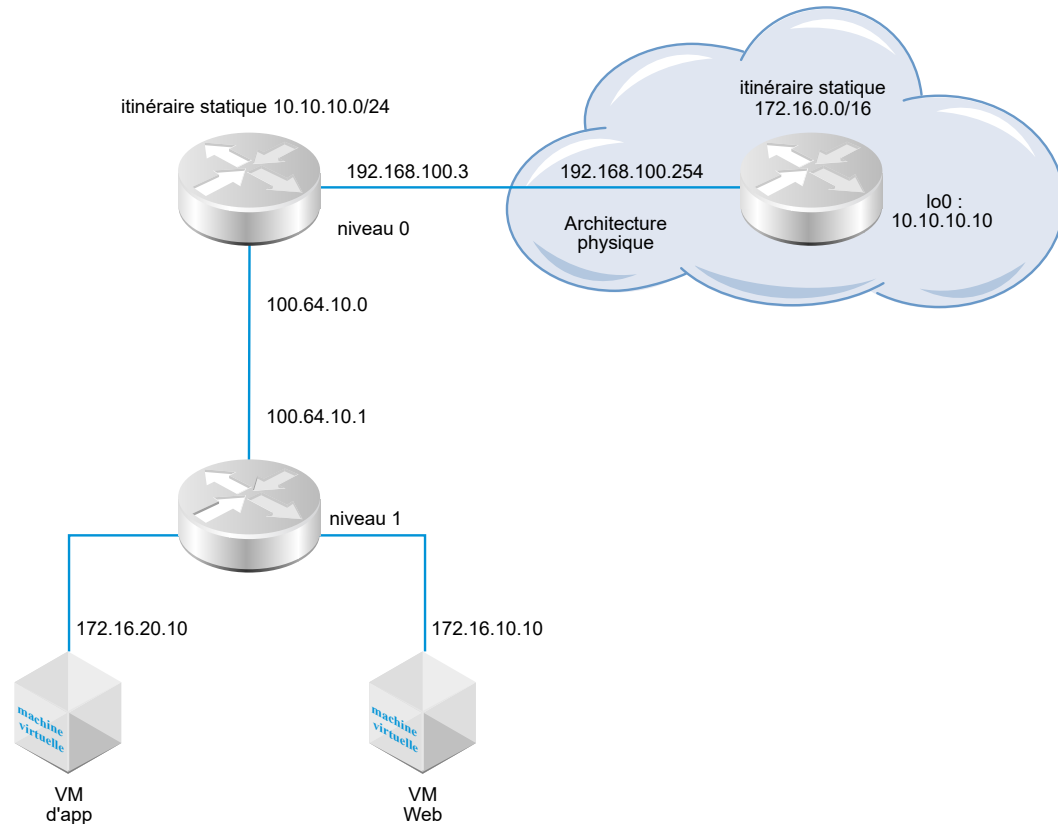
12 Cliquez sur **Ajouter**.

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 14-4. Topologie d'itinéraire statique



Les itinéraires statiques récursifs sont pris en charge.

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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 3 Sélectionnez le routeur logique de niveau 0.
- 4 Cliquez sur l'onglet **Routing** 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 route 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.

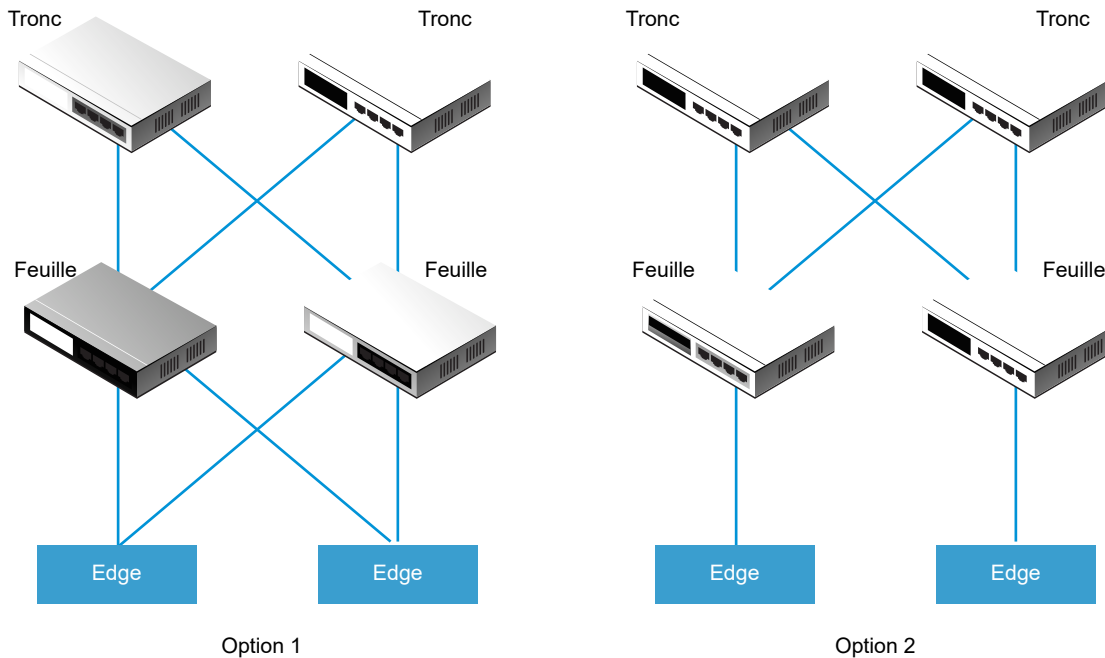
```
ping 10.10.10.10
```

```
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 ou interne (eBGP/iBGP) entre un routeur logique de niveau 0 et un routeur dans votre infrastructure physique.

La fonctionnalité iBGP présente les capacités et restrictions suivantes :

- La redistribution, les listes de préfixes et les cartes d'itinéraire sont prises en charge.
- Les réflecteurs d'itinéraire ne sont pas pris en charge.
- La confédération BGP n'est pas prise en charge.

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. Les voisins EBGP doivent être connectés directement et se trouver dans le même sous-réseau que la liaison montante de niveau 0. S'ils ne se trouvent pas dans le même sous-réseau, une traversée de tronçons multiples BGP doit être utilisée.

Un routeur logique de niveau 0 en mode actif-actif prend en charge le routage entre routeurs de service. Si le routeur n° 1 ne parvient pas à communiquer avec un routeur physique ascendant, le trafic est alors routé vers le routeur n° 2 dans le cluster actif-actif. Si le routeur #2 est capable de communiquer avec le routeur physique, le trafic entre le routeur #1 et le routeur physique n'est pas affecté.

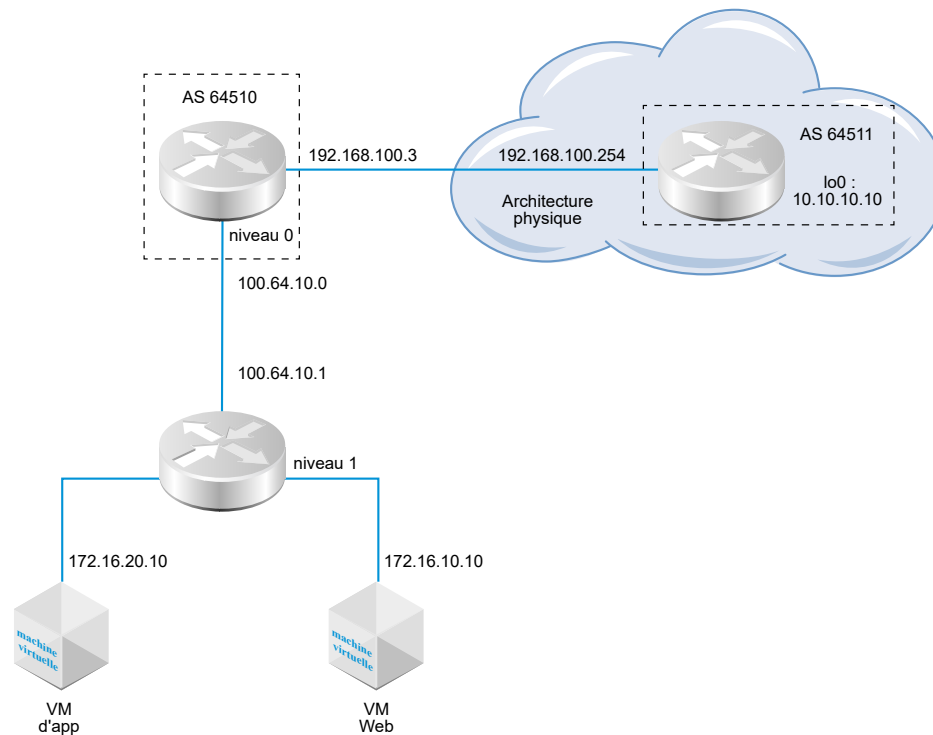
Dans une topologie avec un routeur logique de niveau 0 en mode actif-actif associé à un routeur logique de niveau 1 en mode actif-en veille, vous devez activer le routage inter SR pour gérer le routage asymétrique. Vous disposez d'un routage asymétrique si vous configurez une route statique sur l'un des SR ou si un SR doit atteindre la liaison montante d'un autre SR. De plus, notez ce qui suit :

- Dans le cas d'une route statique configurée sur un SR (par exemple, SR 1 sur le nœud Edge 1), un autre SR (par exemple, SR 2 sur le nœud Edge 2) peut apprendre la même route d'un homologue eBGP et préférer la route apprise à la route statique sur SR 1, ce qui peut être plus efficace. Pour vous assurer que SR 2 utilise la route statique configurée sur SR 1, configurez le routeur logique de niveau 1 en mode préventif et configurez le nœud Edge 1 comme nœud préféré.

- Si le routeur logique de niveau 0 dispose d'un port de liaison montante sur le nœud Edge 1 et d'un autre port de liaison montante sur le nœud Edge 2, le trafic ping des machines virtuelles de locataire vers les liaisons montantes fonctionne si les deux liaisons montantes se trouvent dans des sous-réseaux différents. Le trafic ping échoue si les deux liaisons montantes se trouvent dans le même sous-réseau.

Note L'ID de routeur utilisé 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 14-5. Topologie de connexion BGP



Prenez connaissance des scénarios suivants en cas d'échecs de la connexion impliquant BGP ou BFD :

- Lorsque BGP uniquement est configuré, si tous les voisins BGP sont arrêtés, l'état du routeur de service est inactif.
- Lorsque BFD uniquement est configuré, si tous les voisins BFD sont arrêtés, l'état du routeur de service est inactif.
- Lorsque BGP et BFD sont configurés, si tous les voisins BGP et BFD sont arrêtés, l'état du routeur de service est inactif.

- Lorsque les routes BGP et statiques sont configurées, si tous les voisins BGP sont arrêtés, l'état du routeur de service est inactif.
- Lorsque les routes statiques uniquement sont configurées, l'état du routeur de service est toujours actif, sauf si le nœud subit une panne ou est en mode de maintenance.

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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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 Entrez le nombre AS local.

Par exemple, 64510.

- b Cliquez sur le bouton **État** pour activer ou désactiver BGP.
- c Cliquez sur le bouton **ECMP** pour activer ou désactiver ECMP.
- d Cliquez sur le bouton bascule **Redémarrage normal** pour activer ou désactiver le redémarrage normal.

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.

- e Si ce routeur logique est en mode actif-actif, faites basculer le bouton **Routage Inter SR** pour activer ou désactiver le routage inter SR.
- f Configurez l'agrégation d'itinéraires.
- g 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 Spécifiez la limite maximale de tronçon.
La valeur par défaut est 1.
- 9 Entrez le nombre AS distant.
Par exemple, 64511 (voisin eBGP) ou 64510 (voisin iBGP).
- 10 Configurez les temporisateurs (durée de survie et durée de retenue) et un mot de passe.
- 11 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 Cliquez sur l'onglet **Familles d'adresses** pour ajouter une famille d'adresses.
- 13 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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.

- 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 **Modifier** pour activer ou désactiver la redistribution d'itinéraire.
- 6 Cliquez sur **Ajouter** pour ajouter un ensemble de critères de redistribution d'itinéraire.

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	Sélectionnez une ou plusieurs des sources suivantes : <ul style="list-style-type: none"> ■ TO connecté ■ Liaison montante TO ■ Liaison descendante TO ■ CSP TO ■ Bouclage TO ■ TO statique ■ NAT TO ■ IP du transmetteur DNS TO ■ Adresse IP locale IPSec TO ■ T1 connecté ■ CSP T1 ■ Liaison descendante T1 ■ T1 statique ■ SNAT D'ÉQUILIBRAGE DE CHARGE T1 ■ NAT T1 ■ VIP D'ÉQUILIBRAGE DE CHARGE T1 ■ IP du transmetteur DNS T1
Carte de route	(Facultatif) Attribuez une carte de route pour filtrer une séquence d'adresses IP à partir de la redistribution d'itinéraire.

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. Après 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-edgel(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.

```
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  100.91.176.1 (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

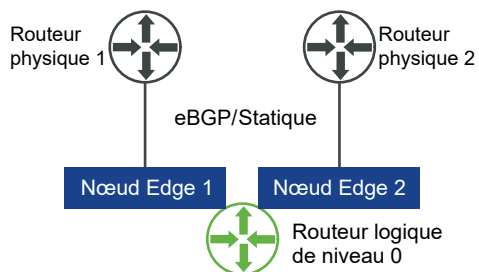
Configurez la fonctionnalité de routage supplémentaire, par exemple ECMP.

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.

Le routeur logique de niveau 0 doit être en mode actif-actif pour qu'ECMP soit disponible. Un maximum de huit chemins ECMP sont pris en charge. L'implémentation d'ECMP sur NSX Edge est basée sur les 5 tuples du numéro de protocole, de l'adresse source, de l'adresse de destination, du port source et du port de destination. L'algorithme utilisé pour distribuer les données entre les chemins ECMP n'est pas de type Round Robin. Par conséquent, certains chemins peuvent supporter un chemin plus important que d'autres. Notez que si le protocole est IPv6 et que l'en-tête IPv6 comporte plusieurs en-têtes d'extension, ECMP sera basé uniquement sur les adresses source et de destination.

Figure 14-6. Topologie du routage ECMP



Par exemple, la topologie ci-dessus montre un routeur logique de niveau 0 unique en mode actif-actif exécuté sur un cluster NSX Edge à 2 nœuds. Deux ports de liaison montante sont configurés, un sur chaque nœud Edge.

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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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 .
MTU	Si vous laissez ce champ vide, la valeur par défaut est 1500.
Nœud de transport	Attribuez le nœud de transport Edge à partir du menu déroulant.
Mode URPF	URPF (Unicast Reverse Path Forwarding) est une fonctionnalité de sécurité. Il est recommandé de la définir sur Aucun si vous disposez de plusieurs nœuds Edge actifs-actifs en mode ECMP. La valeur par défaut est Strict .
Commutateur logique	Attribuez le commutateur logique VLAN à partir du menu déroulant.
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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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 Vérifiez que le routeur distribué de niveau 0 est connecté.

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

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

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

- 9 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>
```

- 10 Utilisez n'importe quel outil capable de générer le trafic d'une VM source connectée au routeur de niveau 0 vers une VM de destination.

- 11 Observez le trafic sur les deux nœuds Edge.

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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.

- 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	<p>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 :</p> <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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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**.

Vous pouvez configurer NAT à partir de l'onglet **Mise en réseau et sécurité avancées**.

Note Si vous utilisez l'interface utilisateur **Mise en réseau et sécurité avancées** pour modifier des objets créés dans l'interface de stratégie, il se peut que certains paramètres ne soient pas configurables. Cette icône est située à côté de ces paramètres en lecture seule : ⊖. Pour plus d'informations, reportez-vous à la section [Chapitre 1 Présentation de NSX Manager](#).

Ce chapitre contient les rubriques suivantes :

- [Traduction d'adresse réseau](#)

Traduction d'adresse réseau

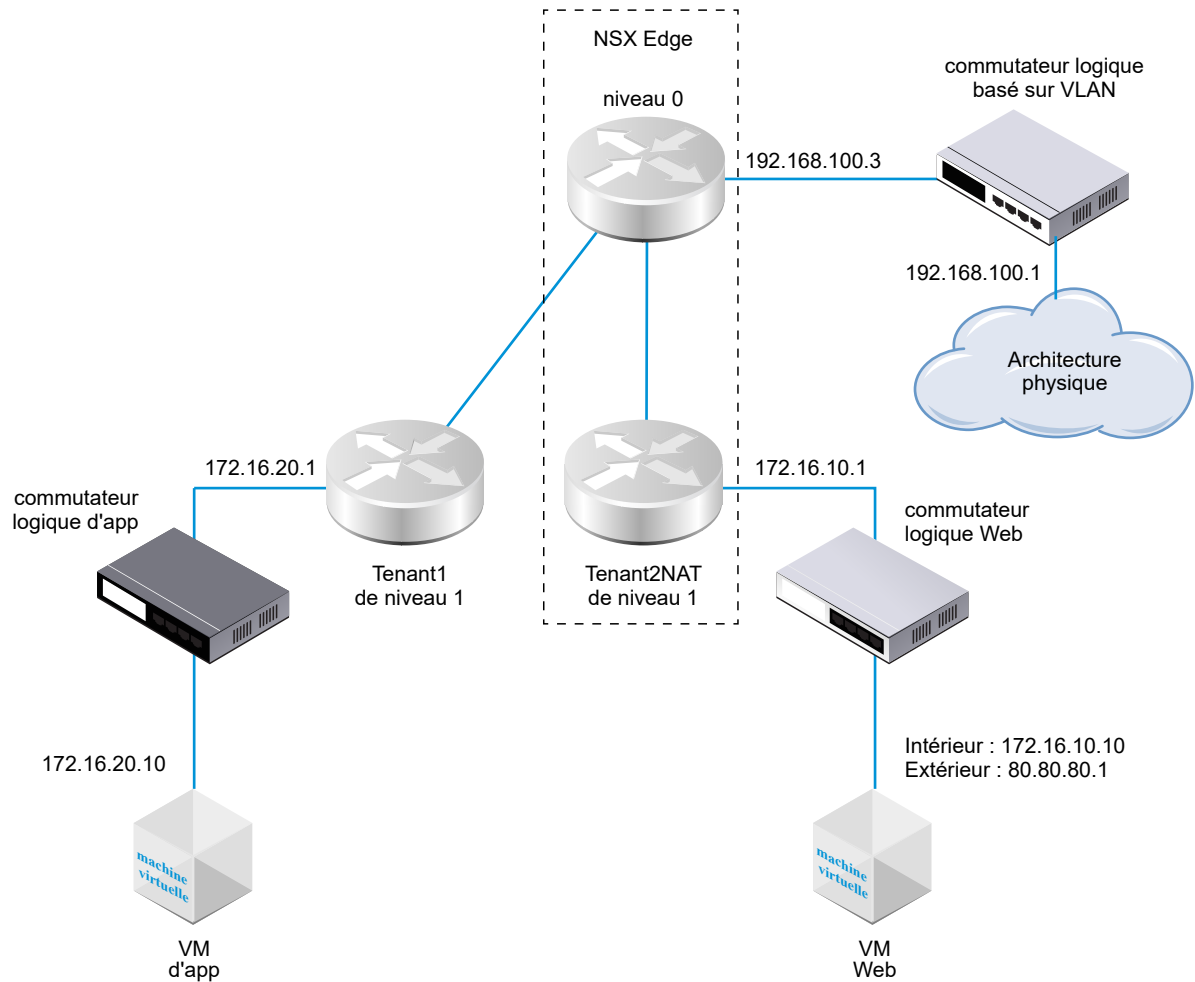
La traduction d'adresse réseau (NAT) dans NSX-T Data Center peut être configurée sur des routeurs logiques de niveau 0 et de niveau 1.

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.

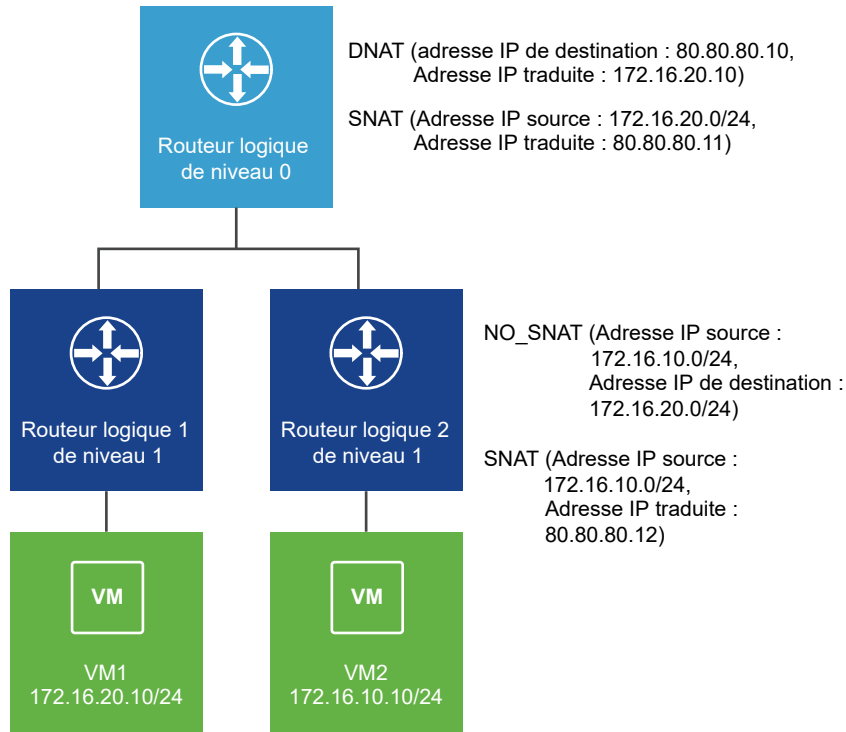
La NAT est appliquée au niveau de la liaison montante du routeur logique Tenant2NAT sur sa connexion au routeur logique de niveau 0.

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 15-1. Topologie de la NAT



Remarque : dans le scénario suivant, NAT hairpinning n'est pas pris en charge. DNAT et SNAT sont configurés sur le routeur logique de niveau 0. NO_SNAT et SNAT sont configurés sur le routeur logique 2 de niveau 1. VM2 ne pourra pas accéder à VM1 en utilisant l'adresse externe 80.80.80.10 de VM1.



Les sections suivantes décrivent comment créer des règles NAT à l'aide de l'interface utilisateur du gestionnaire. Vous pouvez également effectuer un appel d'API (`POST /api/v1/logical-routers/<logical-router-id>/nat/rules?action=create_multiple`) pour créer plusieurs règles NAT en même temps. Pour plus d'informations, reportez-vous au *Guide de l'API de NSX-T Data Center*.

NAT de niveau 1

Un routeur logique de niveau 1 prend en charge la traduction de l'adresse de réseau source (SNAT), la traduction de l'adresse de réseau de destination (DNAT) et la traduction de l'adresse de réseau réflexive.

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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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 :

Tenant2NAT

Présentation Configuration ▾ Routage ▾ Services ▾

NAT | ACTUALISER

Aucune statistique n'a été collectée

+ AJOUTER ✎ MODIFIER 🗑 SUPPRIMER

ID	Action	Correspondance					Traduit		Appliq	Statist
		Protocole	IP source	Ports source	Adresse IP de destination	Ports de destination	IP	Ports		
▼ Priorité: 1024										
✓ 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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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 :

Tenant2NAT

Présentation

Configuration

Routage

Services

NAT

ACTUALISER

Aucune statistique n'a été collectée

+ AJOUTER

MODIFIER

SUPPRIMER

ID	Action	Correspondance					Traduit		Appliqué à	Statistique
		Protocole	IP source	Ports source	Adresse IP de destination	Ports de destination	IP	Ports		
Priorité: 1024										
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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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 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**
- **Annoncer toutes les routes du redirecteur DNS**

- 6 Cliquez sur **Enregistrer**.

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://<nsx-manager-ip-address>>.
- 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 Cliquez sur **Modifier** pour activer ou désactiver la redistribution d'itinéraire.
- 6 Cliquez sur **Ajouter** pour ajouter un ensemble de critères de redistribution d'itinéraire.

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	Sélectionnez une ou plusieurs des sources suivantes : <ul style="list-style-type: none"> ■ TO connecté ■ Liaison montante TO ■ Liaison descendante TO ■ CSP TO ■ Bouclage TO ■ TO statique ■ NAT TO ■ IP du transmetteur DNS TO ■ Adresse IP locale IPSec TO ■ T1 connecté ■ CSP T1 ■ Liaison descendante T1 ■ T1 statique ■ SNAT D'ÉQUILIBRAGE DE CHARGE T1 ■ NAT T1 ■ VIP D'ÉQUILIBRAGE DE CHARGE T1 ■ IP du transmetteur DNS T1
Carte de route	(Facultatif) Attribuez une carte de route pour filtrer une séquence d'adresses IP à partir de la redistribution d'itinéraire.

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, rl - 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

Un routeur logique de niveau 0 en mode actif-en veille prend en charge la NAT source (SNAT), la NAT de destination (DNAT) et la NAT réflexive. Un routeur logique de niveau 0 en mode actif-actif prend en charge uniquement la NAT réflexive.

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

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

Vous pouvez également désactiver la SNAT ou la DNAT 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.

Une SNAT configurée sur la liaison montante d'un routeur logique niveau 0 traite le trafic depuis un routeur logique de niveau 1 comme toute autre liaison montante sur le routeur logique de niveau 0.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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**, **Réflexive**, **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.

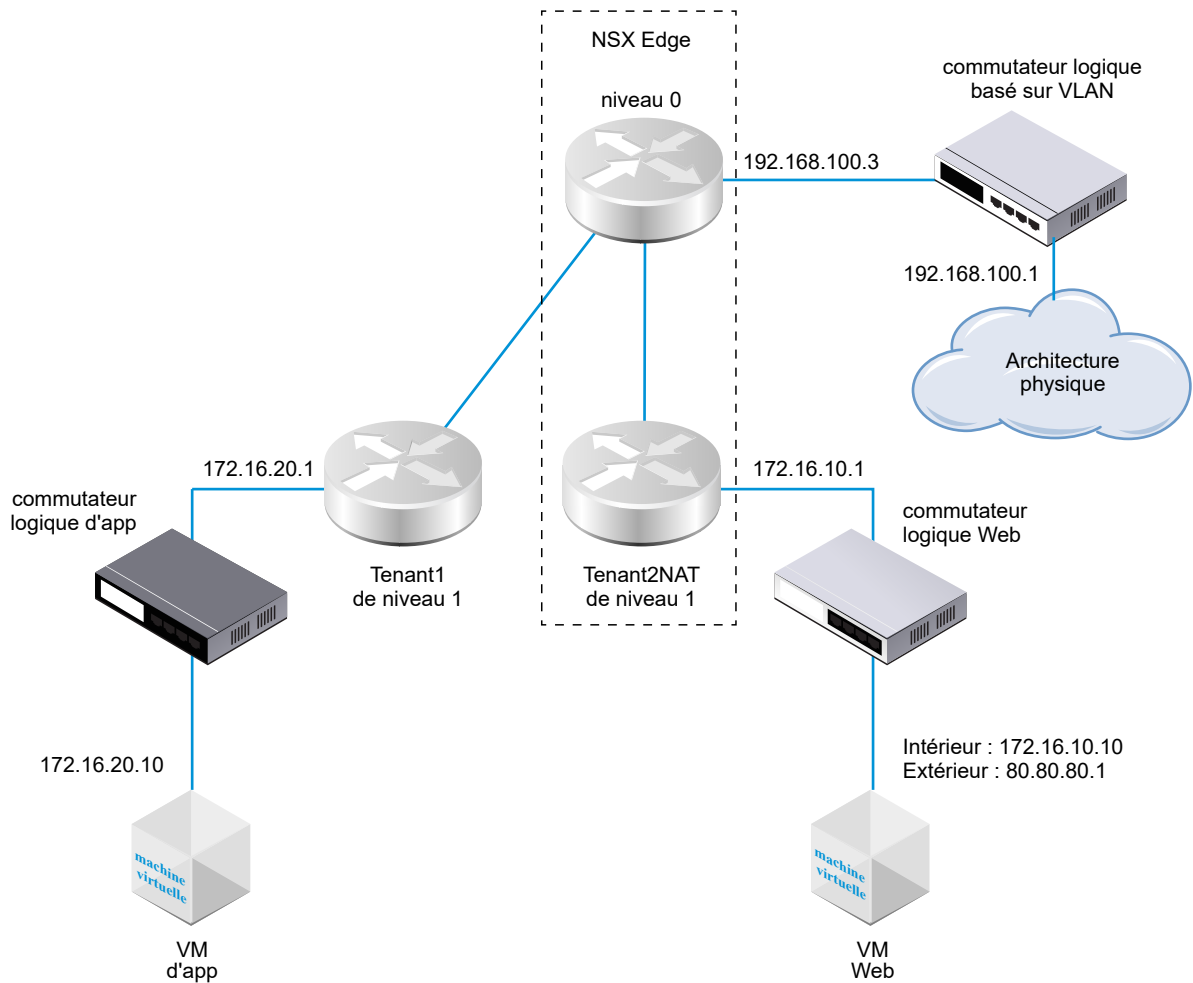
16 (Facultatif) Modifiez le paramètre de contournement de pare-feu.

Ce paramètre est activé par défaut.

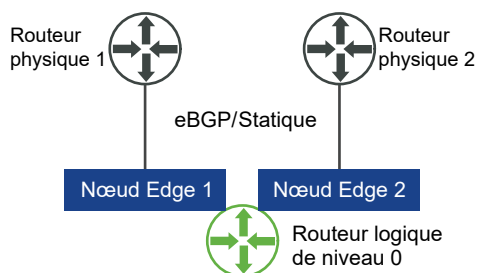
NAT réflexive

Lorsqu'un routeur logique de niveau 0 est exécuté en mode ECMP actif-actif, vous ne pouvez pas configurer une NAT avec état où des chemins d'accès asymétriques peuvent causer des problèmes. Pour les routeurs en mode actif-actif, vous pouvez configurer 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 ci-dessous, 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 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 destinatic	IP	Ports		
▼ Priorité: 1024										
✓ 2048	Réflexif	Quelconque	80.80.80.1	Quelconque	Quelconque	Quelconque	172.16.10.10	Quelconque		

Regroupement d'objets avancé

16

Vous pouvez créer des ensembles d'IP, des pools d'IP, des ensembles d'adresses MAC, des NSGroups et des NSServices. Vous pouvez également gérer des balises pour les machines virtuelles.

Note Si vous utilisez l'interface utilisateur **Mise en réseau et sécurité avancées** pour modifier des objets créés dans l'interface de stratégie, il se peut que certains paramètres ne soient pas configurables. Cette icône est située à côté de ces paramètres en lecture seule : . Pour plus d'informations, reportez-vous à la section [Chapitre 1 Présentation de NSX Manager](#).

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 qui peuvent être utilisées comme sources et destinations dans les 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 NSGroups. Aucun ensemble d'adresses IP créé par cette méthode ne sera visible en mode Stratégie. En mode Stratégie, nous pouvons créer un groupe et ajouter des membres sous forme d'adresses IP, de plages, d'adresses réseau ou d'adresses MAC en accédant à **Inventaire > Groupes > Définir les membres** et en spécifiant des adresses IP ou MAC.

Note Les adresses IPv4 et IPv6 sont prises en charge pour les plages source ou de destination 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Inventaire > Groupes > Ensembles d'adresses IP > Ajouter**.
- 3 Entrez un nom.
- 4 (Facultatif) Entrez une description.
- 5 Dans le champ **Membres**, entrez des adresses IP individuelles, des plages d'adresses IP et des sous-réseaux sous la forme d'une liste d'éléments séparés par des virgules.
- 6 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Inventaire > Groupes > IP Pools > Ajouter**.
- 3 Entrez le nom que vous souhaitez attribuer au nouveau pool d'adresses IP.
- 4 (Facultatif) Entrez une description.
- 5 Cliquez sur **Ajouter**.
- 6 Cliquez sur la cellule Plages d'adresses IP et entrez les plages d'adresses IP.
 Passez le curseur de la souris sur le coin supérieur droit de chaque cellule et cliquez sur l'icône de crayon pour la modifier.
- 7 (Facultatif) Entrez une passerelle.
- 8 Entrez une adresse IP CIDR avec un suffixe.
- 9 (Facultatif) Entrez des serveurs DNS.
- 10 (Facultatif) Entrez un suffixe DNS.
- 11 Cliquez sur **Enregistrer**.

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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Inventaire > Groupes > Ensembles d'adresses MAC > Ajouter**.
- 3 Entrez un nom.
- 4 (Facultatif) Entrez une description.
- 5 Entrez les adresses MAC sous la forme d'une liste d'adresses séparées par une virgule.
- 6 Cliquez sur **AJOUTER**.

Créer un NSGroup

Les NSGroups peuvent être configurés de manière à inclure une combinaison d'ensembles d'adresses IP, d'ensembles d'adresses MAC, de ports logiques, de commutateurs logiques et d'autres NSGroups. Les NSGroups comprenant des commutateurs logiques, des ports logiques et des machines virtuelles peuvent être spécifiés en tant que sources et destinations, ainsi que dans le champ `Applied To` d'une règle de pare-feu. Les NSGroups comprenant des ensembles d'adresses IP et des ensembles d'adresses MAC sont ignorés dans le champ `Applied To` d'un pare-feu distribué.

NSX Cloud Note Si vous utilisez NSX Cloud, consultez [Fonctionnalités de NSX-T Data Centerprises en charge avec NSX Cloud](#) pour obtenir la liste des entités logiques générées automatiquement, des fonctionnalités prises en charge et des configurations requises pour NSX Cloud.

Un NSGroup a les caractéristiques suivantes :

- 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 que d'un membre effectif, LogicalSwitch-1. Ensuite, vous ajoutez NSGroup-3 et spécifiez NSGroup-2 comme membre. NSGroup-3 dispose désormais du membre direct NSGroup-2 et des

membres effectifs LogicalSwitch-1 et LogicalSwitch-2. Si, dans la table des groupes principaux, vous cliquez sur un groupe et sélectionnez **Éléments associés > NSGroups**, NSGroup-1, NSGroup-2 et NSGroup-3 s'affichent, car LogicalSwitch-1 est membre de chacun d'eux, directement ou indirectement.

- 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. NSX Manager vérifie deux fois par jour (à 7 h et à 19 h) que les NSGroups respectent la limite. Un dépassement de cette limite n'affecte aucune fonctionnalité, mais peut avoir un impact négatif sur les performances.
 - 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. Lorsque le nombre dépasse 5 000, un message d'avertissement signale que le NSGroup a atteint le nombre maximal et indique le nombre total actuel dans le NSGroup.
 - 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 traductions actuel dans le conteneur - IP : ..., MAC : ..., VIF : ...` s'affiche dans le fichier journal.
- Le nombre maximal pris en charge de machines virtuelles est de 10 000.
- Vous pouvez créer un maximum de 10 000 NSGroup.

Vous pouvez accéder à l'écran pour tout objet qu'il est possible d'ajouter en tant que membre d'un NSGroup, puis sélectionner **Éléments associés > NSGroups**.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Inventaire > Groupes > Ajouter**.
- 3 Entrez un nom pour le NSGroup.
- 4 (Facultatif) Entrez une description.
- 5 (Facultatif) Cliquez sur **Critères d'appartenance**.

Pour chaque critère, vous pouvez spécifier jusqu'à cinq règles qui sont combinées avec l'opérateur logique AND. Le critère d'appartenance disponible peut s'appliquer aux éléments suivants :

- **Port logique** : peut spécifier une balise et éventuellement une étendue.
- **Commutateur logique** : peut spécifier une balise et éventuellement une étendue.

- **Machine virtuelle** : peut spécifier un nom, une balise, un nom de SE d'ordinateur ou un nom d'ordinateur qui est égal à, contient, commence par, se termine par ou n'est pas égal à une chaîne donnée.
- **Nœud de transport** : peut spécifier un type de nœud correspondant à un nœud Edge ou à un nœud hôte.
- **Ensemble d'adresses IP** : peut spécifier une balise et éventuellement une étendue.

6 (Facultatif) Cliquez sur **Membres** pour sélectionner des membres.

Les types de membres disponibles sont les suivants :

- **Groupe AD** : les NSGroups contenant des groupes AD ne peuvent être utilisés que dans le champ `extended_source` d'une règle de pare-feu distribué. En outre, ils doivent être les seuls membres du groupe. Par exemple, aucun NSGroup ne peut contenir à la fois des ensembles d'adresses IP et des groupes AD.
- **Ensemble d'adresses IP** : peut inclure des adresses IPv4 et IPv6.
- **Port logique** : peut inclure des adresses IPv4 et IPv6.
- **Commutateur logique** : peut inclure des adresses IPv4 et IPv6.
- **Ensemble d'adresses MAC**
- **NSGroup**
- **Nœud de transport**
- **VIF**
- **Machine virtuelle**

7 Cliquez sur **AJOUTER**.

Le groupe est ajouté à la table des groupes. Cliquez sur le nom d'un groupe pour en afficher un aperçu et modifier les informations du groupe (critères d'appartenance, membres, applications et groupes associés). Faites défiler l'écran jusqu'au bas de l'onglet **Présentation** pour ajouter et supprimer des balises. Pour plus d'informations, reportez-vous à [Ajouter des balises à un objet](#). Si vous sélectionnez **Éléments associés > NSGroups**, tous les NSGroups dont le NSGroup sélectionné est membre s'affichent.

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 supérieure

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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Inventaire > Services > Ajouter**.
- 3 Entrez un nom.
- 4 (Facultatif) Entrez une description.
- 5 Sélectionnez **Spécifier un protocole** pour configurer un service individuel ou sélectionnez **Grouper des services existants** pour configurer un groupe de NSServices.
- 6 Pour un service individuel, sélectionnez un type de service et un protocole.
Les types disponibles sont **Ether**, **IP**, **IGMP**, **ICMP**, **ALG** et **Ensemble de ports L4**.
- 7 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**.
- 8 Cliquez sur **AJOUTER**.

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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Inventaire > Machines virtuelles** dans le panneau de navigation.

La liste des machines virtuelles affiche 4 colonnes : Machine virtuelle, ID externe, Source et Balise. Cliquez 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 **Inventaire > Machines virtuelles** dans le panneau de navigation.
- 4 Sélectionnez une machine virtuelle.
- 5 Cliquez sur **GÉRER LES BALISES**.
- 6 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 .

Le nombre de balises que vous pouvez attribuer à une machine virtuelle à partir de NSX Manager est limité à 25. Le nombre de balises pour tous les autres objets gérés (ports ou commutateurs logiques, par exemple) est limité à 30.

- 7 Cliquez sur **Enregistrer**.

Vous pouvez configurer DHCP à partir de l'onglet **Mise en réseau et sécurité avancées**.

Note Si vous utilisez l'interface utilisateur **Mise en réseau et sécurité avancées** pour modifier des objets créés dans l'interface de stratégie, il se peut que certains paramètres ne soient pas configurables. Cette icône est située à côté de ces paramètres en lecture seule : ⊖. Pour plus d'informations, reportez-vous à la section [Chapitre 1 Présentation de NSX Manager](#).

Ce chapitre contient les rubriques suivantes :

- [DHCP](#)
- [Proxys de métadonnées](#)

DHCP

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.

Dans cette version, le serveur DHCP ne prend pas en charge le balisage de VLAN invité.

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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > DHCP > Profils de serveurs > Ajouter**.
- 3 Entrez un nom et une description facultative.
- 4 Sélectionnez un cluster NSX Edge dans le menu déroulant.
- 5 (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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > DHCP > Serveurs > Ajouter**.
- 3 Entrez un nom et une description facultative.
- 4 Entrez l'adresse IP du serveur DHCP et son masque de sous-réseau au format CIDR.
Par exemple, entrez `192.168.1.2/24`.
- 5 (Requis) Choisissez un profil DHCP dans le menu déroulant.
- 6 (Facultatif) Entrez les options courantes, telles que nom de domaine, passerelle par défaut, serveurs DNS et masque de sous-réseau.
- 7 (Facultatif) Entrez les options d'itinéraire statique sans classe.
- 8 (Facultatif) Entrez les autres options.
- 9 Cliquez sur **Enregistrer**.
- 10 Sélectionnez le serveur DHCP nouvellement créé.

- 11 Développez la section Pools d'adresses IP.
- 12 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.
- 13 Développez la section Liaisons statiques.
- 14 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.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Commutation**.
 - a Cochez la case d'un commutateur logique.
 - b Cliquez sur **Actions > Attacher un serveur DHCP**.
- 3 Vous pouvez également sélectionner **Mise en réseau et sécurité avancées > DHCP**.
 - a Cliquez sur l'onglet **Serveurs**.
 - b Cochez la case d'un serveur DHCP.
 - c Cliquez sur **Actions > Attacher à un commutateur logique**.

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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Commutation**.
- 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 ou DHCPv6 externes. Lorsque vous créez un service de relais DHCP/DHCPv6, 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > DHCP > Profils de relais > Ajouter**.
- 3 Entrez un nom et une description facultative.
- 4 Entrez une ou plusieurs adresses de serveur DHCP/DHCPv6 externe.

Étape suivante

Créez un service de relais DHCP/DHCPv6. 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > DHCP > Services de relais > Ajouter**.
- 3 Entrez un nom et une description facultative.
- 4 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 de relais DHCP à un port de routeur logique](#).

Ajouter un service de relais DHCP à un port de routeur logique

Vous pouvez ajouter un service de relais DHCP à un port de routeur logique. Les machines virtuelles qui se trouvent 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](#).

- Vérifiez que le port de routeur est de type **Liaison descendante**.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Routeurs**.
- 3 Sélectionnez le routeur approprié pour afficher plus d'informations et d'options de configuration.
- 4 Sélectionnez **Configuration > Ports de routeur**.
- 5 Sélectionnez le port de routeur connecté au commutateur logique de votre choix et cliquez sur **Modifier**.
- 6 Sélectionnez un service de relais DHCP dans la liste déroulante **Service de relais** et cliquez sur **Enregistrer**.

Vous pouvez également sélectionner un service de relais DHCP lorsque vous ajoutez un nouveau port de routeur logique.

Supprimer un bail DHCP

Dans certaines situations, il est possible que vous souhaitiez supprimer un bail DHCP. Par exemple, si vous voulez qu'un client DHCP obtienne une adresse IP différente, ou si un client s'arrête sans libérer son adresse IP et que vous voulez que l'adresse soit disponible pour d'autres clients.

Vous pouvez utiliser l'API suivante pour supprimer un bail DHCP :

```
DELETE /api/v1/dhcp/servers/<server-id>/leases?ip=<ip>&mac=<mac>
```

Pour vous assurer que le bail correct est supprimé, appelez l'API suivante avant et après l'API DELETE :

```
GET /api/v1/dhcp/servers/<server-id>/leases
```

Après avoir appelé l'API DELETE, assurez-vous que la sortie de l'API GET n'affiche pas le bail qui a été supprimé.

Pour plus d'informations, reportez-vous à la *Référence API de NSX-T Data Center*.

Proxys de métadonnées

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.

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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > DHCP > Proxys de métadonnées > Ajouter**.
- 3 Entrez un nom pour le serveur proxy de métadonnées.
- 4 (Facultatif) Entrez une description.
- 5 Entrez l'URL et le port du serveur Nova.
La plage de ports valide est 3 000 - 9 000.
- 6 Entrez une valeur pour **Secret**.
- 7 Sélectionnez un cluster NSX Edge dans la liste déroulante.
- 8 (Facultatif) Sélectionnez les membres du cluster NSX Edge.

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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > DHCP > Proxys de métadonnées**.
- 3 Sélectionnez un serveur proxy de métadonnées.
- 4 Sélectionnez l'option de menu **Actions > Attacher à un commutateur logique**
- 5 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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > DHCP > Proxys de métadonnées**.
- 3 Sélectionnez un serveur proxy de métadonnées.
- 4 Sélectionnez l'option de menu **Actions > Détacher du commutateur logique**
- 5 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 avancée des adresses IP

18

Avec la gestion des adresses IP (IPAM), vous pouvez créer des blocs d'adresses IP pour prendre en charge NSX 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*.

Note Si vous utilisez l'interface utilisateur **Mise en réseau et sécurité avancées** pour modifier des objets créés dans l'interface de stratégie, il se peut que certains paramètres ne soient pas configurables. Cette icône est située à côté de ces paramètres en lecture seule : . Pour plus d'informations, reportez-vous à la section [Chapitre 1 Présentation de NSX Manager](#).

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 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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées** > **Mise en réseau** > **IPAM**.
- 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > IPAM**.
- 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**.

Équilibrage de charge avancé

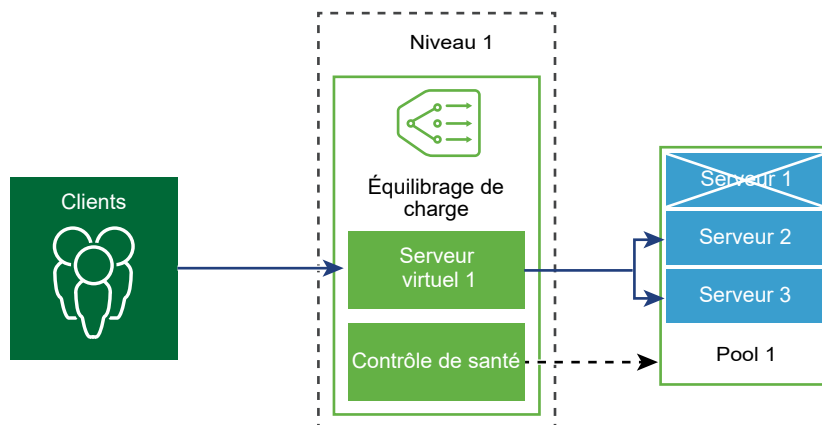
19

Ces informations couvrent la configuration de l'équilibrage de charge NSX-T Data Center disponible sous l'onglet **Mise en réseau avancée et sécurité**.

Pour plus d'informations sur l'équilibreur de charge avancé NSX (réseaux AVI), consultez <https://www.vmware.com/products/nsx-advanced-load-balancer.html>.

Note Si vous utilisez l'interface utilisateur **Mise en réseau et sécurité avancées** pour modifier des objets créés dans l'interface de stratégie, il se peut que certains paramètres ne soient pas configurables. Cette icône est située à côté de ces paramètres en lecture seule : . Pour plus d'informations, reportez-vous à la section [Chapitre 1 Présentation de NSX Manager](#).

L'équilibreur 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'équilibreur 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'équilibreur 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'équilibreur de charge en augmentant le nombre de serveurs virtuels et de membres du pool existants pour gérer un trafic réseau intense.

Note L'équilibreur 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 :

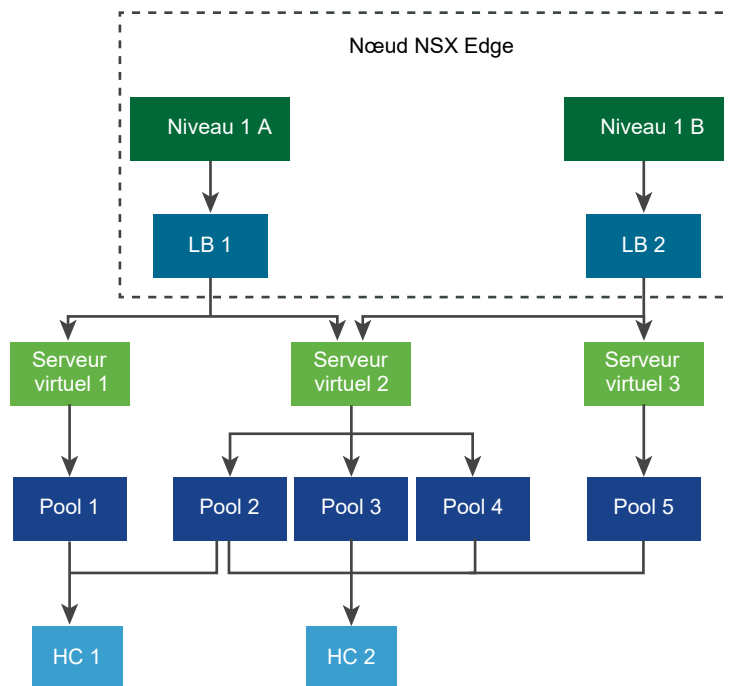
- [Concepts clés de l'équilibreur de charge](#)
- [Configuration des composants d'équilibreur de charge](#)

Concepts clés de l'équilibreur de charge

L'équilibreur de charge inclut des serveurs virtuels, des pools de serveurs et des moniteurs de contrôle de santé.

Un équilibreur 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.

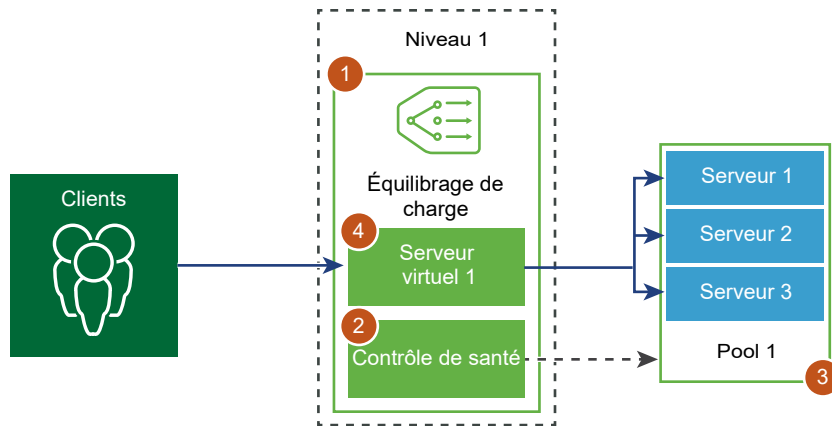
Pour vérifier que chaque serveur exécute correctement l'application, vous pouvez ajouter des moniteurs de contrôle de santé qui vérifient l'état de santé d'un serveur.



Configuration des composants d'équilibreur de charge

Pour utiliser des équilibreurs de charge logiques, vous devez commencer par configurer un équilibreur 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'équilibreur de charge. Enfin, vous devez créer un serveur virtuel de couche 4 ou de couche 7 pour l'équilibreur de charge.

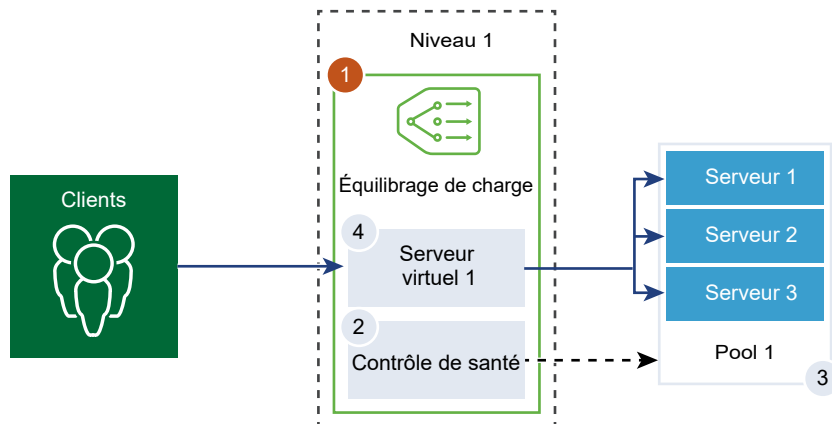


Créer un équilibrage de charge

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 équilibres 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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Équilibreur 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

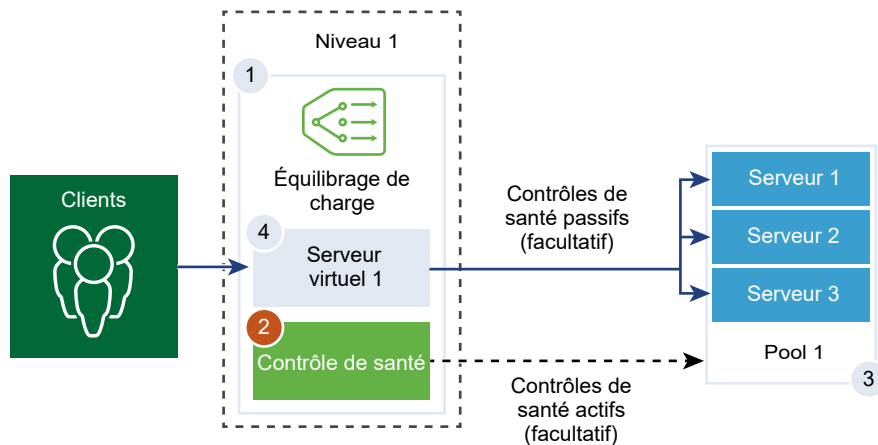
Le moniteur de santé actif est utilisé pour tester la disponibilité d'un serveur. Pour cela, il utilise plusieurs types de tests, notamment l'envoi d'une commande ping de base aux serveurs ou de demandes HTTP avancées pour surveiller la santé d'une application.

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 associé à une passerelle de niveau 1 (appelée précédemment routeur logique de niveau 1).

Si la passerelle de niveau 1 est connectée à une passerelle de niveau 0, un port de lien de routeur est créé et son adresse IP (généralement au format 100.64.x.x) est utilisée pour effectuer le contrôle de santé du service d'équilibrage de charge. Si la passerelle de niveau 1 est autonome (dispose d'un seul port de service centralisé et n'est pas connectée à une passerelle de niveau 0), l'adresse IP du port de service centralisé est utilisée pour effectuer le contrôle de santé du service d'équilibrage de charge. Reportez-vous à la section [Créer un routeur logique de niveau 1 autonome](#) pour plus d'informations sur les passerelles de niveau 1 autonomes.

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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Équilibreur de charge > 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.
Versión 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 les données envoyées et attendues ne sont pas répertoriées, 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 équilibres 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Équilibreur de charge > Moniteurs > Moniteurs de santé passifs > 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.

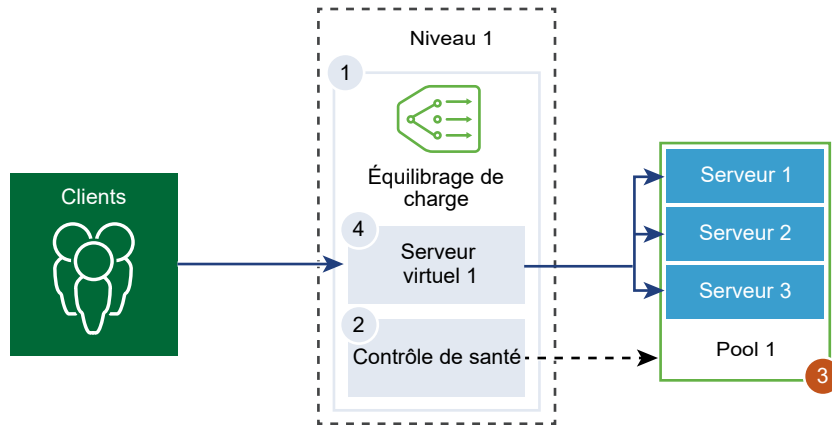
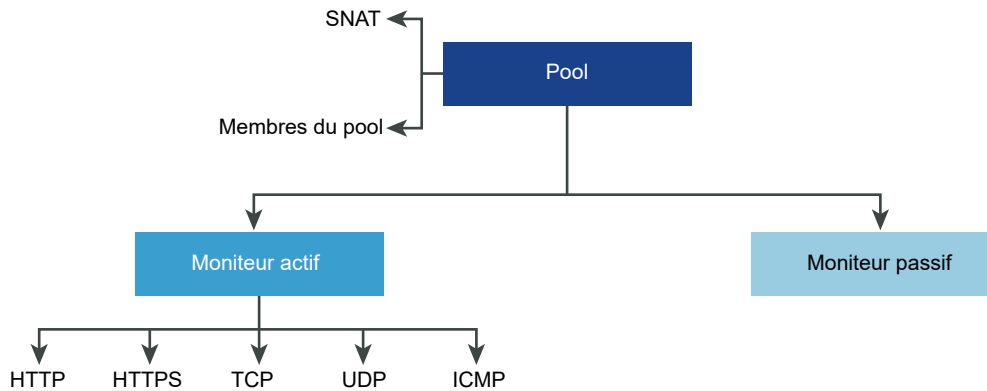


Figure 19-1. Configuration des paramètres du pool de serveurs



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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Équilibreur 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 DOWN.
- La limite maximale de connexions simultanées pour le pool de serveurs a été atteinte.

Option	Description
ROUND_ROBIN	Les demandes entrantes des clients sont analysées en fonction d'une liste de serveurs disponibles capables de les traiter. Les pondérations des membres du pool de serveurs sont ignorées, même si elles sont configurées.
WEIGHTED_ROUND_ROBIN	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. L'algorithme d'équilibrage de charge est conçu pour répartir équitablement la charge entre les ressources de serveur disponibles.
LEAST_CONNECTION	Diffuse les requêtes client à plusieurs serveurs en se basant sur le nombre de connexions déjà sur le serveur. 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.
WEIGHTED_LEAST_CONNECTION	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. 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. Par défaut, la pondération est 1 si la valeur n'est pas configurée et si le démarrage lent est activé.
IP-HASH	Sélectionne un serveur en fonction d'un hachage de l'adresse IP source et du poids total des serveurs en cours d'exécution.

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. Si les membres actifs échouent lors d'un contrôle de santé, le basculement de trafic se produit pour les membres de sauvegarde.

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.

La configuration d'un moniteur de santé actif et passif pour le pool de serveurs est facultative. Lorsque vous sélectionnez un moniteur de santé actif et que la passerelle de niveau 1 est connectée à une passerelle de niveau 0, un port de lien de routeur est créé. L'adresse IP du port de lien de routeur (généralement au format 100.64.x.x) est utilisée pour effectuer le contrôle de santé du service d'équilibrage de charge. Si la passerelle de niveau 1 est autonome (dispose d'un seul port de service centralisé et n'est pas connectée à une passerelle de niveau 0), l'adresse IP du port de service centralisé est utilisée pour effectuer le contrôle de santé du service d'équilibrage de charge. Reportez-vous à la section [Créer un routeur logique de niveau 1 autonome](#) pour plus d'informations sur les passerelles de niveau 1 autonomes.

Ajoutez une règle de pare-feu pour permettre à l'adresse IP d'effectuer le contrôle de santé du service d'équilibrage de charge.

- 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'équilibreur de charge.

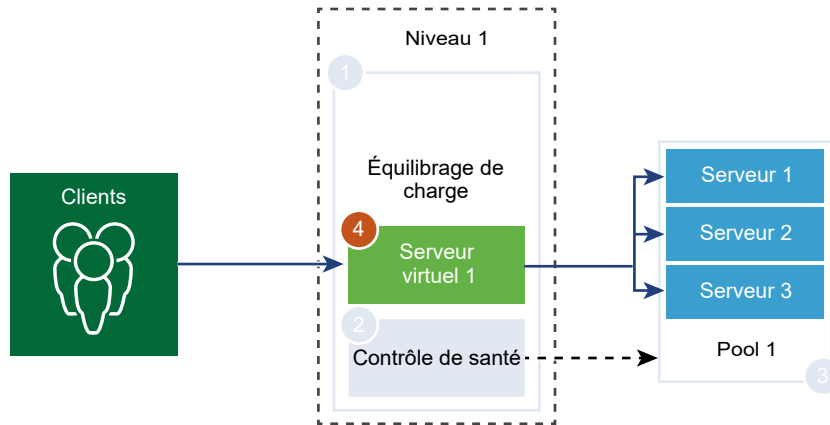
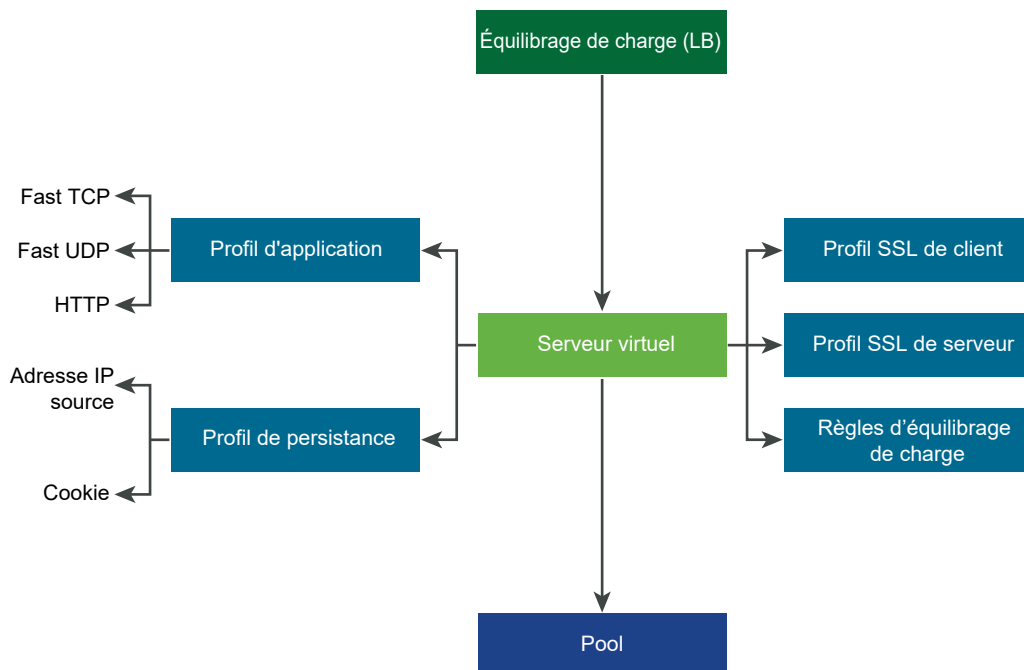


Figure 19-2. Composants de serveur virtuel



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 19-3. Profil d'application TCP et UDP de couche 4

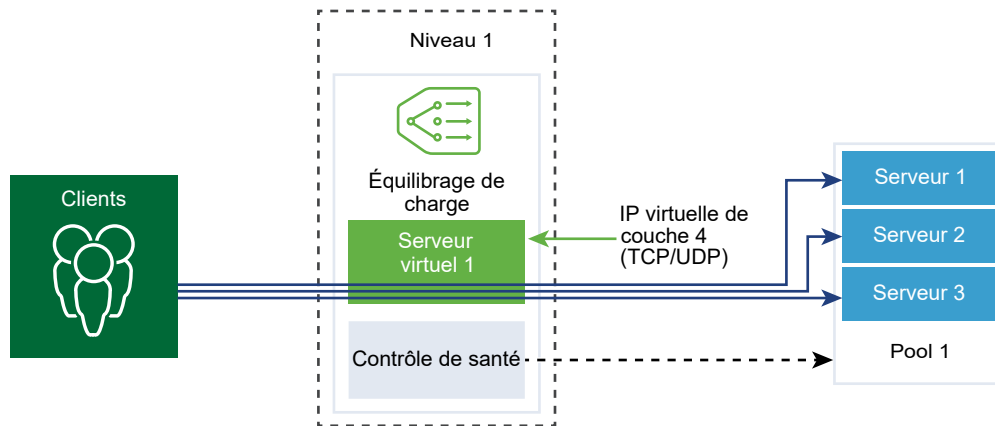
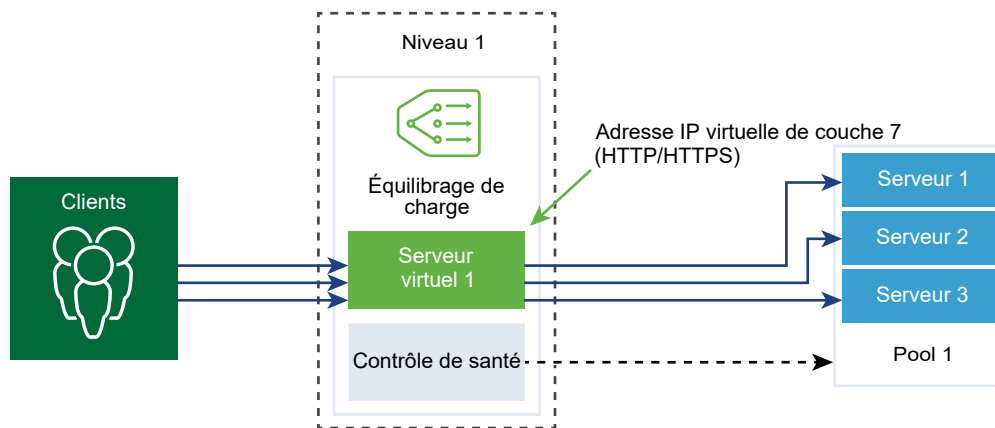


Figure 19-4. Profil d'application HTTPS de couche 7



Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Équilibreur 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
Redirection	<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>
X-Forwarded-For (XFF)	<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. Si l'en-tête HTTP XFF figure dans la demande entrante, l'équilibrage de charge insère l'en-tête XFF comprenant l'adresse IP du client. ■ Remplacer : si l'en-tête HTTP XFF est présent dans la demande entrante, l'équilibrage de charge remplace 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>
Délai d'inactivité de la connexion	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.

Option	Description
Taille de l'en-tête de la demande	Spécifiez la taille maximale de tampon en octets utilisée pour stocker les en-têtes de demande HTTP.
Authentification NTLM	<p>Faites basculer ce bouton pour que l'équilibrage de charge désactive le multiplexage TCP et active les connexions HTTP persistantes.</p> <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**.

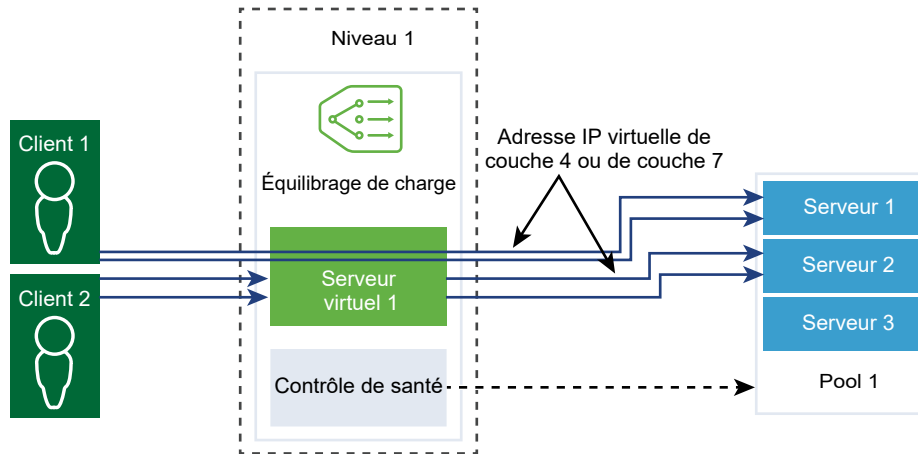
Configurer des profils persistants

Pour garantir la stabilité des applications avec état, les équilibreurs 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'équilibreur 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'équilibreur 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. Notez qu'un espace vide dans un nom de cookie 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Équilibreur 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'équilibreur 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.

- Sélectionnez **Ajouter > Persistance des cookies** dans le menu déroulant.
- 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'équilibreur 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. Notez qu'un espace vide dans un nom de cookie n'est pas pris en charge.
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. Le cookie de session n'est pas stocké et sera perdu lors de la fermeture du navigateur. Le cookie de persistance est stocké par le navigateur et n'est pas perdu lorsque le navigateur est fermé.
Durée d'inactivité maximale	Entrez la durée en secondes pendant laquelle un cookie peut être inactif avant son expiration.
Durée de vie maximale de cookie	Pour un cookie de session uniquement. Entrez l'âge maximal en secondes pendant lequel un cookie peut être actif.

- 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 19-5. Déchargement SSL

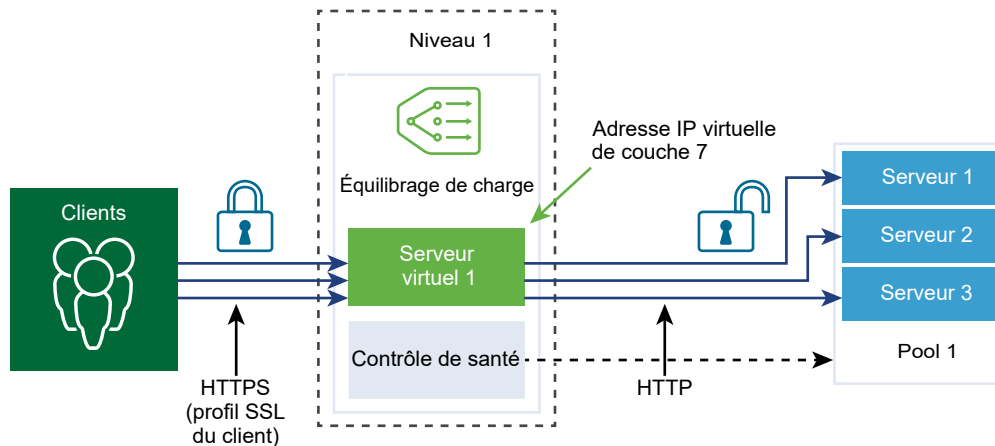
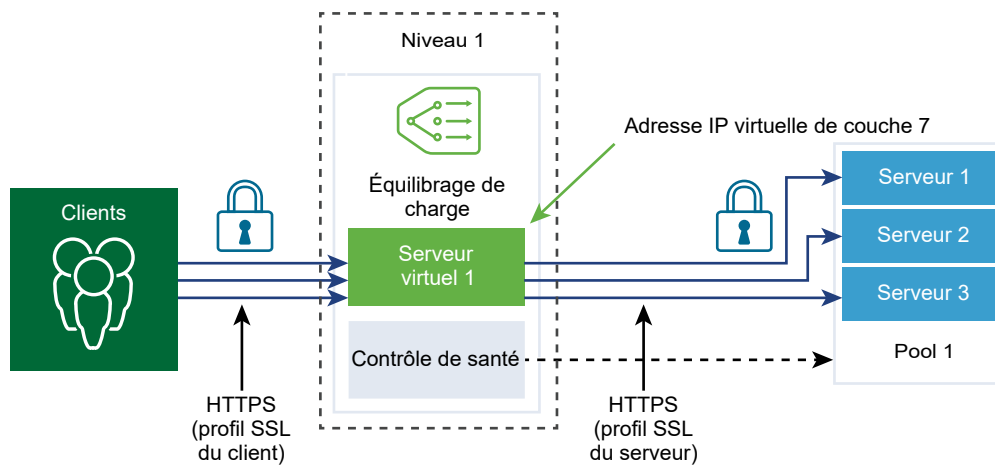


Figure 19-6. SSL de bout en bout



Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Équilibreur 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Équilibreur 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'équilibreur 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'équilibreur 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Mise en réseau > Équilibreur 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'équilibreur de charge et personnaliser le comportement de l'équilibrage de charge à l'aide de règles de correspondance ou d'action.

Les règles d'équilibreur 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 (?:s)ensitive » mais plutôt « Case ((?: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'équilibreur 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 `_`.

- `$_args` : arguments de la demande
- `$_arg_<nom>` : argument `<nom>` dans la ligne de demande
- `$_cookie_<nom>` : valeur du cookie `<nom>`
- `$_upstream_cookie_<nom>` : cookie avec le nom spécifié envoyé par le serveur en amont dans le champ d'en-tête de réponse « Set-Cookie »
- `$_upstream_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

- `$_host` - dans l'ordre de priorité - nom d'hôte de la ligne de demande, ou nom d'hôte du champ d'en-tête de demande « Host » ou nom du serveur correspondant à une demande
- `$_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
- `$_uri` - chemin d'accès URI dans la demande
- `$_ssl_ciphers` : renvoie les chiffrements SSL du client
- `$_ssl_client_i_dn` : renvoie la chaîne « issuer DN » du certificat client pour une connexion SSL établie conformément à la norme RFC 2253
- `$_ssl_client_s_dn` : renvoie la chaîne « subject DN » du certificat client pour une connexion SSL établie conformément à la norme RFC 2253
- `$_ssl_protocol` : renvoie le protocole d'une connexion SSL établie
- `$_ssl_session_reused` : renvoie « r » si une session SSL a été réutilisée ou « . » sinon

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 équilibreur 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'équilibreur 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
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

Condition de correspondance prise en charge	Description
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'équilibreur 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
Charge utile de demande HTTP	Correspondance au contenu du corps d'une demande HTTP. http_request.body_value - valeur à faire correspondre

Condition de correspondance prise en charge	Description
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'équilibreur 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'équilibreur de charge, des profils SSL côté client et des profils SSL côté serveur.

Note Le profil SSL n'est pas pris en charge dans la version Limited Export de NSX-T Data Center.

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 Fast TCP.

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'équilibreur 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**.

Note Si vous utilisez l'interface utilisateur **Mise en réseau et sécurité avancées** pour modifier des objets créés dans l'interface de stratégie, il se peut que certains paramètres ne soient pas configurables. Cette icône est située à côté de ces paramètres en lecture seule : . Pour plus d'informations, reportez-vous à la section [Chapitre 1 Présentation de NSX Manager](#).

Ce chapitre contient les rubriques suivantes :

- [Ajouter ou supprimer une règle de pare-feu à un routeur logique](#)
- [Configurer le pare-feu pour un port de pont de commutateur logique](#)
- [Sections de pare-feu et règles de pare-feu](#)
- [À propos des règles de pare-feu](#)

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.

Edge Fire-Walling est implémenté sur des ports de routeur de liaison montante, ce qui signifie que les règles de pare-feu ne s'appliqueront que si le trafic atteint ces ports sur le dispositif Edge. Pour appliquer des règles de pare-feu à une destination IP particulière, vous devez configurer des groupes avec le réseau /32. Si vous fournissez un sous-réseau autre que /32, les règles de pare-feu seront appliquées au sous-réseau complet.

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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Mise en réseau et sécurité avancées** > **Mise en réseau** > **Routeurs**.

- 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.

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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Mise en réseau et sécurité avancées > Sécurité > Pare-feu de pont**.
- 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.

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*.

Activer et désactiver un pare-feu distribué

Vous pouvez activer ou désactiver la fonctionnalité de pare-feu distribué.

Si elle est désactivée, aucune règle de pare-feu n'est appliquée au niveau du plan de données. Lors de la réactivation, les règles sont appliquées à nouveau.

Procédure

- 1 Accédez à **Mise en réseau et sécurité avancées > Sécurité > Pare-feu distribué**.
- 2 Cliquez sur l'onglet **Paramètres**.
- 3 Cliquez sur Pare-feu distribué **Modifier**.

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

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 **Mise en réseau et sécurité avancées > Sécurité > Pare-feu distribué**.
- 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. Pour les flux TCP et UDP, après le premier paquet, un cache est créé et conservé pour le tuple de trafic dans les deux sens, si le résultat du pare-feu est AUTORISER. Cela signifie que le trafic n'a plus besoin de vérifier les règles de pare-feu, ce qui entraîne une latence inférieure. 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 peuvent observer les flux de trafic d'une extrémité à l'autre. Le pare-feu est toujours consulté pour chaque paquet, afin de valider les numéros d'état et de séquence. 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 **Mise en réseau et sécurité avancées > Sécurité > Pare-feu distribué**.
- 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 **Mise en réseau et sécurité avancées > Sécurité > Pare-feu distribué**.
- 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/dfwpktlogs.log` sur des hôtes ESXi et KVM.

Procédure

- 1 Sélectionnez **Mise en réseau et sécurité avancées > Sécurité > Pare-feu distribué**.
- 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**.

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.

Note NSX-T Data Center ajoute automatiquement les machines virtuelles de nœuds NSX Manager et NSX Edge à la liste d'exclusion de pare-feu.

Procédure

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

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 TCP strict peut être activé sur une base par section pour désactiver la prise en charge en milieu de session et pour appliquer la condition requise pour un établissement de liaison à trois voies. Lors de l'activation du mode strict TCP pour une section de pare-feu distribué particulière et de l'utilisation d'une règle ANY-ANY Block par défaut, les paquets qui ne remplissent pas les conditions requises de connexion d'établissement de liaison à trois voies, et qui correspondent à une règle TCP dans cette section sont abandonnés. Strict s'applique uniquement aux règles TCP avec état et est activé au niveau de la section du pare-feu distribué. TCP strict n'est pas appliqué pour les paquets qui correspondent à une valeur par défaut ANY-ANY Allow qui n'a aucun service TCP spécifié.

Tableau 20-1. 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. Les protocoles IPv4 et IPv6 sont pris en charge pour la plage source ou de destination.

Tableau 20-1. Propriétés d'une règle de pare-feu (suite)

Propriété	Description
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. Les protocoles IPv4 et IPv6 sont 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 /var/log/dfwptlogs.log 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 In , Out et In/Out . La valeur par défaut est In/Out . 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 .
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 **Mise en réseau et sécurité avancées > Sécurité > Pare-feu distribué**.
- 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 contenu	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 contenu	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 **Mise en réseau et sécurité avancées > Sécurité > Pare-feu distribué**.
- 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 **Mise en réseau et sécurité avancées > Sécurité > Pare-feu distribué**.
- 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 **Mise en réseau et sécurité avancées > Sécurité > Pare-feu distribué**.
- 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 **Mise en réseau et sécurité avancées > Sécurité > Pare-feu distribué**.
- 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.

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 :

- [Afficher les tableaux de bord de surveillance](#)
- [Afficher l'utilisation et la capacité des catégories d'objets](#)
- [Vérification de l'état réalisé d'un changement de configuration](#)
- [Rechercher des objets](#)
- [Filtrer par attributs d'objet](#)
- [Ajouter un gestionnaire de calcul](#)
- [Ajout d'Active Directory](#)
- [Ajouter un serveur LDAP](#)
- [Synchroniser Active Directory](#)
- [Gestion des comptes d'utilisateur et du contrôle d'accès basé sur les rôles](#)
- [Sauvegarde et restauration de NSX Manager](#)
- [Supprimer l'extension NSX-T Data Center de vCenter Server](#)
- [Gestion du cluster NSX Manager](#)
- [Remplacement d'un nœud de transport NSX Edge dans un cluster NSX Edge](#)
- [Récupération de NSX-T lorsque vCenter Server est perdu et ne peut pas être récupéré](#)
- [Déploiement multisite de NSX-T Data Center](#)
- [Configuration de dispositifs](#)
- [Ajouter une clé de licence et générer un rapport d'utilisation de licence](#)

- [Configuration de certificats](#)
- [Configuration basée sur la conformité](#)
- [Collecter des bundles de support](#)
- [Messages de journal et codes d'erreur](#)
- [Programme d'amélioration du produit](#)
- [Ajouter des balises à un objet](#)
- [Rechercher l'empreinte digitale SSH d'un serveur distant](#)
- [Afficher des données sur les applications exécutées sur des machines virtuelles](#)
- [Configuration d'un équilibreur de charge externe](#)

Afficher les tableaux de bord de surveillance

L'interface NSX Manager fournit de nombreux tableaux de bord de surveillance qui présentent des informations détaillées sur l'état du système, la mise en réseau et la sécurité, et le rapport de conformité. Ces informations sont affichées ou accessibles dans toute l'interface NSX Manager, mais peuvent être consultées ensemble dans la page **Accueil > Tableaux de bord de surveillance**.

Vous pouvez accéder aux tableaux de bord de surveillance à partir de la page d'accueil de l'interface NSX Manager. Dans les tableaux de bord, vous pouvez cliquer et accéder aux pages sources à partir desquelles les données de tableau de bord sont représentées.

Procédure

- 1 Connectez-vous en tant qu'administrateur à l'interface NSX Manager.
- 2 Cliquez sur **Accueil** si vous n'êtes pas déjà sur la page d'accueil.
- 3 Cliquez sur **Tableaux de bord de surveillance** et sélectionnez la catégorie souhaitée de tableaux de bord dans le menu déroulant.

La page affiche les tableaux de bord dans les catégories sélectionnées. Les graphiques de tableau de bord sont codés par couleur, avec la clé de code couleur affichée directement au-dessus des tableaux de bord.

- 4 Pour accéder à un niveau de détail plus approfondi, cliquez sur le titre du tableau de bord ou sur l'un des éléments du tableau de bord, s'il est activé.

Les tableaux suivants décrivent les tableaux de bord par défaut et leurs sources.

Tableau 21-1. Tableaux de bord du système

Tableau de bord	Sources	Description
Système	Système > Dispositifs > Présentation	Affiche l'état du cluster NSX Manager et de la consommation des ressources (CPU, mémoire, disque).
Infrastructure	Système > Infrastructure > Nœuds Système > Infrastructure > Zones de transport Système > Infrastructure > Gestionnaires de calcul	Affiche l'état de l'infrastructure NSX-T, y compris les nœuds de transport hôte et Edge, les zones de transport et les gestionnaires de calcul.
Sauvegardes	Système > Sauvegarde et restauration	Affiche l'état des sauvegardes NSX-T, si elles sont configurées. Il est fortement recommandé de configurer des sauvegardes planifiées qui sont stockées à distance sur un site SFTP.
Protection de point de terminaison	Système > Déploiements de services	Affiche l'état du déploiement de la protection de point de terminaison.

Tableau 21-2. Tableaux de bord de la mise en réseau et de la sécurité

Tableau de bord	Sources	Description
Sécurité	Inventaire > Groupes Sécurité > Pare-feu distribué.	Affiche l'état des groupes et des stratégies de sécurité. Un groupe est un ensemble de charges de travail, de segments, de ports de segments et d'adresses IP dans lesquels il est possible d'appliquer des stratégies de sécurité, y compris des règles de pare-feu est-ouest.
Passerelles	Mise en réseau > Passerelles de niveau 0 Mise en réseau > Passerelles de niveau 1	Affiche l'état des passerelles de niveau 0 et de niveau 1.
Segments	Mise en réseau > Segments	Affiche l'état des segments de réseau.
Équilibrages de charge	Mise en réseau > Équilibrage de charge	Affiche l'état des machines virtuelles d'équilibrage de charge.
Réseaux VPN	Mise en réseau > VPN	Affiche l'état des réseaux privés virtuels.

Tableau 21-3. Tableaux de bord de Mise en réseau et sécurité avancées

Tableau de bord	Sources	Description
Équilibrages de charge	Mise en réseau et sécurité avancées > Équilibrages de charge	Affiche l'état des services d'équilibrage de charge, des serveurs virtuels d'équilibrage de charge et des pools de serveurs d'équilibrage de charge. Un équilibrage de charge peut héberger un ou plusieurs serveurs virtuels. Un serveur virtuel est lié à un pool de serveurs qui inclut des membres hébergeant des applications.
Pare-feu	Mise en réseau et sécurité avancées > Sécurité > Pare-feu distribué Mise en réseau et sécurité avancées > Sécurité > Pare-feu de pont Mise en réseau et sécurité avancées > Mise en réseau > Routeurs	Indique si le pare-feu est activé et affiche le nombre de stratégies, de règles et de membres de la liste d'exclusions. <hr/> Note Chaque élément détaillé affiché dans ce tableau de bord est issu d'un sous-onglet spécifique dans la page source indiquée.
VPN	Non applicable.	Affiche l'état des réseaux privés virtuels et le nombre de sessions VPN IPSec et L2 ouvertes.
Commutation	Mise en réseau et sécurité avancées > Commutation	Affiche l'état des commutateurs logiques et des ports logiques, y compris les ports de machine virtuelle et de conteneur.

Tableau 21-4. Tableau de bord du rapport de conformité

Colonne	Description
Code de non-conformité	Affiche le code de non-conformité spécifique.
Description	Cause spécifique de l'état de non-conformité.
Nom de la ressource	Ressource NSX-T (nœud, commutateur et profil) en non-conformité.
Type de ressource	Type de ressource de cause.
Ressources affectées	Nombre de ressources affectées. Cliquez sur la valeur de numéro pour afficher la liste.

Consultez la section [Codes de rapport d'état de conformité](#) pour obtenir plus d'informations sur chaque code de rapport de conformité.

Afficher l'utilisation et la capacité des catégories d'objets

Vous pouvez afficher l'utilisation et la capacité de diverses catégories d'objets dans votre environnement NSX-T Data Center. Vous pouvez également définir des alertes pour voir facilement à quel moment certains seuils d'utilisation sont atteints.

Pour voir l'utilisation et la capacité de différentes catégories d'objets, cliquez sur l'un des onglets suivants :

- **Mise en réseau > Présentation du réseau > Capacité**
- **Sécurité > Présentation de la sécurité > Capacité**
- **Inventaire > Présentation de l'inventaire > Capacité**
- **Système > Présentation du système > Capacité**

Vous pouvez également accéder à **Planifier et dépanner > Capacité consolidée** pour voir toutes les catégories d'objets sur une page.

Sur chaque page de capacité, pour chaque catégorie d'objets, les informations suivantes s'affichent :

- Capacité maximale : cette valeur est basée sur la capacité d'un grand dispositif.
- Inventaire actuel (réalisé) : nombre d'objets qui ont été créés ou configurés correctement. Ce nombre reflète les objets NSX Manager affichés dans l'onglet **Mise en réseau et sécurité avancées**. Ces objets peuvent inclure ceux que vous créez dans les onglets **Mise en réseau**, **Sécurité**, **Inventaire** ou **Système**. Une barre de couleur s'affiche pour indiquer le pourcentage d'utilisation. Si l'utilisation est inférieure au niveau d'alerte d'avertissement, la couleur est verte. Si l'utilisation est égale ou supérieure au niveau d'alerte d'avertissement, mais inférieure au niveau d'alerte critique, la couleur est orange. Si l'utilisation est égale ou supérieure au niveau d'alerte critique, la couleur est rouge.
- Alerte d'avertissement : il s'agit du niveau d'utilisation auquel la barre d'utilisation mentionnée ci-dessus indiquera une couleur orange. Vous pouvez modifier cette valeur.
- Alerte critique : il s'agit du niveau d'utilisation auquel la barre d'utilisation mentionnée ci-dessus indiquera une couleur rouge. Vous pouvez modifier cette valeur.

Lorsque vous modifiez la valeur d'alerte d'avertissement ou d'alerte critique, vous pouvez cliquer sur **Restaurer** pour revenir à la dernière valeur enregistrée. Vous pouvez cliquer sur **Réinitialiser les valeurs** pour restaurer les valeurs par défaut de toutes les catégories d'objets.

La page de capacité de mise en réseau affiche les catégories d'objets suivantes :

- Routeurs logiques de niveau 0
- Routeurs logiques de niveau 1
- Listes de préfixes
- Règles NAT à l'échelle du système
- Instances du serveur DHCP
- Plages et pools DHCP à l'échelle du système
- Routeurs logiques de niveau 1 avec NAT activé
- Commutateurs logiques
- Ports de commutateur logique à l'échelle du système

La page de capacité de sécurité affiche les catégories d'objets suivantes :

- Hôtes activés pour la protection des points de terminaison à l'échelle du système
- Machines virtuelles activées pour la protection des points de terminaison à l'échelle du système
- Groupes Active Directory
- Domaines Active Directory
- Règles de pare-feu distribué
- Règles de pare-feu à l'échelle du système
- Sections de pare-feu à l'échelle du système
- Sections de pare-feu distribué

La page de capacité d'inventaire affiche les catégories d'objets suivantes :

- Groupes de mise en réseau et sécurité
- Ensembles d'adresses IP
- Groupes basés sur des ensembles d'adresses IP
- Clusters vCenter
- Hôtes d'hyperviseur

La page de capacité de système affiche les catégories d'objets suivantes :

- Interfaces virtuelles à l'échelle du système
- Clusters Edge
- Nœuds Edge à l'échelle du système

Vérification de l'état réalisé d'un changement de configuration

Lorsque vous modifiez la configuration, NSX Manager envoie généralement une demande à un autre composant pour appliquer la modification. Pour certaines entités de couche 3, si vous modifiez la configuration à l'aide de l'API, vous pouvez suivre l'état de la demande pour voir si la modification a été correctement appliquée.

Le changement de configuration que vous initiez est appelé l'état souhaité. Le résultat de l'application de la modification est appelé l'état réalisé. Si NSX Manager applique bien la modification, l'état réalisé correspond à l'état souhaité. En cas d'erreur, l'état réalisé est différent de l'état souhaité.

Pour certaines entités de couche 3, lorsque vous appelez une API pour modifier la configuration, la réponse inclut le paramètre `request_id`. Vous pouvez utiliser le paramètre `request_id` et `entity_id` pour effectuer un appel d'API afin de connaître l'état de la demande.

Cette fonctionnalité prend en charge les API et entités suivantes :

```

EdgeCluster
  POST /edge-clusters
  PUT /edge-clusters/<edge-cluster-id>
  DELETE /edge-clusters/<edge-cluster-id>
  POST /edge-clusters/<edge-cluster-id>?action=replace_transport_node

LogicalRouter
  POST /logical-routers
  PUT /logical-routers/<logical-router-id>
  DELETE /logical-routers/<logical-router-id>
  POST /logical-routers/<logical-router-id>?action=reprocess
  POST /logical-routers/<logical-router-id>?action=reallocate

LogicalRouterPort
  POST /logical-router-ports
  PUT /logical-router-ports/<logical-router-port-id>
  DELETE /logical-router-ports/<logical-router-port-id>

StaticRoute
  POST /logical-routers/<logical-router-id>/routing/static-routes
  PUT /logical-routers/<logical-router-id>/routing/static-routes/<static-route-id>
  DELETE /logical-routers/<logical-router-id>/routing/static-routes/<static-route-id>

BGPConfig
  PUT /logical-routers/<logical-router-id>/routing/bgp

BgpNeighbor
  POST /logical-routers/<logical-router-id>/routing/bgp/neighbors
  PUT /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>
  DELETE /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>
  POST /logical-routers/<logical-router-id>/routing/bgp/neighbors/<bgp-neighbor-id>

BGPCommunityList
  POST /logical-routers/<logical-router-id>/routing/bgp/community-lists
  PUT /logical-routers/<logical-router-id>/routing/bgp/community-lists/<community-list-id>
  DELETE /logical-routers/<logical-router-id>/routing/bgp/community-lists/<community-list-id>

AdvertisementConfig
  PUT /logical-routers/<logical-router-id>/routing/advertisement

AdvertiseRouteList
  PUT /logical-routers/<logical-router-id>/routing/advertisement/rules

NatRule
  POST /logical-routers/<logical-router-id>/nat/rules
  PUT /logical-routers/<logical-router-id>/nat/rules/<rule-id>
  DELETE /logical-routers/<logical-router-id>/nat/rules/<rule-id>

DhcpRelayService
  POST /dhcp/relays
  PUT /dhcp/relays/<relay-id>
  DELETE /dhcp/relays/<relay-id>

```

DhcpRelayProfile

```
POST /dhcp/relay-profiles
PUT /dhcp/relay-profiles/<relay-profile-id>
DELETE /dhcp/relay-profiles/<relay-profile-id>
```

StaticHopBfdPeer

```
POST /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers
PUT /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers/<bfd-peers-id>
DELETE /logical-routers/<logical-router-id>/routing/static-routes/bfd-peers/<bfd-peers-id>
```

IPPrefixList

```
POST /logical-routers/<logical-router-id>/routing/ip-prefix-lists
PUT /logical-routers/<logical-router-id>/routing/ip-prefix-lists/<ip-prefix-list-id>
DELETE /logical-routers/<logical-router-id>/routing/ip-prefix-lists/<ip-prefix-list-id>
```

RouteMap

```
POST /logical-routers/<logical-router-id>/routing/route-maps
PUT /logical-routers/<logical-router-id>/routing/route-maps/<route-map-id>
DELETE /logical-routers/<logical-router-id>/routing/route-maps/<route-map-id>
```

RedistributionConfig

```
PUT /logical-routers/<logical-router-id>/routing/redistribution
```

RedistributionRuleList

```
PUT /logical-routers/<logical-router-id>/routing/redistribution/rules
```

BfdConfig

```
PUT /logical-routers/<logical-router-id>/routing/bfd-config
```

MplsConfig

```
PUT /logical-routers/<logical-router-id>/routing/mps
```

RoutingGlobalConfig

```
PUT /logical-routers/<logical-router-id>/routing
```

IPSecVPNIKEProfile

```
POST /vpn/ipsec/ike-profiles
PUT /vpn/ipsec/ike-profiles/<ike-profile-id>
DELETE /vpn/ipsec/ike-profiles/<ike-profile-id>
```

IPSecVPNDPDProfile

```
POST /vpn/ipsec/dpd-profiles
PUT /vpn/ipsec/dpd-profiles/<dpd-profile-id>
DELETE /vpn/ipsec/dpd-profiles/<dpd-profile-id>
```

IPSecVPNTunnelProfile

```
POST /vpn/ipsec/tunnel-profiles
PUT /vpn/ipsec/tunnel-profiles/<tunnel-profile-id>
DELETE /vpn/ipsec/tunnel-profiles/<tunnel-profile-id>
```

IPSecVPNLocalEndpoint

```
POST /vpn/ipsec/local-endpoints
PUT /vpn/ipsec/local-endpoints/<local-endpoint-id>
DELETE /vpn/ipsec/local-endpoints/<local-endpoint-id>
```

```

IPSecVPNPeerEndpoint
  POST /vpn/ipsec/peer-endpoints
  PUT /vpn/ipsec/peer-endpoints/<peer-endpoint-id>
  DELETE /vpn/ipsec/peer-endpoints/<peer-endpoint-id>

IPSecVPNService
  POST /vpn/ipsec/services
  PUT /vpn/ipsec/services/<service-id>
  DELETE /vpn/ipsec/services/<service-id>

IPSecVPNSession
  POST /vpn/ipsec/sessions
  PUT /vpn/ipsec/sessions/<session-id>
  DELETE /vpn/ipsec/sessions/<session-id>

DhcpServer
  POST /dhcp/servers
  PUT /dhcp/servers/<server-id>
  DELETE /dhcp/servers/<server-id>

DhcpStaticBinding
  POST /dhcp/servers/static-bindings
  PUT /dhcp/servers/<server-id>/static-bindings/<binding-id>
  DELETE /dhcp/servers/<server-id>/static-bindings/<binding-id>

DhcpIpPool
  POST /dhcp/servers/ip-pools
  PUT /dhcp/servers/<server-id>/ip-pools/<pool-id>
  DELETE /dhcp/servers/<server-id>/ip-pools/<pool-id>

DnsForwarder
  POST /dns/forwarders
  PUT /dns/forwarders/<forwarder-id>
  DELETE /dns/forwarders/<forwarder-id>

```

Vous pouvez appeler les API suivantes pour obtenir les états réalisés :

```

EdgeCluster
Request - GET /edge-clusters/<edge-cluster-id>/state?request_id=<request-id>
Response - An instance of EdgeClusterStateDto which will inherit ConfigurationState. If the
edge cluster is deleted then the state will be unknown and it will return the common entity
not found error.

LogicalRouter / All L3 Entites - All L3 entities can use this API to get realization state
Request - GET /logical-routers/<logical-router-id>/state?request_id=<request-id>
Response - An instance of LogicalRouterStateDto which will inherit ConfigurationState. Delete
operation of any entity other than logical router can be covered by getting the state of
logical router but if the logical router itself is deleted then the state will be unknown and
it will return the common entity not found error.

LogicalServiceRouterCluster - All L3 entities which are the part of services can use this API
to get the realization state
Request - GET /logical-routers/<logical-router-id>/service-cluster/state?request_id=<request-
id>
Response - An instance of LogicalServiceRouterClusterState which will inherit

```

ConfigurationState.

LogicalRouterPort / DhcpRelayService / DhcpRelayProfile

Request - GET /logical-router-ports/<logical-router-port-id>/state?request_id=<request-id>

Response - An instance of LogicalRouterPortStateDto which will inherit ConfigurationState.

IPSecVPNIKEProfile / IPSecVPNDPDProfile / IPSecVPNTunnelProfile / IPSecVPNLocalEndpoint /

IPSecVPNPeerEndpoint / IPSecVPNService / IPSecVPNSession

Request - GET /vpn/ipsec/sessions/<session-id>/state?request_id=<request-id>

Response - An instance of IPSecVPNSessionStateDto which will inherit ConfigurationState. If the session is deleted then the state will be unknown and it will return the common entity not found error. When IPSecVPNService is disabled, IKE itself is down and it does not respond. It will return unknown state in such a case.

DhcpServer

Request - GET /dhcp/servers/<server-id>/state?request_id=<request-id>

Response - An instance of ConfigurationState.

DhcpStaticBinding

Request - GET /dhcp/servers/<server-id>/static-bindings/<binding-id>/state?

request_id=<request-id>

Response - An instance of ConfigurationState.

DhcpIpPool

Request - GET /dhcp/servers/<server-id>/ip-pools/<pool-id>/state?request_id=<request-id>

Response - An instance of ConfigurationState.

DnsForwarder

Request - GET /dns/forwarders/<forwarder-id>/state?request_id=<request-id>

Response - An instance of ConfigurationState.

Pour plus d'informations sur les API, reportez-vous à la *Référence de l'API de NSX-T Data Center*.

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://<nsx-manager-ip-address>>.

- 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 affinée.

- 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.

Filtrer par attributs d'objet

Lors de l'affichage d'objets dans NSX Manager, vous pouvez filtrer les objets avec un ou plusieurs de leurs attributs. Par exemple, lorsque vous affichez les détails de passerelles de niveau 0, vous pouvez choisir de filtrer par **État** et n'afficher que les passerelles avec l'état **Inactif**.


Les types de filtres suivants sont disponibles :

- Filtres prédéfinis : liste de filtres couramment utilisés que vous pouvez appliquer à vos objets.
- Filtre de texte : filtre basé sur la valeur d'attribut que vous entrez. Ce filtre s'applique uniquement aux attributs **Nom**, **Balise**, **Chemin** et **Description** des objets.
- Paires attribut-valeur : menu déroulant d'attributs que vous pouvez utiliser pour spécifier des paires attribut-valeur pour le filtrage.

Vous pouvez utiliser plusieurs attributs d'un objet ou plusieurs valeurs d'un seul attribut pour filtrer les objets. L'opérateur ET est appliqué lorsque vous sélectionnez plusieurs attributs alors que l'opérateur OU est utilisé lorsque vous spécifiez plusieurs valeurs d'un seul attribut.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Accédez à l'onglet qui affiche les objets que vous voulez afficher.
- 3 Spécifiez les attributs que vous voulez utiliser pour filtrer les objets.

- Cliquez sur  et faites une sélection dans une liste de filtres prédéfinis.
- Entrez une valeur pour les attributs **Nom**, **Balise**, **Chemin** ou **Description**.
- Sélectionnez un attribut dans le menu déroulant et spécifiez sa valeur. Par exemple, **État** : **Inactif**

Les objets répondant à vos critères de filtre s'affichent.

- 4 (Facultatif) Cliquez sur **Effacer** pour réinitialiser vos filtres.

Ajouter un gestionnaire de calcul

Un gestionnaire de calcul, par exemple, vCenter Server, est une application qui gère les ressources, telles que des hôtes et des machines virtuelles.

NSX-T Data Center interroge les gestionnaires de calcul pour collecter des informations sur le cluster à partir de vCenter Server.

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

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

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

Conditions préalables

- Vérifiez que vous utilisez la version de vSphere prise en charge. Voir [Version de vSphere prise en charge](#)
- Communication IPv6 et IPv4 avec vCenter Server.

- Vérifiez que vous utilisez le nombre recommandé de gestionnaires de calcul. Reportez-vous à la section <https://configmax.vmware.com/home>.

Note NSX-T Data Center ne prend pas en charge la même instance de vCenter Server à enregistrer avec plusieurs instances de NSX Manager.

Procédure

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

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

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

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

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

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

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

Résultats

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

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

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

Ajout d'Active Directory

Active Directory est utilisé dans la création de règles de pare-feu d'identité basées sur l'utilisateur.

Windows 2008 n'est pas pris en charge comme serveur Active Directory ou système d'exploitation de serveur RDSH.

Vous pouvez enregistrer un ou plusieurs domaines Windows auprès de NSX Manager. NSX Manager obtient de chaque domaine enregistré des informations sur les utilisateurs et les groupes, ainsi que sur la relation entre eux. NSX Manager récupère également les informations d'identification Active Directory (AD).

Une fois qu'Active Directory est synchronisé avec NSX Manager, vous pouvez créer des groupes de sécurité basés sur l'identité des utilisateurs et créer des règles de pare-feu reposant sur l'identité.

Note Pour l'application des règles de pare-feu d'identité, le service de temps Windows doit être **activé** pour toutes les VM utilisant Active Directory. Cela garantit que la date et l'heure sont synchronisées entre Active Directory et les VM. Les modifications apportées à l'appartenance au groupe AD, y compris l'activation et la suppression d'utilisateurs, ne prennent pas immédiatement effet pour les utilisateurs connectés. Pour que les modifications prennent effet, les utilisateurs doivent fermer puis rouvrir leur session. L'administrateur AD doit forcer la fermeture de session lorsque l'appartenance au groupe est modifiée. Ce comportement est une limite d'Active Directory.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Accédez à **Système > Active Directory**.
- 3 Cliquez sur **Ajouter Active Directory**.
- 4 Entrez le nom de l'annuaire Active Directory.
- 5 Entrez le **Nom NetBios** et le **Nom unique de base**.

Pour extraire le nom NetBIOS de votre domaine, entrez `nbtstat -n` dans une fenêtre de commande sur un poste de travail Windows appartenant à un domaine ou situé sur un contrôleur de domaine. Dans la table de noms locaux NetBIOS, l'entrée avec un préfixe <00> et le type Groupe est le nom NetBIOS.

Un nom unique de base est nécessaire pour ajouter un domaine Active Directory. Un nom unique de base est le point de départ qu'un serveur LDAP utilise lors de la recherche d'authentification des utilisateurs dans un domaine Active Directory. Par exemple, si votre nom de domaine est corp.local, le nom unique de base pour Active Directory serait « DC=corp,DC=local ».

- 6 Définissez l'**Intervalle de synchronisation delta** si nécessaire. Une synchronisation delta met à jour les objets AD locaux qui ont changé depuis le dernier événement de synchronisation.

Les modifications apportées dans Active Directory NE s'affichent PAS sur NSX Manager tant qu'une synchronisation delta ou complète n'a pas été effectuée.

- 7 Cliquez sur **Enregistrer**.

Ajouter un serveur LDAP

La configuration et la fonctionnalité du serveur LDAP (Lightweight Directory Access Protocol) ne sont utilisées qu'avec le pare-feu d'identité. LDAP fournit un emplacement central pour l'authentification, ce qui signifie que lorsque vous configurez une connexion à votre serveur LDAP, les enregistrements d'utilisateur sont stockés dans votre serveur LDAP externe.

Conditions préalables

Le compte de domaine doit disposer d'une autorisation d'accès en lecture par AD pour tous les objets dans l'arborescence du domaine. Le compte du lecteur de journaux d'événements doit disposer d'autorisations d'accès en lecture des journaux des événements de sécurité.

Lorsqu'il existe un cluster d'instances de NSX Manager, tous les nœuds doivent pouvoir accéder au serveur LDAP.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Accédez à **Système > Active Directory**.
- 3 Sélectionnez l'onglet **Serveur LDAP**.
- 4 Cliquez sur **Ajouter un serveur LDAP**.
- 5 Entrez le nom d'**hôte** du serveur LDAP.
- 6 Sélectionnez le répertoire actif auquel le serveur LDAP est connecté dans le menu déroulant **Connecté à (Répertoire)**.
- 7 (Facultatif) Sélectionnez le **protocole** : LDAP (non sécurisé) ou LDAPS (sécurisé).
- 8 Si LDAPS a été sélectionné, sélectionnez l'empreinte numérique SHA-256 suggérée par NSX Manager ou entrez une empreinte numérique SHA-256.

9 Entrez le numéro de **port** du serveur LDAP.

Pour les contrôleurs de domaine local, le port LDAP 389 et le port LDAPS 636 par défaut sont utilisés pour la synchronisation Active Directory et ne doivent pas être modifiés à partir des valeurs par défaut.

10 Entrez le **nom d'utilisateur** et le **mot de passe** d'un compte Active Directory avec un minimum d'accès en lecture seule au domaine Active Directory.

11 Cliquez sur **Enregistrer**.

12 Pour vérifier que vous pouvez vous connecter au serveur LDAP, cliquez sur **Tester la connexion**.

Synchroniser Active Directory

Les objets Active Directory peuvent être utilisés pour créer des groupes de sécurité basés sur l'identité de l'utilisateur et des règles de pare-feu basées sur l'identité.

Si vous utilisez l'API pour terminer manuellement une synchronisation complète après son lancement, les statistiques de synchronisation ne seront pas mises à jour correctement.

Note IDFW s'appuie sur la sécurité et l'intégrité du système d'exploitation invité. Il existe plusieurs méthodes pour qu'un administrateur local malveillant usurpe son identité pour contourner les règles de pare-feu. Les informations d'identité d'utilisateur sont fournies par l'agent Guest Introspection dans les machines virtuelles invitées. Les administrateurs de sécurité doivent s'assurer que l'agent NSX Guest Introspection est installé et en cours d'exécution sur chaque machine virtuelle invitée. Les utilisateurs connectés ne doivent pas disposer du privilège pour supprimer ou arrêter l'agent.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Accédez à **Système > Active Directory**.
- 3 Cliquez sur l'icône de menu représentant trois boutons en regard du répertoire Active Directory que vous souhaitez synchroniser et sélectionnez l'une des options suivantes :

Élément de menu	Description
Synchronisation Delta	Effectuez une synchronisation delta dans laquelle les objets AD locaux qui ont changé depuis la dernière synchronisation sont mis à jour.
Tout synchroniser	Effectuez une synchronisation complète dans laquelle l'état local de tous les objets AD est mis à jour.

- 4 Cliquez sur **Afficher l'état de synchronisation** pour voir l'état actuel du répertoire Active Directory, l'état de synchronisation précédent, l'état de synchronisation et l'heure de la dernière synchronisation.

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.

Gérer le mot de passe d'un utilisateur

Chaque NSX Manager et dispositif NSX Edge dispose de trois comptes locaux : admin, audit et racine. Vous pouvez gérer le mot de passe de ces utilisateurs, mais vous ne pouvez pas ajouter ou supprimer des utilisateurs.

L'utilisateur d'audit n'est pas actif par défaut. Pour l'activer, connectez-vous en tant qu'administrateur, puis exécutez la commande `set user audit` et fournissez un nouveau mot de passe. Lorsque vous êtes invité à saisir le mot de passe actuel, appuyez sur la touche Entrée.

Par défaut, les mots de passe d'utilisateur expirent après 90 jours. Vous pouvez modifier ou désactiver l'expiration du mot de passe pour chaque utilisateur.

Lorsque le mot de passe d'un utilisateur local sur NSX Manager expire dans les 30 jours, l'interface Web de NSX Manager affiche une notification d'expiration du mot de passe. Si vous définissez l'expiration du mot de passe d'un utilisateur local sur 30 jours maximum, la notification est toujours présente.

À partir de NSX-T Data Center 2.5.1, la notification inclut un lien « Modifier le mot de passe ». Cliquez sur le lien pour modifier le mot de passe de l'utilisateur local depuis l'interface Web.

Conditions préalables

Familiarisez-vous avec les exigences de complexité de mot de passe pour NSX Manager et NSX Edge. Reportez-vous aux sections « Installation de NSX Manager » et « Installation de NSX Edge » du *Guide d'installation de NSX-T Data Center*.

Procédure

- 1 Connectez-vous à l'interface de ligne de commande du dispositif.
- 2 Pour modifier le mot de passe, exécutez la commande `set user`. Par exemple :

```
nsx> set user admin
Current password:
New password:
Confirm new password:
nsx>
```

- 3 Pour obtenir les informations d'expiration du mot de passe, exécutez la commande `get user <username> password-expiration`. Par exemple :

```
nsx> get user admin password-expiration
Password expires 90 days after last change
nsx>
```

- 4 Pour définir le délai d'expiration du mot de passe en jours, exécutez la commande `set user <username> password-expiration <number of days>`. Par exemple :

```
nsx> set user admin password-expiration 120
nsx>
```

- 5 Pour désactiver l'expiration du mot de passe, exécutez la commande `clear user <username> password-expiration`. Par exemple :

```
nsx> clear user admin password-expiration
nsx>
```

Réinitialisation des mots de passe d'un dispositif

La procédure suivante s'applique aux dispositifs NSX Manager, NSX Edge et Cloud Service Manager.

Note Si vous disposez d'un cluster NSX Manager, la réinitialisation du mot de passe pour l'utilisateur `root`, `admin` ou `audit` sur une instance de NSX Manager réinitialisera automatiquement le mot de passe des autres instances de NSX Manager dans le cluster. Notez que la synchronisation du mot de passe peut prendre plusieurs minutes.

Si vous avez renommé l'utilisateur `admin` ou `audit`, utilisez le nouveau nom dans les procédures suivantes.

Lorsque vous redémarrez un dispositif, le menu de démarrage GRUB ne s'affiche pas par défaut. Pour la procédure suivante, vous devez avoir configuré GRUB afin qu'il affiche le menu de démarrage GRUB. Pour plus d'informations sur la configuration de GRUB et la modification du mot de passe `root` GRUB, reportez-vous à la section « Configurer NSX-T Data Center pour afficher le menu GRUB au démarrage » du *Guide d'installation de NSX-T Data Center*.

Si vous exécutez NSX-T Data Center 2.5.2 ou une version ultérieure et que vous connaissez le mot de passe de `root` mais que vous avez oublié le mot de passe pour `admin` ou `audit`, vous pouvez le réinitialiser à l'aide de la procédure suivante :

- 1 Connectez-vous au dispositif en tant que `root`.
- 2 Pour NSX Edge, exécutez la commande `/etc/init.d/nsx-edge-api-server stop`. Sinon exécutez la commande `/etc/init.d/nsx-mp-api-server stop`.
- 3 Pour réinitialiser le mot de passe pour `admin`, exécutez la commande `passwd admin`.
- 4 Pour réinitialiser le mot de passe pour `audit`, exécutez la commande `passwd audit`.

- 5 Exécutez la commande `touch /var/vmware/nsx/reset_cluster_credentials`.
- 6 Pour NSX Edge, exécutez la commande `/etc/init.d/nsx-edge-api-server start`. Sinon exécutez la commande `/etc/init.d/nsx-mp-api-server start`.

Si vous avez oublié le mot de passe de l'utilisateur `root`, vous pouvez le réinitialiser à l'aide de la procédure suivante. Si vous exécutez NSX-T Data Center 2.5.0 ou 2.5.1 et que vous souhaitez réinitialiser le mot de passe pour `admin` et `audit`, utilisez également la procédure suivante. Si vous exécutez NSX-T Data Center 2.5.2 ou une version ultérieure, vous pouvez utiliser la procédure ci-dessus pour réinitialiser le mot de passe pour `admin` ou `audit` après avoir réinitialisé le mot de passe pour `root`.

Procédure

- 1 Connectez-vous à la console du dispositif.
- 2 Redémarrez le système.
- 3 Lorsque le menu de démarrage GRUB s'affiche, appuyez rapidement sur la touche **Maj** gauche ou sur la touche **Échap**. Si vous attendez trop longtemps et que la séquence de démarrage ne s'arrête pas, vous devrez redémarrer le système une autre fois.
- 4 Appuyez sur la touche **e** pour modifier le menu.

Entrez le nom d'utilisateur (`root`) et le mot de passe GRUB pour `root` (différent de celui de l'utilisateur racine du dispositif `root`).
- 5 Conservez le curseur sur la sélection Ubuntu.
- 6 Appuyez sur la touche **e** pour modifier l'option sélectionnée.
- 7 Recherchez la ligne commençant par `linux`.
- 8 Si vous exécutez NSX-T Data Center 2.5.0 ou 2.5.1, effectuez les étapes suivantes :
 - a Supprimez toutes les options après `root=UUID=<ID number>` et ajoutez `-rw single init=/bin/bash` après l'UUID.
 - b Appuyez sur **Ctrl-X** pour démarrer.
 - c Lorsque les messages du journal s'arrêtent, appuyez sur la touche Entrée.
L'invite `root@ (none) :/#` s'affiche.
 - d Si vous réinitialisez le mot de passe de `root`, exécutez la commande `passwd`.

Si vous réinitialisez le mot de passe de `admin` ou `audit`, exécutez la commande `passwd <admin or audit user ID>`.

Vous pouvez exécuter la commande `passwd` plusieurs fois.
 - e Saisissez un nouveau mot de passe, puis saisissez-le à nouveau pour confirmation.
 - f Si vous réinitialisez le mot de passe sur NSX Manager, exécutez la commande `touch /var/vmware/nsx/reset_cluster_credentials`.

- g Exécutez la commande `sync`.
 - h Exécutez la commande `reboot -f`.
- 9 Si vous exécutez NSX-T Data Center 2.5.2 ou une version ultérieure, effectuez les étapes suivantes :
- a Ajoutez `systemd.wants=PasswordRecovery.service` à la fin de la ligne.
 - b Appuyez sur **Ctrl-X** pour démarrer.
 - c Entrez un nouveau mot de passe pour `root` et entrez-le à nouveau pour confirmer.

Une fois le processus de démarrage terminé, vous pouvez vérifier la modification du mot de passe en vous connectant en tant que `root` avec le nouveau mot de passe.

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 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.

Vous devez utiliser OpenSSL version 1.x ou supérieure pour l'empreinte numérique. Sur l'hôte vIDM, la commande `openssl` exécute une ancienne version d'OpenSSL. Vous devez donc utiliser la commande `openssl1` sur l'hôte vIDM. Cette commande est uniquement disponible à partir de l'hôte vIDM.

Sur un serveur qui n'est pas l'hôte vIDM, vous pouvez utiliser la commande `openssl` qui exécute OpenSSL version 1.x ou une version ultérieure.

Procédure

- 1 Connectez-vous à la console de l'hôte vIDM ou ouvrez une session SSH sur l'hôte vIDM en tant qu'utilisateur **sshuser**, ou connectez-vous à n'importe quel serveur pouvant effectuer un test ping sur l'hôte vIDM.
- 2 Exécutez l'une des commandes suivantes pour obtenir l'empreinte numérique de l'hôte vIDM.
 - Si vous êtes connecté à l'hôte vIDM, exécutez la commande `openssl1` pour obtenir l'empreinte numérique :

```
openssl1 s_client -connect <FQDN of vIDM host>:443 < /dev/null 2> /dev/null | openssl x509 -sha256 -fingerprint -noout -in /dev/stdin
```

Si vous obtenez une erreur lors de l'exécution de la commande, vous devrez peut-être exécuter `openssl1` avec la commande `sudo`, c'est-à-dire, `sudo openssl1`

- Si vous êtes connecté à un serveur qui peut effectuer un test ping sur l'hôte vIDM, exécutez la commande `openssl` 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
```

Configurer l'intégration de VMware Identity Manager

Vous pouvez intégrer NSX-T Data Center à VMware Identity Manager (vIDM), qui propose des services de gestion d'identité. Le déploiement vIDM peut être un hôte vIDM autonome ou un cluster vIDM.

L'hôte vIDM ou tous les composants du cluster vIDM doivent 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, consultez la documentation de VMware Identity Manager à l'adresse <https://docs.vmware.com/fr/VMware-Identity-Manager/index.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.

Si l'accès à l'API NSX-T est nécessaire, l'une des configurations suivantes doit être vraie :

- vIDM dispose d'un certificat signé par une autorité de certification connu.
- vIDM dispose du certificat d'autorité de certification du connecteur approuvé côté service vIDM.
- vIDM utilise le mode connecteur sortant.

Note NSX Manager et vIDM doivent être dans le même fuseau horaire. Il est recommandé d'utiliser UTC.

Vous devez configurer vos serveurs DNS pour qu'ils disposent d'enregistrements PTR si vous n'utilisez pas l'adresse IP virtuelle ou un équilibreur de charge externe (cela signifie que le gestionnaire est configuré à l'aide de l'adresse IP physique ou du nom de domaine complet du nœud).

Si vous configurez vIDM pour qu'il soit intégré à un équilibreur de charge externe, vous devez activer la persistance de session sur l'équilibreur de charge pour éviter des problèmes tels que les pages qui ne se chargent pas ou un utilisateur qui se déconnecte de manière inattendue.

Si le déploiement vIDM est un cluster vIDM, l'équilibreur de charge vIDM doit être configuré pour l'arrêt et le rechargement SSL.

Lorsque vIDM est activé, vous pouvez toujours vous connecter à NSX Manager avec un compte d'utilisateur local si vous utilisez l'URL `https://<nsx-manager-ip-address>/login.jsp?local=true`.

Si vous utilisez l'attribut UserPrincipalName (UPN) pour vous connecter à vIDM, l'authentification sur NSX-T peut échouer. Pour éviter ce problème, utilisez un type d'informations d'identification différent, par exemple, SAMAccountName.

Si vous utilisez NSX Cloud, vous pouvez vous connecter à CSM séparément à l'aide de l'URL `https://<csm-ip-address>/login.jsp?local=true`

Conditions préalables

- Vérifiez que vous disposez de l'empreinte numérique de certificat de l'hôte vIDM ou de l'équilibreur de charge vIDM, selon le type de déploiement vIDM (un hôte vIDM autonome ou un cluster vIDM). La commande permettant d'obtenir l'empreinte numérique est la même dans les deux cas. 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 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://docs.vmware.com/fr/VMware-Workspace-ONE-Access/3.3/idm-administrator/GUID-AD4B6F91-2D68-48F2-9212-5B69D40A1FAE.html>. Lorsque vous créez le client, vous devez uniquement effectuer les opérations suivantes :
 - Définissez **Type d'accès** sur **Jeton du client de service**.
 - Spécifiez un ID de client.
 - Développez le champ **Avancé**, puis cliquez sur **Générer un secret partagé**.
 - Cliquez sur **Ajouter**.

Remarque sur NSX Cloud Si vous utilisez NSX Cloud, vérifiez également que CSM est enregistré en tant que client OAuth sur vIDM.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Système > Utilisateurs**.
- 3 Cliquez sur l'onglet **Configuration**.
- 4 Cliquez sur **Modifier**.
- 5 Pour activer l'intégration de l'équilibreur de charge externe, cliquez sur le bouton bascule **Intégration de l'équilibreur de charge externe**.

Note Si l'adresse IP virtuelle (VIP) est définie (vérifiez **Système > Dispositifs > Adresse IP virtuelle**), vous ne pouvez pas utiliser **l'intégration de l'équilibreur de charge externe** même si vous l'activez. Cela est dû au fait que vous pouvez disposer d'une adresse IP virtuelle ou de l'équilibreur de charge externe lors de la configuration de vIDM, mais pas des deux. Désactivez l'adresse IP virtuelle si vous souhaitez utiliser l'équilibreur de charge externe. Pour plus d'informations, reportez-vous à la section [Configurer une adresse IP virtuelle pour un cluster](#) dans le *Guide d'installation de NSX-T Data Center*.

- 6 Pour activer l'intégration de VMware Identity Manager, cliquez sur le bouton bascule **Intégration de VMware Identity Manager**.

7 Fournissez les informations suivantes.

Paramètre	Description
Dispositif VMware Identity Manager	Nom de domaine complet (FQDN) de l'hôte vIDM ou de l'équilibreur de charge vIDM, selon le type de déploiement vIDM (un hôte vIDM autonome ou un cluster vIDM).
ID de client OAuth	Identifiant créé lors de l'enregistrement de NSX Manager sur vIDM.
Secret du client OAuth	Code secret créé lors de l'enregistrement de NSX Manager sur vIDM.
Empreinte numérique SSL	Empreinte numérique du certificat de l'hôte vIDM.
Dispositif NSX	Adresse IP ou nom de domaine complet (FQDN) de NSX Manager. Si vous utilisez un cluster NSX Manager, utilisez le nom de domaine complet de l'équilibreur de charge ou le nom de domaine complet ou l'adresse IP du VIP du cluster. 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.

8 Cliquez sur **Enregistrer**.

9 Si vous utilisez NSX Cloud, répétez les étapes 1 à 8 à partir du dispositif CSM en vous connectant à CSM au lieu de NSX Manager.

Valider les fonctionnalités de VMware Identity Manager

Après la configuration de VMware Identity Manager, validez les fonctionnalités. Sauf si VMware Identity Manager est correctement configuré et validé, certains utilisateurs peuvent recevoir des messages Non autorisé (code d'erreur 98) lors de la tentative de connexion.

Sauf si VMware Identity Manager est correctement configuré et validé, certains utilisateurs peuvent recevoir des messages Non autorisé (code d'erreur 98) lors de la tentative de connexion.

Procédure

1 Créez un codage en Base64 du nom d'utilisateur et du mot de passe.

Exécutez la commande suivante pour obtenir le codage et supprimer le caractère '\n' de fin.
Par exemple :

```
echo -n 'sfadmin@ad.node.com:password1234!' | base64 | tr -d '\n'
c2ZhzG1pbkZhZC5ub2RlLmNvbTpwYXNzd29yZDEyMzQhCg==
```

2 Vérifiez que chaque utilisateur peut effectuer un appel d'API à chaque nœud.

Utilisez une commande curl d'autorisation à distance : `curl -k -H 'Authorization: Remote <base64 encoding string>' https://<node FQDN>/api/v1/node/aaa/auth-policy`.
Par exemple :

```
curl -k -H 'Authorization: Remote c2ZhZG1pbkZhZC5ub2RlLmNvbTpwYXNzd29yZDEyMzQhCg==' /
https://tmgr1.cptroot.com/api/v1/node/aaa/auth-policy
```

Cela renvoie les paramètres de stratégie d'autorisation, tels que :

```
{
  "_schema": "AuthenticationPolicyProperties",
  "_self": {
    "href": "/node/aaa/auth-policy",
    "rel": "self"
  },
  "api_failed_auth_lockout_period": 900,
  "api_failed_auth_reset_period": 900,
  "api_max_auth_failures": 5,
  "cli_failed_auth_lockout_period": 900,
  "cli_max_auth_failures": 5,
  "minimum_password_length": 12
}
```

Si la commande ne renvoie pas d'erreur, VMware Identity Manager fonctionne correctement. Aucune autre étape n'est requise. Si la commande curl renvoie une erreur, il se peut que l'utilisateur soit verrouillé.

Note Les stratégies de verrouillage de compte sont définies et appliquées au niveau de chaque nœud. Si un nœud du cluster a verrouillé un utilisateur, ce n'est pas forcément le cas des autres nœuds.

3 Pour réinitialiser un verrouillage d'utilisateur sur un nœud :

- a Récupérez la stratégie d'autorisation à l'aide de l'utilisateur admin NSX Manager local :

```
curl -k -u 'admin:<password>' https://nsxmgr/api/v1/node/aaa/auth-policy
```

- b Enregistrez la sortie dans un fichier JSON dans le répertoire de travail actuel.

- c Modifiez le fichier pour changer les paramètres de la période de verrouillage.

Par exemple, un grand nombre des paramètres par défaut appliquent des périodes de verrouillage et de réinitialisation de 900 secondes. Modifiez ces valeurs pour activer la réinitialisation immédiate, par exemple :

```
{
  "_schema": "AuthenticationPolicyProperties",
  "_self": {
    "href": "/node/aaa/auth-policy",
    "rel": "self"
  },
  "api_failed_auth_lockout_period": 1,
  "api_failed_auth_reset_period": 1,
  "api_max_auth_failures": 5,
  "cli_failed_auth_lockout_period": 1,
  "cli_max_auth_failures": 5,
  "minimum_password_length": 12
}
```

- d Appliquez la modification au nœud affecté.

```
curl -k -u 'admin:<password>' -H 'Content-Type: application/json' -d \
@<modified_policy_setting.json> https://nsxmgr/api/v1/node/aaa/auth-policy
```

- e (Facultatif) Rétablissez les paramètres précédents des fichiers de paramètres de la stratégie d'autorisation.

Cela devrait résoudre le problème de verrouillage. Si vous pouvez encore effectuer des appels d'API d'authentification à distance, mais que vous ne parvenez toujours pas à vous connecter via le navigateur, il se peut qu'un cache ou un cookie non valide soit stocké dans le navigateur. Effacez le cache et les cookies, puis réessayez.

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>

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 configurez 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 time.nist.gov
server pool.ntp.org
server time.is dynamic
restrict 192.168.100.0 netmask 255.255.255.0 nomodify notrap
```

- 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
- aucune

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 d'équilibrage de charge
- Auditeur d'équilibrage de charge
- Administrateur de VPN
- Administrateur de Guest Introspection
- Administrateur de l'introspection réseau

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 21-5. Rôles et autorisations](#) et [Tableau 21-6. Rôles et autorisations pour la mise en réseau avancée et la sécurité](#) affichent 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 EC : administrateur d'équilibrage de charge
- Aud EC : auditeur d'équilibrage de charge
- Adm VPN : administrateur de VPN
- Adm GI : administrateur de Guest Introspection
- Adm NI : administrateur de l'introspection réseau
- AC : accès complet
- E : Exécution
- L : Lecture

Tableau 21-5. Rôles et autorisations

Opération	AE	A	IR	OR	IS	OS	Adm SC	Aud SC	Adm EC	Aud EC	Adm VPN	Adm GI	Adm NI
Mise en réseau > Passerelles de niveau 0	AC	L	AC	AC	L	L	AC	L	L	L	L	L	L
Mise en réseau > Interface réseau	AC	L	AC	AC	L	L	AC	L	L	L	L	L	L
Mise en réseau > Routes statiques du réseau	AC	L	AC	AC	L	L	AC	L	L	L	L	L	L
Mise en réseau > Services de paramètres régionaux	AC	L	AC	AC	L	L	AC	L	L	L	L	L	L
Mise en réseau > Configuration statique ARP	AC	L	AC	AC	L	L	AC	L	L	L	L	L	L

Tableau 21-5. Rôles et autorisations (suite)

Opération	AE	A	IR	OR	IS	OS	Adm SC	Aud SC	Adm EC	Aud EC	Adm VPN	Adm GI	Adm NI
Mise en réseau > Segments	AC	L	AC	AC	L	L	AC	L	L	L	L	L	L
Mise en réseau > Segments > Profils de segments	AC	L	AC	AC	L	L	AC	L	L	L	L	L	L
Mise en réseau > Pools d'adresses IP	AC	L	AC	AC	L	L	AC	L	L	L	Aucun	Aucun	aucune
Mise en réseau > Stratégies de transfert	AC	L	AC	L	AC	L	AC	L	Aucun	Aucun	Aucun	Aucun	aucune
Mise en réseau > DNS	AC	L	AC	AC	L	L	AC	L	L	L	Aucun	Aucun	aucune
Mise en réseau > Équilibrage de charge	AC	L	Aucun	aucune	L	Aucun	AC	L	AC	L	Aucun	Aucun	aucune
Mise en réseau > NAT	AC	L	AC	L	AC	L	AC	L	L	L	Aucun	Aucun	aucune
Mise en réseau > VPN	AC	L	AC	L	AC	L	AC	L	Aucun	aucune	AC	Aucun	aucune
Mise en réseau > Profils IPv6													
Sécurité > Pare-feu distribué	AC	L	L	L	AC	L	AC	L	L	L	L	L	L

Tableau 21-5. Rôles et autorisations (suite)

Opération	AE	A	IR	OR	IS	OS	Adm SC	Aud SC	Adm EC	Aud EC	Adm VPN	Adm GI	Adm NI
Sécurité > Pare-feu de passerelle	AC	L	L	L	AC	L	AC	L	Aucun	Aucun	Aucun	aucune	AC
Sécurité > Inspection réseau	AC	L	L	L	L	L	AC	L	Aucun	Aucun	Aucun	aucune	AC
Sécurité > Règles de protection de point de terminaison	AC	L	L	L	L	L	AC	L	Aucun	Aucun	aucune	AC	aucune
Inventaire > Profils de contexte	AC	L	AC	L	AC	L	AC	L	L	L	L	L	L
Inventaire > Machines virtuelles	L	L	L	L	L	L	L	L	L	L	L	L	L
Planifier et dépanner > Mise en miroir de port	AC	L	AC	L	L	L	AC	L	Aucun	Aucun	Aucun	Aucun	aucune
Planifier et dépanner > Liaison de mise en miroir de port	AC	L	AC	AC	L	L	AC	L	L	L	L	L	L

Tableau 21-5. Rôles et autorisations (suite)

Opération	AE	A	IR	OR	IS	OS	Adm SC	Aud SC	Adm EC	Aud EC	Adm VPN	Adm GI	Adm NI
Planifier et dépanner > Liaison de profil de surveillance	AC	L	AC	AC	L	L	AC	L	L	L	L	L	L
Planifier et dépanner > Profils IPFIX de pare-feu	AC	L	AC	L	AC	L	AC	L	L	L	L	L	L
Planifier et dépanner > Profils IPFIX de commutateur	AC	L	AC	L	L	L	AC	L	L	L	L	L	L
Système > Infrastructure > Nœuds > Hôtes	AC	L	L	L	L	L	L	L	Aucun	Aucun	Aucun	Aucun	aucune
Système > Infrastructure > Nœuds > Nœuds	AC	L	AC	L	AC	L	L	L	L	L	Aucun	Aucun	aucune
Système > Infrastructure > Nœuds > Dispositifs Edge	AC	L	AC	L	L	L	L	L	Aucun	Aucun	Aucun	Aucun	aucune

Tableau 21-5. Rôles et autorisations (suite)

Opération	AE	A	IR	OR	IS	OS	Adm SC	Aud SC	Adm EC	Aud EC	Adm VPN	Adm GI	Adm NI
Système > Infras tructure > Nœud s > Clust ers Edge	AC	L	AC	L	L	L	L	L	Aucun	Aucun	Aucun	Aucun	aucune
Système > Infras tructure > Nœud s > Pont s	AC	L	AC	L	L	L	Aucun	aucune	L	L	Aucun	Aucun	aucune
Système > Infras tructure > Nœud s > Nœu ds de transpor t	AC	L	L	L	L	L	L	L	L	L	Aucun	Aucun	aucune
Système > Infras tructure > Nœud s > Tunn els	L	L	L	L	L	L	L	L	L	L	Aucun	Aucun	aucune
Système > Infras tructure > Profils > Profil s de liaison montant e	AC	L	L	L	L	L	L	L	L	L	Aucun	Aucun	aucune
Système > Infras tructure > Profils > Profil s de cluster Edge	AC	L	AC	L	L	L	L	L	L	L	Aucun	Aucun	aucune

Tableau 21-5. Rôles et autorisations (suite)

Opération	AE	A	IR	OR	IS	OS	Adm SC	Aud SC	Adm EC	Aud EC	Adm VPN	Adm GI	Adm NI
Système > Infras tructure > Profils > Confi guration	AC	L	Aucu n	Aucu n	Aucu n	aucun e	L	L	Auc un	Auc un	Aucu n	Aucun	aucune
Système > Infras tructure > Zones de transpor t > Zone s de transpor t	AC	L	L	L	L	L	L	L	L	L	Aucu n	Aucun	aucune
Système > Infras tructure > Zones de transpor t > Zone de transpor t > Profil s	AC	L	L	L	L	L	L	L	Auc un	Auc un	Aucu n	Aucun	aucune
Système > Infras tructure > Gestio nnaires de calcul	AC	L	L	L	L	L	L	L	Auc un	Auc un	aucu ne	L	L
Système > Certifi cats	AC	L	Aucu n	aucu ne	AC	L	Aucu n	aucu ne	AC	L	AC	Aucun	aucune
Système > Déplo iements de services > Instan ces de service	AC	L	L	L	AC	L	AC	L	Auc un	Auc un	aucu ne	AC	AC

Tableau 21-5. Rôles et autorisations (suite)

Opération	AE	A	IR	OR	IS	OS	Adm SC	Aud SC	Adm EC	Aud EC	Adm VPN	Adm GI	Adm NI
Système > Utilitaires > Bundle de support	AC	L	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	aucune
Système > Utilitaires > Sauvegarde	AC	L	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	aucune
Système > Utilitaires > Restaurer	AC	L	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	aucune
Système > Utilitaires > Mettre à niveau	AC	L	L	L	L	L	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	aucune
Système > Utilisateurs > Attributions de rôles	AC	L	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	aucune
Système > Active Directory	AC	L	AC	L	AC	AC	L	L	L	L	L	L	L
Système > Utilisateurs > Configuration	AC	L	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	aucune
Système > Licences	AC	L	L	L	L	L	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	aucune

Tableau 21-5. Rôles et autorisations (suite)

Opération	AE	A	IR	OR	IS	OS	Adm SC	Aud SC	Adm EC	Aud EC	Adm VPN	Adm GI	Adm NI
Système > Administration du système	AC	L	L	L	L	L	L	L	Aucun	Aucun	Aucun	Aucun	aucune
Configuration du tableau de bord personnalisé	AC	L	L	L	L	L	AC	L	L	L	L	L	L
Système > Gestion du cycle de vie > Migrer	AC	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	aucune

Tableau 21-6. Rôles et autorisations pour la mise en réseau avancée et la sécurité

Opération	AE	A	IR	OR	IS	OS	Adm SC	Aud SC	Adm EC	Aud EC	Adm VPN	Adm GI	Adm NI
Outils > Connexion au port	E	L	E	E	E	E	E	L	E	E	Aucun	Aucun	aucune
Outils > Traceflow	E	L	E	E	E	E	E	L	E	E	Aucun	Aucun	aucune
Outils > Mise en miroir de ports	AC	L	AC	L	L	L	AC	L	Aucun	Aucun	Aucun	Aucun	aucune
Outils > IPFIX	AC	L	AC	L	AC	L	AC	L	L	L	L	L	L
Pare-feu > Pare-feu distribué > Général	AC	L	L	L	AC	L	AC	L	Aucun	Aucun	Aucun	aucune	L

Tableau 21-6. Rôles et autorisations pour la mise en réseau avancée et la sécurité (suite)

Opération	AE	A	IR	OR	IS	OS	Adm SC	Aud SC	Adm EC	Aud EC	Adm VPN	Adm GI	Adm NI
Pare-feu > Pare-feu distribué > Configuration	AC	L	L	L	AC	L	AC	L	Aucun	Aucun	Aucun	Aucun	aucune
Pare-feu > Pare-feu Edge	AC	L	L	L	AC	L	AC	L	Aucun	Aucun	Aucun	aucune	AC
Routage > Routeurs	AC	L	AC	AC	L	L	AC	L	L	L	L	Aucun	L
Routage > NAT	AC	L	AC	L	AC	L	AC	L	L	L	Aucun	Aucun	aucune
DHCP > Profils de serveur	AC	L	AC	L	Aucun	aucune	AC	L	Aucun	Aucun	Aucun	Aucun	aucune
DHCP > Serveurs	AC	L	AC	L	Aucun	aucune	AC	L	Aucun	Aucun	Aucun	Aucun	aucune
DHCP > Profils de relais	AC	L	AC	L	Aucun	aucune	AC	L	Aucun	Aucun	Aucun	Aucun	aucune
DHCP > Services de relais	AC	L	AC	L	Aucun	aucune	AC	L	Aucun	Aucun	Aucun	Aucun	aucune
DHCP > Proxys de métadonnées	AC	L	AC	L	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	aucune
IPAM	AC	L	AC	AC	L	L	Aucun	aucune	L	L	Aucun	Aucun	aucune
Communtation > Communtateurs	AC	L	AC	AC	L	L	AC	L	L	L	L	Aucun	L
Communtation > Ports	AC	L	AC	AC	L	L	AC	L	L	L	L	Aucun	L

Tableau 21-6. Rôles et autorisations pour la mise en réseau avancée et la sécurité (suite)

Opération	AE	A	IR	OR	IS	OS	Adm SC	Aud SC	Adm EC	Aud EC	Adm VPN	Adm GI	Adm NI
Commutation > Profils de commutation	AC	L	AC	AC	L	L	AC	L	L	L	Aucun	Aucun	aucune
Mise en réseau > Équilibrages de charge	AC	L	Aucun	aucune	L	Aucun	AC	L	AC	L	Aucun	Aucun	aucune
Équilibrage de charge > Profils > Profils SSL	AC	L	Aucun	aucune	AC	L	AC	L	AC	L	Aucun	Aucun	aucune
Inventaire > Groupes	AC	L	AC	L	AC	L	AC	L	L	L	L	L	L
Inventaire > Ensembles d'adresses IP	AC	L	AC	L	AC	L	AC	L	L	L	L	L	L
Inventaire > Pools d'adresses IP	AC	L	AC	L	Aucun	Aucun	Aucun	aucune	L	L	L	L	L
Inventaire > Ensembles d'adresses MAC	AC	L	AC	L	AC	L	AC	L	L	L	L	L	L
Inventaire > Services	AC	L	AC	L	AC	L	AC	L	L	L	L	L	L

Tableau 21-6. Rôles et autorisations pour la mise en réseau avancée et la sécurité (suite)

Opération	AE	A	IR	OR	IS	OS	Adm SC	Aud SC	Adm EC	Aud EC	Adm VPN	Adm GI	Adm NI
Inventaire > Machines virtuelles	L	L	L	L	L	L	L	L	L	L	L	L	L
Inventaire > Machines virtuelles > Configurer les balises	AC	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	Aucun	aucune

Ajouter une attribution de rôle ou une identité de principal

Vous pouvez attribuer des rôles à des utilisateurs ou groupes d'utilisateurs si VMware Identity Manager est intégré à NSX-T Data Center. Vous pouvez également attribuer des rôles à des identités de principal.

Un principal est un composant NSX-T Data Center ou une application tierce, comme 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 : il peut s'agir de n'importe quelle valeur alphanumérique attribuée à une identité de principal
- Certificat
- Rôle RBAC indiquant les droits d'accès de ce principal

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.

Si le certificat d'un utilisateur d'identité de principal expire, vous devez importer un nouveau certificat et effectuer un appel d'API pour mettre à jour le certificat de l'utilisateur d'identité de principal (voir la procédure ci-dessous). Pour plus d'informations sur l'API NSX-T Data Center, un lien vers la ressource API est disponible à l'adresse <https://docs.vmware.com/fr/VMware-NSX-T-Data-Center>.

Le certificat d'un utilisateur d'identité de principal doit répondre aux exigences suivantes :

- S'appuyer sur SHA256.
- Disposer d'un algorithme de message RSA/DSA avec une taille de clé de 2048 bits ou supérieure.
- Ne pas être un certificat racine.

Vous pouvez supprimer une identité de principal à l'aide de l'API. Toutefois, la suppression d'une identité de principal ne supprime pas automatiquement le certificat correspondant. Vous devez supprimer le certificat manuellement.

Étapes de suppression d'une identité de principal et de son certificat :

- 1 Obtenez les détails de l'identité de principal à supprimer et notez la valeur `certificate_id` dans la réponse.

```
GET /api/v1/trust-management/principal-identities/<principal-identity-id>
```

- 2 Supprimez l'identité de principal.

```
DELETE /api/v1/trust-management/principal-identities/<principal-identity-id>
```

- 3 Supprimez le certificat à l'aide de la valeur `certificate_id` obtenue à l'étape 1.

```
DELETE /api/v1/trust-management/certificates/<certificate_id>
```

Conditions préalables

- Si vous souhaitez attribuer des rôles à des utilisateurs, vérifiez qu'un hôte vIDM est associé à NSX-T. Pour plus d'informations, reportez-vous à la section [Configurer l'intégration de VMware Identity Manager](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Système > Utilisateurs**.
- 3 Pour attribuer des rôles à des utilisateurs, sélectionnez **Ajouter > Attribution de rôle**.
 - a Sélectionnez un utilisateur ou un groupe d'utilisateurs.
 - b Sélectionnez un rôle.
 - c Cliquez sur **Enregistrer**.
- 4 Pour ajouter une identité de principal, sélectionnez **Ajouter > Identité de principal avec rôle**.
 - a Entrez un nom pour l'identité de principal.
 - b Sélectionnez un rôle.
 - c Entrez un ID de nœud.

- d Entrez un certificat au format PEM.
 - e Cliquez sur **Enregistrer**.
- 5 (Facultatif) Si vous utilisez NSX Cloud, connectez-vous au dispositif CSM au lieu de NSX Manager et répétez les étapes 1 à 4.
- 6 Si le certificat de l'identité de principal expire, procédez comme suit :
- a Importez un nouveau certificat et notez l'ID du certificat. Reportez-vous à la section [Importer un certificat](#).
 - b Appelez l'API suivante pour obtenir l'ID de l'identité de principal.
- GET `https://<nsx-mgr>/api/v1/trust-management/principal-identities`
- c Appelez l'API suivante pour mettre à jour le certificat de l'identité de principal. Vous devez fournir l'ID du certificat importé et l'ID de l'utilisateur d'identité de principal.

Par exemple,

```
POST https://<nsx-mgr>/api/v1/trust-management/principal-identities?
action=update_certificate
{
  "principal_identity_id": "ebd3032d-728e-44d4-9914-d4f81c9972cb",
  "certificate_id" : "abd3032d-728e-44d4-9914-d4f81c9972cc"
}
```

Sauvegarde et restauration de NSX Manager

Si le cluster NSX Manager devient inopérable ou si vous souhaitez rétablir l'état précédent de votre environnement, vous pouvez procéder à cette restauration à partir d'une 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.

Deux types de sauvegarde existent :

Sauvegarde de cluster

Cette sauvegarde inclut l'état souhaité du réseau virtuel.

Sauvegarde de nœud

Il s'agit d'une sauvegarde des nœuds NSX Manager.

Il existe deux méthodes de sauvegarde :

Manuel

Vous exécutez manuellement la sauvegarde à tout moment.

Automatisé

Les sauvegardes automatisées sont exécutées selon un planning que vous définissez. Les sauvegardes automatisées sont fortement recommandées pour des sauvegardes à jour.

Vous pouvez restaurer une configuration de NSX-T Data Center à l'état dans lequel elle est capturée dans n'importe quelle sauvegarde. Lors de la restauration d'une sauvegarde, vous devez effectuer la restauration vers de nouveaux dispositifs NSX Manager exécutant la même version de NSX Manager que les dispositifs qui ont été sauvegardés.

Configurer des sauvegardes

Pour pouvoir effectuer des sauvegardes, vous devez configurer un serveur de fichiers de sauvegarde. Après avoir configuré un serveur de fichiers de sauvegarde, vous pouvez démarrer une sauvegarde à tout moment ou configurer une planification pour des sauvegardes automatiques.

Conditions préalables

Vérifiez que vous disposez de l'empreinte digitale SSH du serveur de fichiers de sauvegarde. Seule une clé ECDSA avec hachage SHA256 (256 bits) est acceptée en tant qu'empreinte digitale. Reportez-vous à la section [Rechercher l'empreinte digitale SSH d'un serveur distant](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Système > Sauvegarde et restauration**.
- 3 Cliquez sur **Modifier** dans le coin supérieur droit de la page pour configurer des sauvegardes.
- 4 Entrez l'adresse IP ou le nom d'hôte du serveur de fichiers de sauvegarde.
- 5 Modifiez le port par défaut, si nécessaire.
- 6 Le champ Protocole est déjà renseigné. Ne modifiez pas la valeur.

SFTP est le seul protocole pris en charge.

- 7 Entrez le nom d'utilisateur et le mot de passe requis pour vous connecter au serveur de fichiers de sauvegarde.

La première fois que vous configurez un serveur de fichiers, vous devez fournir un mot de passe. Par la suite, si vous reconfigurez le serveur de fichiers et que l'adresse IP du serveur (ou nom d'hôte), le port et le nom d'utilisateur soient identiques, vous n'avez pas à entrer de nouveau le mot de passe.

- 8 Dans le champ **Répertoire de destination**, entrez le chemin de répertoire absolu d'enregistrement des sauvegardes.

Le répertoire doit déjà exister et ne peut pas être /. Si vous disposez de plusieurs déploiements NSX-T Data Center, vous devez utiliser un répertoire différent pour chaque

déploiement. Si le serveur de fichiers de sauvegarde est une machine Windows, vous utilisez toujours la barre oblique lorsque vous spécifiez le répertoire de destination. Par exemple, si le répertoire de sauvegarde sur la machine Windows est C:\SFTP_Root\backup, spécifiez /SFTP_Root/backup comme répertoire de destination.

Note Le processus de sauvegarde générera un nom pour le fichier de sauvegarde qui peut être assez long. Sur un serveur Windows, la longueur du nom de chemin complet du fichier de sauvegarde peut dépasser la limite définie par Windows et provoquer l'échec des sauvegardes. Pour éviter ce problème, reportez-vous à l'article <https://kb.vmware.com/s/article/76528> de la base de connaissances.

- 9 Pour chiffrer les sauvegardes, cliquez sur le bouton bascule **Modifier la phrase secrète de chiffrement** et entrez la phrase secrète de chiffrement.

Vous aurez besoin de cette phrase secrète pour restaurer une sauvegarde. Si vous oubliez la phrase secrète, vous ne pouvez restaurer aucune sauvegarde.

- 10 Entrez l'empreinte digitale SSH du serveur qui stocke les sauvegardes.

Vous pouvez laisser ce champ vide, et accepter ou refuser l'empreinte digitale fournie par le serveur.

- 11 Cliquez sur l'onglet **Planification**.

- 12 Pour activer les sauvegardes automatiques, cliquez sur le bouton bascule **Sauvegarde automatique**.

- 13 Cliquez sur **Hebdomadaire** et définissez les jours et l'heure de la sauvegarde, ou cliquez sur **Intervalle** et définissez l'intervalle entre les sauvegardes.

- 14 L'activation de **Détecter les modifications apportées à la configuration NSX** déclenche une sauvegarde de configuration complète non planifiée lorsqu'elle détecte des modifications liées à l'exécution ou non liées à la configuration, ou toute modification de la configuration de l'utilisateur.

Vous pouvez définir l'intervalle entre les sauvegardes déclenchées par les modifications apportées à la configuration. La valeur par défaut est de 5 minutes.

Note Cette option peut potentiellement générer un grand nombre de sauvegardes. Utilisez-la avec précaution.

- 15 Cliquez sur **Enregistrer**.

Résultats

Après avoir configuré un serveur de fichiers de sauvegarde, vous pouvez cliquer sur **Sauvegarder maintenant** pour lancer à tout moment une sauvegarde.

Suppression d'anciennes sauvegardes

Les sauvegardes peuvent s'accumuler sur le serveur de fichiers de sauvegarde et utiliser un grand espace de stockage. Vous pouvez exécuter un script fourni avec NSX-T Data Center pour supprimer automatiquement les anciennes sauvegardes.

Vous trouverez le script Python `nsx_backup_cleaner.py` dans le répertoire `/var/vmware/nsx/file-store` sur NSX Manager. Vous devez vous connecter en tant qu'utilisateur racine pour accéder à ce fichier. Généralement, vous planifiez une tâche sur le serveur de fichiers de sauvegarde pour exécuter ce script régulièrement afin de supprimer les anciennes sauvegardes. Les instructions d'utilisation suivantes expliquent comment exécuter le script :

```
nsx_backup_cleaner.py -d backup_dir [-k 1] [-l 5] [-h]
Or
nsx_backup_cleaner.py --dir backup_dir [--retention-period 1] [--min-count 5] [--help]

Required parameters:
  -d/--dir: Backup root directory
  -k/--retention-period: Number of days need to retain a backup file

Optional parameters:
  -l/--min-count: Minimum number of backup files to be kept, default value is 100
  -h/--help: Display help message
```

L'ancienneté d'une sauvegarde est le résultat de la différence entre l'horodatage de la sauvegarde et l'heure à laquelle le script est exécuté. Si cette valeur est supérieure à la période de rétention, la sauvegarde est supprimée si le nombre de sauvegardes sur le disque est supérieur au nombre minimal de sauvegardes.

Pour plus d'informations sur la configuration du script à exécuter périodiquement sur un serveur Linux ou Windows, reportez-vous aux commentaires figurant au début du script.

Liste des sauvegardes disponibles

Le serveur de fichiers de sauvegarde stocke les sauvegardes pour toutes les instances de NSX Manager. Pour obtenir la liste des sauvegardes afin de pouvoir choisir celle que vous souhaitez restaurer, vous devez exécuter le script `get_backup_timestamps.sh`.

Le script se trouve sur NSX Manager. Le nom du chemin d'accès complet est `/var/vmware/nsx/file-store/get_backup_timestamps.sh`. Vous pouvez exécuter ce script sur n'importe quelle machine Linux ou dispositif NSX-T Data Center. Il est recommandé de copier ce script après l'installation de NSX-T Data Center sur une machine qui n'est pas une instance de NSX Manager, afin de pouvoir exécuter ce script même si toutes les instances de NSX Manager deviennent inaccessibles. Si vous avez besoin de restaurer une sauvegarde, mais que vous n'avez pas accès à ce script, vous pouvez installer une nouvelle instance de NSX Manager et exécutez le script depuis celle-ci.

Vous pouvez copier le script vers une autre machine ou vers le serveur de fichiers de sauvegarde en vous connectant au dispositif NSX Manager en tant qu'administrateur et en exécutant une commande CLI. Par exemple :

```
nsxmgr-1> copy file get_backup_timestamps.sh url scp://admin@10.127.1.20/tmp/
admin@10.127.1.20's password:
nsxmgr-1>
```

Le script est interactif et vous invitera à entrer les informations que vous avez spécifiées lors de la configuration du serveur de fichiers de sauvegarde. Vous pouvez spécifier le nombre de sauvegardes à afficher. Chaque sauvegarde est répertoriée avec un horodatage, l'adresse IP du nœud NSX Manager (ou le nom de domaine complet si le nœud NSX Manager est configuré pour publier son nom de domaine complet) et l'ID de nœud. Par exemple,

```
admin@host1:/home/admin# ./get_backup_timestamps.sh
Enter file server ip:
10.108.115.108
Enter port:
22
Enter directory path:
/home/nsx/backups
Enter number of latest backup or press Enter to list all backups:

root@10.108.115.108's password:
Latest backups:
[Backup timestamp; IP address/FQDN; Node id]
2019-01-22;09:00:33 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
2019-01-22;09:01:52 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
2019-01-22;09:13:30 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
2019-01-22;09:14:42 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
2019-01-22;09:16:43 wdc75.platformqe.com 41893642-597b-915f-5117-7da576df4ff2
```

Restaurer une sauvegarde

La restauration d'une sauvegarde entraîne la restauration de l'état du réseau au moment de la sauvegarde. De plus, les configurations gérées par NSX Manager sont également restaurées et toutes les modifications, telles que l'ajout ou la suppression de nœuds, qui ont été apportées à l'infrastructure depuis la sauvegarde sont appliquées.

Vous devez restaurer la sauvegarde sur un nouveau dispositif NSX Manager.

Si vous disposiez d'un cluster NSX Manager lorsque la sauvegarde a été effectuée, vous devez également restaurer un cluster NSX Manager. Le processus de restauration restaure d'abord un nœud NSX Manager, puis vous invite à ajouter les autres nœuds NSX Manager.

Important Si des nœuds du cluster NSX Manager sont toujours disponibles, vous devez les mettre hors tension avant de démarrer la restauration.

Conditions préalables

- Vérifiez que vous disposez des informations d'identification pour la connexion du serveur de fichiers de sauvegarde.
- Vérifiez que vous disposez de l'empreinte digitale SSH du serveur de fichiers de sauvegarde. Seule une clé ECDSA avec hachage SHA256 (256 bits) est acceptée en tant qu'empreinte digitale. Reportez-vous à la section [Rechercher l'empreinte digitale SSH d'un serveur distant](#).
- Vérifiez que vous disposez de la phrase secrète du fichier de sauvegarde.
- Identifiez la sauvegarde que vous souhaitez restaurer en suivant la procédure décrite dans [Liste des sauvegardes disponibles](#). Notez l'adresse IP ou le nom de domaine complet du nœud NSX Manager qui a effectué la sauvegarde.
- Si vous configurez les nœuds NSX Manager pour publier leur nom de domaine complet, vous devez configurer les entrées de recherche directe et inversée pour les nœuds NSX Manager sur le serveur DNS.

Procédure

- 1 Mettez hors tension tous les nœuds du cluster NSX Manager que vous restaurez.
- 2 Installez un nouveau nœud NSX Manager sur lequel restaurer la sauvegarde.

- Si la liste de sauvegarde de la sauvegarde que vous restaurez contient une adresse IP, vous devez déployer le nouveau nœud NSX Manager avec la même adresse IP. Ne configurez pas le nœud NSX Manager pour publier son nom de domaine complet.

```
2019-01-22;09:01:52 10.196.196.77 35163642-6623-8f6d-7af0-52e03f16faed
```

- Si la liste de sauvegarde de la sauvegarde que vous restaurez contient un nom de domaine complet, vous devez configurer le nouveau nœud NSX Manager avec ce nom de domaine complet (reportez-vous à la section « Publication des noms de domaine complets des instances de NSX Manager » dans la rubrique « Installation de NSX Manager » du *Guide d'installation de NSX-T Data Center* pour plus d'informations). En outre, si le nouveau nœud NSX Manager a une adresse IP différente de celle d'origine, vous devez mettre à jour les entrées de recherche directe et inversée du serveur DNS pour le nœud NSX Manager avec la nouvelle adresse IP.

```
2019-01-22;09:16:43 nsxmgr.example.com 41893642-597b-915f-5117-7da576df4ff2
```

Une fois que le nouveau nœud de NSX Manager est en cours d'exécution et en ligne, vous pouvez procéder à la restauration.

- 3 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à la nouvelle instance de NSX Manager.
- 4 Sélectionnez **Système > Sauvegarde et restauration**.
- 5 Cliquez sur l'onglet **Restaurer**.
- 6 Pour configurer le serveur de fichiers de sauvegarde, cliquez sur **Modifier**.

- 7 Entrez l'adresse IP ou le nom d'hôte.
- 8 Si nécessaire, modifiez le numéro de port.
La valeur par défaut est 22.
- 9 Pour vous connecter au serveur, entrez le nom d'utilisateur et le mot de passe.
- 10 Dans la zone de texte **Répertoire de destination**, entrez le chemin de répertoire absolu d'enregistrement des sauvegardes.
- 11 Entrez la phrase secrète utilisée pour chiffrer les données sauvegardées.
- 12 Entrez l'empreinte digitale SSH du serveur qui stocke les sauvegardes.
- 13 Cliquez sur **Enregistrer**.
- 14 Sélectionnez une sauvegarde.
- 15 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 êtes invité à effectuer certaines actions, par exemple, ouvrir une session sur un nœud et exécuter un script.

Si la sauvegarde comporte des informations sur un cluster NSX Manager, vous êtes invité à ajouter des nœuds NSX Manager. Si vous décidez de ne pas ajouter de nœuds NSX Manager, vous pouvez toujours poursuivre la restauration.

Une fois l'opération de restauration terminée, l'écran **Fin de la restauration** affiche le résultat de la restauration, l'horodatage du fichier de sauvegarde ainsi que 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 s'il existait une erreur de restauration de cluster ou de restauration de nœud en vérifiant les fichiers journaux. Exécutez `get log-file syslog` pour afficher le fichier journal système et rechercher les chaînes `Échec de la restauration de cluster` et `Échec de la restauration de nœud`.

Pour redémarrer le gestionnaire, exécutez la commande `restart service manager`.

Pour redémarrer le gestionnaire, exécutez la commande `reboot`.

- 16 Si vous n'avez qu'un seul nœud déployé, une fois que le nœud NSX Manager restauré est opérationnel et fonctionnel, vous pouvez déployer des nœuds supplémentaires pour former un cluster NSX Manager.

Reportez-vous à *Guide d'installation de NSX-T Data Center* pour obtenir des instructions.

- 17 Une fois le nouveau cluster de NSX Manager déployé, supprimez les machines virtuelles du cluster NSX Manager d'origine que vous avez mises hors tension à l'étape 1.

Vous devez également remplacer les certificats sur le deuxième et le troisième nœuds du cluster.

Résultats

Si vous avez ajouté un gestionnaire de calcul après la sauvegarde et que vous essayez d'ajouter de nouveau le gestionnaire de calcul après la restauration, vous obtiendrez un message d'erreur indiquant que l'enregistrement a échoué. Vous pouvez cliquer sur le bouton **Résoudre** pour résoudre l'erreur et ajouter correctement le gestionnaire de calcul. Pour plus d'informations, reportez-vous à l'étape 4 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](#).

Sauvegarde et restauration pendant la mise à niveau

Le plan de gestion cesse de répondre pendant le processus de mise à niveau et vous devez restaurer une sauvegarde effectuée pendant que la mise à niveau était en cours.

Problème

Le coordinateur de mise à niveau a été mis à niveau et le plan de gestion cesse de répondre. Vous disposez d'une sauvegarde qui a été créée alors que la mise à niveau était en cours.

Solution

- 1 Déployez votre nœud Plan de gestion avec la même adresse IP que celle à partir de laquelle la sauvegarde a été créée.
- 2 Téléchargez le bundle de mise à niveau que vous avez utilisé au début du processus de mise à niveau.
- 3 Mettez à niveau le coordinateur de mise à niveau.
- 4 Restaurez la sauvegarde effectuée pendant le processus de mise à niveau.
- 5 Téléchargez un nouveau bundle de mise à niveau si nécessaire.
- 6 Poursuivez le processus de mise à niveau.

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 supprimez le gestionnaire de calcul, l'extension dans vCenter Server sera automatiquement supprimée. Si l'extension n'est pas supprimée pour une raison quelconque, vous pouvez supprimer manuellement l'extension avec la procédure suivante.

Conditions préalables

Activez l'accès au navigateur d'objets gérés (Managed Object Browser, MOB) de vCenter Server en suivant la procédure décrite dans <https://kb.vmware.com/s/article/2042554>.

Procédure

- 1 Connectez-vous au MOB à l'adresse `https://<nom d'hôte ou adresse IP de vCenter Server>/mob`.
- 2 Cliquez sur le lien de **contenu**, qui est la valeur de la propriété **contenu** dans la table Propriétés.
- 3 Cliquez sur le lien **Gestionnaire d'extensions**, qui est la valeur de la propriété **Gestionnaire d'extensions** dans la table Propriétés.
- 4 Cliquez sur le lien **Annuler l'enregistrement de l'extension** dans la table Méthodes.
- 5 Entrez `com.vmware.nsx.management.nsx` dans le champ de texte **valeur**.
- 6 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.
- 7 Pour vérifier que l'extension est supprimée, cliquez sur la méthode **Rechercher l'extension** sur la page précédente et appelez-la en saisissant la même valeur pour l'extension.
Le résultat doit être `void`.

Gestion du cluster NSX Manager

Vous pouvez redémarrer une instance de NSX Manager si elle ne fonctionne plus. Vous pouvez également modifier l'adresse IP d'une instance de NSX Manager.

Dans un environnement de production, il est fortement recommandé que le cluster NSX Manager dispose de trois membres afin d'en garantir la haute disponibilité. Si vous supprimez une instance de NSX Manager et en déployez une nouvelle, la nouvelle instance de NSX Manager peut avoir la même adresse IP ou une adresse IP différente.

Note Le nœud principal de NSX Manager est le nœud que vous créez en premier, avant de créer un cluster de gestionnaires. Ce nœud ne peut pas être supprimé. Après le déploiement de deux autres nœuds de gestionnaires à partir de l'interface utilisateur du nœud de gestionnaires principal pour former un cluster, seuls les deuxième et troisième nœuds de gestionnaires peuvent être supprimés (à partir de l'icône d'engrenage). Pour plus d'informations sur la suppression et l'ajout d'un nœud de gestionnaires, reportez-vous à la section [Modifier l'adresse IP d'un NSX Manager](#).

Afficher la configuration et l'état du cluster NSX Manager

Vous pouvez afficher la configuration et l'état du cluster NSX Manager à partir de l'interface utilisateur de NSX Manager. Vous pouvez obtenir des informations supplémentaires à l'aide de l'interface de ligne de commande.

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 > Présentation**

L'état du cluster NSX Manager s'affiche.

- 3 Pour voir des informations supplémentaires sur la configuration, exécutez la commande d'interface de ligne de commande suivante :

```
manager1> get cluster config
Cluster Id: 18807edd-56d1-4107-b7b7-508d766a08e3
Cluster Configuration Version: 3
Number of nodes in the cluster: 3

Node UUID: 43cd0642-275c-af1d-fe46-1f5200f9e5f9
Node Status: JOINED
```

ENTITY	ADDRESS	PORT	FQDN	UUID	IP
HTTPS	10.160.71.225	443	ychin-nsxmanager-ob-12065118-1-F5	5c8d01f1-f3ee-4f94-b517-a093d8fbfad3	
CONTROLLER	10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5	06fd0574-69c0-432e-a8af-53d140dbef8f	
CLUSTER_BOOT_MANAGER	10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5	da8d535e-7a0c-4dd8-8919-d88bdde006b8	
DATASTORE	10.160.71.225	9000	ychin-nsxmanager-ob-12065118-1-F5	3c9c4ec1-afef-47bd-aadb-1ed6a5536bc4	
MANAGER	10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5	eb5e8922-23bd-4c3a-ae22-d13d9195a6bc	
POLICY	10.160.71.225	-	ychin-nsxmanager-ob-12065118-1-F5	f9da1039-08ad-4a20-bacc-5b91c5d67730	

```
Node UUID: 8ebb0642-201e-6a5f-dd47-ale38542e672
Node Status: JOINED
```

ENTITY	ADDRESS	PORT	FQDN	UUID	IP
HTTPS	10.160.93.240	443	ychin-nsxmanager-ob-12065118-2-F5	3757f155-8a5d-4b53-828f-d67041d5a210	
CONTROLLER	10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5	7b1c9952-8738-4900-b68b-ca862aa4f6a9	
CLUSTER_BOOT_MANAGER	10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5	b5e12db1-5e0d-4e33-a571-6ba258dceb2e	
DATASTORE	10.160.93.240	9000	ychin-nsxmanager-ob-12065118-2-F5	bee1f629-4e23-4ab8-8083-9e0f0bb83178	
MANAGER	10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5	45ccd6e3-1497-4334-944c-e6bbcd5c723e	
POLICY	10.160.93.240	-	ychin-nsxmanager-ob-12065118-2-F5	d5ba5803-b059-4fbc-897c-3aace8cf1219	

```

10.160.93.240 - ychin-nsxmanager-ob-12065118-2-F5

Node UUID: 2e7e0642-df4a-b2ec-b9e8-633d1469f1ea
Node Status: JOINED

```

ENTITY	ADDRESS	PORT	FQDN	UUID	IP
HTTPS	10.160.76.33	443	ychin-nsxmanager-ob-12065118-3-F5	bce3cc4c-7d60-45e2-aa7b-cdc75e445a14	
CONTROLLER	10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5	ced46f5c-9e52-4b31-a1cb-b3dead991c71	
CLUSTER_BOOT_MANAGER	10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5	88b70d31-3428-4ccc-ab57-55859f45030c	
DATASTORE	10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5	fb4aec3c-cae3-4386-b5b9-c0b99b7d9048	
MANAGER	10.160.76.33	9000	ychin-nsxmanager-ob-12065118-3-F5	82b07440-3ff6-4f67-a1c9-e9327d1686ad	
POLICY	10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5	61f21a78-a56c-4af1-867b-3f24132d53c7	
	10.160.76.33	-	ychin-nsxmanager-ob-12065118-3-F5		

- 4 Pour voir des informations supplémentaires sur l'état, exécutez la commande d'interface de ligne de commande suivante :

```

manager1> get cluster status
Cluster Id: 18807edd-56d1-4107-b7b7-508d766a08e3
Group Type: DATASTORE
Group Status: STABLE

Members:
  UUID                                FQDN
  IP      STATUS
  43cd0642-275c-af1d-fe46-1f5200f9e5f9 ychin-nsxmanager-ob-12065118-1-F5
  10.160.71.225 UP
  8ebb0642-201e-6a5f-dd47-a1e38542e672 ychin-nsxmanager-ob-12065118-2-F5
  10.160.93.240 UP
  2e7e0642-df4a-b2ec-b9e8-633d1469f1ea ychin-nsxmanager-ob-12065118-3-F5
  10.160.76.33 UP

Group Type: CLUSTER_BOOT_MANAGER
Group Status: STABLE

Members:
  UUID                                FQDN
  IP      STATUS
  43cd0642-275c-af1d-fe46-1f5200f9e5f9 ychin-nsxmanager-ob-12065118-1-F5
  10.160.71.225 UP
  8ebb0642-201e-6a5f-dd47-a1e38542e672 ychin-nsxmanager-ob-12065118-2-F5
  10.160.93.240 UP
  2e7e0642-df4a-b2ec-b9e8-633d1469f1ea ychin-nsxmanager-ob-12065118-3-F5
  10.160.76.33 UP

Group Type: CONTROLLER
Group Status: STABLE

Members:
  UUID                                FQDN

```

```

IP                STATUS
7b1c9952-8738-4900-b68b-ca862aa4f6a9    ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240    UP
ced46f5c-9e52-4b31-a1cb-b3dead991c71    ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33    UP
06fd0574-69c0-432e-a8af-53d140dbef8f    ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225    UP

Group Type: MANAGER
Group Status: STABLE

Members:
  UUID                FQDN
IP                STATUS
43cd0642-275c-af1d-fe46-1f5200f9e5f9    ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225    UP
8ebb0642-201e-6a5f-dd47-a1e38542e672    ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240    UP
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea    ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33    UP

Group Type: POLICY
Group Status: STABLE

Members:
  UUID                FQDN
IP                STATUS
43cd0642-275c-af1d-fe46-1f5200f9e5f9    ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225    UP
8ebb0642-201e-6a5f-dd47-a1e38542e672    ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240    UP
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea    ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33    UP

Group Type: HTTPS
Group Status: STABLE

Members:
  UUID                FQDN
IP                STATUS
43cd0642-275c-af1d-fe46-1f5200f9e5f9    ychin-nsxmanager-ob-12065118-1-F5
10.160.71.225    UP
8ebb0642-201e-6a5f-dd47-a1e38542e672    ychin-nsxmanager-ob-12065118-2-F5
10.160.93.240    UP
2e7e0642-df4a-b2ec-b9e8-633d1469f1ea    ychin-nsxmanager-ob-12065118-3-F5
10.160.76.33    UP

```

Arrêter et mettre sous tension le cluster NSX Manager

Si vous devez arrêter le cluster NSX Manager, utilisez la procédure suivante.

Procédure

- 1 Pour arrêter un cluster NSX Manager, arrêtez un nœud de gestionnaire à la fois. Vous pouvez vous connecter à l'interface de ligne de commande (CLI) d'un nœud de gestionnaire en tant que `admin` et exécuter la commande `shutdown`, ou arrêter la machine virtuelle de nœud de gestionnaire à partir de vCenter Server.

Assurez-vous que la machine virtuelle est hors tension dans vCenter Server avant de passer à la suivante.

- 2 Pour mettre sous tension un cluster NSX Manager, mettez sous tension une machine virtuelle de nœud de gestionnaire à la fois dans vCenter Server.

Assurez-vous que le nœud est en cours d'exécution avant de passer au suivant.

Redémarrer NSX Manager

Vous pouvez redémarrer NSX Manager avec une commande d'interface de ligne de commande à des fins de récupération après des erreurs critiques.

Si vous avez besoin de redémarrer plusieurs instances de NSX Manager, vous devez les redémarrer l'une après l'autre. Attendez que l'instance de NSX Manager redémarrée soit en ligne pour en redémarrer une autre.

Procédure

- 1 Connectez-vous à l'interface de ligne de commande de NSX Manager.
- 2 Exécutez la commande suivante.

```
nsx-manager> reboot
Are you sure you want to reboot (yes/no): y
```

Modifier l'adresse IP d'un NSX Manager

Vous pouvez modifier l'adresse IP d'un NSX Manager dans un cluster NSX Manager. Cette section décrit plusieurs approches.

Par exemple, si vous disposez d'un cluster composé de Gestionnaire A, Gestionnaire B et Gestionnaire C, vous pouvez modifier l'adresse IP d'un ou de plusieurs des gestionnaires de l'une des manières suivantes :

- Scénario A :
 - Le Gestionnaire A a l'adresse IP 172.16.1.11.
 - Le Gestionnaire B a l'adresse IP 172.16.1.12.
 - Le Gestionnaire C a l'adresse IP 172.16.1.13.
 - Ajoutez le Gestionnaire D avec une nouvelle adresse IP, par exemple, 192.168.55.11.
 - Supprimez Gestionnaire A.
 - Ajoutez le Gestionnaire E avec une nouvelle adresse IP, par exemple, 192.168.55.12.

- Supprimez le Gestionnaire B.
- Ajoutez le Gestionnaire F avec une nouvelle adresse IP, par exemple, 192.168.55.13.
- Supprimez le Gestionnaire C.
- Scénario B :
 - Le Gestionnaire A a l'adresse IP 172.16.1.11.
 - Le Gestionnaire B a l'adresse IP 172.16.1.12.
 - Le Gestionnaire C a l'adresse IP 172.16.1.13.
 - Ajoutez le Gestionnaire D avec une nouvelle adresse IP, par exemple, 192.168.55.11.
 - Ajoutez le Gestionnaire E avec une nouvelle adresse IP, par exemple, 192.168.55.12.
 - Ajoutez le Gestionnaire F avec une nouvelle adresse IP, par exemple, 192.168.55.13.
 - Supprimez le Gestionnaire A, le Gestionnaire B et le Gestionnaire C.
- Scénario C :
 - Le Gestionnaire A a l'adresse IP 172.16.1.11.
 - Le Gestionnaire B a l'adresse IP 172.16.1.12.
 - Le Gestionnaire C a l'adresse IP 172.16.1.13.
 - Supprimez Gestionnaire A.
 - Ajoutez le Gestionnaire D avec une nouvelle adresse IP, par exemple, 192.168.55.11.
 - Supprimez le Gestionnaire B.
 - Ajoutez le Gestionnaire E avec une nouvelle adresse IP, par exemple, 192.168.55.12.
 - Supprimez le Gestionnaire C.
 - Ajoutez le Gestionnaire F avec une nouvelle adresse IP, par exemple, 192.168.55.13.

Les deux premiers scénarios nécessitent une RAM virtuelle, un CPU et un disque supplémentaires pour les NSX Manager supplémentaires lors de ce changement d'adresse IP.

Le scénario C n'est pas recommandé, car il réduit temporairement le nombre de NSX Manager et une perte de l'un des deux gestionnaires actifs pendant le changement d'adresse IP aura un impact sur les opérations de NSX-T. Ce scénario concerne une situation dans laquelle la RAM virtuelle, le CPU et le disque supplémentaires ne sont pas disponibles et un changement d'adresse IP est requis.

Note Si vous utilisez la fonctionnalité d'adresse IP virtuelle du cluster, vous devez utiliser le même sous-réseau pour les nouvelles adresses IP ou désactiver l'adresse IP virtuelle du cluster pendant les changements d'adresse IP, car l'adresse IP virtuelle du cluster requiert que tous les NSX Manager soient dans le même sous-réseau.

Conditions préalables

Familiarisez-vous avec le déploiement d'un NSX Manager dans un cluster. Pour plus d'informations, consultez le *Guide d'installation de NSX-T Data Center*.

Procédure

- 1 Si le NSX Manager que vous voulez supprimer a été déployé manuellement, procédez comme suit.
 - a Exécutez la commande d'interface de ligne de commande suivante pour détacher NSX Manager du cluster.


```
detach node <node-id>
```
 - b Supprimez la machine virtuelle NSX Manager.
- 2 Si NSX Manager que vous souhaitez supprimer a été déployé automatiquement via l'interface utilisateur de NSX Manager, procédez comme suit.
 - a Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://nsx-manager-ip-address`.
Ce NSX Manager ne doit pas être celui que vous souhaitez supprimer.
 - b Dans l'onglet **Systèmes**, cliquez sur **Nœuds de gestion NSX**.
L'état du cluster NSX Manager s'affiche.
 - c Pour NSX Manager que vous souhaitez supprimer, cliquez sur l'icône d'engrenage et sélectionnez **Supprimer**.
- 3 Déployez une nouvelle instance de NSX Manager.

Redimensionner un nœud NSX Manager

Vous pouvez modifier le nombre de cœurs de CPU ou de blocs de mémoire d'un nœud NSX Manager à tout moment.

Notez que dans des conditions normales de fonctionnement, les trois nœuds de gestionnaire doivent avoir le même nombre de cœurs de CPU et de blocs de mémoire. Une non-concordance de CPU ou de mémoire entre les instances de NSX Manager dans un cluster de gestion NSX ne doit être effectuée que lors du passage d'une taille de NSX Manager à une autre taille de NSX Manager.

Si vous avez configuré la réservation d'allocation de ressources pour les machines virtuelles NSX Manager dans vCenter Server, vous devrez peut-être ajuster la réservation. Pour plus d'informations, voir la documentation de vSphere.

Conditions préalables

- Vérifiez que la nouvelle taille répond à la configuration système requise d'un nœud de gestionnaire. Pour plus d'informations, reportez-vous à la section « Configuration système requise des machines virtuelles NSX Manager » du *Guide d'installation de NSX-T Data Center*.

- Familiarisez-vous avec le déploiement d'un NSX Manager dans un cluster. Pour plus d'informations, consultez le *Guide d'installation de NSX-T Data Center*.
- Pour plus d'informations sur la suppression d'un nœud de gestionnaire d'un cluster, reportez-vous à la section [Modifier l'adresse IP d'un NSX Manager](#).

Procédure

- 1 Déployez un nouveau nœud de gestionnaire avec la nouvelle taille.
- 2 Ajoutez le nouveau nœud de gestionnaire au cluster.
- 3 Supprimez un ancien nœud de gestionnaire.
- 4 Répétez les étapes 1 à 3 pour remplacer les deux anciens nœuds de gestionnaire.

Ajout et suppression d'un nœud de transport d'hôte ESXi vers et depuis des serveurs vCenter

Vous pouvez déplacer un nœud de transport d'hôte ESXi d'un vCenter Server (VC) vers un autre, et également d'un cluster NSX Manager vers un autre.

Scénario 1 : VC1 connecté au cluster 1 de NSX Manager et VC2 connecté au cluster 2 de NSX Manager

En supposant qu'ESX1, un nœud de transport hôte d'ESXi, se trouve dans VC1, vous pouvez le déplacer vers VC2 en procédant comme suit :

- 1 Désinstallez NSX d'ESX1.
- 2 Déplacez ESX1 vers VC2.
- 3 Appliquez un profil de nœud de transport à ESX1.

Scénario 2 : VC1 et VC2 sont connectés au cluster de NSX Manager

En supposant qu'ESX1, un nœud de transport hôte d'ESXi, se trouve dans VC1, vous pouvez le déplacer vers VC2 en procédant comme suit :

- 1 Désinstallez NSX d'ESX1.
- 2 Déplacez ESX1 vers VC2.
- 3 Appliquez un profil de nœud de transport à ESX1.

Scénario 3 : VC1 connecté au cluster 1 de NSX Manager

En supposant qu'ESX1, un nœud de transport hôte d'ESXi, se trouve dans VC1, vous pouvez le déplacer vers le cluster 2 de NSX Manager en tant qu'hôte autonome en procédant comme suit :

- 1 Désinstallez NSX d'ESX1.
- 2 Ajoutez ESX1 au cluster 2 de NSX Manager.

Remplacement d'un nœud de transport NSX Edge dans un cluster NSX Edge

Vous pouvez remplacer un nœud de transport NSX Edge dans un cluster NSX Edge à l'aide de l'interface utilisateur ou de l'API de NSX Manager.

Remplacer un nœud de transport NSX Edge à l'aide de l'interface utilisateur de NSX Manager

La procédure suivante décrit le remplacement d'un nœud de transport NSX Edge dans un cluster NSX Edge à l'aide de l'interface utilisateur de NSX Manager. Vous pouvez remplacer le nœud de transport Edge, qu'il soit en cours d'exécution ou non.

Si le nœud Edge à remplacer n'est pas en cours d'exécution, le nouveau nœud Edge peut avoir la même adresse IP de gestion et adresse IP de TEP. Si le nœud Edge à remplacer est en cours d'exécution, le nouveau nœud Edge doit avoir une adresse IP de gestion et une adresse IP de TEP différentes.

Conditions préalables

Familiarisez-vous avec la procédure d'installation d'un nœud NSX Edge, joignez le nœud Edge au plan de gestion et créez un nœud de transport NSX Edge. Pour plus d'informations, consultez le *Guide d'installation de NSX-T Data Center*.

Procédure

- 1 Si vous souhaitez que le nouveau nœud de transport Edge ait les mêmes configurations que le nœud de transport Edge à remplacer, effectuez l'appel d'API suivant pour rechercher les configurations :

```
GET https://<nsx-manager-IP>/api/v1/transport-nodes/<tn-id>
```

- 2 Suivez les procédures du *Guide d'installation de NSX-T Data Center* pour installer et configurer un nœud de transport Edge.

Si vous souhaitez que ce nœud de transport Edge ait les mêmes configurations que le nœud de transport Edge à remplacer, utilisez les configurations obtenues à l'étape 1.

- 3 Dans NSX Manager, sélectionnez **Système > Infrastructure > Nœuds > Clusters Edge**.
- 4 Sélectionnez un cluster Edge en cochant la case dans la première colonne.
- 5 Cliquez sur **Actions > Remplacer le membre du cluster Edge**.

Il est recommandé de placer le nœud de transport en cours de remplacement en mode de maintenance. Si le nœud de transport n'est pas en cours d'exécution, vous pouvez ignorer cette recommandation en toute sécurité.

- 6 Sélectionnez le nœud à remplacer dans la liste déroulante.
- 7 Sélectionnez le nœud de remplacement dans la liste déroulante.
- 8 Cliquez sur **Enregistrer**.

Remplacer un nœud de transport NSX Edge à l'aide de l'API

La procédure suivante décrit le remplacement d'un nœud de transport NSX Edge dans un cluster NSX Edge à l'aide de l'API NSX-T. Vous pouvez remplacer le nœud de transport Edge, qu'il soit en cours d'exécution ou non.

Si le nœud Edge à remplacer n'est pas en cours d'exécution, le nouveau nœud Edge peut avoir la même adresse IP de gestion et adresse IP de TEP. Si le nœud Edge à remplacer est en cours d'exécution, le nouveau nœud Edge doit avoir une adresse IP de gestion et une adresse IP de TEP différentes.

Conditions préalables

Familiarisez-vous avec la procédure d'installation d'un nœud NSX Edge, joignez le nœud Edge au plan de gestion et créez un nœud de transport NSX Edge. Pour plus d'informations, consultez le *Guide d'installation de NSX-T Data Center*.

Procédure

- 1 Si vous souhaitez que le nouveau nœud de transport Edge ait les mêmes configurations que le nœud de transport Edge à remplacer, effectuez l'appel d'API suivant pour rechercher les configurations :

```
GET https://<nsx-manager-IP>/api/v1/transport-nodes/<tn-id>
```

- 2 Suivez les procédures du Guide d'installation de NSX-T Data Center pour installer et configurer un nœud de transport Edge.

Si vous souhaitez que ce nœud de transport Edge ait les mêmes configurations que le nœud de transport Edge à remplacer, utilisez les configurations obtenues à l'étape 1.

- 3 Effectuez un appel d'API pour obtenir l'ID du nouveau nœud de transport et le nœud de transport à remplacer. Le champ `id` contient l'ID du nœud de transport. Par exemple,

```
GET https://<nsx-manager-IP>/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",
```

- Effectuez un appel d'API pour obtenir 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`. Par exemple,

```
GET https://<nsx-manager-IP>/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"
    }
  ],
}
```

- Effectuez un appel d'API pour remplacer un nœud de transport dans un cluster NSX Edge. `member_index` doit correspondre à l'index du nœud de transport à remplacer.

Par 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 `Edge-Cluster-1` de NSX Edge (`9a302df7-0833-4237-af1f-4d826c25ad78`).

```
POST http://<nsx-manager-IP>/api/v1/edge-clusters/9a302df7-0833-4237-af1f-4d826c25ad78?
action=replace_transport_node
{
  "member_index": 0,
  "transport_node_id" : "890f0e3c-aa81-46aa-843b-8ac25fe30bd3"
}
```

Récupération de NSX-T lorsque vCenter Server est perdu et ne peut pas être récupéré

Si vous perdez vCenter Server (VC) et qu'il ne peut pas être récupéré (peut-être parce qu'il n'y a pas de sauvegarde ou si la sauvegarde est endommagée), utilisez la procédure suivante pour récupérer l'environnement NSX-T après le redéploiement de VC.

Le nouveau VC doit avoir le même nom de domaine complet et la même adresse IP que le VC d'origine. En outre, il doit avoir les mêmes clusters contenant les mêmes hôtes. Soyez prudent avec les hôtes qui ont des machines virtuelles sous tension lorsque vous les ajoutez à VC. Assurez-vous qu'ils sont ajoutés aux clusters corrects et non au centre de données VC.

Gestionnaire de calcul

Dans NSX Manager, supprimez l'ancien gestionnaire de calcul. Ajoutez ensuite le nouveau VC en tant que gestionnaire de calcul.

Nœuds de transport d'hôte

Dans NSX Manager, les hôtes s'affichent dans les clusters VC appropriés. Aucune action n'est nécessaire.

Nœuds Edge

Vous devez remplacer les nœuds Edge qui ont été déployés à partir de l'interface utilisateur de NSX Manager.

- 1 Pour remplacer un nœud Edge, suivez la procédure décrite dans [Remplacer un nœud de transport NSX Edge à l'aide de l'interface utilisateur de NSX Manager](#).
- 2 Vérifiez que les passerelles (ou les routeurs logiques) et les tunnels sont configurés sur la nouvelle VM Edge.
- 3 Supprimez l'ancien nœud Edge en accédant à **Système > Infrastructure > Nœuds de transport Edge**. Sélectionnez le nœud Edge et cliquez sur **Actions > Supprimer**. Les erreurs telles que « Échec de la mise hors tension » peuvent être ignorées.
- 4 Dans VC, mettez l'ancienne VM Edge hors tension et supprimez-la.
- 5 Répétez les étapes ci-dessus pour chacun des nœuds Edge.

NSX Manager

Vous devez remplacer les instances de NSX Manager qui ont été déployées depuis l'interface utilisateur de NSX Manager. En général, les deuxième et troisième instances de NSX Manager sont déployées de cette manière.

- 1 Connectez-vous à l'interface utilisateur de la première instance de NSX Manager.
- 2 Accédez à **Système > Dispositifs** et sélectionnez la troisième instance de NSX Manager. Cliquez sur **Actions > Supprimer**. Cela échouera, car la machine virtuelle du gestionnaire ne peut pas être mise hors tension. L'option Forcer la suppression est désormais disponible. Sélectionnez **Actions > Forcer la suppression**.
- 3 Si la suppression forcée ne fonctionne pas, procédez comme suit :
 - a Connectez-vous à la CLI de la première instance de NSX Manager.
 - b Exécutez la commande `get cluster status` afin d'obtenir l'UID de la troisième instance de NSX Manager.
 - c Exécutez la commande `detach node <node-uid>` pour détacher la troisième instance de NSX Manager du cluster.

- d Effectuez l'appel d'API suivant pour forcer la suppression de la troisième instance de NSX Manager :

```
POST : https://<nsx-manager-1>/api/v1/cluster/nodes/deployments/<node-uid>?
action=delete&force_delete=true
```

- 4 Dans VC, mettez hors tension et supprimez la troisième instance de NSX Manager.
- 5 Déployez une nouvelle instance de NSX Manager avec la même configuration que la troisième instance de NSX Manager.
- 6 Répétez les étapes ci-dessus pour supprimer la deuxième instance de NSX Manager.
- 7 Déployez deux nouvelles instances de NSX Manager.

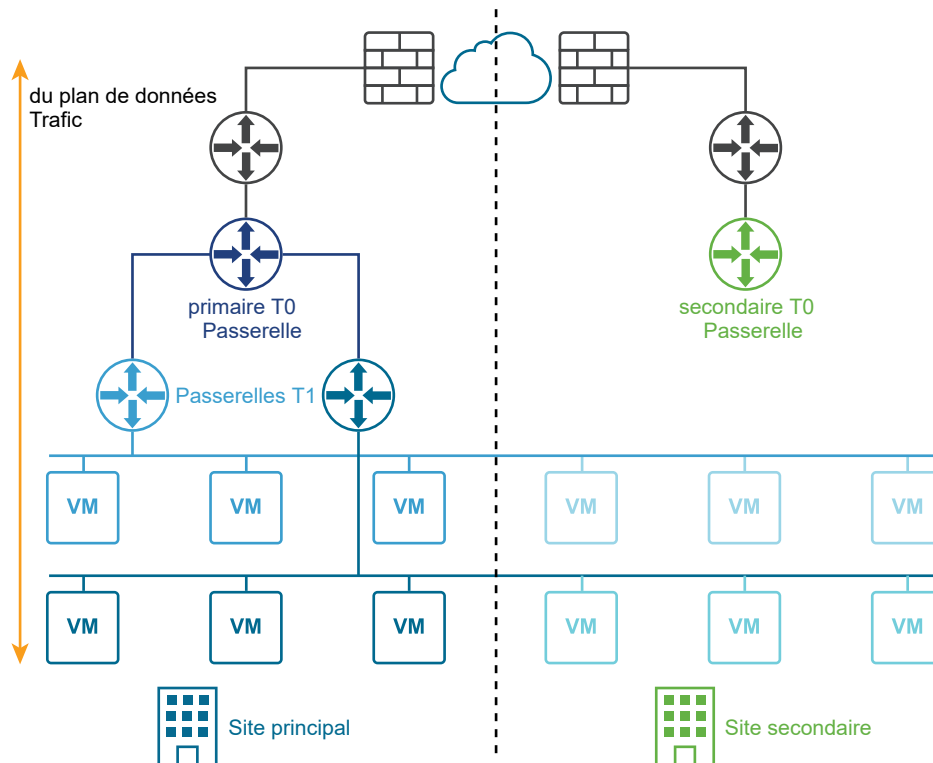
Déploiement multisite de NSX-T Data Center

NSX-T Data Center prend en charge les déploiements multisites dans lesquels vous pouvez gérer tous les sites d'un cluster NSX Manager.

Deux types de déploiements multisites sont pris en charge :

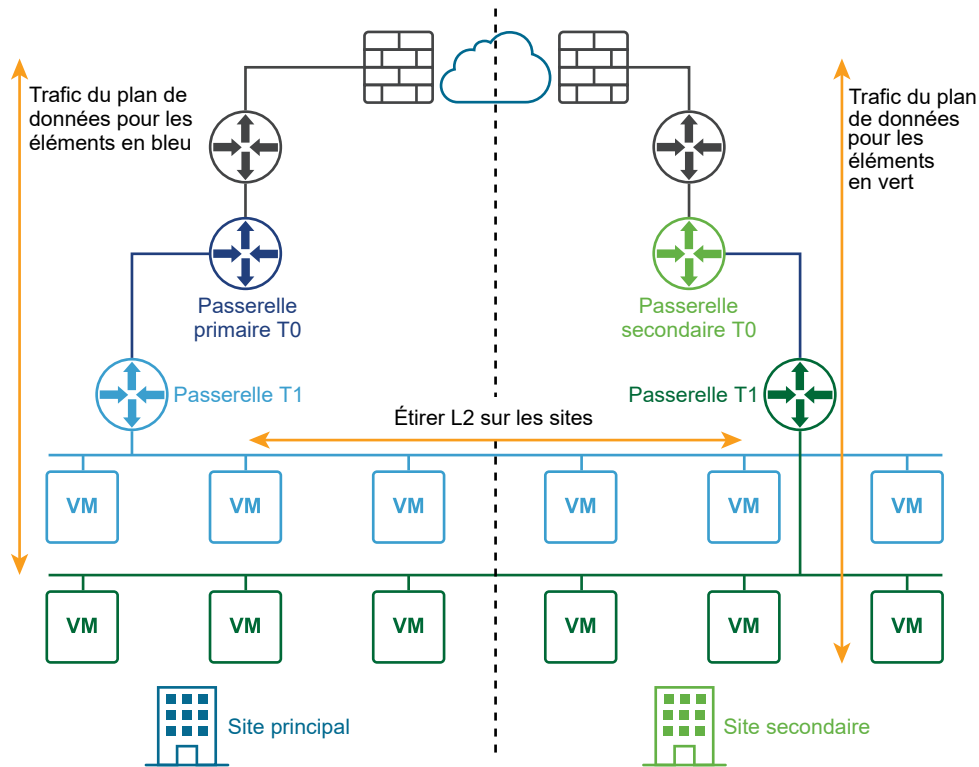
- Récupération d'urgence
- Actif-Actif

Le schéma suivant illustre un déploiement de récupération d'urgence.



Dans un déploiement actif-actif, tous les sites sont actifs et le trafic de couche 2 dépasse les limites du site. Dans un déploiement de récupération d'urgence, NSX-T Data Center sur le site principal gère la mise en réseau de l'entreprise. Le site secondaire est prêt à prendre le relais en cas de défaillance irrémédiable sur le site principal.

Le schéma suivant illustre un déploiement actif-actif.



Vous pouvez déployer deux sites pour une récupération automatique ou manuelle/basée sur un script du plan de gestion et du plan de données.

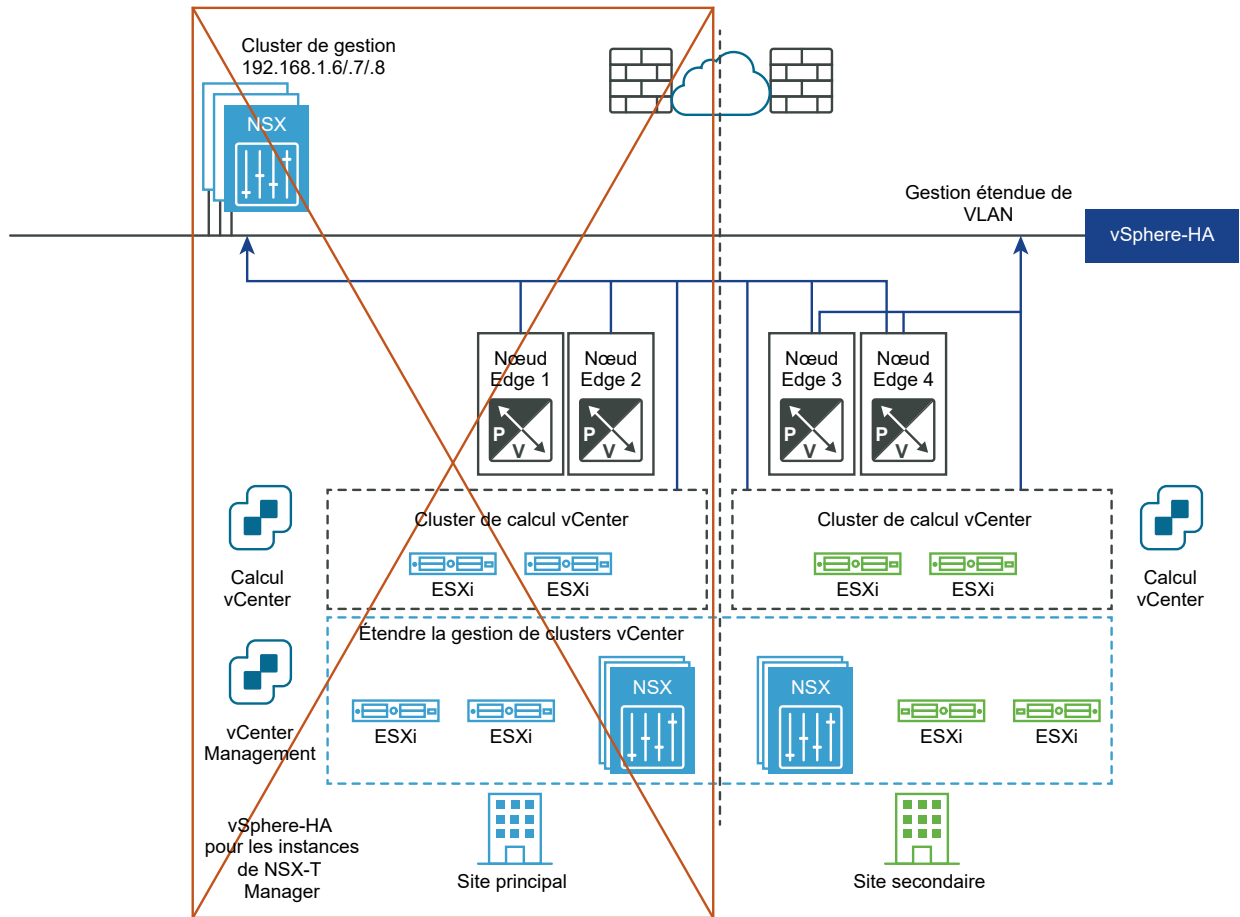
Récupération automatique du plan de gestion

Configuration requise :

- Un cluster vCenter étendu avec HA sur les sites configurés.
- Un VLAN de gestion étendu.

Le cluster NSX Manager est déployé sur le VLAN de gestion et se trouve physiquement dans le site principal. En cas de panne d'un site principal, vSphere HA redémarrera les instances de NSX Manager sur le site secondaire. Tous les nœuds de transport se reconnectent automatiquement aux instances de NSX Manager redémarrées. Ce processus dure environ 10 minutes. Pendant ce temps, le plan de gestion n'est pas disponible, mais le plan de données n'est pas affecté.

Le schéma suivant illustre la récupération automatique du plan de gestion.



Récupération automatique du plan de données

Configuration requise :

- La latence maximale entre les nœuds Edge est de 10 ms.
- Le mode HA pour la passerelle de niveau 0 doit être actif-veille et le mode de basculement doit être préemptif.

Remarque : le mode de basculement de la passerelle de niveau 1 peut être préemptif ou non.

Étapes de configuration :

- À l'aide de l'API, créez des domaines de panne pour les deux sites, par exemple `FD1A-Preferred_Site1` et `FD2A-Preferred_Site1`. Définissez le paramètre `preferred_active_edge_services` sur `true` pour le site principal et définissez-le sur `false` pour le site secondaire.

```
POST /api/v1/failure-domains
{
  "display_name": "FD1A-Preferred_Site1",
  "preferred_active_edge_services": "true"
}
```

```
POST /api/v1/failure-domains
{
  "display_name": "FD2A-Preferred_Site1",
  "preferred_active_edge_services": "false"
}
```

- À l'aide de l'API, configurez un cluster Edge étendu sur les deux sites. Par exemple, le cluster dispose de nœuds Edge EdgeNode1A et EdgeNode1B dans le site principal, et des nœuds Edge EdgeNode2A et EdgeNode2B dans le site secondaire. Les passerelles de niveau 0 et de niveau 1 actives s'exécuteront sur EdgeNode1A et EdgeNode1B. Les passerelles de niveau 0 et de niveau 1 en veille s'exécuteront sur EdgeNode2A et EdgeNode2B.
- À l'aide de l'API, associez chaque nœud Edge au domaine de pannes du site. Appelez d'abord l'API GET /api/v1/transport-nodes/<transport-node-id> pour obtenir les données sur le nœud Edge. Utilisez le résultat de l'API GET comme entrée pour l'API PUT /api/v1/transport-nodes/<transport-node-id>, avec la propriété supplémentaire, failure_domain_id, définie de manière appropriée. Par exemple,

```
GET /api/v1/transport-nodes/<transport-node-id>
Response:
{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  ...
}

PUT /api/v1/transport-nodes/<transport-node-id>
{
  "resource_type": "TransportNode",
  "description": "Updated NSX configured Test Transport Node",
  "id": "77816de2-39c3-436c-b891-54d31f580961",
  ...
  "failure_domain_id": "<UUID>",
}
```

- À l'aide de l'API, configurez le cluster Edge pour allouer des nœuds en fonction du domaine de pannes. Appelez d'abord l'API GET /api/v1/edge-clusters/<edge-cluster-id> pour obtenir les données sur le cluster Edge. Utilisez le résultat de l'API GET comme entrée pour l'API PUT /api/v1/edge-clusters/<edge-cluster-id>, avec la propriété supplémentaire, allocation_rules, définie de manière appropriée. Par exemple,

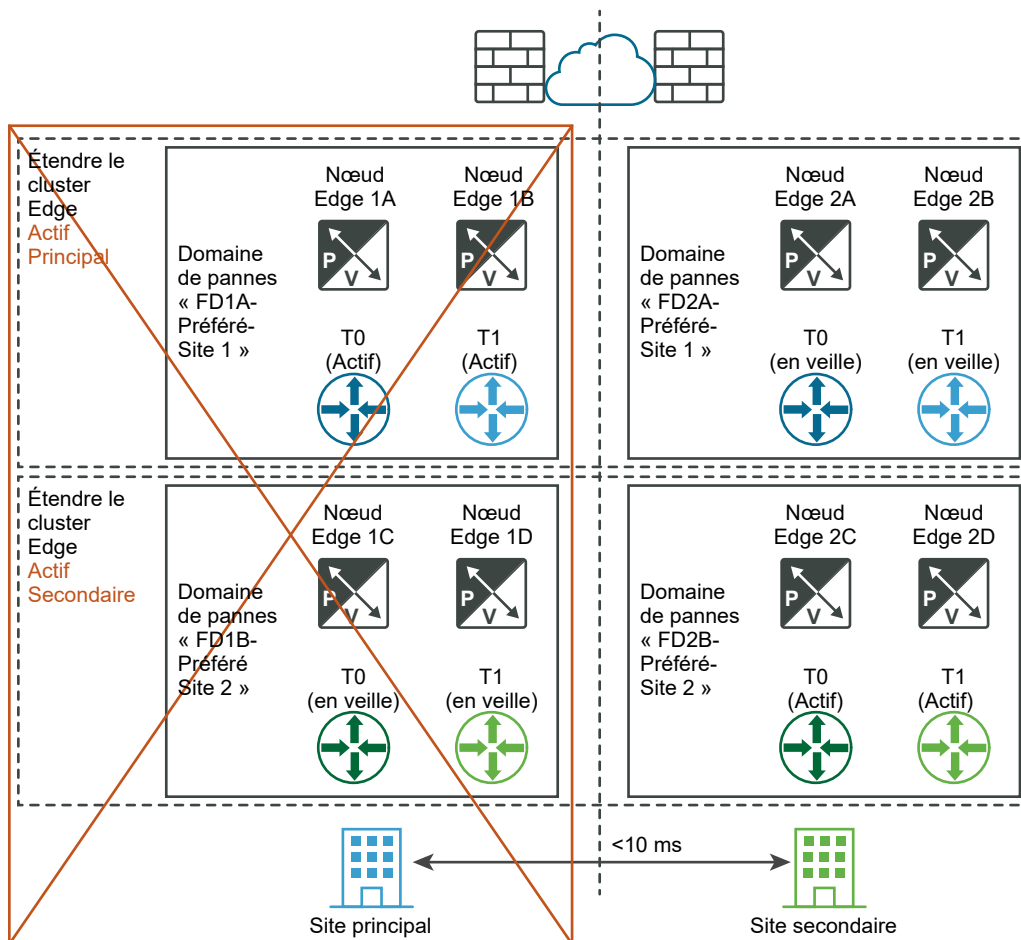
```
GET /api/v1/edge-clusters/<edge-cluster-id>
Response:
{
  "_revision": 0,
  "id": "bf8d4daf-93f6-4c23-af38-63f6d372e14e",
  "resource_type": "EdgeCluster",
  ...
}
```

```
PUT /api/v1/edge-clusters/<edge-cluster-id>
{
  "_revision": 0,
  "id": "bf8d4daf-93f6-4c23-af38-63f6d372e14e",
  "resource_type": "EdgeCluster",
  ...
  "allocation_rules": [
    {
      "action": {
        "enabled": true,
        "action_type": "AllocationBasedOnFailureDomain"
      }
    }
  ],
}
```

- Créez des passerelles de niveau 0 et de niveau 1 à l'aide de l'API ou de l'interface utilisateur NSX Manager.

Lorsqu'un nœud Edge du site principal tombe en panne, les passerelles de niveau 0 et de niveau 1 hébergées sur ce nœud seront migrées vers un nœud Edge dans le site secondaire.

Le schéma suivant illustre la récupération automatique du plan de données.



Récupération manuelle/basée sur un script du plan de gestion

Configuration requise :

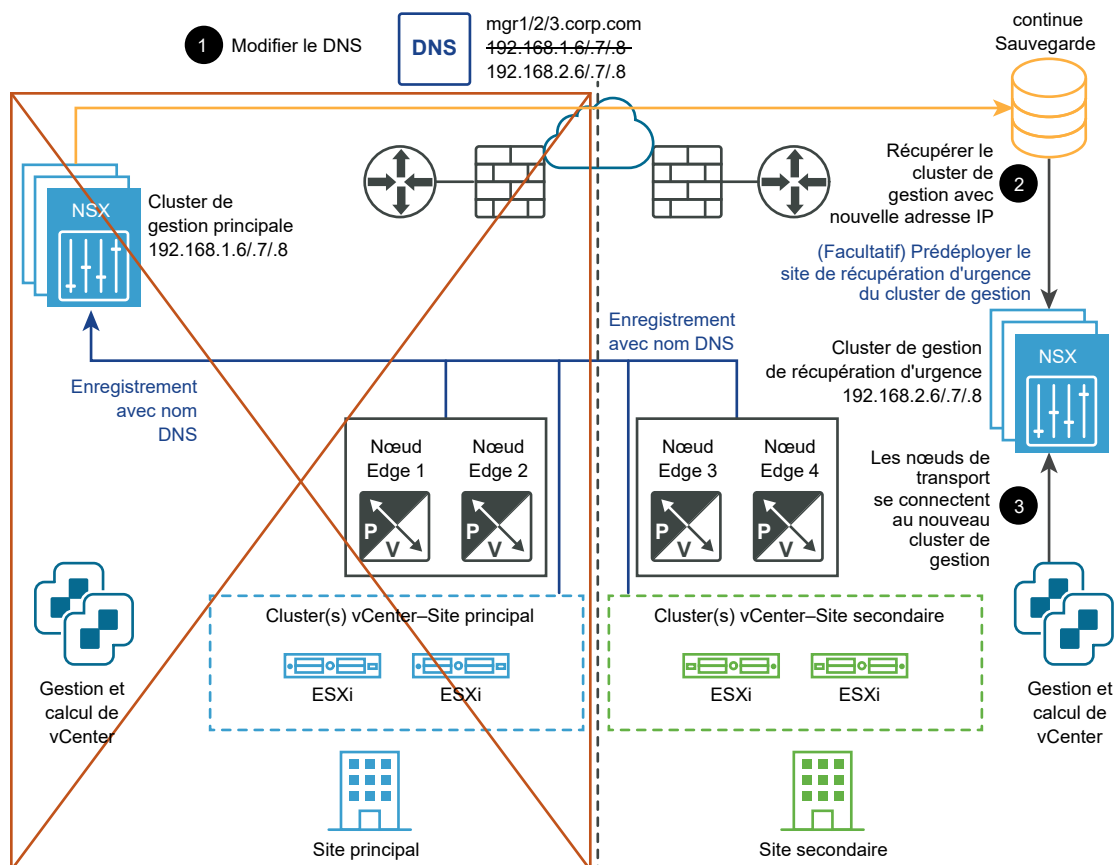
- DNS pour les instances de NSX Manager avec une durée de vie courte (par exemple, 5 minutes).
- Sauvegarde continue

Ni vSphere HA ni un VLAN de gestion étiré n'est requis. Les gestionnaires NSX-T doivent être associés à un nom DNS avec une durée de vie courte. Tous les nœuds de transport (nœuds Edge et hyperviseurs) doivent se connecter au NSX Manager à l'aide de leur nom DNS. Pour gagner du temps, vous pouvez éventuellement pré-installer un cluster NSX Manager sur le site secondaire.

Les étapes de la récupération d'urgence sont les suivantes :

- 1 Modifiez l'enregistrement DNS pour que le cluster NSX Manager possède différentes adresses IP.
- 2 Restaurez le cluster NSX Manager depuis une sauvegarde.
- 3 Connectez les nœuds de transport vers le nouveau cluster NSX Manager.

Le schéma suivant illustre la récupération manuelle/basée sur un script du plan de gestion.



Récupération manuelle/basée sur un script du plan de données

Configuration requise :

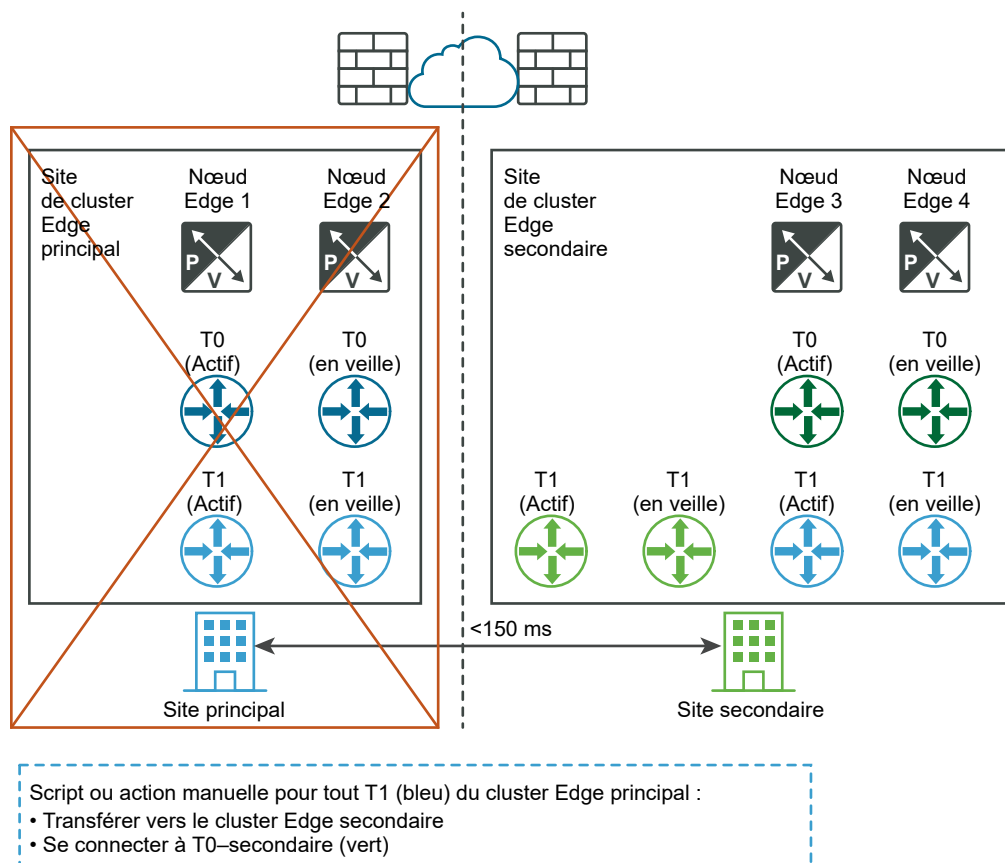
- La latence maximale entre les nœuds Edge est de 150 ms.

Les nœuds Edge peuvent être des machines virtuelles ou Bare Metal. La passerelle de niveau 0 peut être active-en veille ou active-active. Les machines virtuelles de nœuds Edge peuvent être installées sur des serveurs vCenter différents. Aucun vSphere HA n'est requis.

Les étapes de la récupération d'urgence sont les suivantes :

- 1 Créez une passerelle de niveau 0 en veille sur un cluster Edge existant dans le site de récupération d'urgence.
- 2 À l'aide de l'API, déplacez les passerelles de niveau 1 qui sont connectées à une passerelle de niveau 0 vers la passerelle de niveau 0 sur le site de récupération d'urgence.
- 3 À l'aide de l'API, déplacez les passerelles de niveau 1 autonomes vers le site de récupération d'urgence.
- 4 À l'aide de l'API, déplacez les ponts de couche 2 vers le site de récupération d'urgence.

Le schéma suivant illustre la récupération manuelle/basée sur un script du plan de données.



Configuration requise pour les déploiements multisites

Communication entre les sites

- La bande passante doit être supérieure ou égale à 1 Go/s et la latence (RTT) doit être inférieure à 150 ms.
- Le MTU doit être supérieur ou égal à 1 600. Un MTU de 9 000 est recommandé.

Configuration de NSX Manager

- La sauvegarde automatique doit être activée lors de modifications de la configuration de NSX-T Data Center.
- NSX Manager doit être configuré pour utiliser le nom de domaine complet.

Récupération du plan de données

- Le même fournisseur internet doit être utilisé si les adresses IP publiques sont exposées via des services tels que NAT ou l'équilibrage de charge.
- Le mode HA pour la passerelle de niveau 0 doit être actif-veille et le mode de basculement doit être préemptif.

Système de gestion de cloud

- Le système de gestion de cloud (CMS) doit prendre en charge un plug-in NSX-T Data Center. Dans cette version, VMware Integrated OpenStack (VIO) et vRealize Automation (vRA) répondent à cette exigence.

Limitations

- Aucune capacité de sortie locale. Tout le trafic nord-sud doit se produire au sein d'un site.
- Le logiciel de récupération d'urgence de calcul doit prendre en charge NSX-T Data Center, par exemple, VMware SRM 8.1.2 ou version ultérieure.

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 21-7. Commandes de configuration système et demandes API.

Tâche	Ligne de commande (NSX Manager et NSX Edge)	Demande API (NSX Manager uniquement)
Définir le fuseau horaire du système	<code>set timezone <timezone></code>	PUT <a href="https://<nsx-mgr>/api/v1/node">https://<nsx-mgr>/api/v1/node
Définir le serveur NTP	<code>set ntp-server <ntp-server></code>	PUT <a href="https://<nsx-mgr>/api/v1/node/services/ntp">https://<nsx-mgr>/api/v1/node/services/ntp
Définir le serveur DNS	<code>set name-servers <dns-server></code>	PUT <a href="https://<nsx-mgr>/api/v1/node/network/name-servers">https://<nsx-mgr>/api/v1/node/network/name-servers
Définir le domaine de recherche DNS	<code>set search-domains <domain></code>	PUT <a href="https://<nsx-mgr>/api/v1/node/network/search-domains">https://<nsx-mgr>/api/v1/node/network/search-domains

Ajouter une clé de licence et générer un rapport d'utilisation de licence

Vous pouvez ajouter des clés de licence et générer un rapport d'utilisation de licence. Le rapport d'utilisation est un fichier au format CSV.

Les types de licence NSX-T Data Center de non-évaluation suivantes sont disponibles :

- NSX Data Center Standard
- NSX Data Center Professional
- NSX Data Center Advanced
- NSX Data Center Enterprise Plus
- NSX Data Center Remote Office Branch Office (ROBO)
- NSX Advanced (disponible à partir de NSX-T Data Center 2.5.1)
- NSX Enterprise (disponible à partir de NSX-T Data Center 2.5.1)

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 attribuer une nouvelle licence d'évaluation lorsque la licence d'évaluation par défaut est présente. La nouvelle licence d'évaluation remplacera la licence d'évaluation par défaut. Vous pouvez également annuler l'attribution de la licence d'évaluation non définie par défaut. Dans ce cas, la licence d'évaluation par défaut sera restaurée.

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.

Si votre licence expire dans 60 jours ou si elle a expiré, une fois que vous êtes connecté à NSX Manager, une fenêtre de notification s'affiche pour vous informer de la situation. Vous pouvez également cliquer sur l'icône de notification dans le coin supérieur droit de la fenêtre pour afficher la notification.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Système > Licences > Ajouter**.
- 3 Entrez une clé de licence.
- 4 Pour générer un rapport d'utilisation de licence, sélectionnez **Exporter > Rapport d'utilisation de licence**.

Le rapport CSV répertorie les chiffres d'utilisation de machine virtuelle, de CPU, d'utilisateur simultané unique, de vCPU et de cœur pour les fonctionnalités suivantes :

- Commutation et routage
- Équilibrage de charge de NSX Edge
- VPN
- DFW
- Micro-segmentation sensible au contexte - Identification d'application
- Micro-segmentation sensible au contexte - Pare-feu d'identité pour l'hôte de session Bureau à distance
- Insertion de services
- Pare-feu d'identité
- Guest Introspection optimisé

Note Les fonctionnalités suivantes sont désactivées pour la version Limited Export Release :

- VPN IPSec
 - Équilibrage de charge basé sur HTTPS
-

Configuration de certificats

Vous pouvez importer des certificats, créer une demande de signature de certificat (CSR), générer des certificats auto-signés et importer une liste de révocation des certificats (CRL).

Après l'installation de NSX-T Data Center, les nœuds de gestionnaire et le cluster ont des certificats auto-signés. Pour améliorer la sécurité, il est vivement recommandé de remplacer les certificats auto-signés par des certificats signés par une autorité de certification.

Importer un certificat

Vous pouvez importer un certificat avec une clé privée pour remplacer le certificat auto-signé par défaut après l'activation.

Notez que seuls les certificats basés sur RSA sont pris en charge.

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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Système > Certificats**.
- 3 Sélectionnez **Importer > Importer un certificat** et entrez les détails du certificat.

Option	Description
Nom	Attribuez un nom au certificat.
Contenu du certificat	Accédez au fichier du certificat sur votre ordinateur et ajoutez le fichier. Le certificat ne doit pas être chiffré. S'il s'agit d'un certificat signé par une autorité de certification, veillez à inclure toute la chaîne dans l'ordre suivant : certificat - intermédiaire - racine.
Clé privée	Accédez au fichier de clé privée sur votre ordinateur et ajoutez le fichier.
Phrase secrète	Ajoutez une phrase secrète pour ce certificat s'il est chiffré. Dans cette version, ce champ n'est pas utilisé, car le certificat chiffré n'est pas pris en charge.
Description	Entrez la description de ce qui est inclus dans ce certificat.
Certificat de service	Définissez la valeur sur Oui pour utiliser ce certificat pour des services, tels qu'un équilibreur de charge et VPN. Définissez la valeur sur Non si ce certificat est destiné aux nœuds NSX Manager.

- 4 Cliquez sur **Importer**.

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/la région. 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/la région.
- 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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Système > Certificats**.
- 3 Cliquez sur l'onglet **CSR**.
- 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/Région	Ajoutez le pays/la région 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.

Option	Description
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 **Générer**.

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. Après l'importation et l'activation, les autres certificats signés par cette autorité de certification seront approuvés par NSX-T Data Center.

Notez que seuls les certificats basés sur RSA sont pris en charge.

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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Système > Certificats**.

- 3 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.
Certificat de service	Définissez la valeur sur Oui pour utiliser ce certificat pour des services, tels qu'un équilibreur de charge et VPN. Définissez la valeur sur Non si ce certificat est destiné aux nœuds NSX Manager.

- 4 Cliquez sur **Importer**.

Créer un certificat auto-signé

Vous pouvez créer un certificat auto-signé. Toutefois, l'utilisation d'un certificat auto-signé est moins sûre que l'utilisation d'un certificat approuvé.

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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Système > Certificats**.
- 3 Cliquez sur l'onglet **CSR**.
- 4 Sélectionnez une demande de signature de certificat.
- 5 Sélectionnez **Actions > Certificat auto-signé pour la demande de signature de certificat**.
- 6 Entrez le nombre de jours pendant lequel le certificat auto-signé est valide.
La valeur par défaut est de 10 ans.
- 7 Cliquez sur **Ajouter**.

Résultats

Le certificat auto-signé s'affiche dans l'onglet **Certificats**.

Remplacer le certificat d'un nœud NSX Manager ou l'adresse IP virtuelle d'un cluster NSX Manager

Vous pouvez remplacer le certificat d'un nœud de gestionnaire ou l'adresse IP virtuelle (VIP) d'un cluster de gestionnaires en effectuant un appel d'API.

Après l'installation de NSX-T Data Center, les nœuds de gestionnaire et le cluster ont des certificats auto-signés. Pour améliorer la sécurité, il est vivement recommandé de remplacer les certificats auto-signés par des certificats signés par une autorité de certification et d'utiliser un autre certificat pour chaque nœud.

Conditions préalables

Vérifiez qu'un certificat est disponible dans le dispositif NSX Manager. Reportez-vous à la section [Importer un certificat](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur `https://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Système > Certificats**.
- 3 Dans la colonne ID, cliquez sur l'ID du certificat que vous voulez utiliser et copiez l'ID de certificat dans la fenêtre contextuelle.

Assurez-vous que lorsque ce certificat a été importé, l'option **Certificat de service** a été définie sur **Non**.

- 4 Pour remplacer le certificat d'un nœud de gestionnaire, utilisez l'appel d'API `POST /api/v1/node/services/http?action=apply_certificate`. Par exemple,

```
POST https://<nsx-mgr>/api/v1/node/services/http?
action=apply_certificate&certificate_id=e61c7537-3090-4149-b2b6-19915c20504f
```

Remarque : la chaîne de certificats doit être dans l'ordre standard suivant : « certificat-intermédiaire-racine ».

Pour plus d'informations sur l'API, reportez-vous à la *Référence de l'API de NSX-T Data Center*.

- 5 Pour remplacer le certificat de la VIP d'un cluster de gestionnaires, utilisez l'appel d'API `POST /api/v1/cluster/api-certificate?action=set_cluster_certificate`. Par exemple,

```
POST https://<nsx-mgr>/api/v1/cluster/api-certificate?
action=set_cluster_certificate&certificate_id=d60c6a07-6e59-4873-8edb-339bf75711ac
```

Remarque : la chaîne de certificats doit être dans l'ordre standard suivant : « certificat–intermédiaire–racine ».

Pour plus d'informations sur l'API, reportez-vous à la *Référence de l'API de NSX-T Data Center*. Cette étape n'est pas nécessaire si vous n'avez pas configuré de VIP.

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://<nsx-manager-ip-address>>.
- 2 Sélectionnez **Système > Certificats**.
- 3 Cliquez sur l'onglet **CRL**.

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> -----BEGIN X509 CRL----- MIIBODCB4zANBgkqhkiG9w0BAQQFADBGMQswCQYDVQQGEwJBVTEMMaoGA1 UECBMD UUxEMRkwFwYDVQQKEwBNaw5jb20gUHR5LiBMdGQuMQswCQYDVQQLEwJDUz EbMBkG A1UEAxMSU1NMZW51IGRlbW8gc2VydMVFw0wMTAxMTUxNjI2NTdaFw0wMT AyMTQx NjI2NTdaMFwiEgIBARcNOTUxMDA5MjMzMjA1WjASAgEDFw05NTEyMDEwMT AwMDBa MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMA OGCSqG SIB3DQEBBAUAA0EAHPjQ3M93QOj8Ufi+jZM7Y78TfAzG4jJn/ E6MYBPFVQFY0/Gp UZexfjSVo5CIyyS0tYscz8o07avwBxTiMpDEQg== -----END X509 CRL-- </pre>
Description	Entrez un résumé de ce qui est inclus dans cette liste CRL.

5 Cliquez sur **Importer**.

Résultats

La liste CRL importée apparaît sous forme de lien.

Configuration de NSX Manager pour récupérer une liste de révocation des certificats

À l'aide de l'API, vous pouvez configurer NSX Manager pour récupérer une liste de révocation des certificats (CRL). Vous pouvez ensuite vérifier la CRL en effectuant un appel d'API à NSX Manager au lieu de l'autorité de certification.

Cette fonctionnalité offre les avantages suivants :

- Il est plus efficace d'avoir la CRL mise en cache sur le serveur, c'est-à-dire NSX Manager.
- Le client n'a pas besoin de créer une connexion sortante vers l'autorité de certification.

Les API suivantes associées aux listes de révocation des certificats sont disponibles :

```

GET /api/v1/trust-management
GET /api/v1/trust-management/crl-distribution-points
POST /api/v1/trust-management/crl-distribution-points
DELETE /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
GET /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
PUT /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>
GET /api/v1/trust-management/crl-distribution-points/<crl-distribution-point-id>/status
POST /api/v1/trust-management/crl-distribution-points/pem-file

```

Vous pouvez gérer les points de distribution de CRL et récupérer les CRL stockées dans NSX Manager. Pour plus d'informations, reportez-vous à la *Référence API de NSX-T Data Center*.

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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Système > Certificats**.
- 3 Cliquez sur l'onglet **CSR**.
- 4 Sélectionnez une demande de signature de certificat.
- 5 Sélectionnez **Actions > Importer un certificat pour la demande de signature de certificat**.
- 6 Accédez au fichier du certificat signé sur votre ordinateur et ajoutez le fichier.
- 7 Cliquez sur **Ajouter**.

Résultats

Le certificat auto-signé s'affiche dans l'onglet **Certificats**.

Stockage des certificats publics et des clés privées

Les certificats publics et les clés privées sont stockés sur les instances de NSX Manager. Lorsqu'un équilibreur de charge ou un service VPN est créé qui nécessite une clé privée, NSX Manager envoie une copie de la clé privée au nœud Edge sur lequel l'équilibreur de charge ou le service VPN est en cours d'exécution.

Configuration basée sur la conformité

NSX-T Data Center peut être configuré pour utiliser les modules de chiffrement validés FIPS 140-2 pour s'exécuter en mode compatible FIPS. Les modules sont validés par les normes FIPS 140-2 par le programme de validation de module de chiffrement (CMVP) de la NIST.

Toutes les exceptions à la conformité FIPS peuvent être récupérées à l'aide du rapport de conformité. Pour plus d'informations, reportez-vous à la section [Afficher le rapport sur l'état de conformité](#).

Les modules validés suivants sont utilisés dans NSX-T Data Center 2.5 :

- VMware OpenSSL FIPS Object Module version 2.0.9 : [Certificat #2839](#)
- VMware OpenSSL FIPS Object Module version 2.0.20-vmw : [Certificat #3550](#)
- BC-FJA (Bouncy Castle FIPS Java API) version 1.0.1 : [Certificat #3152](#)
- VMware IKE Crypto Module version 1.1.0 : [Certificat #3435](#)
- VMware VPN Crypto Module version 1.0 : [Certificat #3542](#)

Vous pouvez trouver plus d'informations sur les modules cryptographiques que VMware a validés par rapport à la norme FIPS 140-2 ici : <https://www.vmware.com/security/certifications/fips.html>.

Par défaut, l'équilibreur de charge utilise des modules sur lesquels le mode FIPS est désactivé. Vous pouvez activer le mode FIPS pour les modules utilisés par l'équilibreur de charge. Pour plus d'informations, reportez-vous à la section [Configurer le mode de conformité FIPS global pour l'équilibreur de charge](#).

Afficher le rapport sur l'état de conformité

Vous pouvez afficher un rapport de conformité pour les fonctionnalités de NSX-T Data Center. Vous pouvez utiliser le rapport pour configurer votre environnement NSX-T Data Center afin qu'il adhère à vos stratégies informatiques et aux normes industrielles.

Le rapport de conformité inclut des informations sur chaque configuration non conforme.

Tableau 21-8. Informations du rapport de conformité

Colonne du rapport de conformité	Description	Exemple
Code de non-conformité	Code permettant d'identifier le type de non-conformité.	72301
Description	Description du type de non-conformité.	Le certificat n'est pas signé par une autorité de certification.
Nom de la ressource	Nom ou ID de la ressource affectée.	nsx-manager-1
Type de ressource	Type de ressource affecté.	CertificateComplianceReporter
Ressources affectées	Nombre de ressources affectées. Le nombre peut être égal à 0 s'il y a des configurations non conformes présentes, mais que la fonctionnalité n'est pas utilisée.	1

Vous pouvez également récupérer le rapport à l'aide de l'API : `GET /policy/api/v1/compliance/status`.

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Sur la page **Accueil**, cliquez sur **Tableaux de bord de surveillance > Rapport de conformité**.

Codes de rapport d'état de conformité

Vous pouvez trouver plus d'informations sur la signification du rapport d'état de conformité.

Tableau 21-9. Codes de rapport de conformité

Code	Description	Source de l'état de conformité	Correction
72001	Le chiffrement est désactivé.	Cet état est signalé si une configuration de profil VPN IPSec contient les algorithmes de chiffrement NO_ENCRYPTION, NO_ENCRYPTION_AUTH_AES_GMAC_128, NO_ENCRYPTION_AUTH_AES_GMAC_192 ou NO_ENCRYPTION_AUTH_AES_GMAC_256. Cet état affecte les configurations de session IPSec VPN qui utilisent les configurations non conformes signalées.	Pour corriger cet état, ajoutez un profil VPN IPSec qui utilise des algorithmes de chiffrement conformes et utilisez le profil dans toutes les configurations VPN. Reportez-vous à la section Ajouter des profils IPSec .
72011	Messages BGP avec contrôle d'intégrité de contournement du voisin. Aucune authentification de message définie.	Cet état est signalé si aucun mot de passe n'est configuré pour les voisins BGP. Cet état affecte la configuration du voisin BGP.	Pour corriger cet état, configurez un mot de passe sur le voisin BGP et mettez à jour la configuration de la passerelle de niveau 0 pour utiliser le mot de passe. Reportez-vous à la section Configurer BGP .
72012	La communication avec le voisin BGP utilise un contrôle d'intégrité faible. MD5 est utilisé pour l'authentification des messages.	Cet état est signalé si l'authentification MD5 est utilisée pour le mot de passe du voisin BGP. Cet état affecte la configuration du voisin BGP.	Aucune correction disponible, car NSX-T Data Center ne prend en charge que l'authentification MD5 pour BGP.

Tableau 21-9. Codes de rapport de conformité (suite)

Code	Description	Source de l'état de conformité	Correction
72021	SSL version 3 utilisé pour établir une connexion de socket sécurisée. Il est recommandé d'exécuter TLSv 1.1 ou version ultérieure et de désactiver entièrement SSLv3 ayant des faiblesses de protocole.	<p>Cet état est signalé si SSL version 3 est configuré dans le profil SSL du client de l'équilibreur de charge, le profil SSL du serveur d'équilibreur de charge ou le moniteur HTTPS de l'équilibreur de charge.</p> <p>Cet état affecte les configurations suivantes :</p> <ul style="list-style-type: none"> ■ Pools d'équilibreur de charge associés aux moniteurs HTTPS. ■ Serveurs virtuels d'équilibreur de charge associés à des profils SSL de client d'équilibreur de charge ou des profils SSL de serveur. 	Pour corriger cet état, configurez un profil SSL pour utiliser TLS 1.1 ou version ultérieure et utilisez ce profil dans toutes les configurations d'équilibreur de charge. Reportez-vous à la section Ajouter un profil SSL .
72022	TLS version 1.0 est utilisé pour établir une connexion de socket sécurisée. Il est recommandé d'exécuter TLSv 1.1 ou version ultérieure et de désactiver complètement TLSv 1.0 ayant des faiblesses de protocole.	<p>Cet état est signalé si TLSv 1.0 est configuré dans le profil SSL du client de l'équilibreur de charge, le profil SSL du serveur d'équilibreur de charge ou le moniteur HTTPS de l'équilibreur de charge.</p> <p>Cet état affecte les configurations suivantes :</p> <ul style="list-style-type: none"> ■ Pools d'équilibreur de charge associés aux moniteurs HTTPS. ■ Serveurs virtuels d'équilibreur de charge associés à des profils SSL de client d'équilibreur de charge ou des profils SSL de serveur. 	Pour corriger cet état, configurez un profil SSL pour utiliser TLS 1.1 ou version ultérieure et utilisez ce profil dans toutes les configurations d'équilibreur de charge. Reportez-vous à la section Ajouter un profil SSL .

Tableau 21-9. Codes de rapport de conformité (suite)

Code	Description	Source de l'état de conformité	Correction
72023	Un groupe Diffie-Hellman faible est utilisé.	<p>Cette erreur est signalée si un profil VPN IPSec ou une configuration de profil VPN IKE inclut les groupes Diffie-Hellman suivants : 2, 5, 14, 15 ou 16. Les groupes 2 et 5 sont des groupes Diffie-Hellman faibles. Les groupes 14, 15 et 16 ne sont pas des groupes faibles, mais ils ne sont pas compatibles avec FIPS.</p> <p>Cet état affecte les configurations de session IPSec VPN qui utilisent les configurations non conformes signalées.</p>	Pour corriger cet état, configurez les profils VPN pour utiliser le groupe Diffie-Hellman 19, 20 ou 21. Reportez-vous à la section Ajout de profils .
72024	Le paramètre global FIPS de l'équilibreur de charge est désactivé.	<p>Cette erreur est signalée si le paramètre global FIPS de l'équilibreur de charge est désactivé.</p> <p>Cet état affecte tous les services d'équilibreur de charge.</p>	Pour corriger cet état, activez FIPS pour l'équilibreur de charge. Reportez-vous à la section Configurer le mode de conformité FIPS global pour l'équilibreur de charge .
72200	Entropie réelle insuffisante disponible.	<p>Cet état est signalé lorsqu'un pseudo générateur de nombres aléatoires est utilisé pour générer l'entropie plutôt que de s'appuyer sur une entropie générée par le matériel.</p> <p>L'entropie générée par le matériel n'est pas utilisé, car le nœud NSX Manager ne dispose pas de la prise en charge de l'accélération matérielle requise pour créer une entropie réelle suffisante.</p>	<p>Pour corriger cet état, vous devrez peut-être utiliser un matériel plus récent pour exécuter le nœud NSX Manager. La plupart des matériels récents prennent en charge cette fonctionnalité.</p> <hr/> <p>Note Si l'infrastructure sous-jacente est virtuelle, vous n'obtiendrez pas d'entropie réelle.</p> <hr/>

Tableau 21-9. Codes de rapport de conformité (suite)

Code	Description	Source de l'état de conformité	Correction
72201	Source d'entropie inconnue.	Cet état est signalé lorsqu'aucun état d'entropie n'est disponible pour le nœud indiqué.	Pour corriger cet état, vérifiez que le nœud indiqué fonctionne correctement.
72301	Le certificat n'est pas signé par une autorité de certification.	<p>Cet état est signalé lorsque l'un des certificats NSX Manager n'est pas signé par une autorité de certification. NSX Manager utilise les certificats suivants .</p> <ul style="list-style-type: none"> ■ Certificat Syslog. ■ Certificats API pour les nœuds NSX Manager individuels. ■ Certificat de cluster utilisé pour NSX ManagerVIP. 	Pour corriger cet état, installez des certificats signés par une autorité de certification. Reportez-vous à la section Configuration de certificats .

Configurer le mode de conformité FIPS global pour l'équilibreur de charge

Il existe un paramètre global pour la conformité FIPS pour les équilibrages de charge. Par défaut, le paramètre est désactivé pour améliorer les performances.

La modification de la configuration globale pour la conformité FIPS des équilibreurs de charge affecte les nouvelles instances d'équilibreur de charge, mais n'affecte pas les instances d'équilibreur de charge existantes.

Si le paramètre global pour FIPS de l'équilibreur de charge (`lb_fips_enabled`) est défini sur *true*, les nouvelles instances d'équilibreur de charge utilisent des modules conformes à FIPS 140-2. Les instances d'équilibreur de charge existantes peuvent utiliser des modules non conformes.

Pour que la modification prenne effet sur les équilibreurs de charge existants, vous devez détacher et rattacher l'équilibreur de charge de la passerelle de niveau 1.

Vous pouvez vérifier l'état de conformité FIPS global pour l'équilibreur de charge à l'aide de `GET /policy/api/v1/compliance/status`.

```
...
{
  "non_compliance_code": 72024,
  "description": "Load balancer FIPS global setting is disabled.",
  "reported_by": {
    "target_id": "971ca477-df1a-4108-8187-7918c2f8c3ba",
    "target_display_name": "971ca477-df1a-4108-8187-7918c2f8c3ba",
    "target_type": "FipsGlobalConfig",
    "is_valid": true
  }
}
```

```

    },
    "affected_resources": [
      {
        "path": "/infra/lb-services/LB_Service",
        "target_id": "/infra/lb-services/LB_Service",
        "target_display_name": "LB_1",
        "target_type": "LBService",
        "is_valid": true
      }
    ]
  },
  ...

```

Note Le rapport de conformité affiche le paramètre global pour la conformité FIPS pour l'équilibreur de charge. Une instance d'équilibreur de charge quelconque peut avoir un état de conformité FIPS différent du paramètre global.

Procédure

- 1 Récupérez le paramètre FIPS global pour l'équilibreur de charge.

GET <https://nsx-mgr1/policy/api/v1/infra/global-config>

Exemple de texte de réponse :

```

{
  "fips": {
    "lb_fips_enabled": false
  },
  "resource_type": "GlobalConfig",
  "id": "global-config",
  "display_name": "global-config",
  "path": "/infra/global-config",
  "relative_path": "global-config",
  "marked_for_delete": false,
  "_create_user": "system",
  "_create_time": 1561225479619,
  "_last_modified_user": "admin",
  "_last_modified_time": 1561937915337,
  "_system_owned": true,
  "_protection": "NOT_PROTECTED",
  "_revision": 2
}

```

- 2 Modifiez le paramètre FIPS global pour l'équilibreur de charge.

Le paramètre global est utilisé lorsque vous créez des instances d'équilibreur de charge. La modification du paramètre n'affecte pas les instances d'équilibreur de charge existantes.

PUT <https://nsx-mgr1/policy/api/v1/infra/global-config>

Exemple de texte de demande :

```

{
  "fips": {

```



```

    "lb_fips_enabled": true
  },
  "resource_type": "GlobalConfig",
  "_revision": 2
}

```

Exemple de texte de réponse :


```


{
  "fips": {
    "lb_fips_enabled": true
  },
  "resource_type": "GlobalConfig",
  "id": "global-config",
  "display_name": "global-config",
  "path": "/infra/global-config",
  "relative_path": "global-config",
  "marked_for_delete": false,
  "_create_user": "system",
  "_create_time": 1561225479619,
  "_last_modified_user": "admin",
  "_last_modified_time": 1561937960950,
  "_system_owned": true,
  "_protection": "NOT_PROTECTED",
  "_revision": 3
}

```

- 3 Si vous voulez que des instances d'équilibreur de charge existantes utilisent ce paramètre global, vous devez détacher et rattacher l'équilibreur de charge de la passerelle de niveau 1.

Attention Le détachement d'un équilibreur de charge de la passerelle de niveau 1 entraîne une interruption du trafic pour l'instance d'équilibreur de charge.

- a Accédez à **Mise en réseau > Équilibrage de charge**.
- b Sur l'équilibreur de charge que vous voulez détacher, cliquez sur le menu trois points (⋮), puis cliquez sur **Modifier**.
- c Cliquez sur , puis sur **Enregistrer** pour détacher l'équilibreur de charge de la passerelle de niveau 1.

Nom	Taille	Passerelle de niveau 1
LB_1 *	Petit ▼	TLR1_LR 

- d Cliquez sur le menu trois points (⋮), puis cliquez sur **Modifier**.
- e Sélectionnez la passerelle appropriée dans le menu déroulant **Passerelle de niveau 1**, puis cliquez sur **Enregistrer** pour rattacher l'équilibreur de charge à la passerelle de niveau 1.

Collecter 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 un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.

- 2 Sélectionnez **Système > Bundle de support**.

- 3 Sélectionnez les nœuds cibles.

Les types de nœuds disponibles sont les **Nœuds de gestion**, les **Dispositifs Edge**, les **Hôtes** et les **Passerelles de cloud public**.

- 4 (Facultatif) Spécifiez l'âge de journal en jours pour exclure les journaux antérieurs au nombre de jours spécifié.
- 5 (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.

- 6 (Facultatif) Cochez la case pour charger les bundles sur un serveur de fichiers distant.

- 7 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.

- 8 Surveillez l'état du processus de collecte.

L'onglet État affiche la progression de la collecte des bundles de support.

- 9 Cliquez sur **Télécharger** pour télécharger le bundle si l'option pour envoyer le bundle à un serveur de fichiers distant n'a pas été définie.

La collecte de bundles peut échouer pour un nœud de gestionnaire s'il n'y a pas suffisamment d'espace disque. Si vous rencontrez une erreur, vérifiez si d'anciens bundles de support sont présents sur le nœud ayant échoué. Connectez-vous à l'interface utilisateur NSX Manager du nœud de gestionnaire ayant échoué à l'aide de son adresse IP et lancez la collecte de bundles à partir de ce nœud. Lorsque NSX Manager vous y invite, téléchargez l'ancien bundle ou supprimez-le.

Messages de journal et codes d'erreur

Les composants NSX-T Data Center écrivent dans des fichiers journaux dans le répertoire `/var/log/`. Sur les dispositifs NSX-T et les hôtes KVM, les messages Syslog NSX sont conformes à RFC 5424. Sur les hôtes ESXi, les messages Syslog sont conformes à RFC 3164.

Affichage des journaux

Sur les dispositifs NSX-T, les messages Syslog se trouvent dans `/var/log/syslog`. Sur les hôtes KVM, les messages Syslog se trouvent dans `/var/log/vmware/nsx-syslog`.

Sur les dispositifs NSX-T, vous pouvez exécuter la commande CLI NSX-T suivante pour afficher les journaux :

```
get log-file <auth.log | controller | controller-error | http.log | kern.log | manager.log |
node-mgmt.log | policy.log | syslog> [follow]
```

Les fichiers journaux sont les suivants :

Nom	Description
auth.log	Journal des autorisations
controller	Journal du contrôleur
controller-error	Journal des erreurs du contrôleur
http.log	Journal des services HTTP
kern.log	Journal du noyau
manager.log	Journal de Manager Service
node-mgmt.log	Journal de gestion des nœuds
policy.log	Journal du service de stratégie
syslog	Journal système

Sur les hyperviseurs, vous pouvez utiliser des commandes Linux telles que `tail`, `grep` et `more` pour afficher les journaux.

Chaque message Syslog 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 émet des journaux avec l'installation `local6`, qui a une valeur numérique de 22.

Le journal d'audit fait partie de Syslog. Un message de journal d'audit peut être identifié par la chaîne `audit="true"` dans le champ `structured-data`. Par exemple :

```
<182>1 2020-05-05T00:29:02.900Z nsx-manager1 NSX 14389 - [nsx@6876 audit="true"
comp="nsx-manager" level="INFO" reqId="fe75651d-c3e7-4680-8753-9ae9d92d7f0c" subcomp="policy"
username="admin"] UserName="admin", ModuleName="AAA", Operation="GetCurrentUserInfo",
Operation status="success"
```

Chaque appel d'API génère un message de 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>`.

RFC 5424 et RFC 3164 définissent 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.

Formats de message de journal

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.
```

Codes d'erreur

Pour obtenir une liste de codes d'erreur, reportez-vous à l'article 71077 de la base de connaissances [Codes d'erreur de NSX-T Data Center 2.x](#).

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 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

- Familiarisez-vous avec la commande CLI `set logging-server`. Pour plus d'informations, reportez-vous à la *Référence CLI de NSX-T*.
- Si vous utilisez les protocoles TLS ou LI-TLS dans la CLI de NSX pour configurer une connexion sécurisée à un serveur de journalisation, les certificats de serveur et de client doivent être stockés dans `/image/vmware/nsx/file-store` sur chaque dispositif NSX-T Data Center. Notez que les certificats dans le magasin de fichiers sont nécessaires uniquement si l'exportateur est configuré à l'aide de la CLI de NSX. Si vous utilisez l'API, il n'est pas nécessaire d'utiliser le magasin de fichiers. Une fois la configuration de l'exportateur Syslog terminée, vous devez supprimer tous les certificats et clés de cet emplacement pour éviter d'éventuelles vulnérabilités de sécurité.
- Pour configurer une connexion sécurisée à un serveur de journalisation, vérifiez que le serveur est configuré avec des certificats signés par une autorité de certification. Par exemple, si vous disposez d'un serveur Log Insight `vrli.prome.local` comme serveur de journalisation, vous pouvez exécuter la commande suivante à partir d'un client pour voir la chaîne de certificats sur le serveur :

```
root@caserver:~# echo -n | openssl s_client -connect vrli.prome.local:443 | sed -ne '/
^Certificate chain/,/^---/p'
depth=2 C = US, L = California, O = GS, CN = Orange Root Certification Authority
verify error:num=19:self signed certificate in certificate chain
```

```

Certificate chain
 0 s:/C=US/ST=California/L=HTG/O=GSS/CN=vrli.prome.local
  i:/C=US/L=California/O=GS/CN=Green Intermediate Certification Authority
 1 s:/C=US/L=California/O=GS/CN=Green Intermediate Certification Authority
  i:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
 2 s:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
  i:/C=US/L=California/O=GS/CN=Orange Root Certification Authority
---
DONE

```

Procédure

- 1 Pour configurer la journalisation distante sur un dispositif NSX-T Data Center, 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>] [serverca <filename>] [clientca <filename>]
[certificate <filename>] [key <filename>] [structured-data <structured-data>]

```

Vous pouvez exécuter la commande plusieurs fois pour ajouter plusieurs configurations. 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

```

Pour transférer uniquement les journaux d'audit au serveur distant, spécifiez `audit="true"` dans le paramètre `structured-data`. Par exemple :

```

set logging-server <server-ip> proto udp level info structured-data audit="true"

```

- 2 Pour configurer la journalisation à distance sécurisée à l'aide du protocole LI-TLS, spécifiez le paramètre `proto li-tls`. Par exemple :

```

set logging-server vrli.prome.local proto li-tls level info messageid
SWITCHING,ROUTING,FABRIC,SYSTEM,POLICY,HEALTHCHECK,SHA,MONITORING serverca intermed-ca-
full-chain.crt

```

Si la configuration est réussie, vous recevrez une invite sans texte. Pour afficher le contenu de la chaîne de certificats du serveur (intermédiaire suivi de la racine), connectez-vous en tant que `root` et exécutez la commande suivante :

```

root@nsx1:~# keytool -printcert -file /image/vmware/nsx/file-store/intermed-ca-full-
chain.crt
Certificate[1]:
Owner: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd2
Valid from: Sun Mar 15 00:00:00 UTC 2020 until: Mon Mar 17 00:00:00 UTC 2025

```

```

Certificate fingerprints:
  MD5:  94:C8:9F:92:56:60:EB:DB:ED:4B:11:17:33:27:C0:C9
  SHA1: 42:9C:3C:51:E8:8E:AC:2E:5E:62:95:82:D7:22:E0:FB:08:B8:64:29
  SHA256:
58:B8:63:3D:0C:34:35:39:FC:3D:1E:BA:AA:E3:CE:A9:C0:F3:58:53:1F:AD:89:A5:01:0D:D3:89:9E:7B:C
5:69
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[2]:
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
  MD5:  ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
  SHA1: DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
  SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3

```

Les journaux pour les conditions de réussite et d'échec se trouvent dans `/var/log/loginsight-agent/liagent_2020-MM-DD-<file-num>.log`. Si la configuration est réussie, vous pouvez afficher la configuration de Log Insight à l'aide de la commande suivante :

```

root@nsx1:/image/vmware/nsx/file-store# cat /var/lib/loginsight-agent/liagent-effective.ini
; Dynamic file representing the effective configuration of VMware Log Insight Agent
(merged server-side and client-side configuration)
; DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
; Creation time: 2020-03-22T19:41:21.648800

[server]
hostname=vrli.prome.local
proto=cfapi
ssl=yes
ssl_ca_path=/config/vmware/nsx-node-api/syslog/bb466082-996f-4d77-b6e3-1fa93f4a20d4_ca.pem
ssl_accept_any_trusted=yes
port=9543
filter={filelog; nsx-syslog; pri_severity <= 6 and ( msgid == "SWITCHING" or msgid ==
"ROUTING" or msgid == "FABRIC" or msgid == "SYSTEM" or msgid == "POLICY" or msgid ==
"HEALTHCHECK" or msgid == "SHA" or msgid == "MONITORING" ) }

[filelog|nsx-syslog]
directory=/var/log
include=syslog;syslog.*
parser=nsx-syslog_parser

[parser|nsx-syslog_parser]
base_parser=syslog

```

```
extract_sd=yes

[update]
auto_update=no
```

- 3 Pour configurer la journalisation à distance sécurisée à l'aide du protocole TLS, spécifiez le paramètre `proto tls`. Par exemple :

```
set logging-server vrli.prome.local proto tls level info serverca Orange-CA.crt.pem
clientca Orange-CA.crt.pem certificate gc-nsxt-mgr-full.crt.pem key gc-nsxt-mgr.key.pem
```

Notez les points suivants :

- Pour le paramètre `serverCA`, seul le certificat racine est requis, et non la chaîne complète.
- Si `clientCA` est différent de `serverCA`, seul le certificat racine est requis.
- Le certificat doit contenir la chaîne complète du NSX Manager (il doit être conforme à NDcPP - ECU, BASIC et CDP [CDP : ce contrôle peut être ignoré]).

Vous pouvez inspecter le contenu de chaque certificat. Par exemple :

```
root@gc3:~# keytool -printcert -file /image/vmware/nsx/file-store/Orange-CA.crt.pem
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
    MD5: ED:AC:F1:7F:88:05:83:C0:09:03:D5:00:CA:7B
    SHA1: DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
    SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
root@gc3:~#

root@gc3:/image/vmware/nsx/file-store# keytool -printcert -file gc-nsxt-mgr-full.crt.pem
Certificate[1]:
Owner: CN=gc.prome.local, O=GS, L=HTG, ST=California, C=US
Issuer: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
Serial number: bdf43ab31340b87f323b438a2895a075
Valid from: Mon Mar 16 07:26:51 UTC 2020 until: Wed Mar 16 07:26:51 UTC 2022
Certificate fingerprints:
    MD5: 36:3C:1F:57:96:07:84:C0:6D:B7:33:9A:8D:25:4D:27
    SHA1: D1:4E:F9:45:2D:0D:34:79:D2:B4:FA:65:28:E0:5C:DC:74:50:CA:3B
    SHA256:
3C:FF:A9:5D:AA:68:44:44:DD:07:2F:DD:E2:BE:9C:32:19:7A:03:D5:26:8D:5F:AD:56:CA:D2:6C:91:96:2
7:6F
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[2]:
Owner: CN=Green Intermediate Certification Authority, O=GS, L=California, C=US
```



```

Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd2
Valid from: Sun Mar 15 00:00:00 UTC 2020 until: Mon Mar 17 00:00:00 UTC 2025
Certificate fingerprints:
    MD5: 94:C8:9F:92:56:60:EB:DB:ED:4B:11:17:33:27:C0:C9
    SHA1: 42:9C:3C:51:E8:8E:AC:2E:5E:62:95:82:D7:22:E0:FB:08:B8:64:29
    SHA256:
58:B8:63:3D:0C:34:35:39:FC:3D:1E:BA:AA:E3:CE:A9:C0:F3:58:53:1F:AD:89:A5:01:0D:D3:89:9E:7B:C
5:69
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3
Certificate[3]:
Owner: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Issuer: CN=Orange Root Certification Authority, O=GS, L=California, C=US
Serial number: 3e726e7fbb3b0a7a6b4edd767f867fd1
Valid from: Mon Mar 16 07:16:07 UTC 2020 until: Fri Mar 10 07:16:07 UTC 2045
Certificate fingerprints:
    MD5: ED:AC:F1:7F:88:05:83:2A:83:C0:09:03:D5:00:CA:7B
    SHA1: DC:B5:3F:37:DF:BD:E0:5C:A4:B7:F4:4C:96:12:75:7A:16:C7:61:37
    SHA256:
F2:5B:DE:8A:F2:31:9D:E6:EF:35:F1:30:6F:DA:05:FF:92:B4:15:96:AA:82:67:E3:3C:C1:69:A3:E5:27:B
9:A5
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3

```

Exemples de journalisation réussie dans /var/log/syslog :

```

<182>1 2020-03-22T21:54:34.501Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created CA PEM file /
config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_ca.pem for logging
server vrli.prome.local:6514
<182>1 2020-03-22T21:54:36.269Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created client CA PEM
file /config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_client_ca.pem
for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:54:36.495Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert issuer = /C=US/L=California/O=GS/
CN=Green IntermediateCertification Authority
<182>1 2020-03-22T21:54:36.514Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert subject = /C=US/ST=California/L=HTG/
O=GS/CN=gc.promelocal
<182>1 2020-03-22T21:54:36.539Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] certificate trust check succeeded.
status: 200, result: {'status': 'OK'}
<182>1 2020-03-22T21:54:36.612Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] Certificate already exists, skip import
<182>1 2020-03-22T21:54:37.322Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created certificate PEM
file /config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_cert.pem for
logging server vrli.prome.local:6514

```

```
<182>1 2020-03-22T21:54:38.020Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created key PEM file /
config/vmwarensx-node-api/syslog/92a78d8a-acfd-4515-b05a-2927b70ae920_key.pem for logging
server vrli.prome.local:6514
```

Exemples d'échec de journalisation dans /var/log/syslog :

```
<182>1 2020-03-22T21:33:30.424Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully created client CA PEM
file /config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_client_ca.pem
for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:33:30.779Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert issuer = /C=US/L=California/O=GS/
CN=Green IntermediateCertification Authority
<182>1 2020-03-22T21:33:30.803Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="root" level="INFO"] cert subject = /C=US/ST=California/L=HTG/
O=GS/CN=gc.promelocal
<179>1 2020-03-22T21:33:30.823Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-
manager" subcomp="node-mgmt" username="root" level="ERROR" errorCode="NODE10"]
Certificate trust check failed. status:200, result: {'error_message': 'Certificate
CN=gc.prome.local,O=GS,L=HTG,ST=California,C=US was not verifiably signed by
CN=gc.prome.local,O=GS,L=HTG,ST=California,C=US: certificate does not verifywith supplied
key', 'status': 'ERROR'}
<179>1 2020-03-22T21:33:30.824Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-
manager" subcomp="node-mgmt" username="admin" level="ERROR" errorCode="NODE10"]
Failed to create certificate PEM file config/vmware/nsx-node-api/syslog/
76332782-1ec6-483a-95d4-2adeaf2ef112_cert.pem for logging server vrli.prome.local:6514
<182>1 2020-03-22T21:33:31.578Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully deleted CA PEM file /
config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_ca.pem
<182>1 2020-03-22T21:33:32.342Z gc3.prome.local NSX 5187 - [nsx@6876 comp="nsx-manager"
subcomp="node-mgmt" username="admin" level="INFO"] Successfully deleted client CA PEM
file /config/vmwarensx-node-api/syslog/76332782-1ec6-483a-95d4-2adeaf2ef112_ca.pem
<182>1 2020-03-22T21:33:32.346Z gc3.prome.local NSX 16698 - [nsx@6876 comp="nsx-cli"
subcomp="node-mgmt" username="admin" level="INFO" audit="true"] CMD: set logging-server
vrli.prome.local prototls level info serverca Orange-CA.crt.pem clientca Orange-CA.crt.pem
certifi
cate gc-nsxt-mgr.crt.pem key gc-nsxt-mgr.key.pem (duration: 6.365s), Operation status:
CMD_EXECUTED
```

Vous pouvez vérifier si le certificat et la clé privée correspondent à la commande suivante. S'ils correspondent, la sortie sera `writing RSA key`. Toute autre sortie signifie qu'ils ne correspondent pas. Par exemple :

```
root@caserver:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/gc-nsxt-mgr.key.pem -pubout)
writing RSA key
```

Exemple d'une clé privée endommagée :

```
root@caserver:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/gc-nsxt-mgr-corrupt.key.pem -pubout)
unable to load Private Key
140404188370584:error:0D07209B:asn1 encoding routines:ASN1_get_object:too
```

```

long:asn1_lib.c:147:
140404188370584:error:0D068066:asn1 encoding routines:ASN1_CHECK_TLEN:bad object
header:tasn_dec.c:1205:
140404188370584:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1
error:tasn_dec.c:386:Type=RSA
140404188370584:error:04093004:rsa routines:OLD_RSA_PRIV_DECODE:RSA lib:rsa_ameth.c:119:
140404188370584:error:0D07209B:asn1 encoding routines:ASN1_get_object:too
long:asn1_lib.c:147:
140404188370584:error:0D068066:asn1 encoding routines:ASN1_CHECK_TLEN:bad object
header:tasn_dec.c:1205:
140404188370584:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1
error:tasn_dec.c:386:Type=PKCS8_PRIV_KEY_INFO
140404188370584:error:0907B00D:PEM routines:PEM_READ_BIO_PRIVATEKEY:ASN1
lib:pem_pkey.c:141:
1,14d0
< -----BEGIN PUBLIC KEY-----
< MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAv3yH7pZidfkLrEP3zVa9
< EcOKX1FFjkThZRZMfguenlm8s6QHYYVvuUX8IRB48Li3/DUfOj0bzaPWktpv+Q2P0
< N/j4LoX2RzjV/DPxYfLP6GMNMc21L3s9ruBeWUthtUP8khCwd2d2rZ09cUZV10P9
< kIYBb5RMFC7Z10Uth3bKdepEf+sXz3DaKZ/WySzYq9x86QDaA3ABO3Q0i7txBscI
< FvXuMDOMQaC3pPp9FWO6IPRAWB57wahLJv6K5qGIfwubSBFg53grT4snf11DZAHz
< 9hz5JgGr80GVyWyb7rgigpl9iUWAZx8U9De9XoxmvBN5iEGTIuKGaEgICL176crb
< RMkhjnCqNHI+z6sQvpYJ7U0zZc72eBIWoHUKcWWk3eU6Oy4OiyW6jYuXG7hZY1ly
< nSkme3mZUWJKvcoX05+3zeCP623/HzE7X2sNyWFjzeF3XEvauZrIbsJh/xp2ShDa
< uKKEY0gUGhLtCa3TpV9l8d6tFWVy8XjVjdjoVt4s7MfUo/airVmRykfsWrKyNUOQ
< qRZvSbqjt8pm+3bSvKdXX4ul7ptPG2GF20ETWHPwj2JwQpGhR9zK8fsKzvm6hXi
< kq76zi4FefuVps3e1r39+0F+p6d6i2oUoo24sC1iSePTDhU74efVp6iv8HmnDgYX
< Ylm6Kusr0JT5TJFDfASmrj8CAwEAAQ==
< -----END PUBLIC KEY-----

```

Exemple d'une clé privée et d'un certificat valides, mais qui ne sont pas faits l'un pour l'autre :

```

root@caserver:~/server-certs# diff <(openssl x509 -in certs/gc-nsxt-mgr.crt.pem -pubkey
-noout) <(openssl rsa -in private/vrli.key.pem -pubout)
writing RSA key
2,13c2,13
< MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAv3yH7pZidfkLrEP3zVa9
< EcOKX1FFjkThZRZMfguenlm8s6QHYYVvuUX8IRB48Li3/DUfOj0bzaPWktpv+Q2P0
< N/j4LoX2RzjV/DPxYfLP6GMNMc21L3s9ruBeWUthtUP8khCwd2d2rZ09cUZV10P9
< kIYBb5RMFC7Z10Uth3bKdepEf+sXz3DaKZ/WySzYq9x86QDaA3ABO3Q0i7txBscI
< FvXuMDOMQaC3pPp9FWO6IPRAWB57wahLJv6K5qGIfwubSBFg53grT4snf11DZAHz
< 9hz5JgGr80GVyWyb7rgigpl9iUWAZx8U9De9XoxmvBN5iEGTIuKGaEgICL176crb
< RMkhjnCqNHI+z6sQvpYJ7U0zZc72eBIWoHUKcWWk3eU6Oy4OiyW6jYuXG7hZY1ly
< nSkme3mZUWJKvcoX05+3zeCP623/HzE7X2sNyWFjzeF3XEvauZrIbsJh/xp2ShDa
< uKKEY0gUGhLtCa3TpV9l8d6tFWVy8XjVjdjoVt4s7MfUo/airVmRykfsWrKyNUOQ
< qRZvSbqjt8pm+3bSvKdXX4ul7ptPG2GF20ETWHPwj2JwQpGhR9zK8fsKzvm6hXi
< kq76zi4FefuVps3e1r39+0F+p6d6i2oUoo24sC1iSePTDhU74efVp6iv8HmnDgYX
< Ylm6Kusr0JT5TJFDfASmrj8CAwEAAQ==
---
> MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAqvsjay7+o7gCW7szT3ho
> bc34XX216u5Jl4/X/pUDI/YHmIf06bsZ1r/14bTL4Q7BM6+9MI6UYEE7DxUoINGO
> o4FEEQE32KwVFe3gw3homHU39q4pQjsJsxTcTe3oDmLIY0nWJ0PRUst3DffYUH1L
> W0NUN9yDN+fAl2Uf021iuDqVy9V8AH3ON6fu+QCA8nt71zkzeTxSA0ldpl2NA17F
> rD8rm05wxnV7WtuV7V8PstISiClzhHgZRM1+B0r300itnyAzEGLaRT3//PKfe0Oe
> HCdxGmlrUtMqxIItJahEsqvMufyqNYecVscYXLHPelizKCsQfy8c08LnznG8VAdc

```

```
> YILSn3uYGZap6aF1SgVxsvZicwvLYnssmgE13Af0nScmfM96k9h5joHVEkWK6O8v
> oT5DGG1kVL2Qly97x0b6EnzUorziVV5zJMKvFcOektR8HdMHQit5uvmMRY3S5zow
> FtvfSDfWxxKyTy6GBRpP+8F+Jq9lyGy/qa9lhKBzT2lg+rJp7T8k7/Nm9Tjyx7jL
> EggEKZEL4chxpo8ucF98hbxWRuaFHC2iDzGuUmuS1FfjVvHTuIbEMQfjapLZrHx
> 8jHfOP/PL+6kPbvNZ2rTpczuEoGTQFFW9vX48GzIEyMeR6QWpPR0F7r4xak68P5
> 2PJmMveinDhU35IqWEXHawcCAwEAAQ==
```

- 4 Pour afficher la configuration de la journalisation, exécutez 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
```

- 5 Pour effacer la configuration de la journalisation à distance, exécutez la commande suivante :

```
nsx> clear logging-servers
```

- 6 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
```

- 7 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 21-10. 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
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 d'adresses MAC NSGroups NSServices Groupes NSService Pool VNI Pool IP
DHCP	relais DHCP
SYSTEM	Gestion des dispositifs (Syslog distant, NTP, etc.) Gestion des clusters Gestion de l'approbation Attribution de licences Utilisateur et rôles Gestion des tâches Installer Mise à niveau (NSX Manager, NSX Edge, et mises à niveau des modules d'hôte) Réalisation Balises

Tableau 21-10. ID de messages de journal (suite)

ID de message	Exemples
MONITORING	SNMP Connexion au port Traceflow
-	Tous les autres messages de journal.

Résolution des problèmes de Syslog

Si le serveur de journaux distant ne reçoit pas les journaux, procédez comme suit.

- Vérifiez l'adresse IP du serveur de journaux distant.
- Vérifiez que le paramètre `level` est correctement configuré.
- Vérifiez que le paramètre `facility` est correctement configuré.
- Si le protocole est TLS, définissez le protocole sur UDP pour vérifier qu'il n'existe pas une incompatibilité avec le certificat.
- Si le protocole est TLS, vérifiez que le port 6514 est ouvert sur les deux extrémités.
- Supprimez le filtre d'ID du message et vérifiez que le serveur reçoit bien les journaux.
- Redémarrez le service rsyslog avec la commande `restart service rsyslogd`.

Configurer la journalisation série sur une machine virtuelle de dispositif

Vous pouvez configurer la journalisation série sur une machine virtuelle de dispositif pour capturer les messages de journal lorsque la machine virtuelle se bloque.

Procédure

- 1 Connectez-vous à la machine virtuelle en tant que `root`.
- 2 Modifiez `/etc/default/grub`.
- 3 Recherchez le paramètre `GRUB_CMDLINE_LINUX_DEFAULT` et ajoutez `console=ttyS0`
`console=tty0`.
- 4 Exécutez la commande `update-grub2`.
- 5 Vérifiez que le fichier `/boot/grub/grub.cfg` a été modifié à l'étape 3.
- 6 Mettez la machine virtuelle hors tension.

- 7 Modifiez le fichier de configuration (.vmx) de la machine virtuelle et ajoutez les lignes suivantes :

```
serial0.present = "TRUE"
serial0.fileType = "file"
serial0.fileName = "serial.out"
serial0.yieldOnMsrRead = "TRUE"
answer.msg.serial.file.open = "Append"
```

- 8 Mettez sous-tension la machine virtuelle.

Résultats

Si une panique du noyau se produit dans la machine virtuelle, vous pouvez trouver le fichier `serial.out` contenant des messages de journal au même emplacement que celui du fichier `.vmx`.

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 CEIP, 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://<nsx-manager-ip-address>`.
- 2 Sélectionnez **Système > Programme du client**.
- 3 Cliquez sur **Modifier** dans la section Programme d'amélioration du produit.

- 4 Dans la boîte de dialogue Modifier le Programme d'amélioration du produit, sélectionnez la case **Rejoindre le Programme d'amélioration du produit VMware**.
- 5 Basculez le commutateur **Planifier** pour désactiver ou activer la collecte de données.
La planification est par défaut activée.
- 6 (Facultatif) Configurez les paramètres de collecte de données et de récurrence du téléchargement.
- 7 Cliquez sur **Enregistrer**.

Ajouter des balises à un objet

Vous pouvez ajouter des balises à des objets pour faciliter la recherche. Lorsque vous spécifiez une balise, vous pouvez également spécifier une étendue.

NSX Cloud Note Si vous utilisez NSX Cloud, consultez [Fonctionnalités de NSX-T Data Center prises en charge avec NSX Cloud](#) pour obtenir la liste des entités logiques générées automatiquement, des fonctionnalités prises en charge et des configurations requises pour NSX Cloud.

La plupart des objets peuvent contenir au maximum 30 balises. Pour les objets suivants, la valeur maximale est inférieure en raison des balises qui sont créées et utilisées en interne.

Tableau 21-11. Nombre maximal de balises pour les objets créés à l'aide de l'onglet Mise en réseau et sécurité avancées

Objet	Nombre maximal de balises
machine virtuelle	25
Port logique	29

Tableau 21-12. Nombre maximal de balises pour les objets créés à l'aide des onglets Mise en réseau, Sécurité ou Inventaire

Objet	Nombre maximal de balises
Groupe	29
Segment	27
Port de segment	29
Port de routeur logique	30 : nombre d'étiquettes
Règle NAT	27
Session IPSec VPN	29

Tableau 21-13. Nombre maximal de balises pour les objets de Cloud Service Manager

Objet	Nombre maximal de balises
Profil de surveillance de la santé BFD, zone de transport, profil de commutateur d'hôte de liaison montante, nœud de transport, cluster Edge	23

Tableau 21-14. Nombre maximal de balises pour les objets de Public Cloud Manager

Objet	Nombre maximal de balises
Profil de surveillance de la santé BFD, zone de transport, commutateur logique, nœud, nœud de transport, cluster Edge, routeur logique, port de liaison montante de routeur logique, route statique, profil DHCP, NSGroup, liste de règles de section de pare-feu	23
Règle NAT	20
ensemble d'adresses IP, NSGroup	22

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Modifiez un objet.
Par exemple, accédez à l'onglet **Segments** et modifiez un segment.
- 3 Accédez au champ **Balises** et ajoutez des balises.
Chaque balise possède une valeur de balise, qui est obligatoire, et une valeur d'étendue, qui est facultative. La longueur maximale d'une balise est de 256 caractères. La longueur maximale d'une étendue est de 128 caractères.
- 4 Cliquez sur **Enregistrer**.

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 21-15. 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
```

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://<nsx-manager-ip-address>`.

- 2 Sélectionnez **Mise en réseau et sécurité avancées > Inventaire > Groupes**.
- 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.

Configuration d'un équilibreur de charge externe

Vous pouvez configurer un équilibreur de charge externe pour répartir le trafic vers les gestionnaires NSX dans un cluster de gestionnaires.

Un cluster NSX Manager n'a pas besoin d'un équilibreur de charge externe. L'adresse IP virtuelle (VIP) de NSX Manager fournit une résilience en cas d'échec d'un nœud de gestionnaire, mais présente les limitations suivantes :

- L'adresse IP virtuelle n'effectue pas l'équilibrage de charge sur les instances de NSX Manager.
- L'adresse IP virtuelle nécessite que toutes les instances de NSX Manager se trouvent dans le même sous-réseau.
- La récupération d'adresses IP virtuelles dure entre 1 et 3 minutes en cas d'échec d'un nœud de gestionnaire.

Un équilibreur de charge externe peut offrir les avantages suivants :

- Équilibrage de la charge entre les instances de NSX Manager.
- Les instances de NSX Manager peuvent se trouver dans des sous-réseaux différents.
- Temps de récupération rapide en cas d'échec d'un nœud de gestionnaire.

Notez qu'un équilibreur de charge externe ne fonctionnera pas avec l'adresse IP virtuelle de NSX Manager. Ne configurez pas une adresse IP virtuelle NSX Manager si vous utilisez un équilibreur de charge externe.

Lorsque vous accédez à NSX Manager à partir d'un navigateur via un équilibreur de charge externe, la persistance de session doit être activée sur l'équilibreur de charge.

Lorsque vous accédez à NSX Manager à partir d'un client API via un équilibreur de charge externe, quatre méthodes d'authentification sont disponibles (pour plus d'informations, consultez le *Guide de l'API de NSX-T Data Center* pour plus d'informations) :

- Authentification HTTP de base : la persistance de la session d'équilibreur de charge n'est pas requise.
- Authentification par certificat client : la persistance de la session d'équilibreur de charge n'est pas requise.
- Authentification auprès de vIDM : la persistance de la session d'équilibreur de charge n'est pas requise.
- Authentification basée sur une session : la persistance de la session d'équilibreur de charge est requise.

Recommandation :

- Configurez une adresse IP unique sur l'équilibreur de charge externe pour l'accès au navigateur et à l'API. La persistance de session doit être activée sur l'équilibreur de charge.

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 [Installation des composants de NSX Cloud](#) du *Guide d'installation de NSX-T Data Center* pour découvrir le workflow de déploiement de NSX Cloud.

Reportez-vous également à : [cloud public](#).

Ce chapitre contient les rubriques suivantes :

- [Présentation rapide de Cloud Service Manager](#)
- [Détection des menaces à l'aide de la stratégie de mise en quarantaine de NSX Cloud](#)
- [Mode d'application NSX](#)
- [Mode d'application du Cloud natif](#)
- [Fonctionnalités de NSX-T Data Center prises en charge avec NSX Cloud](#)
- [Questions fréquemment posées \(FAQ\)](#)

Présentation rapide de 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 Détection des menaces à l'aide de la stratégie de mise en quarantaine de NSX Cloud 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 VPC/VNet par région.
- Vous pouvez afficher le nombre de machines virtuelles de charge de travail par VPC/VNet.

Il y a quatre onglets sous **Clouds**.

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 possède des VPC/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 public.

Vous pouvez filtrer l'inventaire par compte et par région.

- Chaque carte représente un VPC/VNet.
- Vous pouvez disposer d'une ou de deux instances de PCG (pour HA) déployées sur chaque VPC/VNet de transit.
- Vous pouvez lier des VPC/VNet de calcul à des VPC/VNet de transit.
- Vous pouvez afficher plus de détails pour chaque VPC ou VNet en basculant vers la vue grille.

Note Dans la vue grille, vous pouvez voir trois onglets : **Présentation**, **Instances** et **Segments**.

- **Présentation** répertorie les options sous Actions comme décrit à l'étape suivante.
 - **Instances** affiche une liste d'instances dans le VPC/VNet.
 - **Segments** affiche les segments de superposition dans NSX-T. Cette fonctionnalité n'est pas prise en charge dans la version actuelle de NSX Cloud. Ne balisez pas vos machines virtuelles de charge de travail dans AWS ou Microsoft Azure avec des balises affichées sur cet écran.
-
- Cliquez sur **Actions** pour accéder à ce qui suit :
 - **Modifier la configuration** (disponible uniquement pour les VPC/VNet de transit) :
 - Activez ou désactivez la stratégie de mise en quarantaine si dans le Mode d'application NSX.
 - Fournissez un groupe de sécurité de secours requis lorsque le VPC/VNet n'a plus accès à NSX Cloud lors de l'utilisation du Mode d'application NSX. Reportez-vous à la section [Impact de la stratégie de mise en quarantaine lorsqu'elle est désactivée](#).
 - Modifiez votre sélection de serveur proxy.

- **Lier au VPC/VNet de transit** : cette option est uniquement disponible pour les VPC/VNet sur lesquels aucune instance de PCG n'est déployée. Cliquez sur cette option pour sélectionner un VPC/VNet de transit auquel lier une instance.
- **Déployer la passerelle NSX Cloud** : cette option est uniquement disponible pour les VPC/VNet sur lesquels aucune instance de PCG n'est déployée. Cliquez sur cette option pour lancer le déploiement de PCG sur ce VPC/VNet, et paramétrer ce dernier en tant que VPC/VNet autonome ou de transit. Reportez-vous à la section **Déployer ou lier des passerelles de cloud public NSX** du *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.

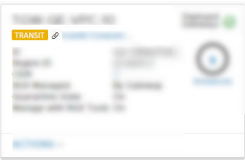
Vous pouvez ajouter des instances dans la liste blanche CSM ou en supprimer. Pour plus d'informations, reportez-vous à [Mise sur liste blanche de machines virtuelles](#).

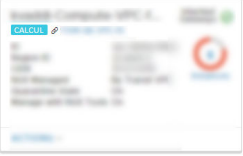
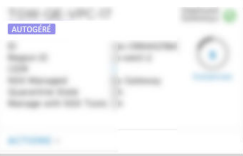
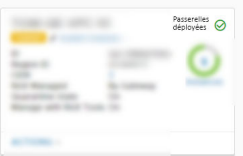
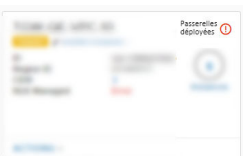
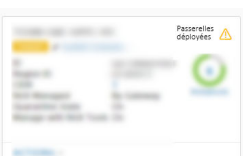
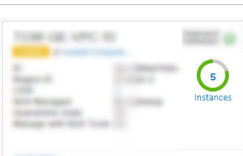
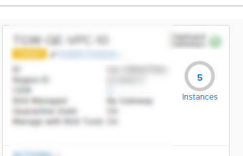
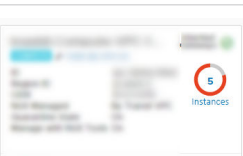
Icônes CSM

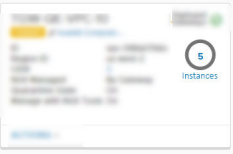

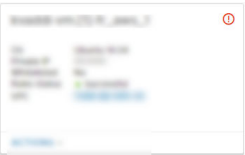
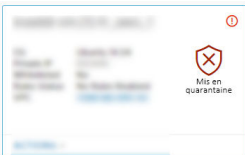
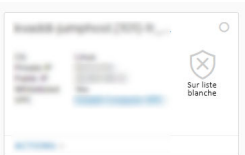
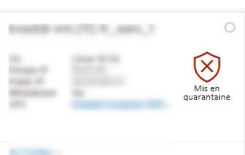
CSM affiche l'état et la santé de vos constructions de cloud public à l'aide d'icônes descriptives.

Note Dans le Mode d'application du Cloud natif : la stratégie de mise en quarantaine est toujours activée et toutes les machines virtuelles sont toujours gérées par NSX. Seuls les états où la stratégie de mise en quarantaine est activée pour les machines virtuelles gérées par NSX s'appliquent dans ce mode.

Dans le Mode d'application NSX : la stratégie de mise en quarantaine peut être désactivée et il est possible d'avoir des machines virtuelles non gérées dans le VPC/VNet. Tous les états pertinents s'appliquent à ce mode.

Section et icône CSM	Description
VPC/VNet	
	VPC/VNet de transit

Section et icône CSM	Description
	VPC/VNet de calcul
	VPC/VNet autogéré
	VPC/VNet affichant des PCG saines
	VPC/VNet affichant des PCG en état d'erreur
	VPC/VNet affichant une PCG en état d'erreur et une autre en bon état.
	VPC/VNet affichant des machines virtuelles gérées par NSX.
	VPC/VNet affichant des machines virtuelles non gérées.
	VPC/VNet affichant des machines virtuelles avec des erreurs.

Section et icône CSM	Description
	VPC/VNet affichant des machines virtuelles hors tension.
Instances	
	Machines virtuelles gérées par NSX sans erreur.
	Machines virtuelles gérées par NSX avec des erreurs et une stratégie de mise en quarantaine désactivée.
	Machines virtuelles gérées par NSX avec des erreurs et une stratégie de mise en quarantaine activée.
	Machines virtuelles non gérées sur liste blanche.
	Machines virtuelles non gérées mises en quarantaine.

Système

Voici les sections sous **Système** :

Système > Paramètres

Ces paramètres 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 du nom d'utilisateur et du mot de passe pour le compte d'administrateur afin de vous connecter à NSX Manager
- CSM doit être installé et vous devez disposer du rôle d'administrateur d'entreprise dans CSM.

Procédure

- 1 Connectez-vous à CSM par le biais d'un navigateur.
- 2 Lorsque vous y êtes invité dans l'Assistant de configuration, cliquez sur **Commencer l'installation**.
- 3 Dans l'écran d'informations d'identification de NSX Manager, entrez les informations suivantes :

Option	Description
Nom d'hôte de NSX Manager	Entrez le nom de domaine complet (FQDN) du dispositif NSX Manager, s'il est disponible. Vous pouvez également entrer l'adresse IP de NSX Manager.
Identifiants de l'administrateur	Entrez un nom d'utilisateur et un mot de passe d'administrateur d'entreprise pour NSX Manager.
Empreinte numérique du responsable	Éventuellement, entrez la valeur de l'empreinte numérique de NSX Manager. Si vous laissez ce champ vide, le système identifie l'empreinte numérique et l'affiche dans l'écran suivant.

- 4 (Facultatif) Si vous n'avez pas fourni de valeur d'empreinte numérique pour NSX Manager, ou si la valeur était incorrecte, l'écran **Vérifier l'empreinte** s'affiche. Cochez la case pour accepter l'empreinte numérique détectée par le système.
- 5 Cliquez sur **Connecter**.

Note Si ce paramètre vous manquait dans l'Assistant de configuration ou si vous souhaitez modifier NSX Manager associé, connectez-vous à CSM, cliquez sur **Système > Paramètres** et cliquez sur **Configurer** sur le panneau intitulé **Nœud NSX associé**.

CSM vérifie l'empreinte numérique du dispositif NSX Manager et établit la connexion.

- 6 (Facultatif) Configurez le serveur proxy. Voir les instructions dans [\(Facultatif\) Configurer les serveurs proxy](#).

(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.
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.

Système> 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.

Système > 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.

Détection des menaces à l'aide de la stratégie de mise en quarantaine de NSX Cloud

La fonctionnalité de stratégie de mise en quarantaine de NSX Cloud fournit un mécanisme de détection des menaces pour vos machines virtuelles de charge de travail gérées par NSX.

La stratégie de mise en quarantaine est implémentée de manière différente dans les deux modes de gestion de machine virtuelle.

Tableau 22-1. Implémentation de la stratégie de mise en quarantaine dans le Mode d'application NSX et le Mode d'application du Cloud natif

Configurations liées à la stratégie de mise en quarantaine	Dans le Mode d'application NSX	Dans le Mode d'application du Cloud natif
État par défaut	Désactivé lors du déploiement de PCG à l'aide de NSX Tools. Vous pouvez l'activer à partir de l'écran de déploiement de PCG ou version ultérieure. Reportez-vous à la section Comment activer ou désactiver la stratégie de mise en quarantaine .	Toujours activé. Ne peut pas être désactivé.
Groupes de sécurité créés automatiquement et uniques pour chaque mode	Le groupe de sécurité <code>vm-underlay-sg</code> est attribué à toutes les machines virtuelles saines gérées par NSX	Les groupes de sécurité <code>nsx-<NSX GUID></code> sont créés pour les machines virtuelles de charge de travail gérées par NSX (et appliquées à celles-ci) qui correspondent à une stratégie de pare-feu distribué dans NSX Manager
Les groupes de sécurité de cloud public créés automatiquement sont communs aux deux modes :	<p>Les groupes de sécurité gw sont appliqués aux interfaces PCG respectives dans AWS et Microsoft Azure.</p> <ul style="list-style-type: none"> ■ gw-mgmt-sg ■ gw-uplink-sg ■ gw-vtep-sg <p>Les groupes de sécurité vm sont appliqués aux machines virtuelles gérées par NSX selon leur état actuel et si la stratégie de mise en quarantaine est activée ou désactivée :</p> <ul style="list-style-type: none"> ■ vm-quarantine-sg dans Microsoft Azure et default dans AWS. <p>Note Dans AWS, le groupe de sécurité <code>default</code> existe déjà. Il n'est pas créé par NSX Cloud.</p>	

Recommandation générale pour le Mode d'application NSX :

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.

Stratégie de mise en quarantaine dans le Mode d'application NSX

L'activation de la stratégie de mise en quarantaine est facultative dans le Mode d'application NSX.

Comment activer ou désactiver la stratégie de mise en quarantaine

Dans le Mode d'application NSX, vous pouvez choisir d'activer la stratégie de mise en quarantaine de deux manières.

La première possibilité d'activer la stratégie de mise en quarantaine est lorsque vous déployez PCG sur un VPC/VNet de transit ou que vous liez un VPC/VNet de calcul à un transit. Déplacez le curseur de la **stratégie de mise en quarantaine sur le VPC/VNet associé** à **Activé** à partir de l'état **Désactivé** par défaut. Reportez-vous à la section **Déployer PCG** du *Guide d'installation de NSX-T Data Center*.

Vous pouvez également activer la stratégie de mise en quarantaine ultérieurement en suivant les étapes.

Conditions préalables

Si vous activez la stratégie de mise en quarantaine après le déploiement ou la liaison à une PCG, vous devez avoir un ou plusieurs VPC/VNet de calcul ou de transit intégrés dans le Mode d'application NSX, que vous avez choisis pour utiliser NSX Tools afin de gérer vos machines virtuelles de charge de travail.

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 de calcul ou de transit.
 - b Si vous utilisez Microsoft Azure, accédez à **Clouds > Azure > VNet**s. Cliquez sur le VNet de calcul ou de transit.
- 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

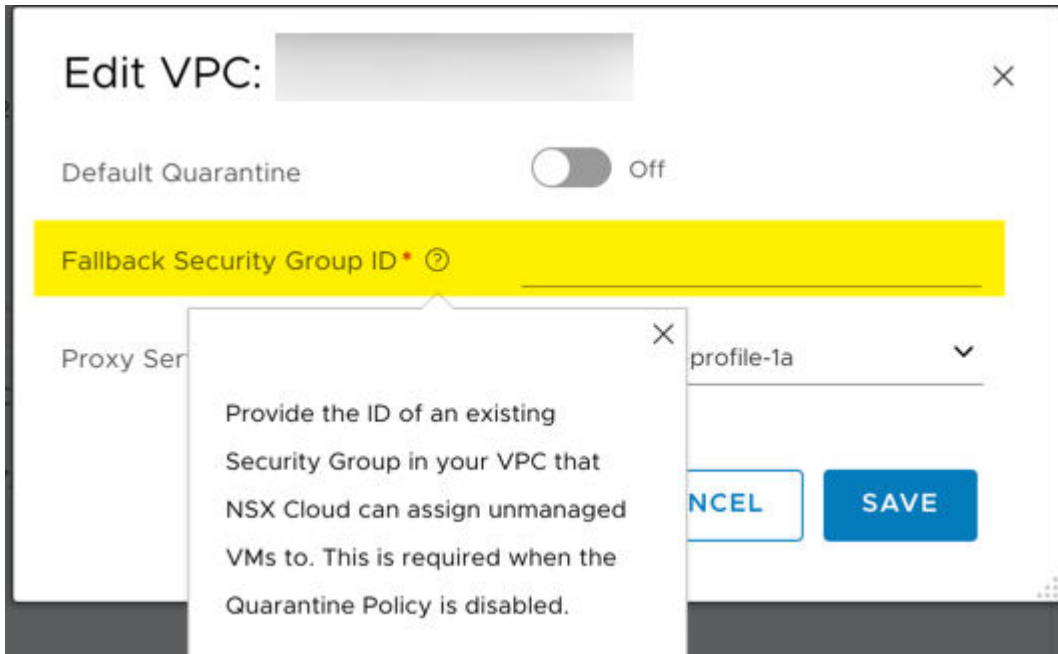
Modifier les configurations.



- 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.



- Toutes les machines virtuelles non gérées 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

NSX Cloud ne gère pas les groupes de sécurité de cloud public de machines virtuelles non balisées lorsque la stratégie de mise en quarantaine est désactivée.

Toutefois, pour les machines virtuelles balisées avec `nsx.network=default` dans le cloud public, NSX Cloud attribue les groupes de sécurité appropriés en fonction de l'état de la machine virtuelle. Ce comportement est semblable à celui constaté lorsque la stratégie de mise en quarantaine est activée, mais les règles dans les groupes de sécurité de quarantaine : `vm-quarantine-sg` dans Microsoft Azure et `default` dans AWS sont moins restrictives. Les modifications manuelles apportées aux groupes de sécurité des machines virtuelles balisées sont annulées sur le groupe de sécurité déterminé par NSX Cloud dans un délai de deux minutes.

Note Si vous ne souhaitez pas que NSX Cloud attribue des groupes de sécurité à vos machines virtuelles gérées par NSX (balisées), mettez-les sur liste blanche dans CSM. Reportez-vous à la section [Mise sur liste blanche de machines virtuelles](#).

Le tableau suivant montre comment NSX Cloud gère les groupes de sécurité de cloud public des machines virtuelles de charge de travail lorsque la stratégie de mise en quarantaine est désactivée.

Tableau 22-2. Attribution par NSX Cloud de groupes de sécurité de cloud public lorsque la stratégie de mise en quarantaine est désactivée

La machine virtuelle est-elle balisée avec <code>nsx.network=default</code> dans le cloud public ?	La machine virtuelle est-elle sur liste blanche ?	Groupe de sécurité de cloud public de la machine virtuelle lorsque la stratégie de mise en quarantaine est désactivée et explication
Balisée	Non sur liste blanche	<ul style="list-style-type: none"> ■ Si la machine virtuelle n'a pas de menaces : <code>vm-underlay-sg</code> ■ Si la machine virtuelle a des menaces potentielles (voir la remarque) : <code>vm-quarantine-sg</code> dans Microsoft Azure ; <code>default</code> dans AWS <p>Note L'attribution de groupes de sécurité de cloud public est déclenchée dans les 90 secondes après l'application de la balise <code>nsx.network=default</code> à vos machines virtuelles de charge de travail. Vous devez toujours installer NSX Tools pour que les machines virtuelles soient gérées par NSX. Jusqu'à ce que NSX Tools soit installé, vos machines virtuelles de charge de travail balisées sont mises en quarantaine.</p>
Non balisée	Non sur liste blanche	Conserve le groupe de sécurité de cloud public existant, car NSX Cloud n'effectue aucune action sur les machines virtuelles non balisées.

Tableau 22-2. Attribution par NSX Cloud de groupes de sécurité de cloud public lorsque la stratégie de mise en quarantaine est désactivée (suite)

La machine virtuelle est-elle balisée avec <i>nsx.network=default</i> dans le cloud public ?	La machine virtuelle est-elle sur liste blanche ?	Groupe de sécurité de cloud public de la machine virtuelle lorsque la stratégie de mise en quarantaine est désactivée et explication
Balisée	Sur liste blanche	Conserve le groupe de sécurité de cloud public existant, car NSX Cloud n'effectue aucune action sur les machines virtuelles sur liste blanche.
Non balisée		

Le tableau suivant montre comment NSX Cloud gère les groupes de sécurité de cloud public des machines virtuelles si la stratégie de mise en quarantaine a été activée avant et qu'elle est maintenant désactivée avec un groupe de sécurité de secours configuré pour gérer les attributions de groupe de sécurité pour ce VPC/VNet.

Tableau 22-3. Attribution par NSX Cloud de groupes de sécurité de cloud public lorsque la stratégie de mise en quarantaine est désactivée après avoir été d'abord activée

La machine virtuelle est-elle balisée avec <i>nsx.network=default</i> dans le cloud public ?	La machine virtuelle est-elle sur liste blanche ?	Groupe de sécurité de cloud public existant de la machine virtuelle lorsque la stratégie de mise en quarantaine est activée	Groupe de sécurité de cloud public de la machine virtuelle une fois que la stratégie de mise en quarantaine est désactivée et qu'un groupe de sécurité de secours est fourni
Non balisée	Non sur liste blanche	vm-quarantine-sg (Microsoft Azure) ou default (AWS)	Cette machine virtuelle se voit attribuer le groupe de sécurité de secours que vous avez fourni lors de la désactivation de la stratégie de mise en quarantaine, car elle n'est pas balisée et n'est donc pas considérée comme étant gérée par NSX. Par conséquent, NSX Cloud rétablit le groupe de sécurité qui a été attribué à cette machine virtuelle lorsque vous désactivez la stratégie de mise en quarantaine.
Balisée	Non sur liste blanche	vm-underlay-sg ou vm-quarantine-sg (Microsoft Azure) ou default (AWS)	Conserve le groupe de sécurité attribué par NSX Cloud, car il est cohérent pour les machines virtuelles balisées dans les modes activé ou désactivé de la mise en quarantaine.
Balisée	Sur liste blanche	Tout groupe de sécurité de cloud public existant	Conserve le groupe de sécurité de cloud public existant, car NSX Cloud n'effectue aucune action sur les machines virtuelles sur liste blanche.
Non balisée			

Note Si vous disposez d'une machine virtuelle sur liste blanche dans tous les groupes de sécurité attribués par NSX Cloud, vous devez la déplacer manuellement vers le groupe de sécurité de secours désigné.

Impact de la stratégie de mise en quarantaine lorsqu'elle est activée

NSX Cloud gère le groupe de sécurité de cloud public de toutes les machines virtuelles de charge de travail dans ce VPC/VNet lorsque la stratégie de mise en quarantaine est activée.

Les modifications manuelles apportées aux groupes de sécurité des machines sont annulées sur le groupe de sécurité attribué par NSX Cloud dans un délai de deux minutes. Si vous ne souhaitez pas que NSX Cloud attribue des groupes de sécurité à vos machines virtuelles, mettez-les sur liste blanche dans CSM. Reportez-vous à la section [Mise sur liste blanche de machines virtuelles](#).

Note Le retrait de la machine virtuelle de la liste blanche entraîne la restauration de cette dernière sur le groupe de sécurité attribué par NSX Cloud.

Tableau 22-4. Attribution par NSX Cloud de groupes de sécurité de cloud public lorsque la stratégie de mise en quarantaine est activée

La machine virtuelle est-elle balisée avec <i>nsx.network=default</i> dans le cloud public ?	La machine virtuelle est-elle sur liste blanche ?	Groupe de sécurité de cloud public de la machine virtuelle lorsque la stratégie de mise en quarantaine est activée et explication
Balisée	Non sur liste blanche	<ul style="list-style-type: none"> ■ Si la machine virtuelle n'a pas de menaces : <code>vm-underlay-sg</code> ■ Si la machine virtuelle a des menaces potentielles (voir la remarque) : <code>vm-quarantine-sg</code> dans Microsoft Azure ; <code>default</code> dans AWS <p>Note L'attribution de groupes de sécurité de cloud public est déclenchée dans les 90 secondes après l'application de la balise <code>nsx.network=default</code> à vos machines virtuelles de charge de travail. Vous devez toujours installer NSX Tools pour que les machines virtuelles soient gérées par NSX. Jusqu'à ce que NSX Tools soit installé, vos machines virtuelles de charge de travail balisées sont mises en quarantaine.</p>
Non balisée	Non sur liste blanche	<code>vm-quarantine-sg</code> dans Microsoft Azure ; <code>default</code> dans AWS. Les machines virtuelles non balisées sont considérées comme non gérées et, en conséquence, mises en quarantaine par NSX Cloud.

Tableau 22-4. Attribution par NSX Cloud de groupes de sécurité de cloud public lorsque la stratégie de mise en quarantaine est activée (suite)

La machine virtuelle est-elle balisée avec <i>nsx.network=default</i> dans le cloud public ?	La machine virtuelle est-elle sur liste blanche ?	Groupe de sécurité de cloud public de la machine virtuelle lorsque la stratégie de mise en quarantaine est activée et explication
Balisée	Sur liste blanche	Conserve le groupe de sécurité de cloud public existant, car NSX Cloud n'effectue aucune action sur les machines virtuelles sur liste blanche.
Non balisée		

Le tableau suivant illustre l'incidence sur les attributions de groupe de sécurité si la stratégie de mise en quarantaine a été d'abord désactivée, puis activée :

Tableau 22-5. Attribution par NSX Cloud de groupes de sécurité de cloud public lorsque la stratégie de mise en quarantaine est activée après avoir été d'abord désactivée

La machine virtuelle est-elle balisée avec <i>nsx.network=default</i> dans le cloud public ?	La machine virtuelle est-elle sur liste blanche ?	Groupe de sécurité de cloud public existant de la machine virtuelle lorsque la stratégie de mise en quarantaine est désactivée	Groupe de sécurité de cloud public de la machine virtuelle après l'activation de la stratégie de mise en quarantaine
Non balisée	Non sur liste blanche	Tout groupe de sécurité de cloud public existant	vm-quarantine-sg (Microsoft Azure) ou default (AWS)
Balisée	Non sur liste blanche	vm-underlay-sg ou vm-quarantine-sg (Microsoft Azure) ou default (AWS)	Conserve le groupe de sécurité attribué par NSX Cloud qui est cohérent pour les machines virtuelles balisées dans les modes activé ou désactivé de la mise en quarantaine.
Balisée	Sur liste blanche	Tout groupe de sécurité de cloud public existant.	Conserve le groupe de sécurité de cloud public existant, car NSX Cloud n'effectue aucune action sur les machines virtuelles sur liste blanche.
Non balisée			

Stratégie de mise en quarantaine dans le Mode d'application du Cloud natif

La stratégie de mise en quarantaine est toujours activée dans le Mode d'application du Cloud natif.

Tableau 22-6. Attribution de groupes de sécurité de cloud public dans le Mode d'application du Cloud natif

La machine virtuelle fait-elle partie d'une stratégie de sécurité NSX-T valide ?	La machine virtuelle est-elle sur liste blanche ?	Groupe de sécurité de cloud public de la machine virtuelle et explication
Oui, la machine virtuelle correspond à une stratégie de sécurité NSX-T valide	Non sur liste blanche	Groupe de sécurité de cloud public créé par NSX Cloud nommé <code>nsx-{NSX-GUID}</code> , qui est le groupe de sécurité de cloud public correspondant pour la stratégie de sécurité NSX-T.
Non, la machine virtuelle ne dispose pas d'une stratégie de pare-feu NSX-T valide	Non sur liste blanche	<code>vm-quarantine-sg</code> dans Microsoft Azure ou <code>default</code> dans AWS, car il s'agit du comportement de détection des menaces de NSX Cloud. Dans le Mode d'application du Cloud natif, les groupes de sécurité créés par NSX Cloud <code>vm-quarantine-sg</code> dans Microsoft Azure ou <code>default</code> dans AWS imitent la stratégie de sécurité de cloud public par défaut. Note Dans CSM, la machine virtuelle affiche un état d'erreur.
Oui, la machine virtuelle dispose d'une stratégie de sécurité NSX-T valide	Sur liste blanche	Conserve le groupe de sécurité de cloud public existant, car NSX Cloud n'effectue aucune action sur les machines virtuelles sur liste blanche.
Non, la machine virtuelle ne dispose pas d'une stratégie de sécurité NSX-T valide		

Mise sur liste blanche de machines virtuelles

La mise sur liste blanche est une option disponible depuis CSM pour toutes les machines virtuelles de charge de travail de votre inventaire de cloud public.

La mise sur liste blanche fonctionne dans les deux modes de gestion de machine virtuelle : Mode d'application NSX et Mode d'application du Cloud natif.

Pourquoi mettre des machines virtuelles sur liste blanche ?

- Dans le Mode d'application NSX : si la stratégie de mise en quarantaine est activée et que vous devez vérifier des stratégies DFW spécifiques avec des applications existantes sur la machine virtuelle, mettez la machine virtuelle sur liste blanche avant de l'intégrer à NSX Cloud.
- Dans le Mode d'application NSX ou le Mode d'application du Cloud natif :
 - Si vous disposez de machines virtuelles avec des erreurs et que vous souhaitez y accéder pour résoudre les erreurs, mettez-les sur liste blanche afin de pouvoir les sortir de l'état de mise en quarantaine et d'utiliser les outils de débogage si nécessaire.
 - Mettez sur liste blanche les machines virtuelles de votre inventaire de cloud public que vous ne voulez pas que NSX-T gère, par exemple le redirecteur DNS, le serveur proxy, etc.

Comment ajouter des machines virtuelles à la liste blanche ou les supprimer de celle-ci

Suivez ces instructions pour ajouter des machines virtuelles à la liste blanche ou les supprimer de celle-ci.

Conditions préalables

Vous devez ajouter un ou plusieurs comptes de cloud public à CSM.

Procédure

- 1 Connectez-vous à CSM à l'aide d'un compte d'administrateur d'entreprise et accédez à votre compte de cloud public.
 - a Si vous utilisez AWS, accédez à **Clouds > AWS > VPC > Instances**.
 - b Si vous utilisez Microsoft Azure, accédez à **Clouds > Azure > VNet > Instances**.
- 2 Si vous êtes en mode en mosaïque, passez en mode Grille en cliquant sur le sélecteur de mode dans le coin droit de la vue Instances.
- 3 Sélectionnez les machines virtuelles (instances) que vous souhaitez ajouter à la liste blanche ou supprimer de celle-ci.
- 4 Cliquez sur **Actions** et sélectionnez **Ajouter à la liste blanche** ou **Supprimer de la liste blanche**.
- 5 Revenez à l'onglet Comptes, sélectionnez la vignette du compte et cliquez sur **Actions > Resynchroniser un compte**.

Résultats

Chaque machine virtuelle ajoutée à la liste blanche reste dans le groupe de sécurité auquel elle a été attribuée avant sa mise sur liste blanche. Vous pouvez désormais appliquer un autre groupe de sécurité à la machine virtuelle, le cas échéant. NSX Cloud ignore les machines virtuelles sur liste blanche, quel que soit l'état de la stratégie de mise en quarantaine.

Si vous supprimez une machine virtuelle de la liste blanche dans le Mode d'application du Cloud natif ou que vous supprimez une machine virtuelle gérée par NSX de la liste blanche dans le Mode d'application NSX, NSX Cloud commence à attribuer des groupes de sécurité à cette machine virtuelle en fonction de son état.

Mode d'application NSX

Dans le Mode d'application NSX, c'est-à-dire en utilisant NSX Tools, vous devez d'abord intégrer des machines virtuelles en les marquant dans le cloud public et en installant NSX Tools sur ces machines virtuelles, avant de commencer à les gérer à l'aide de NSX-T Data Center.

Systèmes d'exploitation actuellement pris en charge pour les machines virtuelles de charge de travail

Il s'agit de la liste des systèmes d'exploitation actuellement pris en charge par NSX Cloud pour vos machines virtuelles de charge de travail dans le Mode d'application NSX.

Les systèmes d'exploitation suivants sont actuellement pris en charge :

Note Reportez-vous à la section Problèmes connus de NSX Cloud dans le document *Notes de mise à jour de NSX-T Data Center* pour les exceptions. Pour les systèmes d'exploitation pris en charge, il est supposé que vous utilisez les versions de noyau Linux standard. Les images du Marketplace de cloud public avec des noyaux personnalisés, par exemple, le noyau Linux en amont avec des sources modifiées, ne sont pas prises en charge.

- Red Hat Enterprise Linux (RHEL) 7.2, 7.3, 7.4, 7.5, 7.6
- CentOS 7.2, 7.3, 7.4, 7.5, 7.6

Note Le noyau RHEL EUS (Extended Update Support) dans RHEL et CentOS n'est pas pris en charge.

Note Seules les images du Marketplace CentOS dont les versions de distribution correspondent à la version mineure attendue pour leur noyau sont prises en charge pour NSX Cloud. Par exemple, les versions de distribution et la version correspondante de leur noyau sont supposées être les suivantes :

Version RHEL	Version du noyau
RHEL 7.6	3.10.0-957
RHEL 7.5	3.10.0-862
RHEL 7.4	3.10.0-693
RHEL 7.3	3.10.0-514
RHEL 7.2	3.10.0-327

- Ubuntu 14.04, 16.04, 18.04
- Microsoft Windows Server 2016 - Version basée sur les services, Expérience utilisateur (1709, 1803, 1809)
- Microsoft Windows Server 2019 Datacenter
- Microsoft Windows Server 2012 R2
- Microsoft Windows 10 versions 1809, 1803 et 1709 (uniquement pris en charge dans Microsoft Azure dans la version actuelle de NSX Cloud)

Intégration de machines virtuelles dans le Mode d'application NSX

Reportez-vous à ce workflow pour obtenir un aperçu des étapes impliquées dans l'intégration et la gestion des machines virtuelles de charge de travail à partir de votre cloud public dans le Mode d'application NSX.

Tableau 22-7. Workflow de jour-n pour l'intégration de vos machines virtuelles de charge de travail dans NSX Cloud

Tâche	Instructions
<input type="checkbox"/> Balisez les machines virtuelles de charge de travail avec la paire clé-valeur <code>nsx.network=default</code> .	Suivez les instructions fournies dans la documentation de votre cloud public pour le balisage de machines virtuelles de charge de travail.
<input type="checkbox"/> Installez NSX Tools sur vos machines virtuelles de charge de travail Windows ou Linux.	Reportez-vous à la rubrique Installer NSX Tools
Note Si la fonctionnalité Installer NSX Tools automatiquement est activée dans CSM pour les VNet Microsoft Azure, NSX Tools est automatiquement installé.	
<input type="checkbox"/> (Facultatif) Dans CSM, supprimez de la liste blanche toutes les machines virtuelles que vous souhaitez inclure dans la gestion NSX.	Reportez-vous à la section Comment ajouter des machines virtuelles à la liste blanche ou les supprimer de celle-ci .
Note La liste des utilisateurs est une étape manuelle recommandée dans le cadre du workflow de jour-0 dès que vous ajoutez votre inventaire de cloud public dans CSM. Vous n'avez pas besoin de supprimer des machines virtuelles de la liste blanche si vous n'en avez ajouté aucune.	

Baliser des machines virtuelles dans le cloud public

Appliquez la balise `nsx.network=default` aux machines virtuelles que vous souhaitez gérer à l'aide de NSX-T Data Center.

Procédure

- 1 Connectez-vous à votre compte de cloud public et accédez au VPC/VNet sur lequel vous souhaitez que les machines virtuelles de charge de travail soient gérées par NSX-T Data Center.
- 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.

```
Key: nsx.network
Value: default
```

Note Appliquez cette balise au niveau de la machine virtuelle.

Résultats

Vous avez peut-être déjà intégré les VPC/VNet sur lesquels vous avez appliqué les balises `nsx.network=default` aux machines virtuelles de charge de travail. Vous pouvez également intégrer ces VPC/VNet après avoir appliqué la balise. Lorsque l'intégration du VPC/VNet réussit, les machines virtuelles de charge de travail sont considérées comme étant gérées par NSX.

Étape suivante

Installez NSX Tools sur ces machines virtuelles. Reportez-vous à la section [Installer NSX Tools](#).

Si vous utilisez Microsoft Azure, vous avez la possibilité d'installer automatiquement NSX Tools sur les machines virtuelles balisées. Reportez-vous à [Installer NSX Tools automatiquement](#) pour plus de détails.

Installer NSX Tools

Installez NSX Tools sur vos machines virtuelles de charge de travail.

Plusieurs options sont disponibles pour l'installation de NSX Tools :

- Téléchargez et installez NSX Tools sur des machines virtuelles de charge de travail individuelles. Les machines virtuelles Linux et Windows présentent quelques différences.
- Utilisez des images répliquables sur lesquelles NSX Tools est installé à l'aide de la méthode prise en charge de votre cloud public, par exemple, créer un AMI dans AWS ou une image gérée dans Microsoft Azure.
- AWS uniquement : lorsque vous lancez des machines virtuelles, fournissez l'emplacement de téléchargement et la commande d'installation de NSX Tools dans **Données utilisateur**.
- Microsoft Azure uniquement : activez l'installation automatique de NSX Tools lors du déploiement de PCG dans un réseau virtuel Microsoft Azure ou lors de la liaison à un VNet de transit, ou en modifiant la configuration d'un VNet de transit/calcul.

Note Si vous disposez de machines virtuelles de charge de travail approuvées sur lesquelles vous souhaitez installer NSX Tools, assurez-vous que les ports suivants sont ouverts dans les groupes de sécurité que vous avez attribués à de telles machines virtuelles :

- UDP 6081 entrant : pour les paquets de données de superposition. Il doit être autorisé pour l'adresse IP (interface eth1) VTEP de la PCG (actif/veille).
 - TCP 5555 sortant : pour les paquets de contrôle. Il doit être autorisé pour l'adresse IP (interface eth0) de gestion de la PCG (actif/veille).
 - TCP 8080 : pour l'installation/la mise à niveau de l'adresse IP de gestion de la PCG.
 - TCP 80 : pour le téléchargement des dépendances tierces lors de l'installation de NSX Tools.
 - UDP 67, 68 : pour les paquets DHCP.
 - UDP 53 : pour la résolution DNS.
-

Installer NSX Tools sur des machines virtuelles Linux

Suivez ces instructions pour installer NSX Tools sur vos machines virtuelles de charge de travail Linux.

Reportez-vous à [Systèmes d'exploitation actuellement pris en charge pour les machines virtuelles de charge de travail](#) pour obtenir la liste des distributions Linux actuellement prises en charge.

Note Pour vérifier le total de contrôle de ce script, accédez à **Téléchargements VMware > Pilotes et outils > Scripts NSX Cloud**.

Conditions préalables

Les commandes suivantes sont nécessaires pour exécuter le script d'installation de NSX Tools :

- **wget**
- **nslookup**
- **dmidecode**

Procédure

- 1 Connectez-vous à CSM et accédez à votre cloud public :
 - a Si vous utilisez AWS, accédez à **Clouds > AWS > VPC**. Cliquez sur un VPC de transit ou de calcul.
 - b Si vous utilisez Microsoft Azure, accédez à **Clouds > Azure > VNet**. Cliquez sur le VNet sur lequel un ou deux PCG sont déployés et en cours d'exécution.

Remarque : le VPC/VNet de transit est l'endroit où une ou deux PCG sont déployées et en cours d'exécution. Le VPC/VNet de calcul est celui lié à un VPC/VNet de transit et qui peut utiliser les instances de PCG qui y sont déployées.

- 2 À partir de la section **Téléchargement et installation de NSX Tools** de l'écran, notez l'**emplacement de téléchargement** et la **commande d'installation** sous **Linux**.

Note Pour les VNet, le suffixe DNS dans la commande d'installation est généré dynamiquement pour correspondre aux paramètres DNS que vous sélectionnez lors du déploiement de PCG. Pour les VNet de transit, le paramètre `-dnsServer <dns-server-ip>` est facultatif. Pour des VNet de calcul, vous devez fournir l'adresse IP du redirecteur DNS pour terminer cette commande.

- 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`.

Note Pour vérifier le total de contrôle de ce script, accédez à **Téléchargements VMware > Pilotes et outils > Scripts NSX Cloud**.

- 5 Modifiez les autorisations sur le script d'installation pour le rendre exécutable, le cas échéant, et exécutez-le :

```
$ chmod +x install_nsx_vm_agent.sh && sudo ./install_nsx_vm_agent.sh
```

Remarque : sur Red Hat Enterprise Linux et ses dérivés, SELinux n'est pas pris en charge. Pour installer NSX Tools, désactivez SELinux.

- 6 Vous perdrez la connectivité avec votre machine virtuelle Linux une fois l'installation de NSX Tools commencée. Des messages semblables à ceux-ci s'affichent à l'écran : `Installation completed!!! Starting NSX Agent service. SSH connection will now be lost..` Pour terminer le processus d'intégration, reconnectez-vous à votre machine virtuelle.

Résultats

NSX Tools est installé sur votre machine virtuelle de charge de travail.

Note

- Une fois que NSX Tools a été installé avec succès, le port 8888 apparaît comme étant ouvert sur la machine virtuelle de charge de travail, 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. Vous pouvez accéder aux machines virtuelles de charge de travail sur le port 8888 à l'aide d'un hôte de saut s'il est également dans le même VPC que les machines virtuelles de charge de travail auxquelles vous souhaitez accéder.
- Le script utilise `eth0` comme interface par défaut.

Étape suivante

[Gestion des machines virtuelles dans le Mode d'application NSX](#)

Installer NSX Tools sur des machines virtuelles Windows

Suivez ces instructions pour installer NSX Tools sur votre VM de charge de travail Windows.

Reportez-vous à la section [Systèmes d'exploitation actuellement pris en charge pour les machines virtuelles de charge de travail](#) pour obtenir la liste des versions de Microsoft Windows prises en charge actuellement.

Note Pour vérifier le total de contrôle de ce script, accédez à [Téléchargements VMware > Pilotes et outils > Scripts NSX Cloud](#).

Procédure

- 1 Connectez-vous à CSM et accédez à votre cloud public :
 - a Si vous utilisez AWS, accédez à **Clouds > AWS > VPC**. Cliquez sur un VPC de transit ou de calcul.
 - b Si vous utilisez Microsoft Azure, accédez à **Clouds > Azure > VNets**. Cliquez sur le VNet sur lequel un ou deux PCG sont déployés et en cours d'exécution.

Remarque : le VPC/VNet de transit est l'endroit où une ou deux PCG sont déployées et en cours d'exécution. Le VPC/VNet de calcul est celui lié à un VPC/VNet de transit et qui peut utiliser les PCG qui y sont déployées.

- 2 À partir de la section **Téléchargement et installation de NSX Tools** de l'écran, notez l'**emplacement de téléchargement** et la **commande d'installation** sous **Windows**.

Note Pour les VNet, le suffixe DNS dans la commande d'installation est généré dynamiquement pour correspondre aux paramètres DNS que vous choisissez lors du déploiement de PCG. Pour les VNet de transit, le paramètre `-dnsServer <dns-server-ip>` est facultatif. Pour des VNet de calcul, vous devez fournir l'adresse IP du redirecteur DNS pour terminer cette commande.

- 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*.

Note Pour vérifier le total de contrôle de ce script, accédez à **Téléchargements VMware > Pilotes et outils > Scripts NSX Cloud**.

Remarque :

- 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 Tools a été installé correctement.

Note Le script considère l'interface réseau principale comme la valeur par défaut.

Étape suivante

Gestion des machines virtuelles dans le Mode d'application NSX

Générer des images répliquables

Vous pouvez générer une AMI dans AWS ou une image gérée dans Microsoft Azure sur une machine virtuelle équipée de NSX Agent.

Avec cette fonctionnalité, vous pouvez lancer plusieurs machines virtuelles avec l'agent configuré et en cours d'exécution.

Deux méthodes de génération d'une AMI/image gérée (« image » dans le reste de cette rubrique) d'une machine virtuelle équipée de NSX Agent sont disponibles :

- **Générer l'image avec un NSX Agent non configuré** : vous pouvez générer une image à partir d'une machine virtuelle équipée de NSX Agent non configuré à l'aide de l'option `-noStart`. Cette option permet l'extraction et l'installation du module de NSX Agent, mais les NSX Services ne sont pas démarrés. Par ailleurs, aucune configuration NSX, comme la génération de certificats, n'est effectuée.
- **Générer l'image après la suppression de configurations de NSX Agent existant** : vous pouvez supprimer des configurations d'une machine virtuelle gérée par NSX existante et utiliser cette dernière pour la génération d'une image.

Génération d'une AMI avec NSX Agent non configuré

Vous pouvez générer une AMI d'une machine virtuelle avec NSX Agent installé sur la machine, mais non configuré.

Pour générer une image à partir d'une machine virtuelle équipée de NSX Agent en utilisant l'option `-noStart`, procédez comme suit :

Procédure

- 1 Copiez-collez la commande d'installation de NSX Agent à partir de CSM. Reportez-vous aux instructions données dans la section [Installer NSX Tools](#).

- a Modifiez la commande pour Windows comme suit :

```
c:\> powershell -file 'nsx_install.ps1' -operation install -dnsSuffix <> -noStart true
```

- b Modifiez la commande pour Linux comme suit :

```
$ chmod +x install_nsx_vm_agent.sh && sudo ./install_nsx_vm_agent.sh --no-start
```

- 2 Accédez à cette machine virtuelle dans votre cloud public et créez une image.

Génération d'une image après la suppression des configurations de NSX Agent existantes

Vous pouvez générer une image d'une machine virtuelle sur laquelle NSX Agent est configuré.

Pour supprimer des configurations d'une machine virtuelle gérée par NSX et utiliser cette dernière pour générer des images, procédez comme suit :

Procédure

1 Suppression des configurations de NSX Agent d'une machine virtuelle Linux ou Windows :

- a Connectez-vous à la machine virtuelle de charge de travail en utilisant de préférence un hôte de saut.
- b Ouvrez l'interface de ligne de commande NSX-T :

```
sudo nsxcli
```

- c Entrez les commandes suivantes :

```
hostname> set debug
hostname> clear nsx-vm-agent state
```

2 Recherchez cette machine virtuelle dans votre cloud public et créez une image.

Installer NSX Tools automatiquement

Actuellement pris en charge uniquement pour Microsoft Azure.

Dans Microsoft Azure, si les critères suivants sont remplis, NSX Tools est installé automatiquement :

- Les extensions de machine virtuelle Azure sont installées sur les machines virtuelles dans le VNet ajouté dans NSX Cloud. Pour plus de détails, reportez-vous à la [Documentation Microsoft Azure sur les extensions de machine virtuelle](#).
- Le groupe de sécurité appliqué aux machines virtuelles dans Microsoft Azure doit permettre l'installation de NSX Tools. Si la stratégie de mise en quarantaine est activée, vous pouvez mettre sur liste blanche les machines virtuelles dans CSM avant l'installation et les supprimer de la liste blanche après l'installation.
- Machines virtuelles balisées avec la clé `nsx.network` et la valeur `default`.

Pour activer cette fonctionnalité :

- 1 Accédez à **Clouds > Azure > VNets**.
- 2 Sélectionnez le VNet sur les machines virtuelles dont vous souhaitez installer automatiquement CSM.

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 de VNet et cliquez sur **ACTIONS >**

Modifier la configuration.



- Si vous êtes dans l'onglet VNet, cliquez sur l'icône ACTIONS pour accéder à **Modifier les configurations.**



4 Déplacez le curseur en regard de **Installer NSX Tools automatiquement** sur la position **ACTIVÉ**.

Note Si l'installation de NSX Tools échoue, procédez comme suit :

- 1 Connectez-vous au portail Microsoft Azure et accédez à la machine virtuelle sur laquelle l'installation de NSX Tools a échoué.
- 2 Accédez aux extensions de la machine virtuelle et désinstallez l'extension nommée `VMwareNsxAgentInstallCustomScriptExtension`.
- 3 Supprimez la balise `nsx.network=default` de cette machine virtuelle.
- 4 Ajoutez de nouveau la balise `nsx.network=default` à cette machine virtuelle.

Dans un délai d'environ trois minutes, NSX Tools est installé sur cette machine virtuelle.

Installer NSX Tools avec des données utilisateur dans AWS

Lors du lancement d'une nouvelle machine virtuelle de charge de travail dans un VPC AWS, vous pouvez installer NSX Tools en fournissant les instructions de téléchargement et d'installation de NSX Tools dans le champ Données utilisateur.

Copiez les instructions de téléchargement et d'installation de NSX Tools depuis CSM et collez-les dans les données utilisateur lors du lancement d'une nouvelle machine virtuelle de charge de travail.

Procédure

- 1 Connectez-vous à la console AWS et démarrez le processus de lancement d'une nouvelle machine virtuelle de charge de travail.

2 Dans une autre fenêtre de navigateur, connectez-vous à CSM.

a Accédez à **Clouds > AWS > VPC**

Note Le VPC/VNet de transit est l'endroit où une ou deux PCG sont déployées et en cours d'exécution. Le VPC/VNet de calcul est celui lié à un VPC/VNet de transit et qui peut utiliser les PCG qui y sont déployées.

b Cliquez sur un VPC de transit ou de calcul.

c Dans la section **Téléchargement et installation de NSX Tools** de l'écran, copiez l'**emplacement de téléchargement** et la **commande d'installation de Linux** ou **Windows** en fonction du système d'exploitation que vous utilisez pour votre machine virtuelle de charge de travail.

3 Dans AWS, dans les étapes de lancement d'une nouvelle instance de machine virtuelle de charge de travail, collez l'emplacement de téléchargement et la commande d'installation sous forme de **Texte** dans Données utilisateur dans la section Détails avancés.

Résultats

La machine virtuelle de charge de travail est lancée et NSX Tools y est installé automatiquement.

Désinstallation de NSX Tools

Utilisez ces commandes spécifiques au système d'exploitation pour désinstaller NSX Tools.

Désinstallation de NSX Tools à partir d'une machine virtuelle Windows

Note Pour voir les autres options disponibles pour le script d'installation, utilisez `-help`.

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
```

Désinstallation de NSX Tools à partir d'une machine virtuelle Linux

Note Pour voir les autres options disponibles pour le script d'installation, utilisez `--help`.

1 Connectez-vous à distance à la machine virtuelle via une connexion SSH.

2 Exécutez le script d'installation avec l'option `uninstall` :

```
sudo ./install_nsx_vm_agent.sh --uninstall
```

Groupes de sécurité après l'intégration dans le Mode d'application NSX

Les configurations de groupe de sécurité suivantes ont lieu automatiquement :

Si la stratégie de mise en quarantaine est activée :

- Les machines virtuelles saines gérées par NSX sont déplacées vers le groupe de sécurité `vm-underlay-sg` du cloud public.
- Les machines virtuelles non gérées ou les machines virtuelles gérées par NSX avec des erreurs sont déplacées vers le groupe de sécurité `default` dans AWS et vers le groupe de sécurité réseau `vm-quarantine-sg` dans Microsoft Azure.
- Les machines virtuelles sur liste blanche ne sont pas concernées.

Si la stratégie de mise en quarantaine est désactivée :

- Les machines virtuelles saines gérées par NSX sont déplacées vers le groupe de sécurité `vm-underlay-sg` du cloud public.
- Les machines virtuelles gérées par NSX avec des erreurs sont déplacées vers le groupe de sécurité `default` dans AWS et vers le groupe de sécurité réseau `vm-quarantine-sg` dans Microsoft Azure.
- Les machines virtuelles non gérées et les machines virtuelles sur liste blanche ne sont pas concernées.

Gestion des machines virtuelles dans le Mode d'application NSX

Suivez ces étapes pour commencer à gérer les machines virtuelles intégrées dans le Mode d'application NSX.

Tableau 22-8. Workflow de microsegmentation pour vos machines virtuelles de charge de travail gérées par NSX dans le Mode d'application NSX

Tâche	Instructions
<input type="checkbox"/> Pour autoriser l'accès entrant aux machines virtuelles de charge de travail, créez des règles de pare-feu distribué (DFW), si nécessaire.	Reportez-vous à la section Stratégie de connectivité par défaut pour les machines virtuelles de charge de travail gérées par NSX dans le Mode d'application NSX .
<input type="checkbox"/> Regroupez vos machines virtuelles de charge de travail à l'aide de balises de cloud public ou de balises NSX-T Data Center et configurez la microsegmentation.	Reportez-vous à la section Configurer la microsegmentation pour les machines virtuelles de charge de travail dans le Mode d'application NSX . Reportez-vous également à la section Regrouper les machines virtuelles à l'aide de NSX-T Data Center et de balises de cloud public .

Stratégie de connectivité par défaut pour les machines virtuelles de charge de travail gérées par NSX dans le Mode d'application NSX

Lorsque vous déployez la PCG sur votre réseau VPC/VNet de transit ou que vous liez un VPC/VNet de calcul à un transit, NSX Cloud crée des stratégies de sécurité et des règles DFW par défaut pour les machines virtuelles de charge de travail gérées par NSX.

Les deux règles sans état sont prévues pour l'accès DHCP et n'affectent pas l'accès à vos machines virtuelles de charge de travail.

Les deux règles avec état sont les suivantes :

Règles DFW créées par NSX Cloud dans le cadre d'une stratégie : <code>cloud-stateful-cloud-<VPC/VNet ID></code>	Propriétés
<code>cloud-<VPC/VNet ID>-managed</code>	Permet d'accéder aux machines virtuelles d'un même réseau VPC/VNet.
<code>cloud-<VPC/VNet ID>-inbound</code>	Bloque l'accès aux machines virtuelles gérées par NSX à partir de n'importe quel emplacement extérieur au réseau VPC/VNet.

Note Ne modifiez aucune des règles par défaut.

Vous pouvez créer une copie de la règle de connexion entrante existante, définir les sources et destinations, et appliquer le paramètre **Autoriser**. Positionnez la règle **Autoriser** au-dessus de la règle par défaut **Refuser**. Vous pouvez également ajouter de nouvelles règles et stratégies. Reportez-vous à la section [Ajouter un pare-feu distribué](#) pour obtenir des instructions.

Configurer la microsegmentation pour les machines virtuelles de charge de travail dans le Mode d'application NSX

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 gérées par NSX, procédez comme suit :

- 1 Créez des groupes 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 [Ajouter un groupe](#).

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

Note Les règles DFW dépendent des balises attribuées aux machines virtuelles. Comme ces balises peuvent être modifiées par toute personne disposant des autorisations de cloud public appropriées, NSX-T Data Center suppose que ces utilisateurs sont dignes de confiance. L'administrateur réseau du cloud public doit s'assurer et auditer que les machines virtuelles sont correctement balisées à tout moment.

- 2 Créez une stratégie et une règle de pare-feu distribué est-ouest et appliquez-les au groupe que vous avez créé. Reportez-vous à la section [Ajouter un pare-feu distribué](#).

Cette microsegmentation prend effet lorsque l'inventaire est manuellement resynchronisé à partir de CSM ou dans un délai d'environ trois minutes lorsque les modifications sont intégrées dans CSM à partir de votre cloud public.

Mode d'application du Cloud natif

Dans le Mode d'application du Cloud natif, toutes vos machines virtuelles de charge de travail sont automatiquement gérées par NSX. Suivez le workflow décrit ici pour commencer à gérer ces machines virtuelles à l'aide de NSX-T Data Center.

Note Tous les systèmes d'exploitation sont pris en charge pour vos machines virtuelles de charge de travail dans le Mode d'application du Cloud natif.

Gestion des machines virtuelles dans le Mode d'application du Cloud natif

Dans le Mode d'application du Cloud natif, NSX Cloud utilise des groupes NSX-T Data Center et des règles de pare-feu distribué pour créer des groupes de sécurité d'application et des groupes de sécurité réseau correspondants dans Microsoft Azure et des groupes de sécurité dans AWS.

Toutes les machines virtuelles de charge de travail de vos VPC/VNet intégrées dans le Mode d'application du Cloud natif sont gérées par NSX.

Suivez ce workflow :

Tableau 22-9. Workflow de microsegmentation pour vos machines de charge de travail dans le Mode d'application du Cloud natif

Tâche	Instructions
<input type="checkbox"/> Créer un ou plusieurs groupes dans NSX Manager pour inclure les machines virtuelles de charge de travail de votre cloud public.	Reportez-vous à la section Configurer la microsegmentation pour les machines virtuelles de charge de travail dans le Mode d'application du Cloud natif
<input type="checkbox"/> Créer une ou plusieurs stratégies de sécurité dans NSX Manager qui s'appliquent au(x) groupe(s) que vous avez créé(s) pour vos machines virtuelles de charge de travail de cloud public.	
<input type="checkbox"/> Supprimer les machines virtuelles de charge de travail de la liste blanche dans CSM si vous voulez qu'elles soient gérées par les stratégies de sécurité de NSX-T.	
<input type="checkbox"/> Resynchroniser votre compte cloud public dans CSM.	
<input type="checkbox"/> À partir de votre VPC/VNet, passez à la vue de détails dans CSM pour résoudre les problèmes de stratégies de sécurité en cas d'erreurs.	Reportez-vous à la section Limites actuelles et erreurs courantes

Configurer la microsegmentation pour les machines virtuelles de charge de travail dans le Mode d'application du Cloud natif

Reportez-vous à ce workflow pour configurer la stratégie de sécurité dans NSX Manager des machines virtuelles de charge de travail dans le Mode d'application du Cloud natif, c'est-à-dire en n'installant pas NSX Tools sur les machines virtuelles de charge de travail.

Conditions préalables

Vous devez disposer d'un VPC/VNet de calcul ou de transit dans le Mode d'application du Cloud natif.

Procédure

- 1 Dans NSX Manager, modifiez ou créez des groupes pour les machines virtuelles de charge de travail ; par exemple, les noms de machines virtuelles commençant par web, app ou db, pourraient être trois groupes distincts. Reportez-vous à la section [Ajouter un groupe](#) pour obtenir des instructions. Reportez-vous à la section [Regrouper les machines virtuelles à l'aide de NSX-T Data Center et de balises de cloud public](#) pour des informations sur l'utilisation de balises de cloud public afin de créer des groupes pour vos machines virtuelles de charge de travail.

Les machines virtuelles de charge de travail qui correspondent aux critères sont ajoutées au groupe. Celles qui ne correspondent à aucun critère de regroupement sont placées dans le groupe de sécurité `default` dans AWS et dans le groupe de sécurité réseau `vm-quarantine-sg` dans Microsoft Azure.

Note Vous ne pouvez pas utiliser les groupes créés automatiquement par NSX Cloud.

Note Les règles DFW dépendent des balises attribuées aux machines virtuelles. Comme ces balises peuvent être modifiées par toute personne disposant des autorisations de cloud public appropriées, NSX-T Data Center suppose que ces utilisateurs sont dignes de confiance. L'administrateur réseau du cloud public doit s'assurer et auditer que les machines virtuelles sont correctement balisées à tout moment.

- 2 Dans NSX Manager, créez des règles de pare-feu distribué (DFW) avec les groupes dans les champs **Source**, **Destination** ou **Appliqué à**. Reportez-vous à la section [Ajouter un pare-feu distribué](#) pour obtenir des instructions.

Note Seules les stratégies avec état sont prises en charge pour les machines virtuelles de charge de travail de cloud public. Les stratégies sans état peuvent être créées dans NSX Manager, mais elles ne correspondront à aucun groupe contenant vos machines virtuelles de charge de travail de cloud public.

- 3 Dans CSM, supprimez de la liste blanche les machines virtuelles que vous souhaitez inclure dans la gestion NSX. Reportez-vous à la section [Comment ajouter des machines virtuelles à la liste blanche ou les supprimer de celle-ci](#) pour obtenir des instructions.

Note La mise sur liste blanche est une étape manuelle fortement recommandée dans le cadre du workflow de jour-0 dès que vous ajoutez votre inventaire de cloud public dans CSM. Si vous n'avez pas mis de machines virtuelles sur liste blanche, vous n'avez pas besoin de les supprimer de la liste blanche.

- 4 Pour les règles de groupes et de DFW qui trouvent une correspondance dans le cloud public, ce qui suit s'effectue automatiquement :
 - a Dans AWS, NSX Cloud crée un nouveau groupe de sécurité nommé `nsx-<NSX GUID>`.
 - b Dans Microsoft Azure, NSX Cloud crée un groupe de sécurité d'application (ASG) correspondant au groupe créé dans NSX Manager et un groupe de sécurité réseau (NSG) correspondant aux règles DFW qui sont mises en correspondance avec les machines virtuelles de charge de travail regroupées.

Note NSX Cloud synchronise NSX Manager, les groupes de cloud public et les règles DFW toutes les 30 secondes.

- 5 Resynchronisez votre compte de cloud public dans CSM :
 - a Connectez-vous à CSM et accédez à votre compte de cloud public.
 - b Dans le compte de cloud public, cliquez sur **Actions > Resynchroniser un compte**. Attendez la fin de la resynchronisation.
 - c Accédez au VPC/VNet et cliquez sur l'indicateur d'erreurs de couleur rouge. Cela vous permet d'accéder à la vue d'instances.
 - d Passez en mode Détails si vous étiez en mode Grille, puis cliquez sur **En échec** dans la colonne Réalisation des règles pour afficher les erreurs, le cas échéant.

Étape suivante

Reportez-vous à la section [Limites actuelles et erreurs courantes](#).

Limites actuelles et erreurs courantes

Reportez-vous à ces limitations connues et erreurs courantes pour résoudre les problèmes de gestion de vos machines virtuelles de charge de travail de cloud public dans le Mode d'application du Cloud natif.

Note Les limites suivantes sont définies par votre cloud public :

- Le nombre de groupes de sécurité pouvant être appliqués à une machine virtuelle de charge de travail.
- Le nombre de règles pouvant être réalisées pour une machine virtuelle de charge de travail.
- Le nombre de règles pouvant être réalisées par groupe de sécurité.
- L'étendue de l'attribution du groupe de sécurité, par exemple, l'étendue du groupe de sécurité réseau (NSG) dans Microsoft Azure est limitée à cette région, tandis que l'étendue du groupe de sécurité (SG) dans AWS est limitée à ce VPC.

Reportez-vous à la documentation du cloud public pour plus d'informations sur ces limites.

Limitations actuelles

La version actuelle présente les limitations suivantes concernant les règles DFW pour les machines virtuelles de charge de travail :

- Les groupes imbriqués ne sont pas pris en charge.
- Les groupes sans machine virtuelle ni adresse IP en tant que membre ne sont pas pris en charge ; par exemple, les critères basés sur le segment ou le port logique ne sont pas pris en charge.
- La source et la destination comme adresse IP ou groupe basé sur CIDR ne sont pas prises en charge.
- La source et la destination définies sur « ANY » ne sont pas prises en charge.
- Le groupe **Appliqué_à** peut uniquement être une Source ou une Destination ou des groupes Source + Destination. Les autres options ne sont pas prises en charge.
- Seule l'application de la règle VPC/VNet locale est prise en charge. Vous pouvez créer des groupes dans NSX Manager qui s'étendent sur les VPC/VNet. Toutefois, la réalisation de ces règles ne fonctionne que dans le VPC/VNet. Les règles DFW inter-VPC/VNet ne sont pas réalisées.

- Seuls TCP et UDP sont pris en charge.

Note Uniquement dans AWS :

Les règles de refus créées pour les machines virtuelles de charge de travail dans vos VPC AWS ne sont pas réalisées sur AWS, car dans AWS, tout est mis sur liste noire par défaut. Cela entraîne les résultats suivants dans NSX-T Data Center :

- S'il existe une règle de refus entre VM1 et VM2, le trafic n'est pas autorisé entre VM1 et VM2 en raison du comportement AWS par défaut, pas en raison de la règle de refus. La règle de refus n'est pas réalisée dans AWS.
- En supposant que les deux règles suivantes sont créées dans NSX Manager pour les mêmes machines virtuelles avec la règle 1 ayant une priorité plus élevée que la règle 2 :
 - a VM1 vers VM2 Refuser SSH
 - b VM1 vers VM2 Autoriser SSH

la règle de refus est ignorée, car elle n'est pas réalisée dans AWS. Par conséquent, la règle Autoriser SSH est réalisée. Cela est contraire à l'attente, mais est une limitation en raison du comportement AWS par défaut.

Erreurs courantes et leur résolution

Erreur : aucune stratégie NSX n'est appliquée à la machine virtuelle.

Si vous voyez cette erreur, aucune des règles DFW n'a été appliquée à la machine virtuelle particulière. Modifiez la règle ou le groupe dans NSX Manager pour inclure cette machine virtuelle.

Erreur : la règle NSX sans état n'est pas prise en charge.

Si vous voyez cette erreur, cela signifie que vous avez ajouté des règles DFW pour les machines virtuelles de charge de travail de cloud public dans une stratégie de sécurité sans état. Cela n'est pas pris en charge. Créez une règle ou utilisez une stratégie de sécurité existante dans le mode avec état.

Fonctionnalités de NSX-T Data Center prises en charge avec NSX Cloud

NSX Cloud crée une topologie réseau pour votre VPC ou VNet de cloud public en générant des entités de mise en réseau logiques dans NSX-T Data Center.

Utilisez cette liste comme référence 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

Reportez-vous à la section « Entités logiques NSX-T créées automatiquement » dans le *Guide d'installation de NSX-T Data Center* pour plus d'informations sur les entités logiques créées lorsqu'un PCG est correctement déployé.

Important Ne modifiez pas ou ne supprimez pas ces entités créées automatiquement.

Note Si vous n'êtes pas en mesure d'accéder à certaines fonctionnalités sur les machines virtuelles de charge de travail Windows, assurez-vous que les paramètres du pare-feu Windows sont configurés correctement.

Tableau 22-10.

Fonctionnalité de NSX-T Data Center	Détails	Remarque à propos de NSX Cloud
Segments ou commutateurs logiques	Reportez-vous à la rubrique Chapitre 4 Segments	Un segment est créé pour chaque sous-réseau de cloud public auquel une machine virtuelle gérée est attachée. Il s'agit d'un segment hybride.
Passerelles ou routeurs logiques	Reportez-vous aux sections Chapitre 2 Passerelles de niveau 0 et Chapitre 3 Passerelle de niveau 1 .	Lorsque PCG est déployé sur un VPC ou VNet de transit, un routeur logique de niveau 0 est automatiquement créé par NSX Cloud. Un routeur de niveau 1 est créé pour chaque VPC/VNet de calcul lorsqu'il est lié à un VPC/VNet de transit
IPFIX	Reportez-vous à la section Configurer IPFIX .	<ul style="list-style-type: none"> ■ IPFIX est pris en charge dans NSX Cloud uniquement sur le port UDP 4739. ■ 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.

Tableau 22-10. (suite)

Fonctionnalité de NSX-T Data Center	Détails	Remarque à propos de NSX Cloud
Mise en miroir de ports	Reportez-vous à la section Surveiller des sessions de mise en miroir de ports .	<p>La mise en miroir de ports est uniquement prise en charge dans AWS dans la version actuelle.</p> <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.
Pare-feu de passerelle	Reportez-vous à la section Configuration d'un pare-feu de passerelle .	Pris en charge uniquement sur les passerelles de niveau 0.

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.

Note Les règles DFW dépendent des balises attribuées aux machines virtuelles. Comme ces balises peuvent être modifiées par toute personne disposant des autorisations de cloud public appropriées, NSX-T Data Center suppose que ces utilisateurs sont dignes de confiance. L'administrateur réseau du cloud public doit s'assurer et auditer que les machines virtuelles sont correctement balisées à tout moment.

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
- azure:transit_vnet_name
- azure:transit_vnet_rg
- aws:account
- aws:availabilityzone
- aws:region
- aws:vpc
- aws:subnet
- aws:transit_vpc

- **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 et de `dis:aws` si elles sont découvertes dans AWS.

Lorsque vous apportez des modifications aux balises dans le cloud public, celles-ci sont reflétées dans NSX Manager en trois 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 22-11. 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:availability zone 	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 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. 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 22-11. 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
	■ 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 22-12.

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=AbcdefghijklmnopqrstuvwxyzAb23690hgjgjuytreswqacvbcdefghijklmnopqrstuvwxyz	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 [Ajouter un groupe](#).
- Reportez-vous à la section [Configurer la microsegmentation pour les machines virtuelles de charge de travail dans le Mode d'application NSX](#).

Utiliser les services cloud natifs

Les services cloud natifs suivants sont pris en charge pour une utilisation avec vos machines virtuelles de charge de travail de cloud public depuis NSX Manager.

Lorsque vous déployez PCG, un groupe est créé dans NSX Manager pour chaque service cloud natif pris en charge.

Les groupes suivants sont créés pour les services de cloud public actuellement pris en charge :

- aws-dynamo-db-service-endpoint
- aws-elb-service-endpoint
- aws-rds-service-endpoint
- aws-s3-service-endpoint
- azure-cosmos-db-service-endpoint
- azure-load-balancer-service-endpoint
- azure-sql-service-endpoint
- azure-storage-service-endpoint

Pour utiliser ces services cloud natif, créez des stratégies DFW contenant le groupe de services cloud natif dans les champs source ou de destination de la règle, si nécessaire.

Les règles DFW sont appliquées sur les machines virtuelles qui ne sont pas sur les services cloud natifs.

Note Dans le Mode d'application NSX, c'est-à-dire la gestion de vos charges de travail avec NSX Tools, il n'existe actuellement aucune prise en charge des services cloud natifs de Microsoft Azure.

Limitations actuelles

POINT DE TERMINAISON			Règle DFW avec le service en tant que DESTINATION		Règle DFW avec le service en tant que SOURCE	
Cloud public	Service	Étendue	Appliquée sur la VM ?	Appliquée sur le service ?	Appliquée sur le service ?	Appliquée sur la VM ?
Microsoft Azure	Stockage Blob	Global	Oui	Non	Non	Oui
	Base de données Cosmos					
	SQL					
	Équilibreur de charge					
AWS	S3	VPC local	Oui	Non	Non	Oui
	Base de données Dynamo					
	RDS					
	ÉQUILIBREUR DE CHARGE					

Insertion de services pour votre cloud public

NSX Cloud prend en charge l'utilisation de services tiers dans votre cloud public pour les machines virtuelles de charge de travail gérées par NSX.

Pour utiliser l'insertion de services pour vos machines virtuelles de charge de travail de cloud public, vous devez héberger le dispositif de service dans le cloud public, pas dans NSX-T Data Center. Il est recommandé d'héberger le dispositif de service dans un VPC/VNet de transit.

Pour que vous puissiez activer l'insertion de services, la PCG doit être déployée dans un VPC ou VNet de transit.

Voici un aperçu des configurations à usage unique autorisant l'insertion de services pour vos machines virtuelles de charge de travail gérées par NSX.

Tableau 22-13. Aperçu des configurations requises pour l'insertion de services pour les machines virtuelles de charge de travail gérées par NSX dans le cloud public

Fréquence	Tâche	Instructions
Une fois pour la configuration initiale	Configurez le dispositif de service dans votre cloud public, de préférence dans un VPC ou VNet de transit (où vous avez déployé la PCG).	Reportez-vous aux instructions spécifiques du dispositif de service tiers et du cloud public.
	Enregistrez le service tiers dans NSX-T Data Center.	Reportez-vous à la rubrique Créer la définition de service et un point de terminaison virtuel correspondant
	Créez un point de terminaison d'instance virtuelle du service à l'aide d'une adresse IP virtuelle de service (VSIP) /32 à utiliser uniquement pour l'insertion de services par le dispositif de service. La VSIP ne doit pas être en conflit avec la plage CIDR des VPC ou VNet. Cette VSIP est annoncée sur BGP à la PCG.	Reportez-vous à la rubrique Créer la définition de service et un point de terminaison virtuel correspondant
	Créez un tunnel VPN IPSec entre le dispositif de service et la PCG.	Reportez-vous à la rubrique Configurer une session VPN IPSec

Tableau 22-13. Aperçu des configurations requises pour l'insertion de services pour les machines virtuelles de charge de travail gérées par NSX dans le cloud public (suite)

Fréquence	Tâche	Instructions
	Configurez BGP entre la PCG et le dispositif de service et publiez la VSIP à partir du dispositif de service et la route par défaut (0.0.0.0/0) à partir de la PCG.	Reportez-vous à la rubrique Configurer le BGP et la redistribution de routes
	Note Dans la version actuelle, l'insertion de services est uniquement prise en charge pour le trafic nord-sud.	
Si nécessaire	Une fois les configurations à usage unique terminées, configurez des règles de redirection pour réacheminer le trafic sélectif des machines virtuelles de charge de travail gérées par NSX vers la VSIP. Ces règles sont appliquées au port de liaison montante de la PCG.	Reportez-vous à la section Configurer les règles de redirection .

Procédure

1 Créer la définition de service et un point de terminaison virtuel correspondant

Vous devez utiliser les API NSX Manager pour créer une définition de service et le point de terminaison virtuel pour le dispositif de service dans votre cloud public.

2 Configurer une session VPN IPSec

Configurez une session VPN IPSec entre la PCG et votre dispositif de service.

3 Configurer le BGP et la redistribution de routes

Configurez le BGP entre la PCG et le dispositif de service via le tunnel VPN IPSec.

4 Configurer les règles de redirection

Les règles de redirection peuvent être ajustées en fonction de vos besoins.

Créer la définition de service et un point de terminaison virtuel correspondant

Vous devez utiliser les API NSX Manager pour créer une définition de service et le point de terminaison virtuel pour le dispositif de service dans votre cloud public.

Conditions préalables

Choisissez une adresse IP réservée /32 devant servir de point de terminaison virtuel pour le dispositif de service dans votre cloud public (par exemple, 100.100.100.100/32). Il s'agit de l'adresse IP de service virtuel (VSIP).

Note Si vous avez déployé votre dispositif de service dans une paire haute disponibilité, ne créez pas d'autre définition de service, mais utilisez la même VSIP lorsque vous l'annoncez à la PCG lors de la configuration BGP.

Procédure

- 1 Pour créer une définition de service pour le dispositif de service, exécutez l'appel d'API suivant à l'aide des informations d'identification de NSX Manager à des fins d'autorisation :

```
POST https://{NSX Manager-IP}/policy/api/v1/enforcement-points/default/service-definitions
```

Exemple de demande :

```
{
  "resource_type": "ServiceDefinition",
  "description": "NS-Service",
  "display_name": "Service_Appliance1",
  "attachment_point": [
    "TIER0_LR"
  ],
  "transports": [
    "L3_ROUTED"
  ],
  "functionalities": [
    "NG_FW", "BYOD"
  ],
  "on_failure_policy": "ALLOW",
  "implementations": [
    "NORTH_SOUTH"
  ],
  "vendor_id" : "Vendor1"
}
```

Exemple de réponse :

```
{
  "resource_type": "ServiceDefinition",
  "description": "NS-Service",
  "id": "33890153-6eea-4c9d-8e34-7b6532b9d65c",
  "display_name": "Service_Appliance1",
  "attachment_point": [
    "TIER0_LR"
  ],
  "transports": [
    "L3_ROUTED"
  ],
  "functionalities": [
    "NG_FW", "BYOD"
  ],
  "vendor_id": "Vendor1",
  "on_failure_policy": "ALLOW",
  "implementations": [
    "NORTH_SOUTH"
  ],
  "_create_time": 1540424262137,
  "_last_modified_user": "nsx_policy",
  "_system_owned": false,
}
```



```

    "_protection": "REQUIRE_OVERRIDE",
    "_last_modified_time": 1540424262137,
    "_create_user": "nsx_policy",
    "_revision": 0
  }

```

- 2 Pour créer un point de terminaison virtuel pour le dispositif de service, exécutez l'appel d'API suivant à l'aide des informations d'identification de NSX Manager à des fins d'autorisation :

```

PATCH https://{NSX Manager-IP}/policy/api/v1/infra/tier-0s/<tier-0 router ID>/locale-
services/cloud/endpoints/virtual-endpoints/Service_Appliance1_Endpoint

```

Exemple de demande :

```

{
  "resource_type": "VirtualEndpoint",
  "display_name": "Service_Appliance1_Endpoint",
  "target_ips": [
    {
      "ip_addresses": [
        "100.100.100.100"
      ],
      "prefix_length": 32
    }
  ],
  "service_names": [
    "Service_Appliance1"
  ]
}

```

Exemple de réponse :

```
200 OK
```

Note Le `display_name` de l'étape 1 doit correspondre aux `service_names` de l'étape 2.

Étape suivante

[Configurer une session VPN IPSec](#)

Configurer une session VPN IPSec

Configurez une session VPN IPSec entre la PCG et votre dispositif de service.

Conditions préalables

- Une passerelle PCG ou une paire HA doit être déployée sur un VPC/VNet de transit.
- Le dispositif de service doit être configuré dans votre cloud public, de préférence dans le VPC/VNet de transit.

Procédure

- 1 Accédez à **Mise en réseau > VPN**.

- 2 Ajoutez un **service VPN** de type IPSec et notez les options de configuration suivantes spécifiques de NSX Cloud. Reportez-vous à la section [Ajouter un service VPN IPSec](#) pour plus d'informations.

Option	Description
Nom	Le nom de ce service VPN est utilisé pour configurer le point de terminaison local et les sessions VPN IPSec. Notez-le.
Type de service	Vérifiez que cette valeur est définie sur IPSec.
Passerelle de niveau 0	Sélectionnez la passerelle de niveau 0 créée automatiquement pour votre VPC/VNet de transit. Son nom contient votre ID VPC/VNet, par exemple, <code>cloud-t0-vpc-6bcd2c13</code> .

- 3 Ajoutez un **point de terminaison local** pour votre PCG. L'adresse IP du point de terminaison local est la valeur de la balise `nsx:local_endpoint_ip` pour la PCG déployée sur votre VPC/VNet de transit. Connectez-vous à votre VPC/VNet de transit pour cette valeur. Notez les configurations suivantes spécifiques de NSX Cloud et reportez-vous à la section [Ajouter des points de terminaison locaux](#) pour plus d'informations.

Option	Description
Nom	Le nom du point de terminaison local est utilisé pour configurer les sessions VPN IPSec. Notez-le.
Service VPN	Sélectionnez le service VPN ajouté à l'étape 2.
Adresse IP	Trouvez cette valeur en vous connectant à la console AWS ou au portail Microsoft Azure. Il s'agit de la valeur de la balise <code>nsx:local_endpoint_ip</code> appliquée à l'interface de liaison montante de la PCG.

- 4 Créez une **session IPSec basée sur la route** entre la PCG et le dispositif de service dans votre cloud public (de préférence hébergée dans le VPC/VNet de transit).

Option	Description
Type	Vérifiez que cette valeur est définie sur Basé sur la route .
Service VPN	Sélectionnez le service VPN ajouté à l'étape 2.
Point de terminaison local	Sélectionnez le point de terminaison local créé à l'étape 3.
Adresse IP distante	Entrez l'adresse IP privée du dispositif de service.
<p>Note Si votre dispositif de service est accessible à l'aide d'une adresse IP publique, attribuez une adresse IP publique à l'adresse IP du point de terminaison local (également appelée adresse IP secondaire) permettant d'accéder à l'interface de liaison montante de la PCG.</p>	

Option	Description
Interface de tunnel	<p>Ce sous-réseau doit correspondre au sous-réseau du dispositif de service pour le tunnel VPN. Entrez la valeur de sous-réseau que vous avez configurée dans le dispositif de service pour le tunnel VPN ou notez la valeur que vous entrez ici et assurez-vous que le même sous-réseau est utilisé lorsque vous configurez le tunnel VPN dans le dispositif de service.</p> <p>Note Vous configurez BGP dans cette interface de tunnel. Reportez-vous à la section Configurer le BGP et la redistribution de routes.</p>
ID distant	Entrez l'adresse IP privée de votre dispositif de service dans le cloud public.
Profil IKE	La session VPN IPSec doit être associée à un profil IKE. Si vous avez créé un profil, sélectionnez-le dans le menu déroulant. Vous pouvez également utiliser le profil par défaut.

Étape suivante

[Configurer le BGP et la redistribution de routes](#)

Configurer le BGP et la redistribution de routes

Configurez le BGP entre la PCG et le dispositif de service via le tunnel VPN IPSec.

Vous configurez des voisins BGP sur l'interface du tunnel VPN IPSec que vous avez établie entre la PCG et le dispositif de service. Reportez-vous à la section [Configurer BGP](#) pour plus d'informations.

Vous devez configurer le BGP de la même façon sur votre dispositif de service. Reportez-vous à la documentation relative à votre service spécifique dans le cloud public pour plus d'informations.

Ensuite, configurez la redistribution de routes comme suit :

- La PCG annonce sa route par défaut (0.0.0.0/0) au dispositif de service.
- Le dispositif de service annonce la VSIP à la PCG. Il s'agit de la même adresse IP que celle utilisée lors de l'enregistrement du service. Reportez-vous à la section [Créer la définition de service et un point de terminaison virtuel correspondant](#).

Note Si votre dispositif de service est déployé dans une paire haute disponibilité, annoncez la même VSIP à partir des deux dispositifs de service.

Procédure

- 1 Accédez à **Mise en réseau > Passerelles de niveau 0**.
- 2 Sélectionnez la passerelle de niveau 0 créée automatiquement pour votre VPC/VNet de transit nommé `cloud-t0-vpc-6bcd2c13` et cliquez sur **Modifier**.
- 3 Cliquez sur le nombre ou l'icône en regard de **Voisins BGP** sous la section **BGP**.

4 Notez ces configurations :

Option	Description
Adresse IP	Utilisez l'adresse IP configurée dans l'interface du tunnel du dispositif de service pour le VPN entre la PCG et le dispositif de service.
Nombre d'AS distants	Ce nombre doit correspondre au nombre d'AS du dispositif de service de votre cloud public.
Filtre de route	Définissez un filtre sortant pour annoncer la route par défaut (0.0.0.0/0) du PCG au dispositif de service.

5 Dans la section **Redistribution des routes**, activez les routes statiques sur la passerelle de niveau 0.

Définir la redistribution des routes

Passerelle de niveau 0 cloud-t0-415... #Redistribution des routes 1

AJOUTER UNE REDISTRIBUTION DES ROUTES Rechercher

Nom	Redistribution des routes	Carte de route
<input type="text" value="Entrer le nom"/>	Définir*	<input type="text" value="Sélectionner la carte de route"/>

Définir la redistribution des routes

Passerelle de niveau 0 cloud-t0-415... #Sources sélectionnées 1

Sélectionner les sources ci-dessous

Sous-réseaux de niveau 0

☒ Routes statiques
 ☐ Adresse IP locale IPSec
 ☐ ADRESSE IP D'EVPN TEP
 ☐ Interfaces et segments connectés
 ☐ Sous-réseau de l'interface de service
 ☐ Sous-réseau d'interface de bouclage

☐ Adresse IP NAT
 ☐ Adresse IP du redirecteur DNS
 ☐ Sous-réseau de l'interface externe
 ☐ Segment connecté

Étape suivante

[Configurer les règles de redirection](#)

Configurer les règles de redirection

Les règles de redirection peuvent être ajustées en fonction de vos besoins.

Une fois la configuration initiale terminée, vous pouvez créer et modifier des règles de redirection comme requis pour la redirection des différents types de trafic pour vos machines virtuelles de charge de travail gérées par NSX, via le dispositif de service.

Conditions préalables

La configuration de l'insertion de services doit être intégralement achevée pour que vous puissiez créer des règles de redirection.

Procédure

- 1 Accédez à **Sécurité > Pare-feu vertical > Introspection réseau (N-S)**.
- 2 Cliquez sur **Ajouter une stratégie**.

Option	Description
Nom :	Fournissez un nom descriptif pour la stratégie, par exemple Insertion de services nord-sud pour les machines virtuelles Azure .
Rediriger vers :	Sélectionnez le nom du point de terminaison virtuel créé pour ce dispositif de service lors de l'enregistrement du service. Reportez-vous à la section Créer la définition de service et un point de terminaison virtuel correspondant .
Appliquer à :	Sélectionnez la passerelle de niveau 0 de la PCG.

- 3 Sélectionnez la nouvelle stratégie et cliquez sur **Ajouter une règle**. Notez les valeurs suivantes spécifiques de l'insertion de services :

Option	Description
Sources	Sélectionnez un groupe de sous-réseaux dont le trafic doit être redirigé, par exemple, un groupe de vos machines virtuelles de charge de travail gérées par NSX.
Destinations	Sélectionnez une liste de services ou d'adresses IP de destination, par exemple Google , que vous souhaitez acheminer via le dispositif de service.
Appliqué à	Sélectionnez le port de liaison montante de la PCG active et en veille.
Action	Sélectionnez Rediriger .

Activer la fonctionnalité NAT sur les machines virtuelles gérées par NSX

NSX Cloud prend en charge l'activation de NAT sur des machines virtuelles gérées par NSX.

À l'aide de balises de cloud public, vous pouvez activer le trafic vertical sur machines virtuelles sur les machines virtuelles gérées par NSX.

Sur la machine virtuelle gérée par NSX pour laquelle vous souhaitez activer NAT, appliquez la balise suivante :

Tableau 22-14.

Clé	Valeur
<code>nsx.publicip</code>	adresse IP publique de votre cloud public, par exemple, 50.1.2.3

Note L'utilisation de l'adresse IP publique que vous fournissez ici doit être libre et elle ne doit pas être attribuée à une machine virtuelle, pas même à la machine virtuelle de charge de travail pour laquelle vous souhaitez activer la NAT. Si vous attribuez une adresse IP publique précédemment associée à une autre instance ou adresse IP privée, la NAT ne fonctionne pas. Dans ce cas, annulez l'attribution de l'adresse IP publique.

Une fois cette balise appliquée, la machine virtuelle de charge de travail peut accéder au trafic Internet.

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>
```

Configurer le VPN en mode NSX appliqué

Vous pouvez configurer un VPN à l'aide des PCG qui s'affichent comme des passerelles de niveau 0 créées automatiquement dans le déploiement de NSX-T Data Center sur site. Ces instructions sont spécifiques aux machines virtuelles de charge de travail en mode NSX appliqué.

Utilisez les PCG de la même manière que vous utilisez des passerelles de niveau 0 dans NSX Manager pour configurer le VPN en suivant les étapes supplémentaires décrites ici. Vous pouvez créer des tunnels VPN entre des PCG déployées dans le même cloud public, des clouds publics différents ou avec une passerelle ou un routeur sur site. Pour plus d'informations sur la prise en charge du VPN dans NSX-T Data Center, consultez le [Chapitre 5 VPN \(Virtual Private Network\)](#).

Conditions préalables

- Vérifiez que vous disposez d'une paire de PCG ou d'une paire HA déployée dans un VPC/VNet.
- Vérifiez que l'homologue distant prend en charge le VPN basé sur route et BGP.

Procédure

- 1 Dans votre cloud public, recherchez le point de terminaison local attribué par NSX à la PCG et attribuez-lui une adresse IP publique si nécessaire :
 - a Accédez à votre instance de PCG dans le cloud public puis accédez à Balises.
 - b Notez l'adresse IP dans le champ de valeur de la balise `nsx.local_endpoint_ip`.
 - c (Facultatif) Si votre tunnel VPN requiert une adresse IP publique, par exemple, si vous souhaitez configurer un VPN sur un autre cloud public ou sur le déploiement de NSX-T Data Center sur site :
 - 1 Accédez à l'interface de liaison montante de l'instance de la PCG.
 - 2 Attachez une adresse IP publique à l'adresse IP `nsx.local_endpoint_ip` que vous avez notée à l'étape **b**.
 - d (Facultatif) Si vous disposez d'une paire HA d'instances de PCG, répétez les étapes **a** et **b** et attachez une adresse IP publique si nécessaire, comme décrit à l'étape **c**.

- 2 Dans NSX Manager, activez le VPN IPsec de la PCG qui apparaît comme une passerelle de niveau 0 nommée `cloud-t0-vpc/vnet-<vpc/vnet-id>` et créez des sessions IPsec basées sur la route entre ce point de terminaison de la passerelle de niveau 0 et l'adresse IP distante de l'homologue VPN souhaité. Reportez-vous à la section [Ajouter un service VPN IPsec](#) pour plus d'informations.

- a Accédez à **Mise en réseau > VPN > Services VPN > Ajouter un service > IPsec**. Fournissez les détails suivants :

Option	Description
Nom	Entrez un nom descriptif pour le service VPN, par exemple <code><VPC-ID>-AWS_VPN</code> ou <code><VNet-ID>-AZURE_VPN</code> .
Passerelle de niveau 0/niveau 1	Sélectionnez la passerelle de niveau 0 pour la PCG dans votre cloud public.

- b Accédez à **Mise en réseau > VPN > Points de terminaison locaux > Ajouter un point de terminaison local**. Fournissez les informations suivantes et reportez-vous à la section [Ajouter des points de terminaison locaux](#) pour plus d'informations.

Note Si vous disposez d'une paire HA d'instances de PCG, créez un point de terminaison local pour chaque instance à l'aide de l'adresse IP du point de terminaison local correspondant dans le cloud public.

Option	Description
Nom	Entrez un nom descriptif pour le point de terminaison local, par exemple <code><VPC-ID>-PCG-preferred-LE</code> ou <code><VNET-ID>-PCG-preferred-LE</code> .
Service VPN	Sélectionnez le service VPN pour la passerelle de niveau 0 de la PCG que vous avez créée à l'étape 2a.
Adresse IP	Entrez la valeur de l'adresse IP du point de terminaison local de la PCG que vous avez notée à l'étape 1b.

- c Accédez à **Mise en réseau > VPN > Sessions IPsec > Ajouter une session IPsec > Basé sur la route**. Fournissez les informations suivantes et consultez la section [Ajout d'une session IPsec basée sur une route](#) pour plus d'informations :

Note Si vous créez un tunnel VPN entre des PCG déployées dans un VPC et des PCG déployées dans un réseau virtuel, vous devez créer un tunnel pour chaque point de terminaison local de PCG dans le VPC et l'adresse IP distante de la PCG dans le réseau virtuel, et inversement de la PCG du réseau virtuel vers l'adresse IP distante de PCG dans le VPC. Vous devez créer un tunnel distinct pour les PCG actives et en veille. Cela entraîne un maillage complet des sessions IPsec entre les deux clouds publics.

Option	Description
Nom	Entrez un nom descriptif pour la session IPsec, par exemple, <code><VPC-ID>-PCG1-to-remote_edge</code> .
Service VPN	Sélectionnez le service VPN créé à l'étape 2a.
Point de terminaison local	Sélectionnez le point de terminaison local créé à l'étape 2b.
Adresse IP distante	Entrez l'adresse IP publique de l'homologue distant avec lequel vous créez le tunnel VPN.

vm NSX-T admin

Accueil Mise en réseau Sécurité Inventaire Planifier et dépanner Système **STRATÉGIE** GESTIONNAIRE

Étape 2a.

SERVICES VPN SESSIONS IPSEC SESSIONS VPN DE COUCHE 2 POINTS DE TERMINAISON LOCAUX PROFILS

AJOUTER UN SERVICE TOUT RÉDUIRE Filtrer par nom, chemin, etc.

Nom	Type de service	Passerelle de niveau 0/niveau 1	Sessions	État
<VPC-ID>-AWS_VPN	IPSec	cloud-to-vpc-073617880a9622d93	1	Réussite
Description: VPN service on AWS Transit VPC ID vpc-073617880a9622d93				
Statut administratif: Actif				
Niveau de journal IKE: Info Balises: 0				
Synchronisation de session: Actif				

vm NSX-T admin

Accueil Mise en réseau Sécurité Inventaire Planifier et dépanner Système **STRATÉGIE** GESTIONNAIRE

Étape 2b.

SERVICES VPN SESSIONS IPSEC SESSIONS VPN DE COUCHE 2 **POINTS DE TERMINAISON LOCAUX** PROFILS

AJOUTER UN POINT DE TERMINAISON LOCAL TOUT RÉDUIRE Filtrer par nom, chemin, etc.

Nom	Service VPN	Adresse IP	Certificat de site	Sessions	État
<VPC-ID>-PCG-preferred-LE	<VPC-ID>-AWS_VPN	10.99.3.35	Non défini	1	Réussite
Description: Non défini ID local: 10.99.3.35					
Certificats d'autorité de certification approuvés: Non défini Liste de révocation de certificat: Non défini					
Balises: 0					

vm NSX-T admin

Accueil Mise en réseau Sécurité Inventaire Planifier et dépanner Système **STRATÉGIE** GESTIONNAIRE

Étape 2c.

SERVICES VPN **SESSIONS IPSEC** SESSIONS VPN DE COUCHE 2 POINTS DE TERMINAISON LOCAUX PROFILS

AJOUTER UNE SESSION IPSEC TOUT RÉDUIRE admin

Nom	Type	Service VPN	Point de terminaison local	Adresse IP distante	État	Alarmes
<VPC-ID>-PCG-to-remote-edge	Basé sur la route	<VPC-ID>-AWS_VPN	<VPC-ID>-PCG-preferred-LE	3.213.92.220	Inactif	0
Description: Non défini Statut administratif: Actif						
Suite de conformité: Aucun Interface de tunnel: 192.168.50.10/24						
Mode d'authentification: PSK ID distant: 172.0.3.145						
Clé prépartagée: *****						
Propriétés avancées						
Profil IKE: nsx-default-ibvpn-ike- Mode d'initialisation de la connexion: Initiateur						


AFFICHER LES STATISTIQUES TÉLÉCHARGER LA CONFIGURATION

ACTUALISER 1 - 1 sur 1 Sessions IPSec

3 Configurez les voisins BGP sur l'interface du tunnel VPN IPSec que vous avez établie à l'étape 2. Reportez-vous à la section [Configurer BGP](#) pour plus d'informations.

- a Accédez à **Mise en réseau > Passerelles de niveau 0**
- b Sélectionnez la passerelle de niveau 0 créée automatiquement pour laquelle vous avez créé la session IPSec, puis cliquez sur **Modifier**.
- c Cliquez sur le nombre ou l'icône en regard de **Voisins BGP** sous la section **BGP** et entrez les détails suivants :

Option	Description
Adresse IP	Utilisez l'adresse IP de la VTI distante configurée sur l'interface de tunnel dans la session IPSec pour l'homologue VPN.
Nombre d'AS distants	Ce nombre doit correspondre au nombre d'AS de l'homologue distant.

 Passerelle de niveau 0

[AJOUTER UNE PASSERELLE](#) [TOUT DÉVELOPPER](#) [Filtrer p](#)

	Nom de la passerelle de niveau 0	Mode VMware HA	Passerelles de niveau 1 liées	Segments liés
>	MULTIDIFFUSION			
∨	BGP			
	AS local	1000	iBGP Inter SR	● Activé
	BGP	● Activé	ECMP	● Activé
	Redémarrage normal	Assistance uniquement	Alléger les chemins multiples	● Activé
	Temporisateur de redémarrage normal	180 secondes	Temporisateur caduc de redémarrage normal	600 secondes
	Agrégation de route	0	Voisins BGP	1

Étape 3.

Voisins BGP

Passerelle de niveau 0 cloud-t0-415... [Voisins](#) 1

	Adresse IP	BFD	Nombre d'AS distants
⋮ ∨	192.168.50.11	Désactivé	1000
	Adresses source	Non défini	
	Limite de tronçon maximale	1	

- 4 Annoncez les préfixes que vous voulez utiliser pour le VPN à l'aide du profil de redistribution. Dans Mode d'application NSX, connectez les routes activées de niveau 1 dans le profil de redistribution.

Passerelle de niveau 0

AJOUTER UNE PASSERELLE ▼ TOUT DÉVELOPPER Filtrer par nom, cherr

	Nom de la passerelle de niveau 0	Mode VMware HA	Passerelles de niveau 1 liées	Segments liés	État ⓘ
>	BGP				
▼	REDISTRIBUTION DES ROUTES				
	Redistribution des routes 2	Actif Actif	0	0	État de redistribution des routes ● Activé
⋮ > [VRF] TORvf					● Réussi

ACTUALISER 1 - 3

Étape 4.

Redistribution des routes

Passerelle de niveau 0 cloud-t0-vpc... #Sources sélectionnées ⓘ

Sous-réseaux de niveau 0

Sous-réseaux de niveau 1 annoncés

- Interfaces et segments connectés
- Sous-réseau de l'interface de service
- Segment connecté

Questions fréquemment posées (FAQ)

Cette rubrique répertorie les questions fréquemment posées.

Comment puis-je vérifier que mes composants NSX Cloud sont installés et en cours d'exécution ?

- 1 Pour vérifier que les outils NSX Tools sur votre machine virtuelle de charge de travail sont connectés à PCG, procédez comme suit :
 - a Entrez la commande `nsxcli` pour ouvrir la CLI de NSX.
 - b 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
```

2 Les machines virtuelles de charge de travail doivent avoir des balises correctes pour se connecter à PCG :

- a Connectez-vous à la console AWS ou au portail Microsoft Azure.
- b Vérifiez la balise `eth0` ou d'interface de la machine virtuelle.

La clé `nsx.network` doit avoir la valeur `default`.

Mes machines virtuelles lancées à l'aide de cloud-init sont mises en quarantaine et n'autorisent pas l'installation d'outils tiers. Que dois-je faire ?

Lorsque la stratégie de mise en quarantaine est activée et que vous lancez des machines virtuelles à l'aide de scripts cloud-init avec les spécifications suivantes, vos machines virtuelles sont mises en quarantaine lors du lancement et vous ne pouvez pas y installer des applications ou des outils personnalisés :

- application de la balise `nsx.network=default` à la machine virtuelle
- installation automatique ou démarrage des services personnalisés lorsque la machine virtuelle est sous tension

Solution :

Mettez à jour le groupe de sécurité `default` (AWS) ou `default-vnet-<vnet-ID>-sg` (Microsoft Azure) pour ajouter des ports entrants/sortants comme requis pour l'installation d'applications personnalisées ou tierces.

J'ai correctement balisé ma machine virtuelle et installé NSX Tools, 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.network` 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 un compte**.

Que dois-je faire si je ne peux pas accéder à ma machine virtuelle de charge de travail ?

À partir de votre Cloud Public (AWS ou Microsoft Azure) :

- 1 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 [Détection des menaces à l'aide de la stratégie de mise en quarantaine de NSX Cloud](#).
 - Règles DFW de NSX-T Data Center. Reportez-vous à [Stratégie de connectivité par défaut pour les machines virtuelles de charge de travail gérées par NSX dans le Mode d'application NSX](#) pour plus de détails.
 - Pare-feu Windows ou IPTables sous Linux.
- 2 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.
 - 3 Vous pouvez redémarrer la machine virtuelle verrouillée.
 - 4 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.

Ai-je besoin d'un PCG même dans le Mode d'application du Cloud natif ?

Oui.

Puis-je modifier le rôle IAM de la PCG après avoir intégré mon compte de cloud public dans CSM ?

Oui. Vous pouvez réexécuter le script de NSX Cloud applicable à votre cloud public pour régénérer le rôle de la PCG. Modifiez votre compte de cloud public dans CSM avec le nouveau nom de rôle après avoir régénéré le rôle de la PCG. Les nouvelles instances de la PCG déployées dans votre compte de cloud public utiliseront le nouveau rôle.

Notez que les instances de PCG existantes continuent d'utiliser l'ancien rôle PCG. Si vous souhaitez mettre à jour le rôle IAM d'une instance de PCG existante, accédez à votre cloud public et modifiez manuellement le rôle de cette instance de PCG.

Puis-je utiliser les licences NSX-T Data Center sur site pour NSX Cloud ?

Oui, vous pouvez si votre ELA possède une clause relative à ce produit.

VMware NSX® Intelligence™ fournit une visualisation de la position de sécurité de votre environnement NSX-T Data Center sur site. La visualisation est basée sur les flux de trafic réseau agrégés dans une période de temps spécifique. NSX Intelligence vous aide également à effectuer une planification de micro-segmentation en établissant des recommandations basées sur des analyses avec une application de la stratégie de sécurité.

Important Vous devez disposer d'un rôle d'administrateur d'entreprise pour avoir l'autorisation d'installer, de configurer et d'utiliser NSX Intelligence.

Avant de pouvoir commencer à utiliser les fonctionnalités de NSX Intelligence, vous devez d'abord installer et configurer le dispositif NSX Intelligence. Reportez-vous à la section « Installation et configuration du dispositif NSX Intelligence » dans le *Guide d'installation de NSX-T Data Center*.

Ce chapitre contient les rubriques suivantes :

- [Démarrage avec NSX Intelligence](#)
- [Présentation des vues et des flux de NSX Intelligence](#)
- [Utilisation des recommandations de NSX Intelligence](#)
- [Sauvegarde et restauration de NSX Intelligence](#)
- [Dépannage des problèmes liés à NSX Intelligence](#)

Démarrage avec NSX Intelligence

Pour commencer à utiliser les fonctionnalités de NSX Intelligence, familiarisez-vous avec l'interface utilisateur graphique de NSX Intelligence.

Une fois le dispositif NSX Intelligence installé et configuré, les fonctionnalités de NSX Intelligence sont activées dans l'onglet **Planifier et dépanner** de l'interface utilisateur de NSX Manager. Dans la section **Découvrir et planifier**, utilisez **Découvrir et prendre une mesure** pour visualiser vos entités de centre de données NSX-T et **Recommandations** pour obtenir des recommandations sur la planification de la micro-segmentation.

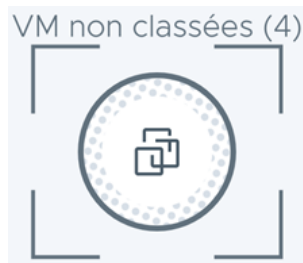
Découverte de la page d'accueil de NSX Intelligence

Vous pouvez accéder à la page d'accueil de NSX Intelligence en cliquant sur **Planifier et dépanner** > **Découvrir et prendre une mesure** dans l'interface utilisateur de NSX Manager.

Après avoir installé et configuré NSX Intelligence pour la première fois, lorsque vous cliquez sur **Découvrir et prendre une mesure**, le message suivant apparaît : *Aucune donnée trouvée.*

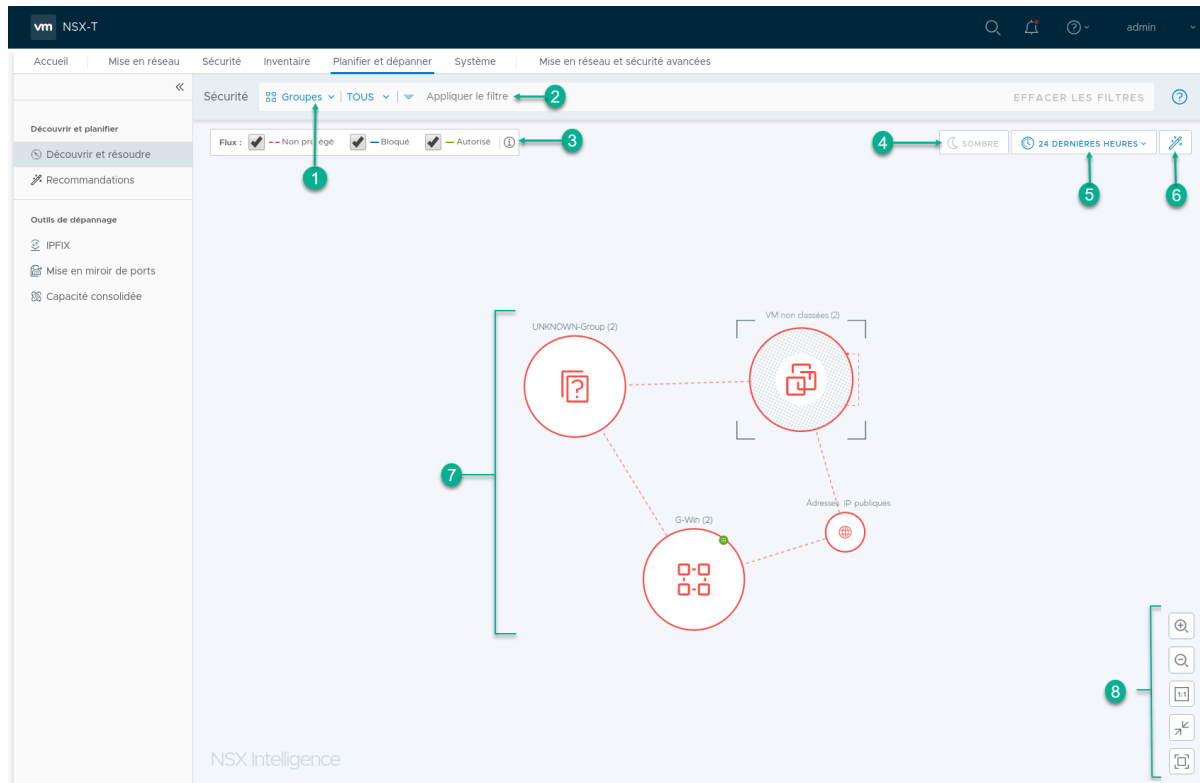
Vous devrez peut-être modifier vos filtres ci-dessus. Ce message est dû au fait que NSX Intelligence n'a pas encore reçu les données de trafic réseau qu'il peut utiliser pour créer une visualisation. Après la réception de certaines données de flux réseau depuis NSX Manager, NSX Intelligence peut commencer à afficher une certaine visualisation.

Par défaut, lorsque vous cliquez sur **Découvrir et prendre une mesure**, vous voyez apparaître la visualisation de l'état de sécurité de tous les groupes de votre NSX-T Data Center sur site qui incluait des flux de trafic non protégés entre leurs membres de VM au cours des dernières 24 heures. Les flux de trafic réseau non protégés sont des flux entre des machines virtuelles pour lesquelles aucune micro-segmentation n'est mise en œuvre. Si aucun groupe n'est encore défini, aucun groupe n'est affiché. S'il existe des VM, mais qu'elles n'appartiennent à aucun groupe, l'icône du groupe VM non classées apparaît.





Si vous avez déjà défini des groupes et que les données de flux de trafic ont été capturées, une visualisation similaire à la capture d'écran suivante peut s'afficher. Le tableau suivant décrit les sections numérotées dans la capture d'écran.

Note NSX Intelligence classe une adresse IP appartenant à l'une des notations CIDR suivantes en tant qu'adresse IP privée : 192.168.0.0/16, 172.16.0.0/12 et 10.0.0.0/8. Toutes les adresses IP qui n'appartiennent à aucune de ces notations CIDR sont classées en tant qu'adresse IP publique. Si l'adresse IP de votre machine virtuelle n'est pas comprise dans l'une de ces notations CIDR, envisagez d'ajouter votre notation CIDR à l'aide de l'API `PATCH /api/v1/intelligence/host-config` dans le *Guide de l'API de NSX-T Data Center*.











Section	Description
1	<p>Dans la zone de sélection de la vue Sécurité, vous pouvez sélectionner le type de visualisation de sécurité à afficher. Il existe deux types de vues Sécurité disponibles : Groupes et VM. Lorsque vous cliquez sur Découvrir et prendre une mesure, la vue Sécurité par défaut affichée correspond à la vue Groupes des objets de groupe de votre NSX-T Data Center qui inclut des flux de trafic non protégés au cours des dernières 24 heures.</p> <ul style="list-style-type: none"> ■ Pour sélectionner la vue VM, cliquez sur la flèche vers le bas en regard de Groupes et sélectionnez VM. ■ Pour sélectionner les groupes ou les machines virtuelles spécifiques à inclure dans la vue, cliquez sur la flèche vers le bas en regard de TOUS et sélectionnez dans la liste. ■ Pour effacer vos filtres de sélection, cliquez sur EFFACER LES FILTRES dans la partie supérieure droite de l'écran. Lorsque vous cliquez sur EFFACER LES FILTRES dans la vue VM, les filtres de sélection sont effacés et vous êtes placé dans la vue Groupes. <p>Reportez-vous aux sections Utilisation de la vue Groupes et Utilisation de la vue VM pour plus d'informations sur l'utilisation des deux types de vues.</p>
2	<p>Grâce à l'option Appliquer le filtre, vous pouvez affiner les critères utilisés pour la visualisation. Dans la liste déroulante, vous pouvez sélectionner les critères à utiliser pour la visualisation. Vous pouvez sélectionner les membres de VM, les balises, les types de flux, l'adresse IP source, l'adresse IP de destination, l'ID de règle ou le nom. Vous pouvez définir plusieurs filtres à appliquer en cliquant à nouveau sur Appliquer le filtre.</p>



Section	Description
3	<p>Grâce à cette section Flux, vous pouvez sélectionner le type de flux à inclure dans la visualisation au cours de la période sélectionnée. Les couleurs utilisées dans la visualisation des types de flux sont également affichées dans cette section.</p> <ul style="list-style-type: none"> ■ Ligne en pointillés rouges pour les flux Non protégés ■ Ligne unie bleue pour les flux Bloqués ■ Ligne pleine verte pour les flux Autorisés <p>Par défaut, le flux de trafic de type Non protégé est sélectionné pour la visualisation de NSX Intelligence actuelle. Pour plus d'informations, reportez-vous à la section Utilisation des flux de trafic.</p>
4	<p>La section de mode d'affichage définit le thème à utiliser pour la visualisation. Le thème clair est le mode par défaut utilisé.</p> <ul style="list-style-type: none"> ■ Pour utiliser le mode thème foncé, cliquez sur l'icône SOMBRE. Vous pouvez utiliser le thème sombre uniquement lorsque vous affichez la visualisation en mode plein écran. ■ Pour passer en mode plein écran, cliquez sur  dans la section de contrôle de l'affichage.
5	<p>Dans cette section, vous sélectionnez la période à utiliser pour déterminer les données de flux réseau qui servent à générer la visualisation et la recommandation souhaitées. Votre sélection détermine les données d'historique qui sont utilisées dans la vue Groupes ou VM. La période est relative à l'heure actuelle et à une période passée.</p> <p>Les dernières 24 heures sont la plage de temps utilisée par défaut. Pour modifier la période sélectionnée, cliquez sur la période actuellement sélectionnée et sélectionnez Dernière heure, 12 dernières heures, 24 dernières heures, Dernière semaine ou Dernier mois.</p>
6	<p>Lorsque vous cliquez sur l'icône de baguette Recommandations , la boîte de dialogue Recommandations affiche le résumé de l'inventaire de la vue actuelle. Si vous êtes dans la vue VM, vous pouvez générer une recommandation NSX Intelligence en cliquant sur Commencer une nouvelle recommandation. Reportez-vous à la section Utilisation des recommandations de NSX Intelligence.</p>
7	<p>Cette section est la visualisation de l'état de sécurité des groupes ou des machines virtuelles dans votre NSX-T Data Center sur site. Elle inclut également la visualisation des flux de trafic réseau qui se sont produits pendant la période sélectionnée. Dans cette section, vous pouvez pointer sur la flèche d'un nœud ou d'un flux spécifique pour obtenir des détails sur cette entité.</p> <p>Pour plus d'informations, reportez-vous aux sections Familiarisation avec les éléments graphiques de NSX Intelligence et Présentation des vues et des flux de NSX Intelligence.</p>
8	<p>Cette section inclut les contrôles d'affichage pour effectuer un zoom avant, un zoom arrière, appliquer le format d'image 1:1, redimensionner/ajuster la vue et passer en mode d'affichage plein écran. Vous pouvez également utiliser des touches de raccourcis clavier pour gérer vos contrôles d'affichage. Pour afficher la fenêtre d'aide Raccourcis clavier, appuyez sur Maj+.</p> <p>Pour accéder à une visualisation affichée précédemment, utilisez le bouton précédent de votre navigateur Web. Lorsque vous êtes en mode plein écran, cliquez sur Précédent (en haut à gauche de l'écran) pour effectuer la même navigation du bouton précédent.</p>

Familiarisation avec les éléments graphiques de NSX Intelligence

L'interface utilisateur de NSX Intelligence fournit plusieurs éléments graphiques pour faciliter la visualisation des entités du centre de données, des flux de trafic et de certaines activités dans votre environnement NSX-T Data Center.

Le tableau suivant répertorie un glossaire d'éléments graphiques de NSX-T Data Center que vous pouvez voir dans une visualisation NSX Intelligence.

Élément graphique	Description
	Cette icône représente un groupe, qui est un ensemble de VM dans lesquelles des stratégies de sécurité, y compris les règles de pare-feu est-ouest, peuvent être appliquées. Reportez-vous à la section Utilisation de la vue Groupes .
	Cette icône représente une machine virtuelle (VM) qui fait partie de votre NSX-T Data Center. Une VM peut appartenir à plusieurs groupes. Reportez-vous à la section Utilisation de la vue VM .
	Cette icône représente les adresses IP publiques sur Internet. Si au moins une VM de votre environnement NSX-T Data Center a communiqué avec une adresse IP publique au cours de la période sélectionnée, ce flux de trafic est inclus dans la visualisation actuelle.
	Une adresse IP, telle qu'une adresse IP de monodiffusion, de diffusion ou de multidiffusion, qui a participé aux activités du trafic réseau au cours de la période sélectionnée.
<div>VM non classées (4)</div> 	Cette icône est utilisée pour le groupe de VM qui n'appartiennent pas à un groupe.
	Une flèche représente un flux de trafic réseau qui s'est produit entre deux VM pendant une période sélectionnée. Il existe trois types différents de flèches : une flèche en pointillés de teinte rouge pour un flux non protégé, une flèche pleine de teinte bleue pour un flux bloqué et une flèche pleine de teinte verte pour un flux Autorisé. Reportez-vous à la section Utilisation des flux de trafic .
	Un nœud qui a été choisi comme nœud actuel est entouré d'un cercle en pointillés. Il s'agit du nœud épinglé pendant le mode de sélection et la vue actuelle affichée.
	Cette icône apparaît sur la bordure d'un nœud de groupe si le groupe a été ajouté dans l'inventaire NSX-T Data Center au cours de la période sélectionnée. Si NSX-T Data Center a découvert une VM au cours de la période sélectionnée, l'icône s'affiche sur la bordure de ce nœud de VM.

Élément graphique	Description
	Cette icône apparaît sur la bordure du nœud de groupe si le groupe a été supprimé au cours de la période sélectionnée et si les membres de la VM n'ont pas été supprimés. Sur la bordure d'un nœud de VM, cette icône indique que la VM a été supprimée au cours de la période sélectionnée. Même si une VM ou un groupe a été supprimé, il apparaît toujours dans la visualisation actuelle pour donner une vue historique que la VM ou le groupe a été supprimé au cours de la période sélectionnée.
	<p>Cette icône s'affiche chaque fois que le groupe et les VM sont regroupés. Par exemple, dans une vue de groupes d'analyse approfondie ou les VM associées d'un groupe.</p> <p>L'icône s'affiche sur la bordure d'un nœud de VM dans les cas suivants.</p> <ul style="list-style-type: none"> ■ Si la VM a été déplacée du groupe actuellement consulté au cours de la période sélectionnée ■ Si, à un moment donné, au cours de la période sélectionnée, la VM faisait partie du groupe que vous êtes en train de consulter, mais n'est plus membre de ce même groupe

Présentation des vues et des flux de NSX Intelligence

La visualisation de NSX Intelligence est composée des groupes ou des VM, ainsi que des flux réseau qui sont survenus avec ces groupes ou VM au cours de la période sélectionnée.

Important La visualisation affichée pour une période spécifique représente l'ensemble des flux et activités du réseau, tels que l'ajout, la suppression ou le déplacement de VM et de groupes, qui sont survenus dans votre centre de données NSX-T pendant cette période. Il est possible qu'une VM apparaisse plusieurs fois dans la visualisation. Par exemple, si une VM a été attachée à un hôte ESXi qui n'a pas été initialement géré et que l'hôte est géré par un serveur VMware vCenter Server™ au cours de la période sélectionnée, la VM apparaît deux fois dans la vue VM. De même, si un hôte ESXi est déconnecté de vCenter Server et ajouté à nouveau pendant la même période sélectionnée, les VM attachées à l'hôte s'affichent comme étant à la fois supprimées et nouvelles au cours de la période sélectionnée. Dans la vue Groupes, si une VM se trouvait dans le groupe Non classées et a été ajoutée à un groupe pendant la même période sélectionnée, la VM apparaît dans le groupe Non classées et dans son nouveau groupe.

NSX Intelligence prend en charge les groupes comptant des membres de type VM uniquement. Si vous disposez de groupes comptant d'autres types de membres, la vue Groupes peut afficher des flux corrélés entre les groupes avec des types de membres de VM plutôt que des groupes réels dans la règle de sécurité.

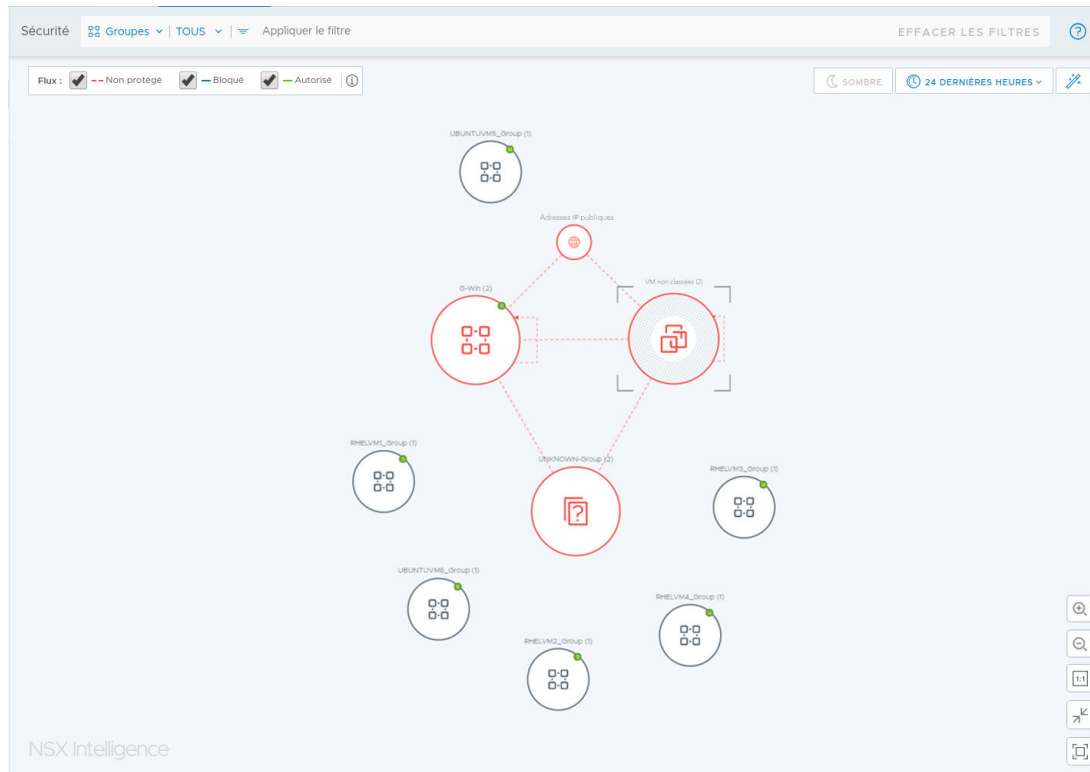
Utilisez les informations de cette section pour en savoir plus sur l'utilisation de la vue Groupes, la vue VM et les différents flux de trafic.

Utilisation de la vue Groupes


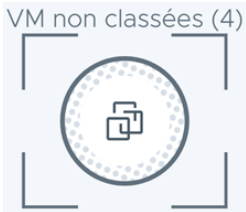
La vue par défaut qui s'affiche sur la page d'accueil de NSX Intelligence est la vue Groupes. Cette vue Groupes est filtrée pour afficher tous les groupes dont le flux de trafic n'a pas été protégé au cours des dernières 24 heures.



Nœuds et flèches dans une vue Groupes

Un nœud dans une vue Groupes représente des objets NSX, tels que des machines virtuelles, des ensembles d'adresses IP, etc., dans votre environnement NSX-T Data Center. La capture d'écran suivante est un exemple d'une vue Groupes.



Le tableau suivant répertorie les types de nœuds de groupe que vous pouvez voir dans la vue Groupes.

Type de nœud de groupe	Icône	Description
Groupe standard		Un nœud de groupe standard dans NSX Intelligence représente tout ensemble d'objets NSX dans votre environnement NSX-T Data Center. Dans cette version, ces objets NSX ne sont que des machines virtuelles et NSX Intelligence prend en charge des groupes standard avec des membres de type VM uniquement. Un objet NSX peut appartenir à plusieurs groupes. Une machine virtuelle peut donc apparaître dans plusieurs nœuds de groupe.
Groupe non classé		Un nœud de groupe non classé représente un ensemble de VM qui n'appartiennent à aucun groupe.

Type de nœud de groupe	Icône	Description
Groupe inconnu		Un nœud de groupe inconnu représente un ensemble d'objets divers qui n'ont pas été trouvés dans votre inventaire NSX-T Data Center. Toutefois, ces objets communiquent avec un ou plusieurs objets NSX de votre environnement NSX-T Data Center.
Groupe d'adresses IP publiques		Un nœud de groupe d'adresses IP publiques représente un ensemble d'adresses IP publiques (IPv4 ou IPv6) qui communiquent avec les objets NSX dans votre NSX-T Data Center.

La taille d'un nœud dans la vue Groupes dépend du nombre d'objets NSX, comme les machines virtuelles, qui appartiennent à ce groupe. Plus le nœud du groupe est grand, plus ce groupe contient de VM, par exemple. Le nom du groupe et le nombre total de VM membres qu'il contient s'affichent au-dessus du nœud.

Les flèches entre les nœuds de groupe représentent les flux de trafic qui se sont produits entre les VM dans les nœuds de groupe connectés pendant la période sélectionnée. Une flèche d'auto-référencement sur un nœud de groupe indique qu'au moins une VM communique avec une autre VM au sein de ce même groupe. Pour plus d'informations, reportez-vous à la section [Utilisation des flux de trafic](#).

Un nœud délimité par une bordure de teinte rouge indique qu'au moins un flux non protégé est survenu avec une VM dans le groupe, quel que soit le nombre de flux bloqués ou autorisés détectés au cours de la période sélectionnée. Une bordure de teinte bleue sur un nœud signifie qu'aucun flux de trafic non protégé n'a été détecté, mais qu'au moins un flux bloqué a été détecté, quel que soit le nombre de flux autorisés détectés au cours de la période sélectionnée. Un nœud délimité par une bordure de teinte verte indique qu'aucun flux non protégé ou bloqué n'a été détecté au cours de la période sélectionnée et qu'au moins un flux autorisé a été détecté. Un nœud délimité par une bordure de teinte grise signifie qu'aucun flux de trafic n'a été détecté pour les VM appartenant à ce groupe au cours de la période sélectionnée.

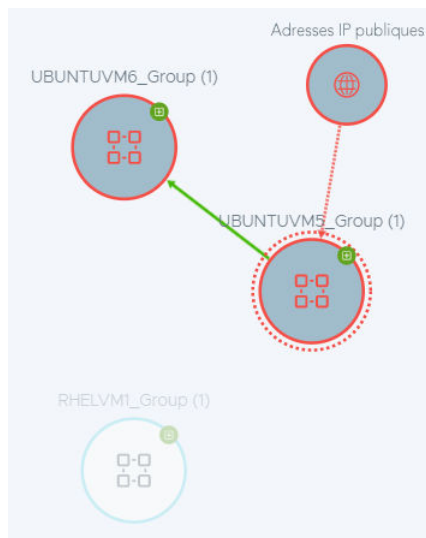
Si vous ne voyez pas apparaître la vue Groupes, cliquez sur la flèche vers le bas en regard de **VM** dans la zone de sélection de la vue Sécurité et sélectionnez **Groupes**. Dans la liste déroulante de sélection affichée, vous pouvez sélectionner **Tous les groupes** ou des groupes spécifiques de la liste, puis cliquer sur **Appliquer**. Utilisez la zone de texte **Rechercher** pour filtrer la liste de sélection. Si vous cliquez en dehors de la liste déroulante de sélection sans effectuer de sélection ou si vous sélectionnez **Tous les groupes** dans la liste déroulante, l'option **Tous les groupes** est appliquée à la vue Groupes.

Sélection de nœud dans la vue Groupes

Lorsque vous pointez vers le nœud d'un groupe, des informations sur ce groupe s'affichent, comme indiqué dans l'exemple suivant pour le groupe G-Win. Le nombre et les types de flux détectés au cours de la période sélectionnée sont également répertoriés. Si le groupe a été ajouté au cours de la période sélectionnée, l'icône Nouveau badge et les détails sur la date de création du groupe s'affichent également.



Lorsque vous cliquez sur le nœud d'un groupe, un cercle en pointillés indique la sélection d'un nœud de VM épinglé. Les autres groupes qui sont connectés au nœud de groupe sélectionné sont également rendus plus visibles dans la vue. Tous les autres nœuds sont grisés. Par exemple, dans la capture d'écran suivante, UBUNTUVM5_Group est sélectionné et les autres groupes qui ont partagé un flux de trafic avec UBUNTUVM5_Group au cours de la période sélectionnée sont également mis en surbrillance. Tous les autres groupes qui n'ont pas communiqué avec UBUNTUVM5_Group sont estompés dans la vue.

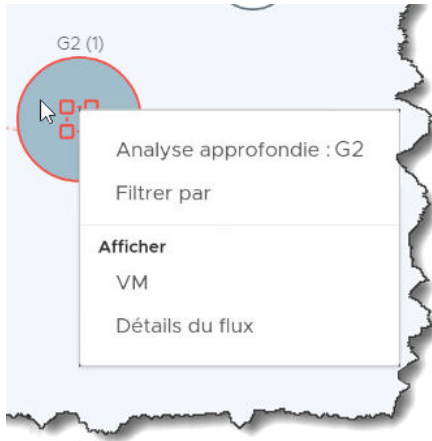


Pour effacer la sélection épinglée, cliquez sur n'importe quelle zone vide de la vue Groupes.

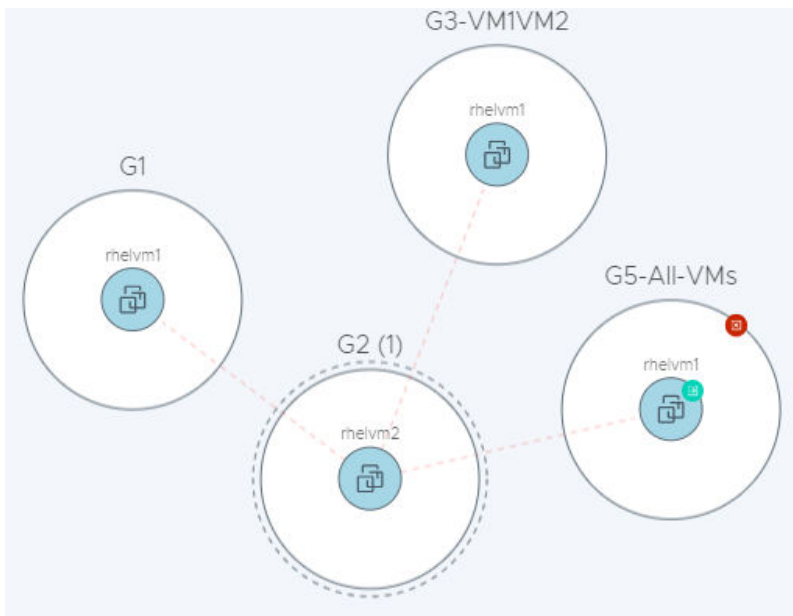
Si vous effectuez un zoom arrière de la vue Groupes et que les détails des nœuds ne sont plus visibles, pointez vers n'importe quelle partie visible d'un nœud et ses détails s'affichent.

Actions disponibles dans la vue Groupes

Un menu contextuel des actions disponibles s'affiche lorsque vous cliquez avec le bouton droit sur le nœud d'un groupe, comme illustré dans l'image suivante.



- La sélection de **Analyse approfondie : *Nom_Groupe*** entoure le nœud du groupe sélectionné d'un cercle en pointillés pour le marquer comme nœud de groupe épinglé ou groupe actuel. Les VM qui appartiennent au groupe sont affichées à l'intérieur du nœud du groupe. Tous les groupes qui comportaient des flux de trafic avec les VM dans le groupe épinglé au cours de la période sélectionnée sont également placés dans la vue Groupes. Dans l'exemple suivant, le groupe G2 est le groupe épinglé et les autres groupes se trouvent dans la vue, car leurs membres de VM incluaient des flux de trafic avec rhelvm2 dans le groupe G2 au cours de la période sélectionnée.



- Lorsque vous sélectionnez **Filtrer par**, le groupe actuel est ajouté au filtre de visualisation utilisé pour la vue Groupes actuelle.

- La sélection de **VM** affiche un tableau de toutes les VM qui appartaient au groupe actuel au cours de la période sélectionnée. À partir de ce tableau de vue des VM, vous pouvez afficher les détails sur les VM qui appartiennent au groupe sélectionné et les autres groupes auxquels chaque VM appartient également. Pour ajouter la VM au filtre de visualisation actuel, cliquez sur l'icône de filtre.
- Lorsque vous sélectionnez **Détails du flux**, le tableau Détails du flux pour le groupe actuellement sélectionné s'affiche, comme indiqué dans la capture d'écran suivante. Il affiche les détails sur les flux qui sont survenus et qui sont actuellement activés avec les VM appartenant au groupe actuel au cours de la période sélectionnée. Les détails incluent le type de flux, les groupes source et cible du flux, l'heure de début et de fin du flux, ainsi que les services qui ont été utilisés. Vous pouvez cliquer sur quelques-uns des détails pour obtenir de plus amples informations. Pour plus d'informations, reportez-vous à la section [Utilisation des flux de trafic](#).

Détails du flux 🕒 24 dernières heures ✕

Affichage des détails de flux pour VM non classées

Flux terminés Flux actifs

Rechercher

Source	Groupe source	Destination	Groupe de destination	Services	Heure de fin	Flux le plus r
ubuntu12.04.1-2G-L...	G5	ubuntu12.04-...	UNCATEGORIZED	SSH... +2 de plus	06/11/2019 08:05	● Non pro
ubuntu12.04.1-2G-L...	G1	ubuntu12.04-...	UNCATEGORIZED	SSH... +2 de plus	06/11/2019 08:05	● Non pro

Actualiser 1 - 2 of 2 Flux

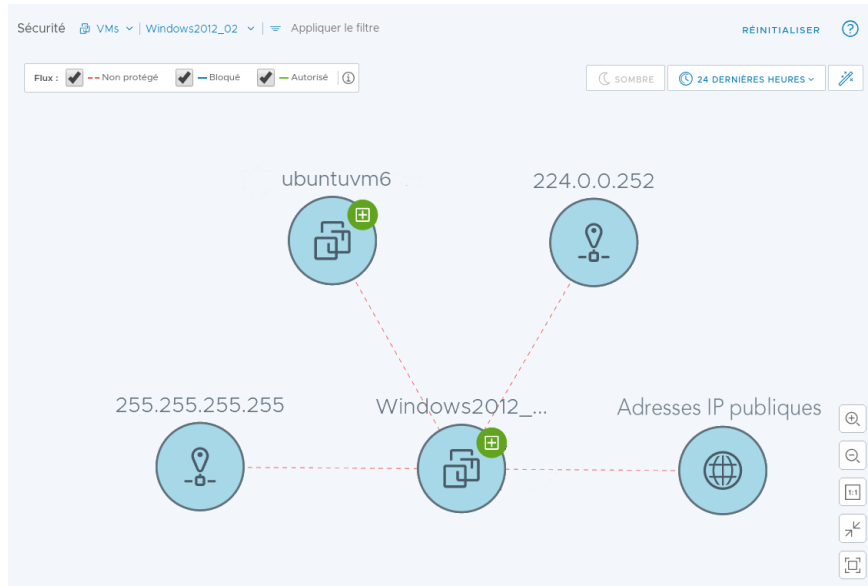
FERMER

Utilisation de la vue VM

Un nœud dans la vue VM représente une machine virtuelle (VM) dans votre environnement NSX-T Data Center sur site.

Nœuds et flèches dans la vue VM

Dans la vue VM, les limites du groupe ne sont pas visibles. Tout nœud qui communique avec l'une des VM dans votre environnement NSX-T Data Center, mais qui n'a pas été identifié comme appartenant à l'inventaire NSX-T Data Center est également représenté dans la vue VM. Les éléments suivants illustrent une vue VM simple.



Le tableau suivant répertorie les types de nœuds VM que vous pouvez voir dans la vue Vues.

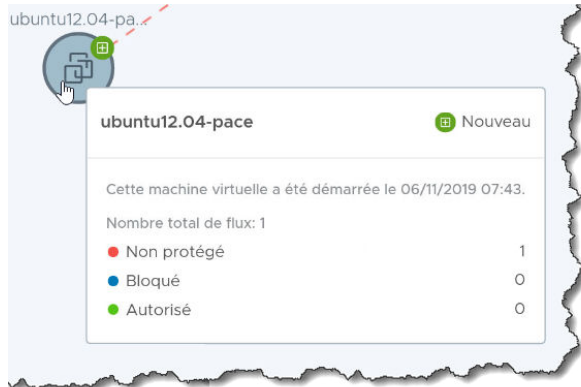
Type de nœud VM	Icône	Description
VM standard		Un nœud VM standard représente une machine virtuelle (VM) qui fait partie de votre environnement NSX-T Data Center. Une VM peut appartenir à plusieurs groupes.
Adresse IP publique		Un nœud Adresse IP publique représente une adresse IP publique, IPv4 ou IPv6, qui communique vers ou depuis votre environnement NSX-T Data Center.
IP		Un nœud IP représente une adresse IP qui a participé aux activités du trafic réseau pendant la période sélectionnée. Une adresse IP peut être une adresse IP de monodiffusion, de diffusion ou de multidiffusion.

Si la vue VM n'est pas visible, cliquez sur la flèche vers le bas en regard de **Groupes** dans la zone de sélection de la vue Sécurité et sélectionnez **VM**. Dans la liste déroulante de sélection qui s'affiche, vous pouvez sélectionner **Toutes les VM** ou des VM spécifiques dans la liste, puis cliquer sur **Appliquer**. Utilisez la zone de texte **Rechercher** pour filtrer la liste de sélection. Si vous cliquez à l'extérieur de la liste déroulante sans effectuer de sélection ou si vous sélectionnez **Toutes les VM** dans la liste déroulante, l'option **Toutes les VM** est appliquée à la vue VM.

Les flèches entre les nœuds VM représentent les flux de trafic qui ont eu lieu entre les VM au cours de la période sélectionnée. Pour plus d'informations, reportez-vous à la section [Utilisation des flux de trafic](#).

Sélection de nœud dans la vue VM

Lorsque vous pointez vers un nœud VM, des informations sur le nœud s'affichent, comme indiqué dans l'exemple suivant. Le nombre et les types de flux vers les VM qui ont été détectés au cours de la période sélectionnée sont répertoriés. Si le groupe a été ajouté au cours de la période sélectionnée, l'icône Nouveau badge et la date d'ajout de la VM s'affichent également.

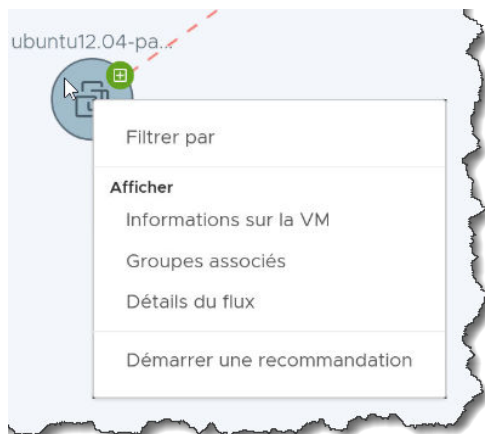


Lorsque vous cliquez sur le nœud d'une VM, un cercle en pointillés indique la sélection d'un nœud de VM épinglé. Les autres nœuds de VM qui avaient des flux de trafic avec ce nœud de VM épinglé sont également plus visibles dans la vue VM. Tous les autres nœuds sont grisés pour les rendre moins visibles. Pour effacer la sélection épinglée, cliquez sur n'importe quelle zone vide de la vue VM.

Lorsque vous effectuez un zoom arrière de la vue VM et que les détails des nœuds de VM ne sont plus visibles, pointez vers n'importe quelle partie visible d'un nœud VM et ses détails s'affichent.

Actions disponibles dans la vue VM

Un menu contextuel des actions disponibles s'affiche lorsque vous cliquez avec le bouton droit sur le nœud d'une VM, comme illustré dans l'image suivante.



Sélection	Description
Filtrer par	La VM est ajoutée au filtre de visualisation qui est utilisé pour la vue VM actuelle.
Informations sur la VM	Les détails de la VM au cours de la période sélectionnée sont affichés.




Sélection	Description
Groupes associés	Tableau Groupes contenant des informations sur les groupes auxquels la VM a appartenu au cours de la période sélectionnée.
Détails du flux	<p>Affiche les détails des flux qui ont eu lieu et qui sont actuellement activés avec la VM au cours de la période sélectionnée. Les détails sont les suivants.</p> <ul style="list-style-type: none"> ■ type de flux ■ groupes source et groupes de destination du flux ■ heure de début et heure de fin du flux ■ services qui ont été utilisés <p>Vous pouvez cliquer sur certains détails pour obtenir de plus amples informations. Pour plus d'informations, reportez-vous à la section Utilisation des flux de trafic.</p>
Démarrer une recommandation	Affiche l'assistant Démarrer de nouvelles recommandations. Pour plus d'informations, reportez-vous à la section Utilisation des recommandations de NSX Intelligence .

Utilisation des flux de trafic

Les flèches entre les nœuds de groupe ou de VM représentent les flux de trafic réseau qui sont survenus entre les VM au cours de la période sélectionnée.

Les flux de trafic réseau sont basés sur les règles de pare-feu distribué de couche 3 (DFW) en place et les flux de trafic qui sont survenus au cours de la période sélectionnée. Tous les flux de trafic réseau qui correspondaient à une règle DFW de couche 3 avec état via IPv4 ou IPv6 avec les protocoles TCP, UDP, GRE, ESP et SCTP sont inclus dans la visualisation et les détails du flux. Les flux TCP et UDP présentent des détails de niveau IP et de port. D'autres comportent uniquement des détails de niveau IP.

Les flux de trafic sont classés selon les types suivants.

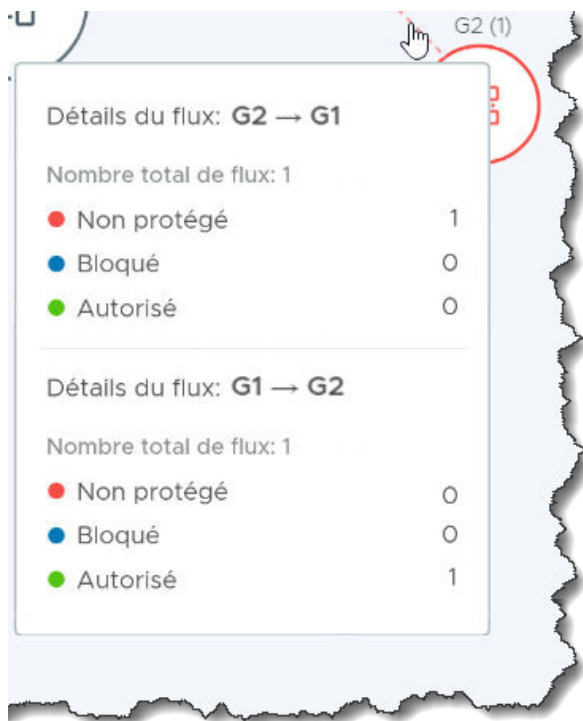
Type de flux	Graphique	Description
Non protégé		Une flèche en pointillés de teinte rouge indique que le système a détecté que le flux de trafic a rencontré une règle (source : Toute Destination : Toute Action : Autoriser, Rejeter ou Abandonner) et que des stratégies de sécurité granulaires sont nécessaires. Cette règle peut être votre règle par défaut, ou elle peut résider n'importe où dans le pare-feu distribué est-ouest.
Bloqué		Une flèche pleine de teinte bleue indique que le système a détecté que le flux de trafic a rencontré une règle « Refuser » ou « Annuler » qui est plus granulaire que celle mentionnée dans la définition de flux « Non protégé ».
Autorisé		Une flèche pleine de teinte verte indique que le système a détecté que le flux de trafic a rencontré une règle « Autoriser » qui est plus granulaire que celle mentionnée dans la définition de flux « Non protégé ».

Pour se concentrer uniquement sur les objets comprenant certains types de flux de trafic, utilisez la zone de sélection de vue Sécurité pour sélectionner le type de vue, et utilisez l'attribut de filtre « Type de flux » pour restreindre la sélection.

Si vous désélectionnez un type de flux, les lignes de flux pour ce type de flux sont masquées du graphique affiché. À moins que les filtres en effet qui excluent certains objets, tous les objets de groupe ou de VM demeurent affichés, quels que soient les types de flux de trafic qui sont survenus avec ces objets au cours de la période sélectionnée. Par exemple, si vous désélectionnez le type de flux « Autorisé », toutes les lignes de flux « Autorisé » sont masquées dans le graphique. Cependant, tous les objets sont toujours affichés, même ceux qui ne comportaient que des flux de trafic « Autorisé » au cours de la période sélectionnée.

La direction d'une flèche de flux indique la source et la destination du flux de trafic détecté. Dans la vue Groupes, une flèche d'auto-référencement sur un nœud de groupe indique qu'au moins une VM communiquait avec une autre VM dans ce même groupe. Dans une vue VM, une flèche d'auto-référencement indique qu'un objet NSX dans la VM a communiqué avec un autre objet NSX dans la même VM.

Lorsque vous pointez vers une flèche de flux, des informations sur les flux impliquant le groupe ou la VM s'affichent, comme indiqué dans l'exemple suivant pour le groupe G2.



Lorsque vous cliquez sur une flèche de flux, la boîte de dialogue Détails du flux est affichée. Elle affiche les détails sur les flux terminés et actifs qui sont survenus au cours de la période sélectionnée. Pour obtenir des informations plus détaillées sur la source, la destination, le type de service et le type de flux, cliquez sur les liens dans le tableau pour afficher d'autres détails.

Utilisation des recommandations de NSX Intelligence

NSX Intelligence peut fournir des recommandations de micro-segmentation basées sur les modèles de flux de trafic qui se sont produits entre les machines virtuelles de votre environnement NSX-T Data Center pendant une période sélectionnée.

Comprendre les recommandations de NSX Intelligence

Les recommandations que NSX Intelligence génère incluent des stratégies de sécurité, des groupes de sécurité de stratégie et des services pour des applications.

Les recommandations sont basées sur les modèles de flux de trafic réseau entre les charges de travail de machine virtuelle sur des hôtes ESXi gérés par un vCenter Server. Elles peuvent vous aider à appliquer une stratégie de sécurité plus dynamique en mettant en corrélation les modèles de trafic de communication qui se produit dans votre environnement NSX-T Data Center.

Les recommandations de stratégie de sécurité font partie de la catégorie Stratégies de sécurité de pare-feu distribué est-ouest d'application. Les recommandations de groupe de sécurité prennent la forme d'une liste de machines virtuelles qui sont visibles dans les flux de trafic réseau qui ont été analysés pendant la période de temps et la limite de machine virtuelle que vous avez spécifiées. Les recommandations de service sont des objets de service qui ont été utilisés dans certains ports par des applications dans les machines virtuelles que vous avez spécifiées, mais les services ne sont pas encore définis dans l'inventaire de NSX-T Data Center.

Il existe plusieurs manières de demander la recommandation, mais la plus simple consiste à utiliser l'onglet **Planifier et dépanner > Recommandations** et à cliquer sur **Commencer une nouvelle recommandation**. Vous fournissez les machines virtuelles qui comprennent les limites d'application et la plage de temps pendant laquelle les flux de trafic réseau doivent être analysés pour ces machines virtuelles spécifiques. Une fois l'analyse de recommandation terminée, vous pouvez afficher les détails de la recommandation et, si nécessaire, modifier la recommandation avant de la publier. Pour plus d'informations, reportez-vous à la section [Générer une nouvelle recommandation de NSX Intelligence](#).

Générer une nouvelle recommandation de NSX Intelligence

La fonctionnalité Recommandations de NSX Intelligence peut vous fournir des recommandations pour vous aider à micro-segmenter vos applications.

La génération d'une recommandation de NSX Intelligence implique des recommandations de stratégies de sécurité, de groupes de sécurité de stratégie et de services pour l'application. Les recommandations sont établies en fonction du modèle de trafic de communication entre les machines virtuelles de votre NSX-T Data Center. Il existe plusieurs manières de générer une recommandation à l'aide de l'interface utilisateur de NSX Intelligence. La procédure suivante décrit les trois méthodes disponibles à utiliser.

Conditions préalables

Installez NSX Intelligence. Reportez-vous à la section « Installation et configuration de NSX Intelligence » dans *Guide d'installation de NSX-T Data Center*.

Procédure

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

2 Initiez la génération d'une nouvelle recommandation.

Utilisez le tableau suivant pour déterminer les trois méthodes disponibles à utiliser.

Méthode	Étape
Sélectionnez Planifier et dépanner > Recommandations .	Cliquez sur Commencer une nouvelle recommandation .
Dans la vue VM, sélectionnez une VM et cliquez dessus avec le bouton droit.	Dans le menu contextuel, sélectionnez Démarrer de nouvelles recommandations .
Sélectionnez Planifier et dépanner > Découvrir et prendre une mesure .	<ol style="list-style-type: none"> 1 Dans le filtre Position de sécurité, cliquez sur la flèche vers le bas et sélectionnez VM. 2 Sélectionnez les VM qui composent la limite d'application et cliquez sur Appliquer. 3 Cliquez sur l'icône en forme de baguette Recommandations . 4 Dans la boîte de dialogue Recommandations, cliquez sur Commencer une nouvelle recommandation.

3 Dans l'assistant Commencer une nouvelle recommandation, modifiez éventuellement la valeur par défaut de **Nom de la recommandation**.

4 Définissez ou modifiez les machines virtuelles à utiliser comme limite pour la recommandation de stratégie de sécurité.

- a Cliquez sur **Sélectionner les machines virtuelles** ou le nombre de **VM sélectionnées**.
- b Dans la boîte de dialogue Sélectionner les machines virtuelles, sélectionnez les machines virtuelles que vous voulez utiliser comme limite pour l'analyse et désélectionnez celles que vous ne voulez pas inclure.

Vous pouvez sélectionner jusqu'à 100 machines virtuelles à utiliser pour la limite de recommandation. Vous pouvez également commencer à entrer le nom dans la barre de sélection pour filtrer les machines virtuelles à sélectionner.

- c Cliquez sur **Enregistrer**.

Le nombre de machines virtuelles sélectionnées est indiqué dans la boîte de dialogue Découvrir une nouvelle recommandation.

5 Développez **Plus d'options** pour modifier les valeurs par défaut de **Description** et **Intervalle de temps** qui sont utilisées pour l'analyse de recommandation. La valeur par défaut **Intervalle de temps** est Dernier mois, ce qui signifie que les flux de trafic réseau qui sont survenus au cours du mois dernier entre les VM sélectionnées sont utilisés lors de l'analyse des recommandations.

6 Cliquez sur **Démarrer la découverte**.

Les recommandations sont traitées en série. En moyenne, la finalisation de chaque recommandation peut prendre entre 3 et 4 minutes, selon que d'autres recommandations sont ou non en attente de traitement. S'il existe de nombreux flux de trafic entre les VM

qui doivent être analysées, la génération d'une recommandation peut prendre entre 10 et 15 minutes. L'état peut être suivi dans l'onglet **Recommandations**. Voici les états successifs : Attente, Analyse, et enfin Prêt à publier. La capture d'écran suivante montre les trois états différents des recommandations générées.

	Nom	État	VM	Heure de création	Dernière modification
⋮ >	REC 20191107 10:09:19	Aucune recommandation disponible	6	07/11/2019 02:09	07/11/2019 02:09
⋮ >	REC 20191106 16:39:30	Aucune recommandation disponible	1	06/11/2019 08:39	06/11/2019 08:39
⋮ >	REC 20191106 16:15:53	Aucune recommandation disponible	1	06/11/2019 08:16	06/11/2019 08:16

Après la publication réussie d'une recommandation, l'état passe à Publié.

Étape suivante

Vérifiez la recommandation générée et décidez de la publier ou non. Reportez-vous à la section [Vérifier et publier une recommandation générée](#).

Vérifier et publier une recommandation générée

Une fois que la recommandation de NSX Intelligence générée atteint l'état Prêt à publier, vous pouvez passer en revue la recommandation, la modifier si nécessaire et décider de la publier ou non.

Conditions préalables

Générez une nouvelle recommandation. Reportez-vous à la section [Générer une nouvelle recommandation de NSX Intelligence](#).

Procédure

- 1 Dans le navigateur, connectez-vous avec des privilèges d'administrateur d'entreprise à un dispositif NSX Manager sur <https://<nsx-manager-ip-address>>.
- 2 Cliquez sur **Planifier et dépanner > Recommandations**.
- 3 Pour faciliter la réduction de la liste des recommandations affichées, cliquez sur **Filtrer par Nom, Chemin ou plus** dans la partie supérieure droite de l'écran, puis spécifiez les critères de filtrage souhaités.
- 4 Si vous décidez de ne pas utiliser la recommandation, cliquez sur l'icône du menu à trois points et sélectionnez **Supprimer**.
- 5 Pour afficher le résumé d'une recommandation, cliquez sur la flèche en regard du nom de la recommandation pour développer la ligne.

Vous voyez apparaître le nombre de règles générées et le nombre de groupes affectés.

6 Vérifiez et gérez les détails de la recommandation.

- a Cliquez sur le nom de la recommandation.

L'assistant **Recommendations** s'affiche, comme illustré dans l'image suivante.

Recommendations

REC 20190719 15:59:02

Showing discovered recommendations. Review, Edit and Proceed with your selections to place the rules in the existing Firewall context.

Recommended FW Rules Recommended Groups Recommended Services

Category: Application Recommended Rules: 6 Recommended Groups: 3 Recommended Services: 0

Name	Sources	Destinations	Services	Profiles	Applied To	Action	
Policy-1 (REC 20190719 15:59:02)	(6)						
Rule-1 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	Win - RPC, DCOM, EP...	None	DFW	Allow	<input checked="" type="checkbox"/>
Rule-2 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	NBDS-Broadcast-V1	None	DFW	Allow	<input checked="" type="checkbox"/>
Rule-3 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	DHCP-Server	None	DFW	Allow	<input checked="" type="checkbox"/>
Rule-4 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	DHCPv6 Server	None	DFW	Allow	<input checked="" type="checkbox"/>
Rule-5 (REC 20190719 15:59:02)	Group-1 (REC 20190719 15:59:02)	Any	NBNS-Broadcast-V1	None	DFW	Allow	<input checked="" type="checkbox"/>
Rule-6 (REC 20190719 15:59:02)	Group-2 (REC 20190719 15:59:02)	Group-3 (REC 20190719 15:59:02)	SSH	None	Group-2 (REC 20190719 15:59:02)	Allow	<input checked="" type="checkbox"/>

1 of 1 Policy

CANCEL CONTINUE LATER NEXT

- b Dans l'onglet **Règles de pare-feu recommandées**, vérifiez les détails des règles de pare-feu. Pour modifier des détails, cliquez sur la valeur dans la colonne appropriée et sélectionnez l'icône d'édition (crayon).
- c Pour définir le mode de traitement des paquets, sélectionnez **Autoriser**, **Annuler** ou **Refuser** dans la colonne **Action**.
- d Basculez le bouton sur le côté droit pour activer ou désactiver la règle. Par défaut, la règle qui a été générée est définie pour être activée lors de la publication, comme indiqué dans l'image à l'étape précédente.
- e Cliquez sur **Groupes recommandés**.
- f Cliquez sur le lien dans la colonne **Membres** pour vérifier les détails des machines virtuelles et des adresses IP qui ont été définies pour la recommandation de groupe.
- g Cliquez sur l'icône du menu (trois points) en regard du nom du groupe et sélectionnez **Modifier** pour modifier la recommandation de groupe.
- h Cliquez sur **Services recommandés** et examinez les détails.
- i Cliquez sur l'icône du menu (trois points) en regard du nom du service et sélectionnez **Modifier** pour modifier le nom ou la description. Avant de supprimer un service, assurez-vous qu'aucune règle ne l'utilise.
- j Cliquez sur **Suivant**.

- 7 Dans le volet **Placer des règles dans le contexte de pare-feu**, vous pouvez modifier l'ordre dans lequel la recommandation de règle doit être appliquée avec les règles de pare-feu existantes. Faites glisser la section en surbrillance ou cliquez sur l'icône du menu à trois points et sélectionnez **Déplacer au-dessus de la section sélectionnée** ou **Déplacer en dessous de la section sélectionnée**.
- 8 Cliquez sur **Publier**.
- 9 Dans la boîte de dialogue **Publier des recommandations**, cliquez sur **Oui**.
- 10 Sur la page Résumé d'application, vérifiez que les stratégies de sécurité ont été correctement publiées et cliquez sur **Fermer**.

La colonne État de la recommandation est remplacée par la colonne Publiée dans le tableau des recommandations.

Résultats

Une fois que les recommandations de stratégie de sécurité ont été publiées correctement, elles sont en mode lecture seule dans l'onglet **Planifier et dépanner > Recommandations**. Pour afficher et gérer les recommandations de règle publiées, accédez à **Sécurité > Pare-feu distribué**.

Important Une fois que vous avez publié les recommandations de règle, la visualisation continue d'afficher les flux concernés entre les VM sous forme de flèches de teinte orange (flux non protégés) jusqu'à ce que de nouveaux flux soient générés entre les VM concernées. La visualisation signale uniquement les flux de trafic en fonction de l'heure à laquelle ils sont survenus sur l'hôte et ne reflète pas l'ensemble de règles publié une fois ces flux de trafic survenus. Une fois que l'ensemble de règles est publié et que de nouveaux flux de trafic sont générés, les nouveaux flux sont affichés sous forme de flèches de teinte verte (flux autorisés).

Sauvegarde et restauration de NSX Intelligence

Si votre configuration actuelle de NSX Intelligence devient inopérable ou si vous voulez rétablir son état précédent, vous pouvez restaurer votre configuration à partir d'une sauvegarde. Le workflow de sauvegarde et de restauration n'est pris en charge qu'à l'aide de l'interface de ligne de commande de NSX Intelligence.

Lorsque vous effectuez une sauvegarde, NSX Intelligence sauvegarde uniquement les fichiers de configuration utilisés par tous les services qui composent le dispositif NSX Intelligence. Aucune donnée de visualisation n'est incluse dans la sauvegarde.

Si les données sont perdues ou corrompues dans NSX Intelligence, toutes les données existantes pour les flux et recommandations corrélés sont également perdues. La réinstallation de NSX Intelligence redémarre la collecte des données de trafic réseau et la visualisation de ces données collectées est disponible à partir de ce moment-là.

Après avoir terminé la configuration de la sauvegarde, vous pouvez exécuter manuellement la commande de sauvegarde sur le dispositif NSX Intelligence à tout moment. La sauvegarde est chiffrée, compressée et stockée sur le serveur distant défini lors de la configuration de la sauvegarde. Lorsque vous créez une sauvegarde, la date et l'heure de la sauvegarde sont ajoutées au nom de fichier de sauvegarde pour que chaque fichier de sauvegarde soit unique. Par exemple, `config-backup-2019-06-21T21_06_07UTC.tar.gz`.

Lorsque vous restaurez une sauvegarde de NSX Intelligence, l'état de configuration lors de la capture de la sauvegarde est restauré. Vous devez restaurer la sauvegarde sur un dispositif NSX Intelligence qui exécute la même version du dispositif NSX Intelligence à partir duquel le fichier de sauvegarde a été créé. Vous pouvez restaurer un dispositif NSX Intelligence existant ou restaurer un dispositif NSX Intelligence récemment installé, mais ils doivent être de la même version que le dispositif NSX Intelligence que vous avez sauvegardé.

Configurer des sauvegardes NSX Intelligence

Vous devez configurer un serveur de fichiers de sauvegarde avant de pouvoir effectuer une sauvegarde de votre configuration de NSX Intelligence. Une fois qu'un serveur de fichiers de sauvegarde est configuré, vous pouvez effectuer une sauvegarde de NSX Intelligence à tout moment.

Conditions préalables

- Vérifiez que vous disposez des informations d'identification d'administrateur d'interface de ligne de commande pour l'interface de ligne de commande de NSX Intelligence.
- Assurez-vous que vous disposez du nom d'utilisateur et du mot de passe du serveur distant.
- Obtenez le chemin d'accès au dossier dans lequel les fichiers de sauvegarde doivent être stockés sur le serveur distant.

Procédure

- 1 À partir d'une invite de ligne de commande, connectez-vous avec des privilèges d'administrateur à l'hôte d'interface de ligne de commande de NSX Intelligence.

```
$ ssh admin@cli-ip-address
admin@cli-ip-address's password:
```

- 2 Configurez le serveur de fichiers de sauvegarde.

La syntaxe de la commande est

```
set backup remote-host remote_host_address remote-path remote_folder_path remote-host-username remote_host_username remote-host-password remote_host_password passphrase pass_phrase
```

où *remote_host_address* est l'adresse IP de l'hôte distant ou l'adresse de nom de domaine complet du serveur de fichiers de sauvegarde et le compte *remote_host_username*

doit disposer des privilèges nécessaires pour créer les fichiers de sauvegarde dans *remote_folder_path*. Vous devez fournir une valeur forte pour le paramètre *passphrase*. Il doit se composer d'au moins huit caractères dont au moins un caractère majuscule, un caractère minuscule et un caractère spécial. Par exemple,

```
set backup remote-host 10.11.22.33 remote-path /root remote-host-username root remote-host-
password MyRemotePassword passphrase MyPassPhra$e
```

3 Vérifiez la configuration.

```
get configuration
```

Dans la sortie, vérifiez que la ligne avec `set backup` est correcte. À l'aide de l'exemple de l'étape précédente, la sortie doit inclure la ligne suivante.

```
set backup remote-host 10.11.22.33 remote-path /root remote-host-username root
```

Sauvegarder NSX Intelligence

Vous pouvez sauvegarder les fichiers de configuration de votre dispositif NSX Intelligence à l'aide de la commande d'interface de ligne de commande.

Conditions préalables

- Assurez-vous que vous disposez d'un accès administrateur à l'interface de ligne de commande de NSX Intelligence.
- Configurez un serveur de fichiers de sauvegarde. Reportez-vous à la section [Configurer des sauvegardes NSX Intelligence](#).

Procédure

- 1 Connectez-vous avec des privilèges d'administrateur à l'interface de ligne de commande de NSX Intelligence.
- 2 Créez la sauvegarde.

```
backup intelligence configuration
```

Si la sauvegarde réussit, un message semblable au message suivant s'affiche.

```
Backup Complete. Archived at: backup_file_server-IP_address:/root/backup_archives/
intelligence-config-backup-2019-07-18T07_00_26UTC.tar.gz
```

- 3 Vous pouvez afficher l'avancée de la sauvegarde à l'aide d'une autre session d'interface de ligne de commande.
 - a Connectez-vous à une autre session d'interface de ligne de commande de NSX Intelligence.
 - b Entrez la commande suivante.

```
get log-file node-mgmt.log follow
```

Restaurer des sauvegardes de NSX Intelligence

Lorsque vous restaurez une sauvegarde, vous restaurez l'état de la configuration de NSX Intelligence au moment de la sauvegarde. Vous pouvez restaurer une sauvegarde de NSX Intelligence à l'aide d'une commande d'interface de ligne de commande.

Vous devez restaurer une sauvegarde sur une installation du dispositif NSX Intelligence ayant la même version que celle de la sauvegarde que vous restaurez. Par défaut, le fichier de sauvegarde restauré est la sauvegarde la plus récemment générée. Si vous restaurez une sauvegarde vers un dispositif NSX Intelligence récemment installé, définissez le nom de l'archive avant de restaurer la sauvegarde.

Conditions préalables

- Vérifiez que vous disposez des informations d'identification de connexion d'administrateur et des informations d'hôte du serveur de fichiers de sauvegarde.
- Assurez-vous que vous disposez d'un accès administrateur à l'interface de ligne de commande de NSX Intelligence.

Procédure

- 1 Connectez-vous avec des privilèges d'administrateur au nouveau serveur d'interface de ligne de commande de NSX Intelligence.
- 2 Configurez le serveur distant sur lequel se trouvent les sauvegardes.

La syntaxe de la commande est

```
set restore remote-host backup_server_IP_address remote-path remote_folder_path remote-host-username remote_host_username remote-host-password remote_host_password passphrase pass_phrase
```

où *backup_server_IP_address* est l'adresse IP de l'hôte distant ou l'adresse de nom de domaine complet du serveur de fichiers de sauvegarde, le compte *remote_host_username* doit disposer des privilèges nécessaires pour accéder aux fichiers de sauvegarde dans *remote_folder_path*. Par exemple,

```
set restore remote-host 10.11.22.33 remote-path /root remote-host-username root remote-host-password MyRemotePassword passphrase MyPassPhra$e
```

3 Vérifiez la configuration de restauration.

```
get configuration
```

Dans la sortie, vérifiez que la ligne avec `set restore` est correcte. À l'aide de l'exemple de l'étape précédente, la sortie doit inclure la ligne suivante.

```
set restore remote-host 10.11.22.33 remote-path /root remote-host-username root
```

4 Restaurez la sauvegarde avec la commande suivante.

```
restore intelligence configuration
```

Si la restauration réussit, un message semblable au message suivant s'affiche.

```
NSX Intelligence Restore Complete.
```

5 Vous pouvez afficher l'avancée de la restauration de sauvegarde à l'aide d'une autre session d'interface de ligne de commande.

- a Connectez-vous à une autre session d'interface de ligne de commande de NSX Intelligence.
- b Entrez la commande suivante.

```
get log-file node-mgmt.log follow
```

Dépannage des problèmes liés à NSX Intelligence

Si le dispositif NSX Intelligence cesse de répondre ou si vous avez besoin de plus amples détails sur un message d'erreur reçu lors de l'utilisation du dispositif, vous pouvez exécuter des commandes spécifiques pour connaître l'état des services NSX Intelligence.

Vous pouvez également collecter des bundles de support pour vous aider, ainsi que le personnel de support VMware, à résoudre les problèmes de débogage que vous avez pu rencontrer.

Vérifier l'état du dispositif NSX Intelligence

Si le dispositif NSX Intelligence ne répond plus, vérifiez l'état des services NSX Intelligence.

Problème

Le dispositif NSX Intelligence ne répond plus ou vous recevez un message d'erreur indiquant que le dispositif ne fonctionne pas comme prévu.

Cause

Il est possible qu'un ou plusieurs des services NSX Intelligence sous-jacents soient arrêtés ou que leur état ne soit pas intègre.

Solution

- 1 Connectez-vous à l'hôte CLI du dispositif NSX Intelligence à l'aide d'un compte doté du rôle d'administrateur d'entreprise.
- 2 Vérifiez l'état des services NSX Intelligence à l'aide de la commande `get services`.

Si tous les services NSX Intelligence fonctionnent correctement, une sortie similaire à l'exemple suivant s'affiche.

```
my_nsx-intel> get services
Service name:          druid
Service state:         running
Coordinator health:    good
Broker health:         good
Historical health:     good
Overlord health:       good
MiddleManager health:  good

Service name:          http
Service state:         running
Session timeout:       1800
Connection timeout:    30
Redirect host:         (not configured)
Client API rate limit: 100 requests/sec
Client API concurrency limit: 40
Global API concurrency limit: 199

Service name:          kafka
Service state:         running
Service health:        good

Service name:          liagent
Service state:         stopped

Service name:          mgmt-plane-bus
Service state:         stopped

Service name:          node-mgmt
Service state:         running

Service name:          nsx-config
Service state:         running

Service name:          nsx-message-bus
Service state:         stopped

Service name:          nsx-upgrade-agent
Service state:         running

Service name:          ntp
Service state:         running
Start on boot:         True

Service name:          pace-server
```

```

Service state:      running

Service name:       postgres
Service state:      running
Service health:     good

Service name:       processing
Service state:      running

Service name:       snmp
Service state:      stopped
Start on boot:      False

Service name:       spark
Service state:      running
Service health:     good

Service name:       spark-job-scheduler
Service state:      running

Service name:       ssh
Service state:      running
Start on boot:      True

Service name:       syslog
Service state:      running

Service name:       ui-service
Service state:      running

Service name:       zookeeper
Service state:      running
Service health:     good

my_nsx-intel>

```

Un service peut être à l'état en cours d'exécution ou arrêté. L'intégrité du service peut être satisfaisant ou dégradé.

- 3 Vous pouvez également afficher le fichier `syslog` et rechercher la sortie du script de vérification de l'intégrité `pace-monitor.sh` qui journalise l'intégrité des services NSX Intelligence dans le fichier `syslog`.

Si tous les services fonctionnent comme prévu, une sortie similaire à l'exemple de sortie suivant s'affiche après l'exécution de la commande `get log-file syslog | find pace-monitor`.

```

my_nsx-intel> get log-file syslog | find pace-monitor
<13>1 2019-08-30T03:19:20.409899+00:00 my_nsx-intel pace-monitor.sh - - -      "_self": {
<13>1 2019-08-30T03:19:20.410253+00:00 my_nsx-intel pace-monitor.sh - - -      "href": "/
node/pace/appliance-health",
<13>1 2019-08-30T03:19:20.410623+00:00 my_nsx-intel pace-monitor.sh - - -      "rel":
"self"
<13>1 2019-08-30T03:19:20.410908+00:00 my_nsx-intel pace-monitor.sh - - -      },

```



```

<13>1 2019-08-30T03:19:20.411162+00:00 my_nsx-intel pace-monitor.sh - - - "appliance-
health": {
<13>1 2019-08-30T03:19:20.411416+00:00 my_nsx-intel pace-monitor.sh - - - "status":
"Following NSX Intelligence first boot services are either PENDING or FAILED - Token-
Registration",
<13>1 2019-08-30T03:19:20.411668+00:00 my_nsx-intel pace-monitor.sh - - - "sub-system-
status": {
<13>1 2019-08-30T03:19:20.411923+00:00 my_nsx-intel pace-monitor.sh - - - "app-
services": {
<13>1 2019-08-30T03:19:20.412280+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [],
<13>1 2019-08-30T03:19:20.412528+00:00 my_nsx-intel pace-monitor.sh - - -
"status": ""
<13>1 2019-08-30T03:19:20.412807+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.413075+00:00 my_nsx-intel pace-monitor.sh - - - "base-
infra-services": {
<13>1 2019-08-30T03:19:20.413303+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [
<13>1 2019-08-30T03:19:20.413613+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.413848+00:00 my_nsx-intel pace-monitor.sh - - -
"druid-health": {
<13>1 2019-08-30T03:19:20.414146+00:00 my_nsx-intel pace-monitor.sh - - -
"broker": "good",
<13>1 2019-08-30T03:19:20.414473+00:00 my_nsx-intel pace-monitor.sh - - -
"coordinator": "good",
<13>1 2019-08-30T03:19:20.414717+00:00 my_nsx-intel pace-monitor.sh - - -
"historical": "good",
<13>1 2019-08-30T03:19:20.414979+00:00 my_nsx-intel pace-monitor.sh - - -
"middlemanager": "good",
<13>1 2019-08-30T03:19:20.415295+00:00 my_nsx-intel pace-monitor.sh - - -
"overlord": "good"
<13>1 2019-08-30T03:19:20.415533+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.415762+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "druid"
<13>1 2019-08-30T03:19:20.415982+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.416269+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.416539+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.416772+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "kafka"
<13>1 2019-08-30T03:19:20.416991+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.417204+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.417510+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.417745+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "postgres"
<13>1 2019-08-30T03:19:20.418133+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.418389+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.418626+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "good",
<13>1 2019-08-30T03:19:20.418855+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "spark"
<13>1 2019-08-30T03:19:20.419157+00:00 my_nsx-intel pace-monitor.sh - - - },
<13>1 2019-08-30T03:19:20.419435+00:00 my_nsx-intel pace-monitor.sh - - - {
<13>1 2019-08-30T03:19:20.419684+00:00 my_nsx-intel pace-monitor.sh - - -

```

```

"health": "good",
<13>1 2019-08-30T03:19:20.419928+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "zookeeper"
<13>1 2019-08-30T03:19:20.420165+00:00 my_nsx-intel pace-monitor.sh - - -      }
<13>1 2019-08-30T03:19:20.420496+00:00 my_nsx-intel pace-monitor.sh - - -      ],
<13>1 2019-08-30T03:19:20.420786+00:00 my_nsx-intel pace-monitor.sh - - -
"status": ""
<13>1 2019-08-30T03:19:20.421022+00:00 my_nsx-intel pace-monitor.sh - - -      },
<13>1 2019-08-30T03:19:20.421255+00:00 my_nsx-intel pace-monitor.sh - - -      "first-
boot-services": {
<13>1 2019-08-30T03:19:20.421539+00:00 my_nsx-intel pace-monitor.sh - - -
"services": [
<13>1 2019-08-30T03:19:20.421777+00:00 my_nsx-intel pace-monitor.sh - - -      {
<13>1 2019-08-30T03:19:20.422010+00:00 my_nsx-intel pace-monitor.sh - - -
"health": "degraded",
<13>1 2019-08-30T03:19:20.422277+00:00 my_nsx-intel pace-monitor.sh - - -
"service-name": "token-registration"
<13>1 2019-08-30T03:19:20.422512+00:00 my_nsx-intel pace-monitor.sh - - -      }
<13>1 2019-08-30T03:19:20.422770+00:00 my_nsx-intel pace-monitor.sh - - -      ],
<13>1 2019-08-30T03:19:20.423012+00:00 my_nsx-intel pace-monitor.sh - - -
"status": "Following NSX Intelligence first boot, services are either PENDING or FAILED
- Token-Registration"
<13>1 2019-08-30T03:19:20.423354+00:00 my_nsx-intel pace-monitor.sh - - -      }
<13>1 2019-08-30T03:19:20.423601+00:00 my_nsx-intel pace-monitor.sh - - -      }
<13>1 2019-08-30T03:19:20.423882+00:00 my_nsx-intel pace-monitor.sh - - -      }
<13>1 2019-08-30T03:19:20.424339+00:00 my_nsx-intel pace-monitor.sh - - -      }
<13>1 2019-08-30T03:19:20.972629+00:00 my_nsx-intel pace-monitor.sh - - - NSX
Intelligence health OK.
<30>1 2019-08-30T03:19:20.973076+00:00 my_nsx-intel pace-monitor 20804 - - <13>Aug 30
03:19:19 pace-monitor.sh: NSX Intelligence health OK.
<182>1 2019-08-30T03:23:23.857Z my_nsx-intel NSX 21752 - [nsx@6876 comp="nsx-cli"
subcomp="node-mgmt" username="admin" level="INFO"] CMD: get log-file syslog | find pace-
monitor

```

En cas de problème avec l'un des services, la ligne suivante peut s'afficher lorsque vous exécutez `get log-file syslog | grep pace-monitor`.

```
NSX Intelligence health DEGRADED. Return code not HTTP OK.
```

- 4 Si vous détectez l'une des sorties suivantes, redémarrez le service à l'aide de la commande `restart service service-name`.

- Après l'exécution de la commande `get services`, l'un des services affiche État du service : arrêté OU Intégrité du service : dégradé.
- Après l'exécution de la commande `get log-file syslog | grep pace-monitor`, la sortie indique une valeur semblable au message Intégrité de PACE DÉGRADÉE. Code de retour non HTTP OK..

Par exemple, si l'état du service `postgres` indique arrêté, ou si son état est en cours d'exécution, mais que son intégrité de service est dégradé, exécutez la commande suivante.

```
restart service postgres
```

Important Vous devez utiliser la commande `restart service service-name` pour redémarrer les services NSX Intelligence. Si vous décidez d'utiliser plutôt les commandes `stop service service-name` et `start service service-name`, vous devez également redémarrer manuellement chacun des services qui dépendent de `service-name`. La liste suivante montre l'ordre de dépendance dans lequel les services NSX Intelligence doivent être redémarrés.

```
zookeeper > druid > kafka > spark > spark-job-scheduler > nsx-config > processing > pace-server
```

Par exemple, si le service `nsx-config` est arrêté, puis démarré à l'aide de la commande `stop | start service service-name`, vous devez également utiliser la commande `restart service service-name` pour redémarrer les services `processing` et `pace-server`.

De plus, si vous utilisez la commande `restart service service-name` pour redémarrer les services affichés dans la liste des ordres de dépendance avant le service `spark-job-scheduler`, vous devez également redémarrer manuellement le service `spark-job-scheduler` à l'aide de la commande `restart service spark-job-scheduler`. Dans le cas contraire, le service `spark-job-scheduler` passe dans un état incorrect.

Collecter des bundles de support NSX Intelligence

Vous pouvez collecter un bundle de support à l'aide de l'interface de ligne de commande de NSX Intelligence.

Le contenu du fichier du bundle de support n'inclut pas de données. Il inclut des fichiers dans les répertoires suivants.

- `/opt/vmware/`*
- `/var/log/`*
- `/etc/`*
- État du système utilisant `journalctl` et `systemctl`

Conditions préalables

Assurez-vous que vous disposez d'un accès administrateur d'entreprise à l'interface de ligne de commande de NSX Intelligence.

Procédure

- 1 Connectez-vous à la CLI de NSX Intelligence à l'aide d'un compte disposant des privilèges du rôle d'administrateur d'entreprise.

2 Générez le bundle de support.

La syntaxe de la commande est la suivante, où vous fournissez la valeur de *support_filename.tgz*.

```
get support-bundle file support_filename.tgz
```

Par exemple,

```
get support-bundle file support_bundle123.tgz
```

Lorsque le fichier de bundle est correctement créé, vous recevez les messages similaires à l'exemple suivant.

```
support_bundle123.tgz créé, utilisez la commande suivante pour transférer le
fichier : copiez le fichier support_bundle123.tgz url <url> Après le transfert de
support_bundle123.tgz, extrayez-le à l'aide de tar xvf support_bundle123.tgz
```

3 Vérifiez que le bundle de support existe à l'aide de la commande suivante.

```
get files
```

Les résultats de la commande sont semblables aux suivants.

```
Directory of filestore:/
-rw- 21377586 June 29 05:29:12 UTC support_bundle123.tgz
```